Security Assumptions in Post-Quantum Cryptography

Romy Minko

Wolfson College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

September 2021

Abstract

This thesis analyses the assumptions present in security proofs of post-quantum cryptosystems using Koblitz and Menezes' critique [62] to guide the focus points. The classical analysis focusses in particular on isogeny-based and multivariate polynomial cryptosystems. Firstly, we present attacks against hardness assumptions on derivative computational problems arising in protocols for isogeny-based undeniable signature schemes [52, 80]. Secondly, we provide upper bounds on the solving degree of over-determined systems of $n + \ell$ multivariate polynomials in n variables as an alternative to the degree of regularity, which gives a heuristic upper bound. We finish with an analysis of the resources of a quantum adversary, providing an improved method for quantum gate approximation that gives shorter sequences by a factor of $\frac{9}{7}$.

Acknowledgements

I would like to thank the following people for their support throughout the four years of my DPhil.

- First and foremost, my supervisors: Dr Christophe Petit and Prof. Artur Ekert. Thank you for trusting me as your student, and for your ever-illuminating advice.
- To my collaborators, spread far and wide across the globe, thank you for providing a space to share my ideas, and listen to yours.
- To my family in Australia, thank you for going along with my dreams and always believing in me.
- To Dr Calvin Lee, I think I will go a lifetime trying to show my gratitude to you and still never quite measure up. You made my dream come true. Thank you from the bottom of my heart.
- To the good people at the Centre for Cyber Safety and Education, Palantir, the Australia Day UK Foundation and the Humanitarian Trust, thank you for your financial support throughout this journey.
- To Prof. Andrew Martin, David Hobbs and the rest of the CDT team, thank you for coordinating such a wonderful programme, for answering my endless emails and creating an unforgettable community.
- Finally, to all my friends in OUARFC and WCBC, thank you for keeping me sane for four years. The memories will last forever.

Statement of Originality

This is to certify that the content of this thesis is my own work and to the best of my knowledge contains no work that has been submitted or published elsewhere, except where due acknowledgement has been given.

I also declare that the intellectual content of this thesis is my own, where any assistance and collaboration in the preparation of the thesis has been explicitly acknowledged.

Romy M. Minko

Contents

List of Figures

Introduction

This thesis concerns assumptions that are made in assessing the security of post-quantum cryptosystems.

The field of post-quantum cryptography (PQC) arose as a response to the threat of quantum computers against legacy cryptosystems such as RSA. Before delving further into specifics, we quickly make the distinction between *classical* and *quantum* computers. Classical computers, or conventional computers, operate with binary bits and can be modelled by a probabilistic Turing machine. Quantum computers, as suggested by the name, operate using the principles of quantum mechanics and it is conjectured that some quantum algorithms cannot be efficiently simulated by a classical computer [72]. Similarly, post-quantum cryptography is not to be confused with quantum cryptography; the former refers to classical cryptosystems that are believed to be resistant to attacks by quantum computers (in addition to those from classical computers), while the latter refers to cryptosytems that employ the laws of quantum mechanics.

Of course, a practical quantum computer, capable of implementing Shor's algorithm for the parameters used in today's cryptosystems, does not yet exist, begging the question: Why should we study post-quantum cryptography if no feasible quantum threat exists? Firstly, it takes time to research, vet and implement new cryptosystems, particularly at scale. Secondly, certain applications, i.e. the encryption of medical data, require security that lasts for decades. Hence, having post-quantum cryptosystems already implemented at such a time that large-scale quantum computers do become a reality ensures robust security against a suite of attacks.

Post-quantum cryptography is still a relatively young field. Security definitions are continually evolving and, as attacks against established primitives improve, so too are security requirements. The framework of reductionist security, originally introduced by Goldwasser and Micali [43] as provable security, was established in response to the recognition that, although a cryptographic protocol may be based on some mathematical primitive, an attack on that protocol is not necessarily equivalent to solving the primitive. As a result, a hardness assumption made on the mathematical primitive may not imply security of the protocol. Reductionist security arguments are made by demonstrating the link between the problem of attacking a given cryptosystem and an intractable mathematical problem, known as a *reduction*. This thesis examines some of the flawed, or invalid, assumptions still occurring within this framework. Our approach is based on the influential paper of Koblitz and Menezes, *Another Look at Provable Security* [62]. The authors identify four primary points for the introduction of error within a security proof:

1. insufficient evidence to support a computational hardness assumption,
2. fallacies or gaps within the proofs,
3. incorrect characterisation of the resources of an adversary, and
4. implicit assumptions within the description of a protocol.

The focus of this thesis is on the first three points, identifying a concrete example of each, covering both classical or quantum perspectives. We have chosen multivariate polynomial and isogeny-based cryptography as case studies for the classical subcase. The security of multivariate cryptography is based on the hardness of solving a system of multivariate polynomial equations, but results in this area are often either asymptotic or based on heuristics. In the case of isogeny-based cryptography, newer schemes are often assumed to be secure, based on the hardness of the fundamental computational supersingular isogeny problem, while in actuality they depend on related computational problems. This can result in schemes that are assumed to be more secure than they actually are.

For the quantum analysis, we adapt a classical algorithm used for cryptanalysis against the CGL hash function [23] to the problem of improving resource efficiency.

Organisation of the Thesis

This thesis is organised as follows:

- In Chapter 1, we provide a more formative literature review of reductionist security proofs and identify the security assumptions that are the focus of the main body of the thesis.
- Chapter 2 presents a case study in isogeny-based cryptography, which illustrates the first of Koblitz and Menezes' identified issues in security proofs. We disprove a number of hardness assumptions of variants of the SSCDH problem [52], motivated by two proposed undeniable isogeny-based signature protocols [52, 80].
- We present an example of Koblitz and Menezes' second point, which occurs

in the space of multivariate public key cryptography, in Chapter 3. We look at the cost analysis of Gröbner basis attacks against multivariate encryption schemes and the assumptions implicit in current methods.

- The final chapter of this thesis deals with the characterisation of the resources of a quantum adversary, in terms of the gate-cost of implementing a quantum algorithm. In Chapter 4, we give an improved method for general unitary approximation techniques for a number of commonly used fault-tolerant gate sets.

These three areas of focus allow this thesis to cover both theoretic and practical approaches to reductionist security, with results for both classical and quantum cryptanalysis.

Main contributions

Several of the results in this thesis have been published. The papers are listed here:

- Simon-Philip Merz, Romy Minko, Christophe Petit. *Another look at some isogeny hardness assumptions.* In proceedings of Cryptography Track at RSA. San Francisco, 2020. `https://eprint.iacr.org/2019/950`
- Mina Bigdeli, Manuela Dizdarevic, Elisa Gorla, Emmanuela De Negri, Romy Minko, Sulaminthe Tsakou. *Semi-regular sequences and other random systems of equations.* In proceedings of Women in Numbers Europe 3. Rennes, 2020. `https://arxiv.org/abs/2011.01032`

Our main contributions are specific to isogeny-based cryptography, multivariate-polynomial cryptography and quantum information. More precisely:

- We present an attack against the One-sided Modified Supersingular Computational Diffie-Hellman (OMSSCDH) problem and the One-more Modified Supersingular Computational Diffie-Hellman (1MSSCDH) problem [52]. These give rise to examples of inherited security assumptions, defined in Section 1.2. We extend the attack to show that the parameters of the protocols in [52] and [80] must be increased to achieve the claimed level of security.
- We prove explicit bounds for the solving degree of over-determined systems of $n + \ell$ multivariate polynomials in n variables, denoted $r(n + \ell, n)$. These are proposed as alternatives to the degree of regularity of [3], are based on fewer assumptions and are not asymptotic. Explicit values of $r(n + \ell, n)$ for $2 \leq n, \ell \leq 100$ are given in Appendix A.
- We present a novel method for approximating an arbitrary single qubit unitary, which results in shorter approximation sequences by a factor of $\frac{9}{7}$.

Chapter 1

Post-quantum hardness assumptions

Post-quantum cryptographers must bridge the mathematical theory behind cryptography and the practical concerns of implementation, covering a wide range of applications (e.g. key encapsulation, signing, encryption). This task almost always necessitates the use of assumptions regarding computational hardness.

The purpose of this chapter is to give an introduction to the reductionist security[1] framework and to define, in general terms, the assumptions that are the central focus of this thesis.

Outline The key concepts underlying the reductionist security approach are defined in Section 1.1. This provides the foundation to identify our three cases of flawed assumptions. In Section 1.2, we define a set of hardness assumptions, namely, inherited hardness assumptions, often based on weak, or no, proofs. Section 1.3 then examines the potential error introduced by flawed assumptions in security proofs that make claims regarding concrete parameters. These first two

[1] Also known as provable security. The term 'reductionist security' was introduced by Bellare [6] and made commonplace by Koblitz and Menezes [62].

sections, and their corresponding chapters in the thesis body, are focussed on classical cryptanalysis of post-quantum cryptosystems. Quantum cryptanalysis concerns are addressed in Section 1.4, where we look at the characterisation of quantum adversaries, motivating this thesis' focus on the resource cost of quantum computation in Chapter 4.

1.1 Introduction to reductionist security

In order to make statements about the security of a cryptographic protocol, we need to consider the resources of a potential adversary and what constitutes a 'broken' protocol.

Let us begin by defining a *computational hardness assumption* as in [71]. Let P be a problem, with instances of size n, determined by some probability distribution. A hardness assumption is defined by n, the time it takes to solve a problem instance t and a probability of success p. Concretely, P is considered hard if no instance of size n can be solved in time less than t with probability greater than p. Therefore, an (n, t, p)-hardness assumption on P is the assumption that P is hard with respect to n, t and p.

Typically, within the reductionist security framework, adversaries are treated as algorithms running in polynomial time.

Definition 1.1.1 (Probabilistic polynomial-time adversary)**.** *A polynomial-time adversary is an algorithm $\mathcal{A}$ that terminates after $p(|x|)$ computations, where p is a polynomial and $x \in \{0,1\}^*$.*

A probabilistic polynomial-time (PPT) adversary additionally has access to a source of randomness that can be used polynomially many times in the adversary's *computation.*

A protocol is considered broken if an adversary's attack succeeds with non-negligible probability. That is, the probability of success should not be more than some negligible function in the security parameter λ for a scheme to be considered secure.

Definition 1.1.2 (Negligible function)**.** *A function f is negligible if for any positive constant c, there exists an $N_c \in \mathbb{N}$ such that for all $\lambda > N_c$, $f(\lambda) \leq \frac{1}{\lambda^c}$.*

Let us now consider a cryptographic reduction. Suppose that P_1 is the problem of breaking a given cryptosystem and let P_2 be an intractable mathematical problem. Let $\mathcal{A}$ be an algorithm for solving P_1. If there exists an algorithm $\mathcal{B}$ for solving P_2 that takes $\mathcal{A}$ as a subroutine, then we say there is a reduction from P_2 to P_1. If $\mathcal{B}$ is a polynomial-time algorithm, treating $\mathcal{A}$ as a black box, then an efficient solution for P_1 implies an efficient solution for P_2. Simply put, if P_2 hard, the reduction implies the hardness of P_1. From this description, it is clear that the burden of proof may be transferred from the hardness assumption

The protocol defining P_1 is secure against a PPT adversary.

to the hardness assumption

A PPT adversary cannot solve P_2 with non-negligible probability of success.

It follows that the veracity of the security proof based on the reduction between P_1 and P_2 can be judged by the quality of the second assumption. Explicitly, such a reduction proves that P_1 is at least as hard as P_2.

Quality of reductions One measure of the quality of a reduction is *tightness.* Suppose that problem P_2 reduces to problem P_1. Suppose that $\mathcal{A}$ takes time at most T_1 to solve problem P_1 and succeeds with probability at least p_1, then $\mathcal{B}$ finds a solution to problem P_2 in time at most T_2 and has success probability at least p_2. The reduction from P_2 to P_1 considered tight if $T_1 \approx T_2$ and $p_1 \approx p_2$. The ratio T_2p_2/T_1p_1 is called the tightness gap and clearly for a tight reduction, this takes a value close to 1. Chaterjee, Menezes and Sankar [24] have investigated the problems arising from large tightness gaps in cryptography.

An equally important property is the direction of a reduction. For two problems to be considered equivalent we require a tight two-way reduction: that is, P_1 reduces to P_2 and P_2 reduces to P_1, so the two problems are equivalent. In a security context, a reduction of this kind implies that that instead of breaking a protocol directly, cryptanalysts may as well focus on solving the underlying mathematical problem. If that problem is considered hard, one can say with confidence that the protocol is secure in the present.

However, one-way reductions, in which an attack on the protocol reduces to some mathematical problem but not *vice versa*, still arise in cryptography as we will see in Chapter 2.

Practice-oriented security Complexity-theoretic approaches to security express the hardness of a problem as an asymptotic function. While this is certainly useful to gain an understanding of the complexity of attacking a protocol, arguing solely based on asymptotics does not provide a complete description of security. Practice-oriented provable security was introduced by Bellare and Rogoway [6] in 1997 in an effort to align the perspectives of cryptography theoreticians and practitioners. That is, in order to make meaningful comparisons it became necessary to quantify explicitly the degree of security that competing schemes would offer.

As Mihir Bellare writes in [6],

> To make provable security useful, reductions and security analyses must be concrete. Theoreticians will say, correctly, that this information can be obtained by looking at their proofs. But this view obscures the importance of working on improving the security of reductions.

The exact characterisations of security coming from the practice-oriented methodology additionally served to shift the point at which practical concerns are addressed to far earlier in the protocol design process than the commencement of implementation.

Errors in reductionist security proofs Reductionist security proofs are not infallible. Koblitz and Menezes' published a thorough review of possible issues within the framework [62], followed a decade later by a comprehensive survey of papers addressing several of these issues in specific protocols [61]. The structure of this thesis is heavily informed by Koblitz and Menezes original critique, focussing on the following three points for the introduction of error in a reductionist security proof:

1. insufficient evidence to support a computational hardness assumption,
2. fallacies or gaps within the proofs, and
3. incorrect characterisation of the resources of an adversary.

1.2 Hardness assumptions based on weak evidence

Koblitz and Menezes highlighted an increasing tendency of cryptographers to rely on hardness assumptions for which there is little or no evidence. These assumptions are typically derived from non-standard problems, or variants of standard intractable problems. These problems are often artificial, constructed from the protocols they support, rather than naturally arising mathematical problems.

In this section we define a set of assumptions known as 'inherited hardness assumptions', an example of which is the focus of Chapter 2, and discuss the impact on security proofs.

1.2.1 Inherited hardness assumptions

We define a class of hardness assumptions, which we will call *inherited* hardness assumptions, that hinge on the existence of a one-way reduction, for which a reduction in the reverse direction is not known. Informally, an inherited hardness assumption arises when the conditions of a standard, or well-studied, mathematical problem are slightly modified and the resulting 'child' problem is assumed to be as hard to solve as the 'parent'.

Consider a problem statement P as a set of information $\mathcal{S}$ combined with a challenge $\mathcal{C}$. For instance, if P is the problem of factorising an RSA integer $N \in \mathbb{Z}$, then $\mathcal{S} = \{N\}$ and

$$\mathcal{C} = \text{“Find } p, q \text{ prime, such that } pq = N\text{”}.$$

Definition 1.2.1 (Inherited hardness assumption)**.** *Given a problem* $P = \{\mathcal{S}, \mathcal{C}\}$,

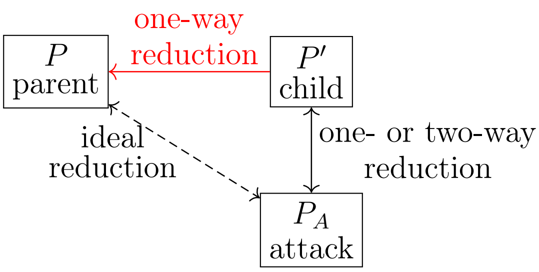

Figure 1.1: The reductions present in a cryptographic security argument based on an inherited hardness assumption. The parent problem, P, is a well-known intractable mathematical problem. The child problem, P', is a variant of P with the same challenge, but different conditions. The attack against the scheme is represented by P_A. Bold lines represent reductions that are present in the security proof. The dashed line represents the desired reduction, which motivates the inherited hardness assumption. Note also that the reduction between P_A and P' could be either one- or two- way.

let $P' = \{\mathcal{S}', \mathcal{C}'\}$ be a problem with information $\mathcal{S}' \subset \mathcal{S}$ and challenge $\mathcal{C} = \mathcal{C}'$. Suppose that there exists a reduction from P' to P, but no reduction in the reverse direction is known. An inherited hardness assumption states that

Solving P' is at least as hard as solving P.

When talking about inherited hardness assumptions in the context of cryptography, we consider protocols with security proofs in which

- there is a reduction from an attack on a protocol to some problem P', and
- the hardness of P' is based on an inherited hardness assumption.

.

Figure 1.1 illustrates the relationships between the three relevant problems. If the reduction between P' and the parent problem P is a one-way reduction, this causes issues for the security proof of the protocol. That is P', and by extension

P_A, may not be equivalent to solving P. Therefore, hardness of the parent problem does *not* imply security of the protocol.

How often do inherited hardness assumptions occur? Given the numerous applications for cryptography and the specific properties each must have, it is unsurprising that not every protocol reduces directly to a standard intractable problem. In fact, at the time of writing, MQDSS [26] is the only multivariate candidate for signature schemes in the NIST process for standardisation of post-quantum cryptography that reduces directly to the well-studied MQ-problem[2]. Several more examples are given in [61]. Note that while the definition of inherited hardness assumptions may seem as contrived as the problems it describes, we purposefully provide a definition distinct from arbitrary one-way reductions in order to emphasise the close relationship between the parent and child problems.

Additionally, we caution cryptanalysts against immediately dismissing protocols based on non-standard problems since lack of attention may result in later acceptance-by-default. Without clear, published disproofs of the flawed assumptions, those protocols employing them may serve as the foundation for future protocols. An example of this scenario is considered in Chapter 2.

1.3 Flawed approximations in security proofs

The previous section explored the impact that an incorrect hardness assumption can have on the validity of a security proof. As a result of this discussion, one may be tempted to conclude that a rigorously proven polynomial-time equivalence

[2] See Problem 3.2.1.

is enough to guarantee the security of a protocol. To understand where other issues may arise, we now focus on the second of Koblitz and Menezes' error points: fallacies, or gaps, within security proofs. In particular, we look at problems occurring when complexity-theoretic proofs are translated to proofs of concrete security parameters, identifying two main vectors of error in security analyses: the use of erroneous approximations and reliance on asymptotic analysis. These are motivated by a case study in multivariate cryptography analysed further in Chapter 3.

1.3.1 The impact of erroneous approximations

Unsurprisingly, computations based on flawed approximations are likely to induce errors in security analyses. We focus on those approximations that arise in practice-oriented provable security proofs.

Suppose a complexity statement depends on some parameter κ. Theoreticians have the freedom to argue in terms of κ, regardless of whether or not κ can be efficiently computed. Practitioners, on the other hand, obviously need concrete values. Hence, a problem arises when computing κ is difficult. Consider, for example, the complexity of the Hassidim-Harrow-Lloyd algorithm for quantum linear system solving [46], which depends on a value known as the condition number of a matrix[3]. For large matrices, it can be difficult to compute the condition number [31], in which case approximations must be used in order to estimate the algorithm's complexity.

A commonly used solution is to substitute κ by an approximation. However, if this approximation is based on a flawed assumption or an unproven heuristic,

[3] The condition number κ of a normal matrix M is the ratio of the largest and smallest eigenvalues of M. A matrix is normal if it commutes with its conjugate transpose.

the resulting security assessment inherits those flaws. The potential error often goes unacknowledged, as a heuristic or assumption may work for the first n tested instances, leading practitioners to believe it is true. However, there is still the possibility of failure on the $n + 1^{th}$ instance.

This thesis argues that, while heuristics are useful, approximations should be proven, although we acknowledge there are often feasibility issues here. This approach will serve to increase trust in the security of not only specific protocols, but the entire methodology of practice-oriented reductionist security.

1.3.2 Asymptotics and implementation

Now we turn to the potential divide between asymptotic security and practical security values. Practice-oriented security proofs enable comparisons between protocols and precise trade-off analysis between efficiency and security by determining an explicit quantification of the level of security provided. This approach exposes an issue in relying on asymptotic arguments: namely, a polynomial-time reduction between two problems might imply security for arbitrarily large parameters, but for parameters for which implementation is efficient, the reduction could be meaningless for security.

We note here that this kind of issue often occurs in conjunction with the previously raised issue of inaccurate approximations. That is, an approximation may only be 'good' for arbitrarily large parameters. Thus it is important to continue searching for good approximations that are within the realm of an implementation.

1.4 The quantum resources of an adversary

It would be remiss to conclude any discussion of post-quantum cryptography security without addressing the quantum perspective. Accordingly, we narrow the focus of Koblitz and Menezes third vector of error to consider the assumptions that are made regarding the computational resources of a *quantum* adversary.

The following section begins by defining computational complexity in the quantum setting. For results that are applicable to a number of applications (both in and out of cryptography), we focus in particular on the resource cost of quantum computers. Typically, this is measured by the number of quantum gates required to implement an algorithm. Throughout this section and Chapter 4 we use resource cost and gate cost interchangeably. The subsequent section discusses methods for decreasing resource costs in general.

1.4.1 Computational complexity with a quantum adversary

Let us begin by considering a new adversary who is now equipped with the resources of a quantum computer. Owing to the fact that physical realisations of quantum computers are still in their infancy, we must also consider the physical resources at the disposal of such an adversary. Where in the classical case we considered time- and space-complexity, we now also consider query-complexity and resource-complexity.

A quantum gate describes a transformation of a quantum state in the quantum circuit model, and can be represented by a unitary matrix[4]. Gate-complexity measures the number of single-qubit gates and two-qubit gates used in an algorithm[5].

[4] A matrix M is unitary if $MM^* = I$ where M^* denotes the conjugate transpose of M.

[5] In the quantum circuit model, time-complexity corresponds to the depth of a circuit: that

In order to make meaningful statements about gate-complexity for algorithms containing n-qubit unitaries, we also require a result from Barenco *et al.* [5], which states that any n-qubit unitary can be implemented by a circuit of c-NOT and single-qubit gates.

What does it mean to be efficient in terms of gate-complexity? It is necessary that a polynomial-time algorithm can be implemented with a polynomial number of gates? We introduce another measure of computational complexity, *query-complexity*, which is used to define relative efficiency of a quantum adversary. In the quantum query model, the input to an algorithm is considered as a black box oracle and the query-complexity is the number of queries to the oracle required for the algorithm to find a solution. Then, we define gate (time) efficiency as follows:

Definition 1.4.1 (Gate and Time Efficiency, [63])**.** *Let $\mathcal{A}$ be a quantum algorithm. Let Q denote the query-complexity of $\mathcal{A}$. We say that $\mathcal{A}$ is gate (time) efficient if the gate-complexity (time-complexity) of $\mathcal{A}$ is $p(Q)$ where p is a polynomial.*

We call $\mathcal{A}$ a quantum polynomial-time adversary if $\mathcal{A}$ terminates after $p(|x|)$ computations, where p is a polynomial and $x \in \{0,1\}^*$. Similarly, we call $\mathcal{A}$ a quantum polynomial-query adversary if $\mathcal{A}$ makes $p(|x|)$ queries to the input oracle, where p is a polynomial and $x \in \{0,1\}^*$.

We will focus on improving the resource costs of a quantum adversary.

1.4.2 Quantum gate approximation

A crucial distinction between quantum and classical computing is the possible vectors for error during computation. Quantum computers, operating on qubits,

is, the longest path in the circuit.

are susceptible to errors from environmental interference, or even internal errors caused by qubit-qubit interactions. Fault-tolerant quantum computing covers the method of computing that allows for a certain threshold of physical error, which can be corrected either after or throughout the computation. Using a practical fault-tolerant quantum device imposes restrictions on the single-qubit unitaries that can be implemented [72], importantly, that only a finite set of unitaries can be used. Thus, to implement arbitrary single-qubit unitaries we require that this finite set is a *universal* set of gates. Informally, this means that any unitary in $SU(2)$ can be approximated by a finite sequence of gates from the gate set.

A central problem of the field of quantum gate approximation is decreasing the sequence length for approximating an arbitrary unitary [47]. Clearly, a shorter sequence corresponds to a lower gate-complexity. The focus of Chapter 4 is on making improvements in quantum gate approximation for fault-tolerant gate sets. Importantly, this is protocol-independent, and so applies to existing and future quantum algorithms. Moreover, the results are applicable to any quantum algorithm, not only to those used in cryptanalysis.

Chapter 2

Inherited security in isogeny-based cryptography

Recall that an inherited hardness assumption is present in a situation in which an attack on a cryptosystem reduces to a mathematical problem that is identical to a well-studied intractable problem in its challenge (and desired outcome), but differs in terms of the initial conditions. As a result, this problem is assumed to have inherited the hardness of the well-known problem. This assumption is usually made with a proof of a one-way reduction, but often is stated with no proof at all.

To demonstrate the impact of inherited hardness assumptions on the security of post-quantum cryptosystems, we now look at an example from the isogeny-based cryptography family: undeniable signature schemes that are extensions of the Supersingular Isogeny Diffie-Hellman (SIDH) key exchange protocol. Koblitz and Menezes undertook a similar study of non-standard Discrete Logarithm and Diffie-Hellman problems [60], showing that in some cases no natural reductions existed. However, Granger [45] later demonstrated that the presence of an effective index calculus could be used to show that two problems have the same complexity, *even* in the absence of a reduction between them.

Results in this chapter are included in a paper written with Simon-Philip Merz and Christophe Petit, included in the Cryptographers' Track at the RSA Conference 2019 [69].

Outline and main contributions We begin by recalling some useful mathematical background. The SIDH protocol, the hardness problem it relies on for security, and A number of variants of this problem are then defined in Section 2.2. There are two examples of signature schemes relying on these problems. These are described in Section 2.3 and we discuss the security proofs, proving two false assumptions, one of which is an inherited hardness assumption. The other assumption comes from the failure to consider the effect of a hash function in the protocol. The proof of falseness is presented in Section 2.4, with an attack against the problem variants, which extends to an attack on the signatures schemes, given in Section 2.5. The chapter ends with a discussion of the impact on the security of the two schemes.

2.1 Preliminaries

For a thorough background on elliptic curves we refer to Silverman [79]. For an introduction to isogeny-based cryptography we refer to De Feo [30].

Let $\mathbb{F}_q$ be a finite field of characteristic p. In this thesis, we assume $p > 3$. Therefore, an elliptic curve E over $\mathbb{F}_q$ can be defined by its short Weierstrass form.

Definition 2.1.1 (Weierstrass Equation). *An elliptic curve over a finite field* $\mathbb{F}_q$

is defined as

$$E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q^2 \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}_E\}$$

where $A, B \in \mathbb{F}_q$ *such that* $4A^3 + 27B^2 \neq 0$ *and* $\mathcal{O}_E$ *is the point* $(X : Y : Z) = (0 : 1 : 0)$ *on the projective curve* $Y^2Z = X^3 + AXZ^2 + BZ^3$*.*

The set of points on an elliptic curve is an abelian group with the following group operation:

Definition 2.1.2 (Group operation on the points on an elliptic curve)**.** *Let* $P, Q \in E$ *and let* L *be the line joining* P *and* Q*. Let the third point of intersection of* L *with* E *be denoted* R*. Let* L' *be the line joining* R *and* $\mathcal{O}_E$ *and let the third point of intersection of* L' *with* E *be* R'*. The group operation* $\oplus$ *is defined as* $P \oplus Q = R'$*.*

The identity element of the group is the point at infinity, $\mathcal{O}_E$. The number of points on an elliptic curve is $\#E(\mathbb{F}_q) = q + 1 - t$ for some integer $|t| \leq 2\sqrt{q}$.

Definition 2.1.3. *The j-invariant of an elliptic curve is*

$$j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2}.$$

Two curves E_1 and E_2 are isomorphic if and only if $j(E) = j(E')$.

Definition 2.1.4. *Given two elliptic curves* E_1 *and* E_2 *over a finite field* $\mathbb{F}_q$*, an isogeny is a surjective group homomorphism* $\phi : E_1 \to E_2$*.*

That is, $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$. For example, the multiplication by n map on an elliptic curve $[n] : E \to E$ given by $[n](P) = nP$ is an isogeny. Two important computational problems for elliptic curve cryptography that relate to the multiplication by

n map are the elliptic curve discrete logarithm problem and the extended elliptic curve discrete logarithm problem:

Problem 2.1.5 (Elliptic Curve Discrete Logarithm Problems)**.** *Given $P, Q \in E$, such that $Q = [n]P$ for some integer n, the elliptic curve discrete logarithm problem is to find n.*

Given a set of points P_i in E and a point $R \in E$ such that $R = \sum_i [n_i]P_i$, the extended elliptic curve discrete logarithm problem is to find the n_i.

Let $\phi : E_0 \to E_1$ be an isogeny between curves over $\bar{\mathbb{F}}_q$ and let ϕ^* be the function field injection induced by composition with ϕ:

$$\phi^* : \bar{\mathbb{F}}_q(E_1) \to \bar{\mathbb{F}}_q(E_0), \qquad \phi^*(f) = f \circ \phi.$$

The degree of an isogeny is the degree of the finite extension of function fields $\bar{\mathbb{F}}_q(E_0)/\phi^*(\bar{\mathbb{F}}_q(E_1))$. The degree can also be taken as the degree of the isogeny when considered as a rational map. Two curves are called *ℓ-isogenous* if there exists a non-constant isogeny of degree ℓ between them. The endomorphism ring $\mathrm{End}(E)$ of E is the set of all isogenies from E to E.

An isogeny is called *separable* if the finite extension $\bar{\mathbb{F}}_q(E_0)/\phi^*(\bar{\mathbb{F}}_q(E_1))$ is separable. If ϕ is a separable isogeny, then $\# \ker(\phi) = \deg(\phi)$. Since an isogeny defines a group homomorphism $E_1 \to E_2$, its kernel is a subgroup of E_1.

Theorem 2.1.6 (Proposition III.4.12, [79])**.** *Let S be a finite subgroup of an elliptic curve E. Then S determines a (separable) isogeny $\phi : E \to E'$ with $\ker(\phi) = S$ and $E' = E/S$.*

An isogeny is called cyclic if its kernel is a cyclic group. This will be the case for all isogenies considered in this thesis. Given a set of points describing the kernel, one can compute the isogeny using Vélu's formulas [84].

Theorem 2.1.7 (Theorem III.6.1, [79])**.** *Given any non-constant isogeny $\phi : E_1 \to E_2$, there exists a unique isogeny $\hat{\phi}$, called the dual isogeny, satisfying*

$$\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = [\deg(\phi)].$$

The n-torsion subgroup of a curve E is defined as

$$E[n] = \{P \in E(\overline{\mathbb{F}_q}) : [n]P = \mathcal{O}_E\}.$$

In other words, $E[n]$ is the kernel of the multiplication by n map over the algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$. For $n \geq 2$ relatively prime to p, the group $E[n]$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Definition 2.1.8. *An elliptic curve E over a finite field $\mathbb{F}_q$ for $q = p^k$ is called supersingular if any of the following hold:*

- $E[p^i] = \{\mathcal{O}\}$.
- $p \mid t$, *where* $\#E(\mathbb{F}_q) = q + 1 - t$ *for some integer* $|t| \leq 2\sqrt{q}$.
- *End*(E) *is isomorphic to an order in a quaternion algebra.*
- $j(E) \in \mathbb{F}_{p^2}$.

The equivalence of the above definitions of a supersingular curve is proved in Theorem V.3.1 of Silverman [79]. A curve that is not supersingular is called *ordinary*.

Charles, Goren and Lauter [23] introduced the idea of supersingular isogeny graphs.

Definition 2.1.9. *For a prime $\ell \neq p$, the ℓ-isogeny graph is the graph whose vertices are the isomorphism classes of all isogenous curves over the closure $\bar{\mathbb{F}}_q$ and whose edges are the ℓ-isogenies between elliptic curves.*

Note that since vertices are isomorphism classes, isogenies that differ by composition with an isomorphism correspond to the same edge. Vertices can also be labelled by the j-invariant of any elliptic curve within the corresponding isomorphism class. The graph is connected [22, Theorem 4.1], $(\ell + 1)-$regular [30, Proposition 3.5]. A supersingular isogeny graph has approximately $\lfloor \frac{p}{12} \rfloor$ edges [79, Theorem V.4.1].

2.2 Isogeny hardness assumptions

The Supersingular Computational Diffie-Hellman (SSCDH) problem is fundamental to the security of SIDH and many isogeny-based cryptosystems and signature schemes. We start with a description of the SIDH protocol, after which the second part of this section will motivate and illustrate some derivatives of the SSCDH problem, which, although seemingly artificial, are used in the security proofs of isogeny-based signature schemes (namely, [52, 80]). These problems are assumed to have inherited the hardness of SSCDH and are thus conjectured to be hard.

Throughout this section, let p be a prime of the form $\ell_A^{e_A} \ell_B^{e_B} \cdot f \pm 1$ where ℓ_A and ℓ_B are small distinct primes, e_A and e_B are positive integers and f is some small cofactor. Let E be a supersingular elliptic curve defined over the field $K = \mathbb{F}_{p^2}$ and let $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$ be fixed bases of the $\ell_A^{e_A}$ and $\ell_B^{e_B}$ torsions of E, $E[\ell_A^{e_A}]$ and $E[\ell_B^{e_B}]$, respectively.

2.2.1 The SIDH protocol

The SIDH protocol was created in 2014 by De Feo, Jao and Plût [51]. The basic mechanics of this protocol form the basis for the two undeniable signature schemes that are cryptanalysed in Section 2.5.

The SIDH key exchange between two users, Alice and Bob, is described by the following protocol.

SIDH Key Exchange Protocol [51]

$$\begin{array}{lcl}
\textbf{Alice} & & \textbf{Bob} \\
m_A, n_A \overset{\$}{\leftarrow} \mathbb{Z}/\ell_A^{e_A} & & m_B, n_B \overset{\$}{\leftarrow} \mathbb{Z}/\ell_B^{e_B} \\
E_A \leftarrow E/\langle [m_A]P_A + [n_A]Q_A \rangle & & E_B \leftarrow E/\langle [m_B]P_B + [n_B]Q_B \rangle \\
\ker(\phi_A) \leftarrow \langle [m_A]P_A + [n_A]Q_A \rangle & & \ker(\phi_B) \leftarrow \langle [m_B]P_B + [n_B]Q_B \rangle \\
P'_A, Q'_A \leftarrow \phi_A(P_B), \phi_A(Q_B) & & P'_B, Q'_B \leftarrow \phi_B(P_A), \phi_B(Q_A) \\
 & \xrightarrow{P'_A, Q'_A} & \\
 & \xleftarrow{P'_B, Q'_B} & \\
\ker(\phi'_A) \leftarrow \langle [m_A]P'_B + [n_A]Q'_B \rangle & & \ker(\phi'_B) \leftarrow \langle [m_B]P'_A + [n_B]Q'_A \rangle \\
E_{AB} \leftarrow E_B/\ker(\phi'_A) & & E_{BA} \leftarrow E_A/\ker(\phi'_B) \cong E_{AB} \\
\mathsf{sk} \leftarrow j(E_{AB}) & & \mathsf{sk} \leftarrow j(E_{BA}) = j(E_{AB})
\end{array}$$

Alice selects integers $m_A, n_A \in \{0, \ldots, \ell_A^{e_A} - 1\}$, not both divisible by ℓ_A defining the cyclic subgroup $A := \langle [m_A]P_A + [n_A]Q_A \rangle$ of $E[\ell_A^{e_A}]$, as her secret key. These parameters define the secret isogeny $\phi_A : E \to E/A$. Alice's public key is the curve $E_A := E/A$ together with the images $\phi_A(P_B), \phi_A(Q_B)$ of the public basis $\{P_B, Q_B\}$ under her secret isogeny $\phi_A : E \to E/A$. Analogously, Bob chooses his secret key $m_B, n_B \in \{0, \ldots, \ell_B^{e_B} - 1\}$, not both divisible by ℓ_B, defining the cyclic subgroup $B := \langle [m_B]P_B + [n_B]Q_B \rangle \subset E[\ell_B^{e_B}]$, and isogeny $\phi_B : E \to E/B$, and his public key is the tuple $(E_B, \phi_B(P_A), \phi_B(Q_A))$.

Upon receipt of Bob's public key, Alice computes an isogeny $\phi'_A : E_B \to E_{AB}$ with kernel $\langle [m_A]\phi_B(P_A) + [n_A]\phi_B(Q_A) \rangle \subset E/B[\ell_A^{e_A}]$. Bob proceeds analogously, computing the isogeny $\phi'_B : E_A \to E_{AB}$ with kernel $\langle [m_B]\phi_A(P_B) + [n_B]\phi_A(Q_B) \rangle \subset E/A[\ell_B^{e_B}]$. Theorem 2.2.1 shows that the curves computed by Alice and Bob in this manner are isomorphic. Then, since curves belonging to the same isomorphism class have the same the j-invariant, Alice and Bob are able to compute a shared secret: $j(E_{AB})$.

Theorem 2.2.1. *Using the above notation for the SIDH protocol,*

$$E_{AB} := E/\langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B \rangle \cong E_A/\ker(\phi'_B) \cong E_B/\ker(\phi'_A).$$

Proof. We first show that $E_{AB} \cong E_B/\ker(\phi'_A)$. Observe that

$$\phi_B(A) = \phi_B(\langle [m_A]P_A + [n_A]Q_A \rangle) = \langle [m_A]\phi_B(P_A) + [n_A]\phi_B(Q_A) \rangle$$

and so

$$E_B/\ker(\phi'_A) = (E/B)\,/\phi_B(A).$$

Note that $\phi_B(A)$ is isomorphic to A by the First Isomorphism Theorem and the fact that the degree of ϕ_B is coprime to the order of A. Similarly, the subgroups B and A have coprime order. Hence, they are disjoint and so $\langle B, A \rangle := B + A$ is a well-defined subgroup of E of order $\ell_B^{e_B}\ell_A^{e_A}$. It follows that

$$(E/B)\,/\phi_B(A) \cong E/\langle B, A \rangle.$$

Trivially, $\langle B, A\rangle = \langle A, B\rangle$ and so $E_{AB} \cong E_B/\ker(\phi'_A)$.

Showing that $E_A/\ker(\phi'_B) \cong E_{AB}$ is analogous. □

$$\begin{tikzcd}
 & E_A = E/A \arrow[rd, "\phi'_B"] \arrow[dd, dashed, shift left, "\begin{matrix}\phi_B(P_A)\\ \phi_B(Q_A)\end{matrix}"] & \\
E \arrow[ru, "\phi_A"] \arrow[rd, "\phi_B"'] & & E_{AB} = E/\langle A, B\rangle \\
 & E_B = E/B \arrow[ru, "\phi'_A"'] \arrow[uu, dashed, shift left, "\begin{matrix}\phi_A(P_B)\\ \phi_A(Q_B)\end{matrix}"] &
\end{tikzcd}$$

Figure 2.1: The commutative diagram of the SIDH key exchange. Items in blue are known only to Alice and items and in red are known only to Bob.

The hardness of the following problem underlies the security of the SIDH protocol.

Problem 2.2.2 (Supersingular Computational Diffie-Hellman (SSCDH) Problem, [51])**.** *Let m_A, n_A be chosen at random from $\{0, \ldots, \ell_A^{e_A} - 1\}$ not both divisible by ℓ_A. Let m_B, n_B be randomly chosen from $\{0, \ldots, \ell_B^{e_B} - 1\}$ not both divisible by ℓ_B. Furthermore, let $\phi_A : E \to E_A$ and $\phi_B : E \to E_B$ denote the isogenies with kernel $\langle [m_A]P_A + [n_A]Q_A\rangle$ and $\langle [m_B]P_B + [n_B]Q_B\rangle$ respectively.*

Given the curves E_A, E_B and the points $\phi_A(P_B)$, $\phi_A(Q_B)$, $\phi_B(P_A)$ and $\phi_B(Q_A)$, find the j-invariant of

$$E_{AB} = E/\langle [m_A]P_A + [n_A]Q_A,\ [m_B]P_B + [n_B]Q_B\rangle.$$

The hardness of SSCDH is assumed from the presumed hardness of the Computational Supersingular Isogeny (CSSI) problem [51], which is rephrased here as the following assumption:

Assumption 2.2.3 (Computational Supersingular Isogeny (CSSI) Assumption). Let E and E_A be isogenous supersingular curves with isogeny $\phi_A : E \to E_A$, such that $\ker(\phi_A) = \langle [m_A]P + [n_A]Q \rangle$ for some m_A, n_A chosen uniformly at random from $\mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$, not both divisible by ℓ_A. Given E, E_A and two points $\phi_A(P), \phi_A(Q)$, it is infeasible for a polynomial-time adversary to find a generator for $\ker(\phi_A)$.

Clearly, an adversary able to solve the CSSI problem would be able to solve SSCDH. This is an example of a one-way reduction. A decisional variant of SSCDH is also defined in [51].

Problem 2.2.4 (Supersingular Decision Diffie-Hellman (SSDDH) Problem). *Let $E, m_A, n_A, m_B, n_B, \phi_A, \phi_B, E_A, E_B, P_A, Q_A, P_B, Q_B$ be as in the SSCDH problem. Given a curve E' sampled with probability $\frac{1}{2}$ from*

$$E_{AB} = E/\langle [m_A]P_A + [n_A]Q_A,\ [m_B]P_B + [n_B]Q_B \rangle$$

and

$$E_C = E/\langle [m'_A]P_A + [n'_A]Q_A,\ [m'_B]P_B + [n'_B]Q_B \rangle,$$

where m'_A, n'_A are selected at random from $\{0, \ldots, \ell_A^{e_A} - 1\}$ and m'_B, n'_B are selected at random from $\{0, \ldots, \ell_B^{e_B} - 1\}$, determine whether $E' = E_{AB}$ or $E' = E_C$ up to isomorphism.

2.2.2 Variants of the SSCDH problem

The following problems are somewhat natural variants of the SSCDH and SSDDH problems underlying the security of SIDH. The notation used for those problems is fixed throughout this section.

The SSCDH problem imagines a scenario in which Alice and Bob are both honest participants in the protocol and a third-party adversary, Eve, is attempting to gain the shared secret without knowledge of any secrets. Suppose instead that Eve has compromised Bob somehow, and is given partial access to his secret but still receives no secret information from Alice, nor any of her auxiliary points. This scenario gives rise to the following problem:

Problem 2.2.5 (Modified SSCDH (MSSCDH) Problem [52]). *Given E, E_A, E_B and $\ker(\phi_B)$, determine E_{AB} up to isomorphism, i.e. $j(E_{AB})$.*

Note that knowledge of $\ker(\phi_B)$ is equivalent to knowledge of ϕ_B. However, since Eve lacks any information regarding the auxiliary points in the image of ϕ_A, she is unable to compute the final edge in the commutative diagram. The following problem states the decisional variant of MSSCDH.

Problem 2.2.6 (Modified SSDDH (MSSDDH) Problem [52]). *Given E, E_A, E_B and a challenge curve E_C and $\ker(\phi_B)$, determine whether $E_{AB} = E_C$.*

Suppose now that Eve has access to an oracle with the ability to solve MSSCDH for any input curve and isogeny kernel, save a small number of exceptions. Then, to find E_{AB} Eve can solve the following problem, illustrated in Figure 2.2:

Problem 2.2.7 (One-sided Modified SSCDH (OMSSCDH) Problem [52]). *For fixed E, E_A, E_B, given an oracle to solve MSSCDH for E_A, $E_{B'}$, $\ker(\phi_{B'})$ with $E_{B'}$ not isomorphic to E_B and $\ell_B^{e_B}$-isogenous to E, solve MSSCDH for E_A, E_B and $\ker(\phi_B)$.*

We will see that the OMSSCDH problem arises naturally in the security analysis of undeniable signatures proposed in [52]. The authors also define a decisional variant of this problem.

$$\begin{tikzcd}
 & & E \arrow[dll, "\phi_A"'] \arrow[dr, "\phi_B"] \arrow[drr, "\phi_{B'}"] & & \\
E_A \arrow[drr, "\phi'_B"] \arrow[ddrr, "\phi'_{B'}"'] & & & E_B \arrow[dl, "\phi'_A"'] & E_{B'} \arrow[ddll, "\phi''_A"] \\
 & & E_{AB} & & \\
 & & E_{AB'} & &
\end{tikzcd}$$

Figure 2.2: The commutative diagram for OMSSCDH. The oracle provides $E_{AB'}$ for any $E_{B'}$ and $\phi_{B'}$, while E_{AB} is the solution curve to OMSSCDH for E_A, E_B and $\ker(\phi_B)$.

Problem 2.2.8 (One-sided Modified SSDDH (OMSSDDH) Problem [52])**.** *For fixed E_A, E_B and E_C, given an oracle to solve MSSCDH for E_A, $E_{B'}$, $\ker(\phi_{B'})$ with $E_{B'}$ not isomorphic to E_B and $\ell_B^{e_B}$-isogenous to E, solve MSSDDH for E_A, E_B, E_C and $\ker(\phi_B)$.*

Suppose, once more, that Eve has access to an oracle, which solves MSSCDH for any input, but that she only has a fixed number of queries available to her. While this scenario may seem more artificial, it is present in the following problem, which is used in the construction of undeniable blind signatures [80]:

Problem 2.2.9 (One-More SSCDH (1MSSCDH) Problem [80])**.** *Let E be some base curve of the form as in the SIDH protocol and let m_A, n_A be secret integers in $\{0, \ldots, \ell_A^{e_A} - 1\}$.*

Let a signing oracle respond with $E_{AB} \cong E_B/\langle [m_A]P_B + [n_A]Q_B \rangle$ upon receipt of a curve E_B isogenous to E and points P_B, Q_B spanning $E_B[\ell_B^{e_B}]$.

The 1MSSCDH problem is to produce at least $q+1$ distinct pairs of curves (E_{B_i}, E_{AB_i}), where E_{B_i} are $\ell_B^{e_B}$-isogenous to E, P_{B_i} and Q_{B_i} span $E_{B_i}[\ell_B^{e_B}]$ and E_{AB_i} is isomor-

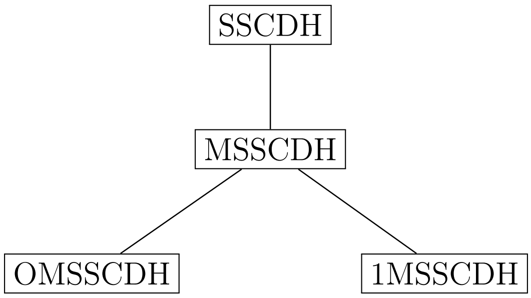

Figure 2.3: Hierarchy of isogeny problems.

phic to $E_{B_i}/\langle [m_A]P_{B_i} + [n_A]Q_{B_i}\rangle$ *for* $1 \leq i \leq q+1$*, after* q *queries to the signing oracle.*

This problem is slightly weaker than OMSSCDH, as it gives the adversary the freedom to choose the additional MSSCDH instance which needs to be solved.

Figure 2.3 shows the parent-child relationship between SSCDH and its variants.

2.3 Isogeny-based undeniable signature schemes

The significance of the SSCDH variants defined in Section 2.2.2 may not be immediately obvious. This section motivates the study of these problems by placing them in the context of two isogeny-based undeniable signature schemes.

Undeniable signature schemes were introduced by Chaum and van Antwerpen [25], differing from traditional signature schemes in that verification of a signature cannot be completed without cooperation from the signer. Undeniability refers to the fact that a signer cannot use the disavowal protocol to deny a valid signature. A signer is also unable to convince the verifier that an invalid signature is valid. Following the notation of [66] an undeniable signature scheme is denoted by Σ where

$$\Sigma = \{\texttt{KeyGen}, \texttt{Sign}, \texttt{Check}, \texttt{Sim}, \pi_{con}, \pi_{dis}\}.$$

`KeyGen` is the PPT (probabalistic polynomial time) key generation algorithm, which outputs (*vk, sk*) - a verification and signing key, respectively. `Sign` is the PPT signing algorithm, taking a message m and *sk* as input to generate a signature σ. `Check` is a deterministic validity checking algorithm, such that Check((*vk,m,σ*),*sk*) returns 1 if (m, σ) is a valid message-pair and 0 if not. `Sim` is a PPT algorithm outputting a simulated signature σ' on input of *vk* and m. Finally, π_{con} and π_{dis} are confirmation and disavowal protocols, respectively, with which the signer can prove the validity (or invalidity) of a signature to the verifier. These are zero-knowledge interactive protocols.

The security definitions of unforgeability and invisibility, both of which must be met for such signature schemes to be considered secure, give rise to the OMSS-CDH and 1MSSCDH problems. The security games defining these properties are described in Section 2.3.1.

This section describes two isogeny-based signature schemes: firstly, the Jao-Soukharev protocol [52] (Section 2.3.2) and, secondly, the Srinath-Chandrasekaran protocol [80] (Section 2.3.4), which extends [52] to include the additional property of blindness. This description includes an appraisal of the security proofs given by the respective authors and identifies the hardness assumptions being made; these will be shown to be false in later sections.

2.3.1 Unforgeability and invisibility

A signature scheme must be shown to satisfy the unforgeability and invisibility properties in order to be considered secure. These properties are defined by the following security games, following the descriptions in [29, 25, 66].

Unforgeability is the notion that an adversary cannot compute a valid message-signature pair with non-negligible probability.

1. The challenger generates a key pair, giving the verification key to the adversary.
2. The adversary is given access to a signing oracle and makes queries adaptively with messages m_i, for $i = 1, 2, \ldots, k$, for some k, receiving corresponding signatures σ_i.
    (a) The adversary additionally has access to a confirmation/disavowal oracle for the protocol, which they can query adaptively with message-signature pairs throughout step 2.
3. The adversary outputs a pair (m, σ).

The adversary wins the game (i.e. successfully forges a signature) if (m, σ) is a valid message-signature pair and $m \neq m_i$ for any $i = 1, 2, \ldots k$. A signature scheme is *unforgeable* if any PPT adversary wins with only negligible probability.

Invisibility requires that an adversary cannot distinguish between a valid signature and a simulated signature with non-negligible probability.

1. The challenger generates a key pair, giving the verification key to the adversary.

2. The adversary is given access to a signing oracle and makes queries adaptively with messages m_i, for $i = 1, 2, \ldots, k$, for some k, receiving corresponding signatures σ_i.
   (a) The adversary additionally has access to a confirmation/disavowal oracle for the protocol, which they can query adaptively with message-signature pairs throughout step 2.
3. The adversary sends a new message m_j to the challenger.
4. The challenger computes a random bit b. If $b = 1$, the challenger computes $\sigma = \texttt{Sign}(m_j, sk)$. If $b = 0$ the challenger computes $\sigma = \texttt{Sim}(m_j, vk)$. The challenger sends σ to the adversary.
5. The adversary is able to query the signing oracle again, with access to the confirmation/disavowal oracles. They cannot submit (m_j, σ) to either oracle.
6. The adversary outputs a bit b^*.

The adversary wins the game if $b^* = b$. An undeniable signature scheme is *invisible* if $|\Pr(b = b^*) - 1/2\ |$ is negligible.

2.3.2 The Jao-Soukharev protocol

The first undeniable signature scheme considered in this chapter was proposed by Jao and Soukharev in 2014 [52]. The Jao-Soukharev protocol, as it is referred to herein, was the second quantum-resistant undeniable signature scheme to exist in the literature, and the first using isogenies.

A set up for the protocol differs slightly from SIDH. Let p be a prime of the form $\ell_A^{e_A} \ell_B^{e_B} \ell_C^{e_C} \cdot f \pm 1$, where ℓ_A, ℓ_B, ℓ_C are primes and f is a small cofactor. In practice, f is usually taken to be 1. Let E be a supersingular curve over $\mathbb{F}_{p^2}$ and let $\{P_A, Q_A\}$, $\{P_B, Q_B\}$ and $\{P_C, Q_C\}$ be bases of the $\ell_A^{e_A}, \ell_B^{e_B}$ and $\ell_C^{e_C}$ torsions of E, $E[\ell_A^{e_A}], E[\ell_B^{e_B}]$ and $E[\ell_C^{e_C}]$, respectively. The public parameters of the scheme are p, E and the three torsion bases, together with a cryptographic hash function $H : \{0,1\}^* \to \mathbb{Z}/\ell_B^{e_B}$.

The signer generates random integers $m_A, n_A \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ and computes the isogeny $\phi_A : E \to E_A = E/\langle [m_A]P_A + [n_A]Q_A \rangle$, defined as in Problem 2.2.2. The public key consists of the curve E_A together with the points $\{\phi_A(P_C), \phi_A(Q_C)\}$ and the integers m_A, n_A constitute the private key. Note that this is equivalent to taking ϕ_A as the private key.

Signing To sign a message M, the signer computes the hash $h = H(M)$ of the message and the isogenies

$$\begin{aligned} \phi_B : E &\to E_B = E/\langle P_B + [h]Q_B \rangle \\ \phi_{AB} : E_A &\to E_{AB} = E_A/\langle \phi_A(P_B + [h]Q_B) \rangle \\ \phi_{BA} : E_B &\to E_{AB} = E_B/\langle \phi_B([m_A]P_A + [n_A]Q_A) \rangle. \end{aligned}$$

The signer then outputs E_{AB} and the set of two auxiliary points,

$$\{\phi_{BA}(\phi_B(P_C)), \phi_{BA}(\phi_B(Q_C))\},$$

as the signature σ.

Confirmation and disavowal Given a signature $\sigma = (E_\sigma, P, Q)$, the first step in the confirmation and disavowal protocols is for the signer to select $m_C, n_C \in$

$$\begin{tikzcd}
E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E_A \arrow[d, "\phi_{AB}"] \\
E_B \arrow[r, "\phi_{BA}"] & E_{AB}
\end{tikzcd}$$

Figure 2.4: The commutative isogeny diagram for signing in the Jao-Soukharev Protocol.

$\mathbb{Z}/\ell_C^{e_C}\mathbb{Z}$ and compute the four curves: $E_C = E/\langle [m_C]P_C + [n_C]Q_C \rangle$ and $E_{AC} = E_A/\langle \phi_A([m_C]P_C + [n_C]Q_C)\rangle$ with their blinded pairs $E_{BC} = E_B/\langle \phi_B([m_C]P_C + [n_C]Q_C)\rangle$ and $E_{ABC} = E_{BC}/\langle \phi_B([m_A]P_A + [n_A]Q_A)\rangle$. The signer outputs these curves and $\ker(\phi_{CB})$ as the commitment, where ϕ_{CB} is the isogeny from E_C to E_{BC}. In addition to the auxiliary points of the signature, this commitment gives the verifier enough information to compute E_{ABC} and $E_{\sigma C} = E_\sigma/\langle [m_C]P + [n_C]Q\rangle$, to check whether $E_{\sigma C} \cong E_{ABC}$.

The confirmation and disavowal protocols are not affected by our attacks, so we do not go in to further detail here. The interested reader can find an in-depth description, as well as proof of zero-knowledge, in [52].

2.3.3 Analysing the security proof of Jao-Soukharev

In [52] the claim is made that forging a signature for this construction is equivalent to solving OMSSCDH. The authors themselves note that OMSSCDH is not well studied. Nevertheless, they argue that the hardness of MSSCDH justifies the hardness of OMSSCDH, captured by the following assumption:

Assumption 2.3.1. Based on the intractability of the MSSCDH problem, the OMSSCDH problem is intractable for a polynomial-time adversary.

This is a case of an inherited hardness assumption. The information given for the MSSCDH problem is $\mathcal{S} := \{E, E_A, E_B, \ker(\phi_B)\}$ and the information given for the OMSSCDH problem is $\mathcal{S}' := \{E, E_A, E_B, \ker(\phi_B), \text{MSSCDH oracle}\}$, so certainly $\mathcal{S} \subset \mathcal{S}'$. Both problems have the same challenge: $\mathcal{C} = \text{Find } j(E_{AB})$.

The hardness of OMSSCDH is examined in Section 2.4. Here we scrutinise the related, protocol-specific assumption:

Assumption 2.3.2. Unforgeability and invisibility in the Jao-Soukharev protocol are equivalent to OMSSCDH.

In the Jao-Soukharev protocol, the adversary knows E_A and can compute E_{B_i} and $\ker(\phi_{B_i})$, corresponding to message M_i, from the public hash function H. A signing oracle takes the message M_i as input, and responds with

$$\sigma = (E_{AB_i}, \phi_{B_iA}(\phi_{B_i}(P_C)), \phi_{B_iA}(\phi_{B_i}(Q_C))$$

as the signature.

Crucially, an adversary wishing to forge a signature can only query the signing oracle with messages, M_i, while the curves E_{B_i} are computed from message hashes, rather than the messages themselves. Equivalence of unforgeability and invisibility to OMSSCDH would only be true if an adversary had the ability to submit arbitrary *curves* to the signing oracle. In essence, an adversary would need the ability to compute the message that corresponds to a specific curve. This is equivalent to the adversary inverting the hash function, H.

Since it is assumed in the construction of the protocol that H is cryptographically secure, we conclude that breaking the unforgeability and invisibility properties for the Jao-Soukharev protocol is not equivalent to solving OMSSCDH.[1]

2.3.4 The Srinath-Chandrasekaran protocol

Srinath and Chandrasekaran [80] extend the Jao-Soukharev construction to an undeniable *blind* signature scheme, introducing a third actor, the requestor, to the scheme. It is a four-prime variant of the original scheme and adds to the public parameters the points $\{P_D, Q_D\}$, a basis for $E[\ell_D^{e_D}]$.

Let p to be of the form $\ell_A^{e_A}\ell_B^{e_B}\ell_C^{e_C}\ell_D^{e_D} \cdot f \pm 1$, where ℓ_A, ℓ_B, ℓ_C and ℓ_D are primes and f is a small cofactor. Let E be a supersingular curve over $\mathbb{F}_{p^2}$ and let $\{P_A, Q_A\}$, $\{P_B, Q_B\}$, $\{P_C, Q_C\}$ and $\{P_D, Q_D\}$ be bases for the $\ell_A^{e_A}, \ell_B^{e_B}, \ell_C^{e_C}$ and $\ell_D^{e_D}$ torsions E, $E[\ell_A^{e_A}], E[\ell_B^{e_B}], E[\ell_C^{e_C}]$ and $E[\ell_D^{e_D}]$, respectively. The public parameters of the scheme are p, E, the four torsion bases and a cryptographic hash function $H : \{0,1\}^* \to \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$.

As in the Jao-Soukharev protocol, the signer generates random integers m_A, n_A from $\mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ and computes the isogeny $\phi_A : E \to E_A = E/\langle [m_A]P_A + [n_A]Q_A \rangle$. The signer's public key consists of the tuple $(E_A, \phi_A(P_C), \phi_A(Q_C))$ and the private key is (m_A, n_A) or, equivalently, ϕ_A.

The signing protocol proceeds in this order: 1. blind, 2. sign, 3. unblind. A requestor chooses a message, which is blinded and sent to the signer. The signer signs the blinded message and returns a blinded signature to the requestor. The requestor then unblinds the received tuple, resulting in the actual signature for

[1] Observe that the requirement that H is a cryptographic hash function is an example of the fourth point of potential error identified by Koblitz and Menezes: implicit assumptions within the description of a protocol.

the message.

Blinding For a message M, the requestor computes computes the hash $h = H(M)$ of the message and computes the curve $E_B = E/\langle P_B + [h]Q_B\rangle$ and the isogeny $\phi_B : E \to E_B$. The requestor then blinds the message curve by taking a random integer $0 < d < \ell_D^{e_D}$ to compute $E_{BD} = E_B/\langle \phi_B(P_D) + [d]\phi_B(Q_D)\rangle$, with the corresponding isogeny $\phi_{BD} : E_B \to E_{BD}$ and a basis $\{P'_D, Q'_D\}$ for the $\ell_D^{e_D}$ torsion of E_{BD}, $E_{BD}[\ell_D^{e_D}]$. The requestor additionally computes the points

$$P'_i = \phi_{BD}(\phi_B(P_i)), Q'_i = \phi_{BD}(\phi_B(Q_i)), \quad i = A, C$$

and sends these, along with the blinded curve E_{BD}, to the signer.

Signing Signing functions in much the same way as for the Jao-Soukharev protocol, albeit shifted through ϕ_{BD}. Upon receipt of the blinded curve and auxiliary points, the signer computes the curve $E_{BDA} = E_{BD}/\langle [m_a]P'_A + [n_A]Q'_A\rangle$, the corresponding isogeny $\phi_{BDA} : E_{BD} \to E_{BDA}$ and the points $\phi_{BDA}(P'_C)$, $\phi_{BDA}(Q'_C)$, $\phi_{BDA}(P'_D)$ and $\phi_{BDA}(Q'_D)$. The curve and auxilliary points are returned to the requestor for unblinding.

Unblinding In preparation for unblinding, the requestor computes a point $R \in E[\ell_D^{e_D}]$ such that $R \notin \ker(\phi_{BD})$. They then solve the extended elliptic curve discrete logarithm problem to find $m'_D, n'_D \in \mathbb{Z}/\ell_D^{e_D}\mathbb{Z}$ such that

$$[m'_D]P'_D + [n'_D]Q'_D = \phi_{BD}(R).$$

$$\begin{tikzcd}
E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"] & E_A \\
E_B \arrow[d, "\phi_{BD}"] & E_{AB} \\
E_{BD} \arrow[r, "\phi_{ABD}"] & E_{ABD} \arrow[u, "\hat{\phi}_{BD}"']
\end{tikzcd}$$

Figure 2.5: The isogeny diagram for signing in the Srinath-Chandrasekaran Protocol.

Unblinding the curve E_{BDA} requires the requestor to compute the curve $E_{AB} = E_{BDA}/\langle [m'_D]\phi_{BDA}(P'_D) + [n'_D]\phi_{BDA}(Q'_D)\rangle$ and the isogeny $\phi_{BAD} : E_{BDA} \to E_{AB}$. The unblinded signature is the tuple $\sigma = (E_{AB}, P, Q)$ where $P = \phi_{BAD}(\phi_{BDA}(P'_C))$ and $Q = \phi_{BAD}(\phi_{BDA}(P'_C))$.

Confirmation and disavowal The confirmation and disavowal protocols for the Srinath-Chandrasekaran protocol are identical to those in the Jao-Soukharev protocol.

2.3.5 Analysing the security proof of Srinath-Chandrasekaran

The security proof for the Srinath-Chandrasekaran protocol, with respect to the properties of unforgeability and invisibility, unsurprisingly bears strong similarity with that of Jao-Soukharev. In particular, the authors adopt Assumption 2.3.1 without further proof. Their protocol-specific security assumption is:

Assumption 2.3.3. Unforgeability and invisibility in the Srinath- Chandrasekaran protocol are equivalent to 1MSSCDH.

In the next section, we show that 1MSSCDH can be reduced to an instance of OMSSCDH.

Remark 2.3.4. The blindness property is not included in Assumption 2.3.3. In consideration of unforgeability and invisibility we imagine the adversary as playing the role of a malicious requestor. That is, the adversary has the freedom to choose messages, and thus we do not consider blindness. We will discuss the impact on blindness in Section 2.6.2.

In the Srinath-Chandrasekaran protocol, the adversary knows E_A and can compute E_{B_i} and $\ker(\phi_{B_i})$, corresponding to message M_i, from the public hash function H. A signing oracle takes the message M_i as input, and responds with $\sigma = (E_{AB_i}, \phi_{B_iA}(\phi_{B_i}(P_C)), \phi_{B_iA}(\phi_{B_i}(Q_C))$ as the signature. Notice that these signatures are equivalent to Jao-Soukharev signatures.

In [80] the claim is made that forging a signature for this construction is equivalent to solving 1MSSCDH. However, as in the case of the Jao-Soukharev protocol, the authors did not account for the hash function. Hence, we similarly conclude that breaking unforgeability and invisibility in the Srinath-Chandrasekaran protocol is not equivalent to solving 1MSSCDH or OMSSCDH.

2.4 Attack on SSCDH variants

The variants of the SSCDH problems defined in Section 2.2.2 arise in the security proofs of [52, 80]. Due to the presumed hardness of SSCDH, these problems are conjectured by the authors to be computationally infeasible. This section introduces new attacks on both the OMSSCDH and 1MSSCDH problems which give a polynomial-time adversary a non-negligible advantage. We assume that the adversary has access to an MSSCDH oracle, as defined here:

Definition 2.4.1 (MSSCDH Oracle)**.** *For fixed curves E and E_A, let $\mathcal{O}$ be an oracle that solves MSSCDH for E_A, $E_{B'}$, $\ker(\phi_{B'})$ for any curve $E_{B'}$ that is $\ell_B^{e_B}$-isogenous to E.*

Note an adversary cannot query the oracle with curves isomorphic to a given target curve, E_B.

Theorem 2.4.2. *A solution to the OMSSCDH problem (Problem 2.2.7) can be guessed with probability $\frac{1}{(\ell_B+1)\ell_B}$ after a single query to the MSSCDH oracle.*

Proof. Let E_A, E_B and $\ker(\phi_B)$ be the parameters of the OMSSCDH problem. Let $E_{B'} \neq E_B$ be a curve ℓ_B^2-isogenous to E_B and $\ell_B^{e_B}$-isogenous to E. Recall that ϕ_B is separable and so can be written as the composition of e_B isogenies, each of degree ℓ_B. Finding $E_{B'}$ from E_B amounts to inverting the last ℓ_B-isogeny step of ϕ_B, then applying another ℓ_B-isogeny. Thus, with knowledge of $\ker(\phi_B)$ the adversary can compute $\ker(\phi_{B'})$ and $E_{B'}$.

Then, querying the oracle on $E_A, E_{B'}, \ker(\phi_{B'})$ produces $E_{AB'}$. Since any curve in the isomorphism class of E_{AB} is ℓ_B^2-isogenous to $E_{AB'}$ as depicted in Figure 2.6, it follows that the adversary can guess the isomorphism class of E_{AB} correctly with probability $\frac{1}{(\ell_B+1)\ell_B}$. □

Remark 2.4.3. Even without prior knowledge of ϕ_B, an adversary can guess an appropriate $E_{B'}$ with probability $\frac{\ell_B-1}{(\ell_B+1)\ell_B}$.

In practice the prime ℓ_B is chosen to be small (usually 2 or 3) and thus Theorem 2.4.2 breaks the OMSSCDH problem completely.

$$\begin{tikzcd}
E \arrow[r] \arrow[ddr] & \circ \arrow[r, dotted] & \circ \arrow[r] \arrow[dr] & E_B \arrow[ddr] & \\
 & & & E_{B'} \arrow[ddr, blue] & \\
 & E_A \arrow[r] & \circ \arrow[r, dotted] & \circ \arrow[r] \arrow[dr] & E_{AB} \\
 & & & & E_{AB'}
\end{tikzcd}$$

Figure 2.6: Isogeny diagram showing that a query to the OMSSCDH oracle on an ℓ_B^2-isogenous curve $E_{B'}$ yields an elliptic curve close to target curve. The blue arrow from $E_{B'}$ to $E_{AB'}$ represents the output of the oracle.

Without the condition on the degree of the isogeny between the curves submitted to the MSSCDH oracle and the base curve, the attack's success probability can be improved. We define the Free Degree OMSSCDH problem, which describes this situation.

Problem 2.4.4 (Free Degree OMSSCDH Problem)**.** *For fixed E_A, E_B, given an oracle to solve MSSCDH for E_A, $E_{B'}$, $\ker(\phi_{B'})$ with $E_{B'}$ not isomorphic to E_B, solve MSSCDH for E_A, E_B and $\ker(\phi_B)$.*

An adversary can always solve Problem 2.4.4 after two queries to the oracle as described in the proof of the following corollary to Theorem 2.4.2.

Corollary 2.4.5. *A solution to the Free Degree OMSSCDH problem (Problem 2.4.4) can be found with two queries to the MSSCDH oracle.*

Proof. Let E_A, E_B and $\ker(\phi_B)$ be the parameters of the Free Degree OMSSCDH problem. Using the method outlined in the proof of Theorem 2.4.2, the adversary computes two curves E_{B_1} and E_{B_2}, $E_{B_1} \not\cong E_{B_2}$, that are ℓ_B-isogenous to E_B. The adversary queries the oracle to solve MSSCDH for E_A, E_{B_i} and $\ker(\phi_{B_i})$ for $i = 1, 2$, receiving E_{AB_i} in response. The curves E_{AB_i} are ℓ_B-isogenous to the target E_{AB}

as shown in Figure 2.7. Each of E_{AB_1} and E_{AB_2} have $\ell_B + 1$ isomorphism classes to which they are ℓ_B-isogenous. The intersection of the two sets of isomorphism classes contains only one element, namely, the isomorphism class of E_{AB}. □

$$\begin{tikzcd}
E \arrow[r] \arrow[dr] & \circ \arrow[r, dotted] & \circ \arrow[r] & E_{B_1} \arrow[r] \arrow[dr, blue] & E_B \arrow[r] \arrow[dr] & E_{B_2} \arrow[dr, blue] & \\
 & E_A \arrow[r] & \circ \arrow[r, dotted] & \circ \arrow[r] & E_{AB_1} \arrow[r] & E_{AB} \arrow[r] & E_{AB_2}
\end{tikzcd}$$

Figure 2.7: Isogeny diagram of the attack on the Free Degree OMSSCDH problem. The blue diagonal arrows (E_{B_1} to E_{AB_1}, and E_{B_2} to E_{AB_2}) represent the output of the MSSCDH oracle, which sends ℓ_B-isogenous curves of E_B to ℓ_B-isogenous curves of target curve E_{AB}.

Clearly, the attack described in Theorem 2.4.2 can be generalised to OMSSDDH, the decisional variant of OMSSCDH, yielding the following theorem.

Theorem 2.4.6. *A solution to the OMSSDDH problem (Problem 2.2.8) can be guessed with probability* $\frac{1}{(\ell_B+1)\ell_B}$ *after a single query to the MSSCDH oracle.*

Proof. Given E_A, E_B and E' as in Problem 2.2.8, the adversary can apply the attack of Theorem 2.4.2 to E_A and E_B to obtain the the isomorphism class of E_{AB}. The adversary then checks whether $E' \cong E_{AB}$. □

Furthermore, a solution to the OMSSCDH problem implies a solution to the 1MSSCDH problem which yields the following theorem.

Theorem 2.4.7. *A solution to the 1MSSCDH problem (Problem 2.2.9) can be guessed with probability* $\frac{1}{(\ell_B+1)\ell_B}$ *after a single query to the MSSCDH oracle.*

Proof. Let E, E_A be the parameters of the 1MSSCDH problem. Let E_{B_1} be a curve $\ell_B^{e_B}$-isogenous to E. Theorem 2.4.2 solves the OMSSCDH problem for E_A, E_{B_1} and

$\ker E_{B_1}$ after a single query to the oracle. Let E_{B_2} be the curve ℓ_B^2-isogenous to E_{B_1} found in the attack, with corresponding oracle response E_{AB_2}. Let E_{AB_1} be the solution to the OMSSCDH problem, guessed correctly with success probability $\frac{1}{(\ell_B+1)\ell_B}$. The adversary then has tuples (E_{B_1}, E_{AB_1}) and (E_{B_2}, E_{AB_2}) and so solves the 1MSSCDH problem with $q = 1$ queries to the oracle. □

2.5 Attack on undeniable isogeny signature schemes

Both signature schemes schemes assume that forging a signature is equivalent to breaking OMSSCDH. However, as shown in Section 2.3.3 and Section 2.3.5, we see that the inclusion of a cryptographic hash function in the protocol precludes equivalence to the SSCDH variant. As a consequence the attack of Section 2.4 disproves the hardness assumption in [52] and [80], but does not break either protocol. While this is sufficient to disprove the validity of the inherited assumption that variants of hard problems are also hard, and in particular disproves the OMSSCDH hardness assumption, we now justify the practical impact of the attack.

This section extends the attack on OMSSCDH, introducing a 'hybrid' version, which involves finding 'near-collisions' in the hash function as well as using a signing oracle. We apply the attack to the Jao-Soukharev protocol in detail first, then discuss the differences in application to Srinath-Chandrasekaran, although for the most part the attack proceeds identically.

For the purposes of the succeeding discussion, let $H : \{0,1\}^* \to \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$ be the public hash function used in both signature schemes. Let λ be a security parameter. The hash function determines a coefficient of a point in the $E[\ell_B^{e_B}]$ torsion group and can therefore be treated as a function to a group of cardinality

$2^{2\lambda}$ for classical security levels and $2^{3\lambda}$ for quantum security levels [17]. Let 2^L denote the cardinality of this group in the image of ϕ_B.

2.5.1 Attack on Jao-Soukharev protocol

Once again, we recall that the adversary knows E_A and can compute E_{B_i} and $\ker(\phi_{B_i})$, corresponding to message M_i, from the public hash function H. The adversary additionally has access to a signing oracle subject to the following definition.

Definition 2.5.1. *A signing oracle takes the message M_i as input, and responds with*

$$\sigma = (E_{AB_i}, \phi_{B_iA}(\phi_{B_i}(P_C)), \phi_{B_iA}(\phi_{B_i}(Q_C))$$

as the signature.

Algorithm 1 summarises the hybrid attack against the Jao-Soukharev signature scheme.

```
Input  : Jao-Soukharev public parameters and a message $M \in \{0,1\}^*$
Output: $\sigma$, a valid Jao-Soukharev signature for $M$
Build a near-collision on $H$ with respect to the $\ell_B$-adic metric, $M'$;
Submit $M'$ to the signing oracle to obtain the signature
  $\sigma' = \big(E_{AB'}, P_1 := \phi_{B'A}(\phi_{B'}(P_C)), P_2 := \phi_{B'A}(\phi_{B'}(Q_C))\big)$;
Guess the $\ell_B^{2k}$-isogeny $\psi : E_{AB'} \to E_{AB}$;
Find $s$ such that $s\ell_B^k \equiv 1 \bmod \ell_C^{e_C}$;
Compute the auxilary points of the signature as $\{[s] \cdot \psi(P_1), [s] \cdot \psi(P_2)\}$;
Output $\sigma = (E_{AB}, [s] \cdot \psi(P_1), [s] \cdot \psi(P_2))$;
```

Algorithm 1: Algorithm to compute a Jao-Soukharev signature for a message M

In detail, the attack proceeds as follows: Let M be the message upon which the adversary wishes to forge a signature, with corresponding message curve E_B. The adversary finds M', a near collision with M on H, such that the difference between $H(M)$ and $H(M')$ is divisible by a large power of ℓ_B, say a power of size roughly 2^{L_1}, for $L_1 < L$. The adversary submits M' to the oracle, receiving the signature $\sigma' = \big(E_{AB'}, P_1 := \phi_{B'A}(\phi_{B'}(P_C)), P_2 := \phi_{B'A}(\phi_{B'}(Q_C))\big)$ in response. The curve $E_{AB'}$ is ℓ_B^{2k}-isogenous to the target curve E_{AB}, where $\ell_B^k \approx 2^{L_2}$ for $L_2 = L - L_1$ (see Lemma 2.5.2 below for proof).

The attacker must then guess the ℓ_B^{2k} isogeny $\psi : E_{AB'} \to E_{AB}$. The probability of correctly identifying ψ in a single guess is $\frac{1}{(\ell_B+1)\ell_B^{2k-1}}$. Let $\psi = \psi_B \circ \hat{\psi}_{B'}$, the composition of two degree ℓ_B^k isogenies. Informally, $\hat{\psi}_{B'}$ corresponds to k backwards steps on the isogeny path from $E_{AB'}$ and ψ_B corresponds to k forward steps to E_{AB}.[2] This is illustrated in Figure 2.8. Letting $\phi_{AB'} = \phi_{e_{B'}} \circ \phi_{e_{B'}-1} \circ \cdots \circ \phi_1$, it is clear that $\hat{\psi}_{B'} = \hat{\phi}_{e_{B'}-k} \circ \cdots \circ \hat{\phi}_{e_{B'}}$. Applying ψ to P_1 and Q_1 therefore appends a factor of ℓ_B^k to the auxiliary signature points. The adversary computes s, where $s\ell_B^k \equiv 1 \mod \ell_c^{e_C}$. The signature $\sigma = (E_{AB}, [s] \cdot \psi(P_1), [s] \cdot \psi(P_2))$ is then a valid signature for M.

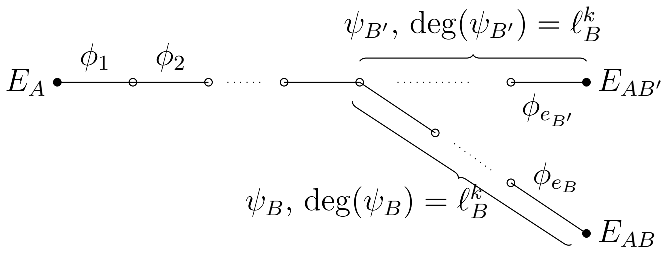
$\psi_{B'}$, $\deg(\psi_{B'}) = \ell_B^k$
ϕ_1
ϕ_2
E_A
$E_{AB'}$
$\phi_{e_{B'}}$
ϕ_{e_B}
ψ_B, $\deg(\psi_B) = \ell_B^k$
E_{AB}

Figure 2.8: Isogeny paths between E_A, E_{AB} and $E_{AB'}$ in the attack on the Jao-Soukharev protocol.

[2] A step corresponds to an ℓ_B-isogeny.

The following lemma allows the adversary to proceed despite the scheme's loss of malleability due to the hash function.

Lemma 2.5.2. *Let E be a supersingular elliptic curve, let ℓ be a prime, let e be an integer, and let $\{P, Q\}$ be a basis for $E[\ell^e]$. Let $n, m < \ell^e$ be positive integers congruent modulo ℓ^k for some integer $k < e$. Then the ℓ-isogeny paths from E to $E_A = E/\langle P + [n]Q\rangle$ and $E_B = E/\langle P + [m]Q\rangle$ are equal up to the k-th step.*

Proof. Let $m = n + \alpha\ell^k$, for some $\alpha > 0$. Let $\phi_A : E \to E_A$ be a separable, cyclic isogeny of $\deg(\phi_A) = \ell^e$ and $\ker(\phi_A) = \langle P + [n]Q\rangle$. We can express ϕ_A as the composition of e ℓ-isogenies such that $\phi_A = \phi_1^A \circ \cdots \circ \phi_e^A$. Likewise, $\phi_B : E \to E_B$ can be expressed as $\phi_B = \phi_1^B \circ \cdots \circ \phi_e^B$. The single ℓ-isogenies correspond to the single steps in the ℓ-isogeny graph. We will show that $\phi_i^A = \phi_i^B$ for $1 \leq i \leq k$.

For $i = 1, \ldots, e$, let $\phi_i^A : E_{i-1} \to E_i$ be an isogeny with kernel $\langle \ell^{e-i} S_{i-1}^A \rangle$, where $E_0 = E$, $S_0^A = P + [n]Q$ and $S_{i-1}^A = \phi_{i-1}^A(S_{i-2}^A)$. Define the ϕ_i^B similarly, with B substituted for A and m for n. By [27], these are ℓ-isogenies and $\phi_1^A \circ \cdots \circ \phi_e^A = \phi_A$ up to composition with an automorphism on E_A (similarly for ϕ_B). We also have the recursion

$$\ell^{e-i} S_{i-1}^A = \ell^{e-i} \phi_{i-1}^A(S_{i-2}^A) = \phi_{i-1}^A \circ \cdots \circ \phi_1^A(\ell^{e-i} S_0^A)$$

with the analogous result for $\ell^{e-i}S^B_{i-1}$. For $1 \leq i \leq k$, we have $e - i + k \geq e$ and so

$$\begin{aligned} \ell^{e-i}S^B_0 &= \ell^{e-i}(P + [m]Q) \\ &= \ell^{e-i}(P + [n]Q) + \ell^{e-i+k}[\alpha]Q \\ &= \ell^{e-i}(P + [n]Q) \\ &= \ell^{e-i}S^A_0 \end{aligned}$$

using that isogenies are group homomorphisms and $Q \in E[\ell^e]$. It follows that $\phi^A_i = \phi^B_i$ for $1 \leq i \leq k$. □

With this result in mind, the validity of the signature output by Algorithm 1 is proven in the following theorem.

Theorem 2.5.3 (Correctness)**.** *Let s, ψ, P_1 and P_2 be defined as in Algorithm 1. Let σ be the signature $(E_{AB}, [s]\cdot\psi(P_1), [s]\cdot\psi(P_2))$ output by Algorithm 1. Assuming that E_{AB} is guessed correctly, σ is a valid signature.*

Proof. Since ψ maps points on $E_{AB'}$ to points on E_{AB}, the points $\psi(P_1), \psi(P_2)$ both lie on the target curve. Moreover, as $\psi(P_1) = \psi(\phi_{B'A}(\phi_{B'}(P_C)))$, the point lies in the $\ell_C^{e_C}$ torsion of E_{AB}, $E_{AB}[\ell_C^{e_C}]$. The same holds for $\psi(P_2)$. Although these points would already pass the validation process for the signature scheme, they can be easily distinguished from the honestly generated points by computing Weil pairings. This is due to the factor ℓ_B^k. Multiplication by the factor $[s]$ ensures that forged and honest signatures cannot be distinguished as described in the following.

Recall that $\psi = \psi_B \circ \hat{\psi}_{B'}$ and $P_1 = \phi_{B'A}(\phi_{B'}(P_C))$. Since the order of P_C is coprime to $\deg(\phi_{B'A})$ and $\deg(\phi_{B'})$, and the isogeny diagram is commutative, we can write $P_1 = \phi_{AB'}(\phi_A(P_C))$.

By expanding $\phi_{AB'}$ we obtain

$$\begin{aligned}\hat{\psi}_{B'} \circ \phi_{AB'} &= \hat{\phi}_{e_{B'}-k} \circ \cdots \circ \hat{\phi}_{e_{B'}} \circ \phi_{e_{B'}} \circ \cdots \circ \phi_{e_{B'}-k} \circ \cdots \circ \phi_{e_B-k} \circ \cdots \circ \phi_1 \\ &= [\ell_B^k] \circ \phi_{e_{B'}-k-1} \circ \cdots \circ \phi_1.\end{aligned}$$

Since s is the multiplicative inverse of ℓ_B^k modulo $\ell_C^{e_C}$, we have

$$[s] \cdot \psi(P_1) = \phi_{AB}(\phi_A(P_C)) \in E_{AB}[\ell_C^{e_C}].$$

Analogously, we have $[s] \cdot \psi(P_2) = \phi_{AB}(\phi_A(Q_C)) \in E_{AB}[\ell_C^{e_C}]$.

Let $P = \phi_{BA}(\phi_B(P_C)) \in E_{AB}[\ell_C^{e_C}]$ and $Q = \phi_{BA}(\phi_B(Q_C)) \in E_{AB}[\ell_C^{e_C}]$. These are the points we expect in an honest signature. In both the confirmation and disavowal protocols of the Jao-Soukharev scheme, the verifier uses the auxiliary points to compute an isogeny from E_{AB} to a curve $E_\sigma = E_{AB}/\langle [m_C \cdot s]\psi(P_1) + [n_C \cdot s]\psi(P_2)\rangle$, where $m_C, n_C \in \mathbb{Z}/\ell_C^{e_C}\mathbb{Z}$ are integers chosen by the signer. This curve is checked against $E_{ABC} = E_{AB}/\langle [m_C]P + [n_C]Q\rangle$ to determine the validity of σ. The two points obtained in Algorithm 1 span the subgroup $E_{AB}[\ell_C^{e_C}]$, and we have E_{AB} as the correct signature curve, so it follows that $E_\sigma = E_{ABC}$ up to isomorphism and thus the signature is accepted as valid. □

Clearly, this attack breaks the unforgeability property of the scheme with a single call to the signing oracle. Moreover, this implies that the scheme also fails to satisfy invisibility, since any adversary with the ability to forge signatures with non-negligible probability can simply check whether the challenge signature obtained in the invisibility game matches a potential forgery, as follows.

Theorem 2.5.4 (Invisibility). *Let E, E_A, $\{P_A, Q_A\}$, $\{P_B, Q_B\}$ and $\{P_C, Q_C\}$ be the public parameters of a Jao-Soukharev signature protocol. Let M be a message with corresponding message curve E_B. Given b sampled uniformly from $\{0,1\}$, let $\sigma' = (E', P', Q')$ be a challenge signature as in the invisibility game, where*

$$\sigma' = \begin{cases} \texttt{Sign}(M) \text{ if } b = 1 \\ \texttt{Sim}(M) \text{ if } b = 0 \end{cases}$$

An adversary can determine b^* such that $b^* = b$ with a single query to the signing oracle.

Proof. The adversary applies Algorithm 1 to the message M, to receive $\sigma_A = (E_{AB}, P, Q)$. By Theorem 2.5.3, this is a valid signature for M. The adversary then checks whether $E_{AB} \cong E'$ by computing $j(E_{AB})$ and $j(E')$ and returns $b^* = 1$ if the statement holds, or $b^* = 0$ otherwise. □

2.5.2 Attack on Srinath-Chandrasekaran protocol

In the Srinath-Chandrasekaran protocol, the adversary knows E_A and can compute E_{B_i} and $\ker(\phi_{B_i})$, corresponding to message M_i, from the public hash function H. Additionally, the adversary has access to a signing oracle, subject to the following conditions, as defined in [80].

Definition 2.5.5 (Signing Oracle [80]). *Given a curve E over $\mathbb{F}_{p^2}$ with $\#E = (\ell_A^{e_A} \ell_B^{e_B} \ell_C^{e_C} \ell_D^{e_D} f)^2$ and points $P, Q \in E$ of order $\ell_A^{e_A}$, the signing oracle outputs*

$$E' = E/\langle [m_A]P + [n_A]Q \rangle$$

where m_A, n_A are the Srinath-Chandrasekaran private key.

The scenario created by the unforgeability and invisibility games treats the adversary as a malicious requestor. Suppose the target message is M, corresponding to the message curve E_B. Since the signature curve E_{AB} resulting from the Srinath-Chandrasekaran protocol is isomorphic to that returned by the Jao-Soukharev protocol for the same message and signer, the scheme is vulnerable to the attack in Section 2.5.1. As in the Jao-Soukharev case, both unforgeability and invisibility can be broken.

Note that the auxiliary points gain a factor of $\ell_D^{e_D}$ as a result of the unblinding (which amounts to applying an isogeny and its dual). As noted by the authors in [80], as this factor is coprime to $\ell_C^{e_C}$, verification remains unaffected.

2.6 Impact on security

2.6.1 Parameter

Let us analyse the cost of Algorithm 1 in terms of the security parameter, λ. Note that this cost analysis applies to the security of both the Jao-Soukharev protocol and the Srinath-Chandrasekaran protocol.

To summarise Section 2.5, the attack proceeds by computing a near-collision on the public hash function H and guessing an ℓ_B^{2k}-isogeny between an honest signature produced by the oracle for one message to the target forgery curve. Recall that H is a function to a group of size 2^L, where $L = 2\lambda$ for classical security levels and $L = 3\lambda$ for quantum security levels.

A direct approach for an adversary would be to find a collision on H, then apply the attack in *Algorithm* 1. This is infeasible, as H is chosen to be cryptographically secure. The cost of finding a collision in L bits is $O(2^{L/2}) = O(2^{\lambda})$, for a classical adversary. We similarly see the quantum cost of a direct attack is $O(2^{L/3}) = O(2^{\lambda})$.

Lemma 2.6.1. *Algorithm 1 costs $O(2^{4\lambda/5})$ for a classical adversary and $O(2^{6\lambda/7})$ for a quantum adversary.*

Proof. Finding a near-collision of L_1 bits on H classically has cost $O(2^{L_1/2})$. In Step 3 of *Algorithm* 1 the adversary guesses the correct isogeny and curve E_{AB} with probability approximately $2^{-2L_2} = 2^{-2(L-L_1)}$. Taking $L_1 = 4L/5$ the attack then has a total classical cost of $O(2^{2L/5})$, as opposed to the expected $O(2^{L/2})$.

Under the assumption that it is possible to find near-collisions of the hash function with lower complexity using a quantum computer[3] [17], the first step of the attack has cost $O(2^{L_1/3})$. Taking $L_1 = 6L/7$, the total cost of the attack for a quantum adversary is lowered to $O(2^{2L/7})$, as opposed to the expected $O(2^{L/3})$.

The classical cost for this attack is $O(2^{4\lambda/5})$, with the hash function output length equal to 2λ. With the assumption above, the quantum cost for this attack is $O(2^{6\lambda/7})$. □

Let λ be the desired level of security and let λ' be the parameter defining the length of the hash function. Then, in order to achieve the security level λ, we need

$$\frac{4\lambda'}{5} = \lambda \tag{2.1}$$

for classical security and

$$\frac{6\lambda'}{7} = \lambda \tag{2.2}$$

[3] Bernstein [8] argues that quantum collision search is practically inferior to classical collision search algorithms due to expensive memory access and quantum memory.

for quantum security. Hence, the size of the protocol parameters should be increased by 25% to achieve the same classical security level (17% for quantum security).

2.6.2 Blindness

Here we briefly discuss why the blindness property of the Srinath-Chandrasekaran protocol is unaffected by our attack. First, we define blindness via the following security game [29, 25, 66]:

1. The adversary generates a key pair (sk, vk).
2. The adversary chooses two messages, m_0 and m_1, and sends them to the challenger.
3. The challenger computes a random bit b and reorders the messages as (m_b, m_{1-b}).
4. The challenger blinds the messages and sends them to the adversary.
5. The adversary signs the blinded messages, generating the signatures σ_b^{blind} and σ_{1-b}^{blind}, which are returned to the challenger.
6. The challenger applies an unblinding algorithm to σ_b^{blind} and σ_{1-b}^{blind} and reveals the unblinded signatures, σ_b and σ_{1-b}, to the adversary.
7. The adversary outputs a bit b'.

The adversary wins if $b' = b$. A signatures scheme is *blind* if $|\Pr(b = b') - 1/2\ |$ is negligible.

The most obvious difference, in comparison to unforgeability and invisibility, is that in this game the adversary does not have access to an oracle. In fact, the blindness game corresponds to neither the OMSSCDH nor the 1MSSCDH problems. Hence, the attacks of Section 2.4 and Section 2.5 are not applicable.

2.6.3 Adversarial restrictions

In order to test the boundaries of the attack model, we now look at the efficacy of our attacks under certain restrictions to the adversary.

Restricted oracle Let us first explicitly define the oracle in Problem 2.2.7 (OMSSCDH).

Definition 2.6.2 (Unrestricted oracle)**.** *For fixed curves E_A, E_B, given $E_{B'}$ and* $\ker(\phi_{B'})$*, such that*

- *$E_{B'}$ is $\ell_B^{e_B}$-isogenous to E, and*
- *$E_{B'}$ not isomorphic to E_B,*

the oracle $\mathcal{O}$ returns $E_{AB'}$, a solution to MSSCDH for E_A, $E_{B'}$ and $\ker(\phi_{B'})$*.*

The attack against OMSSCDH (Section 2.4) requires the adversary to query the oracle with an $E_{B'}$ that is additionally ℓ_B^2-isogenous to E_B. We now consider a situation in which we are unable to choose curves this 'close' to the target message curve. That is, we place a third restriction on the oracle.

Definition 2.6.3 (Restricted Oracle)**.** *For fixed curves E_A, E_B and a positive integer $k < 2e_B$ given $E_{B'}$ and* $\ker(\phi_{B'})$*, such that*

- *$E_{B'}$ is $\ell_B^{e_B}$-isogenous to E,*
- *$E_{B'}$ not isomorphic to E_B, and*
- *$E_{B'}$ is $\ell_B^{k'}$-isogenous to E_B, where $k < k' < 2e_B$,*

the oracle $\mathcal{O}_k$ returns $E_{AB'}$, a solution to MSSCDH for E_A, $E_{B'}$ and $\ker(\phi_{B'})$*.*

Assume that k' is even. The adversary proceeds as in the proof of Theorem 2.4.2. With knowledge of $\ker(\phi_B)$, finding $E_{B'}$ from E_B amounts to inverting the last $k'/2$ ℓ_B-isogeny steps of ϕ_B, then applying another $\ell_B^{k'/2}$-isogeny. The probability of guessing E_{AB} correctly is then $\frac{1}{(\ell_B+1)\ell_B^{k'-1}}$. This is analogous to the situation at Step 3 in Algorithm 1. Clearly, for large k' this probability becomes negligible.

Restricted message We now consider changing the role of the adversary in our security analysis of the Srinath-Chandrasekaran protocol. In Section 2.5 we treated the adversary as a malicious requestor. Suppose now that the adversary is attempting to impersonate the signer, but is not privy to the message to be signed. That is, the adversary intercepts the blinded curve sent by the requestor to the signer and wants to forge a signature. In this situation, the adversary knows E and E_{BD}, and seeks to compute E_{ABD}. Figure 2.9 illustrates a comparison of the two attack scenarios.

$$\begin{tikzcd}
E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"] & E_A \\
E_B \arrow[d, "\phi_{BD}"] & E_{AB} \\
E_{BD} \arrow[r, "\phi_{ABD}"] & E_{ABD} \arrow[u, "\hat{\phi}_{BD}"']
\end{tikzcd}
\qquad
\begin{tikzcd}
E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"] & E_A \\
E_B \arrow[d, "\phi_{BD}"] & E_{AB} \\
E_{BD} \arrow[r, "\phi_{ABD}"] & E_{ABD} \arrow[u, "\hat{\phi}_{BD}"']
\end{tikzcd}$$

Figure 2.9: Comparison of attack scenarios against the Srinath-Chandrasekaran protocol. Items in blue are known to the attacker, while items in red are known only to the signer. The left-most diagram shows the 'malicious requestor' scenario and the right-most diagram illustrates the 'restricted message' scenario.

In order to apply Algorithm 1, the adversary would need to determine either the message, thus breaking blindness, or $\ker(\phi'_{BD})$, where $\phi'_{BD} : E \to E_{BD}$. The latter would allow the adversary to find an appropriate near-collision on H. However, under the CSSI assumption this problem is infeasible. Hence an attacker cannot forge a signature for M under these restrictions. We note that the ability to forge signatures on chosen messages (as described in Section 2.5) is enough to break the scheme, even if the restricted message attack is not possible.

2.7 Conclusion

The objective of this chapter was to illustrate a real-world example of Koblitz and Menezes' first point of error in reductionist security proofs. Specifically, we looked at hardness assumptions positing that variants of intractable problems are necessarily as difficult as the original problems, themselves. We have disproved such hardness assumptions on the OMSSCDH and 1MSSCDH problems, and their decisional variants. We have moreover addressed the incorrect assumptions in the security proofs of two undeniable signature schemes (namely, that unforgeability and invisibility are equivalent to solving OMSSCDH and 1MSSCDH, respectively) and then outlined an attack against these schemes. The protocols of [52, 80] illustrate that if insufficient scrutiny is given to problem variants, then the flawed hardness assumption may propagate into extensions of the protocol in which it is initially used. The resulting impact on security requires an increase in parameter size by 25%, assuming a classical adversary, or 17%, assuming a quantum adversary. We note that this does not represent a devastating attack, but that the security claims must nonetheless be updated to reflect this new attack. A question for future work is whether another attack exists against the blindness property of

[80].

Chapter 3

Practical security of multivariate quadratic cryptography

Practitioners of post-quantum cryptography need to compute explicit parameters for achieving a desired level of security, or conversely, determine the level of security that is provided by a given parameter set. However, translating complexity-theoretic security results to precise values may require approximations, if certain parameters are difficult to compute exactly. This chapter looks at the errors which may be induced by such approximations through the lens of multivariate public key cryptosystems (MPKCs). In particular, we look at the complexity analysis of direct attacks on multivariate cryptosystems using algorithms for computing Gröbner bases.

The best known approach for solving a zero-dimensional multivariate system of equations $\mathcal{F} = 0$ is to find a Gröbner basis of the ideal generated by the polynomials in $\mathcal{F}$ [12, 19]. This approach is applicable to any multivariate cryptosystem and is therefore considered the 'direct attack', as it does not take advantage of any additional structure in the system. This attack is generally an improvement on exhaustive search of the solution space [33], which has size q^n for a field with q elements and for polynomials in n variables. Hence, the complexity of computing a Gröbner basis of the public key of a multivariate cryptosystem or a multivariate digital signature algorithm gives an upper bound on the security of that system. Consequently, finding tight upper bounds on the complexity of Gröbner basis algorithms is an important area of research.

The first algorithm for computing Gröbner bases was introduced by Buchberger [18] in 1965. Subsequently, several more system-solver algorithms have been proposed, including [9, 37, 54, 67]. The system solvers fall into two categories [19]: Buchberger's Algorithm and variations thereof; and algorithms based on instances of Gaussian eliminations, an idea introduced by Lazard in [67]. The latter category is the focus of this chapter. These algorithms use matrices that correspond to systems of polynomials. The complexity of these algorithms is dependent on the size of the matrices involved in the computation, which depends on the degree d and the number of variables in the corresponding polynomials. This d is not always known in advance, so heuristics have been developed to approximate the cost of these algorithms.

The purpose of this chapter is to examine the veracity of a heuristic bound that is based on work by Bardet, Faugère and Salvy [3] and to provide better estimates of the complexity of Gröbner basis system solvers. Bardet, Faugère and Salvy introduced the concept of the degree of regularity, which is commonly used in the cryptography community to estimate the security of multivariate cryptosystems and digital signature schemes. However, this chapter provides evidence that the degree of regularity is not a valid upper bound for all systems.

Results in the chapter appear in a paper written with Elisa Gorla, Emmanuela De Negri, Manuela Dizdarevic, Mina Bigdeli and Sulaminthe Tsakou for Women in Numbers Europe 3 2020 at the University of Rennes [11].

Outline and main contributions We begin by covering some relevant definitions from commutative algebra. This is followed by a review of the literature with regard to Gröbner bases and semi-regular sequences in Section 3.2, then a summary of current methods for approximating the solving degree of a multivariate system of polynomials in Section 3.3. The most common method is to take the degree of regularity, defined by Bardet, Faugère and Salvy [3]. We identify two assumptions made in this method that can potentially impact the security analysis of multivariate cryptosystems: namely, that the degree of regularity is an upper bound for the solving degree and that the similarity in asymptotic behaviour is sufficient for security analyses. Counterexamples disproving the first of these assumptions are given in Section 3.4. These are significant in that the difference between solving degree and degree of regularity is greater than 1. We then present an alternative upper bound, which is based on a proven upper bound on the solving degree (the Castelnuovo-Mumford regularity). The bound applies to over-determined systems of semi-regular multivariate systems (which correspond to encryption protocols). Section 3.5 gives explicit formulas for systems of $n + \ell$ polynomials in n variables, for small values of ℓ, which are not covered by the asymptotic formulas of Bardet and Chyzak. Subsequently, we discuss how to apply these results to systems arising in cryptography.

3.1 Preliminaries

For a thorough mathematical background in commutative algebra we refer to [34]. For the following, and the entirety of this chapter, let K be a field and let $R = K[x_1, \dots, x_n]$ be the polynomial ring over K in n variables. Let $\mathcal{F} = \{f_1, \dots, f_m\} \subseteq R$ and let $I = \langle f_1, \dots, f_m \rangle$ be the ideal generated by the polynomials in $\mathcal{F}$.

An *algebraic subset* of K^n, with respect to a subset $S \subseteq R$ is the set of common zeroes of all polynomials $f \in S$.

Definition 3.1.1 (Zariski topology)**.** *The Zariski topology on an algebraic subset X is defined by taking the closed sets to be the algebraic subsets of X.*

The general linear group of $n \times n$ matrices over a field K, denoted $GL_n(K)$, is an example of a set with the Zariski topology [19].

Definition 3.1.2 (Discrete topology)**.** *The discrete topology on a space X is defined by taking all subsets to be open sets.*

Over a finite field the Zariski topology is the discrete topology. This is because every algebraic subset is the complement to another algebraic subset and so is both open and closed.

A polynomial ideal I is a complete intersection, if it is generated by its codimension number of polynomials. In our notaion, this implies $m = n$. An *almost complete intersection* is generated by the codimension $+1$ elements; that is, $m = n + 1$.

For any set $S \subseteq R$, let S_d denote the set of polynomials of degree d.

Definition 3.1.3. *Let $I \subseteq R$ be a homogeneous ideal. We say that I is Artinian if there exists a $d \geq 0$ s.t. $I_d = R_d$.*

Let $\succ$ be a monomial ordering. For a polynomial $f \in R$, the intial term of f, $in(f)$, is the greatest term of f with respect to $\succ$. The *initial ideal* of a polynomial ideal I is the ideal generated by the initial terms of all polynomials $f \in I$. We can now define the Gröbner basis of a polynomial ideal I.

Definition 3.1.4 (Gröbner Basis, [18])**.** *Let I be a polynomial ideal. The polynomials $\{g_1, \ldots, g_t\} \in I$ are a Gröbner basis for I if the initial ideal of I, $in(I)$, is generated by the leading terms of the g_i. Letting $in(f)$ denote the leading term of the polynomial f with respect to some monomial ordering, $G = \{g_1, \ldots, g_m\}$ is a Gröbner basis for I if $in(I) = \langle in(g_1), \ldots, in(g_m)\rangle$.*

A reduced Gröbner basis, G contains only monic polynomials and for all $g_i \in G$ it holds that for all i $in(g_i)$ does not divide any term of $g_j, j \neq i$.

Finally, we define the Hilbert series of R/I.

Definition 3.1.5. *Let $I \subseteq R$ be a homogeneous ideal. The Hilbert function of R/I is the function*

$$\begin{aligned} H_{R/I} : \mathbb{N} &\longrightarrow \mathbb{N} \\ d &\longmapsto \dim_{\mathbb{K}}(R/I)_d. \end{aligned}$$

The Hilbert series of R/I is the formal power series

$$HS_{R/I}(z) = \sum_{d \geq 0} H_{R/I}(d) z^d.$$

3.2 Gröbner Bases and semi-regular sequences

In general, MPKCs are constructed from a central map $\mathcal{F} \subseteq R$, belonging to the class of systems of multivariate polynomials over a finite field K that are relatively easy to invert. The central map is then hidden by secret affine maps $\mathcal{S}$ and $\mathcal{T}$ via the composition $\mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$. This composition is published as the public map, $\mathcal{P}$. The private key of such an MPKC is $\mathsf{sk} := \{\mathcal{F}, \mathcal{S}, \mathcal{T}\}$.

The security of an MPKC rests on the difficulty of solving systems of multivariate polynomial equations over finite fields. These systems are usually chosen to be quadratic, although exceptions exist [32]. The problem of solving multivariate quadratic (MQ) polynomial equations is formalised in the following statement.

Problem 3.2.1 (The *MQ*-Problem). *Given a system of m multivariate quadratic polynomials in n variables,*

$$\mathcal{P} := \{p_1(x_1, \dots, x_n), \dots, p_m(x_1, \dots, x_n)\},$$

with coefficients in $\mathbb{F}_q$, find a vector $\hat{x} = (x_1, \dots, x_n)$ such that $p_1(\hat{x}) = \cdots = p_m(\hat{x}) = 0$.

The MQ-problem is known to be NP-hard for systems in which the coefficients of the constituent polynomials are sampled uniformly at random from finite K [42]. Since in practice multivariate cryptosystems are equipped with a backdoor to facilitate decryption by a trusted user, these systems certainly do not satisfy this definition of random. Moreover, this additional structure means the systems may be more easily solved. Nevertheless, analysing the behaviour of sets of random polynomials provides insight into the 'general' security of multivariate cryptosystems. Hence, before discussing direct attacks against Problem 3.2.1, we must first rigorously define what is meant by random, or *generic*, sequences of polynomials.

3.2.1 Generic and semi-regular Sequences

The systems of polynomials arising in cryptography are designed to appear 'random', in the sense that the coefficients appear to be chosen uniformly at random from the coefficient field. To formalise the concept of 'randomness' as defined above, we adapt the following definition of 'genericity' from algebraic geometry.

Definition 3.2.2 ([65]). *A property is generic or holds generically if there exists a nonempty Zariski-open set where the property holds.*

Let us apply this to systems of polynomials. First we associate any polynomial with the vector of its coefficients. Then the set of homogeneous polynomials of degree d can be regarded as a projective space and, similarly, the set of polynomials of degree $\leq d$ can be treated as an affine space. Hence, we have the following definition for generic homogeneous polynomials.

Definition 3.2.3. *A* generic homogeneous *polynomial of degree d is a homogeneous polynomial of degree d, which belongs to a nonempty Zariski-open set in the projective space of all homogeneous polynomials of degree d.*

Similarly, a generic polynomial of degree $\leq d$ is a polynomial of degree $\leq d$, which belongs to a nonempty Zariski-open set in the affine space of all polynomials of degree $\leq d$.

We define a generic sequence of polynomials as a sequence $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R$, such that f_i is a generic polynomial, for all i.

Since we will be considering ideals generated by systems of polynomials, we also define a genericity property for ideals, following [19]. Let U be a Zariski open subset in $GL_n(K)$, where K is an infinite field[1]. Each element $u \in U$ represents a change in coordinates. We say that an ideal I is in *generic coordinates* if the initial ideal $in(I)$ is unchanged by all $u \in U$. Explicitly, this means $in(uI) = in(I)$ for all $u \in U$. A simpler, sufficient condition states: if I is generated by generic polynomials, then I is in generic coordinates.

Remark 3.2.4. Recall that every set of polynomials is a Zariski-open set if the coefficient field is finite. Hence, for genericity to be meaningful, the coefficient field must be an infinite field. Obviously, this affects our ability to apply results to cryptography, since MPKCs are typically defined over finite fields. We address this irregularity in Section 3.5.

Semi-regular sequences were first introduced by Pardue.

Definition 3.2.5 (Semi-regular sequence [73])**.** *Let $R = K[x_1, \ldots, x_n]$ and assume that K is an infinite field. If $A = R/I$, where I is a homogeneous ideal, and $f \in R_d$, then f is semi-regular on A if for every $e \geq d$, the map $A_{e-d} \to A_e$ given by multiplication by f is of maximal rank. A sequence of homogeneous polynomials $f_1, \ldots, f_m$ is a semi-regular sequence if each f_i is semi-regular on $A/\langle f_1, \ldots, f_{i-1}\rangle$, $1 \leq i \leq m$.*

The following conjecture suggests a connection between generic sequences of polynomials and semi-regular sequences of polynomials.

Conjecture 3.2.6 (Conjecture B, [73])**.** *If K is an infinite field and $R = K[x_1, \ldots, x_n]$, and $d_1, \ldots, d_r$ are non-negative integers, then a generic sequence of polynomials of*

[1] For existence of U and further properties of generic initial ideals, see §15.9 of [34].

degrees $d_1, \ldots, d_r$ is semi-regular.

Semi-regular sequences are interesting because their *Hilbert series* is known. Pardue proved that Conjecture 3.2.6 is equivalent to Fröberg's Conjecture [41], which suggests an expression for the Hilbert series of an ideal generated by generic polynomials and is known to be true for many ideals.

Let $h(z) = \sum_{d \geq 0} h_d z^d \in \mathbb{Z}[z]$ be a formal power series with integer coefficients. We denote by $[h(z)]$ the formal power series obtained by truncating $h(z)$ at the first non-positive coefficient, that is

$$[h(z)] = \sum_{d=0}^{D} h_d z^d,$$

where $D = \sup\{d \geq 0 \mid h_0, \ldots, h_d > 0\}$. The following proposition gives an explicit formula for the Hilbert series of a semi-regular sequence of m homogeneous polynomials in n variables. The proposition also gives an equivalent condition for semi-regularity, which is simpler to verify than Definition 3.2.5.

Proposition 3.2.7 ([73], Proposition 1)**.** *Let $f_1, \ldots, f_m \in R$ be homogeneous polynomials of degrees $d_1, \ldots, d_m$. Then $f_1, \ldots, f_m$ is a semi-regular sequence on R if and only if*

$$HS_{R/\langle f_1, \ldots, f_\ell \rangle}(z) = \left[\frac{\prod_{i=1}^{\ell}(1 - z^{d_i})}{(1-z)^n} \right]$$

for $1 \leq \ell \leq m$.

Semi-regular sequences were first considered in the context of multivariate cryptography by Bardet, Faugère, and Salvy in [3]. The definition of semi-regular sequences used in [3] differs from the one given by Pardue, notably by taking K to be an arbitrary field. Thus, the definition is applicable to systems arising in multivariate cryptography. To avoid ambiguity, the term cryptographic semi-regular sequence will be associated with the definition of Bardet, Faugère and Salvy [3] below:

Definition 3.2.8. *A sequence of homogeneous polynomials $f_1, \ldots, f_m \in R$ is a cryptographic semi-regular sequence if and only if*

$$HS_{R/\langle f_1,\ldots,f_m\rangle}(z) = \left[\frac{\prod_{i=1}^{m}(1-z^{d_i})}{(1-z)^n}\right].$$

Clearly, any semi-regular sequence is a cryptographic semi-regular sequence.

3.2.2 Gröbner bases

This section describes how a Gröbner basis can be used to solve a system of polynomial equations.

The Macaulay bound was shown by Lazard [67, Theorem 2] to be an upper bound for the degrees of the polynomials in a Gröbner basis of I, generated by a homogeneous system $\mathcal{F}$ that has finitely many solutions over the algebraic closure of K.

Definition 3.2.9. *Suppose $n \leq m$ and $d_1 \leq \cdots \leq d_m$. The Macaulay bound is*

$$\sum_{i=1}^{m}(d_i - 1) + 1.$$

Under the assumption that K is an infinite field, and that I is a radical ideal, the Shape Lemma [64] gives the general form of the reduced Gröbner basis of I with respect to the lexicographic ordering. Namely, the reduced lexicographic

Gröbner basis of I is of the form

$$\{g_n(x_n), x_{n-1} - g_{n-1}(x_n), \dots, x_1 - g_1(x_n)\}, \tag{3.1}$$

where $g_1, \dots, g_n$ are univariate polynomials in x_n and $\deg(g_1)$, …, $\deg(g_{n-1}) < \deg(g_n)$. However, in cryptography, systems are usually defined over finite fields and the condition that $\mathcal{F}$ generates a radical ideal does not always hold. Caminata and Gorla [19, Theorem 2.6] use the Elimination Theorem [28, Theorem 2] to prove that the reduced Gröbner basis of I can be used to solve the system $\mathcal{F} = 0$, even when these conditions are not satisfied. The Gröbner basis obtained has a similar form to Equation (3.1). Crucially, it contains a univariate polynomial. Thus, at least one variable can be eliminated and the system is simplified.

The most efficient ordering for computing a Gröbner basis is the degree reverse lexicographic (DRL) ordering. Faugère, Gianni, Lazard and Mora [39] developed an algorithm for transforming a Gröbner basis with respect to one ordering to a Gröbner basis for the same ideal with respect to another ordering. In particular, it is faster to compute a DRL Gröbner basis and convert it to a lexicographic one with this algorithm, than to directly compute a lexicographic Gröbner basis. Throughout this chapter, results on complexity are given with respect to the DRL ordering.

3.3 Estimating the solving degree

The complexity of Gröbner basis algorithms that employ Gaussian elimination is primarily determined by a quantity known as the *solving degree*.

Definition 3.3.1. *The solving degree of $\mathcal{F}$, $d_{\text{solve}}(\mathcal{F})$, is the degree d at which a Gröbner basis algorithm returns a DRL Gröbner basis of I.*

The solving degree dictates the size of the matrices occurring in the algorithm. This section begins by describing the family of Gröbner basis algorithms we are interested in, and showing the dependence of the complexity on the solving degree. Unfortunately, computing the solving degree is costly in practice and hence cryptographers work with approximations and bounds. Since the algorithm cost is bounded by an increasing function of the solving degree, finding an upper bound for the solving degree corresponds to bounding the complexity of the Gröbner basis algorithm. This, in turn, gives an estimate of the complexity of computing the solutions of the system $\mathcal{F}$.

Remark 3.3.2. To say that solving the system $\mathcal{F} = 0$ is at least as hard as solving some other system $\mathcal{F}' = 0$, one requires that $d_{\text{solve}}(\mathcal{F}') \leq d_{\text{solve}}(\mathcal{F})$. Using an upper bound to estimate the hardness of solving $\mathcal{F} = 0$ is a case of Koblitz and Menezes' first type of error. That is not to say, however, that efforts to find an upper bound for the solving degree are therefore irrelevant to cryptography. In fact, as highlighted by Koblitz and Menezes, and demonstrated throughout this thesis, proven results in cryptography are often difficult to obtain. Results of *this* kind, then, albeit not ideal, are still useful in telling cryptographers *something* about the systems they work with. We must still endeavour to make these results as strong as possible.

Bounding the solving degree is not a new focus of study, and cryptanalysts commonly use the results of [3], [38] to assess the security of multivariate cryptosystems. This section will end by recapitulating proposed upper bounds on the solving degree in literature:

1. the Castelnuovo-Mumford regularity (Section 3.3.2), and
2. the degree of regularity (Section 3.3.3).

Throughout, let $\mathcal{F} = \{f_1, \dots, f_m\} \subseteq R$ and fix the DRL order on R. Let $\mathcal{F}^{\text{top}}$ denote the system of equations comprising the homogeneous parts of highest degree of the polynomials in $\mathcal{F}$. Let $\mathcal{F}^h \subseteq R[t]$ denote the system of equations obtained by homogeonising the polynomials in $\mathcal{F}$ with the variable t. Additionally, let $d_{\text{solve}}(\mathcal{F})$ denote the solving degree of $\mathcal{F}$ and $d_{\text{reg}}(\mathcal{F})$ denote the degree of regularity of $\mathcal{F}$.

Example 3.3.3. Let $p = x_1x_2^2 + x_1x_2x_3 + x_1$. Then $p^{top} = x_1x_2^2 + x_1x_2x_3$ and $p^h = x_1x_2^2 + x_1x_2x_3 + x_1t^2$.

3.3.1 Complexity of a class of algorithms for computing Gröbner bases

We consider algorithms for computing Gröbner bases that use Gaussian elimination on Macaulay matrices of increasing degree.

Let $\text{Mon}(R)$ denote the set of all monomials in R. For $d \geq 1$, the Macaulay matrix $M_d(\mathcal{F})$ of a polynomial system $\mathcal{F} = \{f_1, \dots, f_m\}$ is a matrix with entries in K with:

– **Columns** indexed by all elements of $\text{Mon}(R)$ of degree $\leq d$, in decreasing order from left to right, and

– **Rows** indexed by the polynomials m_if_j, where $f_j \in \mathcal{F}$, $m_i \in \text{Mon}(R)$, and $\deg m_if_j \leq d$.

Therefore, the (k, l)-th entry of the matrix is the coefficient of the monomial indexed by l in the polynomial which is indexed by k.

Concretely, we consider the following (summarised) algorithm to compute the reduced Gröbner basis of I:

1. Start in degree $d = \max\{d_1, \ldots, d_m\}$ where d_i is the degree of f_i.
2. Perform Gaussian elimination on $M_d(\mathcal{F})$ to compute its reduced row echelon form (RREF). Since the rows of $M_d(\mathcal{F})$ correspond to the polynomials $m_i f_j$, Gaussian elimination corresponds to taking linear combinations of these polynomials. Hence, every row in the RREF corresponds to a polynomial in the ideal generated by $\mathcal{F}$.[2]
3. For each row[3], check the following condition:
   (a) If computing the RREF produces a row which corresponds to a polynomial f which has leading term strictly smaller than that of $m_i f_j$ and $\deg(f) < d$, then one appends to the matrix a new row uf for all $u \in \mathrm{Mon}(R)$ such that $\deg(uf) \leq d$.
4. Perform Gaussian elimination on the resulting matrix and repeat Step 3 until no further degree reductions are produced.
5. Check whether a Gröbner basis of I has been found. If yes, the algorithm terminates, otherwise d is increased by 1 and the process is repeated.

The complexity of such an algorithm is dominated by the complexity of computing the reduced row echelon form of the Macaulay matrices involved. This depends on the size to which the Macaulay matrices grow, which is determined by d. The maximum degree of the polynomials involved in the computation of the reduced DRL Gröbner basis of I is known as the solving degree.

[2] In order to track each row carefully, we use a variant of Gaussian elimination which does not permute rows.

[3] Suppose the kth row of $M_d(\mathcal{F})$ corresponds to the polynomial $m_i f_j$. Then the kth row in the RREF corresponds to a polynomial of the form $[m_i f_j +$ a linear combination of other rows of $M_d(\mathcal{F})]$.

The complexity of finding a Gröbner basis using Macaulay matrices and Gaussian elimination is bounded by a known function of the solving degree [3]:

Proposition 3.3.4. *The number of operations required to compute a Gröbner basis for $\mathcal{F}$, an over-determined system of m polynomials in n variables, is*

$$O\left(md\binom{n+d-1}{d}^{\omega}\right),$$

where d is the solving degree of the system and $2 \leq \omega < 2.39$ [3] is the linear algebra constant.

The algorithm as described will compute a Gröbner basis for I. It does not, however, give a method for verifying whether the final matrix output corresponds to a Gröbner basis. One stopping criterion is that the principal syzygies[4] corresponding to the output basis reduce to 0. However, this has its own obstruction. Suppose one wishes to verify the output after d iterations. The stopping criterion can be verified by Gaussian elimination, however, this will be of a matrix in degree d', where $d < d' < 2d - 1$.

Another possible stopping criterion is to identify an *a priori* bound on the solving degree. Concretely, if the solving degree of a system $\mathcal{F}$ is at most D, then the Gröbner basis algorithm can stop at degree D. This motivates the need to find good bounds for the solving degree.

3.3.2 Castelnuovo-Mumford regularity

The first approximation of the solving degree of a system of polynomials $\mathcal{F}$ is an invariant from commutative algebra: the Castelnuovo-Mumford regularity. Let

[4] Also known as S-polynomials, see [53].

$I \subseteq R$ be a homogeneous ideal where $\mathcal{F}$ comprises a minimal set of generators of I.

Definition 3.3.5 ([21])**.** *The Castelnuovo-Mumford regularity of I, $\operatorname{reg}_R(I)$, is defined as*

$$\operatorname{reg}_R(I) = \sup\{j - i : \ \beta^R_{i,j}(I) \neq 0\},$$

where the $\beta_{i,j}$ are the graded Betti numbers of I in the graded minimal free resolution of I. If $\mathcal{F} = \{f_1, \dots, f_m\}$ is a sequence of homogeneous polynomials, let $\operatorname{reg}_R(\mathcal{F})$ denote the regularity of the ideal $I = \langle \mathcal{F} \rangle$.

When the ring R is clear from context the notation $\operatorname{reg}(I)$ is used. Caminata and Gorla proved the following useful result in 2017.

Theorem 3.3.6 (Castelnuovo-Mumford bound on the solving degree [19])**.** *Let $\mathcal{F} = \{f_1, \dots, f_m\}$ be such that $\mathcal{F}^h$ is in generic coordinates. Then*

$$d_{\text{solve}}(\mathcal{F}) \leq \operatorname{reg}(\mathcal{F}^h).$$

Remark 3.3.7. Suppose $\mathcal{F}$ is a homogeneous cryptographic semi-regular sequence. The Castelnuovo-Mumford regularity of the ideal I generated by $\mathcal{F}$ is the least degree $d \geq 0$ for which $I_d = R_d$ [19]. This motivates a link between the Hilbert series of a sequence and the Castelnuovo-Mumford regularity.

The following lemma allows us to bound the degree of the elements of the DRL Gröbner basis of I. Note that this bound does not require I to be in generic coordinates.

Lemma 3.3.8. *Let $\mathcal{F}$ be cryptographic semi-regular sequence, generating the ideal I. Then,*

$$\deg_{\max}(I) \leq \operatorname{reg}(I).$$

Proof. By Theorem 7 of [19], $\deg_{\max}(I) \leq d_{\text{solve}}(\mathcal{F})$. Applying Theorem 3.3.6 then gives the desired result. □

Although the Castelnuovo-Mumford regularity is a proven upper bound on the solving degree of a system, in practice it is difficult to compute. Cryptographers largely use the degree of regularity instead.

3.3.3 The degree of regularity

The concept of degree of regularity of a system of equations was introduced by Bardet, Faugère and Salvy in [4] and in Bardet's PhD thesis [1].

Definition 3.3.9 (Degree of Regularity (Definition 4, [4]))**.** *Let $\mathcal{F}$ be a system of polynomial equations and assume that $(\mathcal{F}^{\text{top}})_d = R_d$ for $d \gg 0$. The degree of regularity of $\mathcal{F}$ is*

$$d_{\text{reg}}(\mathcal{F}) = \min\{d \geq 0 \mid (\mathcal{F}^{\text{top}})_d = R_d\}.$$

If $(\mathcal{F}^{\text{top}})_d \neq R_d$ for all $d \geq 0$, we let $d_{\text{reg}}(\mathcal{F}) = \infty$.

Crucial to Definition 3.3.9 being useful is the fact that $I_d^{\text{top}} = R_d$ for some d, that is, I_d^{top} should be Artinian (Definition 3.1.3).

Remark 3.3.10. The ideal $I \subseteq R$ is Artinian if and only if $HS_{R/I}(z)$ is a polynomial. Observe that for $d \geq 0$, $I_d = R_d \iff \dim_K(R/I)_{d'} = 0$ for $d' \geq d \iff HS_{R/I}(z)$ is a polynomial. As a consequence, any cryptographic semi-regular sequence with $m \geq n$ generates an Artinian ideal.

The degree of regularity is widely used as a heuristic upper bound for the solving degree of systems of equations arising in multivariate cryptography [10, 83, 87]. In [4], inhomogeneous cryptographic semi-regular sequences are defined as sequences $\mathcal{F}$ such that $\mathcal{F}^{\text{top}}$ is a cryptographic semi-regular sequence, according to Definition 3.2.8. Let $I^{\text{top}} = \langle \mathcal{F}^{\text{top}} \rangle$. If $I^{\text{top}}_d = R_d$ for $d \geq 0$, then $d_{\text{reg}}(\mathcal{F}) = \text{reg}(\mathcal{F}^{\text{top}})$ [19]. The bound follows from the following assumption.

Assumption 3.3.11. Let $\mathcal{F}$ be an inhomogeneous cryptographic semi-regular sequence of polynomials. Then, $\text{reg}(\mathcal{F}^{\text{top}}) \geq \text{reg}(\mathcal{F})$.

Clearly, if Assumption 3.3.11 holds, then the degree of regularity is an upper bound for the solving degree of $\mathcal{F}$. Bardet and Chyzak give asymptotic formulas for the degree of regularity for over-determined systems in [2].

3.4 Validity of the degree of regularity bound

There are several known examples in the literature that show that the degree of regularity is not a strict upper bound for the solving degree [19]. However, the difference between both degrees in these cases has been at most 1. The examples in this section demonstrate that the difference between the solving degree and the degree of regularity can be greater than 1.

3.4.1 Method for computing step degree and degree of regularity

The solving degree and degree of regularity of the examples in Section 3.4.2 were computed using the computer algebra system `Magma` [15].

Computing the solving degree `Magma` does not directly compute the solving degree, so the *maximum step degree* is used as a substitute. Concretely, the maximum step degree is the largest step degree output in the `Magma` implementation of the F4 Gröbner basis algorithm. Since the implementation is not publicly available, equality between the two degrees remains a working assumption. Having corresponded with representatives of `Magma` at the University of Sydney to determine the veracity of this conjecture, we received confirmation that the maximum step degree was a valid substitute for solving degree, as it is defined herein. However, without access to the implementation, in particular, the stopping criterion, we have not been able to verify this independently.

Computing the degree of regularity The degree of regularity was computed by calling `Regularity(GradedModule(F^top))`, where $\texttt{F}^{\texttt{top}}$ is the `Magma` instantiation of $\mathcal{F}^{\mathrm{top}}$ as defined in Section 3.3.3.

3.4.2 Greater differences between solving degree and degree of regularity

The following examples are of multivariate polynomial systems which yield a solving degree that is both greater than the degree of regularity for the system, and with a difference greater than 1. They are inspired by examples from [7].

Example 3.4.1. Let $R = \mathbb{F}_7[x, y, z]$ and let $f_x = x^7 - x$, $f_y = y^7 - y$, $f_z = z^7 - z$ be the field equations. Consider the equations

$$f_1 = x^5 + y^5 + z^5 - 1,\ f_2 = x^3 + y^3 + z^2 - 1,\ f_3 = y^6 - 1,\ f_4 = z^6 - 1.$$

Consider the systems of equations

$$\mathcal{F} = \left\{ \prod_{j=1}^{3} f_{i_j} \,\middle|\, 1 \leq i_1 \leq i_2 \leq i_3 \leq 4 \right\} \cup \{f_x, f_y, f_z\}.$$

Using `Magma` the solving degree and degree of regularity are computed as

$$d_{\text{solve}}(\mathcal{F}) = 24 > 15 = d_{\text{reg}}(\mathcal{F}).$$

Example 3.4.2. Let $R = \mathbb{F}_7[x, y, z]$ and let $f_x = x^7 - x$, $f_y = y^7 - y$, $f_z = z^7 - z$ be the field equations. Consider the equations

$$f_1 = x^5 + y^5 + z^5 - 1,\ f_2 = x^3 + y^3 + z^2 - 1,\ f_3 = f_x,\ f_4 = f_y,\ f_6 = f_z.$$

Consider the systems of equations

$$\mathcal{F} = \left\{ \prod_{1 \leq i \leq j \leq 6} f_i f_j \right\} \cup \{f_x, f_y, f_z\}.$$

Using `Magma` the solving degree and degree of regularity are computed as

$$d_{\text{solve}}(\mathcal{F}) = 21 > 13 = d_{\text{reg}}(\mathcal{F}).$$

Relevance to cryptography Since the degree of regularity is used to assess the security of cryptographic systems, it would be very helpful to find counterexamples that arise naturally in cryptography. It should be clear immediately that the two examples provided in Section 3.4.2 are too small to make effective cryptosystems. Moreover, they were not intentionally constructed with a well-defined ‘trapdoor’, as would be the case for a multivariate cryptosystem.

It is unclear whether there are certain properties of a system of polynomials that will lead to a larger difference between solving degree and degree of regularity. Hence, finding counterexamples is an exercise in trial-and-error and the parameter sizes used in cryptography make computing the solving degree of most instances infeasible. That is not to say the examples provided are without consequence: clearly, it is not inconceivable that a multivariate cryptosystem will or does exist, for which the degree of regularity is not an upper bound on the solving degree. For this reason, we argue that it is preferable to use a proven bound to make complexity (and, thereby, security) arguments.

3.5 Upper bounds on the solving degree for over-determined systems

Since there exist examples of polynomial systems for which the degree of regularity is not a valid upper bound for the solving degree, the focus turns to the Castelnuovo-Mumford regularity. Caminata and Gorla proved that this gives a proven upper bound for the solving degree [19].

If $m > n$, asymptotic formulas for the degree of regularity of a cryptographic semi-regular sequence are given in [3, 4]. We have discussed the limitations of relying on asymptotic formulas when determining concrete security values in Chapter 1. The focus on this section is therefore to find an explicit formula for upper bounds on the solving degree of certain over-determined systems.

Let $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R$ be a system of multivariate polynomial equations.

We first restrict to polynomial systems where $m-n$ is small: explicitly, systems of equations where $m=n+1$, systems of quadratic equations where $n+2 \leq m \leq n+5$ and systems of cubic equations for $m=n+2$. We note that there are no current multivariate cryptosystems with such small values for $m-n$. However, we also show that the upper bounds on solving degrees for these systems can be extended to larger systems, that is, where $m > n+5$.

Section 3.5.1 contains explicit formulas for bounds on the solving degree of $\mathcal{F}$ when the polynomials are homogeneous. To motivate the application to systems arising in cryptography, systems over both infinite and finite fields are considered. These results are then applied to systems of inhomogeneous polynomials in Section 3.5.2, again covering infinite and finite fields.

Throughout, let $d_{\text{solve}}(\mathcal{F})$ denote the solving degree of $\mathcal{F}$, $\deg_{\max}(I)$ denote the maximum degree of the polynomials in the DRL Gröbner basis of I and $d_{\text{reg}}(\mathcal{F})$ denote the degree of regularity of $\mathcal{F}$.

3.5.1 Homogeneous cryptographic semi-regular sequences

Let $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R$ be a system of homogeneous multivariate polynomial equations in n variables and let $d_i = \deg(f_i)$.

3.5.1.1 Case 1: $m = n+1$

Suppose $m = n+1$ and, without loss of generality, let $d_1 \leq \cdots \leq d_{n+1}$ and take $\mathcal{F}$ defined over an infinite field. Recall that this is necessary for the polynomials in $\mathcal{F}$ to be generic. Assuming Pardue's conjecture, such a sequence is also a semi-regular sequence.

The following result of Migliore and Mirò-Roig [70] applies to systems of generic polynomials that generate the ideal I, when I is an almost complete intersection.

Lemma 3.5.1 ([70], Lemma 2.5)**.** *The maximal socle degree of R/I is*

$$\left\lfloor \frac{1}{2}\left(\left(\sum_{i=1}^{n+1} d_i\right) - n - 1\right)\right\rfloor,$$

where the maximal socle degree refers to the degree of the last non-zero component of the minimal resolution of R/I.

Assume $\mathcal{F}$ is a system of generic polynomials. Then $\langle f_1, \dots, f_n\rangle$ is a complete intersection, as the polynomials are defined in n variables. Suppose that $\deg(f_{n+1}) \geq \left(\sum_{i=1}^{n} d_i\right) - n$. Then $f_{n+1} \in \langle f_1, \dots, f_n\rangle$ and so I is a complete intersection. Hence, without loss of generality, we take $\deg(f_{n+1}) < \left(\sum_{i=1}^{n} d_i\right) - n$. Then I is an almost complete intersection and so Lemma 3.5.1 applies. Note that in this case the socle degree coincides with the Castelnuovo-Mumford regularity. The following theorem uses these results to bound the solving degree.

Theorem 3.5.2. *Let K be an infinite field and let $\mathcal{F} = \{f_1, \dots, f_{n+1}\}$ consist of $n+1$ generic homogeneous polynomials of degrees $d_i = \deg(f_i)$ in n variables. Let $d_1 \leq d_2 \leq \cdots \leq d_{n+1}$. Assume without loss of generality that $d_{n+1} < d_1 + \cdots + d_n - n$. Then $\mathcal{F}$ is a cryptographic semi-regular sequence and*

$$d_{\text{solve}}(\mathcal{F}) \leq \left\lfloor \frac{d_1 + \cdots + d_{n+1} - n - 1}{2} \right\rfloor + 1.$$

Proof. The Hilbert series of $\mathcal{F}$ is known, by results from Watanabe [86] (in particular Theorem 3.8) and satisfies Definition 3.2.8 [70, §2]. Hence, $\mathcal{F}$ is a cryptographic semi-regular sequence.

Since $d_{n+1} < d_1 + \cdots + d_n - n$, I is an almost complete intersection. By Lemma 3.5.1,

$$\mathrm{reg}(I) = \left\lfloor \frac{d_1 + \cdots + d_{n+1} - n - 1}{2} \right\rfloor + 1.$$

Moreover I is in generic coordinates, as it is generated by generic polynomials. Therefore, applying Theorem 3.3.6 yields the bound for the solving degree of $\mathcal{F}$. □

Remark 3.5.3. Since $d_{n+1} < d_1 + \cdots + d_n - n$, $\mathrm{reg}(I) < d_1 + \cdots + d_n - n + 1$, which is, of course, the Macaulay bound (Definition 3.2.9). Therefore, the bound on the solving degree resulting from Theorem 3.5.2 is *better* than the Macaulay bound.

Corollary 3.5.4. *Let K be an infinite field and let $\mathcal{F} = \{f_1, \ldots, f_{n+1}\}$ consist of $n+1$ generic homogeneous quadratic polynomials in n variables. Then* $\deg(f_i) = 2$ *for all $i = 1, \ldots, n+1$ and*

$$d_{\mathrm{solve}}(\mathcal{F}) \leq \left\lfloor \frac{n+1}{2} \right\rfloor + 1$$

Corollary 3.5.5. *Let K be an infinite field and let $\mathcal{F} = \{f_1, \ldots, f_{n+1}\}$ consist of $n+1$ generic homogeneous cubic polynomials in n variables. Then* $\deg(f_i) = 3$ *for all $i = 1, \ldots, n+1$ and*

$$d_{\mathrm{solve}}(\mathcal{F}) \leq n + 2.$$

To apply these results to systems arising in multivariate cryptography, we assume $\mathcal{F}$ is a cryptographic semi-regular sequence as in Definition 3.2.8. The probability of this assumption holding is discussed in Section 3.6.1. If $\mathcal{F}$ generates an ideal in generic coordinates then the same bound on the solving degree holds.

Theorem 3.5.6. *Let K be a finite field and let $\mathcal{F} = \{f_1, \ldots, f_{n+1}\}$ be a homoge-*

neous cryptographic semi-regular sequence of polynomials of degrees $d_i = \deg(f_i)$ *in* n *variables. Let* $I = \langle \mathcal{F} \rangle$ *and suppose* I *is in generic coordinates. Let* $d_1 \leq d_2 \leq \cdots \leq d_{n+1}$*. Assume without loss of generality that* $d_{n+1} < d_1 + \cdots + d_n - n$*.*

Then

$$d_{\text{solve}}(\mathcal{F}) \leq \left\lfloor \frac{d_1 + \cdots + d_{n+1} - n - 1}{2} \right\rfloor + 1.$$

Additionally, by Theorem 3.5.6 and Lemma 3.3.8, for $m = n + 1$, the degree of the elements of the DRL Gröbner basis of I, are bounded as:

$$\deg_{\max}(I) \leq \left\lfloor \frac{d_1 + \cdots + d_{n+1} - n - 1}{2} \right\rfloor + 1.$$

Moreover, for systems of all quadratic or all cubic polynomials, Theorem 3.5.6 yields the following bounds on the solving degree.

Corollary 3.5.7. *Let* K *be a finite field and let* $\mathcal{F} = \{f_1, \ldots, f_{n+1}\}$ *be a homogeneous cryptographic semi-regular sequence of* $n + 1$ *quadratic polynomials in* n *variables. Suppose* $I = \langle \mathcal{F} \rangle$ *is in generic coordinates. Then* $\deg(f_i) = 2$ *for all* $i = 1, \ldots, n + 1$ *and*

$$d_{\text{solve}}(\mathcal{F}) \leq \left\lfloor \frac{n+1}{2} \right\rfloor + 1$$

Corollary 3.5.8. *Let* K *be a finite field and let* $\mathcal{F} = \{f_1, \ldots, f_{n+1}\}$ *be a homogeneous cryptographic semi-regular sequence of* $n+1$ *cubic polynomials in* n *variables. Let* $I = \langle \mathcal{F} \rangle$*, and suppose* I *is in generic coordinates. Then* $\deg(f_i) = 3$ *for all* $i = 1, \ldots, n + 1$ *and*

$$d_{\text{solve}}(\mathcal{F}) \leq n + 2.$$

3.5.1.2 Case 2: $n+2 \leq m \leq n+5, d_i = 2$ for all $i = 1, \ldots, m$

Let $n+2 \leq m \leq n+5$ and assume that $\mathcal{F}$ is a cryptographic semi-regular sequence of homogeneous quadratic equations. By Definition 3.2.8 and Definition 3.1.3, and since $m > n$, there exists a d such that $I_d = R_d$. The Castelnuovo-Mumford regularity of I is the least such degree. Consequently, $\text{reg}(I)$ is the least degree d for which the coefficient of z^d in the power series $(1-z^2)^m/(1-z)^n$ is non-positive. We hence also refer to this value as the *index of regularity*. Expanding the Hilbert series for $n, m = n + \ell$ gives

$$\begin{aligned}\frac{(1-z^2)^m}{(1-z)^n} &= (1-z)^\ell(1+z)^m \\ &= \left(1 - \binom{\ell}{1}z + \cdots + \binom{\ell}{\ell}(-1)^\ell z^\ell\right)\left(1 + \binom{m}{1}z + \cdots + \binom{m}{m}z^m\right) \\ &= \sum_{k=0}^{m+\ell} \alpha_k z^k,\end{aligned}$$

where α_k, the coefficient of z^k, is

$$\alpha_k = \sum_{j=0}^{k} (-1)^j \binom{\ell}{j}\binom{m}{k-j}. \tag{3.2}$$

The smallest k for which α_k is non-positive will give $\text{reg}(I)$. However, this k is not easily read from Equation (3.2). Note that for $k \geq \ell$, $\binom{\ell}{k} = 0$ and so by expanding and simplifying the binomial coefficients

$$\begin{aligned}\alpha_k &= \sum_{j=0}^{\ell}\left((-1)^j\binom{\ell}{j}\binom{m}{k-j}\right) \\ &= \frac{m!}{k!(2\ell+n-k)!}f(\ell,k),\end{aligned}$$

where

$$f(\ell, k) = \ell! \sum_{j=0}^{\ell} \left((-1)^j \binom{2\ell + n - k}{\ell - j} \binom{k}{j} \right). \tag{3.3}$$

Clearly, $\alpha_k \leq 0 \iff f(\ell, k) \leq 0$. Hence, finding $\operatorname{reg}(I)$ is reduced to finding minimal k such that $f(\ell, k) \leq 0$. Expanding Equation (3.3) and finding zeroes for $r = 2, 3, 4, 5$ gives the following theorem.

Theorem 3.5.9. *Let $\mathcal{F} = \{f_1, \ldots, f_m\}$ be a cryptographic semi-regular sequence of homogeneous polynomials of degree 2 in n variables. Let $I = \langle \mathcal{F} \rangle$ and let*

$$r(m, n) = \begin{cases} \left\lceil (4 + n - \sqrt{4 + n})/2 \right\rceil & \text{if } m = n + 2, \\ \left\lceil (6 + n - \sqrt{16 + 3n})/2 \right\rceil & \text{if } m = n + 3, \\ \left\lceil (8 + n - \sqrt{20 + 3n + \sqrt{2}\sqrt{128 + 39n + 3n^2}})/2 \right\rceil & \text{if } m = n + 4, \\ \left\lceil (10 + n - \sqrt{40 + 5n + \sqrt{2}\sqrt{288 + 75n + 5n^2}})/2 \right\rceil & \text{if } m = n + 5. \end{cases}$$

Then

$$\deg_{\max}(I) \leq r(m, n).$$

If in addition we assume that I is in generic coordinates, then

$$d_{\text{solve}}(\mathcal{F}) \leq r(m, n).$$

Proof. We have that the Castelnuovo-Mumford regularity of I is $\operatorname{reg}(I) = r(m, n)$.

Let $\ell = 2, 3, 4, 5$ in Equation (3.3), yielding the following functions:

$$\begin{aligned}
f(2,k) =& 4k^2 - 4(4+n)k + n^2 + 7n + 12, \\
f(3,k) =& -8k^3 + 12(6+n)k^2 - 2(92 + 33n + 3n^2)k + n^3 + 15n^2 + 74n + 120, \\
f(4,k) =& 16k^4 - 32(8+n)k^3 + 8(172 + 45n + 3n^2)k^2 \\
& - 8(352 + 148n + 21n^2 + n^3)k \\
& + n^4 + 26n^3 + 251n^2 + 1066n + 1680 \\
\text{and } f(5,k) =& -32k^5 + 80(10+n)k^4 - 80(92 + 19n + n^2)k^3 \\
& - 2(27024 + 12450n + 2175n^2 + 170n^3 + 5n^4)k \\
& + 40(760 + 246n + 27n^2 + n^3)k^2 \\
& + n^5 + 40n^4 + 635n^3 + 5000n^2 + 19524n + 30240.
\end{aligned}$$

Considering $f(\ell, k)$ as a function of k, we solve for k_ℓ, the point at which $f(\ell, k)$ first becomes non-positive[5]. We find

$$\begin{aligned}
k_2 &= (4 + n - \sqrt{4+n})/2 \\
k_3 &= (6 + n - \sqrt{16+3n})/2 \\
k_4 &= (8 + n - \sqrt{20 + 3n + \sqrt{2}\sqrt{128 + 39n + 3n^2}})/2 \\
\text{and } k_5 &= \frac{1}{2}\left(10 + n - \sqrt{40 + 5n + \sqrt{2}\sqrt{288 + 75n + 5n^2}}\right).
\end{aligned}$$

Recall that the index must be an integer, so taking $k = \lceil k_\ell \rceil$ gives the first non-positive α_k for a particular ℓ.[6]

[5] The zeroes of the functions $f(\ell, k)$ were computed using Mathematica [88].

[6] For each ℓ, it was checked that $\lceil k_\ell \rceil$ is not larger than that next largest zero of $f(\ell, k)$, so this α_k is indeed non-positive.

If I is in generic coordinates, applying Theorem 3.3.6 bounds the solving degree. The bound on degrees $\deg_{\max}$ follows from Lemma 3.3.8. □

3.5.1.3 Case 3: $m = n+1, d_i = 3$ for all $i = 1, \ldots, m$

Let $m = n+1$ and assume that $\mathcal{F}$ is a cryptographic semi-regular sequence of cubic equations. Analogous to Theorem 3.5.9, examining the Hilbert series for m, n, yields the following theorem.

Theorem 3.5.10. *Let $\mathcal{F} = \{f_1, \ldots, f_{n+1}\}$ be a cryptographic semi-regular sequence of homogeneous polynomials of degree 3 in n variables. Let $I = \langle \mathcal{F} \rangle$, then*

$$\deg_{\max}(I) \leq n+2.$$

If in addition we assume that I is in generic coordinates, then

$$d_{\text{solve}}(\mathcal{F}) \leq n+2.$$

Proof. Consider the Hilbert series for $m = n+1, d_i = 3$ for all $i = 1, \ldots, m$,

$$\begin{aligned}\frac{(1-z^3)^{n+1}}{(1-z)^n} &= (1-z)(1+z+z^2)^{n+1} \\ &= (1-z)\sum_{k=0}^{2n+2} \binom{n+1}{k}_2 z^k \\ &= 1 + \sum_{i=1}^{2n+3} \left(\binom{n+1}{k}_2 - \binom{n+1}{k-1}_2 \right) z^k,\end{aligned}$$

where $\binom{n}{k}_p$ is the polynomial coefficient[7] of z^k in the polynomial $(1+z+\cdots+z^p)^n$.

[7] $\binom{n}{k}_p$ is also referred to as the extended binomial coefficient.

Many of the known binomial coefficient identities can be extended to polynomial coefficients [36]. In particular, symmetry, where

$$\binom{n}{k}_p = \binom{n}{pn-k}_p, \; n \geq 0. \tag{3.4}$$

For $p = 2$, these are known as the trinomial coefficients. For fixed n, the trinomial coefficients $\binom{n}{k}_2$ increase for $0 \leq k \leq n$ due to the recurrence relation $\binom{n}{k}_2 = \binom{n-1}{k-1}_2 + \binom{n-1}{k}_2 + \binom{n-1}{k+1}_2$. The central trinomial coefficient, $\binom{n}{n}_2$ for fixed n, is the largest coefficient. The sequence of central trinomial coefficients was studied in depth by Euler [35], so we do not belabour the details here.

The coefficient of z^k is

$$\alpha_k = \binom{n+1}{k}_2 - \binom{n+1}{k-1}_2. \tag{3.5}$$

Since the trinomial coefficients increase with increasing k (up to n), α_k is positive for all $0 \leq k \leq n+1$. Now, consider $k = n+2$. Then,

$$\begin{aligned}\alpha_{n+2} &= \binom{n+1}{n+2}_2 - \binom{n+1}{n+1}_2 \\ &= \binom{n+1}{n}_2 - \binom{n+1}{n+1}_2 \text{ by Equation (3.4)} \\ &= -\alpha_{n+1} < 0.\end{aligned}$$

The bound on degrees $\deg_{\max}$ follows from Lemma 3.3.8. If I is in generic coordinates, applying Theorem 3.3.6 bounds the solving degree. □

3.5.1.4 Case 4: Greater values of m

Suppose $\mathcal{F}$ is a homogeneous cryptographic semi-regular sequence of equations. Then, Theorem 3.5.9 and Theorem 3.5.10 can be used to obtain an upper bound for the solving degree of $\mathcal{F}$ for greater values of m.

Corollary 3.5.11. *Let $\mathcal{F} = \{f_1, \ldots, f_m\}$ be a cryptographic semi-regular sequence of homogeneous polynomials of degree $d = 2, 3$ in n variables. Assume that $m \geq n + 5$ if $d = 2$ and that $m \geq n + 1$ if $d = 3$. Let $I = \langle \mathcal{F} \rangle$ and let*

$$r(n,d) = \begin{cases} \left\lceil (10 + n - \sqrt{40 + 5n + \sqrt{2}\sqrt{288 + 75n + 5n^2}})/2 \right\rceil & \text{if } d = 2, \\ n + 2 & \text{if } d = 3. \end{cases}$$

Then

$$\deg_{\max}(I) \leq r(n,d).$$

If in addition we assume that I is in generic coordinates, then

$$d_{\text{solve}}(\mathcal{F}) \leq r(n,d).$$

Proof. For $d = 2$, $m \geq n + 5$. Note that I contains an ideal J generated by a cryptographic semi-regular sequence consisting of $n + 5$ homogeneous quadratic polynomials (for instance, take the first $n + 5$ polynomials in $\mathcal{F}$ as generators).

For $d = 3$, $m \geq n + 1$. Again, observe that I contains an ideal J generated by a cryptographic semi-regular sequence consisting of $n + 1$ homogeneous quadratic polynomials (for instance, take the first $n + 1$ polynomials in $\mathcal{F}$ as generators).

Note that J is Artinian as $m \geq n$. Then, $\text{reg}(I) \leq \text{reg}(J)$ [19]. Theorem 3.5.9 and Theorem 3.5.10 provide values for $\text{reg}(J)$ for $d = 2$ and $d = 3$, respectively.

The bound on degrees $\deg_{\max}$ follows from Lemma 3.3.8. If I is in generic coordinates, applying Theorem 3.3.6 bounds the solving degree. □

3.5.2 Inhomogeneous cryptographic semi-regular sequences

Let $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R$ be a system of inhomogeneous multivariate polynomial equations in n variables and let $d_i = \deg(f_i)$. We expect this type of sequence to arise more often from MPKCs.

Consider I^h, the homogenised ideal of $\mathcal{F}$, which is generated by $\mathcal{F}^h$. We have the following definition for inhomogeneous cryptographic semi-regular sequences of equations.

Definition 3.5.12. *An inhomogeneous system of polynomials $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R$ is a cryptographic semi-regular sequence if $\mathcal{F}^h = \{f_1^h, \ldots, f_m^h\} \subseteq S = R[t]$ is a cryptographic semi-regular sequence.*

Definition 3.5.12 allows us to apply the results on homogeneous systems from Section 3.5.1 to systems of inhomogeneous polynomials.

3.5.2.1 Case 1: $m = n + 1$

Let $m = n + 1$ and suppose $\mathcal{F}$ is a semi-regular sequence of generic polynomials. Then the homogenisation $\mathcal{F}^h$ is a semi-regular sequence of $n+1$ generic polynomials in $n + 1$ variables. The next theorem now follows from Theorem 3.5.2.

Theorem 3.5.13. *Let K be an infinite field and let $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R$ be a sequence of generic inhomogeneous polynomials of degrees $d_i = \deg(f_i)$, with $m \in \{n + 1, n + 2\}$. If $m = n + 2$, assume without loss of generality that $d_{n+2} <$*

$d_1 + \cdots + d_{n+1} - n - 1$. *Then $\mathcal{F}$ is a cryptographic semi-regular sequence and*

$$d_{\text{solve}}(\mathcal{F}) \leq \begin{cases} d_1 + \cdots + d_{n+1} - n & \text{if } m = n+1, \\ \left\lfloor \frac{d_1+\cdots+d_{n+2}-n-2}{2} \right\rfloor + 1 & \text{if } m = n+2. \end{cases}$$

Proof. If $m = n+1$, then $\mathcal{F}^h$ is a sequence of $n+1$ generic homogeneous polynomials in $n+1$ variables, hence it is a regular sequence. The result follows from the Macaulay bound. If $m = n+2$, applying Theorem 3.5.2 to $\mathcal{F}^h$ bounds the solving degree of $\mathcal{F}$. □

Corollary 3.5.14. *Let K be an infinite field and let $\mathcal{F} = \{f_1, \ldots, f_{n+1}\}$ consist of $n+1$ generic inhomogeneous quadratic polynomials in n variables. Then* $\deg(f_i) = 2$ *for all $i = 1, \ldots, m$ and*

$$d_{\text{solve}}(\mathcal{F}) \leq \begin{cases} n+2 & \text{if } m = n+1, \\ \left\lfloor \frac{n}{2} \right\rfloor + 2 & \text{if } m = n+2, \end{cases}$$

Corollary 3.5.15. *Let K be an infinite field and let $\mathcal{F} = \{f_1, \ldots, f_{n+1}\}$ consist of $n+1$ generic inhomogeneous cubic polynomials in n variables. Then* $\deg(f_i) = 3$ *for all $i = 1, \ldots, m$ and*

$$d_{\text{solve}}(\mathcal{F}) \leq \begin{cases} 2n+3 & \text{if } m = n+1, \\ n+3 & \text{if } m = n+2. \end{cases}$$

For systems arising in multivariate cryptography, we assume $\mathcal{F}$ is a cryptographic semi-regular sequence as in Definition 3.5.12 and that $\mathcal{F}^h$ generates an ideal in generic coordinates. Then, the same bound on the solving degree holds.

Theorem 3.5.16. *Let K be a finite field and let $\mathcal{F} = \{f_1, \dots, f_m\} \subseteq R$ be a cryptographic semi-regular sequence of inhomogeneous polynomials of degrees $d_i = \deg(f_i)$, with $m \in \{n+1, n+2\}$. Let $I = \langle \mathcal{F} \rangle$. If $m = n+2$, assume without loss of generality that $d_{n+2} \leq d_1 + \cdots + d_{n+1} - n - 1$. Let*

$$r(n, d_1, \dots, d_m) = \begin{cases} d_1 + \cdots + d_{n+1} - n & \text{if } m = n+1, \\ \left\lfloor \frac{d_1 + \cdots + d_{n+2} - n - 2}{2} \right\rfloor + 1 & \text{if } m = n+2. \end{cases}$$

Then

$$\deg_{\max}(I) \leq r(n, d_1, \dots, d_m).$$

If $I^h = \langle \mathcal{F}^h \rangle$ is in generic coordinates, then

$$d_{\text{solve}}(\mathcal{F}) \leq r(n, d_1, \dots, d_m).$$

Corollary 3.5.17. *Let K be a finite field and let $\mathcal{F} = \{f_1, \dots, f_{n+1}\}$ be a cryptographic semi-regular sequence of inhomogeneous quadratic polynomials in n variables. Suppose I^h is in generic coordinates. Then* $\deg(f_i) = 2$ *for all $i = 1, \dots, m$ and*

$$r(n, 2, \dots, 2) = \begin{cases} n+2 & \text{if } m = n+1, \\ \left\lfloor \frac{n}{2} \right\rfloor + 2 & \text{if } m = n+2, \end{cases}$$

Corollary 3.5.18. *Let K be a finite field and let $\mathcal{F} = \{f_1, \dots, f_{n+1}\}$ cryptographic semi-regular sequence of inhomogeneous cubic polynomials in n variables. Suppose*

I^h is in generic coordinates. Then $\deg(f_i) = 3$ *for all* $i = 1, \ldots, m$ *and*

$$r(n, 3, \ldots, 3) = \begin{cases} 2n+3 & \textit{if } m = n+1, \\ n+3 & \textit{if } m = n+2. \end{cases}$$

3.5.2.2 Case 2: $m \geq n+3, d_i = 2$ for all $i = 1, \ldots, m$

Let $m \geq n+3$ and assume that $\mathcal{F}$ is a cryptographic semi-regular sequence of quadratic equations. Using the same techniques as in the previous subsection, the next theorem follows from Theorem 3.5.9 and Corollary 3.5.11.

Theorem 3.5.19. *Let* $\mathcal{F} = \{f_1, \ldots, f_m\}$ *be a cryptographic semi-regular sequence of inhomogeneous polynomials of degree* 2 *in* n *variables. Let* $I = \langle \mathcal{F} \rangle$ *and let*

$$r(m,n) = \begin{cases} \left\lceil (5+n-\sqrt{5+n})/2 \right\rceil & \textit{if } m = n+3, \\ \left\lceil (7+n-\sqrt{19+3n})/2 \right\rceil & \textit{if } m = n+4, \\ \left\lceil (9+n-\sqrt{23+3n+\sqrt{2}\sqrt{170+45n+3n^2}})/2 \right\rceil & \textit{if } m = n+5, \\ \left\lceil (11+n-\sqrt{45+5n+\sqrt{2}\sqrt{368+85n+5n^2}})/2 \right\rceil & \textit{if } m \geq n+6. \end{cases}$$

then

$$\deg_{\max}(I) \leq r(m,n).$$

If $I^h = \langle \mathcal{F}^h \rangle$ *is in generic coordinates, then*

$$d_{\text{solve}}(\mathcal{F}) \leq r(m,n).$$

3.5.2.3 Case 3: $m \geq n+2, d_i = 3$ for all $i = 1, \ldots, m$

Let $m \geq n+2$ and assume that $\mathcal{F}$ is a cryptographic semi-regular sequence of cubic equations. Using the same techniques as in the previous two subsections, the next theorem follows from Theorem 3.5.10 and Corollary 3.5.11.

Theorem 3.5.20. *Let $m \geq n+2$ and let $\mathcal{F} = \{f_1, \ldots, f_m\}$ be a cryptographic semi-regular sequence of inhomogeneous polynomials of degree* 3 *in n variables. Let $I = \langle \mathcal{F} \rangle$, then*

$$\deg_{\max}(I) \leq n+3.$$

If $I^h = \langle \mathcal{F}^h \rangle$ is in generic coordinates, then

$$d_{\text{solve}}(\mathcal{F}) \leq n+3.$$

3.6 Impact and limitations

3.6.1 Genericity assumptions in proofs

There are two major assumptions made in the proofs of Section 3.5 regarding sequences of polynomials over finite fields:

1. $\mathcal{F}$ generates an ideal in generic coordinates.

and

2. $\mathcal{F}$ is a cryptographic semi-regular sequence.

Generic coordinates MPKCs are usually defined over finite fields, whereas the definition of generic coordinates is given for systems over an infinite field. However, applying a generic change of coordinates to the ideal generated by $\mathcal{F}$, over a large enough extension field of K, will put I in generic coordinates [19]. Furthermore, Caminata and Gorla proved that if $\mathcal{F}$ contains the field equations then the ideal $I = \langle \mathcal{F} \rangle$ will be in generic coordinates [19, Theorem 3.26]. The same result holds when we consider the homogenised system determined by $\mathcal{F}$. Specifically, the ideal $\langle \mathcal{F}^h \rangle$ is in generic coordinates if $\mathcal{F}$ contains the field equations.

For cryptanalysis it is often common practice to include the field equations for security analysis. Therefore, the first assumption would not affect applicability of the results contained in this chapter to these cryptographic systems. We note, however, that over large fields including the field equations can make Gröbner basis computation infeasible.

Cryptographic semi-regular sequences The assumption that the sequences of polynomials arising in cryptography are cryptographic semi-regular is not new to this thesis and is in fact used by Bardet, Faugère and Salvy [3]. Hence, this assumption has no real impact in terms of comparing the two methods of approximation.

We will now discuss the existence of cryptographic semi-regular sequences. To begin with, recall that any semi-regular sequence is a cryptographic semi-regular sequence. Pardue's conjecture implies that most systems of polynomial equations with coefficients that are chosen at random from an infinite field are semi-regular. The same conjecture is made for 'large enough' finite fields. With greater relevance for cryptography, Hodges, Molina and Schlather show that the proportion of sequences of homogeneous polynomials with coefficients in $\mathbb{F}_2$ of degree $d \geq 2$ that are semi-regular tends to 1 as the number of variables tends to infinity [49, Theorem 6.4]. It remains for future work to prove these results in finite fields other than $\mathbb{F}_2$.

3.6.2 Large values of ℓ

The method we use to find an exact formula for the index of regularity $r(n+\ell, n)$, requires a solution to the function $f(\ell, k)$, which is a degree ℓ polynomial in k. We do not determine a general equation for $r(n+\ell, n)$ for $\ell \geq 6$, primarily due to our use of Mathematica to compute the zeroes of $f(\ell, k)$. Nonetheless, we have shown that it is still possible to find an explicit bound on the index of regularity by looking at ideals contained in the ideal generated by $\mathcal{F}$. The resulting bounds are unfortunately not tight, as illustrated by Figure 3.1. However, we note that for arbitrarily large values of n the bounds of [3] can be used.

For the purposes of achieving a more accurate approximation of the solving degree of cryptographic semi-regular systems of $m = n+\ell$ homogeneous quadratic polynomials, we have therefore computed the exact values of $r(n+\ell, n)$ for $2 \leq \ell, n \leq 500$. These are available at: `http://bit.ly/wine-3`. This thesis includes the values for $2 \leq n, \ell \leq 100$ in Appendix A.

3.6.3 Impact on complexity

We now look at the effect that $d_{\text{reg}} < d_{\text{solve}}$ has on bounding the complexity of computing a Gröbner basis algorithm. To illustrate our analysis, we consider parameters with existing multivariate cryptosystems in mind: the Simple Matrix (or ABC) encryption System [82] and HFERP [50]. Recall that for a system $\mathcal{F}$ of m polynomials in n variables, the number of operations required to compute a

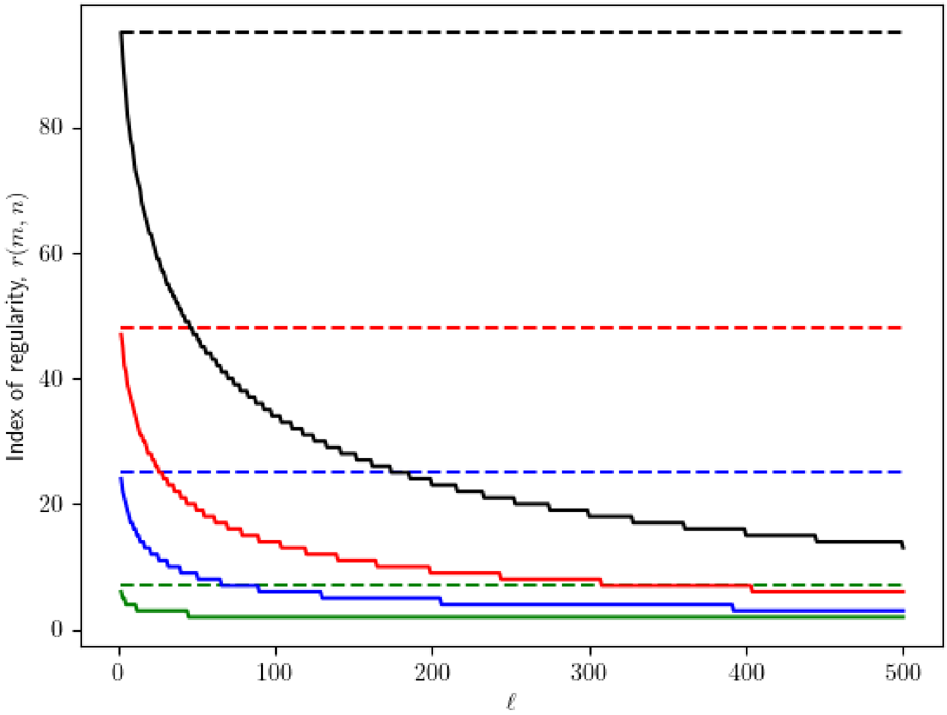

Figure 3.1: The index of regularity $r(m,n)$, where, in order from bottom to top, $m = n + \ell$, for $n = 10$ (green), $n = 50$ (blue), $n = 100$ (red) and $n = 500$ (black). The dashed lines represent the bound on $r(m,n)$ from Theorem 3.5.19 for each value of n.

Gröbner basis is bounded above by

$$O\left(md_{\text{solve}}\binom{n+d_{\text{solve}}-1}{d_{\text{solve}}}^{\omega}\right),$$

where $2 \leq \omega < 2.39$ [3] is the linear algebra constant. For the remainder of this section we set $\omega = 2$ to consider a powerful adversary. We will represent the exact cost symbolically by C.

We call $C_d := md\binom{n+d-1}{d}^{\omega}$ the cost parameter for $\mathcal{F}$, a system of m polynomials in n variables, with solving degree $d_{\text{solve}} = d$. By inspection and from the literature we know that C_d increases as d increases. Figure 3.2 illustrates this relationship for (m, n) associated with HFERP ((95,63) and (226,164)) and the Simple Matrix Encryption system (128,64). We include the additional parameter set $(m = 107, n = 103)$ to illustrate the change in cost for a small offset $m - n$, matching the scenarios considered in Section 3.5.

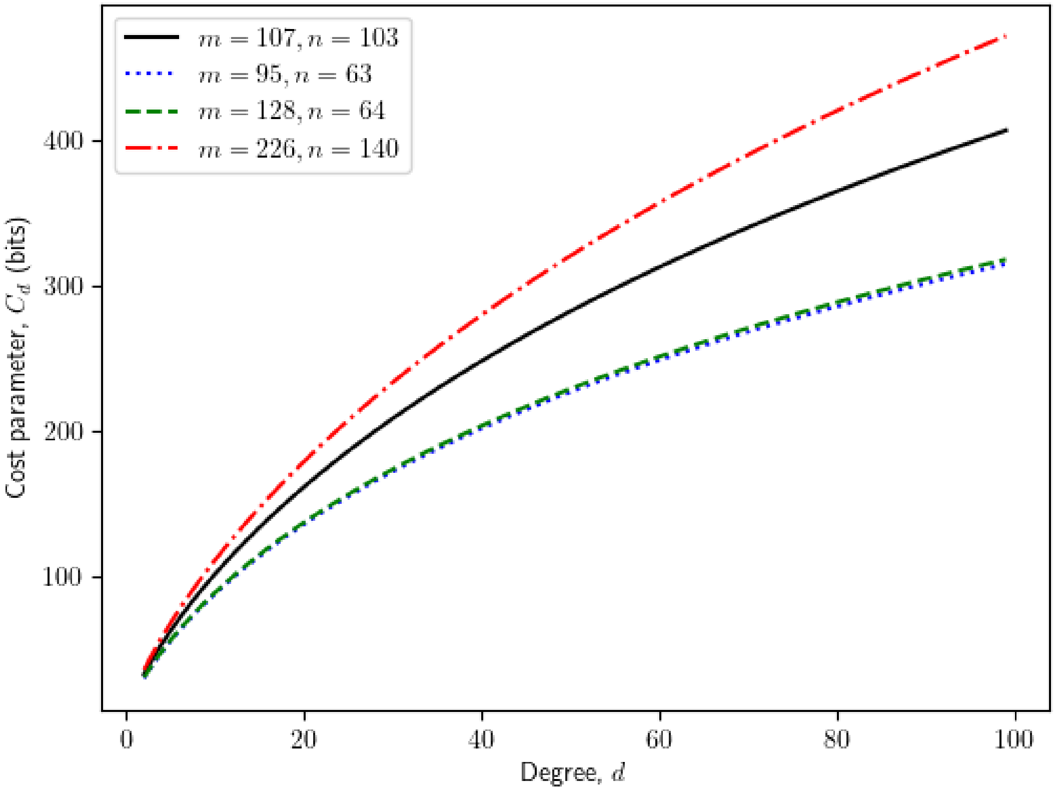

Figure 3.2: The cost parameter C_d for finding a Gröbner basis of a system, $\mathcal{F}$, of m multivariate polynomials in n variables, for $2 < d < 100$.

Let us assume that $\mathcal{F}$ is a system of polynomials for which the degree of regularity is *not* an upper bound for the solving degree. Then, clearly $C_{d_{\text{reg}}} \leq C_d$.

Although we can surmise from Figure 3.2 that C_d grows dramatically with respect to increasing d, we consider a simple model to clarify this impact. Define the cost differential as $\Delta_{d,d'} := |C_d - C_{d'}|$ and the cost ratio as $R_{d,d'} := \frac{C_d}{C_{d'}}$. We are interested in the change in $\Delta_{d,d'}$ and $R_{d,d'}$ as $|d - d'|$ varies.

We model d_{solve} as a function $d_{\text{reg}} + \alpha$, where $\alpha \in \mathbb{Z}$ is an offset parameter. For ease of notation, let $\Delta_\alpha = \Delta_{d+\alpha,d}$ and $R_\alpha = R_{d+\alpha,d}$. The change in Δ_α and R_α with increasing α is shown in Figure 3.3. For this model, we have fixed a d_{reg} for each of the parameter sets used in Figure 3.2.

The examples in Section 3.4 and in literature correspond to this model with small α. Here, we can see from Figure 3.3 that the cost difference and ratio can still be large. For instance, consider $\alpha = 2$. The cost difference and cost ratio for the four different parameter sets are given in Table 3.1.

m	n	d	Δ_2	R_2
95	63	10	98.8	11.0
128	64	50	233.6	4.6
226	140	12	140.4	14.2
107	103	10	114.9	13.5

Table 3.1: The cost difference and cost ratio (bits) when $d_{\text{solve}} = d_{\text{reg}} + 2$ for different parameter sets (m, n, d).

Though we have considered a simple model, it demonstrates the impact even a small difference between the solving degree and the degree of regularity can have.

What does this mean for the security of multivariate cryptosystems? Assume there exists a cryptosystem represented by $\mathcal{F}$, for which $d_{\text{solve}}(\mathcal{F}) > d_{\text{reg}}(\mathcal{F})$. We must remain cognisant of the fact that $C_{d_{\text{solve}}}$ is an asymptotic representation of the actual cost, C. Hence, even though we know $C_{d_{\text{reg}}} \leq C_{d_{\text{solve}}}$ we are not able to say concretely how $C_{d_{\text{reg}}}$ compares to C. We suggest that the introduction of even

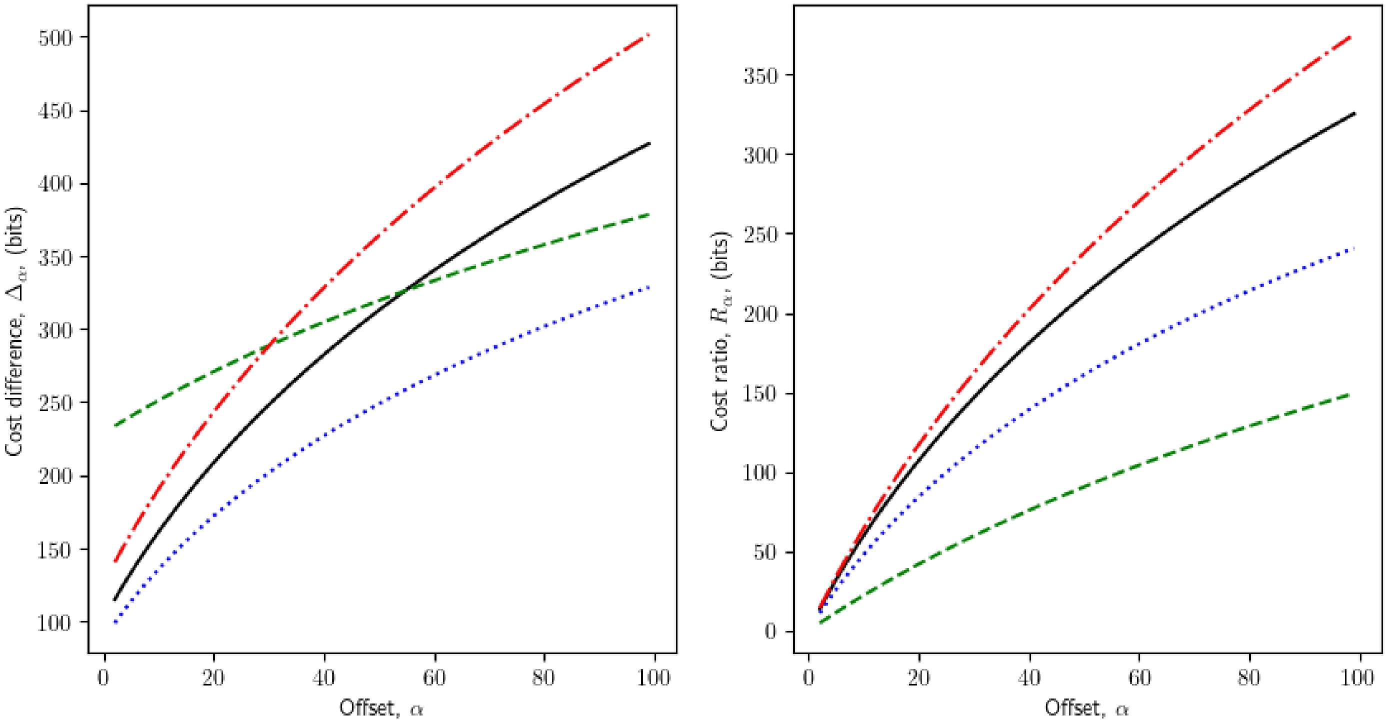

Figure 3.3: The change in cost difference Δ_α and cost ratio R_α for systems of multivariate polynomials where the solving degree is modelled as an affine function of the degree of regularity: $d_{\text{solve}} = d_{\text{reg}} + \alpha$. The lines correspond to the following parameter sets (m, n, d): blue (dotted) - (95,63,10), green (dashed) - (128,64,50), red (dash dot) - (226,140,12) and black (solid) - (107,103,10).

this small degree of uncertainty means a proven bound is preferable.

3.7 Conclusions

The objective of this chapter was to provide an alternative to the degree of regularity for bounding the solving degree of systems of polynomials equations, particularly those in the field of multivariate cryptography. We have again shown that the use of degree of regularity as an upper bound is based on a flawed assumption. While other counterexamples exist in the literature, those presented here display differences between the two degrees that are greater than one. We argue that larger differences have significant impact on the total cost of the algorithm. An interesting question for future research is

> Does there exist $M(n, m)$ such that $|d_{\text{solve}} - d_{\text{reg}}| \leq M(n, m)$ for all cryptographic semi-regular sequences of m polynomials in n variables?

As an alternative to the degree of regularity, this thesis recommends the Castelnuovo-Mumford regularity, proven to be an upper bound for the solving degree. We have given explicit formulas for these bounds, for a small set of over-determined systems. We have additionally explicitly computed the index of regularity for systems with parameters expected in practical implementations. These results address the secondary issue that results on the degree of regularity are largely asymptotic. It was also acknowledged that making security statements based on an *upper* bound for the solving degree is another case of Koblitz and Menezes' first type of error, although with present knowledge, somewhat unavoidable.

This chapter concludes the classical cryptanalysis focus of this thesis.

Chapter 4

Resource costs of quantum computation

Pursuant to the inceptive motivation for post-quantum cryptography as a field of research, understanding the complexity of quantum attacks is fundamental to security analysis. Security arguments employing a quantum adversary may follow the same complexity-theoretic principles as in the classical cases we have seen in earlier chapters, and consider time-, space-, and resource-complexity measures. However, without a complete understanding of which problems are solvable by a polynomial-time quantum algorithm there will remain an implicit issue in any quantum security argument. Namely, a protocol can be deemed secure against *known* quantum algorithms. For instance, within multivariate cryptography the best known quantum attack is to simply apply Grover's algorithm to speed up an exhaustive search attack. Adopting parameters that make this approach infeasible does not, unfortunately, constitute proven quantum security of the protocol, as there may be another as-yet-undiscovered quantum algorithm possible. This is captured in Koblitz and Menezes' third point of error in security proofs: incorrect characterisation of the resources of an adversary.

This chapter focusses on the resource costs of quantum computation, as results in this area can apply to a broad range of known - and as-yet unknown - quantum attacks. In particular, we look at improving the resource costs of fault-tolerant quantum computation through better quantum gate synthesis. We will show that the total gate count for approximating single-qubit unitaries can be reduced to $\frac{7}{9}$ of the previously known best count.

The results contained in this chapter are based on continuing work with Vadym Kliuchnikov, Kristin Lauter, Adam Paetznick, and Christophe Petit.

Outline and main contributions The rest of this chapter is organised as follows. We begin with mathematical background in Section 4.1 and then, in Section 4.2, we introduce the main concept of quantum gate synthesis and review the literature, before briefly discussing connections between gate synthesis and cryptography. In Section 4.3 we define three unitary approximation problems: diagonal unitary approximation, projective rotation approximation and general unitary approximation. These problems have been the subject of research for some time, with many results pertaining to specific gate sets [76, 58, 13, 14, 59, 56]. For each problem, we show that the accuracy constraint in an approximation can be reduced to a constraint on a single complex number. The set of feasible solutions is represented geometrically as a region in $\mathbb{R}^2$.

The key result in this chapter is a new method for solving the general unitary approximation problem, which exploits the connection between unitary approximation and LPS graphs (See Section 4.2). Explicitly, we adapt the path-finding algorithm of Pinto and Petit [75] to the quantum setting, requiring only two diagonal approximations and one 'efficient' general approximation. The sequence lengths obtained using our method improve on the standard Euler decomposition, which requires three diagonal approximations, by roughly one-third. We acknowledge that Stier [81] has concurrently and independently produced a similar result considering Clifford+T basis, specifically.

A complete method for solving these problems is outlined in Section 4.5, restricting the scope to considering arbitrary gate sets that are represented by quaternion algebras. For the sake of completeness, Section 4.4 includes a process for constructing quaternion gate sets, as defined in [56]. To summarise, a gate set is defined by a complex field L, its maximal totally real subfield K and a fixed set of elements in K. A solution to an approximation problem involves finding a matrix $M = \left(\begin{smallmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{smallmatrix}\right)$ with entries in the integer ring of L. The approach to finding M can be summarised in two steps: point enumeration in a region defined by the approximation problem to find m_1, followed by solving a relative norm equation to recover m_2. We work through three pedagogical examples: the V basis (Section 4.5.1), the Clifford+T basis (Section 4.5.2), and the Clifford+$\sqrt{\mathrm{T}}$ basis (Section 4.5.3). A worked example for the V basis is given in Section 4.5.1.2.

4.1 Preliminaries

Here we will recall some useful definitions and lemmas from quantum information. For a thorough background, we refer to [72].

A quantum bit, or *qubit*, can exist in the state $|0\rangle$, $|1\rangle$, or a linear combination of those states, $\alpha|0\rangle + \alpha|1\rangle$, where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. We are here using the standard Dirac notation for quantum states, $|\cdot\rangle$. In other words, the state of a qubit is represented by an element in a two-dimensional complex vector space. In vector notation, the quantum state $\alpha|0\rangle + \beta|1\rangle$ is written

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

The values α, β are called the *probability amplitudes* of the state. In this thesis we deal primarily with single qubits, however, we note that the vector representation can be generalised to multi-qubit systems. That is, the state of a system of n qubits can be represented by a vector in a 2^n-dimensional complex vector space. The *computational basis* for this space is the set of states $\{|k\rangle\}$ for $k = 0, \ldots, 2^n - 1$.

In the quantum circuit model, quantum algorithms are expressed as sequences of operations, or *gates*, each of which can be represented by a matrix. Let M be a square matrix, with conjugate tranpose M^*. We call M *Hermitian* if $M = M^*$, *normal* if $MM^* = M^*M$, and *unitary* if $MM^* = I$. Since the norm of a quantum state, considered as a vector, must be 1, quantum gates correspond only to unitary matrices. Some commonly used gates are the Pauli gates, the Hadamard gate and the controlled-NOT gate. We use the notation I, X, Y, Z for Pauli matrices:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The Pauli matrices are Hermitian and self-inverse. We additionally have the identities:

$$YZ = iX, \quad XY = iZ, \quad ZX = iY.$$

The Hadamard gate is represented by the matrix

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

and the controlled-NOT, or $c-$NOT, gate is represented by the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Whereas the Pauli and Hadamard gates act on a single qubit, the c-NOT gate operates on two qubits: a control qubit and a target qubit. The effect of the operation is the identity if the control qubit is in the state $|0\rangle$ and a bit-flip if the control qubit is in the state $|1\rangle$.

Denote the special unitary group, that is the group of all 2×2 unitary matrices with determinant equal to 1, by $SU(2)$. Single-qubit gates are represented by matrices in $SU(2)$. An arbitrary unitary in $SU(2)$ can be written as:

$$U = \begin{pmatrix} u & -v^* \\ v & u^* \end{pmatrix} \text{ for } u, v \in \mathbb{C} \text{ such that } |u|^2 + |v|^2 = 1$$

and we can write $u = \alpha \exp(i\phi)$ and $v = i\beta \exp(i\theta)$ with $\alpha, \beta \in [0, 1]$ and $\phi, \theta \in \mathbb{R}$.

Hence, the unitary U can be expressed as:

$$U = \alpha e^{i\phi Z} + \beta i X e^{i\theta Z} \text{ for } \phi, \theta \in \mathbb{R}, \alpha, \beta \in [0,1] \text{ such that } \alpha^2 + \beta^2 = 1 \tag{4.1}$$

A third parameterisation is obtained from the Euler angle decomposition. To see this we first require the following useful properties of matrix norms and matrix exponentials.

Let $\|\cdot\|$ be a matrix norm. We say that $\|\cdot\|$ is *submultiplicative* if $\|AB\| \leq \|A\|\|B\|$. We call $\|\cdot\|$ *unitarily invariant* if, for any unitary U and matrix A, $\|UA\| = \|A\| = \|AU\|$, providing the matrix multiplication is possible. For the rest of this chapter, we use $\|A\|$ to represent the spectral norm of A, $\|A\| = \max_k \sigma_k$ where σ_k are the singular values of A, and $\|A\|_2$ to represent the Frobenius norm of A, which is defined as the square root of the sum of the squares of the elements of A. Both norms are submultiplicative and unitarily invariant. The two norms are related as follows:

Lemma 4.1.1. *Let U, V be 2×2 unitary matrices with* $\det(U) = \det(V) = 1$ *then* $\|U \pm V\|\sqrt{2} = \|U \pm V\|_2$.

Proof. Let $W = UV^\dagger$, with eigenvalues $e^{\pm i\phi}$, so $\det(W) = 1$. Then $\|W \pm I\| = \left\|(U \pm V) \cdot V^\dagger\right\| = \|U \pm V\|$, where the final inequality holds since the spectral norm is unitarily invariant. Similarly, $\|W \pm I\|_2 = \|U \pm V\|_2$. We then compute $\|W \pm I\| = \sqrt{2 \pm 2\cos(\phi)}$ and $\|W \pm I\|_2 = \sqrt{2 \cdot (2 \pm 2\cos(\phi))}$ to finish the proof. □

Remark 4.1.2. For U, V, 2×2 unitary matrices with determinant equal to 1, $\min_\varphi \|U - e^{i\varphi}V\|$ is obtained when $\varphi \in \{0, \pi\}$.

The next two lemmas are crucial for the Euler angle decomposition representation of a unitary matrix.

Lemma 4.1.3. *For any invertible $n \times n$ matrix A and any $n \times n$ complex-valued matrix B, it is the case that $Ae^B A^{-1} = e^{ABA^{-1}}$.*

Proof. First observe that for any square matrix $\|B^k\| \leq \|B\|^k$, since the spectral norm is submultiplicative. Hence, the series $\sum_{k=0}^{\infty} \frac{\|B^k\|}{k!}$ converges, and so by absolute convergence the series $\sum_{k=0}^{\infty} \frac{B^k}{k!}$ also converges. So the matrix exponential e^B is well defined.

Then it is straightforward to see that

$$\begin{aligned} Ae^B A^{-1} &= A\left(I + \frac{B}{2} + \frac{B^2}{6} + \cdots\right)A^{-1} \\ &= I + \frac{ABA^{-1}}{2} + \frac{ABA^{-1}ABA^{-1}}{6} + \cdots = \sum_{k=0}^{\infty} \frac{(ABA^{-1})^k}{k!} = e^{ABA^{-1}}. \end{aligned}$$

□

Lemma 4.1.4. $e^{i\phi Z} X = X e^{-i\phi Z}$.

Proof. Note that $X^{-1} = X$. Then, by the previous lemma and since $XZX = -Z$, we have $Xe^{i\phi Z}X = e^{i\phi XZX} = e^{-i\phi Z}$. □

The Euler decomposition guarantees that any single-qubit unitary can be decomposed into R_z- and R_x-rotations.

Definition 4.1.5 (Euler angle decomposition)**.** *Let $U = \alpha e^{i\phi Z} + \beta i X e^{i\theta Z} \in SU(2)$ be a unitary, with $\alpha, \phi, \beta, \theta \in \mathbb{R}$. The Euler angle decomposition of U is obtained by solving for real numbers ϕ_1, ϕ_2, θ_X such that*

$$U = e^{i\phi_1 Z} e^{i\theta_X X} e^{i\phi_2 Z} = \cos(\theta_X) e^{i(\phi_1+\phi_2)Z} + \sin(\theta_X) i X e^{i(\phi_2-\phi_1)Z}. \tag{4.2}$$

The second equality in the Euler angle decomposition follows immediately from *Lemma* 4.1.4.

As Definition 4.1.5 suggests, general unitary approximation will require a combination of approximations. Consequently, we make use of the chain rule:

Lemma 4.1.6 (Chain rule for spectral norm). *Let U_1, U_2, V_1, V_2 be 2×2 unitary matrices, then*

$$\|U_1U_2 - V_1V_2\| \leq \|U_1 - V_1\| + \|U_2 - V_2\|.$$

Proof. By the triangle inequality, $\|U_1U_2 - V_1V_2\| \leq \|U_1U_2 - U_1V_2\| + \|U_1V_2 - V_1V_2\|$. Then, by submultiplicativity of the spectral norm,

$$\begin{aligned} \|U_1U_2 - U_1V_2\| + \|U_1V_2 - V_1V_2\| &\leq \|U_1\|\|U_2 - V_2\| + \|U_1 - V_1\|\|V_2\| \\ &= \|U_2 - V_2\| + \|U_1 - V_1\|. \end{aligned}$$

□

4.2 Introduction to quantum gate synthesis

In this section we review the relevant literature for quantum information and quantum synthesis, then look at the connections between gate approximations and path finding algorithms.

4.2.1 Quantum gate approximation

By [5], any n-qubit unitary can be implemented by a circuit of elementary gates, comprising C-NOT gates and single-qubit gates. Fault-tolerant quantum computers require that these single-qubit gates belong to a finite set. In order to retain full functionality, this set is required to have a special property: universality.

Definition 4.2.1 (Universal set of gates)**.** *A set of unitaries $\mathcal{G}$ is called universal if it generates a dense covering in $SU(2)$.*

That is, any unitary $U \in SU(2)$ can be approximated by a finite sequence of gates from a universal set to any degree of accuracy. Quantum gate approximation is the problem of finding a unitary V in the span of a given universal set of gates, which approximates a target unitary U to some chosen degree of accuracy, ε. The distance between two unitaries is computed by evaluating some norm of $U - V$. Typically, this is the spectral norm, which we use throughout this chapter. Quantum gate synthesis is then the problem of decomposing V into a sequence of basis gates from the gate set.

The cost of a quantum approximation is quantified by the gate complexity, or gate cost.

Definition 4.2.2 (Gate cost)**.** *Let $G = \{g_1, \dots, g_n\}$ be a universal set of gates. Let $w_G : \langle G \rangle \to \mathbb{R}^+$ be the weight function associated with G, and let $w_i := w_G(g_i)$. Given a sequence of gates s from G,*

$$s = g_{i_0} \cdots g_{i_k}, \quad i_0, \dots, i_k \in \{1, \dots, n\}$$

the gate cost *of s is given by*

$$w_G(s) = \sum_{j=0}^{k} w(g_{i_j}).$$

The gate cost of approximating U to within ε is then taken as the minimum gate cost of all possible approximating sequences.

Note that select gates, such as the Pauli or Clifford gates, are considered cheap to implement and so are given zero weight. Typically, expensive gates will be given a weight of 1, so that the gate cost of an approximation corresponds to the length of the sequence. Consequently, minimizing the length of an approximating sequence is a problem integral to the subject of gate synthesis.

A fundamental and general result is the Solovay-Kitaev theorem:

Theorem 4.2.3 (Solovay-Kitaev, [55]). *Let G be a finite set of gates in $SU(2)$ containing its own inverses, such that $\langle G\rangle$ is dense in $SU(2)$. Let $\varepsilon > 0$ be given. Then, for any $U \in SU(2)$, there exists a constant c and a sequence of gates $g_1 \cdots g_\ell$ from G such that*

$$\|g_1 \cdots g_\ell - U\| < \varepsilon,$$

where $\ell \in O(\log^c(1/\varepsilon))$.

Essentially, any unitary can be approximated by a short sequence of gates from a universal set. Significant progress has been made since Solovay-Kitaev for specific gate sets associated with fault-tolerant quantum computers. Bourgain and Gamburd [16] showed that universal gate sets of unitaries with algebraic entries give approximating sequences with lengths $O(\log(1/\varepsilon))$. This result was quickly applied to find efficient constructive algorithms for the Clifford+T gate set [57, 78] and, later, the V basis [13]. Research has since focussed on finding approximation methods to obtain close to optimal values t, such that the expected sequence length is $t\log(1/\varepsilon)$. For approximations of diagonal unitaries, this optimal t is known to be 3 [77].

4.2.2 Connections to path-finding algorithms

In this section we explain the connection between the Charles, Goren and Lauter hash construction [23], built from LPS graphs, to unitary synthesis problems. We first recall some definitions and results about cryptographic hash functions.

A *hash function* $h : \{0,1\}^* \to \{0,1\}^m$ is a function which takes bitstrings of arbitrary length as inputs, and outputs bitstrings of fixed length. A hash function is required to be *preimage resistant*; that is, given a value $y \in \{0,1\}^m$ in the image of h, it must be computationally infeasible to find a bitstring x which hashes to that value. This is formalised in Problem 4.2.4.

Problem 4.2.4 (Preimage Finding Problem)**.** *Given a hash function h and a value $y \in \mathrm{Im}(h)$, find x such that $h(x) = y$.*

There are several constructions of hash functions built on Cayley graphs. Given a group $\mathcal{G}$ with generating set $S = \{s_0, \dots, s_k\}$, the corresponding Cayley graph has vertices associated with elements g in $\mathcal{G}$ and directed edges (g, h) if and only if $gh^{-1} \in S$. Writing a message $m = m_1 m_2 \dots m_N$ with $m_i \in \{0, \dots, k\}$, the hash function is defined by $H(m) = s_{m_1} s_{m_2} \dots s_{m_N}$. For such constructions, called Cayley hash functions, Problem 4.2.4 can be reformulated as the group theoretic problem below.

Problem 4.2.5 (Constructive Membership Problem)**.** *Let $\mathcal{G}$ be a group with generating set $S = \{s_1, \dots, s_k\}$. Given an element $g \in \mathcal{G}$, find a sequence $m_1, \dots, m_N$ such that $g = \prod_i s_{m_i}$ for some $N \in \mathbb{N}$.*

Recall that the unitary synthesis problem is the search for a circuit, or sequence, of unitaries from a specified gate set that is equal to some target unitary. This is clearly similar to Problem 4.2.5.

In [23], Charles, Goren and Lauter (CGL) proposed a Cayley hash function based on LPS graphs. LPS graphs were introduced by Lubotsky, Phillips and Sarnak in [68]. Let p, ℓ be distinct primes congruent to 1 mod 4, where $\left(\frac{\ell}{p}\right) = 1$. Let $\mathbb{F}_p$ denote the finite field with p elements and let ι such that $\iota^2 = -1 \mod p$. An LPS graph $X_{p,\ell}$ is the Cayley graph with $\mathcal{G} = PSL(2, \mathbb{F}_p)$, the projective special linear group of 2×2 matrices over $\mathbb{F}_p$, and generating set

$$S = \left\{ \left(\begin{smallmatrix} a+\iota b & c+\iota d \\ -c+\iota d & a-\iota b \end{smallmatrix} \right) : a^2 + b^2 + c^2 + d^2 = \ell \right\}, \quad a > 0 \text{ and } b, c, d \text{ even.}$$

We can write $g \in \mathcal{G}$ as $\left(\begin{smallmatrix} a+\iota b & c+\iota d \\ -c+\iota d & a-\iota b \end{smallmatrix} \right)$ with $a, b, c, d \in \mathbb{F}_p$ and define the norm function $n(g) = a^2+b^2+c^2+d^2$. The preimage problem for the CGL hash function amounts to path finding on an LPS graph. Since these are Cayley graphs, the preimage problem is equivalent to Problem 4.2.5.

Petit, Lauter and Quisquater [74] proposed an algorithm for finding short paths in LPS graphs in which a matrix from the group $\mathcal{G}$ is decomposed into the product of four diagonal matrices with square determinant and graph generators, up to multiplication by a unit. This decomposition is reminiscent of the Euler decomposition for unitary synthesis, in which the target unitary is decomposed into the product of R_z-rotations.[1] Pinto and Petit [75] later improved upon the algorithm in [74], by decomposing the target matrix into the product of two diagonal matrices and a third non-diagonal, easily-factorisable matrix, resulting in path lengths of $7 \log_\ell(p)$. In Section 4.3 we translate the algorithm to the setting of general unitary approximation.

We summarise Pinto and Petit's method here.

[1] Notably, R_z-rotations can be expressed as diagonal matrices: $R_z(\theta) = \left(\begin{smallmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{smallmatrix} \right)$.

– Let $M \in PSL(2, \mathbb{F}_p)$ be the target for factorisation. The matrix M is 'lifted' to a matrix $M' \in GL(\mathbb{Z}[i])$, such that the corresponding entries of each matrix are congruent modulo p.

– M' is factorised over $GL(\mathbb{Z}[i])$, subject to conditions on the magnitude of the determinant.

– Each factor is mapped back to $PSL(2, \mathbb{F}_p)$.

The similarities and differences between the cryptographic and quantum settings are summarised in Table 4.1. The length of a sequence indicates the cost of approximating the target unitary in the context of gate synthesis. For the CGL hash function, the sequence length will equal the length of the corresponding path in the LPS graph, and is similarly used as measure of performance for path-finding algorithms. The length of a sequence is determined by taking the norm of the target matrix. In [75], the desired distance between M and M' is $O(p^{-1})$ with respect to some well-defined p-adic norm. For matrices over $\mathbb{C}$, we can use some complex matrix norm, for instance the spectral norm, with ε as the measure of accuracy. 'Lifting' is similar to approximation in the sense that we look for a 'close' matrix, with respect to some norm, which we can factorise[2]. Of course, in the LPS hash setting p is fixed, whereas for quantum approximation ε is chosen. Note, however, that the other properties of cryptographic hash functions - collision resistance and second preimage resistance - do not have natural quantum analogues. Likewise, fallback circuits (in which measurements are used to aid approximation) and unitary mixing (taking a probabilistic combination of unitaries) do not have cryptographic counterparts.

[2] We acknowledge that this is not a perfect analogy, but the similarities motivate our use of techniques similar to those used by Pinto and Petit.

Path-finding/Hash functions	Quantum Synthesis
Matrices over $\mathbb{F}_p$	Matrices over $\mathbb{C}$
Lifting: G to $GL_2(\mathbb{Z}[i])$	Approximation: $SU(2)$ to gate set
Accuracy: p^{-1}	Accuracy: ε
Fixed p	Chosen ε
ℓ^N, lifted determinant	ℓ^N, scaled determinant
Collision resistance	–
2^{nd} preimage resistance	–
–	Fallback

Table 4.1: Summary of the similarities and differences between path-finding for classical LPS hashes and quantum synthesis.

4.3 Approximation problems

In this section we introduce three approximation problems. For the remainder of this chapter, any arbitrary gate set G is assumed to be universal.

Recall that our main goal in this chapter is find an improved solution to the general unitary approximation problem.

Problem 4.3.1 (General qubit unitary approximation). *Given:*

- *target unitary $U \in SU(2)$,*
- *gate set G, a finite set of 2×2 unitary matrices with determinant one*
- *accuracy ε, a positive real number*

Find a sequence $g_1, \ldots, g_n$ of elements of G and real number φ such that the following inequality holds:

$$\left\| U - e^{i\varphi} g_1 \ldots g_n \right\| \leq \varepsilon$$

Of particular interest is the case where U is a diagonal unitary, namely $U = e^{i\theta Z}$ for real θ (see Problem 4.3.2, below). Indeed, the state-of-the-art method for solving the general unitary approximation problem is to use Euler angle decomposition (Definition 4.1.5) to reduce the problem to three diagonal unitary approximation problems.

In this section, we first introduce two problems for approximating diagonal unitaries, the second of which uses the fallback protocol introduced in [14]. We give reductions of both problems to the search for elements in two-dimensional regions. We then demonstrate how the general unitary approximation problem is reduced to two diagonal approximations and a search for elements in a one-dimensional region, improving on the traditional Euler angle decomposition approach.

4.3.1 Diagonal unitary approximation

Since an arbitrary unitary can be expressed, up to a global phase, as the product of R_z and R_x rotations, the problem of diagonal unitary approximation is of significance to the general unitary approximation problem. In this section we recall some of the known results regarding the diagonal approximation problem.

Problem 4.3.2 (Diagonal unitary approximation)**.** *Given:*

- *target angle θ, a real number,*
- *gate set G, a finite set of 2×2 unitary matrices with determinant one,*
- *accuracy ε, a positive real number,*

Find a sequence $g_1, \ldots, g_n$ of elements of G and a real number φ such that the following inequality holds:

$$\left\|e^{i\theta Z} - e^{i\varphi} g_1 \ldots g_n\right\| \leq \varepsilon$$

Observe that Problem 4.3.2 is a special case of the general unitary approximation problem, where the target unitary is always diagonal. The diagonal unitary approximation problem is easier to solve because it imposes the following condition on the top left entry of $V = g_1 \dots g_n$.

Proposition 4.3.3 (Diagonal approximation condition)**.** *The unitary*

$$V = g_1, \dots, g_n = \begin{pmatrix} u & -v^* \\ v & u^* \end{pmatrix}.$$

is a solution to the diagonal approximation problem for target angle θ, gate set G and accuracy ε if and only if

$$\left|\mathrm{Re}\left(ue^{-i\theta}\right)\right| \geq 1 - \varepsilon^2/2.$$

Proof. Suppose $0 \leq \theta \leq \pi$. Recall that by Lemma 4.1.1 we have $\|U - V\|\sqrt{2} = \|U - V\|_2$. Expanding $\|U - V\|_2$, gives

$$\left\|e^{i\theta Z} - V\right\|_2^2 = \left|u - e^{i\theta}\right|^2 + \left|u^* - e^{-i\theta}\right|^2 + |v|^2 + |v^*|^2 = 2 + 2\big(|u|^2 + |v|^2\big) - 4\mathrm{Re}\big(ue^{-i\theta}\big).$$

Hence, we conclude that $\left\|e^{i\theta Z} - V\right\|_2 = 2\sqrt{1 - \mathrm{Re}(ue^{-i\theta})}$. Therefore $\left\|e^{i\theta Z} - V\right\| \leq \varepsilon$ is true if and only if

$$\begin{aligned} \left(2\sqrt{1 - \mathrm{Re}(ue^{-i\theta})}\right)/\sqrt{2} \leq \varepsilon \quad &\iff 1 - \mathrm{Re}\big(ue^{-i\theta}\big) \leq \varepsilon^2/2 \\ &\iff \mathrm{Re}(ue^{-i\theta}) \geq 1 - \varepsilon^2/2. \end{aligned}$$

Applying the same analysis to $\theta + \pi$ changes the condition on top-left entry u of V to $\mathrm{Re}(ue^{-i(\theta+\pi)}) \geq 1 - \varepsilon^2/2$, which can be written as $-\mathrm{Re}(ue^{-i\theta}) \geq 1 - \varepsilon^2/2$. □

Figure 4.1 illustrates the constraint on the top-left element of the approximating unitary defined by Proposition 4.3.3.

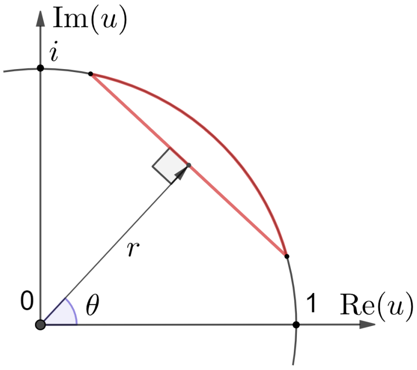

Figure 4.1: Geometric interpretation of constraints on complex number u appearing in Proposition 4.3.3. The region with red boundary contains complex numbers u that satisfy constraints $\mathrm{Re}\big(ue^{-i\theta}\big) \geq r$ and $|u| \leq 1$, where $r = 1 - \varepsilon^2/2$.

4.3.2 Diagonal approximation with projective measurement

Bocharov, Roetteler and Svore's fallback protocol [14] uses measurement to approximate diagonal unitaries more efficiently. The protocol comprises two steps: a projective rotation step and a fallback step.

Let V be a 2×2 unitary matrix with determinant one defined as

$$V = \left(\begin{array}{cc} u & -v^* \\ v & u^* \end{array} \right).$$

The key observation made by the authors of [14] is that the circuit in Figure 4.2 applies $e^{i\mathrm{Arg}(u)Z}$ to the state $|\psi\rangle$ when the measurement outcome on the top qubit is zero. The probability of this outcome is $|u|^2$. When the measurement outcome is one, the circuit applies $Ye^{i\mathrm{Arg}(v)Z}$ to the state $|\psi\rangle$, up to a global phase. The probability of this measurement outcome is $|v|^2$.

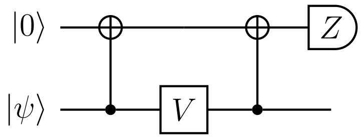

Figure 4.2: The circuit from [14] that implements a projective rotation, V on input $|\psi\rangle$ when the measurement outcome on the top qubit is zero.

How can this circuit be used for unitary approximation? Let $U = e^{i\theta Z}$ be a diagonal unitary operator that we want to approximate. The fallback protocol has two steps, which are repeated until success occurs:

1. Projective rotation: We apply the circuit in Figure 4.2 with $V = e^{i\theta' Z}$, $\theta' \approx \theta$, an approximation of U within chosen accuracy ε.
2. Fallback: The second step of the protocol depends on the measurement outcome. If the measurement outcome is zero we are done, and otherwise we apply Y followed by a fallback circuit, $\mathcal{B}$. This is essentially the same circuit as in Figure 4.2, but with an updated V to account for the acquired error.

If p is the probability of measuring zero in the first step, the expected cost of the algorithm is the cost of the first step plus $1-p$ times the cost of the second step. After a pre-determined maximum number of failures, the final circuit is implemented with probability of success equal to 1. For a more detailed description of the fallback protocol we refer the reader to [14].

The fallback protocol motivates the following approximation problem for diagonal unitaries.

Problem 4.3.4 (Projective rotation approximation)**.** *Given:*

- *target angle θ, a real number,*
- *success probability p, a positive real number between 0 and 1,*
- *gate set G, a finite set of 2×2 unitary matrices with determinant one*
- *accuracy ε, a positive real number*

Find a sequence $g_1, \ldots, g_n$ of elements in G and a real number φ such that for $U = g_1 \ldots g_n$ the circuit given on Figure 4.2 has the following two properties:

- *the probability of measuring zero in computational basis is at least p,*
- *when the measurement outcome is zero, the circuit implements rotation $e^{i\theta' Z}$ such that $\left\| e^{i\theta Z} - e^{i\varphi} e^{i\theta' Z} \right\| \leq \varepsilon$.*

Much like the case of the diagonal approximation problem, solutions to Problem 4.3.4 are characterised by constraints on u, the top-left entry of the circuit unitary V. The above discussion of the fallback protocol shows that the probability of measuring zero depends on $|u|$, so the first property required for solutions to Problem 4.3.4 immediately implies a constraint on $|u|$. The proposition below shows that the second property additionally imposes a constraint on u.

Proposition 4.3.5 (Projective rotation condition)**.** *Let δ be such that*

$$[\theta - \delta, \theta + \delta] = \left\{ \theta' : \cos(\theta - \theta') \geq 1 - \varepsilon^2/2 \right\},$$

for real θ. Then the unitary

$$V = g_1, \ldots, g_n = \begin{pmatrix} u & -v^* \\ v & u^* \end{pmatrix}.$$

is a solution to the fallback approximation problem (Problem 4.3.4) if and only if u lies in the sector defined by $\mathrm{Arg}(u) \in [\theta + \varphi - \delta, \theta + \varphi + \delta]$ *and* $|u| \geq r = \sqrt{p}$*, where* $\varphi = 0$ *or* $\varphi = \pi$*. For a geometric interpretation of these constraints see Figure 4.3.*

Proof. The probability of measuring zero in the fallback circuit in Figure 4.2 with V is at least p, which implies $|u|^2 \geq p$.

Let $\mathrm{Arg}(u) = \theta'$, such that θ' belongs to interval $[\theta - \delta, \theta + \delta]$. Then $e^{i\theta' Z}$ is the rotation performed by the fallback circuit in Figure 4.2 with $\varphi = 0$ when the measurement outcome is zero. By unitary invariance of the spectral norm we have

$$\left\| e^{i\theta' Z} - e^{i\theta Z} \right\| = \left\| e^{i(\theta' - \theta)Z} - I \right\| = \max\Big(\left| e^{i(\theta' - \theta)} - 1 \right|, \left| e^{-i(\theta' - \theta)} - 1 \right| \Big).$$

Then $\left\| e^{i\theta' Z} - e^{i\theta Z} \right\| \leq \varepsilon \iff \sqrt{2 - 2\cos(\theta' - \theta)} \leq \varepsilon \iff \theta' \in [\theta - \delta, \theta + \delta]$.

Now, take $\mathrm{Arg}(u) := \theta'' \in [\theta + \pi - \delta, \theta + \pi + \delta]$, and let $e^{i\theta'' Z}$ be the rotation performed by the fallback circuit in Figure 4.2 when the measurement outcome is zero. In this case the relevant spectral norm is

$$\left\| e^{i\theta'' Z} - e^{i\pi} e^{i\theta Z} \right\| = \sqrt{2 + 2\cos(\theta'' - \theta)} = \sqrt{2 - 2\cos((\theta'' - \pi) - \theta)}.$$

Since $\theta'' - \pi \in [\theta - \delta, \theta + \delta]$, this implies that $\left\| e^{i\theta'' Z} - e^{i\pi} e^{i\theta Z} \right\| \leq \varepsilon$ as required. □

Figure 4.3 illustrates the geometric representation of the constraint on the top-left element of the approximating unitary defined by Proposition 4.3.5. These constraints are less strict than those of Proposition 4.3.3, albeit with a probability of failure.

The approximation method outlined in [14] constructs a solution to Prob-

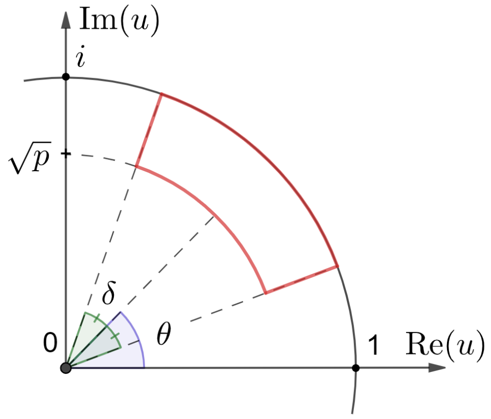

Figure 4.3: Geometric interpretation of constraint on complex number u appearing in Proposition 4.3.5. The region with red boundary contains complex numbers u that satisfy constraints $\operatorname{Arg}(u) \in [\theta - \delta, \theta + \delta]$ and $|u| \geq \sqrt{p}$, where p is the probability of a zero measurement outcome and $\delta = \arccos(1 - \varepsilon^2/2)$.

lem 4.3.4 by first representing the target phase factor $e^{i\theta}$ by a cyclotomic rational of the form z^*/z, then searching for a real-valued modifier to achieve the desired success probability p. The above reduction of the fallback approximation problem is new and differs from [14]. The constraints on u, illustrated in Figure 4.2 address the accuracy and success probability conditions simultaneously. The geometric description of these constraints is itself novel, although follows naturally given the representation of the diagonal approximation problem.

4.3.3 General unitary approximation

We now return to the general unitary approximation problem (Problem 4.3.1), where we want to approximate an arbitrary unitary $U = \alpha e^{i\phi Z} + \beta i X e^{i\theta Z}$.

We propose a new approximation approach using the following observation.

Let ϕ', θ' be arbitrary angles, and let $U' := \alpha e^{i\phi' Z} + \beta i X e^{i\theta' Z}$. The unitary U' is identical to U in parameters α and β, but not necessarily in parameters ϕ and θ. We say that U' is *magnitude equivalent* to U. Similarly, we call a unitary U'' that is identical to U in parameters ϕ and θ *phase equivalent* to U. Let $\phi_1 := \frac{(\phi-\phi')-(\theta-\theta')}{2}$ and $\phi_2 = \frac{(\phi-\phi')+(\theta-\theta')}{2}$. Then, by Definition 4.1.5, we have

$$e^{i\phi_1 Z} U' e^{i\phi_2 Z} = \alpha e^{i(\phi_1+\phi_2+\phi')Z} + \beta i X e^{i(\phi_2-\phi_1+\theta')Z} = \alpha e^{i\phi Z} + \beta i X e^{i\theta Z} = U.$$

The Euler decomposition method for approximation reduces Problem 4.3.1 to three diagonal unitary approximation problems. Our strategy is to first construct one unitary U' of the form above which we can approximate to within accuracy $\varepsilon/3$, and then to approximate both diagonal unitaries $e^{i\phi_1 Z}$ and $e^{i\phi_2 Z}$ as in the previous subsections. This results in a circuit that is $\frac{7}{9}$ the length of the solution resulting directly from Euler decomposition. We prove this result in Section 4.6.

To construct U', we use the following proposition, which determines the approximate synthesis of any unitary by imposing the condition that the norm of its upper left element lies in a given interval.

Proposition 4.3.6 (Magnitude condition for general unitary approximation)**.** *Let α, ε be a real numbers in the interval* $[0, 1]$ *and let* $U' = \alpha e^{i\phi' Z} + \sqrt{1-\alpha^2} i X e^{i\theta' Z}$ *for arbitrary real numbers θ', ϕ'. Let $I_{\alpha,\varepsilon}$ be the interval of all solutions α' to the inequality*

$$|\alpha' - \alpha|^2 + \left|\sqrt{1-(\alpha')^2} - \sqrt{1-\alpha^2}\right|^2 \leq \varepsilon^2.$$

Let W_ε be the special unitary

$$W_\varepsilon = g_1 \dots g_n = \begin{pmatrix} u & -v^* \\ v & u^* \end{pmatrix}$$

where $|u| \in I_{\alpha,\varepsilon}$, $u = |u|e^{i\phi'}$ and $v = |v|e^{i\theta'}$. Then

$$\|U' - W_\varepsilon\| \leq \varepsilon.$$

Proof. Recall that for any matrix A its Frobenius norm $\|A\|_2$ is equal to the square root of the sum of the absolute values squared of it entries. Next observe that as U' and W_ε are phase equivalent,

$$\|U' - W_\varepsilon\|_2^2 = 2||u| - \alpha|^2 + 2\Big||v| - \sqrt{1-\alpha^2}\Big|^2.$$

Recall that $|v| = \sqrt{1 - |u|^2}$. Since $|u|$ lies in $I_{\alpha,\varepsilon}$, we have that $\|U' - W_\varepsilon\|_2^2 \leq 2\varepsilon^2$. According to Lemma 4.1.1, for 2×2 unitary matrices $\|U' - W_\varepsilon\| = \|U' - W_\varepsilon\|_2/\sqrt{2}$ and therefore $\|U' - W_\varepsilon\| \leq \varepsilon$. □

In practice we construct U' by first finding u with $|u| \in I_{\alpha,\varepsilon/3}$ then solving $u = |u|e^{i\phi'}$ for ϕ' (and similarly for θ'). The above proposition motivates a complete solution to the general unitary approximation problem.

Proposition 4.3.7 (General unitary approximation)**.** *Given real numbers $\alpha, \varepsilon \in [0,1]$, let $U = \alpha e^{i\phi Z} + iX\sqrt{1-\alpha^2}e^{i\theta Z}$. Let $W_{\varepsilon/3}$ be the special unitary defined by $u = |u|e^{i\phi'}$ and $v = |v|e^{i\theta'}$, where $|u| \in I_{\alpha,\varepsilon/3}$.*

Let $\phi_1 = (\phi - \phi')/2 - (\theta - \theta')/2$, let $\phi_2 = (\phi - \phi')/2 + (\theta - \theta')/2$. For $k = 1, 2$, let $V_k = g_1^{(k)} \dots g_{n_k}^{(k)}$ be a solution to the diagonal approximation problem for angle

ϕ_k and accuracy $\varepsilon/3$.

Then $V_1 W_{\varepsilon/3} V_2 = g_1^{(1)} \cdots g_{n_1}^{(1)} g_1 \cdots g_n g_1^{(2)} \cdots g_{n_2}^{(2)}$ is a solution to the general approximation problem for target unitary U with accuracy ε.

Proof. Let $U' = \alpha e^{i\phi' Z} + iX\sqrt{1-\alpha^2} e^{i\theta' Z}$. By Proposition 4.3.6, we have $\left\|U' - W_{\varepsilon/3}\right\| \leq \varepsilon/3$. By Proposition 4.3.3 the following condition is ensured:

$$\left\|e^{i\phi_k Z} - V_k\right\| \leq \varepsilon/3 \text{ for } k = 1, 2.$$

Using the chain inequality $\|U_1 U_2 - V_1 V_2\| \leq \|U_1 - V_1\| + \|U_2 - V_2\|$ for the spectral norm (see Lemma 4.1.6) we establish the required bound:

$$\left\|U - V_1 W_{\varepsilon/3} V_2\right\| \leq \left\|e^{i\phi_1 Z} - V_1\right\| + \left\|U' - W_{\varepsilon/3}\right\| + \left\|e^{i\phi_2 Z} - V_2\right\| \leq \varepsilon.$$

□

Figure 4.4 illustrates the geometric interpretation of the constraint on the top-left element of the approximating unitary defined by Proposition 4.3.6 and Proposition 4.3.7.

4.3.4 Geometric comparisons for diagonal approximation

Proposition 4.3.7 establishes that to solve the general unitary approximation problem, we require two diagonal unitary approximations and one magnitude approximation. Either Proposition 4.3.3 or Proposition 4.3.5 can be chosen to obtain the diagonal approximations. Recall that both approaches place a constraint on a single complex number u, the top-left element of the approximating unitary, which

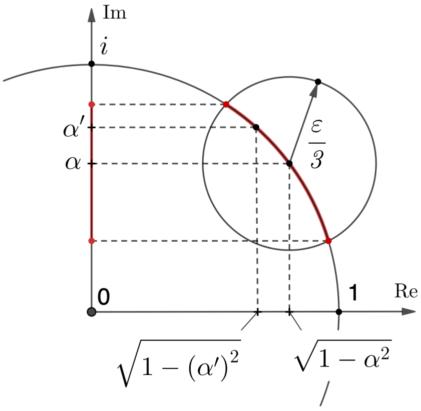

Figure 4.4: Geometric interpretation of the constraint on complex number u appearing in Proposition 4.3.6. Solutions to inequality $|\alpha' - \alpha|^2 + \left|\sqrt{1-(\alpha')^2} - \sqrt{1-\alpha^2}\right|^2 \leq (\varepsilon/3)^2$ for given $\alpha \in [0,1]$ and $\varepsilon > 0$ are shown in red on the vertical axis. These correspond to complex numbers u by $|u| = \alpha'$.

defines a feasible region in the complex plane. Here, we compare the areas of the regions defined by each problem.

Note that the segment in Figure 4.1 spans points with angular coordinates $[\theta-\delta, \theta+\delta]$ for $\delta = \arccos(1-\varepsilon^2/2)$. Letting $x = 1-\varepsilon^2/2$, so $\theta = 2\delta = 2\arccos(x)$, and equating areas, we obtain

$$\begin{aligned} \theta - \sin(\theta) = \theta(1-p) \quad &\iff \quad p = \sin(\theta)/\theta \\ &\iff \quad p = x\sqrt{1-x^2}/\arccos(x). \end{aligned}$$

Observe that since $x \in [0,1]$, we see that for p satisfying this equality, we have $p \leq x$. Hence, provided that the probability of success p satisfies $p \leq 1-\varepsilon^2/2$, the projective approximation corresponds to a feasible region with greater area and hence a greater number of candidates for u. However this is a probabilistic procedure. Note that, in order to guarantee termination of the fall-back protocol, eventually a circuit with $p = 1$ should be implemented. In practice this would amount to the standard diagonal approximation.

4.4 General solution to approximation problems

This section outlines a general method for solving approximate gate synthesis problems, and describes the properties required by gate sets to which this method applies. Throughout, we make reference to the V, Clifford+T and Clifford+$\sqrt{\mathrm{T}}$ gate sets, which will be looked at in detail in Section 4.5.

4.4.1 Gate sets

We consider quaternion gate sets as defined by Kliuchnikov, Bocharov, Roetteler and Yard in [56]. Informally, these are gate sets which are described by *totally definite quaternion algebras.*

Let K be a totally real number field and take totally positive elements $a, b \in K$. Define L to be the extension $L := K(\sqrt{-a})$ and let $i \in L$ be such that $i^2 = -a$. There are $2d$ embeddings from L into $\mathbb{C}$, where $d = [K : \mathbb{Q}]$. Fix $\sigma_1, \ldots, \sigma_d$ as any d embeddings from L that are pairwise distinct when restricted to K.

A quaternion algebra $(\frac{-a,-b}{K}) := Q$ over the field K is an algebra of the form $K + K\mathbf{i} + K\mathbf{j} + K\mathbf{k}$ where $\mathbf{i}^2 = -a, \mathbf{j}^2 = -b$ and $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$. A totally definite quaternion algebra has $a, b > 0$. An element in Q is written $q = q_0 + q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k}$, $q_0, q_1, q_2, q_3 \in K$, with conjugate $\bar{q} = q_0 - q_1\mathbf{i} - q_2\mathbf{j} - q_3\mathbf{k}$. The reduced norm of q is $\mathrm{nrd}(q) = q\bar{q}$.

Let $M_2(L)$ be the set of 2×2 matrices with elements in L. Define the K-linear map $\kappa : Q \to M_2(L)$ by

$$\kappa(1) = I, \quad \kappa(\mathbf{i}) = \sqrt{-a}Z, \quad \kappa(\mathbf{j}) = -\sqrt{-b}Y, \quad \kappa(\mathbf{k}) = \sqrt{-ab}X, \tag{4.3}$$

where X, Y, Z are the Pauli matrices. Notice that κ defines an isomorphism of quaternion algebras, with $\kappa(\mathbf{k}) = \kappa(\mathbf{i})\kappa(\mathbf{j})$. Concretely, we have a correspondence between elements in Q and matrices in $M_2(L)$ of the form

$$M = \begin{pmatrix} q_0+q_1\sqrt{-a} & -q_2\sqrt{b}+q_3\sqrt{-ab} \\ q_2\sqrt{b}+q_3\sqrt{-ab} & q_0-q_1\sqrt{-a} \end{pmatrix},$$

where the corresponding quaternion is $q := q_0+q_1\mathbf{i}+q_2\mathbf{j}+q_3\mathbf{k}$, such that $\kappa(q) = M$. Observe that $\det(M) = \mathrm{nrd}(q) = q_0 - aq_1^2 - bq_2^2 + abq_3^2$. The set of matrices of this form corresponds to SU(2) via the map

$$\sigma'(M) = \frac{1}{\sqrt{\sigma_1(\det(M))}} \cdot \sigma_1(M), \tag{4.4}$$

where σ_1 is the natural extension over matrices of the embedding from L into $\mathbb{C}$. Let S be a set of elements from K. Consider the gate set to be those matrices with determinant in S.

For the V, Clifford+T and Clifford+$\sqrt{\mathrm{T}}$ bases, the corresponding fields and integer rings are given in Table 4.2. Note that for these gate sets, the corresponding O_K and O_L are principal ideal domains.

Table 4.2: Number field correspondences for the V, Clifford+T and Clifford+$\sqrt{T}$ gate sets.

Gate set	K	L	O_K	O_L
V basis	$\mathbb{Q}$	$\mathbb{Q}(i)$	$\mathbb{Z}$	$\mathbb{Z}[i]$
Clifford+T	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(\zeta_8)$	$\mathbb{Z}[\sqrt{2}]$	$\mathbb{Z}[\zeta_8]$
Clifford+$\sqrt{\text{T}}$	$\mathbb{Q}(\zeta_{16}+\zeta_{16}^{-1})$	$\mathbb{Q}(\zeta_{16})$	$\mathbb{Z}[\zeta_{16}+\zeta_{16}^{-1}]$	$\mathbb{Z}[\zeta_{16}]$

4.4.2 Quaternion order

For a given gate set, K and L, there exists $\mathcal{O}$, an order of $M_2(L)$, containing the preimages of the gate set unitaries under σ'. We note here that while this order does not need to be maximal, maximal orders have several properties which allow for efficient factorisation of elements [56]. For a thorough background on quaternion orders, we direct the reader to [85].

The order $\mathcal{O}$ is constructed as follows. The gate set elements are mapped to matrices in $M_2(L)$. Let $\mathcal{L}_K$ be the O_K-lattice obtained by taking an O_K linear combination of the elements of the ring generated by these matrices. Then, $\mathcal{O}$ can be taken as any order containing this lattice. Note that, due to the multiplicative properties of the determinant, elements in $\mathcal{O}$ with determinant equal to ℓ^N for some $N \in \mathbb{Z}^*, \ell \in \langle S \rangle$ will correspond to gate set elements. Moreover, N is the length of a sequence of basis elements that produces the corresponding gate set element. However, two distinct elements in $\mathcal{O}$ could correspond to the same gate set element, each with a distinct N value[3]. We look for minimal N, as this will correspond to the shortest possible basis sequence. This will be the N for which the entries of $M \in \mathcal{O}$ with $\det(M) = \ell^N$ are integral and not all divisible by ℓ. Such a minimal N always exists and since the approximation method outlined here

[3] See Example 4.5.2.

iterates over increasing N, the sequence obtained will be optimal.

Remark 4.4.1. In addition, we look for orders $\mathcal{O}$ in which gates that are considered 'low-cost' in the gate set behave as units. This forces the determinant of matrices corresponding to low-cost gates to be 1, ensuring that N is a count of 'expensive' gates in a sequence. In essence, this makes the determinant a useful cost measure for approximation.

The definitions for $\mathcal{O}$ and ℓ that we will use for the V, Clifford+T and Clifford+$\sqrt{\text{T}}$ bases are given in the Table 4.3.

Table 4.3: Maximal orders for V, Clifford+T and Clifford+$\sqrt{T}$ gate sets.

Gate set	ℓ	$\mathcal{O}$
V basis	5	$O_K \cdot I + O_K \cdot iX + O_K \cdot iY + O_K \cdot iZ$
Clifford+T	$2+\sqrt{2}$	$O_K \cdot I + O_K \cdot \frac{I+iX}{\sqrt{2}} + O_K \cdot \frac{I+iY}{\sqrt{2}} + O_K \cdot \frac{I+iZ+iX+iY}{2}$
Clifford+$\sqrt{\text{T}}$	$2+2\cos(\frac{\pi}{16})$	$O_K \cdot I + O_K \cdot \frac{I+iX}{\sqrt{2}} + O_K \cdot \frac{I+iY}{\sqrt{2}} + O_K \cdot \frac{I+iZ+iX+iY}{2}$

4.4.3 Solving approximation problems

For fixed $N \in \mathbb{N}$, finding a solution to any approximation problem over a gate set involves finding a matrix

$$M = \begin{pmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{pmatrix} \in \mathcal{O},$$

with additional constraints on m_1 depending on the approximation problem, such that $\det(M) = \ell^N$. Our approach to finding M can be summarised in two steps:

1. point enumeration in a target region to find m_1 (Section 4.4.3.2), followed by
2. solving a relative norm equation to recover m_2 (Section 4.4.3.3).

From each pair (m_1, m_2) we deduce the matrix $M = \left(\begin{smallmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{smallmatrix}\right)$. The unitary $\sigma'(M)$ is factorised over the desired gate set to obtain a solution to the approximation problem. If no solution exists for the given N, set $N := N + 1$ and repeat the process. Thus, iterating over N will give a solution corresponding to the shortest gate sequence.

For the diagonal and fallback approximation problems we look for elements $M = \left(\begin{smallmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{smallmatrix}\right)$ of $\mathcal{O}$, such that

$$\sigma_1(m_1)/\sqrt{\sigma_1(\ell^N)} \in R_{\text{approx}} \subset D_1,$$

where R_{approx} is the region defined by the problem, as shown in Section 4.3. For the general unitary approximation problem, m_1 is required to satisfy

$$\sigma_1(m_1 m_1^*)/\sigma_1(\ell^N) \in I_{\text{approx}} \subset [0, 1],$$

where I_{approx} is the real interval defined by the parameters of the problem. We observe that for the relative norm equation

$$m_2 m_2^* = \ell^N - m_1 m_1^*$$

to have a solution, it is necessary that, for all k, $\sigma_k(\ell^N - m_1 m_1^*) > 0$. This means we only need to consider those candidates m_1 that satisfy either

$$\sigma_k(m_1)/\sqrt{\sigma_k(\ell^N)} \in D_1 \text{ or, equivalently, } \sigma_k(m_1 m_1^*)/\sigma_k(\ell^N) \in [0, 1]$$

for all $k > 1$.

4.4.3.1 Restrictions on the order

Define the map h from L to Q by

$$h(a_0 + ia_1) = a_0 + a_1\mathbf{i}.$$

Clearly, $\kappa(h(m))$ sends an element from L to the diagonal matrix $\left(\begin{smallmatrix} m & 0 \\ 0 & m^* \end{smallmatrix}\right) \in M_2(L)$. Define the set of elements corresponding to diagonal matrices in $\mathcal{O}$ as $M_{\mathcal{O}} := \{m \in L : \kappa(h(m)) \in \mathcal{O}\}$. The subsets of L containing candidates for m_1 and m_2 are respectively defined as

- $M_{\text{diag}} = \{m_1 : \exists m_2 \in L \text{ s.t. } \kappa(h(m_1)) + h(m_2)\mathbf{j}) \in \mathcal{O}\}$, and
- $M_{\text{off}-\text{diag}} = \{m_2 : \exists m_1 \text{ s.t. } \kappa(h(m_1) + h(m_2)\mathbf{j}) \in \mathcal{O}\}$.

Given a candidate $m_1 \in M_{\text{diag}}$, the valid associated candidates for m_2 are restricted to the smaller set $M^{m_1}_{\text{off}-\text{diag}} = \{m_2 : \kappa(h(m_1) + h(m_2)\mathbf{j}) \in \mathcal{O}\}$.

We will consider orders of the form $\mathcal{O} = \sum_{i=1}^{4} O_K\omega_i$, with

$$\omega_1 = I, \quad \omega_2 = \frac{I + iX}{\sqrt{2}}, \quad \omega_3 = \frac{I + iY}{\sqrt{2}}, \quad \omega_4 = \omega_3\omega_2 = \frac{I + iX + iY + iZ}{2}. \tag{4.5}$$

as for the Clifford+T and Clifford+$\sqrt{\text{T}}$ gate sets. In these cases, we have $M_{\mathcal{O}} = O_K + \frac{1+i}{\sqrt{2}}O_K \subseteq O_L$ and also that $M_{\text{diag}}, M_{\text{off}-\text{diag}}$ are fractional $M_{\mathcal{O}}$ ideals. We additionally will restrict to the case that $M_{\text{diag}}, M_{\text{off}-\text{diag}}$ are principal ideals.

4.4.3.2 Finding m_1: an enumeration problem

Finding candidates $m_1 \in L$ satisfying the conditions of an approximation problem can be reduced to an integer point enumeration problem. Observe that enumerating m_1 from M_{diag} is equivalent to enumerating $a_0, a_1 \in K$ from the set

$$\mathcal{L}_{\mathcal{O}} = \{(a_0, a_1) : \exists a_2, a_3 \in K \text{ s.t. } a_0 I + a_1\sqrt{-a}Z - a_2\sqrt{-b}Y + a_3\sqrt{-ab}X \in \mathcal{O}\}.$$

We make use of the following lemma to find a $\mathbb{Z}$-basis for M_{diag}.

Lemma 4.4.2. *$\mathcal{L}_{\mathcal{O}}$ is a full rank O_K-lattice in K^2.*

Proof. Since $\mathcal{O}$ is closed under addition and scalar multiplication over O_K, so is $\mathcal{L}_{\mathcal{O}}$. Consider an O_K-linearly independent generating set G of $\mathcal{L}_{\mathcal{O}}$ and let $g_1, \ldots, g_r$ be the subset of these that are K-linearly independent. Then $r \leq 2$. We have $I \in \mathcal{O}$, so $(1, 0) \in \mathcal{L}_{\mathcal{O}}$. Suppose for a contradiction that $\mathcal{L}_{\mathcal{O}}$ contains no elements of the form $(a_0, a_1), a_1 \neq 0$ in $\mathcal{L}_{\mathcal{O}}$. Let $\{\omega_i\}_{i=1,\ldots,4}$ be a basis for $\mathcal{O}$, with corresponding elements in $\mathcal{L}_{\mathcal{O}}$ denoted by $(\omega_{i,0}, \omega_{i,1})$. By assumption, $\omega_{i,1} = 0$ for $i = 1, 2, 3, 4$. We can write each basis element in the form $\omega_{i,0}I - \omega_{i,2}\sqrt{-b}Y + \omega_{i,3}\sqrt{-ab}X$. Then, by simple linear algebra over K, we can see that at least two of the basis elements must be K-linearly dependent. Hence, we have a contradiction and so $r = 2$. So $\mathcal{L}_{\mathcal{O}}$ spans K^2 as a K vector space and clearly $\text{rank}(\mathcal{L}_{\mathcal{O}}) = 2d$. □

Hence, we can conclude that there exists a $\mathbb{Z}$-basis for $\mathcal{L}_{\mathcal{O}}$ and so also for M_{diag}, which we denote $\{y_i\}$, for $i = 0, \ldots, 2d - 1$.

Recall that under the restriction that M_{diag} is a principal fractional ideal, we have

$$M_{\text{diag}} = \frac{1}{\xi} M_{\mathcal{O}}, \quad \xi \in L. \tag{4.6}$$

Remark 4.4.3. We observe that $M_{\mathcal{O}} \subseteq \frac{1}{\xi} M_{\mathcal{O}} \implies \xi \in M_{\mathcal{O}}$. To see this, note that $I \in \mathcal{O}$ and if $M_{\mathcal{O}} \subseteq \frac{1}{\xi} M_{\mathcal{O}}$ then $\xi x \in M_{\mathcal{O}}, \forall x \in M_{\mathcal{O}}$.

Case 1: Diagonal Approximation For diagonal approximation the first normalised embedding of m_1, $\sigma_1(m_1)/\sigma_1(\ell^N)$, falls in a two dimensional region, R_{approx}. Define the $2d \times 2d$ matrix $\Sigma_{\mathcal{O}}$ with rows:

$$\begin{aligned}
\Sigma_{\mathcal{O}}^{(2j)} &= (\text{Re}(\sigma_j(y_0)), \ldots, \text{Re}(\sigma_j(y_{2d-1}))) \\
\Sigma_{\mathcal{O}}^{(2j+1)} &= (\text{Im}(\sigma_j(y_0)), \ldots, \text{Im}(\sigma_j(y_{2d-1}))\,.
\end{aligned}$$

So $\Sigma_{\mathcal{O}}$ is the matrix with entries corresponding to the real and imaginary components of the images of the l_i under each of the σ_ds. Let Λ be the diagonal matrix with $\left(\sqrt{\sigma_1(\ell^N)}, \sqrt{\sigma_1(\ell^N)} \ldots, \sqrt{\sigma_d(\ell^N)}, \sqrt{\sigma_d(\ell^N)}\right)$ on the diagonal. Then the operation $\Lambda^{-1}\Sigma_{\mathcal{O}}z$ first embeds z into the Euclidean space corresponding to M_{diag}, then normalises the result with respect to the norm ℓ^N. Finding m_1 is now an integer point enumeration problem:

Problem 4.4.4. *Find $z \in \mathbb{Z}^{2d}$ such that $\Lambda^{-1}\Sigma_{\mathcal{O}}z \in R_{\text{approx}} \times D_1^{d-1}$.*

Each solution $z = (z_0, \ldots, z_{2d-1})$ yields a candidate for m_1 by setting $m_1 = z_0y_0 + \cdots + z_{2d-1}y_{2d-1}$.

Case 2: General Approximation For general unitary approximation the first normalised embedding of m_1, $\sigma_1(m_1m_1^*)/\sigma_1(\ell^N)$, belongs to the interval I_{approx} and the remaining $d-1$ embeddings satisfy $\sigma_k(m_1m_1^*)/\sigma_k(\ell^N) \in [0,1]$.

We are looking for values $n = m_1m_1^*$ satisfying the above conditions, such that $m_1 \in M_{\text{diag}}$. Consider the set $\{n : \exists m_1 \in M_{\text{diag}} \text{ such that } m_1m_1^* = n\}$ and let M_{norm} be the set generated multiplicatively by the above set. From Equation (4.6), we see that

$$M_{\text{norm}} \subseteq \frac{1}{\xi\xi^*}O_K,$$

a fractional O_K ideal. For this reason we can enumerate points $\hat{n} = \xi\xi^* n \in O_K$. Let $k_0, \ldots, k_{d-1}$ be an integral basis for K and define Σ' as the $d \times d$ matrix with rows:

$$\Sigma'_j = (\sigma_j(k_0), \ldots, \sigma_j(k_{d-1}))\,.$$

Define Λ' as the diagonal normalisation matrix with $\left(\sigma_1(\xi\xi^*) \cdot \sigma_1(\ell^N), \ldots, \sigma_d(\xi\xi^*) \cdot \sigma_d(\ell^N)\right)$ on the diagonal. Finding $\hat{n}$ is now an integer point enumeration problem in a parallelotope.

Problem 4.4.5. *Find $z \in \mathbb{Z}^d$ such that $\Lambda'^{-1}\Sigma' z \in I_{\text{approx}} \times [0,1]^{d-1}$.*

Each solution $z = (z_0, \ldots, z_{d-1})$ yields a candidate for $\hat{n}$ by setting $\hat{n} = z_0 k_0 + \cdots + z_{d-1} k_{d-1}$. Recovery of m_1 requires a solution to the norm equation

$$\hat{m_1}\hat{m_1}^* = \hat{n}, \quad \hat{m_1} \in M_{\mathcal{O}}.$$

Finally the candidate m_1 is defined as $m_1 = \hat{m_1}/\xi$.

4.4.3.3 Finding m_2: solving a norm equation

Given m_1, finding a candidate for m_2 amounts to solving a norm equation,

$$m_2 m_2^* = \ell^N - m_1 m_1^*, \quad m_2 \in M^{m_1}_{\text{off-diag}}, \tag{4.7}$$

with the added constraint ensuring that the pair (m_1, m_2) corresponds to a matrix in the order $\mathcal{O}$. In the following discussion, we show that a solution for m_2 can be recovered from a related norm equation, in which we solve for elements in $M_{\mathcal{O}}$.

Recall the assumption that $M_{\text{off}-\text{diag}}$ is a principal fractional ideal, with

$$M_{\text{off}-\text{diag}} = \frac{1}{\xi'} M_{\mathcal{O}}, \quad \xi' \in L.$$

For any two $m_2, m_2' \in M_{\text{diag}}^{m_1}$ we have $\kappa(h(m_2)\mathbf{j} - h(m_2')\mathbf{j}) \in \mathcal{O}$. Therefore, we can write $M_{\text{off}-\text{diag}}^{m_1} = m_2 + M_{\text{off}-\text{diag}}^0$, where $M_{\text{off}-\text{diag}}^0$ is the principal fractional $M_{\mathcal{O}}$ ideal $\{m_2' : \kappa(h(m_2')\mathbf{j}) \in \mathcal{O}\}$. We will take $M_{\text{off}-\text{diag}}^0 = \frac{1}{\chi} M_{\mathcal{O}}, \quad \chi \in L$.

The norm equation in Equation (4.7) can now be reformulated to look for a solution in $M_{\mathcal{O}}$.

Problem 4.4.6. *Given $\hat{z}/\xi' \in M_{\text{off}-\text{diag}}, m_1 \in M_{\text{diag}}$, find $z \in M_{\mathcal{O}}$ such that*

$$\left(\frac{\hat{z}}{\xi'} + \frac{z}{\chi}\right)\left(\frac{\hat{z}}{\xi'} + \frac{z}{\chi}\right)^* = \ell^N - m_1 m_1^*.$$

A solution z yields a candidate for m_2 by setting $m_2 = \hat{z}/\xi' + z/\chi$. Since $m_1 = \hat{m_1}/\xi$ for some $m_1 \in M_{\mathcal{O}}$, if $\xi = \xi'$ and $\chi = 1$, then Problem 4.4.6 is simplified to:

Problem 4.4.7. *Find $z \in M_{\mathcal{O}}$ such that $(\hat{z}+\xi z)(\hat{z}+\xi z)^* = \xi\xi^*\ell^N - \hat{m_1}\hat{m_1}^*$, where $\hat{z}, \hat{m_1} \in M_{\mathcal{O}}$.*

Remark 4.4.8. By applying the variable substitution $z' = \hat{z} + \xi z$, we see that Problem 4.4.6 is equivalent to solving

$$z'(z')^* = r \in O_K, \quad z' \in \hat{z} + \xi M_{\mathcal{O}}, \tag{4.8}$$

where $r = \xi\xi^*\ell^N - \hat{m_1}\hat{m_1}^*$. In other words, z' must lie in the same coset in $M_{\mathcal{O}}/\xi M_{\mathcal{O}}$ as $\hat{z}$. Fieker, Jurk and Pohst [40] give an algorithm for solving general relative norm equations. A method for solving relative norm equations pertaining to quaternion gate sets (over number fields with fixed degree) is given in [56], which runs in polynomial time for the number fields associated with the V, Clifford+T and Clifford+$\sqrt{\text{T}}$ bases. We conjecture that the condition on the coset makes this a more difficult problem to solve for general number fields. However, there may be fields with possessing useful properties, for which this problem can be solved in polynomial time. We conjecture that this is again the case for the V, Clifford+T and Clifford+$\sqrt{\text{T}}$ bases.

To summarise, the definitions for ξ, ξ' and χ corresponding to the V, Clifford+T and Clifford+$\sqrt{\text{T}}$ bases are given in the Table 4.4. Note that the order $\mathcal{O}$ we use for the V basis is actually of a different form than that of the Clifford+T and Clifford+$\sqrt{\text{T}}$ bases, as we will see in the next section.

Table 4.4: Fractional ideal representatives for V, Clifford+T and Clifford+$\sqrt{T}$ gate sets.

Gate set	ξ	ξ'	χ	$M_{\mathcal{O}}$
V basis	1	1	1	O_L
Clifford+T	$\sqrt{2}$	$\sqrt{2}$	1	O_L
Clifford+$\sqrt{\text{T}}$	$\sqrt{2}$	$\sqrt{2}$	1	$O_K + \frac{1+i}{\sqrt{2}} O_K$

4.5 Solutions for commonly used gate sets

4.5.1 V Basis

The V basis consists of the following six matrices:

$$V_{\pm Z} = \frac{1}{\sqrt{\ell}} \begin{pmatrix} 1 \pm 2i & 0 \\ 0 & 1 \mp 2i \end{pmatrix},$$

$$V_{\pm Y} = \frac{1}{\sqrt{\ell}} \begin{pmatrix} 1 & \mp 2 \\ \pm 2 & 1 \end{pmatrix},$$

$$V_{\pm X} = \frac{1}{\sqrt{\ell}} \begin{pmatrix} 1 & \pm 2i \\ \pm 2i & 1 \end{pmatrix},$$

where $\ell = 5$. Let $K = \mathbb{Q}$ and let $L = \mathbb{Q}(i) = \{a_0 + ia_1 : a_0, a_1 \in \mathbb{Q}\}$, where $i^2 = -1$. Let $O_K = \mathbb{Z}$ and $O_L = \mathbb{Z}[i] = \{a_0 + ia_1 : a_0, a_1 \in \mathbb{Z}\}$ be the rings of integers of K and L respectively. Any element $t = a_0 + ia_1 \in O_L$ can be written as a 2-dimensional vector over O_K, namely (a_0, a_1). There are two distinct embeddings from L into $\mathbb{C}$ related by complex conjugation. Denote by σ the embedding such that $\sigma(i) = i$.

Let $M_2(L)$ be the algebra of all 2 × 2 matrices with entries in L, and let $\mathcal{O}$ be an order in $M_2(L)$ that contains all the V basis elements scaled by $\sqrt{\ell}$. Concretely, we set

$$\mathcal{O} := \mathbb{Z} \cdot I + \mathbb{Z} \cdot iX + \mathbb{Z} \cdot iY + \mathbb{Z} \cdot iZ. \tag{4.9}$$

We extend σ over $\mathcal{O}$ in a natural way, namely for $M \in \mathcal{O}$ we define $\sigma(M)$ as the matrix whose elements are the images of the elements of M under σ. As observed in [13, 56], elements of $\mathcal{O}$ with determinant ℓ^N correspond to unitaries that can be expressed as a product of N matrices from the V gate set via the map $\sigma'(M) = \frac{1}{\sqrt{\ell^N}}\sigma(M)$.

Example 4.5.1. Let $V = V_Z \cdot V_X = \frac{1}{5}\left(\begin{smallmatrix} 1+2i & 2i-4 \\ 2i+4 & 1-2i \end{smallmatrix}\right)$. Then, $M_V = \left(\begin{smallmatrix} 1+2i & 2i-4 \\ 2i+4 & 1-2i \end{smallmatrix}\right) = I + 2 \cdot iX - 4 \cdot iY + 2 \cdot iZ \in \mathcal{O}$ and $\sigma'(M_V) = V$. Since $\det(M_V) = 5^2$, we have $N = 2$ as expected, as V is the product of two V basis matrices. Note that the sequence $V_Z V_X$ cannot be simplified (over the V basis) so N is minimal.

Example 4.5.2. Let $V = V_Z V_X V_{-X} V_Y V_{-Z} = \frac{1}{\sqrt{3125}}\left(\begin{smallmatrix} 25 & 30-40i \\ -30-40i & 25 \end{smallmatrix}\right)$. Then,

$$M_V = \left(\begin{smallmatrix} 25 & 30-40i \\ -30-40i & 25 \end{smallmatrix}\right) = 25 \cdot I - 40 \cdot iX + 30 \cdot iY \in \mathcal{O}$$

and $\sigma'(M_V) = V$. Then $\det(M_V) = 3125 = 5^5$ so V can be expressed as the product of five V basis elements. However, $M_V' = \left(\begin{smallmatrix} 5 & 6-8i \\ -6-8i & 5 \end{smallmatrix}\right) = 5 \cdot I - 8 \cdot iX + 6 \cdot iY \in \mathcal{O}$, is also such that $\sigma'(M_V') = V$. Here, $\det(M_V') = 125 = 5^3$, giving $N = 3$. Since $V_P V_{-P} = V_{-P} V_P = I$, for $P \in \{X, Y, Z\}$, the sequence $V_Z V_X V_{-X} V_Y V_{-Z}$ simplifies to $V_Z V_Y V_{-Z}$, so V can in fact be expressed as a product of *three* V basis elements. The sequence cannot be simplified further, by checking all combinations of $V_{P_1} V_{P_2}$ for $P_1, P_2 \in \{\pm X, \pm Y, \pm Z\}$, so this N is minimal.

4.5.1.1 Solving approximation problems

Finding a solution to any approximation problem over the V basis involves finding a matrix $M = \begin{pmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{pmatrix}$ with additional constraints on m_1 depending on the approximation problem, such that $\det(M) = \ell^N$. The following procedure is described for fixed N.

For the diagonal (Problem 4.3.2) and projective (Problem 4.3.4) approximation problems, M is such that $\sigma_1(m_1)/\sqrt{\sigma_1(\ell^N)} \in R_{\text{approx}}$, where R_{approx} is a specific region of $\mathbb{C}$ depending on the problem. Namely, we consider R_{approx} as one of the regions defined in Proposition 4.3.3 and Proposition 4.3.5. For general unitary approximation (Problem 4.3.1) with our new decomposition, M must be such that $\sigma_1(m_1 m_1^*)/\sigma_1(\ell^N) \in I_{\text{approx}}$, where $I_{\text{approx}} \subset [0,1]$ where I_{approx} is an interval of $\mathbb{R}$ as defined in Proposition 4.3.6. Formally, we solve the following point enumeration problems.

Problem 4.5.3 (2D point enumeration (V basis)). *Let R_{approx} be a 2D region corresponding to a particular approximation problem and fix $N \in \mathbb{N}$.*

$$\textit{Find all } (a_0, a_1) \in \mathbb{Z}^2 \textit{ such that } \frac{1}{\sqrt{\ell^N}}(a_0, a_1) \in R_{\text{approx}}.$$

Problem 4.5.4 (1D point enumeration (V basis)). *Let $I_{\text{approx}} \subset [0,1]$ be a real interval corresponding to a particular approximation problem and fix $N \in \mathbb{N}$.*

$$\textit{Find all } n \in \mathbb{Z} \textit{ such that } \frac{n}{\ell^N} \in I_{\text{approx}}.$$

In the first case we set $m_1 = a_0 + i a_1$ for every solution (a_0, a_1). In the second case we first solve the norm equation $n = a_0^2 + a_1^2$, and for every solution we obtain a candidate value $m_1 = a_0 + i a_1$.

To satisfy the determinant condition, solving the approximation problems requires that we keep only those m_1 for which the following problem is solvable.

Problem 4.5.5 (Norm equation (V basis)). *Given $m_1 \in \mathbb{Z}[i]$ and integer N, find $m_2 \in \mathbb{Z}[i]$ such that*

$$m_2 m_2^* = \ell^N - m_1 m_1^* \in \mathbb{Z}.$$

For every pair of solutions (m_1, m_2) we then deduce a matrix $M = \left(\begin{smallmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{smallmatrix}\right)$. Since m_2 is a solution to Problem 4.5.5 we have $\det(M) = \ell^N$ and the matrix $\sigma'(M) = \frac{1}{\sqrt{\ell^N}}\sigma_1(M) = \frac{1}{\sqrt{\ell^N}}\left(\begin{smallmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{smallmatrix}\right)$ is unitary.

In summary, given a target unitary and associated region or interval, the following procedure finds an approximation over the V basis. For a fixed value of N, an element $m_1 \in \mathbb{Z}[i]$ is obtained by solving an integer point enumeration problem defined by the target region. Together with N, m_1 defines a norm equation, which is solved to obtain an element $m_2 \in \mathbb{Z}[i]$. If no solution to either problem is found, the value of N is increased. The point enumeration and norm equation steps are repeated for each value of N until a valid pair (m_1, m_2) is obtained. Each pair defines a matrix $M \in \mathcal{O}$ as above with determinant ℓ^N. Then, the unitary $\sigma'(M)$ is factorised over the V basis using an existing exact synthesis algorithm (for example, [59]) to obtain a solution to the approximation problem.

4.5.1.2 Example: Diagonal approximation of $e^{i\frac{\pi}{4}Z}$

Let $\theta = \frac{\pi}{4}$ and suppose we want to approximate $U = e^{i\theta Z} = \left(\begin{smallmatrix} e^{i\pi/4} & 0 \\ 0 & e^{-i\pi/4} \end{smallmatrix}\right)$ using the V basis within accuracy $\varepsilon = 0.05$. In other words, we look for V, a product of unitaries from the V basis, which satisfies $\|U - V\| \leq \varepsilon$. Writing V as $\left(\begin{smallmatrix} u & -v^* \\ v & u^* \end{smallmatrix}\right)$, with $u, v \in \mathbb{C}$, we obtain the following:

$$\left|\mathrm{Re}(ue^{-i\theta})\right| \geq 1 - \varepsilon^2/2 \implies \|U - V\| \leq \varepsilon. \tag{4.10}$$

The constraint on u is represented geometrically by the region in Figure 4.5.

Since V is a product of V basis matrices, there exists $N \in \mathbb{N}$ such that $V = \frac{1}{\sqrt{5^N}}\left(\begin{smallmatrix} u' & -(v')^* \\ v' & (u')^* \end{smallmatrix}\right)$, with $u', v' \in \mathbb{Z}[i]$. It follows that $u = u'/\sqrt{5^N}$ and $v = v'/\sqrt{5^N}$.

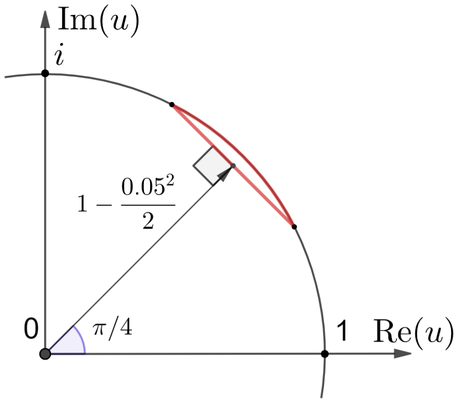

Figure 4.5: Geometric interpretation of constraint on complex number u in Equation (4.10). The region with the red boundary contains candidate points $(a, b) \in \mathbb{Z}^2$, such that $u = a + ib$ and $\left|\mathrm{Re}(ue^{-i\theta})\right| \geq 1 - (0.05)^2/2$.

Hence, we scale the region in Figure 4.5 by $\sqrt{5^N}$ and look for integer points $(a, b) \in \mathbb{Z}^2$, each corresponding to a candidate $u' = a + ib$. We initialise $N := 1$, and iterate over N until a solution is found.

We find that there are no integer solutions for $N = 1, 2, 3, 4$. At $N = 5$, there are four candidates for u', namely $\{38 + 41i, 39 + 40i, 40 + 39i, 41 + 38i\}$, shown in Figure 4.6. Since V is unitary, we require $\det(V) = uu^* + vv^* = 1$ or, equivalently, $u'(u')^* + v'(v')^* = 5^5 = 3125$. So we must have $0 \leq v'(v')^* = 3125 - u'(u')^*$. Then,

$$u' = 38 + 41i \implies u'(u')^* = 38^2 + 41^2 = 3125 \tag{4.11}$$

$$u' = 39 + 40i \implies u'(u')^* = 39^2 + 40^2 = 3121 \tag{4.12}$$

$$u' = 40 + 39i \implies u'(u')^* = 3121 \tag{4.13}$$

$$u' = 41 + 38i \implies u'(u')^* = 3125. \tag{4.14}$$

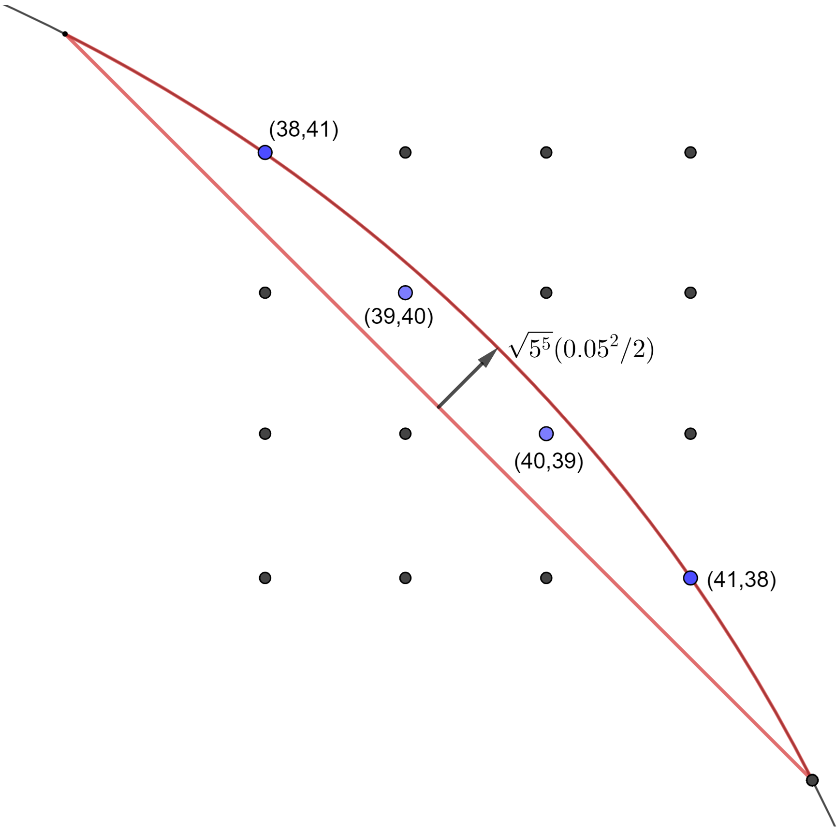

Figure 4.6: Geometric interpretation of the constraint on complex number u', such that $V = \frac{1}{\sqrt{5^5}}\begin{pmatrix} u' & -(v')^* \\ v' & (u')^* \end{pmatrix}$ approximates $e^{i\frac{\pi}{4}Z}$ to accuracy $\varepsilon = 0.05$. The region with the red boundary contains four candidate complex numbers satisfying $\left|\mathrm{Re}(u'e^{-i\theta})\right| \geq \sqrt{5^5}(1-\varepsilon^2/2)$.

Let $v' = c + id$, so

$$v'(v')^* = c^2 + d^2 = 5^5 - (a^2 + b^2). \tag{4.15}$$

For Equations (4.11) and (4.14), we have $v'(v')^* = 0$ so $v = 0$ is the only solution. Equations (4.12) and (4.13) yield $v'(v')^* = 4$, so $c^2 + d^2 = 4 = 2^2$ then either $c = \pm 2, d = 0$ or $c = 0, d = \pm 2$. The two corresponding values for v' are ± 2 and $\pm 2i$. In general, Equation (4.15) admits a solution for $v \in \mathbb{Z}[i]$ if and only if all terms p^k in the prime factorisation of $5^5 - (a^2 + b^2)$, with $p \equiv 3 \bmod 4$, have even exponent k. Each candidate pair (u', v') defines an approximation unitary $V = \frac{1}{\sqrt{3125}} \begin{pmatrix} u' & -(v')^* \\ v' & (u')^* \end{pmatrix}$, which is factorised over the V basis. These factorisations are given in Table 4.5.

u'	v'	V basis factorisation
$41 + 38i$	0	$(V_{-Z})^5$
$38 + 41i$	0	$iZ \cdot (V_{+Z})^5$
$39 + 40i$	$2i$	$e^{i\pi} \cdot V_{-X}V_{-Y}V_{+X}V_{+Y}V_{-X}$
	2	$e^{i\pi} \cdot V_{+Y}V_{-X}V_{-Y}V_{+X}V_{+Y}$
	$-2i$	$e^{i\pi} \cdot V_{+X}V_{+Y}V_{-X}V_{-Y}V_{+X}$
	-2	$e^{i\pi} \cdot V_{-Y}V_{+X}V_{+Y}V_{-X}V_{-Y}$
$40 + 39i$	$2i$	$-iZ \cdot V_{-Y}V_{-X}V_{+Y}V_{+X}V_{-Y}$
	2	$-iZ \cdot V_{+X}V_{-Y}V_{-X}V_{+Y}V_{+X}$
	$-2i$	$-iZ \cdot V_{+Y}V_{+X}V_{-Y}V_{-X}V_{+Y}$
	-2	$-iZ \cdot V_{-X}V_{+Y}V_{+X}V_{-Y}V_{-X}$

Table 4.5: V basis factorisations of unitaries $V := \frac{1}{\sqrt{5^5}} \begin{pmatrix} u' & -(v')^* \\ v' & (u')^* \end{pmatrix}$, satisfying $\left\| e^{i\frac{\pi}{4}Z} - V \right\| \leq \varepsilon = 0.05$.

4.5.2 Clifford + T basis

4.5.2.1 Gate set

The single-qubit Clifford group is defined as the set of unitaries that preserve the Pauli matrices under conjugation. That is, $\mathcal{C}$ is in the single-qubit Clifford group if and only if for any Pauli matrix P, the matrix $\mathcal{C}^* P \mathcal{C}$ is also a Pauli matrix.

We recall that the S, H and T gates are defined as follows:

$$S = e^{-i\pi/4Z} = \begin{pmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, \qquad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$
$$T = e^{-i\pi/8Z} = \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}.$$

The single-qubit Clifford group is generated by the H and S gates, and the Clifford+T group is generated by the single-qubit Clifford group and the T gate. Observe that $T^2 = S$, so the Clifford+T group is generated by H and T. We also recall the matrices T_x, T_y defining rotations by $\frac{\pi}{4}$ about the x and y axes, namely

$$T_x := \begin{pmatrix} \cos(\frac{\pi}{8}) & -i\sin(\frac{\pi}{8}) \\ -i\sin(\frac{\pi}{8}) & \cos(\frac{\pi}{8}) \end{pmatrix} = \frac{1}{\sqrt{\ell}}\left(I + \frac{I - iX}{\sqrt{2}}\right),$$
$$T_y := \begin{pmatrix} \cos(\frac{\pi}{8}) & -\sin(\frac{\pi}{8}) \\ \sin(\frac{\pi}{8}) & \cos(\frac{\pi}{8}) \end{pmatrix} = \frac{1}{\sqrt{\ell}}\left(I + \frac{I - iY}{\sqrt{2}}\right)$$

where $\ell = 2 + \sqrt{2}$. Note that T similarly defines the rotation of $\frac{\pi}{4}$ about the z axis and we can write $T = \frac{1}{\sqrt{\ell}}\left(I + \frac{I-iZ}{\sqrt{2}}\right)$. We can obtain T_x and T_y from T, and vice versa, by conjugation with single-qubit Clifford unitaries. Synthesis via a circuit of T_x, T_y, T and Hadamard gates therefore corresponds to synthesis in the Clifford+T basis, up to a global phase.

In evaluating the cost of approximate synthesis with Clifford+T gates, we assume that Clifford gates are low cost, and only count T gates, or equivalently the total number of T_x, T_y and T matrices.

4.5.2.2 Quaternion order

Let $K = \mathbb{Q}(\sqrt{2})$ and let $L = \mathbb{Q}(\zeta_8)$, where $\zeta_8 = e^{2\pi i/8}$. The ring of integers of L is

$$O_L = \mathbb{Z}[\zeta_8] = \left\{a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3 : a_k \in \mathbb{Z}\right\} = \mathbb{Z}[\sqrt{2}] + \frac{1+i}{\sqrt{2}} \cdot \mathbb{Z}[\sqrt{2}].$$

The ring of integers of K is the real subring $O_K = \mathbb{Z}[\sqrt{2}] = \{b_0 + b_1\sqrt{2} : b_0, b_1 \in \mathbb{Z}\} \subset O_L$. We can identify any element m in O_L with a 4-dimensional vector $\boldsymbol{m} = (a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$ using the integral basis above. There are four distinct embeddings from L into $\mathbb{C}$, related to one another by complex conjugation and $\sqrt{2}$-conjugation. We fix two embeddings σ_1, σ_2 such that

$$(\operatorname{Re}\sigma_1(m), \operatorname{Im}\sigma_1(m), \operatorname{Re}\sigma_2(m), \operatorname{Im}\sigma_2(m))^T = \Sigma\boldsymbol{m}^T$$

where

$$\Sigma := \begin{pmatrix} 1 & 1/\sqrt{2} & 0 & -1/\sqrt{2} \\ 0 & 1/\sqrt{2} & 1 & 1/\sqrt{2} \\ 1 & -1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 0 & -1/\sqrt{2} & 1 & -1/\sqrt{2} \end{pmatrix}.$$

Let $n = mm^*$ and write $n = b_0 + b_1\sqrt{2}$, $b_0, b_1 \in \mathbb{Z}$. We can identify n with the 2-dimensional vector $\boldsymbol{n} = (b, b_1)$ or with $(\sigma_1(n), \sigma_2(n))^T = \left(\begin{smallmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{smallmatrix}\right)\boldsymbol{n}^T$ through the above embeddings. We choose one embedding arbitrarily, say σ_1, to embed elements into Euclidean space. Note that both σ_1 and σ_2 are necessary to express the solvability constraints imposed by the norm equation for elements in L.

Let $M_2(L)$ be the algebra of 2×2 matrices with entries in L, and let $\mathcal{O}$ be a maximal order in $M_2(L)$ which contains T_x, T_y and T. Concretely, we set $\mathcal{O} =$

$\sum_{i=1}^{4} O_K \cdot \omega_i$ in what follows, where

$$\omega_1 = I, \qquad \omega_2 = \frac{I + iX}{\sqrt{2}}, \qquad \omega_3 = \frac{I + iY}{\sqrt{2}}, \qquad \omega_4 = \omega_3\omega_2 = \frac{I + iX + iY + iZ}{2}.$$

The embeddings σ_1, σ_2 extend over $\mathcal{O}$ in a natural way. Elements of $\mathcal{O}$ correspond to 2×2 unitaries via the map $\sigma'(M) = \frac{1}{\sqrt{\sigma_1(\det(M))}}\sigma_1(M)$. Elements of $\mathcal{O}$ with determinant equal to 1 correspond to Clifford gates, and elements of $\mathcal{O}$ with determinant ℓ^N correspond to unitaries that can be expressed as a product of N gates T_x, T_y and T [44].

4.5.2.3 Solving approximation problems

Finding a solution to any approximation problem (as defined in Section 4.3) over the Clifford+T gate set involves finding a matrix

$$M = \left(\begin{smallmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{smallmatrix}\right) = X_1\omega_1 + X_2\omega_2 + X_3\omega_3 + X_4\omega_4, \tag{4.16}$$

or equivalently finding $X_i \in O_K$, with additional constraints on m_1 depending on the approximation problem, such that $\det(M) = \ell^N$. Recall that these matrices will correspond to unitaries which are products of gates from the Clifford+T basis.

Let us first examine the sets M_{diag} and $M_{\text{off-diag}}$, in which we will look for elements m_1 and m_2, respectively. From Equation (4.16) we have

$$\begin{aligned} M_{\text{diag}} &= \left\{X_1 + \frac{X_2 + X_3}{\sqrt{2}} + \frac{X_4}{2} + \frac{X_4}{2}i : X_i \in O_K\right\} \\ &= \frac{1}{\sqrt{2}}O_K + \left(\frac{1+i}{2}\right)O_K \\ &= \frac{1}{\sqrt{2}}O_L. \end{aligned}$$

Let $M_{\mathcal{O}}$ denote the elements of L corresponding to diagonal elements of $\mathcal{O}$. That is elements m_1 such that $\left(\begin{smallmatrix} m_1 & 0 \\ 0 & m_1^* \end{smallmatrix}\right) \in \mathcal{O}$. By Equation (4.16), we can see $M_{\mathcal{O}} = O_L$.

Similarly, we have

$$\begin{aligned} M_{\mathrm{off-diag}} &= \left\{ \frac{\sqrt{2}X_1 - X_3}{2} + \frac{\sqrt{2}X_2 + X_3}{2} i : X_i \in O_K \right\} \\ &= \frac{1}{\sqrt{2}} O_K + \left(\frac{1+i}{2} \right) O_K \\ &= \frac{1}{\sqrt{2}} O_L. \end{aligned}$$

For fixed m_1, $M_{\mathrm{off-diag}}$ is restricted to the subset

$$M_{\mathrm{off-diag}}^{m_1} = \left\{ m_2 \in M_{\mathrm{off-diag}} : \left(\begin{smallmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{smallmatrix}\right) \in \mathcal{O} \right\}.$$

Noticing that iY, $(iY)^{-1} \in \mathcal{O}$, we see that $m_2 \in M_{\mathrm{off-diag}}^{0} \iff m_2 \in M_{\mathcal{O}}$.

Since for all $m_1 \in M_{\mathrm{diag}}, m_2 \in M_{\mathrm{off-diag}}$ there exist $\hat{m}_1, \hat{m}_2 \in O_L$, such that $m_1 = \frac{\hat{m}_1}{\sqrt{2}}$ and $m_2 = \frac{\hat{m}_2}{\sqrt{2}}$ we can scale the conditions on $\sigma_1(\hat{m}_1)$ and $\sigma_1(\hat{m}_1 \hat{m}_1{}^*)$ accordingly. Concretely, we have

$$\sigma_1(\hat{m}_1)/\sqrt{\sigma_1(2\ell^N)} \in R_{\mathrm{approx}} \text{ or } \sigma_2(\hat{m}_1\hat{m}_1{}^*)/\sigma_2(2\ell^N) \in I_{\mathrm{approx}},$$

depending on the approximation problem, and

$$\sigma_2(\hat{m}_1)/\sqrt{\sigma_2(2\ell^N)} \in D_1 \text{ or, equivalently, } \sigma_2(\hat{m}_1\hat{m}_1{}^*)/\sigma_2(2\ell^N) \in [0,1].$$

In the following sections, the point enumeration and norm equation steps are described for fixed N. For every pair of solutions (m_1, m_2) we deduce a matrix $M = \left(\begin{smallmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{smallmatrix}\right)$. The unitary $\sigma'(M)$ is factorised over the Clifford+T basis to obtain a solution to the approximation problem.

4.5.2.4 Finding m_1: an enumeration problem

We write $\hat{m_1} = a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3$ and $\hat{n} = \hat{m_1}\hat{m_1}^* = b_0 + b_1\sqrt{2}$, with all coefficients in $\mathbb{Z}$. Let Σ be as defined in Section 4.5.2.2 and let $\Sigma' = \left(\begin{smallmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{smallmatrix}\right)$. The operation Σ (respectively Σ') embeds $\hat{m_1}$ (respectively $\hat{n}$) into the Euclidean space of the approximation regions. In order to satisfy the constraints imposed by both the approximation regions and the norm equation, we define normalisation matrices Λ and Λ' for Σ and Σ', respectively. Let Λ and Λ' be the diagonal matrices with $\left(\sqrt{\sigma_1(2\ell^N)}, \sqrt{\sigma_1(2\ell^N)}, \sqrt{\sigma_2(2\ell^N)}, \sqrt{\sigma_2(2\ell^N)}\right)$ and $\left(\sigma_1(2\ell^N), \sigma_2(2\ell^N)\right)$ on their respective diagonals. Candidate values for $\hat{m_1}$ are obtained by solving the point enumeration problems below.

Problem 4.5.6 (2D point enumeration (Clifford+T basis)). *Let R_{approx} be a two-dimensional region corresponding to a particular approximation problem. Find $(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$ such that $\Lambda^{-1}\Sigma \cdot (a_0, a_1, a_2, a_3)^T \in R_{\text{approx}} \times D_1$.*

Problem 4.5.7 (1D point enumeration (Clifford+T basis)). *Let $I_{\text{approx}} \subset [0, 1]$ be a real interval corresponding to a particular approximation problem. Find $(b_0, b_1) \in \mathbb{Z}^2$ such that $\Lambda'^{-1}\Sigma' \cdot (b_0, b_1)^T \in I_{\text{approx}} \times [0, 1]$.*

In the first case, we immediately recover a candidate value for $\hat{m_1}$. In the second case, we recover a candidate value for $\hat{n}$, then solve the norm equation

$\hat{m_1}\hat{m_1}^* = \hat{n}$ and for every solution we obtain a candidate value $\hat{m_1}$. Finally, we set $m_1 = \frac{\hat{m_1}}{\sqrt{2}}$.

4.5.2.5 Finding m_2: solving a norm equation

Given a candidate value for m_1, we proceed to solve a norm equation problem, restricting m_2 to $M^{m_1}_{\text{off}-\text{diag}}$:

Problem 4.5.8. *Given $m_1 \in \frac{1}{\sqrt{2}}O_L$ and integer N, find $m_2 \in M^{m_1}_{\text{off}-\text{diag}}$ such that*

$$m_2 m_2^* = \ell^N - m_1 m_1^* \in \frac{1}{2}O_K.$$

Fixing an arbitrary $m \in M^{m_1}_{\text{off}-\text{diag}}$, we have $M^{m_1}_{\text{off}-\text{diag}} = m + O_L$. Since $M_{\text{off}-\text{diag}} = M_{\text{diag}} = \frac{1}{\sqrt{2}}O_L$, Problem 4.5.8 can then be reformulated as

Problem 4.5.9. *Given $\hat{m_1} \in \mathbb{Z}[\zeta_8]$, integer N, and $m \in \sqrt{2}M^{m_1}_{\text{off}-\text{diag}}$ find $\hat{m_2} \in m + \sqrt{2}\mathbb{Z}[\zeta_8]$ such that*

$$\hat{m_2}\hat{m_2}^* = 2\ell^N - \hat{m_1}\hat{m_1}^* \in \mathbb{Z}[\sqrt{2}].$$

Solving Problem 4.5.9 for $\hat{m_2}$ then yields a solution to Problem 4.5.8: $m_2 = \hat{m_2}/\sqrt{2}$.

4.5.3 Clifford+$\sqrt{T}$ basis

4.5.3.1 Gate set

Let $\ell = 2 + 2\cos(\frac{\pi}{8}) = 2 + (\zeta_{16} + \zeta_{16}^{-1})$, where $\zeta_{16} = e^{2\pi i/16}$. Let also $\theta = 2\cos(\frac{\pi}{8})$, $\beta = \theta^3 + 3\theta$ and $\mu = \theta^2 - 3$. We recall that the $\sqrt{T}$ gate is defined as follows:

$$\sqrt{T} = \begin{pmatrix} e^{-i\pi/16} & 0 \\ 0 & e^{i\pi/16} \end{pmatrix}.$$

The $\sqrt{T}$ gate defines a rotation about the z axis by $\frac{\pi}{8}$. The Clifford+$\sqrt{T}$ group is generated by the single-qubit Clifford group and the $\sqrt{T}$ gate. Note that we will use the notation $T^{1/2}$ interchangeably with $\sqrt{T}$ in the following discussion. We also recall the matrices $T_x^{1/2}, T_y^{1/2}$ defining rotations by $\frac{\pi}{8}$ about the x and y axes, namely

$$T_x^{1/2} = \begin{pmatrix} \cos(\frac{\pi}{16}) & -i\sin(\frac{\pi}{16}) \\ -i\sin(\frac{\pi}{16}) & \cos(\frac{\pi}{16}), \end{pmatrix} = \frac{1}{\sqrt{\ell}}\left(I + \frac{\theta(I - i\mu X)}{2}\right)$$

$$T_y^{1/2} = \begin{pmatrix} \cos(\frac{\pi}{16}) & -\sin(\frac{\pi}{16}) \\ \sin(\frac{\pi}{16}) & \cos(\frac{\pi}{16}) \end{pmatrix} = \frac{1}{\sqrt{\ell}}\left(I + \frac{\theta(I - i\mu Y)}{2}\right).$$

We can additionally write $\sqrt{T} = \frac{1}{\sqrt{\ell}}\left(I + \frac{\theta(I-iZ)}{2}\right)$. Observe that $\sqrt{T}^2 = T$ and $\left(T_a^{1/2}\right)^2 = T_a$ with $a = x, y$, as suggested by the notation. We can obtain the unitaries $\mathrm{T}_x^{k/2}$ and $\mathrm{T}_y^{k/2}$ from $T^{k/2}$, for $k = 1, 2, 3$, and vice versa, by conjugation with single-qubit Clifford unitaries. Here $T_a^{3/2} = \left(T_a^{1/2}\right)^3$. Synthesis via a circuit of unitaries in $\{T^{k/2}, \mathrm{T}_a^{k/2} : a = x, y \quad k = 1, 2, 3\}$ and the Hadamard gate therefore corresponds to synthesis in the Clifford $+\sqrt{T}$ basis, up to a global phase.

4.5.3.2 Quaternion order

Let K be the totally real number field $K = \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$, and let L be the field $L = \mathbb{Q}(\zeta_{16})$. The ring of integers of L is

$$O_L = \mathbb{Z}[\zeta_{16}] = \left\{ \sum_{k=0}^{7} a_k \zeta_{16}^k : a_k \in \mathbb{Z} \right\} = \mathbb{Z}\left[2\cos\left(\frac{\pi}{8}\right)\right] + \zeta_{16}\mathbb{Z}\left[2\cos\left(\frac{\pi}{8}\right)\right]$$

and the ring of integers of K is the real subring

$$\begin{aligned} O_K &= \mathbb{Z}\left[2\cos\left(\frac{\pi}{8}\right)\right] \\ &= \left\{ b_0 + b_1 \cdot 2\cos\left(\frac{\pi}{8}\right) + b_2\sqrt{2} + b_3 \cdot 2\cos\left(\frac{3\pi}{8}\right) : b_k \in \mathbb{Z} \right\} \subset O_L. \end{aligned}$$

We can identify any element m in O_L with an 8-dimensional vector $\boldsymbol{m} = (a_0, a_1, \ldots, a_7) \in \mathbb{Z}^8$ using the integral basis above. There are 8 distinct embeddings from L into $\mathbb{C}$, which can be grouped into pairs depending on their images when restricted to K. We fix four such embeddings $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ such that $\Sigma\boldsymbol{m}^T$ is equal to

$$(\operatorname{Re}\sigma_1(m), \operatorname{Im}\sigma_1(m), \operatorname{Re}\sigma_2(m), \operatorname{Im}\sigma_2(m), \operatorname{Re}\sigma_3(m), \operatorname{Im}\sigma_3(m), \operatorname{Re}\sigma_4(m), \operatorname{Im}\sigma_4(m))^T$$

where

$$\Sigma := \begin{pmatrix} 1 & \cos(\tfrac{\pi}{8}) & \tfrac{1}{\sqrt{2}} & \cos(\tfrac{3\pi}{8}) & 0 & -\cos(\tfrac{3\pi}{8}) & -\tfrac{1}{\sqrt{2}} & -\cos(\tfrac{\pi}{8}) \\ 0 & \cos(\tfrac{3\pi}{8}) & \tfrac{1}{\sqrt{2}} & \cos(\tfrac{\pi}{8}) & 1 & \cos(\tfrac{\pi}{8}) & \tfrac{1}{\sqrt{2}} & \cos(\tfrac{3\pi}{8}) \\ 1 & \cos(\tfrac{3\pi}{8}) & -\tfrac{1}{\sqrt{2}} & -\cos(\tfrac{\pi}{8}) & 0 & \cos(\tfrac{\pi}{8}) & \tfrac{1}{\sqrt{2}} & -\cos(\tfrac{3\pi}{8}) \\ 0 & \cos(\tfrac{\pi}{8}) & \tfrac{1}{\sqrt{2}} & -\cos(\tfrac{3\pi}{8}) & -1 & -\cos(\tfrac{3\pi}{8}) & \tfrac{1}{\sqrt{2}} & \cos(\tfrac{\pi}{8}) \\ 1 & -\cos(\tfrac{3\pi}{8}) & -\tfrac{1}{\sqrt{2}} & \cos(\tfrac{\pi}{8}) & 0 & -\cos(\tfrac{\pi}{8}) & \tfrac{1}{\sqrt{2}} & \cos(\tfrac{3\pi}{8}) \\ 0 & \cos(\tfrac{\pi}{8}) & -\tfrac{1}{\sqrt{2}} & -\cos(\tfrac{3\pi}{8}) & 1 & -\cos(\tfrac{3\pi}{8}) & -\tfrac{1}{\sqrt{2}} & \cos(\tfrac{\pi}{8}) \\ 1 & -\cos(\tfrac{\pi}{8}) & \tfrac{1}{\sqrt{2}} & -\cos(\tfrac{3\pi}{8}) & 0 & \cos(\tfrac{3\pi}{8}) & -\tfrac{1}{\sqrt{2}} & \cos(\tfrac{\pi}{8}) \\ 0 & \cos(\tfrac{3\pi}{8}) & -\tfrac{1}{\sqrt{2}} & \cos(\tfrac{\pi}{8}) & -1 & \cos(\tfrac{\pi}{8}) & -\tfrac{1}{\sqrt{2}} & \cos(\tfrac{3\pi}{8}) \end{pmatrix}.$$

Let $n = mm^*$ and write $n = b_0 + b_1 \cdot 2\cos(\frac{\pi}{8}) + b_2\sqrt{2} + b_3 \cdot 2\cos(\frac{3\pi}{8})$. We can identify n with the 4-dimensional vector $\boldsymbol{n} = (b_0, b_1, b_2, b_3)$, or with $(\sigma_1(n), \sigma_2(n), \sigma_3(n), \sigma_4(n))^T = \Sigma' \boldsymbol{n}^T$ where

$$\Sigma' := \begin{pmatrix} 1 & 2\cos(\tfrac{\pi}{8}) & \sqrt{2} & 2\cos(\tfrac{3\pi}{8}) \\ 1 & -2\cos(\tfrac{3\pi}{8}) & -\sqrt{2} & -2\cos(\tfrac{\pi}{8}) \\ 1 & -2\cos(\tfrac{3\pi}{8}) & \sqrt{2} & 2\cos(\tfrac{\pi}{8}) \\ 1 & -2\cos(\tfrac{\pi}{8}) & \sqrt{2} & -2\cos(\tfrac{3\pi}{8}) \end{pmatrix}$$

through the above embeddings. As for the Clifford+T basis, we choose a embedding arbitrarily, for example σ_1, to embed elements into Euclidean space.

Let $M_2(L)$ be the algebra of all 2×2 matrices with entries in L. Let $\mathcal{O}$ be a maximal order in $M_2(L)$ which contains $T_x^{1/2}$, $T_y^{1/2}$ and $T^{1/2}$, namely $\mathcal{O} = \sum_{i=1}^{4} O_K \cdot \omega_i$, where

$$\omega_1 = I, \qquad \omega_2 = \frac{I + iX}{\sqrt{2}}, \qquad \omega_3 = \frac{I + iY}{\sqrt{2}}, \qquad \omega_4 = \omega_3\omega_2 = \frac{I + iX + iY + iZ}{2}.$$

The embeddings $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ extend over $\mathcal{O}$ in a natural way. Elements of $\mathcal{O}$ correspond to 2×2 unitaries via the map $\sigma'(M) = \frac{1}{\sqrt{\sigma_1(\det(M))}}\sigma_1(M)$. Elements of $\mathcal{O}$ with determinant ℓ^N correspond to unitaries that can be expressed as a product of N gates $\mathrm{T}_x^{k/2}$, $\mathrm{T}_y^{k/2}$ and $\mathrm{T}^{k/2}$ with $k = 1, 2, 3$ [44]), hence in the Clifford + $\sqrt{T}$ gates.

4.5.3.3 Solving approximation problems

Finding a solution to any approximation problem over the Clifford+$\sqrt{T}$ gate set involves finding a matrix

$$M = \left(\begin{smallmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{smallmatrix}\right) = X_1\omega_1 + X_2\omega_2 + X_3\omega_3 + X_4\omega_4 \in \mathcal{O}, \tag{4.17}$$

or equivalently finding $X_i \in O_K$, with additional constraints on m_1 depending on the approximation problem, such that $\det(M) = \ell^N$. The unitary $\sigma'(M)$ will be factorised over the Clifford+$\sqrt{\mathrm{T}}$ basis.

Let us first examine the sets M_{diag} and $M_{\mathrm{off-diag}}$, in which we will look for elements m_1 and m_2, respectively. From Equation (4.17) we have

$$\begin{aligned} M_{\mathrm{diag}} &= \left\{X_1 + \frac{X_2 + X_3}{\sqrt{2}} + \frac{X_4}{2} + \frac{X_4}{2}i : X_i \in O_K\right\} \\ &= \frac{1}{\sqrt{2}}O_K + \frac{1+i}{2}O_K. \end{aligned}$$

As before, let $M_{\mathcal{O}}$ denote the set of elements $m_1 \in L$ such that $\left(\begin{smallmatrix} m_1 & 0 \\ 0 & m_1^* \end{smallmatrix}\right) \in \mathcal{O}$. From Equation (4.17), we have $M_{\mathcal{O}} = O_K + \frac{1+i}{\sqrt{2}}O_K$ and so clearly $M_{\mathrm{diag}} = \frac{1}{\sqrt{2}}M_{\mathcal{O}}$. Similarly, we have $M_{\mathrm{off-diag}} = \frac{1}{\sqrt{2}}M_{\mathcal{O}}$. Note that $O_L \subsetneq M_{\mathcal{O}}$, since ζ_{16} is in O_L but not in $M_{\mathcal{O}}$.

Again, since for all $m_1 \in M_{\text{diag}}, m_2 \in M_{\text{off-diag}}$ there exist $\hat{m_1}, \hat{m_2} \in O_L$, such that $m_1 = \frac{\hat{m_1}}{\sqrt{2}}$ and $m_2 = \frac{\hat{m_2}}{\sqrt{2}}$ we can scale the conditions on $\sigma_1(\hat{m_1})$ and $\sigma_1(\hat{m_1}\hat{m_1}^*)$ accordingly. Concretely, we have

$$\sigma_1(\hat{m_1})/\sqrt{\sigma_1(2\ell^N)} \in R_{\text{approx}} \text{ or } \sigma_2(\hat{m_1}\hat{m_1}^*)/\sigma_2(2\ell^N) \in I_{\text{approx}},$$

depending on the approximation problem, and, for $k = 2, 3, 4$,

$$\sigma_k(\hat{m_1})/\sqrt{\sigma_k(2\ell^N)} \in D_1 \text{ or, equivalently, } \sigma_k(\hat{m_1}\hat{m_1}^*)/\sigma_k(2\ell^N) \in [0, 1].$$

In the following sections, the point enumeration and norm equation steps are described for fixed N.

4.5.3.4 Finding m_1: an enumeration problem

Writing any $m_1 = a_0 + a_1 i$ with $a_0, a_1 \in K$, we see that M_{diag} can be considered as a full rank O_K lattice in K^2. We therefore have a $\mathbb{Z}$-basis, $\{y_0, \ldots, y_7\}$, for M_{diag} and can write any element $m_1 \in M_{\text{diag}}$ as $m_1 = \sum_{i=0}^{7} a_i y_i, a_i \in \mathbb{Z}$.

Since $M_{\text{diag}} = \frac{1}{\sqrt{2}} O_K + \frac{1+i}{2} O_K$, we also have $n := m_1 m_1^* \in \frac{1}{2} O_K$. Since $m_1 \in \frac{1}{\sqrt{2}} M_{\mathcal{O}}$, there exists $\hat{m_1} \in M_{\mathcal{O}}$ such that $m_1 = \frac{\hat{m_1}}{\sqrt{2}}$ and furthermore, $\hat{m_1}\hat{m_1}^* = 2n := \hat{n} \in O_K$. We write $\hat{n} = b_0 + b_1 \cdot 2\cos(\frac{\pi}{8}) + b_2\sqrt{2} + b_3 \cdot 2\cos(\frac{3\pi}{8})$ with all coefficients in $\mathbb{Z}$. Let $\Sigma_{\mathcal{O}}$ be defined as the matrix with rows:

$$\begin{aligned} \Sigma_{\mathcal{O}}^{(2j)} &= (\text{Re}(\sigma_j(y_0)), \ldots, \text{Re}(\sigma_j(y_7)) \\ \Sigma_{\mathcal{O}}^{(2j+1)} &= (\text{Im}(\sigma_j(y_0)), \ldots, \text{Im}(\sigma_j(y_7)), \end{aligned}$$

for $1 \leq j \leq 7$, where the σ_j are defined in Section 4.5.3.2. Additionally, take Σ' as defined in Section 4.5.3.2, and define normalization matrices Λ and Λ' as the diagonal matrices with the entries $\left(\sqrt{\sigma_1(\ell^N)}, \sqrt{\sigma_1(\ell^N)}, \ldots, \sqrt{\sigma_4(\ell^N)}, \sqrt{\sigma_4(\ell^N)}\right)$ and $(\sigma_1(2\ell^N), (\sigma_2(2\ell^N), (\sigma_3(2\ell^N), \sigma_4(2\ell^N))$ on the main diagonal, respectively. Hence the operations $\Lambda^{-1}\Sigma_{\mathcal{O}}$ and $\Lambda'^{-1}\Sigma'$ first embed an element m_1 or $\hat{n}$ into the Euclidean space of our approximation regions, then normalises it to satisfy the constraints. Candidate values for m_1 are then obtained by solving point enumeration problems below.

Problem 4.5.10 (2D point enumeration (Clifford+$\sqrt{T}$ basis)). *Let R_{approx} be a 2D region corresponding to a particular approximation problem.*

Find $(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7) \in \mathbb{Z}^8$ such that

$$\Lambda^{-1}\Sigma_{\mathcal{O}} \cdot (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)^T \in R_{\text{approx}} \times D_1 \times D_1 \times D_1.$$

Problem 4.5.11 (1D point enumeration (Clifford+$\sqrt{T}$ basis)). *Let $I_{\text{approx}} \subset [0,1]$ be a real interval corresponding to a particular approximation problem. Find $(a'_0, a'_1, a'_2, a'_3) \in \mathbb{Z}^4$ such that*

$${\Lambda'}^{-1}\Sigma' \cdot (b_0, b_1, b_2, b_3)^T \in I_{\text{approx}} \times [0,1] \times [0,1] \times [0,1].$$

In the first case, we immediately recover a candidate value for m_1. In the second case, we recover a candidate value for $\hat{n}$, solve the norm equation $\hat{m}_1\hat{m}_1{}^* = \hat{n}$ and for every solution $\hat{m}_1$ we obtain a candidate value m_1 by setting $m_1 = \frac{\hat{m}_1}{\sqrt{2}}$.

4.5.3.5 Finding m_2: solving a norm equation

Given a candidate value for m_1, we proceed to solve a norm equation problem (or determine there is no solution), restricting m_2 to $M^{m_1}_{\mathrm{off-diag}}$:

Problem 4.5.12. *Given* $m_1 \in \frac{1}{\sqrt{2}} M_{\mathcal{O}}$ *and integer* N, *find* $m_2 \in M^{m_1}_{\mathrm{off-diag}}$ *such that*

$$m_2 m_2^* = \ell^N - m_1 m_1^* \in \frac{1}{2} O_K.$$

Fixing an arbitrary $m \in M^{m_1}_{\mathrm{off-diag}}$, we have $M^{m_1}_{\mathrm{off-diag}} = m + M_{\mathcal{O}}$, since for any two $m, m' \in M^{m_1}_{\mathrm{off-diag}}$ we have $m - m' \in M^{0}_{\mathrm{off-diag}} = M_{\mathcal{O}}$. Since $M_{\mathrm{off-diag}} = M_{\mathrm{diag}} = \frac{1}{\sqrt{2}} M_{\mathcal{O}}$, Problem 4.5.12 can then be reformulated as

Problem 4.5.13. *Given* $\hat{m_1} \in M_{\mathcal{O}}$, *integer* N, *and* $m/\sqrt{2} \in M^{m_1}_{\mathrm{off-diag}}$ *find* $\hat{m_2} \in m + \sqrt{2} M_{\mathcal{O}}$ *such that*

$$\hat{m_2} \hat{m_2}^* = 2\ell^N - \hat{m_1} \hat{m_1}^* \in O_K.$$

Solving Problem 4.5.13 for $\hat{m_2}$ then yields a solution to Problem 4.5.12: $m_2 = \hat{m_2}/\sqrt{2}$.

4.6 Impact on resource cost

The following lemma proves that the new approach for solving the general unitary synthesis established in Section 4.3.3 results in shorter sequences for approximation, under a reasonable heuristic regarding diagonal approximations.

Lemma 4.6.1. *Solutions to Problem 4.3.1 that satisfy the conditions of Proposition 4.3.7 yield sequence lengths of* $O(7 \log_\ell(\frac{1}{\varepsilon}))$.

Proof. Recall that Proposition 4.3.7 establishes that a solution to Problem 4.3.1 involves two diagonal unitary approximations and a 'magnitude approximation'. As outlined in Section 4.4, each of these steps amounts to point enumeration in a feasible region, followed by solving a norm equation. For the magnitude approximation, we can *a priori* bound the size of the norm for which we accept candidates for u to $\approx \frac{1}{\varepsilon}$. Then, since the norm is equivalent to ℓ^N by design, we have $N \approx \log_\ell(\frac{1}{\varepsilon})$. For the diagonal approximations, it is known that sequence lengths of $3\log_\ell(\frac{1}{\varepsilon})$ [78] are optimal. Hence, the total sequence length for the general unitary approximation is $7\log_\ell(\frac{1}{\varepsilon})$. □

In comparison to the Euler decomposition method, which requires three diagonal approximations resulting in total length of $9\log_\ell(\frac{1}{\varepsilon})$ [78], our magnitude approximation method achieves shorter sequences.

We have assumed in Lemma 4.6.1 that the same accuracy is chosen for the diagonal and magnitude approximations. In practice, it is of course possible to choose different levels of accuracy and thus model the sequence length as

$$SL := 6\log_\ell(1/\varepsilon_1) + \log_\ell(1/\varepsilon_2),$$

where ε_1 is the accuracy for diagonal approximation and ε_2 is the accuracy for magnitude approximation. Recall that the total accuracy of the approximation is given by $\varepsilon = 2\varepsilon_1 + \varepsilon_2$. Rewriting ε_2 as $\varepsilon - 2\varepsilon_1$, we have $SL = \log_\ell(1/(\varepsilon_1^6(\varepsilon - 2\varepsilon_1)))$. Hence, to minimise sequence lengths we then look to maximise $y = \varepsilon_1^6\varepsilon - 2\varepsilon_1^7$, for $0 < \varepsilon_1 < \varepsilon \leq 1$. The maximum occurs when $\varepsilon_1 = \frac{3\varepsilon}{7}$ (and so $\varepsilon_2 = \frac{\varepsilon}{7}$). Put in terms of the approximations, this would mean that the magnitude approximation is completed to a closer degree of accuracy than the two diagonal approximations.

4.7 Conclusions

With this chapter, we sought to better establish the computational resources of a quantum adversary, thus addressing the third of Koblitz and Menezes' points of error. Our approach was inspired by the protocol-independent criterion for security assumptions from [43].

Specifically, we showed that the resource costs of approximating a general unitary can be improved by a factor of $\frac{7}{9}$, using a new method of approximation. Sequence lengths linear in $\log(\frac{1}{\varepsilon})$ are expected, and have been seen before in literature. Nevertheless, reducing the constant factor represents progress towards optimal sequence lengths. We see that our result will have greatest impact on algorithms that already require several hundreds of unitaries to implement. Moreover, we argue that our new approach, which borrows from path-finding algorithms, is itself a worthwhile contribution.

We note also that while these results are directly applicable to the approximation of single-qubit unitaries, there already exist algorithms for the decomposition of multi-qubit unitaries into circuits of single-qubit unitaries. Hence, our results are applicable to these cases as well. It remains for future research to make further improvements in the multi-qubit landscape.

Summary and conclusions

This thesis has examined three points in reductionist security proofs that are susceptible to errors induced by flawed assumptions, guided by the work of Koblitz and Menezes [62]. We firstly introduced two classes of assumptions arising in classical cryptanalysis, the relevance of which was demonstrated through examples in real-world cryptography (isogeny-based and multivariate-based), and closed by addressing the resource costs of quantum cryptanalysis. By highlighting these three areas, this thesis presents a holistic overview of the many approaches to cryptography security analysis. The results contained herein both pertain to the security of specific protocols, in terms of changing parameters, and provide evidence for the importance of studying cryptographic security assumptions, in general.

In Chapter 2, this thesis demonstrated that the security assurances derived from the difficulty of well-studied, intractable mathematical problems cannot necessarily be transferred to problem variants when only one-way reductions are proven. Specifically, we disproved the hardness assumptions on the OMSSCDH and 1MSSCDH problems, and provided attacks against two undeniable isogeny signature schemes that employed them.

That is not to say that a two-way reduction is sufficient to guarantee a faultless security analysis due to issues that can occur when complexity-theoretic results are translated to practical values for implementation. The example of Gröbner basis finding algorithms in Chapter 3 supports the argument that if approximations are necessary they are better based on proven results rather than heuristics. We have provided explicit formulas for proven bounds on the solving degree of overdetermined systems, as an alternative to the degree of regularity.

Finally, this thesis provides an improved understanding of the resource costs that would affect a quantum adversary. In Chapter 4, we have shown that the cost of fault-tolerantly approximating single-qubit unitaries is *less* than previously possible. The improvement is a factor of $\frac{7}{9}$. This is a sufficiently general result so can be applied to as-yet undiscovered algorithms.

There are a few open problems pertaining to this work:

1. Are there possible attacks against the Decisional Supersingular Product problem [52, 80]? This problem is used by Srinath and Chandrasekaran to prove the blindness property and by Jao and Soukharev to argue zero-knowledge of their confirmation and disavowal protocols.
2. Does there exist $M(n, m)$ such that $|d_{\text{solve}} - d_{\text{reg}}| \leq M(n, m)$ for all cryptographic semi-regular sequences of m polynomials in n variables? What is a lower bound for the solving degree?
3. What properties (if any) of number fields make solving relative norm equations with restrictions on coset membership computationally feasible?
4. What effect do the mixing strategies of Campbell [20] and Hastings [48] have on sequence lengths when used in conjunction with our method for solving the general unitary approximation problem?

The work contained in this thesis serves to caution that continued scrutiny is needed to ensure that only *good* assumptions are used in post-quantum security analyses. Our contention is that confidence in reductionist security proofs can only be established through the use of these good assumptions and that our understanding of what this means needs to be continually assessed and updated. We have argued that proven results, even if only applicable to a smaller set of protocols, are preferable to unproven (or, more pertinently, disproven) results and that cryptanalysts should remain cognisant of all aspects of quantum cost to give a realistic appraisal of security. In conclusion, although assumptions are an inevitable and important part of post-quantum security analyses, the field must remain vigilant of the vectors of error that can exist and work to eliminate them.

Bibliography

[1] Magali Bardet. "Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie". PhD thesis. 2004.

[2] Magali Bardet and Frédéric Chyzak. "On the complexity of a Gröbner basis algorithm". In: *Algorithms Seminar*. 2005, pp. 85–92.

[3] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. "On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations". In: *Proceedings of the International Conference on Polynomial System Solving*. 2004, pp. 71–74.

[4] Magali Bardet, Jean-Charles Faugère, Bruno Salvy, and Bo-Yin Yang. "Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems". In: *Proceedings of MEGA*. Vol. 5. 2005.

[5] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. "Elementary gates for quantum computation". In: *Physical Review A* 52.5 (Nov. 1995), pp. 3457–3467. ISSN: 1050-2947. DOI: `10.1103/PhysRevA.52.3457`. arXiv: `9503016 [quant-ph]`.

[6] Mihir Bellare. "Practice-oriented provable-security". In: *International Workshop on Information Security*. Springer. 1997, pp. 221–231.

[7] Philip Benge, Valerie Burks, and Nicholas Cobar. *Gröbner Basis Conversion Using the FGLM Algorithm*. URL: `https://www.math.lsu.edu/system/files/Groeb_Project_revised_final.pdf`.

[8] Daniel J Bernstein. "Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete". In: *SHARCS* 9 (2009), p. 105.

[9] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. "Hybrid approach for solving multivariate systems over finite fields". In: *Journal of Mathematical Cryptology* 3.3 (2009), pp. 177–197.

[10] Ward Beullens and Bart Preneel. "Field lifting for smaller UOV public keys". In: *International Conference on Cryptology in India*. Springer. 2017, pp. 227–246.

[11] Mina Bigdeli, Emanuela De Negri, Manuela M Dizdarevic, Elisa Gorla, Romy Minko, and Sulamithe Tsakou. "Semi-regular sequences and other random systems of equations". In: *Women in Numbers Europe III*. Springer. 2020.

[12] Olivier Billet and Jintai Ding. "Overview of Cryptanalysis Techniques in Multivariate Public Key Cryptography". In: *Gröbner Bases, Coding, and Cryptography*. Ed. by Massimiliano Sala, Shojiro Sakata, Teo Mora, Carlo Traverso, and Ludovic Perret. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 263–283. ISBN: 978-3-540-93806-4. DOI: `10.1007/978-3-540-93806-4_15`.

[13] Alex Bocharov, Yuri Gurevich, and Krysta M Svore. "Efficient Decomposition of Single-Qubit Gates into V Basis Circuits". In: *Physical Review A* 88.1 (July 2013), pp. 1–13. DOI: `10.1103/PhysRevA.88.012313`. arXiv: `1303.1411`.

[14] Alex Bocharov, Martin Roetteler, and Krysta M Svore. "Efficient synthesis of probabilistic quantum circuits with fallback". In: *Physical Review A* 91.5 (May 2015), p. 052317. ISSN: 1050-2947. DOI: `10.1103/PhysRevA.91.052317`. arXiv: `1409.3552`.

[15] Wieb Bosma, John Cannon, and Catherine Playoust. "The Magma algebra system I: The user language". In: *Journal of Symbolic Computation* 24.3-4 (1997), pp. 235–265.

[16] Jean Bourgain and Alex Gamburd. "A spectral gap theorem in SU(d)". In: *Journal of the European Mathematical Society* 14.5 (2012), pp. 1455–1511.

[17] Gilles Brassard, Peter Høyer, and Alain Tapp. "Quantum cryptanalysis of hash and claw-free functions". In: *Lecture Notes in Computer Science* (1998), 163–169. ISSN: 1611-3349. DOI: `10.1007/bfb0054319`. URL: `http://dx.doi.org/10.1007/BFb0054319`.

[18] Bruno Buchberger. "Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal". In: *PhD thesis, Universitat Insbruck* (1965).

[19] Alessio Caminata and Elisa Gorla. "Solving multivariate polynomial systems and an invariant from commutative algebra". In: *International Workshop on the Arithmetic of Finite Fields*. Springer. 2020, pp. 3–36.

[20] Earl Campbell. "Shorter gate sequences for quantum computing by mixing unitaries". In: *Physical Review A* 95.4 (Apr. 2017), p. 042306. ISSN: 2469-9926. DOI: `10.1103/PhysRevA.95.042306`. arXiv: `1612.02689`.

[21] Enrico Carlini, Huy Tài Hà, Brian Harbourne, and Adam Van Tuyl. *Ideals of powers and powers of ideals: Intersecting algebra, geometry, and combinatorics*. Vol. 27. Springer Nature, 2020.

[22] Denis X Charles, Eyal Z Goren, and Kristin E Lauter. “Families of Ramanujan graphs and quaternion algebras”. In: *Groups and symmetries: from Neolithic Scots to John McKay* 47 (2009), pp. 53–63.

[23] Denis X Charles, Kristin E Lauter, and Eyal Z Goren. “Cryptographic hash functions from expander graphs”. In: *Journal of Cryptology* 22.1 (2006), pp. 93–113.

[24] Sanjit Chatterjee, Alfred Menezes, and Palash Sarkar. “Another look at tightness”. In: *International Workshop on Selected Areas in Cryptography*. Springer. 2011, pp. 293–319.

[25] David Chaum and Hans Van Antwerpen. “Undeniable signatures”. In: *Conference on the Theory and Application of Cryptology*. Springer. 1989, pp. 212–216.

[26] Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe. “MQDSS specifications”. In: *NIST PQC Round* 2 (2018), p. 13.

[27] Anamaria Costache, Brooke Feigon, Kristin Lauter, Maike Massierer, and Anna Puskás. “Ramanujan graphs in cryptography”. In: *Research Directions in Number Theory*. Springer, 2019, pp. 1–40.

[28] David Cox, John Little, and Donal O’Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer Science & Business Media, 2013.

[29] Ivan Damgard and Torben Pedersen. “New convertible undeniable signature schemes”. In: *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 1996, pp. 372–386.

[30] Luca De Feo. “Mathematics of isogeny based cryptography”. In: *arXiv preprint arXiv:1711.04062* (2017).

[31] James Weldon Demmel. “On condition numbers and the distance to the nearest ill-posed problem”. In: *Numerische Mathematik* 51.3 (1987), pp. 251–289.

[32] Jintai Ding, Albrecht Petzoldt, and Lih-chung Wang. “The cubic simple matrix encryption scheme”. In: *International Workshop on Post-Quantum Cryptography*. Springer. 2014, pp. 76–87.

[33] Jintai Ding and Bo-Yin Yang. “Multivariate public key cryptography”. In: *Post-quantum cryptography*. Springer, 2009, pp. 193–241.

[34] David Eisenbud. *Commutative algebra: with a view toward algebraic geometry*. Vol. 150. Springer Science & Business Media, 2013.

[35] Leonhard Euler. “De evolutione potestatis polynomialis cuiuscunque $(1 + x + x^2 + x^3 + x^4 + \text{etc.})^n$”. In: *Nova Acta Academiae Scientiarum Imperialis Petropolitanae* (1801), pp. 47–57.

[36] Nour-Eddine Fahssi. “Some identities involving polynomial coefficients”. In: *Fibonacci Quarterly* 54.2 (2015), pp. 125–136.

[37] Jean-Charles Faugère. “A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5)”. In: *Proceedings of ISSAC*. 2002, pp. 75–83.

[38] Jean-Charles Faugère. *Algebraic cryptanalysis of HFE using Gröbner bases*. Research Report RR-4738. INRIA, 2003, p. 19. URL: https://hal.inria.fr/inria-00071849.

[39] Jean-Charles Faugère, Patrizia Gianni, Daniel Lazard, and Teo Mora. “Efficient computation of zero-dimensional Gröbner bases by change of ordering”. In: *Journal of Symbolic Computation* 16.4 (1993), pp. 329–344.

[40] C. Fieker, A. Jurk, and M. Pohst. “On Solving Relative Norm Equations in Algebraic Number Fields”. In: *Mathematics of Computation* 66.217 (1997), pp. 399–410. ISSN: 00255718, 10886842. URL: http://www.jstor.org/stable/2153662.

[41] Ralf Fröberg. “An inequality for Hilbert series of graded algebras”. In: *Mathematica Scandinavica* 56.2 (1985), pp. 117–144.

[42] Michael R Garey and David S Johnson. *Computers and intractability: a guide to the theory of NP-completeness*. W.H. Freeman and Company, 1979, pp. 72–89. ISBN: 0716710447.

[43] Shafi Goldwasser and Silvio Micali. “Probabilistic encryption”. In: *Journal of computer and system sciences* 28.2 (1984), pp. 270–299.

[44] David Gosset, Vadym Kliuchnikov, Michele Mosca, and Vincent Russo. “An Algorithm for the T-Count”. In: *Quantum Info. Comput.* 14.15–16 (Nov. 2014), 1261–1276. ISSN: 1533-7146.

[45] Robert Granger. “On the static Diffie-Hellman problem on elliptic curves over extension fields”. In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2010, pp. 283–302.

[46] Aram W Harrow, Avinatan Hassidim, and Seth Lloyd. “Quantum algorithm for linear systems of equations”. In: *Physical review letters* 103.15 (2009), p. 150502.

[47] Aram W Harrow, Benjamin Recht, and Isaac L Chuang. “Efficient discrete approximations of quantum gates”. In: *Journal of Mathematical Physics* 43.9 (2002), pp. 4445–4451.

[48] Matthew B Hastings. “Turning Gate Synthesis Errors into Incoherent Errors”. In: *Quantum Information & Computation* 17.5-6 (Mar. 2017), pp. 488–494. ISSN: 1533-7146. arXiv: `1612.01011`.

[49] Timothy J Hodges, Sergio D Molina, and Jacob Schlather. “On the existence of homogeneous semi-regular sequences in $\mathbb{F}_2[X_1, ..., X_n]/(X_{12}, ..., X_{n2})$”. In: *Journal of Algebra* 476 (2017), pp. 519–547.

[50] Yasuhiko Ikematsu, Ray Perlner, Daniel Smith-Tone, Tsuyoshi Takagi, and Jeremy Vates. “HFERP-a new multivariate encryption scheme”. In: *International Conference on Post-Quantum Cryptography*. Springer. 2018, pp. 396–416.

[51] David Jao and Luca De Feo. “Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies”. In: *International Workshop on Post-Quantum Cryptography*. Springer. 2011, pp. 19–34.

[52] David Jao and Vladimir Soukharev. “Isogeny-based quantum-resistant undeniable signatures”. In: *International Workshop on Post-Quantum Cryptography*. Springer. 2014, pp. 160–179.

[53] Antoine Joux. *Algorithmic cryptanalysis*. Chapman and Hall/CRC, 2009.

[54] Aviad Kipnis and Adi Shamir. “Cryptanalysis of the HFE public key cryptosystem by relinearization”. In: *Annual International Cryptology Conference*. Springer. 1999, pp. 19–30.

[55] Aleksei Y Kitaev. “Quantum computations: algorithms and error correction”. In: *Uspekhi Matematicheskikh Nauk* 52.6 (1997), pp. 53–112.

[56] Vadym Kliuchnikov, Alex Bocharov, Martin Roetteler, and John Yard. “A Framework for Approximating Qubit Unitaries”. In: *arXiv e-prints* (Aug. 2015). arXiv: `1510.03888 [quant-ph]`.

[57] Vadym Kliuchnikov, David Maslov, and Michele Mosca. “Asymptotically Optimal Approximation of Single Qubit Unitaries by Clifford and T Circuits Using a Constant Number of Ancillary Qubits”. In: *Physical Review Letters* 110.19 (May 2013), p. 190502. DOI: `10.1103/PhysRevLett.110.190502`. arXiv: `1212.0822 [quant-ph]`.

[58] Vadym Kliuchnikov, Dmitri Maslov, and Michele Mosca. “Fast and Efficient Exact Synthesis of Single-Qubit Unitaries Generated by Clifford and T Gates”. In: *Quantum Info. Comput.* 13.7–8 (July 2013), 607–630. ISSN: 1533-7146.

[59] Vadym Kliuchnikov and John Yard. “A framework for exact synthesis”. In: *arXiv e-prints* (Apr. 2015). arXiv: `1504.04350 [quant-ph]`.

[60] Neal Koblitz and Alfred Menezes. "Another look at non-standard discrete log and Diffie-Hellman problems". In: *Journal of Mathematical Cryptology* 2.4 (2008), pp. 311–326.

[61] Neal Koblitz and Alfred Menezes. "Critical perspectives on provable security: Fifteen years of "another look" papers". In: *Advances in Mathematics of Communications* 13.4 (2019), p. 517.

[62] Neal Koblitz and Alfred J Menezes. "Another look at "provable security"". In: *Journal of Cryptology* 20.1 (2007), pp. 3–37.

[63] Robin Kothari. "Efficient algorithms in quantum query complexity". In: *PhD Thesis* (2014).

[64] Martin Kreuzer and Lorenzo Robbiano. *Computational commutative algebra.* Vol. 1. Springer, 2000.

[65] Martin Kreuzer and Lorenzo Robbiano. *Computational commutative algebra 2.* Vol. 2. Springer Science & Business Media, 2005.

[66] Kaoru Kurosawa and Jun Furukawa. "Universally composable undeniable signature". In: *International Colloquium on Automata, Languages, and Programming.* Springer. 2008, pp. 524–535.

[67] Daniel Lazard. "Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations". In: *European Conference on Computer Algebra.* Springer. 1983, pp. 146–156.

[68] Alexander Lubotzky, Ralph Phillips, and Peter Sarnak. "Ramanujan graphs". In: *Combinatorica* 8.3 (1988), pp. 261–277.

[69] Simon-Philipp Merz, Romy Minko, and Christophe Petit. "Another look at some isogeny hardness assumptions". In: *Cryptographers' Track at the RSA Conference.* Springer. 2020, pp. 496–511.

[70] Juan Migliore and Rosa Miró-Roig. "On the minimal free resolution of $n + 1$ general forms". In: *Transactions of the American Mathematical Society* 355.1 (2003), pp. 1–36.

[71] Moni Naor. "On cryptographic assumptions and challenges". In: *Annual International Cryptology Conference.* Springer. 2003, pp. 96–109.

[72] Michael Nielsen and Isaac Chuang. *Quantum Computation and Quantum Information.* Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2002. ISBN: 9780521635035. URL: `https://books.google.co.uk/books?id=65FqEKQOfP8C`.

[73] Keith Pardue. "Generic sequences of polynomials". In: *Journal of Algebra* 324.4 (2010), pp. 579–590.

[74] Christophe Petit, Kristin Lauter, and Jean-Jacques Quisquater. "Full cryptanalysis of LPS and Morgenstern hash functions". In: *International Conference on Security and Cryptography for Networks*. Springer. 2008, pp. 263–277.

[75] Eduardo C Pinto and Christophe Petit. "Better path-finding algorithms in LPS Ramanujan graphs". In: *Journal of Mathematical Cryptology* 12.4 (2018), pp. 191–202.

[76] Neil J Ross and Peter Selinger. "Optimal ancilla-free Clifford+T approximation of z-rotations". In: *Quantum Information & Computation* 15.11-12 (2015), pp. 932–950. arXiv: `1403.2975`.

[77] Peter Sarnak. *Letter to Aaronson and Pollington on the Solvay-Kitaev Theorem and Golden Gates*. 2015. URL: `http://publications.ias.edu/sarnak/paper/2637`.

[78] Peter Selinger. "Efficient Clifford+T approximation of single-qubit operators". In: *Quantum Information & Computation* 15.1-2 (Dec. 2015), pp. 159–180. arXiv: `1212.6253`.

[79] Joseph H Silverman. *The arithmetic of elliptic curves*. Vol. 106. Springer Science & Business Media, 2009.

[80] M S Srinath and V Chandrasekaran. "Isogeny-based Quantum-resistant Undeniable Blind Signature Scheme". In: *International Journal of Network Security* 20.1 (2018), pp. 9–18.

[81] Zachary Stier. "Short paths in PU(2)". In: *Quantum Information and Computation* 21.9–10 (2021), pp. 771–780.

[82] Chengdong Tao, Adama Diene, Shaohua Tang, and Jintai Ding. "Simple matrix scheme for encryption". In: *International Workshop on Post-Quantum Cryptography*. Springer. 2013, pp. 231–242.

[83] Enrico Thomae and Christopher Wolf. "Solving underdetermined systems of multivariate quadratic equations revisited". In: *International Workshop on Public Key Cryptography*. Springer. 2012, pp. 156–171.

[84] Jacques Vélu. "Isogénies entre courbes elliptiques". In: *Comptes-Rendus de l'Académie des Sciences, Série I* 273 (July 1971), pp. 238–241.

[85] John Michael Voight. *Quadratic forms and quaternion algebras: Algorithms and arithmetic*. University of California, Berkeley, 2005.

[86] Junzo Watanabe. "The Dilworth number of Artinian rings and finite posets with rank function". In: *Commutative algebra and combinatorics*. Mathematical Society of Japan. 1987, pp. 303–312.

[87] Christopher Wolf and Bart Preneel. “Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations.” In: *IACR Cryptology ePrint Archive* 2005 (2005), p. 77.

[88] Wolfram Research, Inc. *Mathematica*. Version 11.0. 2016. URL: `https://www.wolfram.com/mathematica/`.

Appendix A

Index of regularity for over-determined systems

This appendix lists the index of regularity $r(n+\ell, n)$ of the ideal generated by a cryptographic semi-regular system of $n+\ell$ homogeneous quadratic equations in n variables. The formula for the k^{th} coefficient in the Hilbert series expansion for a cryptographic semi-regular system of $n+\ell$ homogeneous quadratic equations in n variables was calculated iteratively, until the first k was reached for which the coefficient is negative. This gives the value of $r(n+\ell, n)$, as discussed in Section 3.5.1. The value of $r(n+\ell, n)$ bounds the solving degree of cryptographic semi-regular systems of $n+\ell$ homogeneous polynomials in n variables or $n+\ell$ inhomogeneous polynomials in $n-1$ variables (under the assumption that the system is in generic coordinates, as discussed in Section 3.2).

Table A.1: $r(n+\ell, n)$ for $2 \leq \ell \leq 100, 2 \leq n \leq 26$

ℓ/n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
2	2	3	3	3	4	4	5	5	6	6	6	7	7	8	8	9	9	10	10	10	11	11	12	12	13
3	2	2	3	3	4	4	4	5	5	5	6	6	7	7	7	8	8	9	9	10	10	10	11	11	12
4	2	2	3	3	3	4	4	4	5	5	5	6	6	7	7	7	8	8	8	9	9	10	10	10	11
5	2	2	3	3	3	3	4	4	4	5	5	5	6	6	7	7	7	8	8	8	9	9	9	10	10
6	2	2	2	3	3	3	4	4	4	5	5	5	6	6	6	7	7	7	8	8	8	9	9	9	10
7	2	2	2	3	3	3	3	4	4	4	5	5	5	6	6	6	7	7	7	8	8	8	9	9	9
8	2	2	2	3	3	3	3	4	4	4	4	5	5	5	6	6	6	7	7	7	8	8	8	9	9
9	2	2	2	3	3	3	3	4	4	4	4	5	5	5	5	6	6	6	7	7	7	8	8	8	9
10	2	2	2	2	3	3	3	3	4	4	4	4	5	5	5	6	6	6	6	7	7	7	8	8	8
11	2	2	2	2	3	3	3	3	4	4	4	4	5	5	5	5	6	6	6	6	7	7	7	8	8
12	2	2	2	2	3	3	3	3	3	4	4	4	4	5	5	5	5	6	6	6	7	7	7	7	8
13	2	2	2	2	3	3	3	3	3	4	4	4	4	5	5	5	5	6	6	6	6	7	7	7	7
14	2	2	2	2	3	3	3	3	3	4	4	4	4	4	5	5	5	5	6	6	6	6	7	7	7
15	2	2	2	2	2	3	3	3	3	3	4	4	4	4	5	5	5	5	6	6	6	6	7	7	7
16	2	2	2	2	2	3	3	3	3	3	4	4	4	4	5	5	5	5	5	6	6	6	6	7	7
17	2	2	2	2	2	3	3	3	3	3	4	4	4	4	4	5	5	5	5	6	6	6	6	7	7
18	2	2	2	2	2	3	3	3	3	3	4	4	4	4	4	5	5	5	5	5	6	6	6	6	7
19	2	2	2	2	2	3	3	3	3	3	3	4	4	4	4	4	5	5	5	5	6	6	6	6	7
20	2	2	2	2	2	3	3	3	3	3	3	4	4	4	4	4	5	5	5	5	5	6	6	6	6
21	2	2	2	2	2	2	3	3	3	3	3	4	4	4	4	4	5	5	5	5	5	6	6	6	6
22	2	2	2	2	2	2	3	3	3	3	3	3	4	4	4	4	4	5	5	5	5	5	6	6	6
23	2	2	2	2	2	2	3	3	3	3	3	3	4	4	4	4	4	5	5	5	5	5	6	6	6
24	2	2	2	2	2	2	3	3	3	3	3	3	4	4	4	4	4	5	5	5	5	5	6	6	6
25	2	2	2	2	2	2	3	3	3	3	3	3	4	4	4	4	4	4	5	5	5	5	5	6	6
26	2	2	2	2	2	2	3	3	3	3	3	3	3	4	4	4	4	4	5	5	5	5	5	6	6
27	2	2	2	2	2	2	3	3	3	3	3	3	3	4	4	4	4	4	5	5	5	5	5	5	6
28	2	2	2	2	2	2	2	3	3	3	3	3	3	4	4	4	4	4	4	5	5	5	5	5	6
29	2	2	2	2	2	2	2	3	3	3	3	3	3	4	4	4	4	4	4	5	5	5	5	5	6
30	2	2	2	2	2	2	2	3	3	3	3	3	3	4	4	4	4	4	4	5	5	5	5	5	5
31	2	2	2	2	2	2	2	3	3	3	3	3	3	3	4	4	4	4	4	4	5	5	5	5	5
32	2	2	2	2	2	2	2	3	3	3	3	3	3	3	4	4	4	4	4	4	5	5	5	5	5
33	2	2	2	2	2	2	2	3	3	3	3	3	3	3	4	4	4	4	4	4	5	5	5	5	5
34	2	2	2	2	2	2	2	3	3	3	3	3	3	3	4	4	4	4	4	4	5	5	5	5	5
35	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	4	4	4	4	4	4	5	5	5	5
36	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	4	4	4	4	4	4	5	5	5	5
37	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	4	4	4	4	4	4	5	5	5	5
38	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	4	4	4	4	4	4	4	5	5	5
39	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	4	4	4	4	4	4	4	5	5	5
40	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	4	4	4	4	4	4	5	5	5
41	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	4	4	4	4	4	4	5	5	5
42	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	5	5
43	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	5	5
44	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	5	5
45	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	4	4	4	4	4	4	4	5	5
46	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	5
47	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	5
48	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	5
49	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	5
50	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4
51	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4
52	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4
53	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4
54	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4
55	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4
56	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4
57	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4
58	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4
59	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4
60	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4
61	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4
62	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4
63	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4
64	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4
65	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4
66	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	4	4	4	4	4
67	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	4	4	4	4	4
68	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	4	4	4	4	4
69	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	4	4	4	4	4
70	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4
71	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4
72	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4
73	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4
74	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4
75	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4
76	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4
77	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	4	4	4
78	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4
79	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4
80	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4
81	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4
82	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4
83	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4
84	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4
85	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	4	4
86	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	4	4
87	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	4	4
88	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	4	4
89	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	4	4
90	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	4	4
91	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4
92	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	4
93	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	4
94	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	4
95	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	4
96	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	4
97	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	4
98	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	4
99	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	4
100	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	3

Table A.2: $r(n+\ell,n)$ for $2 \leq \ell \leq 100, 27 \leq n \leq 51$

ℓ/n	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
2	25	25	26	26	27	27	28	28	28	29	29	30	30	31	31	32	32	33	33	34	34	35	35	36	36
3	23	23	24	24	25	25	26	26	26	27	27	28	28	29	29	30	30	31	31	31	32	32	33	33	34
4	22	22	22	23	23	24	24	25	25	25	26	26	27	27	28	28	28	29	29	30	30	31	31	31	32
5	20	21	21	22	22	22	23	23	24	24	25	25	25	26	26	27	27	27	28	28	29	29	30	30	30
6	20	20	20	21	21	21	22	22	23	23	23	24	24	25	25	26	26	26	27	27	28	28	28	29	29
7	19	19	19	20	20	21	21	21	22	22	23	23	23	24	24	25	25	25	26	26	27	27	27	28	28
8	18	18	19	19	19	20	20	21	21	21	22	22	23	23	23	24	24	24	25	25	26	26	26	27	27
9	17	18	18	18	19	19	20	20	20	21	21	21	22	22	23	23	23	24	24	24	25	25	26	26	26
10	17	17	18	18	18	19	19	19	20	20	20	21	21	21	22	22	23	23	23	24	24	24	25	25	26
11	16	17	17	17	18	18	18	19	19	19	20	20	20	21	21	22	22	22	23	23	23	24	24	24	25
12	16	16	17	17	17	18	18	18	19	19	19	20	20	20	21	21	21	22	22	22	23	23	23	24	24
13	15	16	16	16	17	17	17	18	18	18	19	19	19	20	20	20	21	21	21	22	22	22	23	23	24
14	15	15	16	16	16	17	17	17	18	18	18	19	19	19	20	20	20	21	21	21	22	22	22	23	23
15	15	15	15	16	16	16	17	17	17	18	18	18	18	19	19	19	20	20	20	21	21	21	22	22	22
16	14	15	15	15	16	16	16	16	17	17	17	18	18	18	19	19	19	20	20	20	21	21	21	22	22
17	14	14	15	15	15	16	16	16	16	17	17	17	18	18	18	19	19	19	20	20	20	21	21	21	22
18	14	14	14	15	15	15	15	16	16	16	17	17	17	18	18	18	19	19	19	19	20	20	20	21	21
19	13	14	14	14	15	15	15	15	16	16	16	17	17	17	18	18	18	18	19	19	19	20	20	20	21
20	13	13	14	14	14	15	15	15	15	16	16	16	17	17	17	18	18	18	18	19	19	19	20	20	20
21	13	13	13	14	14	14	15	15	15	15	16	16	16	17	17	17	18	18	18	18	19	19	19	20	20
22	13	13	13	13	14	14	14	15	15	15	15	16	16	16	17	17	17	18	18	18	18	19	19	19	20
23	12	13	13	13	14	14	14	14	15	15	15	15	16	16	16	17	17	17	17	18	18	18	19	19	19
24	12	13	13	13	13	14	14	14	14	15	15	15	16	16	16	16	17	17	17	17	18	18	18	19	19
25	12	12	13	13	13	13	14	14	14	14	15	15	15	16	16	16	16	17	17	17	17	18	18	18	19
26	12	12	12	13	13	13	13	14	14	14	14	15	15	15	16	16	16	16	17	17	17	17	18	18	18
27	12	12	12	12	13	13	13	13	14	14	14	15	15	15	15	16	16	16	16	17	17	17	18	18	18
28	11	12	12	12	12	13	13	13	14	14	14	14	15	15	15	15	16	16	16	16	17	17	17	18	18
29	11	12	12	12	12	13	13	13	13	14	14	14	14	15	15	15	15	16	16	16	16	17	17	17	18
30	11	11	12	12	12	12	13	13	13	13	14	14	14	14	15	15	15	15	16	16	16	16	17	17	17
31	11	11	11	12	12	12	12	13	13	13	13	14	14	14	14	15	15	15	15	16	16	16	17	17	17
32	11	11	11	12	12	12	12	13	13	13	13	14	14	14	14	15	15	15	15	16	16	16	16	17	17
33	11	11	11	11	12	12	12	12	13	13	13	13	14	14	14	14	15	15	15	15	16	16	16	16	17
34	11	11	11	11	11	12	12	12	12	13	13	13	13	14	14	14	14	15	15	15	15	16	16	16	16
35	10	11	11	11	11	12	12	12	12	13	13	13	13	13	14	14	14	14	15	15	15	15	16	16	16
36	10	11	11	11	11	11	12	12	12	12	13	13	13	13	14	14	14	14	15	15	15	15	16	16	16
37	10	10	11	11	11	11	12	12	12	12	12	13	13	13	13	14	14	14	14	15	15	15	15	16	16
38	10	10	10	11	11	11	11	12	12	12	12	13	13	13	13	13	14	14	14	14	15	15	15	15	16
39	10	10	10	11	11	11	11	11	12	12	12	12	13	13	13	13	14	14	14	14	14	15	15	15	15
40	10	10	10	10	11	11	11	11	12	12	12	12	12	13	13	13	13	14	14	14	14	15	15	15	15
41	10	10	10	10	11	11	11	11	11	12	12	12	12	13	13	13	13	13	14	14	14	14	15	15	15
42	10	10	10	10	10	11	11	11	11	12	12	12	12	12	13	13	13	13	14	14	14	14	14	15	15
43	10	10	10	10	10	11	11	11	11	11	12	12	12	12	13	13	13	13	13	14	14	14	14	15	15
44	9	10	10	10	10	10	11	11	11	11	12	12	12	12	12	13	13	13	13	13	14	14	14	14	15
45	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13	13	14	14	14	14	14
46	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	13	13	13	13	13	14	14	14	14
47	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13	13	14	14	14	14
48	9	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	13	13	13	13	13	14	14	14
49	9	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13	13	13	14	14
50	9	9	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	13	13	13	13	13	14	14
51	9	9	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13	13	13	14
52	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13	13	14
53	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13	13	13
54	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13	13
55	9	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13	13
56	8	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13
57	8	9	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13
58	8	8	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13
59	8	8	9	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13
60	8	8	9	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	11	12	12	12	12	12	13
61	8	8	8	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13
62	8	8	8	9	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	11	12	12	12	12	12
63	8	8	8	8	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12
64	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	11	12	12	12	12
65	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12	12	12	12
66	8	8	8	8	8	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12	12	12	12
67	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	11	12	12	12
68	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12	12	12
69	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	11	12	12
70	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12	12
71	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	11	12
72	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12
73	7	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	11
74	7	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	11
75	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11
76	7	7	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11
77	7	7	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11
78	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11
79	7	7	7	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11
80	7	7	7	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11
81	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11
82	7	7	7	7	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11
83	7	7	7	7	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10	10	10	10	11	11
84	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11
85	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	10	11
86	7	7	7	7	7	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10	10	10	10	11
87	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11
88	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	10
89	7	7	7	7	7	7	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10	10	10	10
90	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10
91	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10
92	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10	10	10
93	7	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10
94	7	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10
95	7	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10	10
96	7	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10	10
97	7	7	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10
98	6	7	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10
99	6	7	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10
100	6	7	7	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10

Table A.3: $r(n+\ell,n)$ for $2 \leq \ell \leq 100, 52 \leq n \leq 76$

ℓ/n	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76
2	25	25	26	26	27	27	28	28	28	29	29	30	30	31	31	32	32	33	33	34	34	35	35	36	36
3	23	23	24	24	25	25	26	26	26	27	27	28	28	29	29	30	30	31	31	31	32	32	33	33	34
4	22	22	22	23	23	24	24	25	25	25	26	26	27	27	28	28	28	29	29	30	30	31	31	31	32
5	20	21	21	22	22	22	23	23	24	24	25	25	25	26	26	27	27	27	28	28	29	29	30	30	30
6	20	20	20	21	21	21	22	22	23	23	23	24	24	25	25	26	26	26	27	27	28	28	28	29	29
7	19	19	19	20	20	21	21	21	22	22	23	23	23	24	24	25	25	25	26	26	27	27	27	28	28
8	18	18	19	19	19	20	20	21	21	21	22	22	23	23	23	24	24	24	25	25	26	26	26	27	27
9	17	18	18	18	19	19	20	20	20	21	21	21	22	22	23	23	23	24	24	24	25	25	26	26	26
10	17	17	18	18	18	19	19	19	20	20	20	21	21	21	22	22	23	23	23	24	24	24	25	25	26
11	16	17	17	17	18	18	18	19	19	19	20	20	20	21	21	22	22	22	23	23	23	24	24	24	25
12	16	16	17	17	17	18	18	18	19	19	19	20	20	20	21	21	21	22	22	22	23	23	23	24	24
13	15	16	16	16	17	17	17	18	18	18	19	19	19	20	20	20	21	21	21	22	22	22	23	23	24
14	15	15	16	16	16	17	17	17	18	18	18	19	19	19	20	20	20	21	21	21	22	22	22	23	23
15	15	15	15	16	16	16	17	17	17	18	18	18	18	19	19	19	20	20	20	21	21	21	22	22	22
16	14	15	15	15	16	16	16	16	17	17	17	18	18	18	19	19	19	20	20	20	21	21	21	22	22
17	14	14	15	15	15	16	16	16	16	17	17	17	18	18	18	19	19	19	20	20	20	21	21	21	22
18	14	14	14	15	15	15	15	16	16	16	17	17	17	18	18	18	19	19	19	19	20	20	20	21	21
19	13	14	14	14	15	15	15	15	16	16	16	17	17	17	18	18	18	18	19	19	19	20	20	20	21
20	13	13	14	14	14	15	15	15	15	16	16	16	17	17	17	18	18	18	18	19	19	19	20	20	20
21	13	13	13	14	14	14	15	15	15	15	16	16	16	17	17	17	18	18	18	18	19	19	19	20	20
22	13	13	13	13	14	14	14	15	15	15	15	16	16	16	17	17	17	18	18	18	18	19	19	19	20
23	12	13	13	13	14	14	14	14	15	15	15	15	16	16	16	17	17	17	17	18	18	18	19	19	19
24	12	13	13	13	13	14	14	14	14	15	15	15	16	16	16	16	17	17	17	17	18	18	18	19	19
25	12	12	13	13	13	13	14	14	14	14	15	15	15	16	16	16	16	17	17	17	17	18	18	18	19
26	12	12	12	13	13	13	13	14	14	14	14	15	15	15	16	16	16	16	17	17	17	17	18	18	18
27	12	12	12	12	13	13	13	13	14	14	14	15	15	15	15	16	16	16	16	17	17	17	18	18	18
28	11	12	12	12	12	13	13	13	14	14	14	14	15	15	15	15	16	16	16	16	17	17	17	18	18
29	11	12	12	12	12	13	13	13	13	14	14	14	14	15	15	15	15	16	16	16	16	17	17	17	18
30	11	11	12	12	12	12	13	13	13	13	14	14	14	14	15	15	15	15	16	16	16	16	17	17	17
31	11	11	11	12	12	12	12	13	13	13	13	14	14	14	14	15	15	15	15	16	16	16	17	17	17
32	11	11	11	12	12	12	12	13	13	13	13	14	14	14	14	15	15	15	15	16	16	16	16	17	17
33	11	11	11	11	12	12	12	12	13	13	13	13	14	14	14	14	15	15	15	15	16	16	16	16	17
34	11	11	11	11	11	12	12	12	12	13	13	13	13	14	14	14	14	15	15	15	15	16	16	16	16
35	10	11	11	11	11	12	12	12	12	13	13	13	13	13	14	14	14	14	15	15	15	15	16	16	16
36	10	11	11	11	11	11	12	12	12	12	13	13	13	13	14	14	14	14	15	15	15	15	16	16	16
37	10	10	11	11	11	11	12	12	12	12	12	13	13	13	13	14	14	14	14	15	15	15	15	16	16
38	10	10	10	11	11	11	11	12	12	12	12	13	13	13	13	13	14	14	14	14	15	15	15	15	16
39	10	10	10	11	11	11	11	11	12	12	12	12	13	13	13	13	14	14	14	14	14	15	15	15	15
40	10	10	10	10	11	11	11	11	12	12	12	12	12	13	13	13	13	14	14	14	14	15	15	15	15
41	10	10	10	10	11	11	11	11	11	12	12	12	12	13	13	13	13	13	14	14	14	14	15	15	15
42	10	10	10	10	10	11	11	11	11	12	12	12	12	12	13	13	13	13	14	14	14	14	14	15	15
43	10	10	10	10	10	11	11	11	11	11	12	12	12	12	13	13	13	13	13	14	14	14	14	15	15
44	9	10	10	10	10	10	11	11	11	11	12	12	12	12	12	13	13	13	13	13	14	14	14	14	15
45	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13	13	14	14	14	14	14
46	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	13	13	13	13	13	14	14	14	14
47	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13	13	14	14	14	14
48	9	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	13	13	13	13	13	14	14	14
49	9	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13	13	13	14	14
50	9	9	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	13	13	13	13	13	14	14
51	9	9	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13	13	13	14
52	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13	13	14
53	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13	13	13
54	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13	13
55	9	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13	13
56	8	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13
57	8	9	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13	13
58	8	8	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13
59	8	8	9	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13	13
60	8	8	9	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	11	12	12	12	12	12	13
61	8	8	8	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12	13
62	8	8	8	9	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	11	12	12	12	12	12
63	8	8	8	8	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12	12	12	12	12
64	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	11	12	12	12	12
65	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12	12	12	12
66	8	8	8	8	8	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12	12	12	12
67	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	11	12	12	12
68	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12	12	12
69	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	11	11	11	11	11	11	12	12
70	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12	12
71	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	11	12
72	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	12
73	7	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	11
74	7	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11	11
75	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11
76	7	7	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11	11
77	7	7	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11
78	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11
79	7	7	7	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11	11
80	7	7	7	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11
81	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11
82	7	7	7	7	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11	11
83	7	7	7	7	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10	10	10	10	11	11
84	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11	11
85	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	10	11
86	7	7	7	7	7	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10	10	10	10	11
87	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	11
88	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10	10
89	7	7	7	7	7	7	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10	10	10	10
90	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10
91	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10	10
92	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10	10	10
93	7	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10
94	7	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10	10
95	7	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10	10
96	7	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10	10
97	7	7	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10	10
98	6	7	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10
99	6	7	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	9	10	10	10
100	6	7	7	7	7	7	7	7	7	8	8	8	8	8	8	8	9	9	9	9	9	9	10	10	10

Table A.4: $r(n+\ell,n)$ for $2 \leq \ell \leq 100, 77 \leq n \leq 100$

ℓ/n	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
2	36	37	37	38	38	39	39	40	40	41	41	42	42	43	43	44	44	45	45	45	46	46	47	47
3	34	35	35	35	36	36	37	37	38	38	39	39	40	40	40	41	41	42	42	43	43	44	44	45
4	32	33	33	34	34	35	35	35	36	36	37	37	38	38	38	39	39	40	40	41	41	42	42	42
5	31	31	32	32	33	33	33	34	34	35	35	36	36	36	37	37	38	38	39	39	39	40	40	41
6	30	30	30	31	31	32	32	32	33	33	34	34	35	35	35	36	36	37	37	37	38	38	39	39
7	28	29	29	30	30	30	31	31	32	32	33	33	33	34	34	35	35	35	36	36	37	37	37	38
8	28	28	28	29	29	29	30	30	31	31	31	32	32	33	33	33	34	34	35	35	35	36	36	37
9	27	27	27	28	28	29	29	29	30	30	30	31	31	32	32	32	33	33	34	34	34	35	35	36
10	26	26	27	27	27	28	28	28	29	29	30	30	30	31	31	32	32	32	33	33	33	34	34	35
11	25	26	26	26	27	27	27	28	28	28	29	29	30	30	30	31	31	31	32	32	33	33	33	34
12	25	25	25	26	26	26	27	27	27	28	28	28	29	29	30	30	30	31	31	31	32	32	33	33
13	24	24	25	25	25	26	26	26	27	27	27	28	28	29	29	29	30	30	30	31	31	31	32	32
14	23	24	24	24	25	25	25	26	26	26	27	27	28	28	28	29	29	29	30	30	30	31	31	31
15	23	23	23	24	24	25	25	25	26	26	26	27	27	27	28	28	28	29	29	29	30	30	30	31
16	22	23	23	23	24	24	24	25	25	25	26	26	26	27	27	27	28	28	28	29	29	29	30	30
17	22	22	23	23	23	23	24	24	24	25	25	25	26	26	26	27	27	28	28	28	29	29	29	30
18	21	22	22	22	23	23	23	24	24	24	25	25	25	26	26	26	27	27	27	28	28	28	29	29
19	21	21	22	22	22	23	23	23	24	24	24	25	25	25	26	26	26	26	27	27	27	28	28	28
20	21	21	21	22	22	22	22	23	23	23	24	24	24	25	25	25	26	26	26	27	27	27	28	28
21	20	21	21	21	21	22	22	22	23	23	23	24	24	24	25	25	25	26	26	26	27	27	27	28
22	20	20	20	21	21	21	22	22	22	23	23	23	24	24	24	25	25	25	25	26	26	26	27	27
23	20	20	20	20	21	21	21	22	22	22	23	23	23	23	24	24	24	25	25	25	26	26	26	27
24	19	20	20	20	20	21	21	21	22	22	22	23	23	23	23	24	24	24	25	25	25	26	26	26
25	19	19	20	20	20	20	21	21	21	22	22	22	22	23	23	23	24	24	24	25	25	25	26	26
26	19	19	19	19	20	20	20	21	21	21	22	22	22	22	23	23	23	24	24	24	25	25	25	25
27	18	19	19	19	19	20	20	20	21	21	21	22	22	22	22	23	23	23	24	24	24	24	25	25
28	18	18	19	19	19	19	20	20	20	21	21	21	21	22	22	22	23	23	23	24	24	24	24	25
29	18	18	18	19	19	19	19	20	20	20	21	21	21	21	22	22	22	23	23	23	24	24	24	24
30	18	18	18	18	19	19	19	19	20	20	20	21	21	21	21	22	22	22	23	23	23	23	24	24
31	17	18	18	18	18	19	19	19	20	20	20	20	21	21	21	21	22	22	22	23	23	23	23	24
32	17	17	18	18	18	18	19	19	19	20	20	20	20	21	21	21	21	22	22	22	23	23	23	23
33	17	17	17	18	18	18	18	19	19	19	20	20	20	20	21	21	21	21	22	22	22	23	23	23
34	17	17	17	17	18	18	18	19	19	19	19	20	20	20	20	21	21	21	21	22	22	22	23	23
35	16	17	17	17	17	18	18	18	19	19	19	19	20	20	20	20	21	21	21	21	22	22	22	23
36	16	17	17	17	17	18	18	18	18	19	19	19	19	20	20	20	20	21	21	21	22	22	22	22
37	16	16	17	17	17	17	18	18	18	18	19	19	19	19	20	20	20	20	21	21	21	22	22	22
38	16	16	16	17	17	17	17	18	18	18	18	19	19	19	19	20	20	20	20	21	21	21	22	22
39	16	16	16	16	17	17	17	17	18	18	18	18	19	19	19	19	20	20	20	21	21	21	21	22
40	16	16	16	16	17	17	17	17	17	18	18	18	19	19	19	19	20	20	20	20	21	21	21	21
41	15	16	16	16	16	17	17	17	17	18	18	18	18	19	19	19	19	20	20	20	20	21	21	21
42	15	15	16	16	16	16	17	17	17	17	18	18	18	18	19	19	19	19	20	20	20	20	21	21
43	15	15	15	16	16	16	16	17	17	17	17	18	18	18	18	19	19	19	19	20	20	20	20	21
44	15	15	15	16	16	16	16	17	17	17	17	17	18	18	18	18	19	19	19	19	20	20	20	20
45	15	15	15	15	16	16	16	16	17	17	17	17	18	18	18	18	19	19	19	19	20	20	20	20
46	15	15	15	15	15	16	16	16	16	17	17	17	17	18	18	18	18	19	19	19	19	20	20	20
47	14	15	15	15	15	16	16	16	16	17	17	17	17	17	18	18	18	18	19	19	19	19	20	20
48	14	15	15	15	15	15	16	16	16	16	17	17	17	17	18	18	18	18	18	19	19	19	19	20
49	14	14	15	15	15	15	15	16	16	16	16	17	17	17	17	18	18	18	18	19	19	19	19	20
50	14	14	14	15	15	15	15	16	16	16	16	16	17	17	17	17	18	18	18	18	19	19	19	19
51	14	14	14	15	15	15	15	15	16	16	16	16	17	17	17	17	17	18	18	18	18	19	19	19
52	14	14	14	14	15	15	15	15	16	16	16	16	16	17	17	17	17	18	18	18	18	19	19	19
53	14	14	14	14	15	15	15	15	15	16	16	16	16	17	17	17	17	17	18	18	18	18	19	19
54	14	14	14	14	14	15	15	15	15	15	16	16	16	16	17	17	17	17	17	18	18	18	18	19
55	13	14	14	14	14	14	15	15	15	15	16	16	16	16	16	17	17	17	17	18	18	18	18	18
56	13	13	14	14	14	14	15	15	15	15	15	16	16	16	16	17	17	17	17	17	18	18	18	18
57	13	13	14	14	14	14	14	15	15	15	15	16	16	16	16	16	17	17	17	17	17	18	18	18
58	13	13	13	14	14	14	14	15	15	15	15	15	16	16	16	16	16	17	17	17	17	18	18	18
59	13	13	13	14	14	14	14	14	15	15	15	15	15	16	16	16	16	17	17	17	17	17	18	18
60	13	13	13	13	14	14	14	14	14	15	15	15	15	16	16	16	16	16	17	17	17	17	18	18
61	13	13	13	13	14	14	14	14	14	15	15	15	15	15	16	16	16	16	17	17	17	17	17	18
62	13	13	13	13	13	14	14	14	14	14	15	15	15	15	16	16	16	16	16	17	17	17	17	17
63	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15	16	16	16	16	16	17	17	17	17
64	12	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15	16	16	16	16	17	17	17	17
65	12	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15	16	16	16	16	16	17	17	17
66	12	12	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15	16	16	16	16	17	17	17
67	12	12	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15	16	16	16	16	16	17	17
68	12	12	12	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15	16	16	16	16	16	17
69	12	12	12	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15	16	16	16	16	16	17
70	12	12	12	12	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15	16	16	16	16	16
71	12	12	12	12	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15	16	16	16	16	16
72	12	12	12	12	13	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15	16	16	16	16
73	12	12	12	12	12	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15	16	16	16	16
74	12	12	12	12	12	13	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15	16	16	16
75	12	12	12	12	12	12	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15	16	16	16
76	11	12	12	12	12	12	13	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15	16	16
77	11	12	12	12	12	12	12	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15	15	16
78	11	11	12	12	12	12	12	13	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15	16
79	11	11	12	12	12	12	12	12	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15	15
80	11	11	12	12	12	12	12	12	13	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15
81	11	11	11	12	12	12	12	12	12	13	13	13	13	13	14	14	14	14	14	15	15	15	15	15
82	11	11	11	12	12	12	12	12	12	13	13	13	13	13	14	14	14	14	14	14	15	15	15	15
83	11	11	11	11	12	12	12	12	12	13	13	13	13	13	13	14	14	14	14	14	15	15	15	15
84	11	11	11	11	12	12	12	12	12	12	13	13	13	13	13	14	14	14	14	14	14	15	15	15
85	11	11	11	11	12	12	12	12	12	12	13	13	13	13	13	13	14	14	14	14	14	15	15	15
86	11	11	11	11	11	12	12	12	12	12	12	13	13	13	13	13	14	14	14	14	14	14	15	15
87	11	11	11	11	11	12	12	12	12	12	12	13	13	13	13	13	13	14	14	14	14	14	15	15
88	11	11	11	11	11	11	12	12	12	12	12	13	13	13	13	13	13	14	14	14	14	14	14	15
89	11	11	11	11	11	11	12	12	12	12	12	12	13	13	13	13	13	13	14	14	14	14	14	15
90	11	11	11	11	11	11	12	12	12	12	12	12	13	13	13	13	13	13	14	14	14	14	14	14
91	10	11	11	11	11	11	11	12	12	12	12	12	12	13	13	13	13	13	14	14	14	14	14	14
92	10	11	11	11	11	11	11	12	12	12	12	12	12	13	13	13	13	13	13	14	14	14	14	14
93	10	11	11	11	11	11	11	11	12	12	12	12	12	12	13	13	13	13	13	14	14	14	14	14
94	10	10	11	11	11	11	11	11	12	12	12	12	12	12	13	13	13	13	13	13	14	14	14	14
95	10	10	11	11	11	11	11	11	12	12	12	12	12	12	13	13	13	13	13	13	14	14	14	14
96	10	10	10	11	11	11	11	11	11	12	12	12	12	12	12	13	13	13	13	13	13	14	14	14
97	10	10	10	11	11	11	11	11	11	12	12	12	12	12	12	13	13	13	13	13	13	14	14	14
98	10	10	10	11	11	11	11	11	11	12	12	12	12	12	12	12	13	13	13	13	13	14	14	14
99	10	10	10	10	11	11	11	11	11	11	12	12	12	12	12	12	13	13	13	13	13	13	14	14
100	10	10	10	10	11	11	11	11	11	11	12	12	12	12	12	12	13	13	13	13	13	13	14	14