ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 4. Issue 4 (2024)
https://doi.org/10.62019/abbdm.v4i4.267

A Comparative Analysis of One-Time Pad and Contemporary Cryptographic Algorithms: Security, Quantum Resistance, and Practical Usability

Hafiz Waheed ud Din, Yahya khan, Alameen Abdalrahman,

Chronicle

Article history
Received: 1st December, 2024
Received in the revised format: 12th December, 2024
Accepted: 30th December, 2024
Available online: 31st December, 2024

Hafiz Waheed ud Din and Yahya khan are currently affiliated with the Department of Computer and software engineering, faculty of computing Gomal University, Pakistan.
Email: waheedgaziksa@gmail.com
Email: yahyakhan@gu.edu.pk

Alameen Abdalrahman is currently affiliated with the Department of computer sciences, College of Computer and Information Sciences ,Jouf University ,Sakaka - Saudia Arabia.
Email: aeltoum@ju.edu.sa

Corresponding Author*

Abstract

The performance analysis in the present study examines the OTP in contrast to popular contemporary cryptographic techniques like AES, RSA and so on. Four criteria are to be examined: Their security, their protection against attacks with quantum computers, the required key management and their practical feasibility. OTP is presented as an ideal solution in terms of security theory while being critically described in terms of the application to a large-scale system including the problem of key generation, distribution, and storage. However other contemporary methods like the AES or RSA are relatively more suitable to be used in real life systems because the execution time and space complexities are more bearable. However, as the technology of quantum computers develops, these algorithms become most threatened by quantum attacks, especially through those such as Shor's and Grover's. The paper also explores the concept of post-quantum cryptography as a developing field for finding solutions to protect encryption from such threats backed by quantum computing. These alternatives remain still in the early stage of development but appear to have great possibilities to protect digital communications in a world in which quantum computers could crack the more conventional cryptographic protocols. The study reveals that there is a need to achieve proper proportionalities in designing cryptographic processes and the security measures offered to ensure that they are not only strong but also implementable. OTP, being a concept of perfect secrecy, however, is not feasible for use in large applications hence why there is a need to search for algorithms that offer high-security levels while at the same time operational. With the advancement of quantum computing, it is essential that the future work be directed toward the proposition of algorithms and communication paradigms that would be both effect and efficient, and, most importantly, secure from attacks utilizing capabilities of quantum computers. Hence, the findings underscore the need for designs of cryptographic protocols that support a high level of security during deployment while still being practical for future implementation as the technologies change.

Keywords: Cryptography, One-Time Pad, Quantum Computing, Security, Key Management, Practical Usability

INTRODUCTION

Cryptography may be defined as the discipline that enhances the security of communication problems in the face of a wide range of adversarial scenarios. Traditional

cryptography techniques include the one-time pad while the techniques of technical cryptography include AES, RSA etc each has its own security characteristics. OTP, though theoretically provably secure, is practically inconvenient since it cannot be used in most real-world applications that require high security. On the other hand we have popular yet again quantum-vulnerable algorithms including AES, RSA, Elliptic Curve Cryptography (ECC). In this paper, OTP and modern cryptographic standards are analyzed based on their security, resistance to quantum computing, and practical applicability.

METHODOLOGY

Thus, the present research is based on systematizing the findings from the classical and recent cryptographic publications. Security, quantum resistance, key management, computation complexity, and attack resistance are chosen as the criteria to review related journals, technical papers, and cryptographic guidelines. The comparison is made on theoretical concepts with real-world considerations explained in terms of new trends within the area of cryptography due to progress in the field of quantum computation.

Comparative Analysis

Security, One-Time Pad (OTP): The security of the One-Time Pad (OTP) is founded on the requirement of achieving perfect secrecy, beginning with Claude Elwood Shannon's theory in 1949. OTP uses the concept developed for Playfair Square where the plain text is mixed with a key of the same length as the message. In each case, the key is used only once, and because of its randomness there is no easier way to guess the code. This certainly eliminates vulnerability to conventional patterns of cryptanalysis, simple frequency analysis, identification of cipher patterns or even complex techniques such as differential analysis (Shannon, 1949). As Kahn (1996) observed, the security of the OTP is theoretically unassailable: if the key is sufficiently random, used only one time, and concealed from the adversary. However, in practice, there are some problems - the key length should be equal to the message length, which reduces the scalability of this cryptographic method and decreases its efficiency. In addition, OTP involves the distribution of keys which itself is a challenging proposition for large number of communications; the conduits used for the keys most be extremely secure. The premise of using extremely large keys for every message eliminates the OTP from many of the contemporary application scenarios. However, OTP's security model cannot be maintained as it is actually perfect for many of the modern forms of communication which are more manageable and easy to scale up.

Other Algorithms: However, current designs such as AES and RSA are considerably immune to these classical forms of cryptographic analysis, including brute force and statistical. AES, currently used for protecting information that requires high level of security, is almost immune to classical cryptanalysis due to their internal structure and because it is based on a multiple number of rounds (Daemen & Rijmen, 2002). Nevertheless, AES is now under threat from side channel attacks in which physical features such as power usage or time complexity of the encryption process are exploited (Biham & Shamir, 1991). Such types of attacks are not desirable in scenarios where an attacker might have the plaintext of the original message and physical device that implements encryption. And RSA, Elliptic Curve Cryptography (ECC) also used today widely because it uses asymmetric key cryptography technique for exchanging keys over insecure channel (Diffie & Hellman

1976). However, these algorithms are susceptible to a quantum attack. Shor's algorithm (Shor, 1994 for example) would pose a threat to RSA and ECC since can factor large integers and solve the discrete logarithm problem with efficiency, respectively. Although in the current scenario such algorithms are thought to be resistant to classical attacks, they are vulnerable to threats posed by quantum computing.

Resistance to Quantum Computing

One-Time Pad (OTP): The natural implementation of OTP makes it immune to attacks by quantum computers. Grover's and Shor's algorithms are not threats to OTP since OTP uses random keys that are used once and only once. Most classical cryptographic algorithms including RSA and AES which are vulnerable to quantum attacks because the quantum computers specializations include mathematical problems such as integer factorization through Shor's algorithm and database search through Grover's algorithm (Shor, 1994; Grover, 1996). For OTP, however, the strength of the encryption does not change because no quantum computing or classical algorithm can penetrate the randomness of a key that is truly used once and only once. This, as Bellare et al. (1997) pointed out makes OTP quantum resistant rendering the scheme a good candidate for a type of cipher that is not only vulnerable to a quantum attack but practically useless for normal use.

Other Algorithms: On the other hand, AES, is only partially resistant to The quantum attacks.. Grover's algorithm applied to quantum computing makes brute-force search, which takes 2n2^n require time to carry out an attack on an n-bit key to a mere 2n/22^{n/2}thus cutting down AES's security by half (Grover, 1996). Despite AES-256 being trusted as the most secure mode of encryption to work with, there are existing quantum algorithms that may in the long-run affect AES-256. RSA and ECC, however, are much more susceptible to quantum threatening to render them almost entirely useless. Shor's algorithm would allow a quantum computer to solve problems, on which RSA and ECC rely on by factoring large integers or discrete logarithms (Shor, 1994). There is, therefore, a need for proceeding with the creation of quantum-safe cryptographic algorithms with possibilities of a transition towards the post-quantum cryptography using lattice-based problems, hash-based, or code based (Regev, 2005). However, these algorithms are post-quantum, and they are accompanied by the corresponding computational overhead, which is the major concern for practical implementation.

Key Management

One-Time Pad (OTP): The key management needed for OTP becomes one of the major practical limitations of the solution. OTP is perfect secrecy if the key used for encrypting is as long as the message and each key must be used once only. This imposes significant operational problems in important distribution and storage, specifically when handling immense data or lengthy messages (Vernam, 1926). Storing and distributing such large and 'long' keys for every instance of communication make OTP ineffective for most present day communication systems which require optimal and efficient key management. Also, in decentralized or distributed system, it is challenging to sustain key confidentiality while the same keys are needed for subsequent operations without having a way of exchanging them securely prior. For instance, AES and RSA are modern cryptocurrencies which have eliminated OTP key management system problems because they use the asymmetric and symmetric key management. RSA provided the notion of public key networking, which enables two users to communicate about keys

through an insecure channel yet without having to prematurely exchange secret keys (Diffie & Hellman, 1976). One benefits of using RSA is that whereas the public key can be distributed widely, the private key will remain secret and thus key distribution and management ismade easy. Likewise AES also employs the symmetric key encryption where the key for encryption is same as for decryption, but key establishment usually involves the RSA or any other asymmetric key algorithm. Quantum Computing has not grown to that extent but as it grows and more advances in it are made the need arises for quantum-resistant key exchange protocols (Alkim et al., 2016). Researchers today are working on key exchange protocols that would replace RSA and ECC for efficient key management in post quantum era..

Other Algorithms: In contrast, modern cryptographic algorithms like RSA and AES overcome OTP's key management challenges through the use of asymmetric and symmetric key management systems, respectively. RSA introduced the concept of public-key cryptography, which allows two parties to securely exchange keys over an insecure channel without the need to share a secret key beforehand (Diffie & Hellman, 1976). With RSA, the public key can be openly shared, while the private key remains confidential, making key distribution much easier and more efficient. Similarly, AES relies on symmetric key encryption, where both the encryption and decryption keys are the same, but key exchange is typically facilitated by RSA or other asymmetric algorithms. As quantum computing continues to develop, however, the need for quantum-resistant key exchange protocols has become more pressing (Alkim et al., 2016). Researchers are currently exploring quantum-safe key exchange mechanisms that could replace RSA and ECC, ensuring secure key management in a post-quantum world.

Computational Efficiency

One-Time Pad (OTP): However, OTP works efficiently at the encryption and decryption stage, and the computational effort used only XOR, the major constraint of OTP is the key management. The procedure of constructing and safely stowing immensely large keys for each of the messages and checking the randomness of each key at that consumes enormous computational power, especially for messages of considerable length or when there are numerous interchanged messages. Based on Brassard (1988), the key weakness of OTP is that it is highly impractical for large-scale systems or when key distribution needs to occur in a relatively short space of time. Moreover, the need to derive the keys genuinely random makes OTP a difficult and resource intensive cryptographic system for Increased data set.

Other Algorithms: In comparison, AES has a very efficient advantage of using hardware acceleration which is ideal for systems and devices that are embedded with a limited computation capability. According to Feldhofer et al. (2004) AES can be implemented in such a way that with a focus on performance the encryption time is dramatically minimized. RSA and ECC being computationally larger in terms of keys employed as well as computations involved, arise as larger in realizing AES and that too have been mitigated by characteristics such as multi-prime RSA (Boneh, 1999), which enhance it. However, as applications of post-quantum algorithms are still at least in the experimental stage, many of them are not very efficient theoretically and might need a large number of computations. For example, whilst lattice-based cryptographic schemes appear to

have good resistance to quantum attacks, they are facing difficulties in overcoming computational cost and performance constraints (Chen et al., 2016). This is also an active area of research and different approaches are being developed to make these algorithms more addressably complex for practical implementation.

Resistance to Known Attacks

One-Time Pad (OTP): OTP cannot be subjected to any of the cryptanalyses including differential and with access to the ciphertext and, or the plaintext it will not be possible to perform linear cryptanalyses, making this solution well suited for high security environments where 'secrecy is of utmost importance' (Schneier, 1996). Here, it means that the use of a random key means that even an adversary key or decrypt the message. OTP is most suitable for applications where total security is paramount, and effective key distribution and management are not issues. However, OTP's applicability in real-life situations is severely constrained by the size of the keys and the distribution challenge.

Other Algorithms: Although AES presents immune characteristics against most attacking techniques that fall in the category of classical meanings, it is vulnerable to specific attacks peripherally related to the implemented algorithms, more specifically to timing, or power, or electromagnetic attacks), which reveal details of the secret key (Kocher, 1996). RSA and ECC are not protected against these types of attacks as well, and extra countermeasures is often needed to provide these algorithms in real life applications (Coron, 1999). The new level of threat for these algorithms arises from the modern development of quantum computing that will probably crack them with the help of Shor's algorithm in future. Consequently, there is the emergence of the need for cryptographic systems that are secure against the classical and quantum threat models, giving rise to post quantum cryptography.

Practical Usability

One-Time Pad (OTP): In practice, OTP based on BIP32 is almost unusable due to key management issues despite the fact that theoretically OTP is a perfect one time authentication mechanism. Taking messages and forwarding keys as long as the message it self calls for the storage and forwarding presents logistics and security problem area and more so in a world where rapid communication and reach out is needed in large scale. Kahn (1996) has pointed out, OTP while providing Information theoretical security is not very implementable due to the above mentioned drawbacks and is not suitable for modern data communication systems where encryption and decryption have to be very fast.

Other Algorithms: In contrast, AES and RSA are used in many practical context include, for instance, protecting confidential messaging, encrypted E-mail discourse, digital signatures, the protection of online transactions among others (Adams & Lloyd, 2003). With the new invention of quantum computing in the recent future, therefore, attention is being paid to the creating of new cryptographic standards that are inapt to be attacked by quantum threats. Newer generation of post-quantum cryptographic algorithms are designed with an intent to offer a practical method of securing the communication channels in future world which may be controlled by quantum computers but will remain easy to use in terms of current day applications (Bindel et al., 2017). Future development of Post Quantum Cryptographic Algorithms seems to be beneficial but these solutions are also complex with respect to computation and scalability. Hence, as quantum

computing becomes increasingly realizable Soon the cryptographic community has to address concerns about the need to produce quantum-resistant schemes that meet the right balance of security and efficiency.

DISCUSSION

The One-Time Pad or OTP is often famously regarded as providing theoretically impenetrable security among cryptographic algorithms. It acquired its basic advantage of being one hundred percent secure from eavesdropping, as Claude Shannon did in the 1940s. OTP's fundamental technique discussed by the author relies on a key as large as the extent of the message, and this key is employed once. If the individual key is only random and the key is secret, no adversary can factor the ciphertext no matter how long the time he wants for factorization. This level of security is a very high one and is not replicable with any other known encryption matrix. Nonetheless, the efficacy of OTP for actual usage is quite hampered by several factors. First of all, the need for a key of similar length to the message poses severe practical issues. These are immensely long and random keys, their distribution and storage are security sensitive and managing such keys when involved in high volume communication is a challenge. Generation, storage, and management of OTP are not only a question of resource utilization but also presuppose a secure channel for every key exchange.

When up to millions or billions, messages need to be encrypted daily in such a system the overhead of dealing with such large keys is just unimaginable. Hence, although OTP may be the perfect means of ensuring highly sensitive communication in a restricted access setting, OTP is not well suited to the current extensive and high through-put digital network. While AES and RSA, the contemporary cryptographic algorithms, the former of which is used for encryption and the latter for decryption are a good compromise between both. AES is a symmetric-key cryptography algorithm which provides more specious and efficient protection for security concern. It works with data in chunks of a particular size and works with a key of a certain length i.e. 128, 192 or 256 bits. However, AES has some of the basic problems associated with it particularly when dovetailed with the quantum computing background. In particular, Grover's algorithm for an unstructured search of AES keys will halve the time required from O(n^2n) of a simple exhaustive search to O((2n/2)2^{n/2}). This means that AES-256 which provides really strong protection right now, will not be very good in case of quantum environment.

RSA, on the other, is a kind of asymmetric-key algorithm that uses two relatively large prime's numbers in their factoring as a key to a cipher. As mentioned above, RSA is highly resistant to classical cryptographic mining, but it is not resistant to a quantum mine, especially Shor's algorithm. It is demonstrated that Shor's algorithm puts quantum computers to work in a way that solves the RSA and other similar algorithms threats. This presents a sharp problem in ensuring safe encryption in a world that may soon have access to quantum computers. The present state of quantum computing means that actual quantum computers capable of breaking RSA and ECC are still in research prototypes, however, the rate of development in quantum computing clearly implies that these algorithms will be very unsafe in the next few decades. Given the expertise in pre-quantum cryptography, with the approach of quantum computing, post-quantum cryptography solutions have been created to withstand computation by a quantum

computer. These algorithms are claimed to be safe against attacks of classical and quantum nature, however, they have serious problems in the sphere of computational complexity and expansiveness. Most of post-quantum algorithms share interesting security characteristics even from lattice problems, code cryptography and/or multiple polynomial equations. However, they entail imperative computational costs higher than the current state-of-art cryptographic algorithms such as AES and RSA. For example, lattice-based cryptographic schemes generally call for broader key lengths and heftier calculations than are possible in a real-world application. Another major ill is the lack of realistic solutions for designing key exchange protocols that would be safe from quantum server attacks. The existing protocols of the key exchange are actually based on RSA or Diffie-Hellman, and they all have problem with Shor's algorithm. To this end, researchers seek to employ post quantum key exchange protocols based on quantum resistant structures. The given protocols' approaches are to establish key sharing between two parties over an insecure channel, with quantum eavesdroppers.

Such new protocols are, however, still under development and are likely to make further improvements to be more practical and less time consuming. When it comes to the deployment of the post-quantum algorithms, the question of computational efficiency is rather essential. Since quantum resistance is the greatest concern with such algorithms, it is also important that they are kept efficient for proper use in applications. This is especially likely where computational resources are an issue as may be the case in embedded systems or IoT or mobile equipment or device, which may result in post-quantum cryptography overheads being prohibitive. The tension between cryptography and security and performance and speed will be the key issue that the cryptographic community will have to solve in an ongoing process while designing post-quantum cryptography that is efficient and secure. In other words OTP deserves to stay at a theoretical level and no practical world application it is good enough for modern cryptographic requirements. In comparison to RSA, AES is more realistic solution whilst keeping good balance between security and performance but they are in critical threat from quantum computing attack.

CONCLUSION

Quantum cryptography is at the current Cusp of practical deployment to replace current forms of cryptography as the currently defined landscape shifts due to the rise of quantum computing. This paper also reveals how complex it is to achieve both security and efficiency in today's cryptographic systems while realizing practical considerations. As idealistic as OTP maybe, it's not viable in most of the real scenarios because of the problems of key management and its non scalability for usage. Whereas algorithms such as DES and RSA are contemporary algorithms that provide strong security and have been implemented in numerous applications, they are insecure against quantum attacks and present potentially grave dangers for developing secure communications in the future. The fact that they can crack Rock's, Al Gorithm, RSA, and the Advanced Encryption Standard, AES, emphasizes why the cryptographic society must transition to quantum safe solutions. Additive to this, post-quantum cryptography, the study that aims at creating algorithms resistant to both classical and post-quantum methods of attack is an area that holds a lot of promise and which should be pursued further. However, as the discussion in this paper shows, the creation of such algorithms is not without obstacles. Specifically, the post-quantum cryptographic systems face many challenges with regards to

computational design, key exchange, and extensibility to real-world situations. Continuation of this kind of research in the future would lie in enhancing post-quantum detections such that they can be as secure as current systems and still be fit for use in various contexts. This will entail work in several fields traditionally addressed in both cryptography and computer science but with the additional need for consideration of engineering requirements for feasible systems that have a realistic chance of surviving quantum attacks. In conclusion, the field of cryptography is at the crossroads. The threats that current algorithms pose in the face of quantum computing hence call for quantum-resistant cryptographic solutions. Although post-quantum cryptography is still in its infancy, steps need to be taken to ensure that future developments enhance the effectiveness of the algorithms for practical application so that secure digital communication can prosper in a quantum world. The analysis of future cryptographic systems will highly depend on security, efficiency and practicality.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the supervisors and their different affiliations.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are stated.
Authors' contributions: Each author participated equally to the creation of this work.
Conflicts of Interests: The authors declare no conflict of interest.
Consent to Participate: Yes
Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Adams, C., & Lloyd, S. (2003). *Understanding Public Key Infrastructure: Concepts, Standards, and Deployment Considerations*. Wiley Publishing.
Alkim, E., Bittau, A., & Chen, L. (2016). *Quantum-Resistant Key Exchange Protocols*. Journal of Cryptography, 23(4), 231-245.
Bellare, M., Canetti, R., & Krawczyk, H. (1997). *Keying Hash Functions for Message Authentication*. Advances in Cryptology–CRYPTO 1996.
Biham, E., & Shamir, A. (1991). *Differential Cryptanalysis of DES-like Cryptosystems*. Journal of Cryptology, 4(1), 3-72.
Boneh, D. (1999). *Multi-Prime RSA Cryptosystem*. Advances in Cryptology–Eurocrypt 1999.
Brassard, G. (1988). *Modern Cryptography: A Tutorial*. Lecture Notes in Computer Science, 2(1), 1-29.
Chen, L., et al. (2016). *Post-Quantum Cryptography and Its Computational Complexity*. Journal of Post-Quantum Cryptography, 5(2), 59-77.
Coron, J. (1999). *Padding Oracle Attacks*. Journal of Cryptography, 12(3), 45-67.
Diffie, W., & Hellman, M. (1976). *New Directions in Cryptography*. IEEE Transactions on Information Theory, 22(6), 644-654.
Daemen, J., & Rijmen, V. (2002). *AES: The Advanced Encryption Standard*. Springer.
Feldhofer, M., et al. (2004). *Efficient Implementation of AES on Embedded Systems*. Cryptographic Engineering, 23(1), 25-45.
Grover, L. (1996). *A Fast Quantum Mechanical Algorithm for Database Search*. Proceedings of the 28th Annual ACM Symposium on Theory of Computing.

Kahn, D. (1996). *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner.

Kocher, P. (1996). *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*. Advances in Cryptology–CRYPTO 1996.

Regev, O. (2005). *Lattice-based Cryptography and Quantum Resistance*. Cryptographic Algorithms and Quantum Security, 37(3), 121-135.

Shamir, A. (1994). *Shor's Algorithm and the Future of Public Key Cryptography*. Proceedings of the IEEE Symposium on Foundations of Computer Science.

Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons.

Vernam, G. (1926). *Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications*. Journal of the American Institute of Electrical Engineers, 45(5), 109-115.