A TYPE OF POST–QUANTUM CRYPTOGRAPHIC ALGORITHM

Hong Dung Luu[1,*]

Abstract

The article proposes a type of post–quantum cryptographic algorithm based on hash function and One–Time Pad cipher. Due to inheriting a property called "perfect secrecy" of the One-Time Pad cipher, the algorithms constructed according to the method proposed here can resist various types of attacks with the help of quantum computers. In addition to high security, algorithms of this type also have the ability to authenticate the origin and integrity of the encrypted messages. On the other hand, the one-time key for encryption/decryption is established for each individual message while the management and distribution of the shared secret key between the sender/encryptor and receiver/decryptor is performed similar to symmetric – key cryptosystems being applied in practice.

Index terms

Symmetric key cryptography, encryption-authentication algorithm, OTP cipher, block cipher, post–quantum cryptography; quantum–resistant cryptography.

1. Introduction

The concept of "post-quantum cryptography" or "quantum-resistant cryptography" can be understood as cryptographic algorithms that are capable of resisting attacks with the help of quantum computers. Currently, the development of post-quantum cryptographic algorithms is being strongly promoted with many different approaches [1]–[25]. This article proposes a type of post-quantum cryptographic algorithm based on a property called "perfect secrecy" of the One-Time Pad (OTP) cipher. For currently widely used cryptosystems such as DES, AES, etc., a brute-force attack with the help of quantum computers is completely feasible, because once the entire key space has been exhaustively searched, the attacker will definitely receive a meaningful message and that is the plaintext being looked for. But with OTP cipher, the problem is completely different. When an attacker performs an exhaustive key search attack, he will receive countless meaningful messages whose size does not exceed the size of the ciphertext. Obviously, in this case the attacker cannot know which post-decrypted message is the plaintext attacker needs to find, this is the factor that creates perfect secrecy of the OTP cipher. The type of post-quantum cryptographic algorithm

[1] Institute of Information and Communication Technology, Le Quy Don Technical University

[*] Corresponding author, email: luuhongdung@gmail.com

DOI: 10.56651/lqdtu.jst.v13.n01.818.ict

proposed here constructed based on the perfect secrecy of OTP cipher to resist attacks with the help of quantum computers.

2. The proposed type of post–quantum cryptographic algorithm

The type of post-quantum cryptographic algorithm proposed here constructed based on the encryption mechanism of OTP cipher to encrypt the message and the random characteristics of the output data of the hash function to generate keys. It includes: the Encryption algorithm (Algorithm 1) and the Decryption - Authentication algorithm (Algorithm 2), the construction method of these algorithms is presented in the following sections 2.1 and 2.2.

2.1. The Encryption algorithm

In proposed type of algorithm, the Encryption algorithm takes as input a plaintext P and a shared secret key K of the sender, here key K has size m bits. The plaintext P is encrypted as n data blocks $P_i(i = 1, 2, .., n)$ of size m bits:

$$P = \{P_1, P_2, \dots, P_n\}$$

The one-time key K_{EOT} used to encrypt plaintext P consists of n subkeys $K_{ei}(i = 1, 2, .., n)$ whose size corresponds to the size of the plaintext block:

$$K_{EOT} = \{K_{e1}, K_{e2}, \dots, K_{en}\}$$

The output data of the Encryption algorithm includes the following components:

- C: The ciphertext includes n data blocks $C_i(i = 1, 2, .., n)$ of size m bits:
  $$C = \{C_1, C_2, \dots, C_n\}$$
- C_0: Component responsible for generates the one-time key K_{DOT} of the receiver.
- R: Component responsible for verifying the origin and the integrity of the post-decrypted message.

The Encryption algorithm is performed through the following steps:

- Step 1: Generate a data block P_0 of size m bits using the random/pseudo-random number generator $PRNG()$:
  $$P_0 = PRNG(1, 2, \dots, 2^m - 1)$$
- Step 2: Calculate the component C_0 from data block P_0 and key K by operator XOR:
  $$C_0 = P_0 \oplus K$$
- Step 3: Generate key K_{e0} from data block P_0 and key K by the hash function $H()$ has an output data size of m bits:
  $$K_{e0} = H(P_0||K)$$
- Step 4: Encrypt n data blocks of plaintext P:

```
for $i = 1$ to $n$ do
    begin
        $K_{ei} = H(P_{i-1} \parallel K_{ei-1} \parallel K_{e0})$
        $C_i = P_i \oplus K_{ei} \oplus K_{e0}$
    end
```

- Step 5: Generate component R from P_n and subkey K_{en} by the hash function $H()$:
  $R = H(P_n \parallel K_{en})$

The Encryption algorithm (Algorithm 1) is described as follows:

Algorithm 1 The Encryption algorithm.

```
Input: $P, K$.
Output: $C_0, C, R$.
$P_0 = PRNG(\{1, 2, \ldots, 2^m - 1\})$
$C_0 = P_0 \oplus K$
$K_{e0} = H(P_0 \parallel K)$
for $i = 1$ to $n$ do
    $K_{ei} = H(P_{i-1} \parallel K_{ei-1} \parallel K_{e0})$
    $C_i = P_i \oplus K_{ei} \oplus K_{e0}$
end for
$R = H(P_n \parallel K_{en})$
```

Note:

– Operator "$\oplus$" is a modulo 2 addition operation (XOR).

– Operator "$\parallel$" is the operation to concatenate bit strings.

– The hash function $H()$ here selectable as: MD5 [24], SHAx [25].

2.2. The Decryption - Authentication algorithm

The Decryption - Authentication algorithm whose input is ciphertext C, components C_0, R and the receiver's shared secret key K. The C ciphertext consists of n data blocks $C_i (i = 1, 2, .., n)$ of size m bits:

$$C = \{C_1, C_2, \ldots, C_n\}$$

The output of the algorithm is a post-decrypted message M consisting of n data blocks $M_i (i = 1, 2, .., n)$ of size m bits:

$$M = \{M_1, M_2, \ldots, M_n\}$$

The one-time key K_{DOT} used to decrypt the received message - similar to the sender side, consists of n subkeys $K_{di} (i = 1, 2, .., n)$ of size m bits:

$$K_{DOT} = \{K_{d1}, K_{d2}, \ldots, K_{dn}\}$$

The Decryption - Authentication algorithm is performed through the following steps:

- Step 1: Decrypt the component C_0 using the key K and the operator XOR:
  $M_0 = C_0 \oplus K$

- Step 2: Generate the key K_{d0} from the data block M_0 and the key K by the hash function $H()$ has an output data size of m bits:
  $K_{d0} = H(M_0||K)$
- Step 3: Decrypt the data blocks of ciphertext C to get post-decrypted message M:
  ```
  for $i = 1$ to $n$ do
      begin
          $K_{di} = H(M_{i-1} \parallel K_{di-1} \parallel K_{d0})$
          $M_i = C_i \oplus K_{di} \oplus K_{d0}$
      end
  ```
- Step 4: Generate the value V from subkey K_{dn} and data block M_n by $H()$:
  $V = H(M_n \parallel K_{dn})$
- Step 5: Check if $V = R$ then the integrity of the post-decrypted message M is authenticated. Otherwise, the message has been modified.

The Decryption - Authentication algorithm (Algorithm 2) is described as follows:

Algorithm 2 The Decryption algorithm

```
Input: $C_0, C, R, K$.
Output: $M, TRUE/FALSE$.
$M_0 = C_0 \oplus K$
$K_{d0} = H(M_0 \parallel K)$
for $i = 1$ to $n$ do
    $K_{di} = H(M_{i-1} \parallel K_{di-1} \parallel K_{d0})$
    $M_i = C_i \oplus K_{di} \oplus K_{d0}$
end for
$V = H(M_n \parallel K_{dn})$
if $V = R$ then
    return $(M, TRUE)$
else
    return $(M, FALSE)$
end if
```

Note:
– If the return is $(M, TRUE)$, then the post-decrypted message M is exactly the plantext P, that is: $M = P$.
– If the return is $(M, FALSE)$, the post-decrypted message has been modified, that is: $M \neq P$.

2.3. The correctness of the proposed type of algorithm

What needs to be proved here is: if the received ciphertext is exactly the sent ciphertext, then the post-decrypted message is also the plaintext: $M = P$ and the conditions: $V = R$ will be satisfied. Therefore, after decryption, if the condition: $V = R$ is satisfied, the receiver can confirm with certainty about the origin and integrity of the received message.

Indeed, since the sender's shared secret key and the receiver's shared secret key is only one and the value C_0 received is also the value C_0 sent, so we have:

$$M_0 = C_0 \oplus K = P_0 \oplus K \oplus K = P_0$$

and:

$$K_{d0} = H(M_0||K) = H(P_0||K) = K_{e0}$$

Because $M_0 = P_0, K_{d0} = K_{e0}$ and how to generate subkey $K_{ei}(i = 1, 2, .., n)$ of sender: $K_{ei} = H(P_{i-1} \parallel K_{ei-1} \parallel K_{e0})$ is also the way to generate the subkey $K_{di}(i = 1, 2, .., n)$ of the receiver: $K_{di} = H(M_{i-1} \parallel K_{di-1} \parallel K_{d0})$. Infer that the key K_{DOT} of the receiver is also the key K_{EOT} of the sender. From here we have the first thing to prove:

$$M = C \oplus K_{DOT} = C \oplus K_{EOT} = P \oplus K_{EOT} \oplus K_{EOT} = P$$

And there's the second thing to prove:

$$V = H(M_n \parallel K_{dn}) = H(P_n \parallel K_{en}) = R$$

2.4. Some evaluation of the secure level of the proposed type of algorithm

Similar to the OTP cipher, the K_{EOT}/K_{DOT} keys here is only used once for each encrypted message, so types of attacks such as differential cryptanalysis, linear cryptanalysis, etc. and in general all known attack types for typical block ciphers such as DES, AES,... are not effective with the proposed type of algorithm. The secure level of the proposed type of algorithm is assessed by its ability to resist some typical attacks as follows:

– *Ciphertext-only attack*: According to C. E. Shannon's theory of perfect secrecy [26], if the key K_{EOT}/K_{DOT} is a random bit sequence, there will not be any relationship between the plaintext and the ciphertext, then: $Probability(P|C) = Probability(P)$ and the proposed algorithm will have "perfect secrecy" similar to the OTP cipher. This can be understood in way: a "brute force" attack can decrypt a received ciphertext into any meaningful message whose size/length does not exceed the size/length of the ciphertext. Since there is no relationship between the plaintext and the ciphertext, there is no information in the ciphertext that would allow an attacker (cryptanalyst) to select the plaintext from the post-decrypted meaningful messages. For the attacker, all post-decrypted messages are likely to be the plaintext attacker is looking for. Therefore, the attacker cannot find the plaintext from the post-decrypted messages. In the proposed type of algorithm, a hash function is used to generate the keys K_{EOT}/K_{DOT}, since the size of the subkeys K_i (128/256/512 bits) is very small compared to the repetition period of data at the output of the hash function, so it is possible to completely meet the requirement of randomness of the key. Therefore, the proposed type of algorithm can resist the "brute force" attack when the attacker only knows the ciphertext even with the help of quantum computers.

– *Known-plaintext attack*: Assuming that with the help of quantum computers, the one-way nature of the hash function used in the algorithm can be broken, then from a known subkey K_{ei} the attacker can find ($P_{ei-1} \parallel K_{ei-1} \parallel K_{e0}$). Although P_{ei-1} is known, it does not allow the attacker to find the shared secret key K, because both K_{e0} and $K_{ei-1}(i = 2, 3, .., n)$ here are random (secret) values. It can be clearly seen that this case is completely similar to the Ciphertext-only attack case mentioned above. Furthermore, unlike the OTP cipher, with the type of algorithm proposed here, even if the plaintext is public, the attacker cannot calculate the one-time key K_{EOT}/K_{DOT}. Thus, even if the one-way nature of the hash function is broken, the attacker will not have a chance to attack the secret key. In addition, if for some reason the attacker knows the first data block of the plaintext, the attacker cannot decrypt the remaining data blocks of the ciphertext.

– *Spoofing attack*: The OTP cipher does not provide verification for an encrypted message, so an attacker could block the ciphertext sent and send the recipient a fake ciphertext of the same size. In the case of decrypt to a meaningless message, the receiver may speculate that the tampering was done or caused by a communication error. However, if decrypt to a meaningful message, then the receiver has no way to know whether the post-decrypted message is true or fake. With the proposed type of algorithm, the origin and the integrity of the post-decrypted message are verified by the condition: $V = R$.

An issue that needs to be considered here is how much does the algorithm's resistance to spoofing attacks depend on the collision resistance of the hash function used in this algorithm? It can be clearly seen that the authentication mechanism of this type of algorithm is completely different from the authentication mechanism of the digital signature algorithm. For the digital signature algorithm, the input data to the authentication function are the message and the signature to be verified, along with the signer's public key, so if an attacker can create a message has the hash value identical to the hash value of a previously signed message, then the spoofing attack is successful. Therefore, the collision resistance of the hash function is decisive for the resistance to spoofing attacks ability of the digital signature algorithm. With this type of algorithm, the input data of the authentication function are the components C_0, C, R and the shared secret key K. Therefore, if the hash function used in this algorithm has such weak collision resistance that the attacker can create a meaningful message, whose hash value matches the hash value of the plaintext P, the spoofing attack cannot be performed. Thus, it can be seen that the weak collision resistance of the hash function along with the high speed of quantum computers does not have any significance for the resistance to spoofing attacks ability of the proposed algorithm.

3. Conclusions

The type of post–quantum cryptographic algorithm proposed here are developed based on the OTP cipher and hash function. The advantage of these algorithms of this type is that their secure and performance are inherited from the OTP cipher, so they can resist types of attacks with the help of quantum computers. In addition, because of the mechanism to authenticate the origin and integrity of the encrypted message, the proposed type of algorithm can resist types of spoofing attacks, which is one of the basic requirements that practical applications posed.

References

[1] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," *SIAM journal on Computing*, vol. 26, no. 5, 1997, pp. 1510–1523. doi: 10.1137/S0097539796300933

[2] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical review letters*, vol. 68, no. 21, 1992, p. 3121. doi: 10.1103/PhysRevLett.68.3121

[3] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of cryptology*, vol. 5, 1992, pp. 3–28. doi: 10.1007/BF00191318

[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical computer science*, vol. 560, pp. 7–11, 2014.

[5] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, 2017, pp. 188–194. doi: 10.1007/978-3-540-88702-7

[6] A. Broadbent and C. Schaffner, "Quantum cryptography beyond quantum key distribution," *Designs, Codes and Cryptography*, vol. 78, 2016, pp. 351–382. doi: 10.1007/s10623-015-0157-4

[7] C. Elliott, "Quantum cryptography," *IEEE Security and Privacy*, vol. 2, no. 4, 2004, p. 57–61. doi: 10.1109/MSP.2004.54

[8] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of modern physics*, vol. 74, no. 1, 2002, p. 145. doi: 10.1103/RevModPhys.74.145

[9] L. K. Grover, "From schrödinger's equation to the quantum search algorithm," *American Journal of Physics*, vol. 69, no. 7, 2001, pp. 769–777. doi: 10.1007/s12043-001-0128-3

[10] S. S. Mehrdad, "Quantum cryptography: An emerging technology in network security," in *Technologies for Homeland Security (HST), IEEE International Conference*, 2011, pp. 13–19, doi:10.1109/THS.2011.6 107 841.

[11] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, 1999, pp. 303–332. doi: 10.1137/S0097539795293172

[12] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?" *IEEE Security & Privacy*, vol. 16, no. 5, 2018, pp. 38–41. doi: 10.1109/MSP.2018.3761723

[13] L. Chen, S. Jordan, Y.-K. Liu ..., and D. Smith-Tone, *Report on post-quantum cryptography*. US Department of Commerce, National Institute of Standards and Technology, vol. 12, 2016.

[14] T. Takagi, "Recent developments in post-quantum cryptography," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 101, no. 1, 2018, pp. 3–11. doi: 10.1587/transfun.E101.A.3

[15] S. K. Sehgal and R. Gupta, "Quantum cryptography and quantum key," in *2021 International Conference on Industrial Electronics Research and Applications (ICIERA).* IEEE, 2021, pp. 1–5, doi:10.1109/ICIERA53 202.2021.9 726 722.

[16] A. Cohen, R. G. D'Oliveira, S. Salamatian, and M. Médard, "Network coding-based post-quantum cryptography," *IEEE journal on selected areas in information theory*, vol. 2, no. 1, 2021, pp. 49–64. doi: 10.1109/JSAIT.2021.3054598

[17] O. S. Althobaiti and M. Dohler, "Quantum-resistant cryptography for the internet of things based on location-based lattices," *IEEE Access*, vol. 9, 2021, pp. 133 185–133 203. doi: 10.1109/ACCESS.2021.3115087

[18] I. P. A. E. Pratama and I. G. N. A. K. Adhitya, "Post quantum cryptography: Comparison between RSA and McEliece," in *2022 International Conference on ICT for Smart Society (ICISS).* IEEE, 2022, pp. 01–05, doi: 10.1109/ICISS55 894.2022.9 915 232.

[19] E. Lella, A. Gatto, A. Pazienza ..., and G. Schmid, "Cryptography in the quantum era," in *2022 IEEE 15th Workshop on Low Temperature Electronics (WOLTE).* IEEE, 2022, pp. 1–4 doi: 10.1109/WOLTE55 422.2022.9 882 585.

[20] J. Pinto, "Post-quantum cryptography," *ARIS2-Advanced Research on Information Systems Security*, vol. 2, no. 2, 2022, pp. 4–16, doi: 10.56 394/aris2.v2i2.17.

[21] A. C. Chen, "Post-quantum cryptography neural network," in *2023 International Conference on Smart Systems for applications in Electrical Sciences (ICSSES).* IEEE, 2023, pp. 1–6, doi: 10.1109/ICSSES58 299.2023.10 201 083.

[22] S. K. Sood and Pooja, "Quantum computing review: A decade of research," *IEEE Transactions on Engineering Management*, vol. 71, pp. 6662–6676, 2023. doi: 10.1109/TEM.2023.3284689

[23] J. Jency Rubia, R. Babitha Lincy, N. Ezhil E, C. Sherin Shibi, and A. Rosi, "A survey about post quantum cryptography methods," *EAI Endorsed Transactions on Internet of Things*, vol. 10, Feb. 2024. doi: 10.4108/eetiot.5099

[24] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 2018.

[25] *Federal information processing standards publication 180-4*. National Institute of Standards and Technology, 2015.

[26] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, 1949, pp. 656–715. doi: 10.1002/j.1538-7305.1949.tb00928.x

Manuscript received 19-03-2024; Accepted 25-06-2024. ■

Hong Dung Luu graduated in Radio Electronics in 1989 and PhD in 2013 at Le Quy Don Technical University. Currently working in the Institute of Information and Communication Technology, Le Quy Don Technical University. Research field: Cryptography and information security. E-mail: luuhongdung@gmail.com.

MỘT DẠNG THUẬT TOÁN MẬT MÃ HẬU LƯỢNG TỬ

Lưu Hồng Dũng

Tóm tắt

Bài báo đề xuất một dạng thuật toán mật mã hậu lượng tử dựa trên hàm băm và OTP (One–Time Pad) cipher. Do được thừa kế một đặc tính được gọi là "độ mật hoàn thiện" của OTP cipher, các thuật toán được xây dựng theo phương pháp đề xuất ở đây có thể chống lại các kiểu tấn công với sự trợ giúp của máy tính lượng tử. Ngoài tính bảo mật cao, các thuật toán dạng này còn có khả năng xác minh nguồn gốc và tính toàn vẹn của bản tin được mã hóa. Mặt khác, khóa sử dụng một lần cho việc mã hóa/giải mã được thiết lập cho từng bản tin riêng biệt còn việc quản lý và phân phối khóa bí mật chia sẻ giữa người gửi/mã hóa và người nhận/giải mã được thực hiện tương tự như các hệ mật khóa đối xứng đang được ứng dụng trong thực tế.

Từ khóa

Mật mã khóa đối xứng, thuật toán mã hóa–xác thực, mật mã OTP, mật mã khối, mật mã hậu lượng tử, mật mã kháng lượng tử.