International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Traditional and Quantum Approaches Against Shor's Algorithm: A Review

Bannishikha Banerjee, Ashish Jani, Niraj Shah

School of Engineering, PP Savani University, India

.

A B S T R A C T

Securing blockchain is the need of this era, with the emergence of Quantum computers. It will become fairly easy to break the existing encryption algorithms which were considered secure a while back. Quantum computers can compromise the security of RSA as well as Elliptic Curve and many similar algorithms using Shor's algorithm. In this paper, several encryption algorithms were studied and a matrix-based approach was implemented for post quantum blockchain. The focus was to provide security using matrices since they are immune to Shor's algorithm, as matrices can't be factorized using brute force. Different methodologies are studied, which are able to provide security in blockchain based IoT devices in polynomial time. The considered parameters are time complexity and sensitivity test to measure avalanche effect. It was concluded that the post quantum approach provides higher sensitivity than Elliptic Curve Cryptography but lower than RSA. But since RSA can be easily broken by Shor's algorithm, the post quantum algorithm can be considered optimum to provide security in post quantum blockchain in polynomial time

Keywords: Quantum Computing, Internet of Things, Blockchain, Avalanche Effect, Cryptography.

1. Introduction

In the last few years, blockchain has emerged as an efficient digital ledger in managing transactions [1]. Blockchain is a decentralized technology. A global network of computers uses blockchain technology to jointly manage the database that records various transactions. This means, the transactions are managed by the network, and not any one central authority [2]. Information held on a blockchain exists as a shared and continually reconciled database. The blockchain database isn't stored in any single location, but is distributed among various systems over the network. The records it keeps are completely public and easily verifiable. No centralized version of this information exists for an attacker to corrupt. The information is hosted by millions of computers simultaneously, its data is accessible to anyone on the internet. Due to decentralization of the information among multiple systems, an attacker cannot overload a server using Distributed Denial of Service attack [2]. This provides higher security and better accessibility for the users. The network becomes more user friendly as anyone can access the recent and updated data at any time. Blockchain is an emerging technology which ensures that there are no missed transactions due to any overload on server, or machine error, or human error or even due to an exchange that was not done without the consent of the parties involved [3]. The most critical area where Blockchain proves its efficiency is to guarantee the validity of a transaction by recording it not only on a main register but on a connected distributed system of registers, which are connected through a secure validation mechanism. Blockchain uses various hashing functions and digital signatures to ensure the authenticity of the transaction [3]. Blockchain provides transparency by letting the users know about the status of their transactions [4].

2. The Research Method

In [5], the NASA scientists showed that quantum speedup is achievable in a real-world system and is not precluded by any hidden physical laws. The main task that they demonstrated has an immediate application in generating certifiable random numbers. To achieve quantum supremacy, they proposed a

* *Corresponding author*
E-mail address: bannishikha.banerjee@ppsu.ac.in

number of technical advances which also pave the way towards error correction. They developed fast, high-fidelity gates that can be executed simultaneously across a two-dimensional qubit array. They calibrated and benchmarked the processor at both the component and system level using a powerful cross-entropy benchmarking. Finally, they used component-level fidelities to accurately predict the performance of the whole system. Further, they proved that quantum information behaves as expected when scaling to large systems. However, realizing the full promise of quantum computing like Shor's algorithm for factoring, still requires technical leaps to engineer fault-tolerant logical qubits.

In [6], In this paper, the authors selected blockchain framework as a solution for their IoT devices to deploy across their network. It is a private, permissioned blockchain whose functions are closely coupled with each other. It also decouples transaction validation from ledger block. Peer nodes carry out validation and ledger maintenance. The monitor nodes handle consensus and block broadcasting to the peers. Their framework leverages the containerization of this setup so that the network can operate between the edge devices and the cloud in a single, private system.

In [7] the authors noticed that before adding any IoT device, integrity checking is performed by comparing the Reference Integrity Metrics (RIM). The RIM is pre-computed and stored in a secure location. The RIM stores hash values of the identity of the devices. To ensure reliability of the activity, the integrity of the RIM is very important. The RIM is usually stored in read only memory. But when the firmware is updated, the corresponding RIM also gets updated.

If an intruder manages to modify the RIM, then the integrity of the device is compromised. To overcome this, the authors proposed blockchain to be used to protect RIM. In blockchain, all the participating devices maintain the same records, so unless an intruder manages to compromise the majority of the devices, the integrity of the records shall remain maintained.

In [8], firstly they demonstrate the impacts of quantum computers on the security of the cryptographic schemes used today, and then give an overview of the recommendations for cryptographic schemes that can be secure under the attacks of both classical and quantum computers. Then they present the existing implementations of quantum-resistant cryptographic schemes on constrained devices suitable for the IoT. Finally, they gave an introduction to the ongoing projects for quantum-resistant schemes that will help develop future security solutions for the IoT.

In [9], several identity-based encryption schemes from lattice hardness assumptions are proposed. In the standard model, these schemes are indistinguishable against inner adaptively chosen ciphertext attacks and strongly unforgeable against inner chosen message attacks. They used identity matrix and introduced appropriate compensation vector in the ciphertext to design an identity-based deterministic encryption scheme. They developed strong unforgeable signature used to guarantee the non-malleable property of ciphertext. The scheme is efficient because new identity-based signature schemes with shorter signature length are proposed to construct the encryption.

In [10], the authors proposed a possible solution to the quantum era blockchain challenge and report an experimental realization of a quantum-safe blockchain platform that utilizes quantum key distribution across an urban fiber network for information-theoretically secure authentication. These results address important questions about realizability and scalability of quantum-safe blockchains for commercial and governmental applications. In this, instead of adding new blocks in the hands of a miner, they proposed a broadcast protocol where all the nodes reach an agreement about a new block on equal terms.

In [11], they proposed a novel nodes selection algorithm based on AI technology that exploits nearly complementary information of each nodes, and relies on a particular designed convolutional neural network to reach the consensus. To ensure the decentralization and safety of the network, a dynamic threshold was employed to obtain the super nodes and the random nodes. Their algorithm avoided the complicated hash operation and redundant verification operation, which can be beneficial to save energy. Their scheme provides decentralization, network cost, security and the speed of transaction confirmation. Experimental results with the proposed algorithm demonstrate that it can be adopted to every cryptocurrency and can be developed to a complete consensus protocol in the near future.

In [12], the authors have discussed about the quantum computing attack. This attack threatens the security of blockchain. It is similar to a brute force attack, except that the intruder has greater and faster number of resources. To handle this situation, the authors defined Post Quantum Blockchain (PQB) and proposed a secure cryptocurrency scheme based on lattice cryptography, which can resist quantum computing attacks. The algorithm was implemented using standard model of cryptography.

3. Problems

When a block is created, it is necessary to check whether it is legitimate or not. Block's legitimacy is checked by consensus of the miners. To add a block, the miners do a bunch of cryptographic computations. All the miners start calculating the hash. This block then gets added to the blockchain and all the users of the blockchain update their copies. In earlier time, this technique would have been considered safe as it consumes lot of resource and time. An attacker would have no other option than guessing each and every input until he gets the desired output. This would take a lot of time for an attacker to find out the desired result. In Quantum computers, it is easier to find the desired solution using prime factorization method [9].

According to Shor's Hypothesis [10], finding prime factors of the hash value would reduce the number of computations required to find the secret key dramatically.

These are the major research gaps that were identified during literature review:

- IoT devices should be secured to avoid intrusion in the Blockchain.

- Using conventional cryptographic operations to provide security is not efficient because it is vulnerable to quantum computing attacks.
- Quantum computers can easily break conventional cryptographic algorithms.

4. Cryptographic Approaches

Instead of using classical cryptographic algorithms which use prime numbers to generate public – private key pair, it is better to use lattice-based cryptography.

Quantum computers are capable of parallel processing brute force attack to find out the key. To protect this lattice-based cryptography is to be used [12]. One of the significant problems in lattice-based cryptography is the Shortest Vector Problem (SVP). This problem is to find the non-zero shortest vector in lattice. SVP is an NP-hard problem under randomized reductions, and many cryptosystems are secure under the assumption that SVP is hard. Classical algorithms like Rivest, Shamir, Adleman (RSA), Elliptic Curve Cryptography (ECC) use co-primes to calculate key. But by Shor's algorithm [12], it is possible to perform prime factorization in polynomial time. RSA is implemented to show the encryption/decryption time, then Shor's approach is applied to show how easy it is to break it.

Table 1. RSA Implementation

Plaintext: Bannishikha		
Security Parameter	**Ciphertext**	**Time (ms)**
(35,221), (11, 221)	1961932062069212319592113195193	1.9965171545
(91,323), (19, 323)	924953531019116110278161249	2.9974708566
(83,143), (107, 143)	663711111185891118359137	6.9254813728
(207,667), (247, 667)	2173882102102341154123416841388	7.1577622108
(1409,5893), (4029, 5893)	8526410171017300816272264300840162264264	9.9547543334

Table 2. Shor's Approach for Prime Factorization

Number	**Prime Factors**	**Time (ms)**
315	3,3,5,7	9.368280792236328
315095	5, 11, 17, 337	9.995896606445312
315095984	2, 2, 2, 2, 7, 197, 14281	19.94609832763672
315095984856	2, 2, 2, 3, 3, 547, 8000609	22.923707962036133
315095984856534	2, 3, 7, 211, 35555854757	110.6210708618164

Quantum Computers have powerful parallel computing abilities which can easily break conventional cryptographic algorithms.

Assume n = p*q, where p and q are co-primes.

- For example, 35 = 7*5. Here 7 and 5 are co primes.

Many classical cryptographic algorithms use the concept of prime factorization. It takes a long time to find prime factors of a very large number using a normal computer. Shor proposed quantum algorithm for factoring integers to find the co-primes of a large number on a quantum computer which can break algorithms like RSA, DSA etc in feasible time. Even elliptic curve cryptography (ECC) can be broken by this.

5. Implementation Results

System Specifications:

- Processor: Intel® Core™ i3-6006U CPU @ 2.00GHz
- RAM: 4.00 GB
- System Type: 64-bit Operating System, x64-based processor.

Table 3. Implementation Details

Plaintext: Bannishikha Banerjee		
Security Parameter	**Ciphertext**	**Time Taken**
(73, 323) (217,323)	981921101104811510448l 210419232981921101012 09106101101	5.556767
(365,437) (281,437)	2191530730752115423522 1742315325219153073021 14273302302	6.836476
(169,667) (113,667)	4461019719765611539465 6339394101774461019724 6114628246246	5.018313
(989,1073) (53, 1073)	6862301035103568285399 8268539230681686230103 586239589862862	5.215801
(1027,1333) (703,1333)	590168568511641191123 011645912309017765901 685326921786326326	8.064334

6. Comparative Analysis

We have compared the existing algorithms based on key size, ciphertext size and time complexity in the following table.

Table 4. Time Complexity

Security Model: Standard Model			
Algorithm	**Key Size**	**Ciphertext Size**	**Complexity**
PQB [12]	256 bits	256 bits	O(N².log(N))
RSA	2048 bits	1906 bits	O(log (N))
ECC	512 bits	512 bits	O(N³)

Though RSA has the lowest complexity, it fails to provide security. It can be easily broken by Shor's algorithms as showed earlier in this paper [Table 2]. Another important parameter while developing an encryption algorithm is Avalanche effect. When a single bit of key or plaintext is changed, at least 50% of the bits of the ciphertext must change [18]. This ensures that the algorithm is secure.

Table 5. Avalanche Effect

Plaintext: Bannishikha			
Algorithm	**Key 1**	**Bits Change**	**Sensitivity %**
PQB [12]	(73, 323) (217,323)	100/256	39.06%
RSA	(73, 323) (217,323)	1145/1906	60.07%
ECC	(73, 323) (217,323)	211/512	41.21%

The post quantum blockchain [12] methodology provides 39.06% sensitivity ratio, which shows that avalanche effect is happening. RSA shows better sensitivity, which is the main reason it was so popular in the market, but the emergence of quantum computer will make it vulnerable to Shor's algorithm of prime factorization. Hence, [12] approach is better when it comes to protecting data from quantum computing attacks. Therefore, it is noticed that [12] provides optimum amount of security in polynomial time. This approach is not dependent on prime factors so Shor's algorithm fails to brute force it.

7. Conclusion

The major concern for Blockchain based IoT devices is security. A post quantum approach is studied and compared with traditional approaches. It is able to provide security in IoT devices, against quantum computers, in polynomial time. The algorithm has a complexity of O(N² log N) which is very efficient when it comes to encryption and decryption. It provides security and is immune to brute force attack by Quantum computers using Shor's algorithm.

REFERENCES

- Biswas, R., Jiang, Z., Kechezhi, K., Knysh, S., Mandrà, S., O'Gorman, B. Wang, Z. (2017). A NASA perspective on quantum computing: Opportunities and challenges. Parallel Computing, 64, 81–98. doi: 10.1016/j.parco.2016.11.002
- Noor, M. B. M., & Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer Networks, 148, 283–294. doi: 10.1016/j.comnet.2018.11.025
- Badr, S., Gomaa, I., & Abd-Elrahman, E. (2018). Multi-tier Blockchain Framework for IoT-EHRs Systems. Procedia Computer Science, 141, 159–166.

doi: 10.1016/j.procs.2018.10.162

- Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, 88, 173–190. doi: 10.1016/j.future.2018.05.046
- Rieffel , E. G. (2019). Quantum Supremacy Using a Programmable Superconducting Processor . NASA Ames Research Center. doi: NASA/TP-2019-220319
- Song, J. C., Demir, M. A., Prevost, J. J., & Rad, P. (2018). Blockchain Design for Trusted Decentralized IoT Networks. 2018 13th Annual Conference on System of Systems Engineering (SoSE). doi: 10.1109/sysose.2018.8428720
- Banerjee, M., Lee, J., & Choo, K.-K. R. (2018). A blockchain future for internet of things security: a position paper. Digital Communications and Networks, 4(3), 149–160. doi: 10.1016/j.dcan.2017.10.006
- Cheng, C., Lu, R., Petzoldt, A., & Takagi, T. (2017). Securing the Internet of Things in a Quantum World. IEEE Communications Magazine, 55(2), 116–120. doi: 10.1109/mcom.2017.1600522cm
- Yan, J., Wang, L., Dong, M., Yang, Y., & Yao, W. (2015). Identity-based signcryption from lattices. Security and Communication Networks, 8(18), 3751–3770. doi: 10.1002/sec.1297
- Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V., Fedorov, A. K. (2018). Quantum-secured blockchain. Quantum Science and Technology, 3(3), 035004. doi: 10.1088/2058-9565/aabc6b
- Chen, J., Duan, K., Zhang, R., Zeng, L., & Wang, W. (2018). An AI Based Super Nodes Selection Algorithm in Blockchain Networks. Cryptography and Security. doi: https://arxiv.org/abs/1808.00216
- Gao, Y.-L., Chen, X.-B., Chen, Y.-L., Sun, Y., Niu, X.-X., & Yang, Y.-X. (2018). A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain. IEEE Access, 6, 27205–27213. doi: 10.1109/access.2018.2827203
- Moubarak, J., Filiol, E., & Chamoun, M. (2018). On blockchain security and relevant attacks. 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM). doi: 10.1109/menacomm.2018.8371010
- Kouzinopoulos, C. S., Spathoulas, G., Giannoutakis, K. M., Votis, K., Pandey, P., Tzovaras, D., … Nijdam, N. A. (2018). Using Blockchains to Strengthen the Security of Internet of Things. Communications in Computer and Information Science Security in Computer and Information Sciences, 90–100. doi: 10.1007/978-3-319-95189-8_9
- Elisa, N., Yang, L., Chao, F., & Cao, Y. (2018). A framework of blockchain-based secure and privacy-preserving E-government system. Wireless Networks. doi: 10.1007/s11276-018-1883-0
- Sadique, K. M., Rahmani, R., & Johannesson, P. (2018). Towards Security on Internet of Things: Applications and Challenges in Technology. Procedia Computer Science, 141, 199–206. doi: 10.1016/j.procs.2018.10.168
- Biswas, K., & Muthukkumarasamy, V. (2016). Securing Smart Cities Using Blockchain Technology. 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS). doi: 10.1109/hpcc-smartcity-dss.2016.0198
- Banerjee, B., & Patel, J. (2016). A Symmetric Key Block Cipher to Provide Confidentiality in Wireless Sensor Network. Infocomp Journal of Computer Science, 12-18. Retrieved from http://www.dcc.ufla.br/infocomp/ index.php/INFOCOMP/article/view/515.