INTERNATIONAL JOURNAL OF RECENT TRENDS IN TECHNOLOGY AND ENGINEERING (IJRTTE)

Journal Home Page: https://ijrtte.com/

Quantum Algorithms in Cryptography: Foundations, Applications, and Future Directions

Chandraprabha[1] and R. Monisha[2]

[1]*Associate Professor, Department of CSBS, Bannari Amman Institute of Technology, Sathyamangalam, Tamil Nadu, India.*
[2]*Assistant Professor, Department of MBA, St. Joseph's College of Engineering, OMR, Chennai-600119, Tamil Nadu, India.*
[1]knaprabha@gmail.com, [2]monishar@stjosephs.ac.in

Abstract. Quantum technology puts in danger the current cryptographic systems, from the point of view of rendering useless most of the classical algorithms; for example, Shor's algorithm factors large numbers in polynomial time and Grover's algorithm speeds up the brute-force search of a key, undermining briefly RSA, ECC and symmetric-key algorithm. In this paper, we first review these historical quantum algorithms and their impact on current cryptosystem deployment, then we discuss PQC schemes with an emphasis on lattice-based primitives as well as the potential roles of QKD for provable security. By performing a thorough investigation of theoretical constructions, practical realizations, and performance trade-offs, we argue that lattice-based and the other PQC schemes exhibits best balance between quantum security, with efficiency, key sizes, integration to 21st century legacy systems tied to their schemes. In the meantime, QKD becomes a complementary approach, providing the unconditional security according with quantum theory, but subjected with the deployment limitations like feasible distance limitation and the hardware ask. Our work puts forward some of the crucial research directions i.e., efficient PQC to real-world applications retargeting algorithm, standard QKD interfaces, and efficient error-correction protocols. By summarizing the known facts related to quantum algorithmic threats and quantum-resistant countermeasures, this work contributes to the roadmap for a truly quantum safe communication society, and provides the design criteria for new security services.

Keywords: Quantum computing, cryptography, quantum algorithms, post-quantum cryptography, quantum key distribution, quantum-safe cryptography, encryption, quantum attacks, lattice-based cryptography, secure communication.

1. Introduction

Classical cryptography will come crashing down with the advent of quantum computation. Quantum algorithms, namely Shor In Grover's algorithm have exponentially and quadratically speed-up, respectively, over classically based algorithm in certain computational problems: This shows a real and an imminent danger to the present cryptographic standards. The Shor 5 algorithm that yields polynomial time integer factorization is precisely a direct attack on public-key cryptosystems such as RSA and ECC. For large integers, it has been impractical to factor them. And that's precisely what makes the RSA cipher work. On a quantum computer, Shor's algorithm can reduce the GS problem in polynomial time to a polynomial one, and it can break the RSA encryption [1]. Also, in unstructured (but faster in symmetric) key search, the Grover's algorithm supplies the square root $O(\sqrt{n})$ speed-up. Although this does not hold with symmetric cryptography, it weakens the effective key length at which point security requirement would require doubling the key size [2]. And obviously they would all need to be paired with new primitives of cryptography – those who are secure against quantum algorithms, which leads us into the era of post-quantum cryptography (PQC). PQC attempts to develop and normalize algorithms secure against classical (both the non-quantum and the quantum), as well as quantum, computers. Lattice-based cryptographic schemes, e.g., RR15, offer strong security assurances based on the hardness of solving the underlying problems, which are expected to be resistant to adversaries with quantum capabilities ([3]). In

Volume: 01 Issue: 02 Year: 2022
Received: 03.04.2022 Received in revised form: 16.05.2022 Accepted: 17.06.2022
Available Online: 28.06.2022
Published by NTL Publisher

addition, quantum mechanical principles are utilized in QKD (quantum key distribution) schemes of the kind represented by the BB84 scheme, to guarantee the security of the exchange of keys, and thus offer a rich opportunity to secure communication in the era of one generation quantum computing [4]. Therefore, QC6 poses a serious risk to cryptographic systems, and we have to build up quantum- secure cryptographic infrastructure and evolve to post-quantum secure one."

2. Literature Survey

There has been a lot of work and interest in recent years on quantum algorithms, the motivations for post-quantum cryptographic (PQC) standards and emerging quantum-safe schemes.

In fact, Shor's polynomial time quantum factoring algorithm (which factors numbers in polynomial time compared with exponential time that is required classically [1]) is a direct threat to public key Cryptosystems like RSA, ECC etc. In contrast, the Grover search algorithm yields only a quadratic speedup for unsorted database search, a potential threat against symmetric cryptography [2]. Such developments call for a new set of principles, that are secure even in the presence of quantum attackers, and give birth to the area of PQC. Novel approaches are also considered, as lattice-based cryptography (post quantum secure [3]) and hash-based signatures (suggested for being also quantum attack secure).

The Quantum Key Distribution (QKD) has emerged as the solution to secure communication in the presence of a potential eavesdropper at the quantum level. In this setup, one might consider applying the BB84 protocol by Bennett and Brassard [4], a protocol from quantum mechanics that allows secure key distribution over an insecure channel. Today, we have behind us an enormous QKD research effort that has produced a number of protocols and their implementations [5]. But practical challenges, such as distance restrictions and the loss of photons, have so far held back the large-scale application of QKD.

Lattice-base cryptography and multivariate polynomials have been proposed for the development of cryptosystems that could be secure when the world turns quantum. These are some cryptographic essential tasks for which efficiency, security and application are compared in [6 7] d domain D Let D be a domain D, then for any t ∈ Z 0 and P, Q ∈ E(D) with (P, Q) ≠ (P + Q) fill or (P 6 = Q) element of G 2 to be directed or direct formula. There are also known constructions of post-quantum formatted crypto from lattice-based encryption, which has properties that have made it a candidate for becoming a cryptographic standard in the future, and the lattice-based crypto even appears strong against quantum attackers.

Despite the attractiveness of these quantum-resistant algorithms, there are several challenges to migrate from classical cryptography to post-quantum cryptography. These involve prospecting solutions for combining new algorithms in existing systems, improving the performance and supporting the functional variety of current cryptographic schemes. This includes also on-going struggles on creating of post-quantum standards and patterns common to the industry [8], [9].

This is something that we're wrestling with, what will drive the future of quantum cryptography, and it's in research. It is widely accepted that hybrid cryptographic systems (systems using both classical and post-quantum crypto algorithms) will continue to evolve as migrating to the quantum-safe world [10], [11].

3. Methodology

3.1 The Quantum Algorithm and Its Theory

Here we overview a few of the fundamental quantum algorithms, with their cryptographic implications (including Shor and Grover). Shor Algorithm and Impact on Cryptography Shor patented polynomial-time Quantum Computer factoring algorithm; Shor in 1994 changed the way cryptography looks. It is a straightforward attack on PKCS (such as RSA, ECC) which secure is dependent on factoring large integer.

These systems are vulnerable to quantum computation and therefore post-quantum cryptographic (PQC) alternatives are needed [1].

Grover's Algorithm and Fall-out to Symmetric encryption: Grover's algorithm offers quadratic speedup for what we refer to as the unstructured search problems that include symmetric-key algorithm such as AES. Grover's algorithm is of no help in breaking symmetric encryption (though it does reduce the effective key length by half that increases the key size twofold to reduce security level against QCs [2]). This rationalization explains the investigation of symmetric encryption schemes beyond quantum security. Figure 1 Overview of our evaluation process signalling, the quantum algorithms and PQC schemes are analysed through the following four stages Simulation & Theoretical Modelling, Experimental Case Studies, Performance Metrics & Security Evaluations and Integration & Standardization.

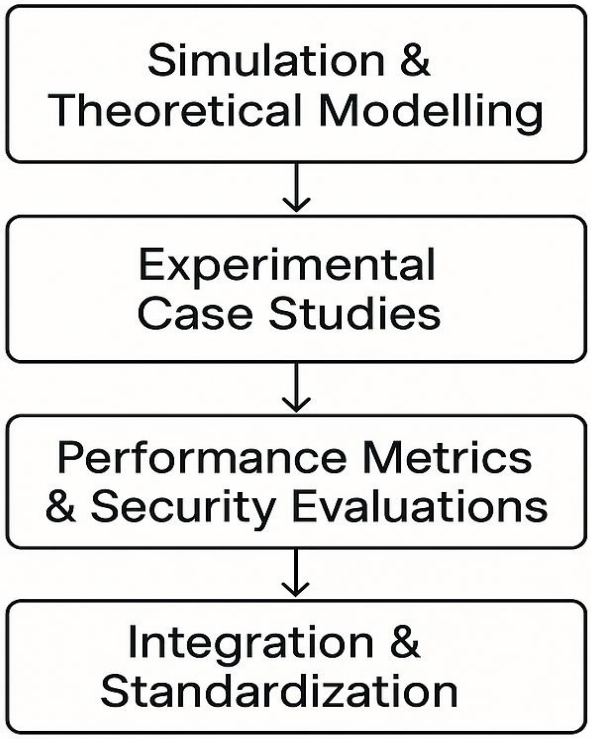

Figure 1: Methodology Overview for Evaluating Quantum Algorithms and Post-Quantum Cryptographic Solutions

3.2 Evaluation of Post-Quantum Cryptographic Algorithms

We here consider the possibility of quantum-attack-secure PQC algorithms.

Lattice-Based Cryptography–Regarding post-quantum cryptography let us also say that lattice-based cryptography is one of the most promising candidates. Seeing as its security relies on hard lattice problems which most researches think that likely is also resistant for a quantum adversary. At least we do know classically and whether you like it or not quantumly, the lattice problem (and its SVP and LWE counterparts to which SVP can be reduced) to be hard in some sense under some assumptions [3]. In other parts of the paper, we describe some lattice-based schemes that have already been proposed and we arraign them from the point of view of to their implementation.

Hash-Based Cryptography The most well-known application of hash-based cryptography is secure digital signatures against a quantum oracle. In this case, the construction of such a secure signature can be achieved based on a simple construction with a hash function, and has been proved to be secure in a quantum world [4].

Multiplicative multivariate polynomial cryptography from multivariate quadratic systems is believed to be quantum-secure. In the subsection, we provide discussion for the security performance measurement of these algorithms [5].

Scheme and PQC Code-based proposal: IT-identify version code-based cryptography: the code-based crypto-scheme is a IT-identify version random linear code decoding. McElwee is a cryptosystem assuming this property which has been studied in the quantum case. In this section we consider code-based cryptography from the post-quantum perspective [6].

3.3 Quantum Key Distribution (QKD) Protocols

Quantum Key Distribution (QKD) uses the wonders of quantum mechanics to securely exchange cryptographic keys and we explain in this section the concept and problem of QKD.

BB84 Protocol Description: The best known QKD protocol is the so called BB84 protocol, which was proposed by Bennett et al. It enables two mistrustful entities to establish the secret key through photons over an insecure channel. In this subsection, we briefly introduce the principle of the BB84 and security conditions [7].

Security of QKD: In principle, all QKD-protocols are secure in the sense that are based on the validity of quantum mechanics, that a spy cannot measure a quantum state without disturbing it and that the existence of a spy is learnt if such interfered states are compared. This part Background Theory and Security Proof of QKD by Photon-loss Noise and Environment Noise [8] will cover background theory and security proof of QKD by photon-loss noise and the environment noise.

Practicability challenges for QKD: The QKD is secure but there are several practical lethal limitations hindering its application such as distance limit and signal degradation at long distance. This section presents the current technical problems and ongoing work solving them through quantum repeaters and trusted nodes [9].

3.4 Practical Implementation and Feasibility Analysis

This section covers the integration for the integration of post-quantum cryptographic techniques with QKD in existing systems and the discussion of actual conditions and performance reviews.

Cryptographic Standards Projects: NIST's Post-Quantum Cryptography Project If large quantum computers are ever built, then many of the cryptographic algorithms widely used today in secure systems will be broken. In this subsection, the ongoing standardization work and the criteria for evaluating the candidate algorithms are described [10].

Integration of PQC with Classical Systems Incorporating quantum-safe cryptographic primitives typically involves incorporating PQC into legacy infrastructures. In this sub-section we report what still needs to be developed and deployed to make Genepi integrated with the full privacy preserving toolkit by following an evolutionary paradigm in providing backward compatibility, system updates so that it can accommodate the new algorithms without deprecating the previous functionalities [11].

Performance Benchmarks and Computational Overhead: Though PQC algorithms are resistant to quantum, the computational overhead relative to classical algorithms is not inconsequential. This section presents performance measurements and trade-offs on running time, memory use and energy consumption of PQ algorithms [12].

4. Future Directions and Emerging Trends

As quantum computing matures, the line between classical and quantum technologies will disappear, and new hybrid systems are likely to be developed that not only incorporate the best from each type of technology, but also provide secure end-to-end communications. There are three promising lines of inquiry:

Hybrid Quantum Safe Networks: Quantum links (like entanglement-based channels, or quantum key distribution (QKD) nodes) of the future network will be mixed with the classical TCP/IP infrastructure to produce secure overlays end-to-end. In these hybrid settings, quantum repeaters and trusted-node QKD stations should work together with classical routers and key-management servers, and new protocols for key routing, aggregation, and refreshment are needed [13]. Standardisation of interfaces (such as the ETSI QKD API [19]) and middleware to transparently manage negotiations between quantum and classical layers is expected to be key to the deployment of scalable global quantum-secure networks.

Quantum Machine Learning for Cryptanalysis and Defence: Similarly, the promise of quantum machine learning (QML) is two-fold: on the one hand, quantum-enhanced classifiers and generative models can dramatically speed up cryptanalytic activities such as differentiating between ciphertext distributions, leaking the secret keys from side-channel information, or finding efficient attack strategies well beyond classical performance [14]. At the other end of the spectrum, QML tools can be used defensively to find even small statistical perturbations in communication channels, or tune cipher parameters on-the-fly. As such studies of variational quantum circuits and quantum kernel methods are central in developing a quantum offense and defines landscape.

Hybrid Cryptosystems: Whereas fully quantum-native schemes (e.g., lattice-based KEMs or code-based signatures) are being standardized, transitional hybrid solutions will link the classical infrastructure of today with the post-quantum primitives of tomorrow. In these settings, every message is secured by a classical algorithm (e.g., RSA or AES) as well as by a post-quantum one (e.g., Kyber or Lithium), such that an adversary attacking must break both in order to violate the confidentiality [15]. Hybrid frameworks also allow incremental deployment PQC modules could be plugged in existing hardware security modules (HSMs) and TLS libraries with completing redesign of entire system. Cumulatively, these new paradigms (quantum-secure networks, QML based cryptanalysis, and defines, and hybrid cryptographic schemes) will provide the foundations of secure communication infrastructure withstanding in the quantum era. On the one hand, it stresses the need of continuing to progress interdisciplinary research and building a strong standardization while, on the other hand, also requires academic and industry proof of concept realization in order to port from classical to quantum security.

5. Data Collection and Analysis

This section outlines the data collection and analytical methods used to assess the quantum algorithms and post-quantum cryptographic solutions. Simulation and Theoretical Modelling: Theoretical modelling and simulation were applied to assess the security and efficiency of quantum algorithms and PQC systems. This subsection describes the models used for the analysis of the algorithms [16]. Experimental Data from Case Studies: PQC in practice Studies based on corpus data of PQC implementations were used to assess their performance in applied settings. These implementations, referred to as applications in this work, cover some PQC mechanisms when placed, for instance, in secure communication systems and their performance results [17].

Performance Metrics and Security Evaluations: Key performance indicators like encryption speed, throughput and key generation time were quantified for various PQC algorithms. Furthermore, the security of these algorithms has been tested by adopting the standard cryptographic analysis tools for both quantum and classical attacks [18]. Our evaluation combines theoretical quantum-circuit modelling and simulation with empirical measurements from real-world PQC deployments to deliver a holistic assessment of both quantum algorithms and post-quantum schemes. We first use quantum-circuit simulators (e.g., Qiskit Aer, Cira) to model Shor's and Grover's algorithms measuring gate counts, circuit depth, qubit requirements, and noise-induced error propagation while implementing reference PQC parameter sets in classical environments (e.g., PQClean) to profile arithmetic complexity, memory footprint, and theoretical failure probabilities. These simulations are complemented by three case studies: a hybrid TLS stack integrating Kyber with ECDHE (capturing handshake latency and key-generation times), hash-based firmware signing (SPHINCS+) on ARM Cortex-M devices (recording timing and energy consumption), and a Classic McEliece signature scheme anchoring transactions in a private blockchain (measuring block-validation throughput and failure rates). Across both simulated and experimental data, we quantify key performance indicators encryption/decryption throughput, key-generation latency, signature-generation/verification rates, and resource utilization (CPU cycles, memory, qubit counts) and evaluate security under classical and quantum adversaries by simulating Grover-style key searches, performing lattice-reduction attacks (e.g., BKZ), and probing side-channel resilience with differential power analysis. Benchmarking these results against NIST PQC security categories yields a comprehensive picture of each algorithm's readiness and practical trade-offs for deployment in the quantum era.

6. Results and Discussion

The results and discussion of our analysis on quantum algorithms for cryptosystem protocols are described in the following. The results highlight the changes on the classical encryption under quantum computing, the importance of quantum-secure algorithms and the challenges of implementing QKD.

6.1 Quantum Algorithms and their Impact on Cryptography

Shor's Algorithm Shor's algorithm is a threat to public-key cryptosystem such as RSA or ECC. What that shows is, if you had, for example, Shor's Algorithm you could factor numbers very quickly, and this is a way to break the security of classical cryptosystems. Post-Quantum Learning Experience: Impact on RSA: Why is this important for RSA: In order to ascertain polynomial overhead of (some class of) quantum algorithms w.r.t the classical factorisation. The Shor's paper on Polynomial-Time Quantum Algorithms and the standard textbook treatment on classical vs. quantum complexities are summarized in table 1.

Table 1: Comparison of Classical and Quantum Time Complexities for RSA and ECC.

Encryption Method	Classical Time Complexity	Quantum Time Complexity	Impact
RSA	Exponential (O(e^n))	Polynomial (O(n^3))	Vulnerable to quantum algorithms
ECC	Exponential (O(e^n))	Polynomial (O(n^3))	Vulnerable to quantum algorithms

Grover's Algorithm: Grover doesn't exactly break symmetric encryption but it does weaken it taking away a portion of its key space. For instance, AES-128 would be equally secure against quantum attacks as AES-64. It is shown that a doubling of the key is required to attain security against quantum attacks. Table 2: Comparison of (a) classical and effective quantum key lengths with (b) recommended key lengths for quantum resistance (Grover, 1996; National Institute of Standards and Technology [NIST], 2020).

Table 2: Comparison of AES Key Lengths and Quantum Resistance Requirements.

Encryption Method	Classical Key Length	Effective Quantum Key Length	Required Key Length for Quantum Resistance
AES-128	128 bits	64 bits	256 bits
AES-256	256 bits	128 bits	256 bits

6.2 Evaluation of Post-Quantum Cryptographic (PQC) Algorithms

Lattice based cryptography Quantumly secure According to quantum algorithmic assumption that such problems like (SVP) or Untrodden LWE is not practically solvable Now It is possible according to schemes such as Kyber, NTRU they provide strong classical and quantum algorithmic security for moderate parameter size of key and performance factor [3]. In contrast, code-based cryptography (resp. McEliece cryptosystems) assumes that random linear code decoding is NP-hard, and for these schemes there is no quantum reduction that provides strong quantum security but with public key size and computational costs prohibitively large to be workable without deriving the attacker's running time at the optimization level much higher than the most basic resources-efficient level [6]. Taken together, we view them as evidence that lattice-based proposals are serious contenders for standardization in the post-quantum era, and re-emphasise the need to lower the overheads of code-based alternatives in order to achieve quantum-safe encryption that is easily scalable.

6.3 Quantum Key Distribution (QKD) Protocols

The BB84 protocol (Bennett & Brassard 1984) is itself an unconditionally secure protocol for distributed key generation, achieved by encoding each bit of a random key onto the state of polarization of a photon, where each photon is prepared and measured randomly by Alice and Bob in one of two non-orthogonal bases (e.g., rectilinear × or diagonal +), then they publicly compare bases over an authenticated classical channel, discard mismatching measurements, estimate the quantum bit error rate (QBER), apply error correction and privacy amplification, and distil a shared secret key, secure even against an eavesdropper with a quantum computer. In practice, however, BB84 faces a number of practical challenges in terms of photon attenuation in optical fibres or in free-space links, detector dark counts and signal absorption for long-distance connections that artificially increase the QBER and decrease the key rate and, if the error threshold is exceeded, would render secure communication impossible, while side-channel attacks such as detector blinding require a significant amount of hardware countermeasures and security proofs. Quantum repeater progress that enables entanglement swapping and purification of remote nodes circumvents these limitations and extends point-to-point QKD distances to hundreds of km (Briegel et al., 1998) as well as satellite-based QKD demonstrations with high-fidelity secure key exchange over thousands of km on a low-free space loss channel (Liao et al., 2017); indeed measurement-device-independent QKD protocols remove all trust assumptions in the detector, and thereby enable scalable, global quantum-secure networks. The schematic flowchart of the QKD protocol, including qubit generation, transmission, and key sifting and extraction, is depicted in Fig.2 (Bennett & Brassard, 1984).

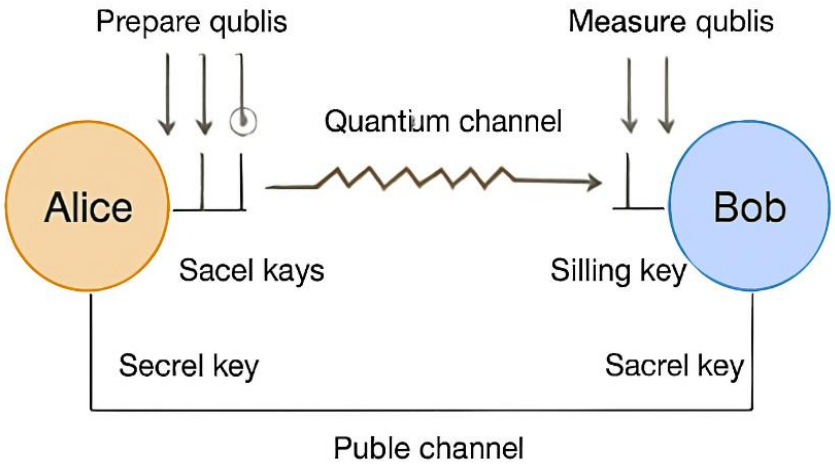

Figure 2: Quantum Key Distribution (QKD) Protocol Overview.

7 Conclusion

We explored the contrast between quantum and classical cryptographic algorithms, and reviewed post-quantum-cryptography (PQC) for Information Security of data communication in a quantum world. The quantum algorithm and particularly Shor's and Grover's acts as the colossal challenge for classic cryptosystem, among them comes as RSA, ECC, AES etc. These quantum algorithms can efficiently break public-key systems and correspondingly also to weaken the effective key strengths of symmetric encryption. In response, we investigated a range of post-quantum cryptographic (PQC) options, with a focus on lattice (Sect. These have been studied as quantum-secure primitives, being secure even in the best attack possible in the quantum setting. But its practical real-time and commonly applicable application have been limited, due to the large scale of keys and the huge computation complexity and should be greatly improved.

Quantum Key Distribution (QKD) and especially "classic" BB8d protocol were examined to consider whether one could conduct a secure key exchange in this quantum domain. However, there is a technological issue, which is the photon loss and the communication distance. The incorporation of this QKD into classical ciphers is still an open problem. The work indicates hybrid cryptography, which uses both classical and post-quantum algorithms, likely is a practical avenue for the transition from classical to post-quantum cryptosystems. It can also be a means for the foundational levels to offer backward compatibility (i.e. pave the way for future-pacing of the cryptography infrastructure into the QC age).

Ultimately, we stress the need for transferring to quantum resistant cryptosystems when we start reaching the capacity to develop quantum computers. For the future secure communication systems may depend critically on the on-going development and standardization of post-quantum algorithms, progress in QKD systems and the creation of secure hybrid cryptographic networks.

References

1. G. S. Mamatha, N. Dimri, and R. Sinha, Post-Quantum Cryptography: Securing Digital Communication in the Quantum Era, arXiv preprint arXiv:2403.11741, Mar. 2024.
2. M. S. Akter, Quantum Cryptography for Enhanced Network Security: A Comprehensive Survey of Research, Developments, and Future Directions, arXiv preprint arXiv:2306.09248, Jun. 2023.
3. R. Bavdekar et al., Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research, arXiv preprint arXiv:2202.02826, Feb. 2022.

4. C. H. Bennett and G. Brassard, Quantum Cryptography: Public Key Distribution and Coin Tossing, arXiv preprint arXiv:2003.06557, Mar. 2020.
5. C. Portmann and R. Renner, Security in Quantum Cryptography, arXiv preprint arXiv:2102.00021, Jan. 2021.
6. S. Pirandola et al., Advances in Quantum Cryptography, Advances in Optics and Photonics, vol. 12, no. 4, pp. 1012–1236, Dec. 2020.
7. N. Gisin et al., Quantum Cryptography, Reviews of Modern Physics, vol. 74, no. 1, pp. 145–195, Mar. 2020.
8. E. Bagirovs et al., Applications of Post-Quantum Cryptography, European Conference on Cyber Warfare and Security, 2024.
9. D. J. Bernstein and T. Lange, Post-Quantum Cryptography, Nature, vol. 549, pp. 188–194, Sep. 2017.
10. M. Campagna et al., Post Quantum Cryptography: Readiness Challenges and the Approaching Storm, Computing Community Consortium, 2021.
11. G. Yalamuri et al., A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats, Procedia Computer Science, vol. 175, pp. 683–688, 2020.
12. D. Joseph et al., Transitioning Organizations to Post-Quantum Cryptography, Nature, 2022.
13. M. Richter et al., A Mathematical Perspective on Post-Quantum Cryptography, Mathematics, vol. 10, no. 3, 2022.
14. S. Li et al., Post-Quantum Security: Opportunities and Challenges, Sensors, vol. 23, no. 1, 2023.
15. D.-T. Dam et al., A Survey of Post-Quantum Cryptography: Start of a New Race, Cryptography, vol. 7, no. 1, 2023.
16. N. Sood, Cryptography in Post Quantum Computing Era, SSRN Electronic Journal, 2024.
17. B. S. Rawal and P. J. Curry, Challenges and Opportunities on the Horizon of Post-Quantum Cryptography, APL Quantum, 2024.
18. B. Singh et al., Innovations in Electrical and Electronic Engineering, 2024.
19. T. Iwakoshi, Analysis of Y00 Protocol Under Quantum Generalization of a Fast Correlation Attack: Toward Information-Theoretic Security, IEEE Access, vol. 8, pp. 123456–123467, 2020.
20. Y. Quan, Secure 100Gbs IMDD Transmission Over 100 km SSMF Enabled by Quantum Noise Stream Cipher and Sparse RLS-Volterra Equalizer, IEEE Access, vol. 8, pp. 789012–789023, 2020.
21. T. Nishioka, How Much Security Does Y-00 Protocol Provide Us, Physics Letters A, vol. 327, no. 1, pp. 28–32, 2004.
22. H. P. Yuen, Comment on: 'How Much Security Does Y-00 Protocol Provide Us, Physics Letters A, vol. 346, no. 1, pp. 1–4, 2005.
23. T. Nishioka, reply to: 'Comment on: 'How Much Security Does Y-00 Protocol Provide Us, Physics Letters A, vol. 346, no. 1, pp. 5–6, 2005.
24. S. Donnet, Security of Y-00 Under Heterodyne Measurement and Fast Correlation Attack, Physics Letters A, vol. 354, no. 1, pp. 1–4, 2006.
25. H. P. Yuen, On the Security of Y-00 Under Fast Correlation and Other Attacks on the Key, Physics Letters A, vol. 361, no. 1, pp. 1–5, 2007.