Unconditionally secure encryption algorithm with unified confidentiality and integrity

Zhen-Hu Ning
College of Computer Science,
Beijing University of Technology, Beijing 100124, China

Abstract One-Time Pad (OTP), introduced by Shannon, is well-known as an unconditionally secure encryption algorithm and has become the cornerstone of modern cryptography. However, the unconditional security of OTP applies solely to confidentiality and does not extend to integrity. Hash functions such as SHA2, SHA3 or SM3 applies only to integrity but not to confidentiality and also can not obtain unconditional security. Encryption and digital signatures based on asymmetric cryptography can provide confidentiality, integrity and authentication, but they can only achieve computational security. Leveraging the fundamental principles of quantum mechanics，Quantum key distribution（QKD）can achieve unconditional security in theory. However, due to limitations in eavesdropping detection, the use of classical channels and imperfections in quantum devices, it cannot reach unconditional security in practical applications. In this paper, based on polynomial rings and the theory of probability, we propose an unconditionally secure encryption algorithm with unified confidentiality and integrity. The main calculation of the encryption algorithm is Cyclic Redundancy Check(CRC). Theoretical analysis proves that the encryption algorithm not only meets the unconditional security of confidentiality, but also guarantees the unconditional security of integrity, especially suitable for high-security communications such as finance, military, government and other fields.

Keywords encryption algorithm, unconditionally secure, unified confidentiality and integrity

1 Introduction

With the rapid development of cloud computing, the internet of things (IoT) and blockchain technologies,etc, cryptography has become increasingly important. Cryptographic algorithms provide essential services such as confidentiality, integrity, and authentication, which are critical for secure data storage and communication. Among all the algorithms, One-Time Pad (OTP), introduced by Shannon[1, 2, 3], is well-known as an unconditionally secure encryption algorithm and has become the cornerstone of modern cryptography. However, the unconditional security of OTP applies solely to confidentiality and does not extend to integrity. Hash functions, mainly including MD5、SHA1、SHA2、SHA3 and SM3, applies solely to integrity and does not suitable to confidentiality. Moreover, the security of hash functions rely on special design structure, such as Merkle-Damgard, Sponge Construction or complex mathematical operations. Due to the complex-

E-mail address: ningzhenhu@bjut.edu.cn, nzh41034@163.com.

ity of the algorithm design, it is inevitable that design flaws may be possibly introduced, making the algorithms susceptible to cryptanalysis and collision attacks. MD5 and SHA-1 algorithms have been successfully broken by Wang [4, 5]. Therefore, hash functions are also not unconditionally secure.

Asymmetric cryptographic algorithms rely on mathematical problems that are computationally difficult for classical computers to solve. For example, RSA is based on the difficulty of factoring large integers , Elliptic Curve Cryptography(ECC) relies on the discrete logarithm problem over elliptic curves. Post-quantum cryptographic(PQC) algorithms are based on hard problems such as LWE and SIS, etc. However, with the development of Quantum computing, these hard problems will no longer be difficult. In 1994, Shor[6, 7] proposed a polynomial time quantum algorithm for solving integer factorization problem and the discrete logarithm problem. In 1996, Lov Grover[8] proposed a polynomial time algorithm efficiently solving the problem of searching an unsorted database with a quadratic speedup. Chen[9] claims that they proposed a polynomial time quantum algorithm for solving LWE problem with certain polynomial modulus-noise ratios. Although their algorithm has been reviewed and found to be flawed, it is highly possible that these hard problems will be cracked on some day in future. In a nutshell, PQC is designed based on mathematical hard problems that cannot be solved in polynomial time by known quantum algorithms and its security relies on computational complexity. However, whether the mathematical problems that PQC depends on will remain intractable in future, whether the algorithm's security will remain valid in the long term and whether it will still be immune to newly emerging quantum attacks are all unknown. And so PQC has also certain vulnerabilities and uncertainties.

Quantum cryptographic algorithms or protocols leverage the principles of quantum mechanics to ensure secure communication, such as quantum no-cloning theorem, quantum uncertainty principle and quantum superposition. Quantum key distribution (QKD), which can achieve unconditional security in theory, is a crucial protocol within quantum cryptography for securely distributing keys between communicating parties. Representative QKD protocols include the BB84 protocol[10], the B92 protocol[11], the EPR protocol[12], measurement-device-independent QKD protocol[13] and Twin-field quantum key distribution (TF-QKD) protocol[14, 15, 16], etc. However, quantum cryptographic protocols face several challenges and limitations in practical applications. First, while eavesdropping detection is theoretically possible, in practice, factors such as channel noise can allow eavesdroppers to obtain partial information undetected. Second, quantum cryptographic protocols rely on classical channels for certain communication processes[17, 18], making the entire system vulnerable to security issues associated with classical channels. Additionally, imperfections in physical devices are a significant concern. Practical quantum devices may have defects[19, 20, 21, 22, 23]that can be exploited by attackers to launch various attacks, thereby compromising the security of the protocol. In a word, although quantum cryptographic protocols offer information-theoretic security in theory, practical implementations often require compromises due to technological limitations, device imperfections and compatibility issues with existing communication networks. Thereby, Quantum cryptographic algorithms or protocols are also not unconditionally secure.

Considering the issues of above algorithms, we propose an unconditionally secure encryption algorithm with unified confidentiality and integrity based on polynomial rings and the theory of probability, which don't rely on complex construction design, mathematical hard problems or the principles of quantum mechanics. The main calculation of the encryption algorithm is CRC. The encryption algorithm not only meets the unconditional security of confidentiality, but also

guarantees the unconditional security of integrity at the same time.

2 Preliminaries

Let $GF(2)[x]$ be a polynomial ring[31]. Then

a). For any $f \in GF(2)[x]$,

$$f = \sum_{i=0}^{n} a_i x^i \quad for\ some \quad a_i = 0\ or\ 1 (0 \le i \le n),\ n \ge 0. \tag{2.1}$$

b). For any $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{n} b_i x^i \in GF(2)[x]$,

$$f + g = \sum_{i=0}^{n} ((a_i + b_i) \mod 2)\, x^i. \tag{2.2}$$

c). For any $f(x) = \sum_{i=0}^{m} a_i x^i$, $g(x) = \sum_{i=0}^{n} b_i x^i \in GF(2)[x]$,

$$fg = f * g = \sum_{i=0}^{m+n} \left(\left(\sum_{k+j=i}^{i} a_k b_j \right) \mod 2 \right) x^i. \tag{2.3}$$

Let $f \in GF(2)[x]$ and $\deg(f)$ be the degree of f, then

$$\deg(f) = n \Leftrightarrow f = x^n + \sum_{i=0}^{n-1} a_i x^i \tag{2.4}$$

for $n \ge 0$. Specially, $\deg(0) = -\infty$.

Define

$$GF(2^n) = \{f \mid f \in GF(2)[x]\ with\ \deg(f) < n\}, \tag{2.5}$$

for $n \ge 1$.

Define the irreducible polynomial f by

$$f \in GF(2)[x]\ with\ \deg(f) \ge 1, \tag{2.6}$$

and

$$\gcd(f(x), g(x)) = 1\ for\ any \quad g(x) \in GF(2^n)\ with\ \deg(g) < \deg(f), g(x) \ne 0. \tag{2.7}$$

Define the set of irreducible polynomials $IGF(n)$ by

$$IGF(n) = \{f \mid f \in GF(2)[x]\ is\ an\ irreducible\ polynomial\ with\ \deg(f) = n\}, \tag{2.8}$$

for $n \ge 1$.

Let $f, g, r \in GF(2)[x]$ with $\deg(f) \ge \deg(g) \ge 1$ and $\deg(r) < \deg(g)$. Define

$$r = f \mod g \Longleftrightarrow f = hg + r\ for\ some\ h \in GF(2)[x]. \tag{2.9}$$

Let S be a finite set and $|S|$ be the cardinality of S.

3 Key Lemmas

Lemma 3.1. *Let S be a finite set and $|S| \geq 4$. Let $A \subset S$ be a subset. Let $x \in S$ be given uniformly and randomly. Then*

$$P(x \in A) = \frac{|A|}{|S|}. \tag{3.1}$$

Proof Note that

$$P\{x = x_i\} = \frac{1}{|S|}, \quad \forall x_i \in S. \tag{3.2}$$

Assume that $A = \{x_1, x_2, ..., x_k\}$. Then

$$P(x \in A) = \sum_{i=1}^{i=k} P(x = x_i) = \frac{|A|}{|S|}. \tag{3.3}$$

□

Lemma 3.2. *Let $m \geq n \geq 4$. Let $N(x) \in GF(2^{m+1})$, $N \neq 0$. Define*

$$S_N = \{g \mid g \in IGF(n) \text{ and } N \mod g = 0\}. \tag{3.4}$$

Then

$$|S_N| \leq \frac{m}{n}. \tag{3.5}$$

Proof If S_N is empty, then

$$|S_N| = 0 \leq \frac{m}{n}. \tag{3.6}$$

If S_N is not empty, it is assumed that

$$S_N = \{g_1, g_2, ..., g_k\}. \tag{3.7}$$

Then

$$N \mod \prod_{i=1}^{k} g_i = 0, \tag{3.8}$$

which implies

$$\deg(N) \geq n|S_N|. \tag{3.9}$$

Then

$$|S_N| \leq \frac{\deg(N)}{n} \leq \frac{m}{n}. \tag{3.10}$$

□

Lemma 3.3. *Let $m \geq n \geq 4$ and $m < 2^n$. Let $N(x) \in GF(2^{m+1})$, $N \neq 0$. Let $f(x) \in IGF(n)$ be given uniformly and randomly. Then*

$$P(N \mod f = 0) \leq \frac{m}{2^n}(1 + \epsilon), \tag{3.11}$$

where $\epsilon = \epsilon(n) > 0$ and $\epsilon(n) << 1$ for $n << 2^n$.

Proof Define

$$S_N = \{g \mid g \in IGF(n) \text{ and } N \mod g = 0\}. \tag{3.12}$$

Then

$$N \mod f = 0 \Leftrightarrow f \in S_N. \tag{3.13}$$

It follows from Möbius inversion formula[31] that

$$\begin{aligned} |IGF(n)| = & \frac{1}{n}\sum_{d|n}\mu(d)2^{n/d} \\ & \geq \frac{1}{n}(2^n - \sum_{i=1}^{n/2} 2^i) \\ & = \frac{2^n - 2^{(n/2+1)} + 2}{n}, \end{aligned} \tag{3.14}$$

where $\mu(x)$ is the Möbius function. Then it follows from (3.1) and (3.5) that.

$$P(N \mod f = 0) = P(f \in S_N) = \frac{|S_N|}{|IGF(n)|} \leq \frac{m}{2^n}(1+\epsilon), \tag{3.15}$$

where $\epsilon = \epsilon(n) > 0$ and $\epsilon(n) < 2^{(-\frac{n}{2}+2)}$ for $n \geq 16$. □

Remark 3.1. *We give some examples of* $\epsilon(n)$.

$$\epsilon(32) < 2^{-14}, \quad \epsilon(64) < 2^{-30}, \quad \epsilon(128) < 2^{-62}, \quad \epsilon(256) < 2^{-126} \quad \textit{and} \quad \epsilon(512) < 2^{-254}. \tag{3.16}$$

Remark 3.2. *We give some examples of* (m, n).

$$n = 32, n \leq m \leq 2^{16}; \quad n = 64, n \leq m \leq 2^{32}; \tag{3.17}$$

$$n = 128, n \leq m \leq 2^{64}; \quad n = 256, n \leq m \leq 2^{128}; \quad \textit{and} \quad n = 512, n \leq m \leq 2^{256}. \tag{3.18}$$

Remark 3.3. *Let* $N(x) \in GF(2)[x]$ *with* $\deg(N) = m$. *Let* $f(x) \in IGF(n)$ *be given uniformly and randomly. Then it follows from Lemma 3.3 that*

$$P(N \mod f = 0) \leq \frac{m}{2^n}(1+\epsilon), \tag{3.19}$$

where $\epsilon = \epsilon(n) > 0$ *and* $\epsilon(n) << 1$ *for* $n << 2^n$.

Remark 3.4. *Let* $N_1(x), N_2(x), ..., N_k(x) \in GF(2^{m+1})$, $N_1, N_2, ..., N_k \neq 0$ *and*

$$N = \prod_{i=1}^{k} N_i. \tag{3.20}$$

Let $f(x) \in IGF(n)$ *be given uniformly and randomly. Note that* $N \in GF(2^{km+1})$ *and*

$$\bigvee_{i=1}^{k} (N_i \mod f = 0) \Leftrightarrow N \mod f = 0. \tag{3.21}$$

Then it follows from Lemma 3.3 that

$$P\left(\bigvee_{i=1}^{k} (N_i \mod f = 0)\right) = P(N \mod f = 0) \leq \frac{km}{2^n}(1+\epsilon), \tag{3.22}$$

where $\epsilon = \epsilon(n) > 0$ *and* $\epsilon(n) << 1$ *for* $n << 2^n$.

4 Unconditional security with integrity

Theorem 4.1. *Let $n \geq 256$. Let $N(x) \in GF(2)[x]$ with $\deg(N) = m+1$ be given with some distribution, where $n \leq m \leq 2^{\frac{n}{2}}$. Let $f(x) \in IGF(n)$ be given uniformly and randomly. Assume that N, f are mutually independent. Let*

$$r(x) = N(x) \mod f(x). \tag{4.1}$$

Assume that N is public, f, r are private and m, n, the distribution of N, the distribution of f are constants, then the unconditional security with integrity holds.

Proof It follows from Bayesian Theorem that

$$P(f|N) = P(f). \tag{4.2}$$

Let $N'(x) \in GF(2)[x]$ with $\deg(N') = m+1$, $N' \neq N$. We estimate the probability that N' is mistaken for N as follows.

Let

$$r'(x) = N'(x) \mod f(x). \tag{4.3}$$

Note that

$$(N' - N) \in GF(2^{m+1}),\ (N' - N) \neq 0, \tag{4.4}$$

and

$$r' = r \Leftrightarrow (N' - N) \mod f = 0. \tag{4.5}$$

From Lemma 3.3, we have

$$P(r' = r) = P\left((N' - N) \mod f = 0\right) \leq \frac{m}{2^n}(1+\epsilon), \tag{4.6}$$

where $0 < \epsilon << 1$. □

Remark 4.1. *It follows from (4.6) that*

$$P(r' = r) \leq 2^{-\frac{n}{2}+1}. \tag{4.7}$$

Then

$$P(r' = r) \leq 2^{-127}\ for\ n = 256, n \leq m \leq 2^{128}, \tag{4.8}$$

and

$$P(r' = r) \leq 2^{-255}\ for\ n = 512, n \leq m \leq 2^{256}. \tag{4.9}$$

Remark 4.2. *Assume that N is public and f, r are stored securely, m, n are stored as constants by User A. Then Theorem 4.1 guarantees any other users will fall to tamper with N.*

5 Unconditional security with unified confidentiality and integrity

Theorem 5.1. *Let $m \geq n \geq 256$ and $m \leq 2^{\frac{n}{2}}$. Let $N(x) \in GF(2)[x]$ with $\deg(N) = m+1$ be given with some distribution. Let $f(x) \in IGF(n)$ be given uniformly and randomly. Let $Key(x) \in$*

$GF(2)[x]$ with $\deg(Key) = m + n + 1$ be given uniformly and randomly for OTP. Assume that N, f, Key are mutually independent. Let

$$r(x) = x^n N(x) \mod f(x), \tag{5.1}$$

$$X(x) = x^n N(x) + r(x). \tag{5.2}$$

Then

$$X \mod f = 0. \tag{5.3}$$

Let

$$EX = X + Key. \tag{5.4}$$

Assume that EX is public, N, f, Key, r, X are private and m, n, the distribution of N, the distribution of f, the distribution of Key are constants, then the unconditional security with unified confidentiality and integrity holds.

Proof .

Unconditional security with confidentiality: It follows from Perfect Secrecy[2] that $P(X|EX) = P(X)$. Then $P(N|EX) = P(N)$ and $P(f|EX) = P(f)$. That is, the only way to crack EK is guessing.

Unconditional security with integrity: Let $EX' \in GF(2^{m+1})$ and $EX' \neq EX$. We estimate the probability that EX' is mistaken for EX as follows.

Let

$$X' = EX' + Key, \tag{5.5}$$

$$X'' = X' - X = EX' - EX. \tag{5.6}$$

Note that

$$X''(x) \in GF(2^{m+n+1}),\ X'' \neq 0, \tag{5.7}$$

and

$$X' \mod f = 0 \Leftrightarrow X'' \mod f = 0. \tag{5.8}$$

Then it follows from Lemma 3.3 that

$$P(X' \mod f = 0) = P(X'' \mod f = 0) \leq \frac{m+n}{2^n}(1+\epsilon), \tag{5.9}$$

where $0 < \epsilon << 1$.

Remark 5.1. *Assume that f, Key are shared and stored securely and m, n are shared and stored as constants by User A and User B. User A sends EK to User B via public networks. Then Theorem 5.1 guarantees that any other users will fall to crack and tamper with EK.*

6 Discussion

The main computation of Theorem 4.1 and Theorem 5.1 is

$$N(x) \mod f(x), \tag{6.1}$$

where $N(x) \in GF(2)[x]$ with $\deg(N) = m + 1$ and $f(x) \in IGF(n)$. The calculation (6.1) is equivalent to CRC of m-bit data with n-bit generator polynomial. Due to high computational

efficiency and low resource usage, CRC[24, 25, 26, 27, 28, 29, 30] has become an international standard and is spreadly used to check errors during data storage and data transmission. Therefore, the algorithms in Theorem 4.1 and Theorem 5.1 are extremely convenient to implement.

The results of this paper also apply to the polynomial ring $GF(q)[x](q \geq 2$ is a prime) [31] and the integer ring Z [32]. By a similar analysis with Lemma 3.3, Theorem 4.1 and Theorem 5.1, we have the following conclusions.

For the polynomial ring $GF(q)[x](q \geq 2$ is a prime):

Let $IGF_q(n)$ be the set of irreducible polynomials with degree n and leading coefficient 1 in $GF(q)[x]$.

Lemma 6.1. *Let $m \geq n \geq 4$ and $m < q^n$. Let $N(x) \in GF(q^{m+1})$, $N \neq 0$. Let $f(x) \in IGF_q(n)$ be given uniformly and randomly. Then*

$$P(N \mod f = 0) \leq \frac{m}{q^n}(1+\epsilon), \tag{6.2}$$

where $\epsilon = \epsilon(n) > 0$ and $\epsilon(n) << 1$ for $n << q^n$.

Theorem 6.1. *Let $n \geq 256$. Let $N(x) \in GF(q)[x]$ with $\deg(N) = m+1$ and leading coefficient 1 be given with some distribution, where $n \leq m \leq q^{\frac{n}{2}}$. Let $f(x) \in IGF_q(n)$ be given uniformly and randomly. Assume that N, f are mutually independent. Let*

$$r(x) = N(x) \mod f(x). \tag{6.3}$$

Assume that N is public, f, r are private and m, n, the distribution of N, the distribution of f are constants, then the unconditional security with integrity holds.

Theorem 6.2. *Let $m \geq n \geq 4$ and $m < q^n$. Let $N(x) \in GF(q)[x]$ with $\deg(N) = m+1$ and leading coefficient 1 be given with some distribution. Let $f(x) \in IGF_q(n)$ be given uniformly and randomly. Let $Key(x) \in GF(q)[x]$ with $\deg(Key) = m+n+1$ and leading coefficient 1 be given uniformly and randomly for OTP. Assume that N, f, Key are mutually independent. Let*

$$r(x) = x^n N(x) \mod f(x), \tag{6.4}$$

$$X(x) = x^n N(x) + r(x), \tag{6.5}$$

and

$$EX = X - Key. \tag{6.6}$$

Assume that EX is public, N, f, Key, r, X are private and m, n, the distribution of f, the distribution of N, the distribution of Key are constants, then the unconditional security with unified confidentiality and integrity holds.

For the integer ring Z :

Let $IS(n)$ be the set of primes in $(2^n, 2^{n+1})$. With Prime number theorem[32], we have the following estimates.

Lemma 6.2. *Let $m \geq n \geq 4$ and $m < 2^n$. Let N be an integer satisfying $1 \leq N \leq 2^m$. Let $f \in IS(n)$ be given uniformly and randomly. Then*

$$P(N \mod f = 0) \leq \frac{m \ln 2}{2^n}(1+\epsilon), \tag{6.7}$$

where $\epsilon = \epsilon(n) > 0$ and

$$\lim_{n \to +\infty} \epsilon(n) = 0. \tag{6.8}$$

Theorem 6.3. *Let $n \geq 256$. Let $N \in (2^m, 2^{m+1})$ be an integer and be given with some distribution, where $n \leq m \leq 2^{\frac{n}{2}}$. Let $f \in IS(n)$ be given uniformly and randomly. Assume that N, f are mutually independent. Let*

$$r = N \mod f. \tag{6.9}$$

Assume that N is public, f, r are private and m, n, the distribution of N, the distribution of f are constants, then the unconditional security with integrity holds.

Theorem 6.4. *Let $m \geq n \geq 256$ and $m \leq 2^{\frac{n}{2}}$. Let $N \in (2^m, 2^{m+1})$ be an integer and be given with some distribution. Let $f \in IS(n)$ be given uniformly and randomly. Let $Key \in (2^{m+n+1}, 2^{m+n+2})$ be an integer and be given uniformly and randomly for OTP. Assume that N, f, Key are mutually independent. Let*

$$r = 2^{n+1}N \mod f, \tag{6.10}$$

$$X = 2^{n+1}N + r, \tag{6.11}$$

and

$$EX = X \oplus Key. \tag{6.12}$$

Assume that EX is public, N, f, Key, r, X are private and m, n, the distribution of N, the distribution of f and the distribution of Key are constants, then the unconditional security with unified confidentiality and integrity holds.

Remark 6.1. *Due to the famous unsolved problem: Riemann hypothesis, the accuracy of $\epsilon(n)$ in Z(Lemma 6.2) is weaker than $\epsilon(n)$ in $GF(q)[x]$(Lemma 6.1).*

7 Acknowledgements

Thanks for Professor Changxiang Shen for his outstanding work on Chinese Trusted Computing, which brings us important inspirations.

Thanks for Professor Yihua Zhou for his excellent insights into cryptography, which improve our work.

References

[1] C. E. Shannon(1948). A mathematical theory of communication. Bell Systems Technical Journal, 27, 379-423, 623-656.

[2] C. E. Shannon(1949). Communication theory of secrecy systems. Bell Systems Technical Journal, 28, 656-715.

[3] D.R. Stinson(2005). Cryptography: Theory and Practice, Third Edition. Champan & Hall/CRC.

[4] X. Wang, H. Yu. How to Break MD5 and Other Hash Functions. In: Cramer, R. (eds) Advances in Cryptology – EUROCRYPT 2005. EUROCRYPT 2005. Lecture Notes in Computer Science, vol 3494. Springer, Berlin, Heidelberg.

[5] X. Wang, Y. L. Yin, H. Yu. Finding Collisions in the Full SHA-1. In: Shoup, V. (eds) Advances in Cryptology – CRYPTO 2005. CRYPTO 2005. Lecture Notes in Computer Science, vol 3621. Springer, Berlin, Heidelberg.

[6] P. W. Shor(1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science. pp. 124 – 134

[7] Peter W. Shor. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing. 26 (5): 1484 – 1509

[8] L. K.Grover. A fast quantum mechanical algorithm for database search. In Proc. Twenty-Eighth Annual ACM Symposium on Theory of Computing 212 – 219 (Association for Computing Machinery, 1996.

[9] Y. Chen,(2024). Quantum Algorithms for Lattice Problems. *Cryptology ePrint Archive*, 2024/555. https://eprint.iacr.org/2024/555.

[10] C. H. Bennett, G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pages 175 – 179. IEEE, 1984

[11] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. Physical Review Letters, 68(21):3121 – 3124, 1992

[12] A. K. Ekert, Quantum cryptography based on Bell's theorem. Physical review letters 1991, 67, 6 661.

[13] H.-K. Lo, M. Curty, B. Qi, Measurement-Device-Independent Quantum Key Distribution.Physical review letters 2012, 108, 13 130503.

[14] S. Wang, ZQ. Yin, DY. He, et al. Twin-field quantum key distribution over 830-km fibre. Nat. Photon. 16, 154 – 161 (2022).

[15] W. Li, L. K. Zhang, Y. C. Lu, et al. Twin-Field Quantum Key Distribution without Phase Locking.Phys. Rev. Lett. 130, 250801(2023)

[16] Y. Zhou, R. Y. Wang, C. M. Zhang, et al. Sending-or-not-sending twin-field quantum key distribution with advantage distillation.Phys. Rev. Applied 21, 014036（2024）

[17] D. Gottesman, H.-K. Lo,(2003). Proof of security of quantum key distribution with two-way classical communications. IEEE Transactions on Information Theory, 49(2), 457 – 475.

[18] M. Stoilov, (2020). A classical attack on the coherent one way protocol for quantum key distribution. arXiv preprint arXiv:2003.07198

[19] L. Lydersen, C. Wiechers, C. Wittmann, et al. Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photon 4, 686 – 689 (2010)

[20] L. Lydersen, C. Wiechers, C. Wittmann , D. Elser, J. Skaar, V. Makarov, (2010). Thermal blinding of gated detectors in quantum cryptography. Optics Express, 18(26), 27938-27954.

[21] A. Q.Huang, A. Navarrete, S. H. Sun, P. Chaiwongkhot, M. Curty, V. Makarov, (2019). Laser-seeding attacks in quantum key distribution. Phys. Rev. Applied, 12(6), 064043.

[22] A. Vakhitov, V. Makarov, D. R. Hjelme,(2001). Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. J. Mod. Opt., 48(13), 2023-2038.

[23] X. L. Sun, F. H. Xu, M. S. Jiang, X. C. Ma, H. K. Lo, L. M. Liang, (2015). Effect of source tampering in the security of quantum cryptography. Phys. Rev. A, 92(2), 022304.

[24] W. W. Peterson, "A Pseudorandom Sequence Generator Based on Cyclic Redundancy Checks," IEEE Transactions on Electronic Computers, vol. EC-10, no. 4, pp. 430 – 431, Dec. 1961.

[25] W. W. Peterson, "Error Detecting Codes," IEEE Transactions on Information Theory, vol. IT-6, no. 3, pp. 198 – 201, Sept. 1960.

[26] D. A. Huffman, "The Cyclic Redundancy Check (CRC) and Its Applications," IEEE Transactions on Communications, vol. COM-32, no. 2, pp. 160 – 167, Feb. 1984.

[27] ISO/IEC 8073:1991, Information technology —Telecommunications and information exchange between systems —Data link layer —Medium Access Control (MAC) and Logical Link Control (LLC) —Frame structure, International Organization for Standardization (ISO), Geneva, Switzerland, 1991.

[28] ITU-T Rec. V.42, Error Correction in Subscriber Line Systems, International Telecommunication Union (ITU), Geneva, Switzerland, 1993.

[29] ISO/IEC 3309:2016, Information technology —Telecommunications and information exchange between systems —High-level data link control (HDLC) procedures —Frame structure, International Organization for Standardization (ISO), Geneva, Switzerland, 2016.

[30] IEEE 802.3-2018, IEEE Standard for Ethernet, IEEE, New York, NY, USA, 2018.

[31] R. Lidl, H. Niederreiter(1986). Introduction to finite fields and their applications. Cambridge University Press.

[32] S. Lang(2002),. Algebra (3rd ed.). Springer.