Cao and Xue *Cybersecurity (2025)8:30*
https://doi.org/10.1186/s42400-024-00316-7

Cybersecurity

RESEARCH

Open Access

Quantum commitments from structured one-way quantum state generators, and more

Shujiao Cao[1,2] and Rui Xue[1,2*]

Abstract

One-way quantum state generators (OWSGs), which serve as the quantum analog of one-way functions (OWFs), have attracted significant interest due to their potential applications and the reduced assumption requirements compared to OWFs. This paper explores the applications of structured OWSGs and presents several results: We construct efficiently samplable, statistically far but computationally indistinguishable pairs of distributions (EFI pairs) from secretly-verifiable OWSGs with somewhat injectivity, which has implications for quantum commitment schemes; We demonstrate that somewhat injective OWSGs can be derived from almost regular OWSGs; We also focus on a specific type of OWSGs, termed SV-eSI-OWSGs, and prove that the existence of a single-copy-secure hard-core predicate for these OWSGs is both necessary and sufficient for constructing EFI pairs; Moreover, we propose a simple quantum commitment scheme based on the decisional LPN assumption, offering improved parameter choices and flexibility over classical schemes. These findings contribute to the understanding and potential applications of OWSGs in quantum cryptography.

Keywords EFI pairs, Quantum commitment, One-way quantum state generators

Introduction

In classical cryptography, one-way functions stand as fundamental conceptual elements. Analogously, Morimae and Yamakawa introduced the concept of one-way quantum state generators (OWSGs) in their work (Morimae and Yamakawa 2022b), which produce a quantum state instead of a classical string as output. Informally, an OWSG takes a classical binary string $x \in \{0,1\}^n$ as input and efficiently yields a quantum state $|\phi_x\rangle$. The security guarantee entails that no quantum polynomial-time (QPT) algorithm can feasibly find any plausible preimage, even when provided with polynomial copies of $|\phi_x\rangle$. Expanding upon this framework, Morimae and Yamakawa evolved their initial definition to encompass mixed states ρ_x as potential outputs (Morimae and Yamakawa 2022a). To verify, a verification algorithm is provided to check the validity.

Numerous findings regarding OWSGs have proven to be consistent with their classical counterparts. Firstly, it is directly implied by the expansion of pseudorandom states (PRS) (i.e., the output length is larger than the input) (Ji et al. 2018). Then, Morimae and Yamakawa demonstrated the equivalence of OWSGs to bounded-time-secure quantum digital signatures with quantum public keys, as well as their implication by private-key quantum money schemes (with pure money states) and quantum pseudo one-time pad schemes (Morimae and Yamakawa 2022a). Recently, Khurana and Tomer showed the feasibility of realizing quantum commitments from pure-state OWSGs. Moreover, various studies have recognized the parallels between OWSGs variants and the spectrum of classical one-way functions, including strong and weak subclasses (Morimae and Yamakawa 2022a; Cao and Xue 2022), as initially delineated by the seminal works of Yao (1982). Additionally, a peculiar and seemingly incommensurable

*Correspondence:
Rui Xue
xuerui@iie.ac.cn
[1] Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

variation called secretly-verifiable and statistically-invertible OWSGs (SV-SI-OWSGs) was proposed by Morimae and Yamakawa (2022a), proving equivalence to the efficiently samplable, statistically far but computationally indistinguishable pairs of distributions (EFI pairs), and hence to quantum commitment.

The notion of OWSGs is indeed a fundamental conceptual object in quantum cryptography, analogous to one-way functions in classical cryptography. However, its applications and relationships with other cryptographic primitives is still an active area of research. Yet, it is undetermined whether the generalized (mixed state version) OWSGs imply the existence of quantum commitment schemes.

The role of commitment in cryptography is of utmost importance, serving as a two-phase interactive protocol that ensures both confidentiality and non-repudiation. These essential security properties are known as the hiding and binding properties, with two variations typically discussed for each, namely computational security and statistical security. Informally, computational (or statistical) hiding implies that a malicious receiver, operating within polynomial time (or unbounded time), is incapable of determining the message committed by the committer. Likewise, computational (or statistical) binding prevents a committer, operating within polynomial time (or unbounded time), from altering the committed message. In classical setting, it has been demonstrated that the existence of commitment is equivalent to the one-way functions (OWFs), as demonstrated by Goldreich (1990), Naor (1991), Håstad et al. (1999), and Haitner et al. (2009). Additionally, the MiniCrypt framework by Impagliazzo (1995) captures these primitives that are equivalent to OWFs.

With the advent of quantum computing, the power of cryptographic primitives has been enhanced, providing new opportunities to realize advanced cryptographic functionality from basic primitives. It has been shown that non-interactive quantum commitments can be constructed from quantum-secure (post-quantum) one-way functions (Koshiba and Odaira 2009, 2011; Yan et al. 2015; Bitansky and Brakerski 2021), which is impossible in the classical setting using a black-box approach. Two recent works by Grilo et al. (2021) and Bartusek et al. (2021) indicate the possibility of using quantum commitments to construct oblivious transfer (OT) and multi-party computations (MPC), which were previously considered impossible in the classical setting using a black-box approach (Impagliazzo and Rudich 1989; Gertner et al. 2000; Mahmoody et al. 2014). Subsequently, Morimae and Yamakawa (2022b) and Ananth et al. (2022) demonstrated that quantum commitments can be realized using pseudorandom quantum state generators (PRSs), which are quantum analogues of pseudorandom generators (PRGs). These results relax the requirement of the underlying assumption, as PRSs appear to be weaker than quantum-secure one-way functions (Kretschmer 2021; Brakerski et al. 2023), while in the classical setting, commitments exist if and only if OWFs exist.

Overall, OWSGs, much like their classical counterparts, serve as essential building blocks for various cryptographic primitives. It is a fundamental concept in quantum cryptography. The applications and relationships with other primitives are still being explored. The questions of constructing quantum commitment, PRS, and other cryptographic primitives from OWSGs, as well as finding practical constructions based on standard assumptions, are open research problems in this field. Studying these problems would emphasize the theoretical importance of OWSGs and demonstrate their feasibility across different quantum cryptographic functionalities, hence contributing to the advancement of the field.

Our Contributions: Building on the motivation above, this work contributes to the field of quantum cryptography by advancing the utility and theoretical understanding of OWSGs. These contributions are summarized as follows and illustrated in Figure 1:

1. *Quantum Commitments with OWSGs:* We give construction of quantum commitment schemes using structured OWSGs. By adapting the underlying structures of somewhat injective one-way primitives, including OWFs, OWSGs, and SV-OWSGs (secretly-verifiable OWSGs), we developed a simple construction of canonical quantum bit commitment. This scheme achieves statistical binding and computational hiding, demonstrating the practical feasibility of such quantum primitives.
2. *Equivalence of EFI Pairs and Hard-Core Predicates:* Our second result establishes an equivalence between EFI pairs and single-copy-secure hard-core predicates for SV-eSI-OWSGs (secretly-verifiable and extremely-statistically-invertible OWSGs). This finding not only underscores the practical usage of such cryptographic primitive but also aligns with the theoretical frameworks proposed in recent studies, such as those by Morimae and Yamakawa (2022a), confirming that SV-eSI-OWSGs are equivalent to the standard SV-SI-OWSGs.
3. *Flexible EFI Pair Construction from LPN:* Lastly, we present a novel and simple approach to constructing EFI pairs based on the decisional Learning Parity with Noise (LPN) assumption. This approach allows for a more flexible selection of parameters, enhancing the adaptability and robustness of quantum cryptographic protocols.

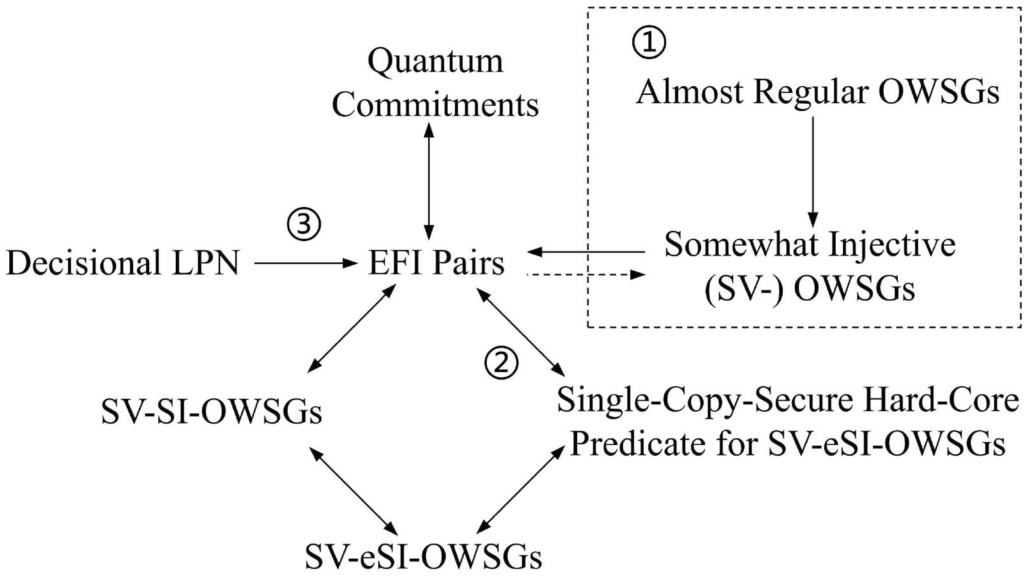

Fig. 1 We use the arrow notation to indicate implications between different primitives. Specifically, the arrow "$A \rightarrow B$" denotes that the primitive A implies the existence or achievability of primitive B. On the other hand, the dotted arrow "$A \dashrightarrow B$" signifies that A implies a special case of B (i.e. the secretly-verifiable case). The ①, ②, and ③ are the main results proved in this paper, and other directions are either implied naturally by their definitions or shown by Brakerski et al. (2023), Morimae and Yamakawa (2022a)

Overview of techniques

To further illustrate the contributions of this paper, we outline the techniques involved in our results. This discussion includes the construction of quantum commitment from somewhat injective one-wayness primitives, establishing the equivalence between a single-copy-secure hard-core predicate of `SV-eSI-OWSGs` and `EFI` pairs, and a `EFI` pairs construction from the decisional `LPN` assumption.

Quantum Commitment from Somewhat Injective One-Wayness Primitives: We begin by revisiting a well-known construction of commitment from one-way permutations, assuming $P : \{0,1\}^n \rightarrow \{0,1\}^n$ is a one-way permutation. The committer sends $(P(x), \langle x, r\rangle_2 \oplus b, r)$ as the commitment for a bit b, and (x, b) in the reveal phase. By Goldreich-Levin's theorem, it is evident that the construction satisfies computational hiding, and perfect binding follows from the injectiveness of $P(\cdot)$.

In the investigation of quantum constructions, we are proposing a relaxation of the bijection requirement. Previous work has demonstrated the equivalence between canonical quantum bit commitments (specifically those that are computationally hiding and sum-binding) and what are known as efficiently samplable, statistically far but computationally indistinguishable pairs of distributions (`EFI` pairs) of distributions (Yan 2022; Brakerski et al. 2023). For the purposes of our discussion, we will focus on constructing these `EFI` pairs due to their conceptual ease.

Informally, `EFI` pair takes as input a bit $b \in \{0,1\}$, and produces a corresponding (mixed) quantum state ρ_b. The two primary conditions for `EFI` pairs are as follows: (i) ρ_0 and ρ_1 must be computationally indistinguishable, meaning they are exceedingly difficult to distinguish using computational methods, (ii) The trace distance between ρ_0 and ρ_1 has to be substantial.

To realize `EFI` pairs from one-wayness, intuitively, since the quantum communication is allowed, we can send a superposition $\mathrm{E}_{\mathrm{x,r}}|\mathrm{P(x)}, \langle \mathrm{x}, \mathrm{r}\rangle_2 \oplus \mathrm{b}, \mathrm{r}\rangle\langle \mathrm{P(x)}, \langle \mathrm{x}, \mathrm{r}\rangle_2 \oplus \mathrm{b}, \mathrm{r}|$ as a commitment for b (i.e. the output state of the `EFI` pairs with b as input). Note that, a superposition state over the all possible input is given, to ensure farness (statistical binding), the $P(\cdot)$ does not have to be injective over the entire domain. Instead, it suffices for only a noticeable subset of the input space to be injective. If we assume a one-way function f that is injective on a fraction of $1/n^c$ of its domain, termed as somewhat injective one-way function (`OWF`), then the indistinguishability follows naturally from the inability to discern between the states ρ_b for $b = 0$ and $b = 1$. Furthermore, the farness is satisfied because the trace distance between ρ_0 and ρ_1 is significant, attributed to the noticeable portion of the injective domain that is featured for the function f. Consequently, this gives rise to a construction of `EFI` pairs from somewhat injective `OWFs`.

Theorem 1 *If there exist somewhat injective* `OWFs`*, then* `EFI` *pairs exist.*

One remaining question is how to realize somewhat injective OWFs. While injective OWFs trivially imply somewhat injective OWFs, we aim to construct the latter from the more general case of OWFs. The black-box barrier for constructing injective OWFs from OWFs does not seem to impede the construction of somewhat injective OWFs. However, extending the injective property while maintaining the one-wayness for an arbitrary one-way function f remains challenging. The core challenge is to construct somewhat injective OWFs from general OWFs without relying on the strong assumptions required for normal injectivity. This involves ensuring that the injective property can be extended without compromising the one-wayness of the function.

One intuition is to use a 2-wise independent hash function h and consider the construction $f'(x,h) := (f(x), h, h(x))$. By leveraging the properties of 2-wise independent hash functions, the injective domain can be expanded with the range of h. However, this strategy may compromise the one-wayness property. If the range of h is too large (e.g., larger than the input space of f), the preimages of $h(x)$ might be easily sampled. That limits the number of preimages for each $h(x)$.

Denoting the output size of a 2-wise independent hash (universal hash) function by an index e, namely, $h_e : \{0,1\}^n \to \{0,1\}^e$. The above discussion suggests that a small e can maintain one-wayness, while a large e can achieve injectiveness. Thus, it is crucial to choose a suitable e that balances the injectivity and the one-wayness. However, this decision depends on the size of preimages of f, leading us to consider the notion of (almost) regular one-wayness primitives instead.

Informally, a function f is (almost, resp.) regular if for any (overwhelming part of, resp.) input x, the size of preimages of $f(x)$ is close to its expected value (with at most a polynomial factor). In this case, setting the output size e to be close to $\log(n^\beta \cdot 2^n/\mathrm{Img(f)})$ for a constant β, using 2-wise independent hash functions (universal hash functions are sufficient), with probability at least $1 - n^{O(1)}$ under the randomness of (x, h_e), we deduce that the image $(f(x), h_e, h_e(x))$ has only one preimage. Furthermore, when e is close to $\log(n^\beta \cdot 2^n/\mathrm{Img(f)})$, the one-wayness holds due to the leftover hash lemma.

Lemma 1 *If almost regular* OWFs *exist, then somewhat injective* OWFs *also exist.*

Therefore, we can obtain a construction of somewhat injective OWFs (and hence the EFI pairs and quantum commitments) from almost regular OWFs. It is worth noting that although non-interactive quantum commitment is already shown to be implied by quantum OWFs (Koshiba and Odaira 2009, 2011; Yan et al. 2015; Bitansky and Brakerski 2021), we believe this aspect is still of independent interest. This is because the aforementioned constructions from quantum OWFs are either complicated or rely on PRGs, whereas our construction is simple and natural (though with additional requirements on the structure). Furthermore, our construction from almost regular OWFs to somewhat injective OWFs also applies to approximate preimage-size (APS) quantum one-way functions (Koshiba and Odaira 2009) (a function for which the number of preimages for each image can be efficiently estimated).

Next, we extend the results above to OWSGs. However, since the image in this case is a quantum state ρ_x for the generalized (mixed) version of OWSGs, we need to consider the distance between pairs of these states, unlike in the classical case where either the images are completely unrelated or they are the same. Therefore, we characterize injectiveness by considering the "small" sphere around the image state. Informally, a one-way state generator $\mathtt{f}$ that takes x as input and outputs ρ_x is somewhat injective if a significant portion of the image states are contained separately within disjoint small spheres. Specifically, there exist constants α and c such that:

$$\Pr_x[\mathbf{Pre}_{\mathtt{f},\alpha}(x) = 1] \geq \frac{1}{n^c},$$

where

$$\mathbf{Pre}_{\mathtt{f},\alpha}(x) := \left\{ x' \mid \mathrm{F}(\rho_{\mathrm{x}}, \rho_{\mathrm{x}'}) \geq 1 - \frac{1}{\mathrm{n}^\alpha} \right\}.$$

Using a similar argument as before, we can show that somewhat injective (SV−)OWSGs imply EFI pairs (quantum commitment). By the quantum Goldreich-Levin theorem for (SV−)OWSGs (Adcock and Cleve 2002; Coladangelo et al. 2021), indistinguishability is maintained because it is difficult to distinguish the hard-core predicate from a random bit. Then, farness follows from the somewhat injectivity of such (SV−)OWSGs, which ensures that two states $\rho_b = \mathrm{E}_{\mathrm{x},\mathrm{r}}\rho_{\mathrm{x}} \otimes |\mathrm{r}, \langle \mathrm{x}, \mathrm{r}\rangle_2 \oplus \mathrm{b}\rangle\langle \mathrm{r}, \langle \mathrm{x}, \mathrm{r}\rangle_2 \oplus \mathrm{b}|$ for $b = 0, 1$ are separated.

Theorem 2 *If somewhat injective* (SV−)OWSGs *exist, then* EFI *pairs exist.*

Similar to the discussion of somewhat injective OWFs, somewhat injective one-wayness in quantum primitive is trivially implied by a normally injective one. However, achieving such functionality without relying on normal injectivity is also a significant area of study. This is because the normal injective property often necessitates stronger underlying assumptions than those required for one-wayness alone. Exploring alternatives

that circumvent these requirements not only broadens the applicational scope but also enhances the theoretical understanding of one-wayness in quantum cryptographic contexts.

Motivated by the reason above, we further demonstrate that the existence of somewhat injective OWSGs is implied by a quantum analogue of (almost) regular OWFs, which we refer to as (almost) regular OWSGs. Informally, an OWSG is (almost) regular if the preimages contained in each small sphere around the image state are concentrated. Specifically, a quantum state generator $\mathtt{f}$ is (α, β)-almost regular OWSGs if the following holds for any $\alpha' > \alpha$:

$$n^{-\beta} \cdot \frac{2^n}{\mathbf{E}_\alpha(\mathtt{f})} \leq \mathbf{Pre}_{\alpha'}(x) \leq n^{\beta} \cdot \frac{2^n}{\mathbf{E}_\alpha(\mathtt{f})},$$

where

$$\mathbf{E}_\alpha(\mathtt{f}) := \min \left| \left\{ x_1, x_2 \ldots | \bigcup_{x_i} \mathbf{Pre}_{\mathtt{f},\alpha}(x_i) = \{0,1\}^n \right\} \right|.$$

Applying the same strategy as before, we consider the case where $\mathtt{f}$ takes x as input and outputs ρ_x. By defining the new OWSG as $\mathtt{f}'(h_e, x) = \rho_x \otimes |h_e, h_e(x)\rangle\langle h_e, h_e(x)|$, where $h_e : \{0,1\}^n \to \{0,1\}^e$ is an 2-wise independent hash with $e = [\log(n^{\beta'} \cdot \mathbf{E}_\alpha(\mathtt{f}))] + 1$ (where $\beta' > 0$ is an arbitrarily fixed constant), we can demonstrate that $\mathtt{f}'$ is a somewhat injective OWSG. Additionally, it should be noted that this strategy appears to be infeasible for achieving somewhat injective SV-OWSGs.Therefore, we establish the existence of somewhat injective OWSGs by leveraging the notion of almost regular OWSGs. Specifically, we present the following lemma:

Lemma 2 *If almost regular* OWSGs *exist, then somewhat injective* OWSGs *also exist.*

Consequently, in this context, we establish an implication from somewhat injective one-wayness objects (including OWFs and OWSGs) to quantum commitment, while demonstrating the feasibility of these objects based on the existence of almost regular ones. It is worth noting that PRSs and pure state OWSG already imply EFI pairs (quantum commitments). However, constructing from generalized version of OWSGs is also meaningful due to the potential requirement of fewer assumptions compared to PRSs and pure state OWSG (as PRSs and pure state OWSG trivially imply OWSGs, while the reverse direction remains challenging and unknown). Additionally, a non-trivial construction of PRSs from a standard cryptographic assumption that cannot simultaneously imply OWFs is still unknown. In contrast, constructing somewhat injective (SV-)OWSGs appears to be more achievable.

Equivalence between Single-Copy-Secure Hard-Core Predicate of SV-eSI-OWSGs and EFI Pairs: As an incomparable variant of OWSGs, Morimae and Yamakawa (2022a) introduced the notion of secretly-verifiable and statistically-invertible quantum state generators (SV-SI-OWSGs). Unlike the standard OWSGs, SV-SI-OWSGs allow outputting mixed states while abandoning the public verification algorithm. To prevent confusion caused by unverifiable output states, they emphasize the statistically-invertible property, which requires the output image states to be sufficiently far from each other (at least $1/\mathtt{poly}(n)$ distance). This property is more stringent than somewhat injectiveness. In this case, only secret verification is feasible, which involves checking whether $x' \neq x$ for two images ρ_x and $\rho_{x'}$. Morimae and Yamakawa demonstrated the equivalence between the existence of SV-SI-OWSGs and EFI pairs (and consequently, quantum commitment). Combining this result with the quanutm Goldreich-Levin theorem for OWSGs discussed earlier, the hard-core predicate for SV-SI-OWSGs is also equivalent to EFI pairs. Based on that, we observe that for a special case of SV-SI-OWSGs, the existence of single-copy-secure hard-core predicate is also essential for EFI pairs.

More specificall, we define a special class of SV-SI-OWSGs called the secretly-verifiable and extremely-statistically-invertible quantum state generators (SV-eSI-OWSGs). In SV-eSI-OWSGs, the trace distance between every pair of image states is extremely large (i.e., $\mathrm{TD}(\rho_x, \rho_{x'}) \geq 1 - \mathtt{negl}(n) \cdot /2^n$ for any distinct pair $x, x' \{0,1\}^n$). It is easy to verify that SV-eSI-OWSGs is a special case of SV-SI-OWSGs. Conversely, SV-eSI-OWSGs is also implied by SV-SI-OWSGs. That is because, if $\mathtt{f}(x) = \rho_x$ is SV-SI-OWSG, then $\mathtt{f}'(x) = \rho_x^{\otimes p(n)}$ for an arbitrary positive polynomial $p(n)$ is also an SV-SI-OWSG.

As the second result, we show that a single-copy-secure hard-core predicate for SV-eSI-OWSGs is both necessary and sufficient for EFI pairs and, consequently, quantum commitments. The large trace distance between pairs of image states implies a noticeable trace distance between $\mathrm{E}_x^{\mathrm{P}(x)=0}\rho_x$ and $\mathrm{E}_x^{\mathrm{P}(x)=1}\rho_x$, where ρ_x is the output of SV-eSI-OWSGs for an input $x \in \{0,1\}^n$, and $\mathrm{P}(\cdot)$ is the single-copy-secure hard-core predicate. The construction yields EFI pairs is as follows:

$$\mathtt{StateGen}'(1^n, b) := \mathop{\mathrm{E}}_x \rho_x \otimes |\mathrm{P}(x) \oplus b\rangle\langle \mathrm{P}(x) \oplus b|. \tag{1}$$

Conversely, the implication from EFI pairs to a single-copy-secure hard-core predicate for SV-eSI-OWSGs

follows immediately from the equivalence between SV-SI-OWSGs and EFI pairs, as well as the Goldreich-Levin theorem for SV-SI-OWSGs. Therefore, we can conclude the second result with the following theorem:

Theorem 3 EFI *pairs exist if and only if a single-copy-secure hard-core predicate for* SV-eSI-OWSGs *exists.*

EFI Pairs from LPN Assumption with Flexible Parameter Choice: The learning parity with noise (LPN) assumption (search version) describes the computational infeasibility of finding the random preimage $x \in \{0,1\}^n$ for a given pair $(A, Ax \oplus e)$, where A is a random binary matrix with dimensions $m \times n$, and e is a noise vector sampled from the Bernoulli distribution B_τ^m with $0 < \tau < 1/2$ (i.e., each entry of e equals 1 with probability τ). The decisional version of LPN characterizes the computational infeasibility of distinguishing an LPN sample $(A, Ax \oplus e)$ from a pair (A, r), where r is a random vector in $\mathbb{Z}_2^m$. Here n is the security parameter and τ called the noise rate. It has been proven that the decisional version and the search version of LPN are polynomially equivalent (Blum et al. 1993; Applebaum et al. 2009; Katz et al. 2010).

The LPN assumption has been extensively studied in various fields such as learning theory and coding theory, where it serves as the average-case analogue of decoding random linear codes. The average-case hardness of LPN is guaranteed by the worst-case hardness of the nearest codeword problem with a low noise rate (Brakerski et al. 2019; Yu and Zhang 2021). As the application to cryptography, the LPN assumption with varying noise rates implies the security of various cryptographic primitives, including one-way functions (OWFs), pseudorandom generators (PRGs), commitment schemes, symmetric (public) encryption, and collision-resistant hash functions (Pietrzak 2012; Jain et al. 2012; Gilbert et al. 2008; Applebaum et al. 2009; Alekhnovich 2003; Döttling et al. 2012; Kiltz et al. 2014; Yu et al. 2019).

It is worth noting that a direct construction of a commitment scheme can be obtained from the decisional (and exact) version of the LPN assumption introduced by Pietrzak (2012) and Jain et al. (2012). The commitment for a message m is defined as $com(m) := A \cdot (r \| m) \oplus e$. Intuitively, when m is sufficiently large (e.g., $m = O(n)$), the image $A \cdot (r \| m) \oplus e$ uniquely determines m with overwhelming probability for a suitable constant noise rate τ (i.e., $\tau < 0.25$), which guarantees the binding property. The computational hiding property holds due to the decisional (and exact) version of the LPN assumption. By the nature of LPN, it should be noted that a restricted number of samples m and a larger noise rate τ provide "stronger" security than treating m as an arbitrary polynomial of n and a constant τ. From an experimental perspective, increasing the number of samples and reducing the noise rate significantly enhances the power for solving the LPN problem (Blum et al. 2000; Lyubashevsky 2005; May et al. 2011), while from a theoretical perspective, the analysis of the learning with error (LWE) assumption (which is highly related to LPN) suggests that a small number of samples offers more flexibility in choosing other parameters (Micciancio and Peikert 2013). To ensure security of cryptographic primitives based on LPN assumptions, it is essential to carefully choose flexible parameters. However, it should be noted that for the classical commitment scheme discussed earlier, choosing such parameters may lead to a loss of the binding property, as an unbounded adversary could potentially find a collision for $A \cdot (r \| m) \oplus e$.

Based on a non-trivial decisional LPN assumption, we can ensure the existence of EFI pairs (and thus the quantum commitment) as the third result. By employing Grover and Rudolph's technique (Grover and Rudolph 2002), a QPT algorithm can produce the superposition $\mathrm{E}_{\mathrm{e}}|\mathrm{e}\rangle\langle\mathrm{e}|$ where $e \leftarrow B_\tau^m$. This directly leads to the construction of EFI pairs as $\mathtt{StateGen}(1^n, 0) = \mathrm{E}_A |A\rangle\langle A| \otimes \left(\mathrm{E}_{x,e} |Ax \oplus e\rangle\langle Ax \oplus e|\right)$, and $\mathtt{StateGen}(1^n, 1) = \mathrm{E}_A |A\rangle\langle A| \otimes (\mathrm{E}_r |r\rangle\langle r|)$. Hence, it is obvious that the indistinguishability directly follows the hardness of the decisional LPN. As for the farness, it is observed that the trace distance between these two states is limited by the statistical distance between the distribution of LPN samples and a random one, which is noticeable as long as the decisional LPN assumption is non-trivial.

Theorem 4 (Informal) *Assuming the non-trivial decisional version* LPN *is hard on average in the quantum case, then* EFI *pairs exist.*

It is worth noting that for any constant noise rate $0 < \tau < 0.5$, $m = O(n)$ is already adequate for the EFI pairs. Additionally, it is believed that for $\tau = (1 - n^C)/2$, a polynomial $m = O(n^{C'})$ is sufficient, where C' is dependent on C, which allows for a superior parameter choice compared to previous works by Pietrzak (2012) and Jain et al. (2012). Furthermore, the construction is akin to the PRG from LPN but does not necessitate the length-increasing property, providing the flexibility for parameter selection.

Related works

The concepts of pseudorandom state generators (PRSs) and pseudorandom unitary (PRU) were introduced by Ji et al. (2018) as the quantum counterparts

of pseudorandom generators and pseudorandom functions, respectively. They demonstrated the implication from quantum OWFs to PRSs and gave a quantum money scheme from PRSs. Then, Brakerski and Shmueli (2019) extended the original proof to the random binary phase setting and developed a scalable construction of pseudorandom quantum states in their subsequent work (Brakerski and Shmueli 2020). Additionally, Kretschmer (2021) provided a quantum oracle $\mathcal{O}$ relative to $\mathsf{QMA}^{\mathcal{O}} = \mathsf{BQP}^{\mathcal{O}}$, demonstrating the existence of PRS (and even PRU), which offers negative evidence for reducing OWF from PRS.

Parallelly, Morimae and Yamakawa (2022b) and Ananth et al. (2022) independently presented constructions of quantum commitments from PRSs, arising the possibility of constructing quantum oblivious transfer and multiparty computation. Subsequently, Brakerski, Canetti, and Qian formalized the concept of EFI pairs, which was implicitly described by Yan (2022), and demonstrated its equivalence to the canonical quantum bit commitment. They also showed that EFI pairs are implied by various quantum cryptographic objects, such as quantum oblivious transfer, general secure multiparty computation, and non-triviality of QCZK (Brakerski et al. 2023). To complement Kretschmer's findings, Kretschmer et al. (2022) further constructed a classical oracle relative to which $\mathsf{P} = \mathsf{NP}$, while a single-copy secure pseudorandom quantum state generator still exists.

As a quantum analogue of OWFs, Morimae and Yamakawa (2022b) defined the concept of OWSGs and provided a construction of a one-time secure signature from it. They then introduced the generalized definition of OWSGs, allowing the output state to be a mixed state and providing an additional verification algorithm for checking the validity in their subsequent work (Morimae and Yamakawa 2022a). They demonstrated the equivalence between OWSGs and weak OWSG using the amplification theorem for weakly verifiable puzzles, and also established the equivalence between OWSG and (bounded-time-secure) quantum digital signatures with quantum public keys, as well as the implication of OWSG from private-key quantum money schemes (with pure money states) and quantum pseudo one-time pad schemes. Additionally, they introduced an incomparable variant of OWSG known as the secretly-verifiable and statistically-invertible quantum state generators (SV-SI-OWSGs), and demonstrated the equivalence between SV-SI-OWSGs and EFI pairs.

Very recently, Khurana and Tomer (2023) showed the feasibility for realizing quantum commitments (and hence EFI pairs, SV-SI-OWSG) from pure state OWSGs. Besides, as an intermediate primitive, they introduced the notion of (quantum) one-way puzzle which seems to be necessary for plenty of quantum cryptographic objects. We remark that their work does not overlap with ours, because we focus on the structured OWSG which also includes the generalized (i.e., the mixed state, and the secretly-verifiable) setting.

Organization of the paper

Basic notions and formal definitions are given in Section . Then in the following sections, the EFI pairs (quantum commitment) are studied from three different perspectives. In Section , we present the construction of quantum commitments using OWSGs. Section establishes the equivalence of EFI pairs and hard-core predicates. Finally, a practical construction of EFI pairs is given in Section from the LPN assumption.

Preliminaries

In this section, we will introduce several notations and cryptographic notions that are useful in the following context. We begin by providing some basic notations.

Notations

We use the following basic notations throughout the paper: $\mathbb{Z}$ and $\mathbb{N}$ denote the sets of positive integers and positive integers, respectively. $[n]$ represents the set of integers $1, 2, \ldots, n$. The bit length of a string x is denoted as $|x|$, and the size of a set $\mathbf{X}$ is denoted as $|\mathbf{X}|$ as well. The mathematical expectation of a random variable X is denoted as E[X]. A function $\mathtt{negl}(\cdot)$ is considered negligible if, for any $c > 0$, $\mathtt{negl}(n) < 1/n^c$ for all sufficiently large n. The injective domain of a function f is denoted as $\mathbf{Inj}(f)$. Furthermore, we define additional notations related to quantum cryptography:

$\mathbb{S}(N)$ denotes the set of N-dimensional pure quantum states, $\mathbb{U}(N)$ represents the group of $N \times N$ unitary operators, and $\mathbb{S}_n$ (resp., $\mathbb{U}_n$) is $\mathbb{S}(2^n)$ (resp., $\mathbb{U}_n$). For a unitary operator $U \in \mathbb{U}(N)$, $U^\dagger$ denotes its adjoint, and $I_n \in \mathbb{U}(2^n)$ denotes the identity map. $\mathrm{Tr}(\rho)$ denotes the trace of a quantum state ρ, and $\mathrm{Tr}_A(\rho)$ represents the partial trace over subsystem A. For two mixed quantum states ρ_0 and ρ_1, $\mathrm{TD}(\rho_0, \rho_1) := \mathrm{Tr}\sqrt{(\rho_0 - \rho_1)^\dagger(\rho_0 - \rho_1)}/2$ and $\mathrm{F}(\rho_0, \rho_1) := \mathrm{Tr}\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ denote the trace distance and fidelity between these two states, respectively.

Quantum cryptographic primitives

Before delving into the specific definitions, we assume that the reader is already familiar with the fundamentals of quantum computing and basic cryptographic notions. We begin by introducing the definition of canonical quantum bit commitments as defined by Yan (2022):

Definition 1 *(Canonical Quantum Bit Commitment)* A canonical quantum bit commitment scheme is an

ensemble of polynomial-time uniform families of quantum circuits $(Q_{0,n}, Q_{0,n})$ that operate on two registers: A (the commitment register) and B (the reveal register). In the commit phase, the committer selects a bit $b \in \{0,1\}$ and applies the circuit $Q_{b,n}$ to the state $|0\rangle_{AB}$, sending the register A to the receiver. In the reveal phase, the committer sends the register B and the bit b to the receiver. The receiver applies the inverse circuit $Q_{b,n}^{\dagger}$ on registers A and B, and accepts if the measurement outcome is 0. The security of a quantum bit commitment scheme is characterized by its hiding and binding properties.

- *Computational (Statistical) Hiding:* For any QPT (resp., unbounded) malicious receiver, it is infeasible to distinguish between $\mathrm{Tr_B}(\mathrm{Q_{0,n}}|0\rangle)$ and $\mathrm{Tr_B}(\mathrm{Q_{1,n}}|0\rangle)$.
- *Statistical (Computational) Honest Binding:* For any state $|\phi\rangle_C$ stored in register C and any unitary U_{BC} acting on registers B and C that can be generated by an unbounded-time (resp., polynomial-time) algorithm, the following holds:

$$\begin{aligned}\Big|\Big[\big(Q_{1,n}|0\rangle\langle 0|Q_{1,n}^{+}\big)\otimes I_C\Big]\cdot(I_A\otimes U_{BC})\\ \cdot\big(Q_{0,n}|0\rangle_{AB}\langle\phi|_C\big)\Big| \le negl(n).\end{aligned} \tag{2}$$

Yan (2022) shows that honest binding is equivalent to the concept of sum-binding. This type of commitment is already sufficient for oblivious transfers and multi-party computation (Morimae and Yamakawa 2022b). Hence, unless specified otherwise, we refer to this canonical quantum bit commitment scheme in this paper. Additionally, we note that the flavor conversion for quantum bit commitments has been proven feasible. This means that computational hiding and statistical (honest) binding can be converted to computational (honest) binding and statistical hiding, and vice versa (Yan 2022; Hhan et al. 2023).

Next, we introduce the definition of efficiently samplable, statistically far but computationally indistinguishable pairs of distributions (EFI pairs), which was first described by Yan (2022) and later formalized by Brakerski et al. (2023).

Definition 2 *(EFI Pairs)* The efficiently samplable, statistically far but computationally indistinguishable pairs of distributions (EFI pairs) consist of a QPT sampler $\mathtt{StateGen}(1^n, b)$ that takes a parameter 1^n and a bit $b \in \{0,1\}$ as input and outputs a quantum state ρ_b. These pairs satisfy the following properties:

- *Distinguishability:* For any QPT $\mathcal{D}$, it is computationally infeasible to distinguish between ρ_0 and ρ_1, meaning:

$$\left|\Pr\left[\mathcal{D}(1^n,\rho_0)\right]-\Pr\left[\mathcal{D}(1^n,\rho_1)\right]\right| \le \mathtt{negl}(n) \tag{3}$$

  for some negligible function $\mathtt{negl}(\cdot)$. Sometimes we omit the security parameter 1^n when it's clear from the context.
- *Farness:* The trace distance between these two states satisfies:

$$\mathrm{TD}(\rho_0,\rho_1) \ge \frac{1}{\mathtt{poly(n)}} \tag{4}$$

  for some positive polynomial $\mathtt{poly}(\cdot)$ when n is sufficiently large.

The equivalence between EFI pairs and quantum commitments has been established in Yan (2022), Brakerski et al. (2023), as shown in Lemma 3.

Lemma 3 EFI *pairs exist if and only if quantum commitment exists.*

This lemma implies that achieving quantum commitments is contingent upon constructing EFI pairs. Due to the more explicit form of EFI pairs, they are often preferred in subsequent discussions over the construction of quantum commitments.

The concept of one-way quantum state generators (OWSGs) was originally introduced by Morimae and Yamakawa (2022b), and subsequently generalized in Morimae and Yamakawa (2022a) to allow for mixed state outputs. We now recall the definition of the mixed state version of OWSGs:

Definition 3 *(One-Way State Generator)* One-way state generator (OWSG) is defined as a triple of QPT algorithms, denoted by $\mathtt{f} = (\mathtt{KeyGen}, \mathtt{StateGen}, \mathtt{Ver})$, where:

- $\mathtt{KeyGen}(1^n)$: The key generation algorithm takes the security parameter 1^n as input and outputs $x \leftarrow \mathtt{KeyGen}(1^n)$.
- $\mathtt{StateGen}(x)$: The state generation algorithm takes x as input and outputs a (mixed) state ρ_x indexed by x.
- $\mathtt{Ver}(x', \rho_x)$: The verification algorithm checks the validity of the pair (x', ρ_x), and outputs 1 if it is valid and 0 otherwise.

The function $\mathtt{f}$ must satisfy the following conditions:

- *Correctness*: There exists a negligible function $\mathtt{negl}(\cdot)$ such that

$$\Pr\big[\mathtt{Ver}(\mathrm{x},\rho_{\mathrm{x}})=1:\mathtt{KeyGen}(1^{\mathrm{n}})\to \mathrm{x},\ \mathtt{StateGen}(x)\to\rho_x\big]\geq 1-\mathtt{negl}(n).$$

- *One-Wayness*: For any QPT adversary $\mathcal{A}$ and polynomial $t(\cdot)$,

$$\Pr\left[Ver(x',\rho_x)=1:\mathcal{A}\left(\rho_x^{\otimes t(n)}\right)\to x', KeyGen(1^n)\to x, StateGen(x)\to\rho_x\right]\leq negl(n) \tag{5}$$

for some negligible function $\mathtt{negl}(\cdot)$. We denote the experiment in inequality (5) as $\mathtt{Exp}^{owsg}_{\mathtt{f},\mathcal{A}}$ for simplicity.

When we refer to pure state version of $\mathtt{OWSGs}$, where $\mathtt{StateGen}(x)$ always outputs a pure state $|\phi_x\rangle$. In this case, $\mathtt{Ver}(x',|\phi_x\rangle)$ can be replaced by measuring $|\phi_x\rangle$ with the basis $\{|\phi_{x'}\rangle\langle\phi_{x'}|, I-|\phi_{x'}\rangle\langle\phi_{x'}|\}$, and output 1 if and only if the measurement result is $|\phi_{x'}\rangle$.

Next, we introduce a more generalized version of $\mathtt{OWSGs}$ called secretly-verifiable quantum state generators ($\mathtt{SV\text{-}OWSGs}$), which was proposed by Morimae and Yamakawa (2022a).

Definition 4 *(*$\mathtt{SV\text{-}OWSGs}$*)* The secretly-verifiable $\mathtt{OWSG}$ ($\mathtt{SV\text{-}OWSG}$) consists of a pair of QPT algorithms $\mathtt{f}=(\mathtt{KeyGen},\mathtt{StateGen})$ such that:

$\mathtt{KeyGen}(1^n)$: The key generation algorithm takes the security parameter 1^n as input and outputs $x\leftarrow\mathtt{KeyGen}(1^n)$.

$\mathtt{StateGen}(x)$: The state generation algorithm takes x as input and outputs a (mixed) state ρ_x indexed by x.

The function $\mathtt{f}$ should satisfy the following condition:

- *One-Wayness*: For any QPT adversary $\mathcal{A}$ and polynomial $t(\cdot)$, there exists a negligible function $\mathtt{negl}(\cdot)$ such that

$$\Pr\left[\mathrm{x}'=\mathrm{x}:\mathcal{A}(\rho_{\mathrm{x}}^{\otimes \mathrm{t(n)}})\to \mathrm{x}', \mathtt{KeyGen}(1^{\mathrm{n}})\to \mathrm{x}, \mathtt{StateGen}(\mathrm{x})\to\rho_{\mathrm{x}}\right]\geq \mathtt{negl}(\mathrm{n}). \tag{6}$$

For simplicity, we denote by $\mathtt{Exp}^{sv-owsg}_{\mathtt{f},\mathcal{A}}$ the experiment in inequality (6).

Additionally, when $\mathtt{KeyGen}$ is clear from the context, we write $\mathtt{f}(x)=\mathtt{StateGen}(x)=\rho_x$ for convenience.

It is worth noting that $\mathtt{SV\text{-}OWSGs}$ exist unconditionally (although they are hard to use in that case). Therefore, additional structural requirements are usually considered for $\mathtt{SV\text{-}OWSGs}$, such as statistical invertibility (i.e., $\mathtt{SV\text{-}SI\text{-}OWSGs}$) defined by Morimae and Yamakawa (2022a) and the somewhat injectiveness discussed in this paper. For example, $\mathtt{f}=(\mathtt{KeyGen},\mathtt{StateGen})$ is δ-statistically-invertible if it meets the following condition

- *δ-Statistical Invertibility*: $\mathtt{f}$ satisfies the δ-statistical invertibility if

$$\mathrm{TD}(\rho_{\mathrm{x}},\rho_{\mathrm{x}'})\geq\delta$$

holds for any $x\neq x'$ in the support of $\mathtt{KeyGen}(1^n)$.

In particular, if $\mathtt{f}$ is $\mathtt{SV\text{-}SI\text{-}OWSG}$ if $\delta=\mathtt{poly}(n)^{-1}$ (Morimae and Yamakawa 2022a). Besides, it satisfies the property of *extremely statistical invertibility* if its output states are *extremely separated* i.e.

$$\mathrm{TD}(\rho_{\mathrm{x}},\rho_{\mathrm{x}'})\geq 1-2^{-\mathrm{n}}\cdot\mathtt{negl}(\mathrm{n}),$$

for all sufficiently large $n\in\mathbb{N}$, we refer to such $\mathtt{SV\text{-}SI\text{-}OWSGs}$ as the *secretly-verifiable and extremely-statistically-invertible quantum state generators* ($\mathtt{SV\text{-}eSI\text{-}OWSGs}$). It is worth noting that, as discussed by Morimae and Yamakawa (2022a), although $\mathtt{SV\text{-}eSI\text{-}OWSGs}$ seems to be a stronger notion than $\mathtt{SV\text{-}SI\text{-}OWSGs}$, these two notions are equivalent in the sense of existence.

In the standard definition of $\mathtt{OWSG}$ ($\mathtt{SV\text{-}SI\text{-}OWSG}$), the adversary is given arbitrary polynomial copies of the challenge state. As a weaker version, we call it meets the *k-copy-security* if only k copies are given in the experiment. We stress that the number of copies might be crucial to its security (Cavalar et al. 2023).

EFI pairs from somewhat injective one-way primitives

In this section, we explore the construction of quantum commitments using one-way quantum state generators but with some compromises on their structure. Since there is an equivalence between EFI pairs and canonical quantum bit commitments, we focus on EFI pairs instead. We begin by discussing the construction of EFI pairs from somewhat injective one-way functions (OWFs).

Warming up with somewhat injective OWFs

In this part, we start by warming up with OWFs. We first present a construction of EFI pairs from somewhat injective OWFs, and then show that somewhat injective OWFs are implied by almost regular OWFs. To begin, we introduce the definition of somewhat injective OWFs, which are one-way functions that preserve injectiveness on a noticeable portion of their domain.

Definition 5 *(Somewhat Injective OWFs)* An ensemble of one-way functions[1] $\{f_n : \{0,1\}^n \to \{0,1\}^{l(n)}\}_n$ is somewhat injective if there exists a constant $c > 0$ such that

$$\Pr_x\left[\left|f_n^{-1}(f_n(x))\right| = 1\right] \geq \frac{1}{n^c}, \tag{7}$$

for any $n \in \mathbb{N}$. For simplicity, we use f when the parameter n is clear from the context.

Since the canonical quantum bit commitments exist if and only if EFI pairs exist, we aim to construct EFI pairs from somewhat injective OWFs instead. Let $f : \{0,1\}^n \to \{0,1\}^{l(n)}$ be a somewhat injective OWF such that

$$\Pr_x\left[\left|f^{-1}(f(x))\right| = 1\right] \geq \frac{1}{n^c}, \tag{8}$$

for a constant $c > 0$. We can construct a candidate of EFI pairs follows.

Construction of EFI Pairs: The generator algorithm $\mathtt{StateGen}(1^n, b)$ for the EFI pairs is constructed as follows:

- For an input bit $b \in \{0,1\}$, the algorithm generates the state (assuming x follows the uniform distribution):

$$|\psi_b\rangle_{AB} := \sum_{x,r\in\{0,1\}^n} \frac{|b,x,r\rangle_A \otimes |f(x),\langle r,x\rangle_2 \oplus b,r\rangle_B}{2^n},$$

where $\langle r,x\rangle_2 := \mathbf{r}\cdot\mathbf{x} \mod 2$. Register A stores the first part of the state (which contains $|b,x,r\rangle$), and register B stores the rest of the state. The algorithm then outputs the state:

$$\mathtt{StateGen}(1^n, b) := \rho_b = \operatorname*{Tr}_A |\psi_b\rangle\langle\psi_b|. \tag{9}$$

Theorem 5 *If somewhat injective OWFs exist in the quantum case, then the construction in (9) is EFI pairs.*

Proof To justify the correctness of that theorem, it is sufficient to show the distinguishability and the farness respectively.

Distinguishability: The security of the construction (9) can be proven using the following lemma that can be regarded as the Goldreich-Levin Theorem.

We aim to show the distinguishability by making a contradiction. Suppose there exists an adversary $\mathcal{A}$ that can distinguish between the two states with non-negligible probability $\varepsilon(n)$, i.e.,

$$\left|\Pr_{\rho_0\leftarrow\mathtt{StateGen}(1^n,0)}[\mathcal{A}(\rho_0)\to 0] - \Pr_{\rho_1\leftarrow\mathtt{StateGen}(1^n,0)}[\mathcal{A}(\rho_1)\to 0]\right| \geq \varepsilon(n). \tag{10}$$

Let $P_0^{x,r,b}$ denote the probability that $\mathcal{A}$ outputs 0 as a decision given some specific $|f(x),\langle r,x\rangle_2 \oplus b,r\rangle$ as the input state. The linearity of $\mathcal{A}$ implies that the inequality (10) can be expressed as:

$$\left|\mathop{\mathrm{E}}_{x,r}\left[P_0^{x,r,0}\right] - \mathop{\mathrm{E}}_{x,r}\left[P_0^{x,r,1}\right]\right| \geq \varepsilon(n). \tag{11}$$

Since f preserves the one-wayness, by the Goldreich-Levin Theorem, we have

$$\left|\Pr_{x,r}[\mathcal{D}(f(x),r,\langle x,r\rangle_2) = 1] - \Pr_{x,r}[\mathcal{D}(f(x),r,\langle x,r\rangle_2 \oplus 1) = 1]\right| \leq \mathtt{negl}(n). \tag{12}$$

However, by (11), we construct a QPT distinguisher $\mathcal{D}$ that contradicts to (12) as follows:

- $\mathcal{D}$ takes as input $(f(x^*), b^*, r^*)$ for some random $x^*, r^* \leftarrow \{0,1\}^n$, its task is to determine whether $b^* = \langle x, r^*\rangle_2$.
- $\mathcal{D}$ invokes $\mathcal{A}$ with input state $|f(x^*),\langle r^*, b^*, r^*\rangle$.
- $\mathcal{D}$ would output $\mathcal{A}$'s result as its decision.

By the definition of $P_0^{x,r,b}$, if $b^* = \langle x^*, r^*\rangle_2$, then the probability of $\mathcal{D}$ outputting 0 is expressed as

[1] We assume the reader is familiar with the definition of one-way functions.

$$\Pr_{x^*,r^*}[\mathcal{D}(f(x^*),\langle x^*,r^*\rangle_2,r^*)=0]=\mathop{\mathrm{E}}_{r,x}P_0^{x,r,0}.$$

On the other hand, if $b^*=\langle x^*,r^*\rangle_2\oplus 1$, the corresponding probability becomes

$$\Pr_{x^*,r^*}[\mathcal{D}(f(x^*),\langle x,r^*\rangle_2\oplus 1,r^*)=0]=\mathop{\mathrm{E}}_{r,x}P_0^{x,r,1}.$$

Taking inequality (11) into account, the success probability of $\mathcal{D}$ is at least $\varepsilon(n)$, leading to a contradiction to (12).

Farness: We begin by considering the trace distance between these two states, which is noticeable. In accordance with the definition of the trace distance, we have

$$\mathrm{TD}(\rho_0,\rho_1)=\max_P \mathrm{Tr}\Big(\mathrm{P}(\rho_0-\rho_1)\Big)$$

Let P_b denote the projection generated by the basis

$$\big\{\lfloor f(x),\langle r,x\rangle_2\oplus b,r\rangle \mid r\in\{0,1\}^n,x\in\mathbf{Inj}(f)\big\},$$

where $\mathbf{Inj}(f)$ represents the injective domain of f.

Since f is injective on $\mathbf{Inj}(f)$, it is evident that

$$\big|\langle f(x),\langle r,x\rangle_2\oplus b,r|f(x'),\langle r',x\rangle_2\oplus b\oplus 1,r'\rangle\big|=0$$

for any $x\in\mathbf{Inj}(f)$, implying $P_0\cdot P_1=0$.

Given that $\mathrm{Pr_x[x}\in\mathbf{Inj}(\mathrm{f})]\geq \mathrm{n}^{-\mathrm{c}}$ and $\mathrm{Tr}(\mathrm{P}_0\rho_1)=0$, we can conclude

$$\begin{aligned}\mathrm{TD}(\rho_0,\rho_1)&\geq \mathrm{Tr}\Big(\mathrm{P}_0(\rho_0-\rho_1)\Big)\\&=\mathrm{Tr}(\mathrm{P}_0\rho_0)-\mathrm{Tr}(\mathrm{P}_0\rho_1)=\mathrm{n}^{-\mathrm{c}}\end{aligned}$$

This completes the proof. □

By establishing the equivalence between quantum commitments and EFI pairs, we can deduce the implication from somewhat injective OWFs to quantum commitments.

Corollary 1 *Assuming the existence of somewhat injective* OWFs *in quantum case, then the canonical quantum bit commitments exist.*

Next, we demonstrate that the existence of somewhat injective OWFs is implied by almost regular OWFs. We adopt the definition of almost regular OWFs by Mazor and Zhang (2021).

Definition 6 *(Almost Regular* OWFs*)* An ensemble of one-way functions $\{f_n:\{0,1\}^n\to\{0,1\}^{l(n)}\}_n$ is said to be β-almost regular for $\beta>0$ if the following conditions are satisfied:

$$n^{\beta}\cdot 2^n/\mathrm{Img(f_n)}\geq\Big|\mathrm{f_n^{-1}(f_n(x))}\Big|\geq \mathrm{n}^{-\beta}\cdot 2^{\mathrm{n}}/\mathrm{Img(f_n)},$$

for any $n\in\mathbb{N}$. Here, $\mathrm{Img(f_n)}$ represents the image space defined as $\{f_n(x)\mid x\in\{0,1\}^n\}$. For simplicity, we use f when the parameter n is clear from the context.

In this definition, we assume that Img(f) can be computed efficiently and is known to the user. We will now show that the existence of almost regular OWFs implies the existence of somewhat injective OWFs.

Lemma 4 *If $f:\{0,1\}^n\to\{0,1\}^{l(n)}$ is a β-almost regular* OWF *in the quantum case, then the function*

$$f'(h_e,x)=\big(h_e,h_e(x),f(x)\big)\tag{13}$$

is somewhat injective OWF*. Here, $h_e:\{0,1\}^n\to\{0,1\}^e$ denotes a 2-wise independent hash function, and $e:=\lceil\log(n^{\beta}\cdot 2^n/\mathrm{Img(f)})\rceil+1$.*

Proof The proof makes heavy use of the leftover hash lemma which is introduced as follows:

Lemma 5 (Leftover Hash Lemma) *Let $h_e:\{0,1\}^n\to\{0,1\}^e$ be a universal hash function, where $n>e$. Then, for every $\varepsilon>0$ and every distribution X on $\{0,1\}^n$ of min-entropy at least $e+2\log(1/\varepsilon)$, the random variable $(h_e,h_e(X))$ is ε-close to the uniform distribution (h_e,U_e).*

We prove Lemma 4 by making a contradiction. Let $\mathcal{A}$ be a QPT adversary breaking the one-wayness of f' with non-negligible advantage $\delta(n)$. We denote by $h_e(x)|_{e'}$ be the first e' bits of $h_e(x)$. Since the min-entropy of X conditioned on $f(X)$ is at least $\lfloor\log(n^{-\beta}\cdot 2^n/\mathrm{Img(f)})\rfloor$, then by Leftover Hash Lemma 5, the distribution of $(h_e,h_e(x)|_{e'},f(x))$ is $\delta(n)/2$-close to $(h_e,r_{e'},f(x))$ when $e'=e-2\beta\log n-2\log(2/\delta(n))-1$, where $x\leftarrow\{0,1\}^n,r_{e'}\leftarrow\{0,1\}^{e'}$ are chosen uniformly at random. Next, since there are $2\beta\log n+2\log(2/\delta(n))+1$ remaining bits in $h_e(x)$ which is not close to random string, we can guess it correctly with probability at least $n^{-2\beta}\cdot\delta(n)/2$, that implies a QPT adversary $\mathcal{B}$ for breaking the one-wayness of f with advantage $n^{-2\beta}\cdot\delta(n)^2/4$ as follows:

- $\mathcal{B}$ takes as input $f(x^*)$ as its challenge.
- $\mathcal{B}$ generates a universal hash function $h_e:\{0,1\}^n\to\{0,1\}^e$.

- $\mathcal{B}$ runs $\mathcal{A}$ with $(h_e, f(x^*), r)$ for a random chosen $r \leftarrow \{0,1\}^e$ and outputs $\mathcal{A}$'s result.

Due to the $\delta/2$-closeness, $\mathcal{A}$ wins with probability at least $\delta/2$ if we replace the first e' bits of $h_e(x^*)$ by a random string $r_{e'} \leftarrow \{0,1\}^{e'}$. Next, for a random chosen $r_{e-e'} \leftarrow \{0,1\}^{e-e'}$, it is equal to the last $e - e'$ of $h_e(x^*)$ with probability $2^{e'-e} = n^{-2\beta} \cdot \delta(n)/2$. Since this event is independent to others, we can conclude that $\mathcal{B}$ wins with probability at least $(\delta/2) \cdot n^{-2\beta} \cdot \delta(n)/2 = n^{-2\beta} \cdot \delta(n)^2/4$. That justifies the one-wayness.

Next, we will focus on the injectiveness part. For any $x' \in \{0,1\}^n$, since h_e is 2-wise independent hash function and f is a β-almost regular OWF, the expected value of collisions is given by

$$\mathop{\mathrm{E}}_{h_e}\left|f'^{-1}(f'(h_e,x')) \setminus (h_e,x')\right| \leq n^{\beta} \cdot 2^n/(\mathrm{Img(f)} \cdot 2^{\mathrm{e}}).$$

Since $e = [\log(n^{\beta} \cdot 2^n/\mathrm{Img(f)})]$, by Markov's inequality, we have

$$\Pr_{he}\left[\left|f'^{-1}(f'(h_e,x')) \setminus (h_e,x')\right| \geq 1\right] \leq n^{\beta} \cdot 2^n/(\mathrm{Img(f)} \cdot 2^{\mathrm{e}}) = \frac{1}{2}.$$

This means for arbitrary x, $f'(h_e, x)$ has only one preimage with probability at least 1/2, which completes the proof of Lemma 4. □

We observe that the construction from almost regular OWFs to somewhat injective OWFs can be extended to a broader class of functions. Specifically, it is applicable to those OWFs for which the number of preimages can be efficiently estimated based on their image. This property is captured by the notion of approximate preimage-size (APS) quantum one-way functions (Koshiba and Odaira 2009). In particular, a function f is considered an approximate preimage-size quantum one-way function if it is one-way against any QPT adversary, and the quantity $d_y := \lceil \log |f^{-1}(y)| \rceil$ can be efficiently computed for any given image y. By employing a similar argument, we can observe that the function $f'(h_{d_{f(x)}}, x) = \left(h_{d_{f(x)}}, h_{d_{f(x)}}(x), f(x)\right)$ also preserves both the one-wayness and the somewhat injectiveness properties.

Furthermore, we note that Koshiba and Odaira (2009) presented a construction of statistically-hiding quantum bit commitment from the combination of APS quantum one-way functions and almost regular quantum one-way functions. This construction can be seen as implying the existence of statistically-binding quantum bit commitments using the flavor conversion technique introduced by Yan (2022) and Hhan et al. (2023). However, our construction offers a more direct approach and can be extended to the setting of OWSGs.

EFI Pairs from somewhat injective OWSGs

In this section, we aim to extend the aforementioned result to the OWSGs. We begin by providing a formal definition of somewhat injective OWSGs.

Definition 7 *(Somewhat Injective OWSGs)* A quantum state generator f that takes x as input and outputs ρ_x is said to be somewhat injective if there exist constants c and α such that

$$\Pr_x\left[\mathbf{Pre}_{\mathrm{f},\alpha}(x) = 1\right] \geq \frac{1}{n^c}, \tag{14}$$

where

$$\mathbf{Pre}_{\mathrm{f},\alpha}(x) := \left\{x' \mid \mathrm{F}(\rho_{\mathrm{x}}, \rho_{\mathrm{x}'}) \geq 1 - \frac{1}{\mathrm{n}^{\alpha}}\right\}. \tag{15}$$

Based on the similarity between OWSGs and SV-OWSGs, we can extend the concept of somewhat injectiveness to SV-OWSGs as well. The formal definition of somewhat injective SV-OWSGs can be omitted since it follows the same principles as somewhat injective OWSGs.

Let us assume that f is a somewhat injective OWSGs that takes $x \in \{0,1\}^n$ as input and outputs ρ_x, such that

$$\Pr_x\left[\mathbf{Pre}_{\mathrm{f},\alpha}(x) = 1\right] \geq \frac{1}{n^c} \tag{16}$$

for some constants $c, \alpha > 0$. Based on the discussion in the last subsection, we establish the following construction of EFI pairs from somewhat injective OWSGs.

Construction of EFI Pairs: Without loss of generality, when the state generation algorithm of f takes x as input, it first invokes a unitary U_x on $|0\rangle$ and gets $|\phi_x\rangle_{AB}$, then it discards (traces out) the B register and gets $\rho_x = \mathrm{Tr_B}|\phi_{\mathrm{x}}\rangle\langle\phi_{\mathrm{x}}|$. Based on that, we construct the generator algorithm $\mathtt{StateGen}(1^n, b)$ for the EFI pairs as follows:

- For an input bit $b \in \{0,1\}$, it generates the state

$$|\psi_b\rangle_{XA^{n^s}B^{n^s}Y} := \frac{1}{2^n} \cdot \sum_{x,r\in\{0,1\}^n} |b,x,r\rangle_X \otimes |\phi_x\rangle_{A^{n^s}B^{n^s}}^{\otimes n^s} \otimes |\langle r,x\rangle_2 \oplus b, r\rangle_Y, \tag{17}$$

  where $\langle r,x\rangle_2 := \mathbf{r} \cdot \mathbf{x} \mod 2$ and $s > 0$ is a constant that will be determined later. It then outputs the state

$$\mathtt{StateGen}(1^n, b) := \rho_b = \mathop{\mathrm{Tr}}_{XB^{n^s}} |\psi_b\rangle\langle\psi_b|. \tag{18}$$

Theorem 6 *If somewhat injective* OWSGs *exist, then the construction in* (18) *is* EFI.

Proof To prove Theorem 6, it is sufficient to show construction in (18) meets the distinguishability and the farness:

Distinguishability: The distinguishability can be shown similarly to its classical counterpart as discussed earlier, it is sufficient to justify the quantum version of Goldreich-Levin Theorem (Adcock and Cleve 2002; Coladangelo et al. 2021).

Lemma 6 (Quantum Goldreich-Levin Theorem) *Let $\mathcal{A}$ be a quantum algorithm that takes as input a random string r and an auxiliary quantum input ρ_x, and outputs a bit b. Then, if*

$$\Pr[\mathcal{A}(r,\rho_x) = \langle x, r\rangle_2] \geq 1/2 + \varepsilon,$$

there exists a quantum algorithm $\mathcal{B}$ that takes as input ρ_x and outputs a string x' such that $\mathcal{B}(\rho_x) = x$ with probability at least $4 \cdot \varepsilon^2$.

By the Goldreich-Levin Theorem, suppose there exists an adversary $\mathcal{A}$ that can distinguish between the two states with non-negligible probability $\varepsilon(n)$, we can hence derive a QPT adversary breaking the one-wayness of $\mathtt{f}$ with non-negligible probability $\varepsilon(n)^2$. That hence justifies the distinguishability.

Next, we turn to the proof of the farness for Theorem 6.

Farness: To show that the trace distance between these two states is significant, we start with the definition of the trace distance:

$$\mathrm{TD}(\rho_0,\rho_1) = \max_{\mathrm{P}} \mathrm{Tr}\Big(\mathrm{P}(\rho_0 - \rho_1)\Big).$$

Let P_b be the projection

$$P_b := \sum_{x,r}^{|\mathbf{Pre}_{\mathtt{f},\alpha}(x')|=1} P_x \otimes |\langle r,x\rangle_2 \oplus b, r\rangle\langle\langle r,x\rangle_2 \oplus b, r|.$$

For $x_1,\ldots,x_{2^n}$, we let the projection P_x be

$$P_x = \prod_{x_i \neq x} \left(\Pi_x^{x_i}\right), \tag{19}$$

where $\Pi_x^{x_i}$ is the projection that maximizes $\mathrm{Tr}[\Pi_{\mathrm{x}}^{\mathrm{x_i}}(\rho_{\mathrm{x}} - \rho_{\mathrm{x_i}})]$. That implies $\mathrm{Tr}[\Pi_{\mathrm{x}}^{\mathrm{x_i}}\rho_{\mathrm{x}}] \geq 1 - (1 - 1/\mathrm{n}^{\alpha})^{\mathrm{n^s}}$ and $\mathrm{Tr}[\Pi_{\mathrm{x}}^{\mathrm{x_i}}\rho_{\mathrm{x}}] \leq (1 - 1/\mathrm{n}^{\alpha})^{\mathrm{n^s}}$.

By the definition of $\Pi_x^{x_i}$ and $\mathbf{Pre}_{\mathtt{f},\alpha}(x)$, when we let $s = \alpha + 2$, it holds that

$$\begin{aligned}
&\mathrm{Tr}[\mathrm{P_x}\rho_{x'}] \geq 1 - 2^n \cdot \exp(-n^2), \quad x = x';\\
&\mathrm{Tr}[\mathrm{P_x}\rho_{x'}] \leq \exp(-n^2), \qquad\qquad x \neq x',
\end{aligned}$$

for any x such that $|\mathbf{Pre}_{\mathtt{f},\alpha}(x)| = 1$ and for all sufficiently large $n \in \mathbb{N}$. Combining the inequality above with the fact that $\Pr_x\left[\left|\mathbf{Pre}_{\mathtt{f},\alpha}(x)\right| = 1\right] \geq n^{-c}$, we have

$$\begin{aligned}
\mathrm{Tr}[\mathrm{P}_0\rho_0] &\geq n^{-c} - O(2^{2n} \cdot \exp(-2n^2))\\
&\geq n^{-c} - \mathtt{negl}(n).
\end{aligned} \tag{20}$$

On the other hand, we can deduce similarly that

$$\mathrm{Tr}[\mathrm{P}_0\rho_1] \leq \mathrm{O}(2^{\mathrm{n}} \cdot \exp(-2\mathrm{n}^2)) \leq \mathtt{negl}(\mathrm{n}). \tag{21}$$

This implies

$$\begin{aligned}
\mathrm{TD}(\rho_0,\rho_1) &\geq \mathrm{Tr}\Big(\mathrm{P}(\rho_0 - \rho_1)\Big) = \mathrm{Tr}(\mathrm{P}\rho_0) - \mathrm{Tr}(\mathrm{P}\rho_0)\\
&\geq n^{-c} - 2 \cdot \mathtt{negl}(n),
\end{aligned}$$

which shows farness of construction (18) and hence completes the proof. □

Furthermore, the verification step of $\mathtt{OWSGs}$ appears unnecessary in the proof of Theorem 6. By combining this observation with the result by Morimae and Yamakawa (2022a), we can deduce the equivalence between somewhat injective $\mathtt{SV\text{-}OWSGs}$ and $\mathtt{EFI}$ pairs:

Corollary 2 *Somewhat injective* $\mathtt{SV\text{-}OWSGs}$ *exist if and only if* $\mathtt{EFI}$ *pairs exist.*

Similarly, we can establish the implication from somewhat injective $\mathtt{OWSGs}$ to canonical quantum bit commitments:

Corollary 3 *Assuming the existence of somewhat injective* ($\mathtt{SV\text{-}}$)$\mathtt{OWSGs}$*, then canonical quantum bit commitments exist.*

Next, we demonstrate that somewhat injective $\mathtt{OWSGs}$ can be achieved using almost regular $\mathtt{OWSGs}$, which we define as follows:

Definition 8 *(Almost Regular* $\mathtt{OWSGs}$*)* A quantum state generator $\mathtt{f}$ is said to be (α,β)-regular $\mathtt{OWSG}$ for $\alpha,\beta > 0$ if the following holds for any constant $\alpha' \geq \alpha$:

$$n^{-\beta} \cdot \frac{2^n}{\mathbf{E}_\alpha(\mathtt{f})} \leq \mathbf{Pre}_{\alpha'}(x) \leq n^{\beta} \cdot \frac{2^n}{\mathbf{E}_\alpha(\mathtt{f})}, \tag{22}$$

where

$$\mathbf{E}_\alpha(\mathtt{f}) := \min\left|\left\{x_1, x_2 \ldots \mid \bigcup_{x_i} \mathbf{Pre}_{\mathtt{f},\alpha}(x_i) = \mathrm{Supp}(\mathtt{KeyGen}(1^\lambda))\right\}\right|,$$

and

$$\mathbf{Pre}_{\mathtt{f},\alpha}(x) := \left\{ x' \mid \mathrm{F}(\rho_{\mathrm{x}}, \rho_{\mathrm{x}'}) \geq 1 - \frac{1}{\mathrm{n}^{\alpha}} \right\}.$$

Additionally, it is almost regular if (22) holds for almost all $x \in \{0,1\}^n$.Here "almost all" means that the set of x for which (22) does not hold is negligible.

Based on the notion of almost regularity, we provide a construction for somewhat injective OWSGs as follows:

Lemma 7 *Assuming* $\mathtt{f}$ *is* (α,β)*-almost regular* OWSG *that takes* $x \in \{0,1\}^n$ *as input and outputs* ρ_x*, we have*

$$\mathtt{f}'(h_e, x) := \eta_{x,h_e} = \rho_x \otimes |h_e, h_e(x)\rangle\langle h_e, h_e(x)| \tag{23}$$

as a somewhat injective OWSG*, where* $h_e : \{0,1\}^n \to \{0,1\}^e$ *is 2-wise independent hash for* $e = \lceil \log(n^{\beta} \cdot \mathbf{E}_{\alpha}(\mathtt{f})) \rceil + 1$.

Proof Since $h_e : \{0,1\}^n \to \{0,1\}^e$ is 2-wise independent hash function, we have

$$\Pr_{he}[h_e(x) = h_e(x')] \leq 2^{-e}.$$

Therefore, we have

$$\mathop{\mathrm{E}}_{h_e}\left[\left|\mathbf{Pre}_{\mathtt{f}',\alpha}(h_e, x) \setminus (h_e, x)\right|\right] = \frac{n^{\beta} \cdot 2^n}{2^e \cdot \mathbf{E}_{\alpha}(\mathtt{f})} \leq \frac{1}{2}.$$

This implies

$$\Pr_{h_e,x}\left[\left|\mathbf{Pre}_{\mathtt{f}',\alpha}(h_e, x) \setminus (h_e, x)\right| > 1\right] \geq \frac{1}{2}. \tag{24}$$

This justifies the somewhat injectiveness.

Next, we show the one-wayness of $\mathtt{f}'$. Before giving the proof, we sirstly revisit the quantum leftover hash lemma (Renner and König 2005; Bartusek et al. 2021) as follows:

Lemma 8 *Let* $\{h_e : \{0,1\}^n \to \{0,1\}^e\}$ *be a family of 2-wise independent hash functions. Then for classical-quantum bipartite state* $\rho_{XY} := \mathrm{E}_{\mathrm{x}}|\mathrm{x}\rangle\langle\mathrm{x}| \otimes \rho_{\mathrm{x}}$ *where X stores the classical input and Y stores the corresponding quantum state* ρ_x*, we have*

$$\mathrm{TD}\left(\mathop{\mathrm{E}}_{h_e,x}\left|h_e, h_e(x)\right\rangle\left\langle h_e, h_e(x)\right| \otimes \rho_x, \mathop{\mathrm{E}}_{h_e,x,u}\left|h_e, u\right\rangle\left\langle h_e, u\right| \otimes \rho_x\right) \leq 2^{-1-\frac{\left(\mathrm{H}_{\min}(X|Y)_{\rho}-e\right)}{2}} \tag{25}$$

where $u \leftarrow \{0,1\}^l$ *is chosen uniformly at random* $\mathrm{H}_{\min}(\mathrm{X} \mid \mathrm{Y})_{\rho}$ *is the quantum conditional min-entropy defined by*

$$\mathrm{H}_{\min}(\mathrm{X} \mid \mathrm{Y})_{\rho} := \sup_{\eta_{\mathrm{B}}} \left\{ \lambda \in \mathbb{R} : 2^{-\lambda}\mathrm{I}_{\mathrm{X}} \otimes \eta_{\mathrm{Y}} \geq \rho \right\}.$$

The proof strategy of one-wayness is similar to its classical counterpart. Assuming there exist a QPT adversary $\mathcal{A}$ breaks the one-wayness of $\mathtt{f}'$ with $t(n)$ copies and wins with non-negligible advantage $\delta(n)$. We denote by $h_e(x)|_{e'}$ be the first e' bits of $h_e(x)$. By the definition of almost regularity, the min-entropy $\mathrm{H}_{\min}(\mathrm{X} \mid \mathrm{Y})_{\rho}$ is at least ,

$$\mathrm{H}_{\min}(\mathrm{X} \mid \mathrm{A})_{\rho} > \log \mathrm{n}^{-\beta-1} \cdot \frac{2^{\mathrm{n}}}{\mathbf{E}_{\alpha}(\mathtt{f})}. \tag{26}$$

Then by quantum leftover hash lemma 8, the trace distance can be bounded as follows:

$$\mathrm{TD}\left(\mathop{\mathrm{E}}_{\mathrm{he,x}}|\mathrm{he}\rangle\langle\mathrm{he}| \otimes |\mathrm{he(x)}|_{\mathrm{e}'}\rangle\langle\mathrm{he(x)}|_{\mathrm{e}'}| \otimes \rho_{\mathrm{x}}, \mathop{\mathrm{E}}_{\mathrm{he,x,r_{e'}}}|\mathrm{he}\rangle\langle\mathrm{he}| \otimes |\mathrm{r_{e'}}\rangle\langle\mathrm{r_{e'}}| \otimes \rho_{\mathrm{x}}\right) \leq 2^{-1-\frac{(\mathrm{H}_{\min}(\mathrm{X}|\mathrm{Y})_{\rho}-\mathrm{e}')}{2}} = \frac{\delta(n)}{2}, \tag{27}$$

where $e' = e - (2\beta+1)\log n - 2\log(2/\delta(n)) - 1$, $x \leftarrow \{0,1\}^n, r_{e'} \leftarrow \{0,1\}^{e'}$ are chosen uniformly at random.

Next, since there are $(2\beta+1)\log n + 2\log(2/\delta(n)) + 1$ remaining bits in $h_e(x)$ which is not close to random string, we can guess it correctly with probability at least $n^{-2\beta-1} \cdot \delta(n)/2$, that implies a QPT adversary $\mathcal{B}$ for breaking the one-wayness of f with advantage $n^{-2\beta-1} \cdot \delta(n)^2/4$ as follows:

- $\mathcal{B}$ takes as input $\rho_{x^*}^{\otimes t(n)}$ as its challenge.
- $\mathcal{B}$ generates a universal hash function $h_e : \{0,1\}^n \to \{0,1\}^e$.
- $\mathcal{B}$ runs $\mathcal{A}$ with $|h_e, r\rangle\langle h_e, r|^{\otimes t(n)} \otimes \rho_{x^*}^{\otimes t(n)}$ for a random chosen $r \leftarrow \{0,1\}^e$ and outputs $\mathcal{A}$'s result.

Due to the $\delta/2$-closeness between these two state in inequality (25), $\mathcal{A}$ wins with probability at least $\delta/2$ if we replace the first e' bits of $h_e(x^*)$ by a random string

$r_{e'} \leftarrow \{0,1\}^{e'}$, we can conclude that $\mathcal{B}$ wins with probability at least $n^{-2\beta-1} \cdot \delta(n)^2/4$. That justifies the one-wayness, hence completes the proof of Lemma 7. □

Similar to its classical counterpart, we note that our construction from almost regular OWSGs to somewhat injective OWSGs can also be extended to the case where the preimage size of OWSG can be efficiently estimated from the image state, using at most polynomially many copies.

However, extending Lemma 7 to SV-OWSGs would face a challenge. In the case of almost regular SV-OWSG, each image state sphere (that is, a sphere that takes the an output state as its centre) may contain exponentially many points, which makes it difficult to suit the lemma (although it still holds when each sphere of the output state contains only polynomially many points).

Single-copy-secure hard-core predicates suffice for EFI Pairs

In this section, we establish the equivalence between EFI pairs and single-copy-secure hard-core predicates of secretly-verifiable and extremely-statistically-invertible quantum state generators (SV-eSI-OWSGs) introduced in Definition 4. We firstly introduce the definition of single-copy-secure hard-core predicate of SV-eSI-OWSGs as follows:

Definition 9 *(Single-Copy-Secure Hard-Core Predicate of* SV-eSI-OWSGs*)* A QPT algorithm $\mathtt{P} : \{0,1\}^n \to \{0,1\}$ is single-copy-secure hard-core predicate of the secretly-verifiable and extremely-statistically-invertible quantum state generator $\mathtt{f}(x) := \rho_x$ if it satisfies the condition

$$\left|\Pr_x[\mathcal{D}(\rho_x, \mathtt{P}(x)) = 1] - \Pr_x[\mathcal{D}(\rho_x, \mathtt{P}(x) \oplus 1) = 1]\right| \leq \mathtt{negl}(n)$$

for any QPT distinguisher $\mathcal{D}$.

By the Quantum Goldreich Levin Theorem 6, it's easy to note that the existence of single-copy-secure hard-core predicate of SV-eSI-OWSGs is implied by the single-copy-secure SV-eSI-OWSGs (i.e., only one copy of the challenge state is given in the experiment $\mathtt{Exp}^{sv-owsg}_{\mathtt{f},\mathcal{A}}$). Notably, the single-copy-secure hard-core predicate of SV-eSI-OWSGs appears to be a weaker primitive, as it only requires one copy of the challenge state. However, the equivalence with EFI pairs demonstrates their underlying connection and reveals that they are conceptually equivalent.

Single-Copy-Secure Hard-Core Predicate of SV-eSI-OWSGs from EFI Pairs: Let $\mathtt{StateGen}(1^n, b)$ be the generation algorithm for EFI pairs, where b and 1^n are the input parameters, and ρ_b is the resulting (mixed) state. Based on the construction by Morimae and Yamakawa (2022a) and the Goldreich-Levin theorem for SV-eSI-OWSGs, it can be shown that the function

$$\mathtt{P}(x_1 \| \ldots \| x_n, r_1 \| \ldots \| r_n) = \bigoplus_{i=1}^{n} r_i \cdot x_i \tag{28}$$

serves as the hard-core predicate for the SV-eSI-OWSG

$$\mathtt{f}(x_1 \| \ldots \| x_n, r_1 \| \ldots \| r_n) = \bigotimes_{i=1}^{n} \rho_{x_i}^{\otimes n^c} \otimes |r_i\rangle\langle r_i| \tag{29}$$

where $c > 0$ is a constant. Based on the argument presented by Morimae and Yamakawa (2022a), it can be established that f is a SV-eSI-OWSGs for a suitable constant $c > 0$ (specifically, a single-copy-secure SV-eSI-OWSGs). Consequently, the Quantum Goldreich-Levin Theorem 6 directly implies that P serves as a single-copy-secure hard-core predicate for f which hence justifies this part of implication.□

EFI Pairs from Single-Copy-Secure Hard-Core Predicate of SV-eSI-OWSGs: Let P be the single-copy-secure hard-core predicate of SV-eSI-OWSGs denoted by $\mathtt{f} = (\mathtt{KeyGen}, \mathtt{StateGen})$. The state generation algorithm of EFI pairs is given by

$$\mathtt{StateGen}'(1^n, b) := \mathop{\mathrm{E}}_x \rho_x \otimes |\mathtt{P}(x) \oplus b\rangle\langle \mathtt{P}(x) \oplus b| \tag{30}$$

which generates EFI pairs. Here, the expectation of x follows the distribution on $\mathtt{KeyGen}(1^n)$ of f.

The distinguishability of the EFI pairs follows directly from the security of P. Since if not, for a challenge $\rho_x \otimes |\mathtt{P}(x) \oplus b\rangle\langle \mathtt{P}(x) \oplus b|$, invoking the distinguisher of EFI pairs with this state would directly induce a distinguisher for the hard-core predicate P.

Next, we demonstrate the farness of this construction. For convenience, let

$$\eta_b := \mathop{\mathrm{E}}_{x}^{\mathtt{P}(x)=b} \rho_x \tag{31}$$

Then, we have

$$\mathop{\mathrm{E}}_x \rho_x \otimes |\mathtt{P}(x) \oplus b\rangle\langle \mathtt{P}(x) \oplus b| = p_0 \cdot \eta_0 \otimes |b\rangle\langle b| + (1 - p_0)\eta_1 \otimes |b \oplus 1\rangle\langle b \oplus 1|$$

for some $|p_0 - 1/2| \leq \mathtt{negl}(n)$ (otherwise, it contradicts the hardness of predicate $\mathtt{P}$).

Since the function $\mathtt{f}$ is statistically invertible, it satisfies the following inequality:

$$\mathrm{TD}(\rho_{\mathrm{x}}, \rho_{\mathrm{x}'}) \geq 1 - 2^{-\mathrm{n}} \cdot \mathtt{negl}(\mathrm{n}) \tag{32}$$

Consequently, there exists a projection $P_x^{x'}$ such that

$$\mathrm{Tr}(\mathrm{P}_{\mathrm{x}}^{\mathrm{x}'} \rho_{\mathrm{x}}) \geq 1 - 2^{-\mathrm{n}} \cdot \mathtt{negl}(\mathrm{n}), \tag{33}$$

and

$$\mathrm{Tr}(\mathrm{P}_{\mathrm{x}}^{\mathrm{x}'} \rho_{\mathrm{x}'}) \leq 2^{-\mathrm{n}} \cdot \mathtt{negl}(\mathrm{n}). \tag{34}$$

Now, consider the product of projections $\prod_{x'}^{\mathtt{P}(x)=1} \left(P_x^{x'}\right)$ (it doesn't matter in which order the projections are taken). Define:

$$\eta_0' := \mathop{\mathrm{E}}_{x}^{\mathtt{P}(x)=0} \frac{\prod_{x'}^{\mathtt{P}(x)=1} \left(P_x^{x'}\right) \rho_x \left(\prod_{x'}^{\mathtt{P}(x)=1} \left(P_x^{x'}\right)\right)^\dagger}{\mathrm{Tr}\left(\prod_{x'}^{\mathtt{P}(x)=1} \left(\mathrm{P}_{\mathrm{x}}^{\mathrm{x}'}\right) \rho_{\mathrm{x}} \left(\prod_{x'}^{\mathtt{P}(x)=1} \left(\mathrm{P}_{\mathrm{x}}^{\mathrm{x}'}\right)\right)^\dagger\right)}$$

and

$$\eta_1' := \mathop{\mathrm{E}}_{x}^{\mathtt{P}(x)=1} \frac{\prod_{x'}^{\mathtt{P}(x)=1} \left(I - P_x^{x'}\right) \rho_x \left(\prod_{x'}^{\mathtt{P}(x)=1} \left(I - P_x^{x'}\right)\right)^\dagger}{\mathrm{Tr}\left(\prod_{x'}^{\mathtt{P}(x)=1} \left(\mathrm{I} - \mathrm{P}_{\mathrm{x}}^{\mathrm{x}'}\right) \rho_{\mathrm{x}} \left(\prod_{x'}^{\mathtt{P}(x)=1} \left(\mathrm{I} - \mathrm{P}_{\mathrm{x}}^{\mathrm{x}'}\right)\right)^\dagger\right)}$$

Using inequalities (33) and (34), we can derive the following inequality:

$$\mathrm{Tr}\left(\prod_{x'}^{\mathtt{P}(x')=1} \left(\mathrm{P}_{\mathrm{x}}^{\mathrm{x}'}\right) \rho_{\mathrm{x}} \left(\prod_{x'}^{\mathtt{P}(x')=1} \left(\mathrm{P}_{\mathrm{x}}^{\mathrm{x}'}\right)\right)^\dagger\right) \geq 1 - \mathtt{negl}(\mathrm{n})$$

for any x such that $\mathtt{P}(x) = 0$.

Similarly, we have:

$$\mathrm{Tr}\left(\prod_{x'}^{\mathtt{P}(x')=1} \left(\mathrm{I} - \mathrm{P}_{\mathrm{x}}^{\mathrm{x}'}\right) \rho_{\mathrm{x}} \left(\prod_{x'}^{\mathtt{P}(x')=1} \left(\mathrm{I} - \mathrm{P}_{\mathrm{x}}^{\mathrm{x}'}\right)\right)^\dagger\right) \geq 1 - \mathtt{negl}(n),$$

for any x such that $\mathtt{P}(x) = 1$. Consequently, we obtain:

$$\begin{aligned}
\mathrm{TD}\left(\eta_0, \eta_0'\right) &\leq \mathop{\mathrm{E}}_{x}^{\mathtt{P}(x)=b} \mathrm{TD}\left(\rho_{\mathrm{x}}, \frac{\left(\prod_{x'}^{\mathtt{P}(x')=1} \mathrm{P}_{\mathrm{x}}^{\mathrm{x}'}\right) \rho_{\mathrm{x}} \left(\prod_{x'}^{\mathtt{P}(x')=1} \mathrm{P}_{\mathrm{x}}^{\mathrm{x}'}\right)^\dagger}{\mathrm{Tr}\left(\prod_{x'}^{\mathtt{P}(x')=1} \mathrm{P}_{\mathrm{x}}^{\mathrm{x}'}\right) \rho_{\mathrm{x}} \left(\prod_{x'}^{\mathtt{P}(x')=1} \mathrm{P}_{\mathrm{x}}^{\mathrm{x}'}\right)^\dagger}\right) \\
&\leq \mathop{\mathrm{E}}_{x}^{\mathtt{P}(x)=b} \left(1 - \mathrm{Tr}\left(\prod_{x'}^{\mathtt{P}(x')=1} \left(\mathrm{P}_{\mathrm{x}}^{\mathrm{x}'}\right) \rho_{\mathrm{x}} \left(\prod_{x'}^{\mathtt{P}(x')=1} \left(\mathrm{P}_{\mathrm{x}}^{\mathrm{x}'}\right)\right)^\dagger\right)\right) \\
&\leq \mathtt{negl}(n).
\end{aligned} \tag{35}$$

Similarly, $\mathrm{TD}(\eta_0, \eta_0') \leq \mathtt{negl}(\mathrm{n})$. Furthermore, since $\mathrm{TD}(\eta_0', \eta_1') = 1$, there exists a projection P_0 satisfying:

$$\mathrm{Tr}(\mathrm{P}_0 \eta_0') = 1, \text{ and } \mathrm{Tr}(\mathrm{P}_0 \eta_1') = 0. \tag{36}$$

We then define $P = P_0 \otimes |0\rangle\langle 0| + (I - P_0) \otimes |1\rangle\langle 1|$, and obtain:

$$\begin{aligned}
&\mathrm{TD}\left(\mathop{\mathrm{E}}_{x} \rho_x \otimes |P(x)\rangle\langle P(x)|, \mathop{\mathrm{E}}_{x} \rho_x \otimes |P(x) \oplus 1\rangle\langle P(x) \oplus 1|\right) \\
&= \mathrm{TD}(p_0 \cdot \eta_0 \otimes |0\rangle\langle 0| + (1 - p_0)\eta_1 \otimes |1\rangle\langle 1|, p_0 \cdot \eta_0 \otimes |1\rangle\langle 1| + (1 - p_0)\eta_1 \otimes |0\rangle\langle 0|) \\
&\geq \mathrm{TD}(p_0 \cdot \eta_{0'} \otimes |0\rangle\langle 0| + (1 - p_0)\eta_{1'} \otimes |1\rangle\langle 1|, p_0 \cdot \eta_{0'} \otimes |1\rangle\langle 1| + (1 - p_0)\eta_{1'} \otimes |0\rangle\langle 0|) \\
&-negl(n) \geq \mathrm{Tr}(P(p_0 \cdot \eta_{0'} \otimes |0\rangle\langle 0| + (1 - p_0)\eta_{1'} \otimes |1\rangle\langle 1| - p_0 \cdot \eta_{0'} \otimes |1\rangle\langle 1| - (1 - p_0)\eta_{1'} \otimes |0\rangle\langle 0|) \\
&-negl(n) \geq 1 - negl(n).
\end{aligned}$$

This completes the proof of the implication from the single-copy-secure hard-core predicate of SV-eSI-OWSGs to the EFI pairs.□

More specifically, since SV-SI-OWSG is equivalent to EFI pairs, we can further shows that k-copy-secure δ -statistically-invertible SV-OWSG is sufficient for normal SV-SI-OWSG when k and δ are chosen appropriately.

Corollary 4 *Assuming the existence of k-copy-secure δ -statistically-invertible* SV-OWSG *such that*

$$\delta^k \leq 2^{-n} \cdot \mathtt{negl}(n), \tag{37}$$

then SV-SI-OWSG *exists.*

Simple construction of EFI Pairs from LPN

In this section, we present a construction of EFI pairs from the decisional Learning with Parity (LPN) assumption. Our construction offers more flexibility in choosing parameters compared to classical constructions.

We begin by introducing the definition of the decisional known as Learning with Parity problem.

Definition 10 *(Learning with Parity* (LPN)*)* For parameters $\tau \in (0, \frac{1}{2})$, $n, m \in \mathbb{N}$, the decisional LPN problem (Learning with Parity problem), denoted as $\mathsf{LPN}_{n,m,\tau}$, is considered hard in the quantum case if

$$\left| \Pr_{A \leftarrow \mathbb{Z}_2^{m\times n}, x \leftarrow \{0,1\}^n, e \leftarrow B_\tau^m} [\mathcal{D}(A, Ax \oplus e) = 1] - \Pr_{A \leftarrow \mathbb{Z}_2^{m\times n}, r \leftarrow \{0,1\}^m} [\mathcal{D}(A, r) = 1] \right| \leq \mathtt{negl}(n),$$

for any quantum polynomial-time distinguisher $\mathcal{D}$, where B_τ is the Bernoulli distribution with parameter τ, i.e., $\Pr_{\mathrm{b} \leftarrow \mathrm{B}\tau}[\mathrm{b} = 1] = \tau$.

In the traditional definition of $\mathsf{LPN}_{n,m,\tau}$, the parameter τ is often chosen as a constant, which is sufficient for many cryptographic primitives such as the one-way functions, pseudorandom generators, and commitments. However, it has been shown that low-noise $\mathsf{LPN}_{n,m,\tau}$ (e.g., $\tau = \frac{1}{\sqrt{N}}$) implies public-key cryptographic primitives. Besides, it is called the high noise $\mathsf{LPN}_{n,m,\tau}$ if $\tau > 1 - \mathtt{poly}(n)^{-1}$ for some polynomial $\mathtt{poly}(\cdot)$.

We define an $\mathsf{LPN}_{n,m,\tau}$ assumption as non-trivial if the statistical distance between the distribution of a real $\mathsf{LPN}_{n,m,\tau}$ sample and a random distribution $(A, r) \leftarrow \mathbb{Z}_2^{m\times n} \times \{0,1\}^m$ is larger than $1/\mathtt{poly}(n)$ for some positive polynomial $\mathtt{poly}(\cdot)$. Next, we demonstrate the feasibility of EFI pairs and, consequently, quantum commitment from the decisional LPN assumption by giving the following construction of EFI pairs.

Construction of EFI Pairs: The description of the generation algorithm $\mathtt{StateGen}(1^n, b)$ is as follows:

- For $b = 0$:

$$\begin{aligned}\mathtt{StateGen}(1^n, 0) := \rho_0 &= \mathop{\mathrm{E}}_{A} |A\rangle\langle A| \otimes \rho_{0,A} \\ &= \mathop{\mathrm{E}}_{A} |A\rangle\langle A| \otimes \left(\mathop{\mathrm{E}}_{x,e} |Ax \oplus e\rangle\langle Ax \oplus e| \right).\end{aligned}$$

- For $b = 1$:

$$\begin{aligned}\mathtt{StateGen}(1^n, 1) := \rho_1 &= \mathop{\mathrm{E}}_{A} |A\rangle\langle A| \otimes \rho_{1,A} \\ &= \mathop{\mathrm{E}}_{A} |A\rangle\langle A| \otimes \left(\mathop{\mathrm{E}}_{r} |r\rangle\langle r| \right).\end{aligned}$$

Here, the expectation in the first equation is taken over the randomness of $A \leftarrow \mathbb{Z}_2^{m\times n}$, $x \leftarrow \{0,1\}^n$, $e \leftarrow B_\tau^m$, while the second equation is taken over $A \leftarrow \mathbb{Z}_2^{m\times n}$ and $r \leftarrow \{0,1\}^m$.

Theorem 7 *(*EFI *Pairs from Decisional* LPN*) Assuming a non-trivial decisional* $\mathsf{LPN}_{n,m,\tau}$ *is quantum hard-on-average,* EFI *pairs exist.*

Proof To justify the statement of Theorem 7, it is sufficient to show the construction above meets the farness and the distinguishability.

Farness: To show the farness property, we note that

$$\begin{aligned}\mathrm{F}(\rho_0, \rho_1) &\leq \mathrm{F}\left(\mathop{\mathrm{E}}_{\mathrm{A}} |\mathrm{A}\rangle\langle \mathrm{A}| \otimes \rho_{0,\mathrm{A}}, \mathop{\mathrm{E}}_{\mathrm{A}} |\mathrm{A}\rangle\langle \mathrm{A}| \otimes \rho_{1,\mathrm{A}} \right) \\ &= \sum_{A,r} \sqrt{(\sum_{x,e}^{Ax\oplus e=r} p_0(A,x,e)) \cdot p_1(A,r)} \\ &\overset{*}{\leq} 1 - \left(\sum_{A,r} |(\sum_{x,e}^{Ax\oplus e=r} \frac{p_0(A,x,e))}{2} - \frac{p_1(A,r)}{2})| \right)^2.\end{aligned}$$

Here, $p_0(A, x, e)$ is the weight of $|A, Ax \oplus e\rangle$ in ρ_0, and $p_1(A, r)$ is defined similarly. The inequality $(*)$ follows from the relation between Hellinger distance and statistical distance. We observe that:

$$\sum_{A,r} \left| (\sum_{x,e}^{Ax\oplus e=r} p_0(A,x,e)) - p_1(A,r)) \right| /2$$

is exactly the statistical distance between an $\mathsf{LPN}_{n,m,\tau}$ sample and a random $(A, r) \leftarrow \mathbb{Z}_2^{m\times n} \times \{0,1\}^m$, which is noticeable due to the non-triviality of the $\mathsf{LPN}_{n,m,\tau}$ assumption. This completes the proof of farness.

Indistinguishability: Next, we consider the notion of indistinguishability. Let us assume that there exists an adversary $\mathcal{A}$ that breaks the security of the EFI pairs with a non-negligible probability $\varepsilon(n)$. We will now construct a distinguisher $\mathcal{D}$ that breaks the decisional $\mathsf{LPN}_{n,m,\tau}$ assumption as follows:

- The distinguisher $\mathcal{D}$ takes (A, y) as input, which is either $(A, Ax \oplus e)$ or (A, r), where A is chosen uniformly at random from $\mathbb{Z}_2^{m\times n}$, x and r are chosen uniformly at random from $\{0,1\}^n$ and $\{0,1\}^m$ respectively , and e is chosen from B_τ^m. The task of $\mathcal{D}$ is to determine which case it is.
- $\mathcal{D}$ runs $\mathcal{A}$ with input (A, y) and outputs its decision.

By exploiting the linearity of quantum operators,

$$\mathcal{A}\left(\mathop{\mathrm{E}}_{A}|A\rangle\langle A|\otimes\mathop{\mathrm{E}}_{x,e}|Ax\oplus e\rangle\langle Ax\oplus e|\right)$$
$$=\mathop{\mathrm{E}}_{A}\left[\mathop{\mathrm{E}}_{x,e}\left(\mathcal{A}(|A\rangle\langle A|\otimes|Ax\oplus e\rangle\langle Ax\oplus e|)\right)\right].$$

Similarly,

$$\mathcal{A}\left(\mathop{\mathrm{E}}_{A}|A\rangle\langle A|\otimes\mathop{\mathrm{E}}_{r}|r\rangle\langle r|\right)=\mathop{\mathrm{E}}_{A}\left[\mathop{\mathrm{E}}_{r}\left(\mathcal{A}(|A\rangle\langle A|\otimes|r\rangle\langle r|)\right)\right].$$

Hence, we can conclude that the distinguisher $\mathcal{D}$ can distinguish these two cases with a probability exactly equal to $\varepsilon(n)$. This justifies the indistinguishability and completes the proof of Theorem 7. □

We remark that the construction described above can be polarized without increasing the sample number m of the underlying $\mathsf{LPN}_{n,m,\tau}$ assumption. To achieve this, we set $\rho_b' = \rho_b^{\otimes n^C}$ as the output state of input bit b for some sufficiently large constant $C > 0$. By doing so, the trace distance can be made exponentially small, while the distinguishability holds by a simple hybrid argument. Assuming $\mathcal{A}$ distinguishes ρ_0' from ρ_1', then for a random $k \in [n^C - 1]$, $\mathcal{A}$ also distinguishes $\rho_0^{\otimes n^C-k-1}\otimes\rho_1^{\otimes k+1}$ from $\rho_0^{\otimes n^C-k}\otimes\rho_1^{\otimes k}$. Therefore, it is sufficient to pad the challenge value of LPN to a random position of the output state and generate the rest of the parts locally.

Note that commitments can also be achieved using the exact version of the decisional LPN assumption with a noise rate τ ($\tau < 0.25$) when $m = O(n)$ (or with significantly larger m from the construction of OWFs or PRGs under the LPN assumption Pietrzak 2012). However, it is easy to see that our construction also makes sense for high noise rates (with large m) and any constant noise τ (with small $m = O(n)$) as long as the decisional $\mathsf{LPN}_{n,m,\tau}$ assumption in that case is non-trivial. Hence, we believe our construction is simple and achieves a better parameter choice than the classical constructions.

Conclusion

In conclusion, our exploration into the intricacies of OWSGs has not only broadened the theoretical landscape of quantum cryptography but also provided concrete methodologies for their application in quantum commitment schemes. By leveraging structured OWSGs, we have successfully demonstrated the construction of quantum commitments that offer robust security features, such as statistical binding and computational hiding. The equivalence established between EFI pairs and hard-core predicates furthers our understanding of the fundamental properties of quantum cryptographic primitives. Additionally, our construction of EFI pair construction based on the decisional LPN assumption highlights the adaptability and potential in enhancing the security parameters of quantum cryptographic systems.

Moving forward, it is crucial to extend our investigations into the property of OWSGs, and their broader implications in other quantum cryptographic primitives. As an open problem, a key challenge that remains is to construct pseudorandom state generators (PRSs) and pseudorandom function-like states (PRFSs) from OWSGs. More specifically, how can we leverage the one-wayness of OWSGs to develop PRSs that meet the rigorous demands of quantum pseudorandomness while maintaining efficient computability and verifiability. This issue is pivotal for advancing the quantum cryptography and deserves focused research efforts.

Abbreviations

EFI pairs	Efficiently samplable, statistically far but computationally indistinguishable pairs of distributions
OWF	One-way function
OWSG	One-way state generator
SV-OWSG	Secretly-verifiable OWSG
SV-SI-OWSG	Secretly-verifiable and statistically-invertible OWSG
SV-ESI-OWSG	Secretly-verifiable and extremely-statistically-invertible quantum state generators
PRG	Pseudorandom generator
PRS	Pseudorandom state
QPT	Quantum polynomial-time
$\lvert\phi\rangle_A$	Pure quantum state in register A
ρ_A	Mixed state in register A
$\mathrm{Tr}(\rho)$	Trace of mixed state (density matrix) ρ
$\mathrm{TD}(\rho_0,\rho_1)$	Trace distance between ρ_0 and ρ_1
$\mathrm{F}(\rho_0,\rho_1)$	Fidelity between ρ_0 and ρ_1
$U^\dagger$	Adjoint matrix of U
$x\|\|y$	Concatenation of string x and y
$\langle x,y\rangle_2$	Sum of product of strings $x, y \in \{0,1\}^n$ over $\mathbb{Z}_2$
$\lceil\cdot\rceil$	Ceiling function
$\mathrm{E}[X]$	Expectation of variable X
$\mathrm{Supp}(X)$	Support of X
$\otimes$	Tensor product
$\oplus$	Bitwise XOR
$\mathrm{Img}(f)$	Image space of function f

$\mathtt{negl}(\cdot)$	Negligible function
$\mathbf{Inj}(f)$	Injective domain of function f
$\mathbf{Pre}_{\mathtt{f},\alpha}(x)$	Preimages collection of state $\mathtt{f}(x)$ within error α
$\mathbf{E}_{\alpha}(\mathtt{f})$	Minimum of preimages covering the support of $\mathtt{f}$ within error α
$\mathrm{H}_{\min}(X \mid Y)_{\rho_{AB}}$	Quantum min-entropy of X conditioned on Y
LPN	Learning Parity with Noise

Acknowledgements
We would like to thank the anonymous reviewers and editors for detailed comments and useful feedback.

Author contributions
CSJ was responsible for conceptualization and methodology, and also wrote the original draft. XR served as the corresponding author, and supervised the project and contributed to writing, review, and editing.

Funding
This work is supported by National Natural Science Foundation of China (62302496, 62172405, and 61932019), and the Key Research Program of the Chinese Academy of Science, Grant No. ZDRW-XX-2022-1.

Availability of data and materials
Not applicable.

Declarations

Competing Interests
The authors declare that they have no competing interests.

Received: 26 May 2024 Accepted: 11 August 2024
Published online: 05 May 2025

References

Adcock M, Cleve R (2002) A quantum goldreich-levin theorem with cryptographic applications. In: Alt H, Ferreira A (eds.) STACS 2002, 19th Annual Symposium on Theoretical Aspects of Computer Science, Antibes - Juan les Pins, France, March 14-16, 2002, Proceedings. Lecture Notes in Computer Science, vol. 2285, pp 323–334. Springer. https://doi.org/10.1007/3-540-45841-7_26

Applebaum B, Cash D, Peikert C, Sahai A (2009) Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In: Halevi S (ed.) Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings. LNCS, vol. 5677, pp. 595–618. Springer. https://doi.org/10.1007/978-3-642-03356-8_35

Applebaum B, Ishai Y, Kushilevitz E (2009) Cryptography with constant input locality. J. Cryptol. 22(4):429–469. https://doi.org/10.1007/s00145-009-9039-0

Alekhnovich M (2003) More on average case vs approximation complexity. In: 44th Symposium on Foundations of Computer Science (FOCS 2003), 11-14 October 2003, Cambridge, MA, USA, Proceedings, pp. 298–307. IEEE Computer Society. https://doi.org/10.1109/SFCS.2003.1238204

Ananth P, Qian L, Yuen H (2022) Cryptography from pseudorandom quantum states. In: Dodis Y, Shrimpton T (eds.) Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part I. LNCS, vol. 13507, pp. 208–236. Springer. https://doi.org/10.1007/978-3-031-15802-5_8

Bitansky N, Brakerski Z (2021) Classical binding for quantum commitments. In: Nissim K, Waters B (eds.) Theory of Cryptography - 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8-11, 2021, Proceedings, Part I. LNCS, vol. 13042, pp. 273–298. Springer. https://doi.org/10.1007/978-3-030-90459-3_10

Bartusek J, Coladangelo A, Khurana D, Ma F (2021) One-way functions imply secure computation in a quantum world. In: Malkin T, Peikert C (eds.) Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I. LNCS, vol. 12825, pp. 467–496. Springer. https://doi.org/10.1007/978-3-030-84242-0_17

Brakerski Z, Canetti R, Qian L (2023) On the computational hardness needed for quantum cryptography. In: Kalai YT (ed.) 14th Innovations in Theoretical Computer Science Conference, ITCS 2023, January 10-13, 2023, MIT, Cambridge, Massachusetts, USA. LIPIcs, vol. 251, pp. 24–12421. Schloss Dagstuhl - Leibniz-Zentrum für Informatik. https://doi.org/10.4230/LIPIcs.ITCS.2023.24

Blum A, Furst ML, Kearns MJ, Lipton RJ (1993) Cryptographic primitives based on hard learning problems. In: Stinson DR (ed.) Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings. LNCS, vol. 773, pp. 278–291. Springer. https://doi.org/10.1007/3-540-48329-2_24

Blum A, Kalai A, Wasserman H (2000) Noise-tolerant learning, the parity problem, and the statistical query model. In: Yao FF, Luks EM (eds.) Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, May 21-23, 2000, Portland, OR, USA, pp. 435–440. ACM. https://doi.org/10.1145/335305.335355

Brakerski Z, Lyubashevsky V, Vaikuntanathan V, Wichs D (2019) Worst-case hardness for LPN and cryptographic hashing via code smoothing. In: Ishai, Y., Rijmen, V. (eds.) Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III. LNCS, vol. 11478, pp. 619–635. Springer. https://doi.org/10.1007/978-3-030-17659-4_21

Brakerski Z, Shmueli O (2019) (pseudo) random quantum states with binary phase. In: Hofheinz D, Rosen A (eds.) Theory of Cryptography - 17th International Conference, TCC 2019, Nuremberg, Germany, December 1-5, 2019, Proceedings, Part I. LNCS, vol. 11891, pp. 229–250. Springer. https://doi.org/10.1007/978-3-030-36030-6_10

Brakerski Z, Shmueli O (2020) Scalable pseudorandom quantum states. In: Micciancio D, Ristenpart T (eds.) Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part II. LNCS, vol. 12171, pp. 417–440. Springer. https://doi.org/10.1007/978-3-030-56880-1_15

Cavalar B, Goldin E, Gray M, Hall P, Liu Y, Pelecanos A (2023) On the computational hardness of quantum one-wayness. CoRR **abs/2312.08363**[SPACE] https://doi.org/10.48550/ARXIV.2312.08363arXiv:2312.08363

Coladangelo A, Liu J, Liu Q, Zhandry M (2021) Hidden cosets and applications to unclonable cryptography. In: Malkin T, Peikert C (eds.) Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12825, pp. 556–584. Springer. https://doi.org/10.1007/978-3-030-84242-0_20

Cao S, Xue R (2022) On constructing one-way quantum state generators, and more. IACR Cryptol. ePrint Arch., 1323

Döttling N, Müller-Quade J, Nascimento ACA (2012) IND-CCA secure cryptography based on a variant of the LPN problem. In: Wang X, Sako K (eds.) Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings. LNCS, vol. 7658, pp. 485–503. Springer. https://doi.org/10.1007/978-3-642-34961-4_30

Gertner Y, Kannan S, Malkin T, Reingold O, Viswanathan M (2000) The relationship between public key encryption and oblivious transfer. In: 41st Annual Symposium on Foundations of Computer Science, FOCS 2000, 12-14 November 2000, Redondo Beach, California, USA, pp. 325–335. IEEE Computer Society. https://doi.org/10.1109/SFCS.2000.892121

Grilo AB, Lin H, Song F, Vaikuntanathan V (2021) Oblivious transfer is in miniqcrypt. In: Canteaut A, Standaert F (eds.) Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part II. LNCS, vol. 12697, pp. 531–561. Springer. https://doi.org/10.1007/978-3-030-77886-6_18

Goldreich O (1990) A note on computational indistinguishability. Inf. Process. Lett. 34(6):277–281. https://doi.org/10.1016/0020-0190(90)90010-U

Grover L, Rudolph T (2002) Creating superpositions that correspond to efficiently integrable probability distributions

Gilbert H, Robshaw MJB, Seurin Y (2008) How to encrypt with the LPN problem. In: Aceto L, Damgård I, Goldberg LA, Halldórsson MM, Ingólfsdóttir

A, Walukiewicz I (eds.) Automata, Languages and Programming, 35th International Colloquium, ICALP 2008, Reykjavik, Iceland, July 7-11, 2008, Proceedings, Part II - Track B: Logic, Semantics, and Theory of Programming & Track C: Security and Cryptography Foundations. LNCS, vol. 5126, pp. 679–690. Springer. https://doi.org/10.1007/978-3-540-70583-3_55

Håstad J, Impagliazzo R, Levin LA, Luby M (1999) A pseudorandom generator from any one-way function. SIAM J. Comput. 28(4):1364–1396. https://doi.org/10.1137/S0097539793244708

Hhan M, Morimae T, Yamakawa T (2023) From the hardness of detecting superpositions to cryptography: Quantum public key encryption and commitments. In: Hazay C, Stam M (eds.) Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part I. LNCS, vol. 14004, pp. 639–667. Springer. https://doi.org/10.1007/978-3-031-30545-0_22

Haitner I, Nguyen M, Ong SJ, Reingold O, Vadhan SP (2009) Statistically hiding commitments and statistical zero-knowledge arguments from any one-way function. SIAM J. Comput. 39(3):1153–1218. https://doi.org/10.1137/080725404

Impagliazzo R (1995) A personal view of average-case complexity. In: Proceedings of the Tenth Annual Structure in Complexity Theory Conference, Minneapolis, Minnesota, USA, June 19-22, 1995, pp. 134–147. IEEE Computer Society. https://doi.org/10.1109/SCT.1995.514853

Impagliazzo R, Rudich S (1989) Limits on the provable consequences of one-way permutations. In: Johnson DS (ed.) Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washigton, USA, pp. 44–61. ACM. https://doi.org/10.1145/73007.73012

Jain A, Krenn S, Pietrzak K, Tentes A (2012) Commitments and efficient zero-knowledge proofs from learning parity with noise. In: Wang X, Sako K (eds.) Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings. LNCS, vol. 7658, pp. 663–680. Springer. https://doi.org/10.1007/978-3-642-34961-4_40

Ji Z, Liu Y, Song F (2018) Pseudorandom quantum states. In: Shacham H, Boldyreva A (eds.) Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III. LNCS, vol. 10993, pp. 126–152. Springer. https://doi.org/10.1007/978-3-319-96878-0_5

Kiltz E, Masny D, Pietrzak K (2014) Simple chosen-ciphertext security from low-noise LPN. In: Krawczyk H (ed.) Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014. Proceedings. LNCS, vol. 8383, pp. 1–18. Springer. https://doi.org/10.1007/978-3-642-54631-0_1

Koshiba T, Odaira T (2009) Statistically-hiding quantum bit commitment from approximable-preimage-size quantum one-way function. In: Childs AM, Mosca M (eds.) Theory of Quantum Computation, Communication, and Cryptography, 4th Workshop, TQC 2009, Waterloo, Canada, May 11-13, 2009, Revised Selected Papers. LNCS, vol. 5906, pp. 33–46. Springer,. https://doi.org/10.1007/978-3-642-10698-9_4

Koshiba T, Odaira T (2011) Non-interactive statistically-hiding quantum bit commitment from any quantum one-way function. arXiv preprint arXiv:1102.3441

Kretschmer W, Qian L, Sinha M, Tal A (2022) Quantum cryptography in algorithmica. CoRR **abs/2212.00879**[SPACE]https://doi.org/10.48550/arXiv.2212.00879arXiv:2212.00879

Kretschmer W (2021) Quantum pseudorandomness and classical complexity. In: Hsieh M (ed.) 16th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2021, July 5-8, 2021, Virtual Conference. LIPIcs, vol. 197, pp. 2–1220. Schloss Dagstuhl - Leibniz-Zentrum für Informatik. https://doi.org/10.4230/LIPIcs.TQC.2021.2

Katz J, Shin JS, Smith AD (2010) Parallel and concurrent security of the HB and hb^+ protocols. J. Cryptol. 23(3):402–421. https://doi.org/10.1007/s00145-010-9061-2

Khurana D, Tomer K (2023) Commitments from quantum one-wayness. IACR Cryptol. ePrint Arch., 1620

Lyubashevsky V (2005) The parity problem in the presence of noise, decoding random linear codes, and the subset sum problem. In: Chekuri C, Jansen K, Rolim JDP, Trevisan L (eds.) Approximation, Randomization and Combinatorial Optimization, Algorithms and Techniques, 8th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems, APPROX 2005 and 9th InternationalWorkshop on Randomization and Computation, RANDOM 2005, Berkeley, CA, USA, August 22-24, 2005, Proceedings. LNCS, vol. 3624, pp. 378–389. Springer. https://doi.org/10.1007/11538462_32

Mahmoody M, Maji HK, Prabhakaran M (2014) On the power of public-key encryption in secure computation. In: Lindell Y (ed.) Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings. LNCS, vol. 8349, pp. 240–264. Springer. https://doi.org/10.1007/978-3-642-54242-8_11

May A, Meurer A, Thomae E (2011) Decoding random linear codes in $\tilde{\mathcal{O}}(2^{0.054n})$. In: Lee DH, Wang X (eds.) Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings. LNCS, vol. 7073, pp. 107–124. Springer. https://doi.org/10.1007/978-3-642-25385-0_6

Micciancio D, Peikert C (2013) Hardness of SIS and LWE with small parameters. In: Canetti R, Garay JA (eds.) Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I. LNCS, vol. 8042, pp. 21–39. Springer. https://doi.org/10.1007/978-3-642-40041-4_2

Morimae T, Yamakawa T (2022) One-wayness in quantum cryptography. IACR Cryptol. ePrint Arch., 1336

Morimae T, Yamakawa T (2022) Quantum commitments and signatures without one-way functions. In: Dodis Y, Shrimpton T (eds.) Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part I. LNCS, vol. 13507, pp. 269–295. Springer. https://doi.org/10.1007/978-3-031-15802-5_10

Mazor N, Zhang J (2021) Simple constructions from (almost) regular one-way functions. In: Nissim K, Waters B (eds.) Theory of Cryptography - 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8-11, 2021, Proceedings, Part II. LNCS, vol. 13043, pp. 457–485. Springer. https://doi.org/10.1007/978-3-030-90453-1_16

Naor M (1991) Bit commitment using pseudorandomness. J. Cryptol. 4(2):151–158. https://doi.org/10.1007/BF00196774

Pietrzak K (2012) Cryptography from learning parity with noise. In: Bieliková M, Friedrich G, Gottlob G, Katzenbeisser S, Turán G (eds.) SOFSEM 2012: Theory and Practice of Computer Science - 38th Conference on Current Trends in Theory and Practice of Computer Science, Špindlerův Mlýn, Czech Republic, January 21-27, 2012. Proceedings. LNCS, vol. 7147, pp. 99–114. Springer. https://doi.org/10.1007/978-3-642-27660-6_9

Renner R, König R (2005) Universally composable privacy amplification against quantum adversaries. In: Kilian J (ed.) Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005, Proceedings. Lecture Notes in Computer Science, vol. 3378, pp. 407–425. Springer. https://doi.org/10.1007/978-3-540-30576-7_22

Yan J (2022) General properties of quantum bit commitments (extended abstract). In: Agrawal S, Lin D (eds.) Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part IV. LNCS, vol. 13794, pp. 628–657. Springer. https://doi.org/10.1007/978-3-031-22972-5_22

Yao AC (1982) Theory and applications of trapdoor functions (extended abstract). In: 23rd Annual Symposium on Foundations of Computer Science, Chicago, Illinois, USA, 3-5 November 1982, pp. 80–91. IEEE Computer Society. https://doi.org/10.1109/SFCS.1982.45

Yan J, Weng J, Lin D, Quan Y (2015) Quantum bit commitment with application in quantum zero-knowledge proof (extended abstract). In: Elbassioni KM, Makino K (eds.) Algorithms and Computation - 26th International Symposium, ISAAC 2015, Nagoya, Japan, December 9-11, 2015, Proceedings. LNCS, vol. 9472, pp. 555–565. Springer. https://doi.org/10.1007/978-3-662-48971-0_47

Yu Y, Zhang J (2021) Smoothing out binary linear codes and worst-case sub-exponential hardness for LPN. In: Malkin T, Peikert C (eds.) Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part III. LNCS, vol. 12827, pp. 473–501. Springer. https://doi.org/10.1007/978-3-030-84252-9_16

Yu Y, Zhang J, Weng J, Guo C, Li X (2019) Collision resistant hashing from sub-exponential learning parity with noise. In: Galbraith SD, Moriai S (eds.) Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part II. LNCS, vol. 11922, pp. 3–24. Springer. https://doi.org/10.1007/978-3-030-34621-8_1

Publisher's Note