A Study of the Use of Euler Totient Function in RSA Cryptosystem and the Future of RSA Cryptosystem

Shuodong Wang

Faculty of Mathematical Sciences, University College London, London, United Kingdom, WC1E 6BT

vincent.wang.21@ucl.ac.uk

Abstract. At the end of the last century, an innovative two-key cryptosystem called RSA was created due to booming demand for secure remote communication. The core for this encryption system is a mathematical function called the Euler totient function (Euler φ function), introduced by Leonhard Euler. This article will first deduce four theorems related to Euler φ function, and then illustrate the correctness of the RSA cryptosystem using Euler's φ function. The study then starts with well-known RSA attacks such as the Coppersmith attack, assesses some of RSA's vulnerabilities, and measures the impact of quantum technologies on RSA. Finally, this study provides projections and recommendations for the future development of RSA based on all evaluation studies completed during the entire research program.

Keywords: RSA, Euler totient function, quantum technology, cryptography.

1. Introduction

Swiss mathematician Leonhard Euler introduced the Euler φ function in 1763. It is a function that takes an input value of any positive integer, then outputs the number of positive integers smaller or equal than this given positive integer and are coprime to it. For example φ (5)=4 , which means that there are 4 positive integers in the interval [1,5] that are coprime to 5, indeed since 1,2,3,4 are all coprime to 5. By further studying some properties of the Euler totient function, the base of the RSA algorithm becomes clear, which was introduced by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. The correctness of RSA can also be examined using analytic number theory. However, with the development of cryptanalytics and quantum technology, the limitations of RSA are beginning to show and there is some need for more secure cryptosystems. This research focuses on assessing the weaknesses of RSA, as well as investigating the potential impact of quantum technologies on RSA. Through this research, we have a more evaluative view of the RSA cryptosystem, and the relationship between quantum technology and RSA is clearer, thus providing better insights for the future development of secure communication systems.

2. The Euler φ function

We denote by $\varphi(n)$ the number of positive integers not greater than n and coprime with n, which is equivalent to

$$\varphi(n) = \# \{1 \leq a \leq n \mid \gcd(a, n) = 1\} \qquad (*)$$

which is also equivalent to $\varphi(n) = \# \{[a] \in \mathbb{Z}/n\mathbb{Z} | [a] \text{is invertible}\}$, where $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots \ldots [n-1]\}$, $[a] = \{a + kn | k \in \mathbb{Z}\}$.

There are four key theorems related to the Euler φ function:

Theorem 1 Consider m,n which are two positive integers and are coprime, then

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \tag{1}$$

Proof for theorem 1:

We define three sets

$A = \{1 \le a \le mn - 1 | \gcd(a, mn) = 1\}$

$B = \{1 \le b \le m - 1 | \gcd(b, m) = 1\}$

$C = \{1 \le c \le n - 1 | \gcd(c, n) = 1\}$

Based on previous definition（*）

$$\# A = \varphi(mn), \# B = \varphi(m), \# C = \varphi(n) \tag{2}$$

Given an element $a \in A, a = mq_1 + r_1 = nq_2 + r_2$, for some integers q_1, r_1, q_2, r_2, and $r_1 \in [1, m-1], r_2 \in [1, n-1]$

We define a function $\psi: A \to B \times C$ then $\psi(a) = (r_1, r_2)$, where $r_1 \in B, r_2 \in C$

For $(b, c) \in B \times C$

And by Chinese remainder theorem, there exists a unique $x, 0 \le x \le mn - 1$

That

$$x \equiv b \bmod m \text{ and } x \equiv c \bmod n \text{ for } \gcd(m, n) = 1 \tag{3}$$

Consider another function $\phi: B \times C \to A$, so $\phi(b, c) = x$, therefore ϕ is the inverse of ψ, and the order of set A is the same as the order of $B \times C$, hence

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \tag{4}$$

Theorem 2 If p is a prime number, then

$$\varphi(p^r) = p^r - p^{r-1} \tag{5}$$

Proof for theorem 2:

According to previous definition（*）

$$\begin{aligned} \varphi(p^r) &= \# \{1 \le a \le p^r - 1 | \gcd(a, p^r) = 1\} \\ &= \# \{1 \le a \le p^r - 1 | p \nmid a\} \\ &= (p^r - 1) - (p^{r-1} - 1) \\ &= p^r - p^{r-1} \end{aligned} \tag{6}$$

Theorem 3 If m is a natural number, then

$$\varphi(m) = m \cdot \prod_{p|m} \left(1 - \frac{1}{p}\right) \tag{7}$$

Proof for theorem 3:

According to the fundamental theorem of arithmetic

$$\varphi(m) = \varphi(\prod p_i^{a_i}) (\text{the prime decompsition of m}) \tag{8}$$

$$\begin{aligned} \text{Based on theorem 1,} \quad &= \prod \varphi(p_i^{a_i}) \\ \text{Based on theorem 2,} \quad &= \prod p_i^{a_i} - p_i^{a_i - 1} \\ &= \prod p_i^{a_i} (1 - 1/p_i) \\ &= \prod p_i^{a_i} \cdot \prod_{p|m} \left(1 - \frac{1}{p}\right) \\ &= m \cdot \prod_{p|m} (1 - \frac{1}{p}) \end{aligned} \tag{9}$$

Theorem 4 If $\gcd(a, m) = 1$, then

$$a^{\varphi(m)} \equiv 1 \bmod m \tag{10}$$

Proof for theorem 4:

Proof involves knowledge of group theory:

Define the set G to be the elements in $\mathbb{Z}/m\mathbb{Z}$ that are invertible, therefore $\# G = \varphi(m)$

So according to Lagrange lemma, for any $g \in G, g^{\# G}$ is the identity element of G, which is $[1]$. Therefore

$$g^{\varphi(m)} \equiv 1 \bmod m \tag{11}$$

3. Rivest-Shamir-Adleman (RSA) in data transmission and proof of correctness using the Euler φ function

RSA is a special cryptosystem with a two-key system, with one public key and one private key, both necessary for the system to operate properly. The message may be encrypted by all users using the public key but one cannot reverse the encryption process without the private key, making RSA an ideal system when the two people are apart and cannot physically meet to agree with a keyword.

Messages encrypted using the RSA cryptosystem is nearly impossible to decrypt due to the difficulty of factorizing the product of two large prime numbers, and there're no existing efficient algorithm to do so. Another base of the RSA is the fact that there exist large positive integers e, d, n such that for any natural numbers $m, 0 \leq m < n$ we have

$$m^{ed} \equiv m \bmod n \tag{12}$$

To prove the correctness of this fact is pretty straightforward using theorem 4. Here we want to show that $m^{ed} \equiv m \bmod n$ for all natural numbers m, and $n = uv$, where u, v are prime numbers, moreover, $ed \equiv 1 \bmod \varphi(n)$, these conditions will be explained later on. As e, d are positive integers, $ed = 1 + h\varphi(n)$ for some non-zero integer h, if we assume m, n are coprime, then we have

$$m^{ed} = m^{1+h\varphi(n)} = m \cdot (m^{\varphi(n)})^h \tag{13}$$

And due to Theorem 4, $m^{\varphi(n)} \equiv 1 \bmod n$

Hence,

$$m^{ed} = m^{1+h\varphi(n)} = m \cdot (m^{\varphi(n)})^h \equiv m \cdot 1^h \equiv m \bmod n \tag{14}$$

Furthermore, knowing m, e, n doesn't help with finding the value of d at all, given the large values of these integers. Therefore e, n would be distributed as part of the public key, while d is kept secret as the private key.

The operation of the RSA contains four steps, key generation, key distribution, encryption and decryption.

Key generation

To generate the public key and private key, one starts by choosing two large prime numbers u, v, then computes n, by $n = u \times v$, then calculates the value of $\varphi(n)$, which is also $\varphi(u) \times \varphi(v)$, and as u, v are prime numbers, $\varphi(u) = u - 1, \varphi(v) = v - 1$, so $\varphi(n) = (u-1) \times (v-1)$, then we choose an integer e, where $1 < e < \varphi(n)$, and $\varphi(n), e$ are coprime, this is an extra step to make the encryption process more efficient, as e would have a much shorter bit length, the conventional choice for the value of e is $2^{16} + 1$, which is 65537, and finally we find $d \equiv e^{-1} \bmod \varphi(n)$, which can also be efficiently done by existing algorithm. Therefore, out of all the values generated, $\varphi(n), u, v, d$ are kept as part of the private key, and n, e are part of the public key.

key distribution

Once the key has been generated, it has to be distributed to another user so that the two users can communicate privately using RSA. For example, if Alice and Bob have agreed to use RSA, Alice first sends her public key (n, e) to Bob and it is not necessary for this transmission to be secret. Bob then encrypts the message using Alice's public key and sends the encrypted message to her. And even if another person, Eve, intercepts the message from Bob, it is hard for her to decrypt the message as she doesn't have Alice's private key (d). Once Alice has received the message from Bob, she may decrypt it using her private key and read the message.

encryption

To encrypt the message, Bob needs to begin by transforming the message into numbers m, using a padding scheme that has to be agreed upon by both Alice and Bob. Then Bob obtains the ciphertext c by computing $\mathrm{m}^{\mathrm{e}} \equiv \mathrm{c} \bmod \mathrm{n}$, which can be efficiently done.

decryption

To decrypt the ciphertext c, Alice uses her private key and computes $\mathrm{c}^{\mathrm{d}} \equiv \mathrm{m}^{\mathrm{e}^{\mathrm{d}}} \equiv \mathrm{m} \bmod \mathrm{n}$, and then transforms m back into the original message using the padding scheme shared by both.

4. Limitations of RSA and an insight to the future

The RSA is a relatively mature and reliable cryptosystem, and it is known to be computationally secured, as theoretically it would be possible to crack the system if one managed to factorize n and obtain the two prime numbers u, v, so the biggest weakness of the RSA lies in the computational power of the attacker's computer and the efficiency of the factoring algorithm to factorize n.

The key idea in both the RSA scheme and the Rabin scheme is the selection of an appropriate trapdoor function; an easy to evaluate function f such that x is not easily computable from f(x), unless some extra information is known.[1] In the case of RSA, this trapdoor function is the Euler totient function, due to its numerical nature. Known attacks on the traditional RSA cryptosystems utilizes theorems from mathematics. The idea behind this weakness is the fact that f is a trapdoor function does not rule out the possibility of computing x from f(x) when x is of a special form.[1] Following this logic, one of the first strongest attacks on RSA known as the coppersmith attack, which shows that RSA encryption with exponent 3 is vulnerable if the opponent knows two-thirds of the message, or if two messages agree over eight-ninths of their length. [2]

Another important weakness of the RSA is that it is semantically insecure, which means that one can differentiate two ciphered texts if given the corresponding plaintexts, therefore attacks can be initiated targeting at this. In 1995, Paul Carl Kocher described an attack on RSA: if the attacker Eve has sufficient details of Alice's hardware, and is able to measure the decryption times of several known ciphertexts, she can then deduce the decryption key d. [3] With the development of internet, eight years later, Dan Boneh and David Brumley proposed a more practical attack over a network connection, and they showed that Kocher's timing attack is possible even if the attacker is far from the victim's hardware.[4]

These attacks all turned out to be very threatening to the security of RSA. However RSA remained strong until now because these attacks are not completely unavoidable. For attacks targeting the numerical weakness of the RSA, such as the coppersmith attack, an adjustment can be made to the trapdoor function to ensure higher security. An example is that S. Goldwasser and S. Micali suggested that the notion of Trapdoor Functions can be replaced by Probabilistic Encryption.[1] In addition, timing attacks and online timing attacks against RSA can be prevented if the key information about the hardware and internet connection is secured, and the encryption of the RSA method itself remains strong.

Compared to these known weaknesses of RSA, what's more threatening to RSA is the emergence of quantum technology, especially quantum computing and quantum communication.

On the one hand, quantum computing posts a direct threat to the heart of RSA, Shor's algorithm. Shor's algorithm (1994) for factoring numbers into their prime factors (15 = 3 × 5, for example) can be shown to be substantially more efficient than any known classical algorithm—and it's immediately applicable to cryptographic attacks on prime-number-based encryption, such as the RSA algorithm widely used in internet security.[5] And a quantum computer has been theoretically proven to be much more efficient than a classical computer at running Shor's algorithm. Therefore, the birth of the quantum computer sadly means the death of RSA, as the Euler totient function, will lose its property of being a practical trapdoor function. As for quantum communication, it posts a threat to RSA in a rather indirect manner. It appears to be a better alternative to secure communication. A quantum communication system exploits superposition and the probabilistic nature of quantum measurements to create a cryptographically secure information channel. Therefore, the eavesdropper can interfere with the communication of the key, but can't steal it.[6] Even more encouraging is the development of quantum communication. Unfortunately, however, this is not that great for the survival of RSA. The technology in this area has made good progress. In Australia, for example, a government quantum network project was launched in 2013 to link Parliament with other government agencies in Canberra. China is currently a world leader in the development of quantum communications. In 2016, China launched the world's first quantum communication satellite (QUESS, or Mozi/Mozi) and realized QKD (Quantum Key Distribution) connecting two ground stations 2,600 kilometers apart.[7] Many believe that quantum communication will be possible in the near future.

One of the biggest obstacles to quantum technology is decoherence, the loss of quantum coherence. When trying to design quantum computers, decoherence can greatly reduce the consistency of results. The more steps of calculation, the greater the chance of getting decoherent interventions, so it can be difficult to turn proof-of-concept demonstrations into systems that solve real-world problems. Davies et al. still have not made significant progress in solving the decoherence problem.[5] Therefore, real-life quantum computing remains a distant goal. In addition, decoherence can also cause problems with quantum communication. Quantum communication over long distances will lose some information due to loss of coherence. The current main solution to this problem is to re-encrypt the signal multiple times during transmission, or through a quantum communication satellite like China's Mozi Project, which will greatly reduce the chance of decoherence since there is little intervening matter in space. However, both solutions are very expensive and difficult to maintain, so unless absolute security is required, it is unlikely that quantum communication will replace all classical means of communication in the near future.

5. Conclusion

RSA is a very delicate system, its delicacy is highlighted by the carefully selected trapdoor function, Euler φ function and its special design of a two-key cryptosystem. Although there are weaknesses that can be targeted due to the mathematical properties of its core, the Euler totient function, the system can always be improved with the development of cryptanalytic technologies. However, if we set eyes on the bigger picture, development of cryptanalytic technologies not only leads to improvements of cryptosystem, it also breeds sneakier attacks on cryptosystems, so the key to approach to the ultimate security in communication lies on quantum technology, because of the fundamental property of quantum communication, and the outstanding computation power that is theoretically achievable by a quantum computer, once these are put into practice, there will be very little chance for RSA to remain as the main way to secure messages.

This research looked into the mathematical basis of the RSA encryption system, and studied the weaknesses of the RSA, evaluated the potential impact of quantum technology on RSA, and finally a prediction about the RSA encryption system was made. During this research, we focused on the impact of quantum technology on the RSA, as a competitive substitute. However there are other cryptanalytic systems that have very mathematically sophisticated designs, so we couldn't carry out very thorough research on the impact of quantum technology on these systems, such as the AES encryption. An ideal follow-up research would be to work with a specialized mathematician and further study the link between quantum technology and some more advanced cryptosystems.

References

[1] S. Goldwasser and S. Micali, "Probabilistic encryption & how to play mental poker keeping secret all partial information", Annual ACM Symposium on Theory of Computing, 1982.

[2] Coppersmith, Don "Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities" (PDF). Journal of Cryptology. 10 (4): 233, 1997

[3] Paul C. Kocher "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", LNCS,volume 1109, 1995, https://link.springer.com/chapter/10.1007/3-540-68697-5_9

[4] David Brumley, Dan Boneh, "Remote timing attacks are practical" (PDF). Proceedings of the 12th Conference on USENIX Security Symposium. SSYM'03. 2003

[5] Davies, Andrew, Patrick Kennedy. “QUANTUM COMPUTING.” From Little Things: Quantum Technologies and Their Application to Defence. Australian Strategic Policy Institute, 2017. http://www.jstor.org/stable/resrep16820.6.

[6] Davies, Andrew, and Patrick Kennedy. “QUANTUM COMMUNICATION.” From Little Things: Quantum Technologies and Their Application to Defence. Australian Strategic Policy Institute, 2017. http://www.jstor.org/stable/resrep16820.5.

[7] https://phys.org/news/2021-01-world-quantum-network.html