ISSN : 2347 - 2243

Indo - American Journal of Life Sciences and Biotechnology

www.iajlb.com
Email : editor@iajlb.com or iajlb.editor@gamil.com

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 3, 2018

Quantum-Resistant Cyber Defence in Nation-State Warfare: Mitigating Threats with Post-Quantum Cryptography

[1]Venkat Garikipati
Network Architect,
EA Team Inc., NJ, USA
venkat44556@gmail.com

[2]Punitha Palanisamy
SNS College of Technology,
Coimbatore, Tamil Nadu, India.
Punithapalanisamy93@gmail.com

Abstract

Quantum computing, very likely going to be a threat against current cryptographic systems especially with respect to war between nations, where secure communication and secured data access are very important. Conventional encrypting schemes such as RSA or ECC depend on mathematical problems that can easily be solved by quantum algorithms, typically Shor's, which makes such schemes vulnerable to attacks in the future. This research investigates how PQC is implemented to combat the looming threats of quantum cyber warfare so that national security is assured. Among the most powerful PQC candidates are lattice based cryptographic techniques like NTRU Encrypt, Kyber and Dilithium, all representing quantum-resilient security. The research looks at the time taken for key generation relative to various security levels and quantum attack detection rates, analyzing in detail how these PQC algorithms stand in protecting military communications and critical infrastructure. The inference seems to be that though security levels increase, so does the computational overhead, calling for optimization strategies for realistic deployment. Also, a novel adaptive quantum attack detection system can be appended to render threat identification more efficient along the years. The joining of lattice-based encryption with quantum-resistant cloud storage and secure communication protocols will thus yield a scalable efficient model for post-quantum cyber defense. Above all, the research states the need for quickly changing cryptographic standards to those which afford resistance to quantum attacks to secure sensitive data.

Keywords: *Quantum Computing, Post-Quantum Cryptography, Lattice-Based Encryption, Cyber Warfare, Quantum-Resistant Security, NTRU Encrypt, Kyber, Dilithium.*

1. Introduction

Quantum computing represents an impending threat to national cyber defense systems' present-day cryptographic practices [1]. In fact, traditional encryption algorithms like the RSA and ECC rely on mathematical problems efficiently solvable by a quantum computer: This means they will be entirely vulnerable to being attacked in the future [2]. Consequently, should quantum-capable adversaries decrypt encrypted communications, sensitive military, governmental, or critical infrastructure data might flow into the adversary's hands [3]. Cyber warfare incorporates traditional hacking techniques, using advanced threats to exploit weaknesses in cryptographic security [4]. Nations are investing heavily in quantum technologies; hence, developing quantum-resistant security is imperative [5]. To counter this threat, researchers are developing post-quantum cryptographic algorithms for long-term security [6]. Among the strongest candidates against quantum attack is lattice-based encryption [7]. The secure key exchange protocol Kyber and the digital signature algorithm Dilithium are being tested for their potential to protect communication networks [8]. The transition to post-quantum security will be difficult, demanding substantial research, extensive testing, and standardization [9]. Cooperation between governments, military organizations, and security experts is needed to introduce quantum-resistant measures capable of safeguarding critical information from future threats posed by quantum computing [10].

The quickening of quantum computing poses an increasing risk for breaking traditional cryptographic algorithms [11]. Nation-state hackers are now investing in quantum to gain an upper hand in cyber warfare, and these advances pose an imminent threat to global cyber security [12]. The mathematical problems that put a foundation to existing encryption, like integer factorization and discrete logarithms, can be solved exponentially faster with quantum algorithms, especially Shor's. The above statements also render ordinary cryptographic techniques void against quantum-powered adversaries. Further, certain government agencies, financial institutions, and military networks gather huge troves of encrypted data that may be under the attention of adversaries willing to collect it for future decrypting once quantum technology becomes feasible [13]. The lack

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 3, 2018

of any immediate quantum-resistant implementations exposes critical infrastructure to future breaches. Another one of the causes behind it is that new cryptographic standards have been slow to get adopted, that post-quantum security will require huge upheavals of interoperable products, therefore large-scale updates will incur computational resource costs [14]. Without decisive action, the world will face an imminent crisis for cyber, where credible bait concerning the trustworthiness of the data will be rendered obsolete. There is a rising urgency to creating and deploying quantum-resistant cryptographic solutions to keep sensitive data safe and sustain global security against cyber threats.

Encryption today like RSA and ECC as well as AES is widely utilized in securing digital communications and storage of data. These algorithms have been based on computational hardness assumptions on which classical computers tend to fail. However, the security claims may tend to crumble because all problems can be solved in efficient time runs by quantum computers [15]. RSA and ECC, to make an example, use prime factorization and discrete logarithm problems respectively. Shor's algorithm works or breaks both classes of challenges in polynomial time. AES theoretically loses the battle to quantum attacks, but stipulates adding much larger keys to equal its security level, which amounts to a computationally expensive overhead. Current limitations are also understood as key exchanges, which really don't stand up against any quantum threat [16]. Plus, many security protocols used today haven't taken quantum resistance into account owing to government directories including military applications [17]. As such, they are completely obsolete as future threats emerge [18]. Furthermore, creating quantum-resistant security solutions is quite difficult due to the monumental upgrading of old systems. To cite further challenges, post-quantum cryptography entails rigorous tests and standards, plus the switching time may be a lot of years.

Developing post-quantum cryptography will counter the threat posed by quantum computers. It is about the possibility of cryptographic algorithms being secure even against adversaries with quantum power. Lattice based encryption, NTRU Encrypt, forms one basis for the generation of secure cryptographic systems resistant against quantum computers. An example of such key exchange methods is Kyber, which would facilitate secure communication between two entities while preventing any risk of decryption through quantum computers. Dilithium, a lattice-structured digital signature algorithm, provides authentication features that protect classified documents and military orders from unauthorized tampering. Countries and organizations are actively exploring practical PQC solutions to roll out in their cybersecurity frameworks. The NIST will oversee these initiatives for standardizing algorithms in post-quantum cryptography for worldwide implementation. While PQC adoption may necessitate computational adjustment and upgrading infrastructure, it is necessary to ensure future bankability. Transitioning toward quantum-resistant encryption will, meanwhile, protect classified information, critical infrastructures, and national security from future quantum cyber threats.

In Section 2 Literature Review, where aim is to look into the cryptographic vulnerabilities. The Section 3 illustrate a statement of the problem, will then establish various challenges with respect to security, while the Section 4 proposed methodology, will apply lattice-based encryption (NTRU Encrypt, Kyber, Dilithium) for secure communication. The Section 5, results and discussion section will compare the time taken to generate keys and the detection rates against quantum attacks in terms of security and performance and final step of Section 6 states the conclusion and future works of the statement will emphasize the application of PQC along with advancements in optimization and integration.

2. Literature Review

[19] created a CKD prediction method with GELU activation, Regressive Dropout, and Bi-LSTM with FL and Edge AI. While GI-KHA manages the optimization feature selection, G-Fuzzy is used to further improve stage categorization. Among the drawbacks include the computational complexity, the potential communication overhead during FL, and the requirement for a substantial amount of data for effective training. [20] introduced a virus identification method for IIOT that blends edge computing with Faster R-CNN. Among these disadvantages are high processing costs, problems with real-time adaptability, and model complexity.

Debugging models for optimal performance in hyperparameter adjustment has been used to perform CSO augmentation for the examined CNN and LSTM applications [21]. Although more factor-sensitive and computationally demanding than GA and PSO, it has issues with real-time implementation. [22] used LDBO and SVM for sentiment analysis as support, which enhances classification and exploration. Preprocessing creates high-quality data, and TF-ICF attributes help with selection. Constraints include vulnerability to uneven data treatment components and the capacity to adapt to gradual changes in sentiment.

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 3, 2018

[23] asserts that despite AES's use of efficient encryption algorithms to safeguard cloud data, it has limitations such computational cost and key management. Future research will continue to improve AES performance in spite of potential quantum dangers [24]. ECC is a very safe and efficient encryption technique created especially for cloud computing. By employing short, tiny key widths, it reduces computation expenses. Its implementation and key management provide a number of challenges, despite its exceptional resource efficiency and guarantee of higher integrity data throughput than AES [25].

3. Problem Statement

Such increasing complexity has been introduced into AI-supported cyber security and encryption schemes that they make enormous and unaffordable demands on computing resources, as though their real-time adaptation capabilities are not sufficient, and they tend to operate on high sources [26]. This makes them hardly usable in a practical sense either in cloud or in the IIoT arenas [27].

Therefore, exceptional solutions must be invoked to balance up security against performance and computational feasibility while these new technologies are made to sit easily without added latencies, or increased energy consumption [28]. Besides, there are traditional encryption techniques such as AES or ECC, which are quite complicated during their application as well as quite likely under quantum threats [29]. This would now require the introduction of the new cryptographic algorithm design activity in terms of efficiency and security improvement.

4. Quantum-Resistant Secure Communication Framework for Military Applications

The diagram describes a quantum-resistant secure communication framework for military applications, beginning with Data Collection, the gathering of sensitive information. The data now is cleaned and structured for secure transmission by means of Preprocessing. Lattice-Based Encryption is then applied to shield against quantum computing threats, and the encrypted data is stored in Quantum-Resistant Cloud Storage to ensure long-term security. Transmission to the military communication network creates a cinema of seamless and protected communication for the eyes of an authorized few. Performance Evaluation finally checks for the efficiency of encryption under different circumstances to tighten security protocols against evolving quantum threats is shown in Figure (1),

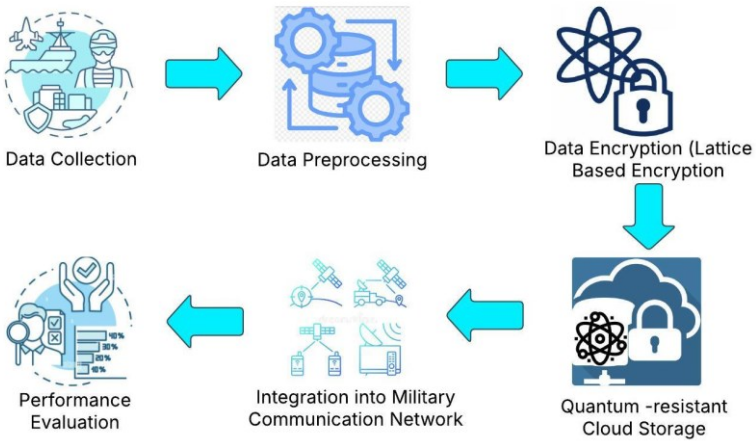

Figure 1: Post-Quantum Secure Communication Architecture for Military Networks

This organized approach purportedly boosts military cybersecurity to be assuredly armed against any cyberattack possibilities. It is periodically updated and has adaptive mechanisms to continue strengthening these encryption techniques. Such work provides national security because it ensures the protection of data crucial for national interests from futuristic threats based on quantum technology.

4.1 Data Collection

The dataset gives a complete picture of military capabilities worldwide and includes data on population, manpower, military personnel, aircraft, tanks, naval assets, defence budgets, and resource production. It also captures information on road, rail and port, providing insights into military strength and logistics. The dataset is

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 3, 2018

available public under a CC0 license and can hence be used for analysis and comparison of the global military power.

Data Set Link: https://www.kaggle.com/datasets/jonathanpettit/military-data

4.2 Data Preprocessing

The data preprocessing stage aims to process the data in order to prepare it for secure encryption by applying certain transformations like sanitizing, normalizing, and anonymizing it. First, removing duplicate or incomplete records by applying a function f, which converts original dataset D into the cleaned version D′ as per Eq. (1),

$$D' = f(D) \tag{1}$$

Next, the sensitive data undergoes tokenization and other data-masking techniques to maintain privacy while transforming the data into their anonymized form. For each data element d_i in the dataset D, the anonymization function g is applied, resulting in an anonymization value d_i' as mentioned in Eq. (2),

$$d_i' = g(d_i)\ \forall d_i \in D \tag{2}$$

These conversion transformations ensure that the data is clean and secure and ready for encryption while keeping in mind privacy factors.

4.3 Data Encryption (Lattice – Based Cryptography)

Lattice-based cryptography is a post-quantum cryptographic method that provides secure key exchanges, message encryption, and authentication services for military communication systems. It will be considered foolproof against quantum attacks in the future.

4.3.1 NTRU Encrypt for Secure Data Encryption

NTRU Encrypt is a lattice-based public-key encryption algorithm that has been designed specially against quantum attacks for the protection of sensitive data, such as military, classified, and intelligence data. The level of security provided by NTRU is based on the difficulty of certain lattice problems such as the SVP and the CVP. These problems have made NTRU resilient to classical as well as quantum attack.

- **Key Generation in NTRU Encrypt**

In NTRU Encrypt, the public-private key pair is formed via polynomial arithmetic over the quotient ring $\mathbb{Z}[x]/(x^N - 1)$. The process starts with two random polynomials f and g from this ring, where f conforms to Eq. (3),

$$f = f_p + pf_q \tag{3}$$

Where, f_p and f_q are small polynomials and p is a small modulus ensuring correct decryption. The public key h is now calculated as follows in Eq. (4),

$$h = g \cdot f^{-1} \bmod q \tag{4}$$

Where, q is a large prime modulus to make security high. Private key remains f, necessary for decryption. As security of a lattice is based on hard-to-find short vectors in high-dimensional spaces, NTRU Encrypt remains equally firm against quantum attacks, making it an effective candidate for post-quantum cryptography.

- **Encryption Process in NTRU Encrypt**

Using polynomial arithmetic in a certain ring, the plaintext message mmm is transformed into ciphertext C. In order to add randomness and security, a random polynomial r is selected during the encryption process according to Eq. (5),

$$C = pf * m + rg \bmod q \tag{5}$$

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 3, 2018

Here, p is a small integer useful for decryption, f is a secret polynomial chosen in key generation, g is a polynomial also from key generation, and q is a big prime modulus giving security. The multiplication (*) represents polynomial multiplication in the ring $\mathbb{Z}[x]/(x^N - 1)$. The ciphertext C is computed so that even if an attacker intercepts C, the computational overhead in recovering mmm without the private key is infeasible, given the hardness of lattice-based problems.

- **NTRU Encrypt Decryption Process**

To decrypt the plaintext message mmm from ciphertext C, the recipient uses his/her private key f. In the first step, one of the intermediate values is computed by taking the product of C and f, and reducing it modulo q indicates Eq. (6),

$$C' = f * C \bmod q \tag{6}$$

Since C was encrypted with the public key polynomial h, this removes the randomness involved in the encryption process. After that, to finally retrieve the plain message, the ciphertext is reduced as C′ mod p to eliminate the extra noise from the ciphertext and recover m, as stated in Eq. (7),

$$m = (C' \bmod p) \tag{7}$$

This step works due to the fact that modular reduction by p isolates the original message polynomial from the encrypted data. Since lattice-based encryption introduces random noise as a means of securing messages, careful parameter choices ensure that decryption is accomplished without error for the parameters chosen. The process ensures that only the intended recipient can decrypt the message while withstanding quantum attacks.

4.4 Quantum-Proof Cloud Storage

Quantum-proof cloud storage will be sound provisioned, by lattice-based encryption (NTRU Encrypt), and Kyber key exchange, to keep data encrypted and protected from quantum attacks. While SHA-3 hashing and Dilithium digital signatures maintain data integrity by proofing that the stored data cannot be altered and is authentic, it serves its purpose mainly in long-term military and governmental security applications.

- **Data Integrity Verification**

Cryptographic hashing and Dilithium digital signatures prevent manipulation, corruption, and unauthorized access of data. Their signature match ensures what is retrieved is the original: making quantum-resistant cloud storage an ultimate solution for secure defense communications.

4.5 Integrating the Network into Military Communications

The extreme condition military communication network uses all these points to secure the transmission of encrypted data from eavesdroppers, interception, and cyberattacks. To build a fairly high-security connection, the commonly used post-quantum key exchange mechanisms, such as Kyber KEM, were designed for generating and sharing symmetric keys between communicating entities. Unauthorized military units, government agencies, or defense systems would have access to Kyber, for this ensures the security sharing of sensitive data against quantum security threats. This encrypted data flows through military-grade secure channels ensuring confidentiality and authenticity, besides being quantum threat proof. These advantages of post-quanta-bound methods ensure a boost to national safety against cyber threats while also promising secure communication during warfare and defense operations.

5. Results and Discussion

In this section, the key generation delays and quantum attack detection rates while emphasizing the security-performance trade-offs. A higher level of security results in a longer key generation delay, whereas continuous monitoring improves detection of attacks. Maximizing the level of efficiency in cryptography and adaptive detection of threats strengthens the defense against cyber.

5.1 Evaluation of Key Generation Time Across Security Levels

The following graph displays the relationship between time taken to generate keys in comparison with their security levels for a cryptographic algorithm. As expected, the time taken increases with increasing security level measured in bits as with earlier increases in key generation time measured in milliseconds. The notice that

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 3, 2018

the function of time does not grow into linear trends, but is rather divergent due to real computational costs associated with the use of advanced encryption techniques that will help improve the overall security of the system against attacks. Key generation time can indeed be viewed from two perspectives: improved security increasing its demand and the fact that the higher the demand put onto service resources, overhead grows with the workload is displayed in Figure (2),

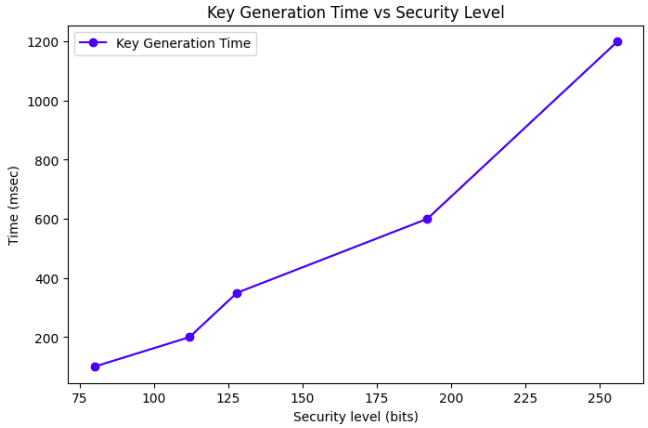

Figure 2: Key Generation Time Analysis for Secure Cryptographic Algorithms

However, this does not mean that security comes at no cost performance-wise: while offering safety and the much-desired heightened overhead incurred will also be expected from computation. Hence it will always be needed to optimize any usage for real-world applications. One needs efficient key-generation algorithms that understand trade-offs between security and performance, such as post-quantum cryptographic design like NTRU, to further reduce the overhead but would hold against attacks. The extent to which these trade-offs can be utilized is critical in developing encryption standards that are secure, efficient, and practically oriented.

5.2 Optimized Quantum Attack Detection Rate Over Time

The graph illustrates the detection rate for quantum attack detection in relation to time. According to this, the detection is likely to become even better with time. Initially, the detection rate starts at 50%, increases quickly within a few seconds, and stabilizes at more than 90% after 20 seconds. This shows that the longer the detection system has been on, the more data it has analyzed over time forming an effective identification of quantum cyber threats is shown in Figure (3),

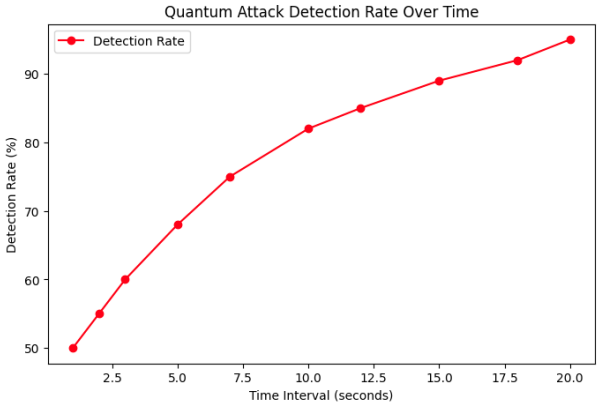

Figure 3: Enhanced Quantum Attack Detection Rate Over Time

The red ray means the ascending detection level that represents the capability of the system to refine its accuracy as it processes data. This will yield a better detection rate, ensuring a more robust defense from quantum attacks. Further improvement of the systems could be achieved through advanced machine learning. Continuous monitoring and adaptive mechanisms ensure accuracy while shifting with the times.

6. Conclusion and Future Works

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 3, 2018

The emergence of quantum computing threatens established means of encryption and security using PQC for democratic countries' national security and military systems. This paper presents studies on lattice-based cryptographic modalities such as NTRU Encrypt, Kyber, and Dilithium, to effectively deal with quantum cyber-attacks. The critical evaluation of key generation time and detection rates during quantum attacks indicates the possible trade-off between security and computational efficiency. While PQC adds more security, making the system much better critical for real-life application is vital. The critical infrastructure protection against quantum-enabled adversaries is secured by incorporating mechanisms like quantum resistance encryption, cloud storage, and secure key-exchanged methodology.

Future work will focus on optimizing the PQC algorithm so that the computational burden is significantly reduced while having strong security guarantees. Hybrid models of cryptography using both classical and post-quantum mechanisms would provide smoother transitions. In addition, incorporation of AI-based detection of quantum attacks with blockchain security will improve preparedness in real-time. Further exploration of hardware acceleration (FPGA, ASIC) for PQC will improve performance in resource-constrained contraints. Joint efforts for standardizing protocols on PQC will be crucial in making the world-state defense stronger in the global cybersecurity domain toward emerging quantum threats.

References

[1] S. Sinha, D. Santhadevi, S. Tokas, and V. Kareer, "Quantum cryptanalysis using digital ant in pervasive environment," in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, Mar. 2016, pp. 3678-3681.

[2] J. Liu, S. Zhang, W. Sun, and Y. Shi, "In-vehicle network attacks and countermeasures: Challenges and future directions," *IEEE Network*, vol. 31, no. 5, pp. 50-58, 2017.

[3] N. Costa, R. Martínez, and P. Morillo, "Proof of a shuffle for lattice-based cryptography," in *Secure IT Systems: 22nd Nordic Conference, NordSec 2017, Tartu, Estonia, November 8–10, 2017, Proceedings 22*, Springer International Publishing, 2017, pp. 280-296.

[4] A. Razzaq, A. Hur, H. F. Ahmad, and M. Masood, "Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications," in *2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)*, Mar. 2013, pp. 1-6.

[5] W. P. Schleich, K. S. Ranade, C. Anton, M. Arndt, M. Aspelmeyer, M. Bayer, et al., "Quantum technology: from research to application," *Applied Physics B*, vol. 122, pp. 1-31, 2016.

[6] B. Koziel, R. Azarderakhsh, M. M. Kermani, and D. Jao, "Post-quantum cryptography on FPGA based on isogenies on elliptic curves," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 1, pp. 86-99, 2016.

[7] K. Bagheri, M. R. Sadeghi, and T. Eghlidos, "An efficient public key encryption scheme based on QC-MDPC lattices," *IEEE Access*, vol. 5, pp. 25527-25541, 2017.

[8] A. Umamageswari and G. R. Suresh, "Novel algorithms for secure medical image communication using Digital Signature with various attacks," in *2013 Fifth International Conference on Advanced Computing (ICoAC)*, Dec. 2013, pp. 152-157.

[9] O. M. Guillen, T. Pöppelmann, J. M. B. Mera, E. F. Bongenaar, G. Sigl, and J. Sepulveda, "Towards post-quantum security for IoT endpoints with NTRU," in *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2017, pp. 698-703.

[10] Ø. D. Fjeldstad, C. C. Snow, R. E. Miles, and C. Lettl, "The architecture of collaboration," *Strategic Management Journal*, vol. 33, no. 6, pp. 734-750, 2012.

[11] G. Parker and A. Zelinsky, "Partner or perish: Research collaboration to secure cyberspace," *Cyber Security: A Peer-Reviewed Journal*, vol. 1, no. 1, pp. 69-79, 2017.

[12] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973-993, 2014.

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 3, 2018

[13] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," *Proceedings of the IEEE*, vol. 100, no. 11, pp. 3056-3076, 2012.

[14] M. I. Dyakonov, "State of the art and prospects for quantum computing," in *Future Trends in Microelectronics: Frontiers and Innovations*, pp. 266-285, 2013.

[15] E. Fraňková, J. Fousek, L. Kala, and J. Labohý, "Transaction network analysis for studying Local Exchange Trading Systems (LETS): Research potentials and limitations," *Ecological Economics*, vol. 107, pp. 266-275, 2014.

[16] D. Husmann, S. Uchino, S. Krinner, M. Lebrat, T. Giamarchi, T. Esslinger, and J. P. Brantut, "Connecting strongly correlated superfluids by a quantum point contact," *Science*, vol. 350, no. 6267, pp. 1498-1501, 2015.

[17] J. D. Van Wyk and F. C. Lee, "On a future for power electronics," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 1, no. 2, pp. 59-72, 2013.

[18] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2322-2358, 2017.

[19] P. Mach and Z. Becvar, "Mobile edge computing: A survey on architecture and computation offloading," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1628-1656, 2017.

[20] Z. Zhang, K. Long, A. V. Vasilakos, and L. Hanzo, "Full-duplex wireless communications: Challenges, solutions, and future research directions," *Proceedings of the IEEE*, vol. 104, no. 7, pp. 1369-1409, 2016.

[21] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1801-1819, 2014.

[22] M. Shirvanimoghaddam, M. Dohler, and S. J. Johnson, "Massive non-orthogonal multiple access for cellular IoT: Potentials and limitations," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 55-61, 2017.

[23] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727-1765, 2016.

[24] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483-2495, 2017.

[25] S. Koteshwara and A. Das, "Comparative study of authenticated encryption targeting lightweight IoT applications," *IEEE Design & Test*, vol. 34, no. 4, pp. 26-33, 2017.

[26] A. Sill, "Cloud, data, and business process standards for manufacturing," *IEEE Cloud Computing*, vol. 3, no. 4, pp. 74-80, 2016.

[27] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125-1142, 2017.

[28] S. Mitra, B. Jana, S. Bhattacharya, P. Pal, and J. Poray, "Quantum cryptography: Overview, security issues and future challenges," in *2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix)*, Nov. 2017, pp. 1-7.

[29] B. K. Mandal, D. Bhattacharyya, and S. K. Bandyopadhyay, "Designing and performance analysis of a proposed symmetric cryptography algorithm," in *2013 International Conference on Communication Systems and Network Technologies*, Apr. 2013, pp. 453-461.