Quantum Resistant Cryptography and Cyberwarfare

Chuck Easttom
Vanderbilt University and Georgetown University, USA

william.easttom@Vanderbilt.Edu

Abstract. Quantum computing poses a significant threat to conventional cryptographic systems that rely on the difficulty of mathematical problems such as integer factorization and discrete logarithms. These systems underpin much of the current security infrastructure, including public key cryptography and digital signatures. As quantum computers approach practical viability, there is an urgent need to transition to quantum-resistant cryptographic solutions that can secure digital communications against adversaries equipped with quantum capabilities. This paper explores the landscape of quantum-resistant cryptography, focusing on those algorithms that have emerged either as standards or as leading algorithm. Furthermore, the paper examines the progress of standardization efforts, such as the National Institute of Standards and Technology (NIST) Post-Quantum Cryptography (PQC) initiative, and the implications of deploying these algorithms in existing systems. By addressing the practical considerations for adoption, this study aims to provide a comprehensive overview of the current state and future directions of quantum-resistant cryptography, ensuring robust security in a post-quantum world.

Keywords: Quantum computing, NIST, Cryptography

1. Introduction

Cyber warfare includes both offensive and defensive elements. A growing concern is the offensive potential for quantum computers to breach currently used cryptographic algorithms. Quantum computing has made substantial advances in the past 10 years. In 2022, IBM announced their Osprey processor with 433 qubits. IBM Condor processor released in 2024 has 1,121 qubits (Puthussery & Poonia, 2024). Atom computing has reached 1180 qubits (Russell, 2023). These facts demonstrate the rapidly increasing pace of quantum computing development. However, the United States is not the only nation pushing forward with quantum computing advances. The JiuZhang has been China's foremost quantum processor. It utilizes photons as qubits. The JiuZhang 3 has 255 qubits (Swayne, 2023). However, China has also been making advances with superconducting qubits. China also announced in October of 2024 that they had used quantum annealing to factor a 50-bit integer. As RSA typically uses 2048 or 4096 bit keys, this is not an immediate danger (McCann, 2024). However, this advance highlights the coming danger of quantum computing.

Advances in quantum computing promise improvements across a number of computing tasks. Grover's algorithm provides a substantial improvement in searching unordered lists over classical computing approaches. Grover's algorithm also promises substantial improvements in processing and analyzing large datasets (Khanal, et al., 2021). Quantum computers can potentially solve optimization problems (e.g., in logistics, finance, or supply chain management) exponentially faster than classical computers. Quantum-inspired algorithms may help approximate solutions to problems where exact answers are computationally infeasible (Fuller, et al., 2024). However, in addition to these advances posed by quantum computers, there are also new threats, particularly to cybersecurity.

The concern for cybersecurity, and thus cyber warfare, stems from the nature of current asymmetric cryptographic algorithms. Virtually all aspects of network security depend, at least to some degree on asymmetric cryptography. This includes e-commerce, virtual private networks, and many authentication protocols (Faruk, et al., 2022). Currently used algorithms are secure because they are based on mathematical problems that are difficult to solve. By difficult, it is meant that they cannot be solved in practical time using classical (i.e. non-quantum) computers. RSA is based on the difficulty of factoring integers into their prime factors (Easttom, 2022). Diffie-Hellman is based on the difficulty of solving the discrete logarithm problem (Kraft & Lindell, 2018). The various improvements to Diffie-Hellman such as Elgamal and MQV are also based on the difficulty of solving the discrete logarithm problem. Elliptic Curve Cryptography, which includes several algorithms, is based on the difficulty of solving discrete logarithm problems of a random elliptic curve element with respect to a publicly known base point (Hankerson & Menezes, 2021). The problem for cyber security is that it has already been proven that these mathematical problems can be solved with quantum computers in a practical amount of time.

Because it has been proven that quantum algorithms can solve the problems that form the basis for current asymmetric cryptography, in a time that is practical, quantum computing will eventually render existing asymmetric or public key algorithms obsolete and ineffective (Rawat, et al., 2023). That means that the cryptography used for key exchange in VPN's, digital certificates, all e-commerce solutions, and even some

network authentication protocols will no longer be secure. TLS which is widely used to secure internet traffic including web traffic, email, and even voice over IP, will no longer be secure (Easttom, 2022; Faruk, et al., 2022). While these dangers to cyber security are not immediate because quantum computing is not yet a practical, usable reality, it is important for anyone in cyber security to be aware of the problem and to be familiar with the progress towards solutions.

2. Analysis

In the following subsections the issues related to quantum resistant cryptography are explored in sufficient detail to provide a cybersecurity professional to understand the issues and to make critical decisions for quantum resistant cryptography.

2.1 Mathematical Foundations

The problem can be elucidated by first examining the mathematical reasons why quantum computers are a threat to currently used cryptographic algorithms. Currently used asymmetric algorithms are based on what are called trap door functions. These are mathematical functions that are quite easy to solve in one direction, but very difficult to solve in the reverse direction. As an example of this process, consider the key generation algorithm for RSA (Imam, et al., 2021):

1. Generate two large random primes, p and q, of approximately equal size such that their product n = pq is of the required bit length (such as 2048 bits, 4096 bits, and so on):
2. Let n = pq
3. Let m = (p – 1)(q – 1)
4. Choose a small number e, co-prime to m. (Note: Two numbers are co-prime if they have no common factors.)
5. Find d, such that de mod m ≡1
6. Now you have both the public and private keys:
    a. Publish e and n as the public key.
    b. Keep d as the secret key.

The reasons why these particular steps work are rooted in number theory topics such as Euler's totient and modular arithmetic (Easttom, 2021). Delving into number theory is beyond the scope of this current paper. However, the steps themselves only require quite rudimentary mathematics. For those readers interested in the mathematics, there are resources available (Easttom, 2022; Kota, et al., 2022; Paar, Pelzl, & Güneysu, 2024). Encryption and decryption, once keys have been generated and a public key is published, are actually quite simple:

Encrypt:

$C = M^e \bmod n$

Put another way: Compute the cipher text $c = m^e \bmod n$.

Decrypt:

$P = C^d \bmod n$

Put another way: Uses his private key (d,n) to compute $m = c^d \bmod n$.

A practical example should help elucidate this process:

1. Select primes: $p = 17$ and $q = 11$.
2. Compute $n = pq = 17 \times 11 = 187$.
3. Compute $\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$.
4. Select e: gcd(e,160) = 1; choose $e = 7$
5. Determine d: $de = 1 \bmod 160$ and $d < 160$.
   Value is d = 23 since $23 \times 7 = 161 = 10 \times 160 + 1$.
6. Publish public key KU = {7,187}
7. Keep secret private key KR = {23,187}

Now as an example of how this works, consider the number 3 as the plain text one wishes to encrypt.
Remember e =7, d=23, and n =187
Encrypt

1. Ciphertext= Plaintext^{e} mod n or
2. Ciphertext = 3^{7} mod 187
3. Ciphertext =2187 mod 187
4. Ciphertext = 130

2. Decrypt
    1. Plaintext = Ciphertext ^{d} mod n
    2. Plaintext = 130^{23} mod 187
    3. Plaintext = 4.175390541341311636704579 7e+48 mod 187
    4. Plaintext = 3

Implementing the mathematics is not overly difficult. But note that the public key contains n and e. The n value was generated by multiplying the prime numbers p and q. Multiplying two prime numbers is a trivial task that can be accomplished by most primary school students. However, taking the n, and factoring it to retrieve the p and q is computationally infeasible with classical computers. Peter Shor of MIT created Shor's algorithm (Rossi, et al., 2022). This is a hybrid algorithm that performs some steps on a classical computer and others on a quantum computer. It has been shown that Shor's algorithm can factor an integer (such as the previously mentioned n) into its prime factors in polynomial time (Iqbal & Zafar, 2024). The general steps of Shor's algorithm are shown here:

Step 1: Pick a random number *a* that is between 1 and N (the N is what you wish to factor)

Step 2 Compute gcd (a,N)

Step 3: If gcd(a,N) != 1 then we are done

Step 4: if gcd(a,N)= 1 then we used the quantum period subroutine to find r. The quantum period function sub steps are given here:

Quantum Step 1: Initialize the registers

Quantum Step 2: Construct f(x) quantum function and apply to the state

Quantum Step 3: Apply inverse quantum Fourier transform to the input register

Quantum Step 4: Measure

Quantum Step 5: Perform classical continued fraction expansion to find approximations.

Quantum Step 6: check if you have found the period, if so, you are done

Quantum Step 7: Otherwise obtain more candidates for r

Step 5: If r is odd go back to step 1

Step 6: If $a^{r/2} \equiv -1 (\text{mod } N)$ then go back to step 1

Step 7: otherwise, you have found nontrivial factors of N and you are done

The actual steps of Shor's algorithm are not particularly difficult to understand, however, the most important fact to realize is that this algorithm will render the integer factorization problem solvable in polynomial time with a quantum computer, thus making RSA no longer secure. Shor's algorithm can factor an integer N in polynomial time (actual time is log N). This is significantly faster than the most efficient known classical factoring algorithm (the general number field sieve) which works in sub-exponential time. It must also be noted that Shor's algorithm can also be used to solve the discrete logarithm problem, which is the basis for the security of Diffie-Hellman, and its variants (Raya & Mariyappn, 2020). Shor's algorithm can also solve the variation of a discrete logarithm related to an elliptic curve used in elliptic curve cryptography (Larasati & Kim, 2021)

2.2 Quantum Resistant Cryptography Algorithms

Replacements for currently used asymmetric algorithms are of critical importance. Fortunately, there are existing algorithms which are resistant to quantum computing attacks. While there have been numerous mathematical approaches to quantum resistant cryptographic algorithms, lattice-based cryptography has emerged as a leader and in fact have been chosen in several standards. For this reason, lattice-based cryptography will be the only quantum resistant cryptography referenced in this current study. Lattice based cryptography involves the construction of cryptographic primitives based on lattices (Wang, Xu, & Yu, 2023). A cryptographic primitive is an algorithm such as a symmetric cipher, asymmetric cipher, cryptographic hash, or message authentication code that is part of a cryptographic application. Essentially, a complete cryptographic system must account for both confidentiality and integrity of the message. This often involves encrypting the message for confidentiality, exchanging symmetric cryptographic keys via some asymmetric algorithm, ensuring integrity with a cryptographic hash function, and digitally signing the message. Each of these aspects of security is accomplished via a different algorithm, a specific cryptographic primitive. The cryptographic primitives are used in combination to provide a complete cryptographic system.

One of the most commonly used problems for lattice cryptography is the Shortest Vector Problem (SVP). This mathematical problem is that given a particular lattice, how do you find the shortest vector within the lattice? (Shorts & Kim, 2024). More specifically, the SVP problem involves finding the shortest non-zero vector in the vector space V, as measured by a norm, N. A norm is a function that assigns a strictly positive length or size to each vector in a vector space (Nestor, 2024). The SVP problem is a good choice for post-quantum computing.

One lattice-based cryptosystem is NTRU. It was invented by Hoffstien, Pipher and Sillverman. It is the most well-known and widely studied lattice based cryptographic system (Easttom, 2019). NTRU is a cryptosystem that provides both encryption and digital signatures(Pellet-Mary & Stehlé, 2021). It has been shown to be resistant to Shor's algorithm and unlike many other asymmetric cryptographic systems. NTRU is more efficient than RSA even in a classical computing context. That makes it a viable option for classical computing.

The CRYSTALS-Kyber (Cryptographic Suite for Algebraic Lattices - Kyber) algorithm is a post-quantum encryption scheme designed to provide security against the potential threats posed by quantum computers (Avanzi, et al., 2019). It is part of the CRYSTALS suite (which also includes the CRYSTALS-Dilithium signature algorithm) and was selected by the U.S. National Institute of Standards and Technology (NIST) as a finalist in its Post-Quantum Cryptography Standardization process. This suite of algorithms uses lattice based mathematical problems, specifically Learning with Errors in a lattice.

2.3 QKD

In addition to quantum resistant cryptography, quantum key distribution (QKD) is another, related issue. The issue of QKD is summarized as follows “Quantum key distribution utilizes the unique properties of quantum mechanical systems to generate and distribute cryptographic keying material using special purpose technology. Quantum cryptography uses the same physics principles and similar technology to communicate over a dedicated communications link. Published theories suggest that physics allows QKD or QC to detect the presence of an eavesdropper, a feature not provided in standard cryptography.” (NSA, 2024b).

There are numerous quantum key distribution protocols available. BB84 was first published in 1984. The Six State Protocol was published in 1998. More recent protocols include KMB09 and SARG04 (Ali & Benlahcene, 2024). In addition to there being protocols for QKD, there have been multiple implementations of QKD. In 2007 Los Alamos National Laboratory created a 148 km QKD link using the BB84 protocol and fibre optic cable (Easttom, 2021).

3. National Security Impact Analysis

As quantum computing advances, it will have a significant impact on cyber security. Quantum computers will render current asymmetric (i.e., public key) cryptographic protocols obsolete (Azhari & Salsabila, 2021; Easttom, 2021). Symmetric algorithms will not be affected so significantly. Algorithms such as AES, Blowfish, and Serpent will still be usable, but may need longer keys. Given that so much of communications, both civilian and military, depends on asymmetric algorithms for key exchange and digital signatures, this poses a substantial national security risk. While quantum computers have not yet reached the point to break these algorithms, they are on track to do so. When quantum computers reach that point, they are referred to as cryptanalytically relevant quantum computers (CRQC) (Steinwandt & Xuereb, 2024).

The United States National Counterintelligence and Security Center stated, "Without effective mitigation, the impact of adversarial use of a quantum computer could be devastating to national security systems and the nation, especially in cases where such information needs to be protected for many decades." (NCSC, 2021). The United States Army has designated a quantum information research centre to research military applications of quantum computing (U.S. Army, 2023).

China has traditionally been focusing on photonic quantum computing. However, they also have developed superconducting qubit quantum computers. Chinese 66-qubit Zuchongzhi 2 processor has outperformed Googles Sycamore processor on several algorithms. The Zuchongzhi 2 is photon based and is much faster than the superconducting qubit-based processors. The name Zu Chonzhi is that of an astronomer and mathematician circa 500 AD. In 2023, China announced a 176-qubit version of Zuchongzhi (Jai, 2023)' This project was spearheaded by University of Science and Technology of China (USTC).

In May 2024, China introduced its largest quantum computing chip to date, featuring 504 qubits named Xiaohong (Swayne, 2024). This chip is being integrated into a new quantum computer by QuantumCTek and China Telecom Quantum Group, aiming to provide global researchers access via a quantum computing cloud platform. The chip was developed by the Center for Excellence in Quantum Information and Quantum Physics under the Chinese Academy of Sciences (CAS).

In October of 2024, a research team at Shanghai University used D-Waves quantum annealing system broke a 22-bit RSA key (Swain, 2024). The research team was able to subsequently break a 50-bit RSA key (Salas, 2024). The key sizes used in these expiriments are orders of magnitude smaller than real RSA keys which are typically from 2048 to 4096 bits. However, the experiment foretells things to come.

China has also made substantial advances in quantum key distribution. Researchers in China have developed a high-speed quantum key distribution (QKD) system to generate secret keys at a rate exceeding 110 Mb/s over a 10 km standard optical fibre (Swayne, 2023). Researchers at the University of Science and Technology of China announced a 1002 km point to point QKD connection (USTC, s2023). This is a record for QKD without using relays. China plans the launching of 2 to 3 quantum communication satellites in 2025 (Jones, 2025)

While the ability to break currently used cryptographic algorithms is one of the clear dangers posed by quantum computing, there are others. Quantum sensors are another technology that promises advantages in the realm of defence. Quantum sensors could potentially detect submarines and even stealth aircraft (van Amerongen, 2021). They may also provide highly accurate position, navigation and timing, without the need to communicate with GPS satellites.

In addition to the threat posed by a rival nation state being able to break widely used asymmetric algorithms, there is a growing issue with foreign intelligence agencies targeting quantum research. According to the FBI nation states including the People's Republic of China are engaging in espionage to attempt to gain an advantage in quantum computing. Targets can include businesses and academia, in addition to government agencies. The FBI is striving to counter this: "The Quantum Information Science Counterintelligence Protection Team leverages partnerships across government, academia, and private industry to protect progress in this field and thwart nation-state and other adversaries' efforts to steal innovations. The QISCPT is working within the interagency framework of the National Counterintelligence Task Force to ensure that the U.S. and like-minded nations do not lose momentum in the successful development of quantum technology." (FBI, 2024).

4. Standards

Fortunately, there are a number of standards one can use to begin implementation of quantum resistant cryptographic protocols. These standards will be discussed in the following subsections.

4.1 NIST

The NIST Post-Quantum Cryptography (PQC) Standards are a set of cryptographic algorithms selected and standardized by the National Institute of Standards and Technology (NIST) to address the vulnerabilities of traditional cryptographic methods in the face of quantum computing advancements. These standards focus on replacing widely used algorithms like RSA, DSA, and ECC, which are susceptible to quantum attacks, with quantum-resistant (or post-quantum) cryptographic algorithms. NIST has selected algorithms to be standardized (Ran, Sung, & Jun, 2024):

- CRYSTALS-KYBER for Public-key Encryption and Key-establishment Algorithms. Note, NIST is now referring to this algorithm as Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM).

- CRYSTALS-DILITHIUM for Digital Signatures
- FALCON for Digital Signatures
- SPHINCS+ for Digital Signatures

4.2 FIPS

Federal Information Processing Standards (FIPS) typically provide guidance for U.S. government agencies to implement NIST standards. There are three FIPS standards related to quantum resistant cryptography.

FIPS 203 (ML-KEM or CRYSTALS-Kyber): This algorithm is designed for key establishment, ensuring that sensitive information can be securely exchanged, even in the presence of quantum-capable adversaries. It stands out for its efficiency in encryption and decryption, making it suitable for a wide range of applications, from secure communications to cloud storage. More details can be found at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

FIPS 204 (ML-DSA or CRYSTALS-Dilithium): Targeting digital signatures, ML-DSA provides a robust mechanism for verifying identities and ensuring the integrity of messages and documents. Its balance of speed and security makes it a strong candidate for use in software updates, code signing, and any scenario where the authenticity of information is critical. More details can be found at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf

FIPS 205 (SLH-DSA or SPHINCS+): Also focused on digital signatures, SLH-DSA offers an alternative that emphasizes resilience against attacks, including those leveraging quantum computing. While it is slightly less efficient than ML-DSA, its stateless nature provides an additional layer of security, particularly for applications requiring long-term integrity. More details can be found at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf

4.3 NSA CNSA Suite 2.0

The National Security Agency has published the Commercial National Security Algorithm Suite 2.0 (NSA, 2024). This document identifies algorithms that can be used for National Security Systems (NSS). Many of the algorithms are the same found in FIPS and NIST standards. The NSA provides the following chart:

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
ML-KEM (aka CRYSTALS-Kyber)	Asymmetric algorithm for key establishment	FIPS PUB 203	Use Category 5 parameter, ML-KEM-1024, for all classification levels.
ML-DSA (aka CRYSTALS-Dilithium)	Asymmetric algorithm for digital signatures in any use case, including signing firmware and software	FIPS PUB 204	Use Category 5 parameter, ML-DSA-87, for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels.
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. LMS SHA-256/192 is recommended.
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels.

Figure 1: CNSAS 2.0

The preceding chart provides an overview of specific algorithms to be implemented for various cryptographic applications.

5. Conclusions

It is quite clear that there needs to be a clear plan for implementing quantum resistant algorithms, as well as quantum key distribution, in both the military and civilian sectors. Failure to do so will leave not only defense systems, but economic networks and national infrastructure vulnerable to cyber-attacks. Defensive preparation for cyber warfare requires the implementation of quantum resistant algorithms.

There are several key actions that can be taken to address the cybersecurity and national security issues related to quantum computing. The clearest step that should be taken is initiating plans to integrate quantum resistant cryptography into the infrastructure. That means digital certificates that utilize quantum resistant algorithms. Another step that is recommended is for organizations, particularly those related to national security, to begin planning for the integration of quantum key distribution for securing network communications.

References

Ali, Sellami, and Benlahcene Djaouida. "Optimizing Quantum Key Distribution Protocols using Decoy State Techniques and Experimental Validation." *Engineering, Technology & Applied Science Research* 14, no. 4 (2024): 15133-15140.

Avanzi, Roberto, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. "CRYSTALS-Kyber algorithm specifications and supporting documentation." *NIST PQC Round* 2, no. 4 (2019): 1-43.

Azhari, R., & Salsabila, A. N. (2024). "Analyzing the Impact of Quantum Computing on Current Encryption Techniques." *IAIC Transactions on Sustainable Digital Innovation (ITSDI),* 5(2), 148-157.

Easttom, C. (2019). "An analysis of leading lattice-based asymmetric cryptographic primitives. " *In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0811-0818). IEEE.

Easttom, C. (2021). "Quantum computing fundamentals." Addison-Wesley Professional.

Easttom, C. (2022). "Modern Cryptography: Applied Mathematics for Encryption and Information Security." Cham: Springer International Publishing.

Faruk, M.J.H., Tahora, S., Tasnim, M., Shahriar, H. and Sakib, N., 2022, May. "A review of quantum cybersecurity: threats, risks and opportunities." In *2022 1st International Conference on AI in Cybersecurity (ICAIC)* (pp. 1-8). IEEE.

FBI (2024). "Protecting Quantum Science and Technology: Foreign adversaries are increasingly targeting a wide range of U.S. quantum companies, universities, and government labs." Retrieved from https://www.fbi.gov/news/stories/protecting-quantum-science-and-technology

Fuller, B., Hadfield, C., Glick, J. R., Imamichi, T., Itoko, T., Thompson, R. J., ... & Mezzacapo, A. (2024). "Approximate solutions of combinatorial problems via quantum relaxations." *IEEE Transactions on Quantum Engineering.*

Gouzien, É., & Sangouard, N. (2021). "Factoring 2048-bit RSA integers in 177 days with 13 436 qubits and a multimode memory." *Physical review letters*, 127(14), 140503.

Hankerson, D., & Menezes, A. (2021). "Elliptic curve cryptography." *In Encyclopedia of Cryptography, Security and Privacy* (pp. 1-2). Berlin, Heidelberg: Springer Berlin Heidelberg.

Imam, Raza, Qazi Mohammad Areeb, Abdulrahman Alturki, and Faisal Anwer. "Systematic and critical review of rsa based public key cryptographic schemes: Past and present status." *IEEE access* 9 (2021): 155949-155976.

Iqbal, S. S., & Zafar, A. (2024). "Enhanced Shor's algorithm with quantum circuit optimization." *International Journal of Information Technology*, 16(4), 2725-2731.

Jia, L. (2023). "China's 176-qubit Quantum Computing Platform Goes Online." Retrieved from https://english.cas.cn/newsroom/cas_media/202306/t20230601_331269.shtml

Jones, A. (2024). "China to launch new quantum communications satellites in 2025." *Space News*. Retrieved from https://spacenews.com/china-to-launch-new-quantum-communications-satellites-in-2025/

Khanal, B., Rivas, P., Orduz, J., & Zhakubayev, A. (2021). "Quantum machine learning: A case study of Grover's algorithm." *In 2021 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 79-84). IEEE.

Kota, C. M., & Aissi, C. (2022, March). Implementation of the RSA algorithm and its cryptanalysis.

Kraft, J., & Washington, L. (2018). "An introduction to number theory with cryptography." Chapman and Hall/CRC.

Larasati, H. T., & Kim, H. (2021). "Quantum cryptanalysis landscape of Shor's algorithm for elliptic curve discrete logarithm problem." *In Information Security Applications: 22nd International Conference, WISA 2021,* Jeju Island, South Korea, August 11–13, 2021, Revised Selected Papers 22 (pp. 91-104). Springer International Publishing

McCann, K. (2024) Cracking with Quantum: What Breakthrough Research Means. Retrieved from https://cybermagazine.com/articles/cracking-with-quantum-what-breakthrough-research-means

NCSC (2021). "Protecting Critical and Emerging U.S. Technologies from Foreign Threats." Retrieved from https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_Emerging%20Technologies_Factsheet_10_22_2021.pdf

Nestor, T. (2024). "Theoretical Approaches to Solving the Shortest Vector Problem in NP-Hard Lattice-Based Cryptography with Post-SUSY Theories of Quantum Gravity in Polynomial Time." *Cryptology ePrint Archive.*

NSA (2024). “The Commercial National Security Algorithm Suite
2.0 and Quantum Computing FAQ.” Retrieved from https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF

NSA (2024b). “Quantum Key Distribution (QKD) and Quantum Cryptography (QC).” Retrieved from https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

Paar, C., Pelzl, J., & Güneysu, T. (2024). Understanding Cryptography: From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms (pp. 1-543). Springer.

Pellet-Mary, Alice, and Damien Stehlé. "On the hardness of the NTRU problem." In *Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part I 27*, pp. 3-35. Springer International Publishing, 2021.

Puthussery, E. S., & Poonia, R. C. (2024). “Quantum Computing’s Path to Supremacy: Progress in the NISQ Epoch.” *In International Conference on Innovative Computing and Communication* (pp. 315-325). Singapore: Springer Nature Singapore.

Ran, C. Y., Sung, C. Y., & Jun, L. H. (2024). Analysis of NIST PQC Standardization Process and Round 4 Selected/Non-selected Algorithms. *Convergence Security Journal*, *24*(2), 71-78.

Rawat, R., Chakrawarti, R.K., Sarangi, S.K., Patel, J., Bhardwaj, V., Rawat, A. and Rawat, H. eds., 2023. *“Quantum Computing in Cybersecurity”*. John Wiley & Sons.

Raya, A., & Mariyappn, K. (2020). “Diffie-Hellman instantiations in pre-and post-quantum world: A review paper.” *In 2020 Fifth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)* (pp. 130-136). IEEE.

Rossi, M., Asproni, L., Caputo, D., Rossi, S., Cusinato, A., Marini, R., ... & Magagnini, M. (2022). “Using Shor’s algorithm on near term Quantum computers: a reduced version.” *Quantum Machine Intelligence*, 4(2), 18.

Russell, J. (2023). “Atom Computing Wins the Race to 1000 Qubits.” Retrieved from https://www.hpcwire.com/2023/10/24/atom-computing-wins-the-race-to-1000-qubits/

Salas, J. (2024). “No, Chinese quantum computers haven't hacked military-grade encryption.” Retrieved from https://newatlas.com/quantum-computing/chinese-quantum-computer-hack-rsa-aes-military-grade-encryption/

Storts, N., & Kim, S. (2024). Lattice-Based Cryptography and the Shortest Vector Problem. *Undergraduate Scholarly Showcase*, *6*.

Steinwandt, R., & Xuereb, A. (Eds.). (2024). “Toward a Quantum-Safe Communication Infrastructure” (Vol. 64). IOS Press.

Swain, G (2024). “Chinese researchers break RSA encryption with a quantum computer.” Retrieved from https://www.csoonline.com/article/3562701/chinese-researchers-break-rsa-encryption-with-a-quantum-computer.html

Swayne, M. (2023). “Chinese Scientists Set Record for Generating Secret Keys for QKD System.” *Quantum Insider.* Retrieved from https://thequantuminsider.com/2023/03/20/chinese-scientists-set-record-for-generating-secret-keys-for-qkd-system/

Swayne, M. (2024). “Chinese Researchers Develop 504-Qubit Superconducting QC Chip, Build Partnership for Cloud Access.” *Quantum Insider*. Retrieved from https://thequantuminsider.com/2024/04/27/chinese-researchers-develop-504-qubit-superconducting-qc-chip-build-partnership-for-cloud-access

U.S. Army (2023). “Army designates Quantum Information Science Research Center.” Retrieved from https://www.army.mil/article/268072/army_designates_quantum_information_science_research_center

USTC (2023). “Scientists achieve 1,000 km quantum key distribution.” Retrieved from https://phys.org/news/2023-06-scientists-km-quantum-key.html

van Amerongen, M. (2021). “Quantum technologies in defence & security.” *NATO Review*. Retrieved from https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html

Wang, X., Xu, G., & Yu, Y. (2023). “Lattice-Based Cryptography: A Survey.” *Chinese Annals of Mathematics, Series B,* 44(6), 945-960.