Extended Abstract   
Post-quantum Cryptographic Primitives

Lake Bu

**Abstract:**

In this report we discuss the necessity and urgency of post-quantum cryptographic primitives. By showing the inadequacy of the classic cryptographic primitives under post-quantum computation power, developing a newer generation of those primitives seems to be crucial in near future. Therefore, we briefly introduce several candidates of post-quantum cryptographic systems, which are believed to be the likely competitors for the national standard for encryption. In the end, we suggest to build the hardware version of those primitives, for their higher efficiency and stronger security than the classic ones.

1. **Introduction**

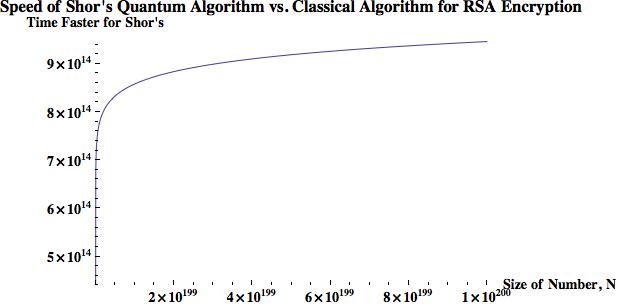
In the past three years, media and security experts have been sending out the warning to all groups and individuals who rely on the security of classic encryption, that quantum commuting will have a enormous negative impact on today’s encryption systems [1, 2, 3, 4, 5]. Some put it as straightforwardly as “Quantum computing kills encryption”. Many suggested that at least the current encryption schemes are in grave situation and may not last long.

1. *Classic Encryptions Vulnerable to Quantum Computers*

Table I. provides a list of popular encryption schemes that are considered as no longer secure in the post-quantum era [6]. In this list once can find both symmetric and asymmetric encryption schemes, and schemes favored by both industry and academia. For example, the popular algorithms such as AES-128, RSA-2048, and ECC-256, may all become unusable when quantum computers are reachable.

|  |  |
| --- | --- |
| Table I. The Encryption Algorithms No Longer Secure | |
| **Algorithm** | **Secure in Post-quantum Era?** |
| RSA-1024, -2048, -4096 | No |
| Elliptic Curve Crypto (ECC)-256, -521 | No |
| Diffie-Hellman | No |
| ECC Diffie-Hellman | No |
| AES-128, -192 | No |

A figurative illustration of the vulnerability of these classical algorithms is shown in Fig. 1 [7]. For a “breakable” RSA system with key size of 768-bit (232 decimal digits), it can take up to 2 years for classic algorithm and computers to break the encryption, while for quantum-computers, 1 nanosecond. The complexity for a quantum algorithm against RSA system is merely (log N)2(log(log (N))(log(log(log(N))), where N stands for the number of decimal digits of the encryption key.

  
Figure 1. Speed comparison of Shor’s algorithm vs. classical algorithm   
in breaking a RSA encrypted cipher [7].

With quantum algorithms, the security level of many classic encryption algorithms can drop drastically. Table II. shows such a case [8], where under the attackers of quantum computers, AES-128, RSA-2048, and RSA-15360 all fail to meet the 112-bit minimum security level recommended by the National Institute of Standards and Technology (NIST) [9].

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Table II. Equivalent Security Levels of AES and RSA under Attacks from Classic and Quantum Computers | | | | | | |
| Attack Platform | Symmetric Encryption | | | Asymmetric (Public-key) Encryption | | |
| Algorithm | Key Size | Security Level | Algorithm | Key Size | Security Level |
| Classic Computers | AES-128 | 128 | 128 | RSA-2048 | 2,048 | 112 |
| AES-256 | 256 | 256 | RSA-15360 | 15,360 | 256 |
| Quantum Computers | AES-128 | 128 | 64 | RSA-2048 | 2,048 | 25 |
| AES-256 | 256 | 128 | RSA-15360 | 15,360 | 31 |

Grover’s algorithm [10] is used against symmetric encryption (e.g., AES) for key search, which reduces the security level by half. Thus increasing AES key size to 256 bits will be barely enough in terms of post-quantum encryption. On the other hand, Shor’s algorithm [11] is able to solve the integer factorization problem efficiently, and so increasing the key size of RSA will not help that much.

1. *Urgency of the Issue*

As shown in Fig. 2, NTRU Innovation posted a projected probability of quantum computers arrival timeline [12]. In early 2015 the estimation was that quantum computers would not come until 2038. However, in late 2015 when several critical breakthrough were achieved by Microsoft, IBM, Google etc., the estimation of quantum computers’ arrival was brought up to as early as 2026.

Moreover, the figure indicates that security infrastructure for post-quantum era must be built before the arrival of general purpose quantum computers, which leaves less than 5 years (from 2020 to later than 2024) from now.

It is notable that more significant achievements have been made in the past two years (c.f. Section I. C.), and so the arrival timeline curve could be even more aggressive than Fig. 2.

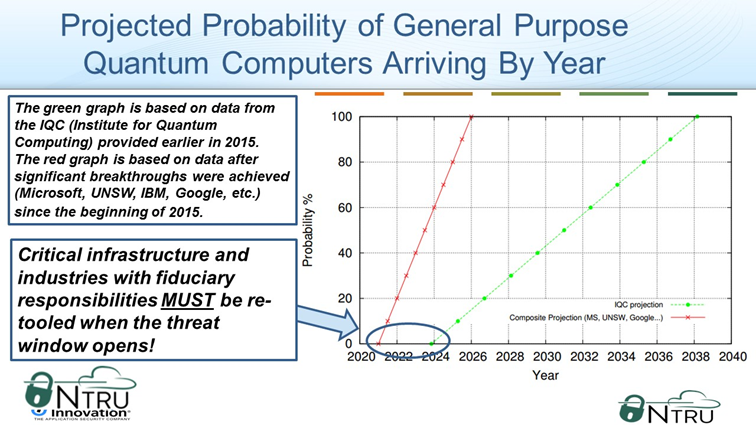


Figure 2. Projected probability of general purpose quantum computers arriving by year.

Although some researchers believe that the life of classic cryptographic schemes still can be extended by using large keys (i.e., a terabyte-size key) [13], their proposed modification to the classic schemes seems not practical. Quantum computer scientists stated that using large keys can be “extremely precarious”, and “vulnerable to even a modest improvement in algorithms or hardware” [14].

Research labs in companies, such as Microsoft, are optimistic about the timeline by claiming the arrival in 5 years [15]. NIST stated 15 years, and is actively evaluating the candidates of the next encryption standard since 2017 [16], which covers the areas of encryption, signing, and key exchange.

It is notable that up to November 29, 2018, among the 69 submissions (5 later withdrew) to NIST, 21 of them are lattice-based algorithms, 18 code-based, and the rest are hash-based and others. Clearly, the lattice- and code-based cryptographic systems are the most probable contenders for the post-quantum cryptographic standard.

1. *Current Status of Quantum Computers*

Several major achievements of quantum computers have been made in the past two years. IBM announced a 50-qubit quantum computer in 2017, followed by a 72-qubit computer from Google in 2018. Intel confirmed development of a 49-qubit superconducting test chip, called "Tangle Lake" in 2018. Also in the same year, 16 superconducting qubits and 18 fully entangled photon qubits computers were made, which is the largest entangled state achieved so far with individual control of each qubit.

While the increase of the number of qubits may seem encouraging, there are still few issues that need to be addressed, before one can anticipate the coming of quantum supremacy, meaning a quantum computer with 49 qubits, whose two-qubit error rate is below 0.5% [17].

The first problem is Quantum Error Correction (QEC), which was initially explored by Shor (the same researcher with Shor’s algorithm) in 1995 [18]. Just as error correction in classic bits on silicon chips, qubits also have reliability issues and demands a much larger overhead. To encode one usable and reliable (fault-tolerant) qubit, 10-50 qubits have to be involved [19].

In addition, computation verification [20] is another research that assists the reliability of quantum computers. It is a relatively new area comparing with QEC and only a few people are working on it.

1. **Public-key Systems for Post-quantum Era**

As mentioned previously, the lattice- and code-based cryptographic schemes are the most likely to be involved in the encryption standard in quantum era. The latter is faster than the former but requires a much larger key size, while both are faster than the classic RSA public-key scheme. In this section we briefly introduce the work principle of the two algorithms.

It is notable that although the lattice-based schemes are usually considered as a more promising technique than code-based schemes, its security reduction (hardness) is relatively new. Some have said that for now, the code-based schemes are still a safer bet since it has withstood many years of crypto-analysis.

1. *Code-based Cryptographic Systems*

McEliece Cryptosystem is a code-based scheme introduced four decades ago [21]. It leverages the classic error control codes (ECCs) to form a public-key system.

For a classic linear t-error control code C, it usually has a generating matrix G, where for a given message m, we have mg = v C. The codeword v has capability of fault tolerance up to t random error bits. The error correction algorithm is closely related to G. In this classic scheme, there is no obfuscation or encryption functionality.

However, McEliece system, two invertible binary square matrices S and P are involved to obfuscate G, where the product of the three matrices (denoted as G’) and t will serve as the public key, and {S, P, G} the private key. Anyone with G’ is able to encode a plaintext message m with the obfuscated matrix, and further obfuscate it into c (the ciphertext) with an arbitrary error vector e weighted t, before sending it to the receiver:

= c (1)

On receiving c, the receiver uses {S, P, G} and computes the inverse of S and P, the error correction algorithm related to G, with which the receiver can successfully decrypt m from c:

] (2)

The code-based schemes, although run under a fast encryption and decryption speed (most of its operations are upon binary matrices), requires a large key size. To make it secure enough (128-bit of security level) against quantum computer attacks, binary Goppa codes with parameters of n = 6960, k = 5413, t = 119 were proposed, leading to a key size of approximately one megabyte (1 MB).

One variation of such scheme is the Niederreiter cryptosystems [22] which leverages the syndrome instead of codewords for encryption, and achieves ten times faster speed of the original McEliece algorithm.

1. *Lattice-based Cryptographic Systems*

Lattice-based schemes and its variants (NTRU, Learning with Errors (LWE), Ring-LWE etc.), are considered as the most promising candidate for the post-quantum cryptographic systems. Some of the reasons are:

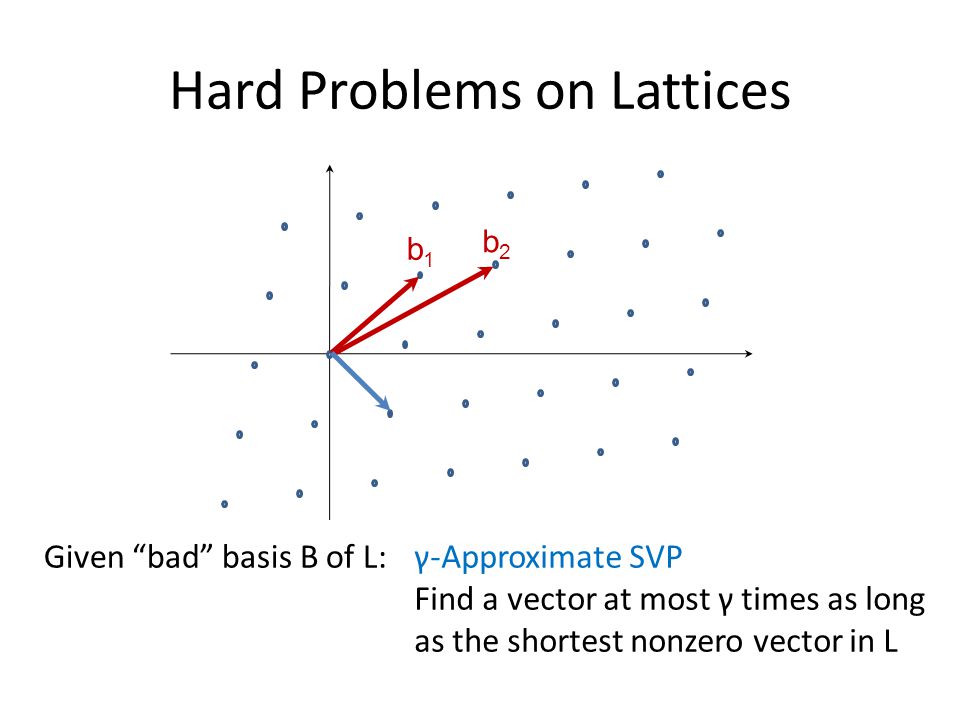
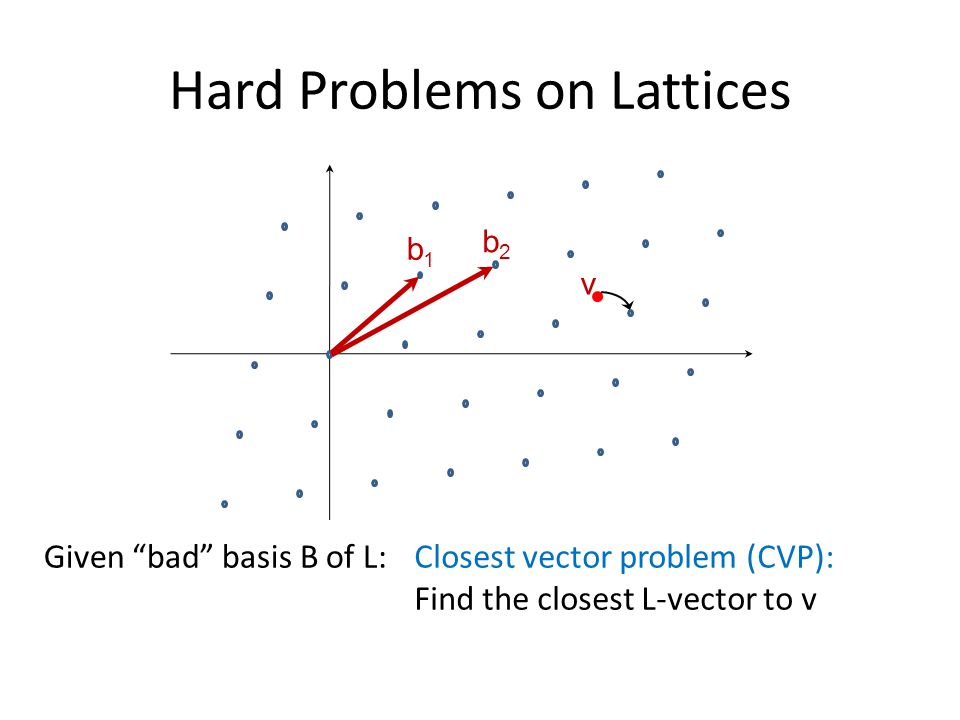
* It can be used for Public-Key Cryptosystems (PKC) that are secure against quantum computer attacks;
* It can also be used for Key Encapsulation Mechanisms (KEM);
* Several Somewhat Homomorphic Encryption (SHE) and Fully Homomorphic Encryption (FHE) are based on it;
* Quantum computation verification and quantum homomorphic encryption [23] can be based it.
* A small key size can be achieved by the variant Ring-LWE;
* It is faster and more area-efficient than RSA.

Among the variants of lattice-based systems, Ring-LWE has become more and more popular among researchers. This is because Ring-LWE provides the same level of post-quantum security with a much smaller key size and smaller computation complexity. While a code-based cryptosystem uses 1 MB storage for the key, and LWE 6 MB, Ring-LWE only asks for 7000 bits.

The security reduction of the lattice-based systems is the Shortest Vector Problem (SVP) and Closest Vector Problem (CVP), which have been known as NP-hard. We define a lattice *L*() by:

,

where are linearly independent vectors in . *L*(*B*) is the set of all the integer linear combinations of the vectors in *B*, and *B* is called a basis for *L*(*B*).

Briefly, as in Fig. 3, the SVP is to find in L(B) the shortest vector s (a linear combination of vectors in B) whose length is larger than 0. The CVP is to find a closest vector v (a linear combination of vectors in B) to a given vector.

1. (b)

Figure 3. The Shortest Vector Problem (a), and the Closest Vector Problem (b)

It is notable that the security reduction of LWE and Ring-LWE cryptosystems are not strictly SVP and CVP, but a modification of them. Therefore, one cannot exclude the possibility of the modification being breached someday.

The LWE problem was proposed in 2005 [24], that given the input x and output y = f(x), where f(x) is unknown, machine learning is able to gradually learn f() or compute it by Gaussian elimination. However, for y = f(x) + e where e is a small noise, learning this noisy function has been mathematically proven to be extremely difficult. At each step in the Gaussian elimination, e gets bigger and bigger until it obfuscates all useful information about f().

Ring-LWE is a variant of LWE where some parameters of the ring can be carefully selected in a way to drastically reduce the computation complexity. In a Ring-LWE system, the generator of the public key first select an arbitrary vector a in the ring, and two “small” vectors s and e, and construct:

, (3)

where {a, b} are the public key, and {s} is the private key.

[Eq. 3] creates a trapdoor, that given {a, s, e} it is easy to compute b, but with {a, b} it is as hard as SVP and CVP to compute s.

When an entity uses {a, b} to encrypt a message, the encryption is strengthened against attackers by e and some other “small” noises selected by the entity. However, at the receiver end, with s the private key, the receiver is able to easily remove those noises by taking the nearest integer after decryption.

Currently, for Ring-LWE-based cryptosystems, there have been a few hardware implementations [25, 26, 27, 28, 29, 30, 31]. However, it is not as many as the existing AES or RSA implementations. Creating efficient FPGA-based Ring-LWE will continue to be a meaningful topic for researchers, as it has for AES and RSA.

For more details of the algorithms and their implementation, please refer to the “PCP Toolbox – Extended Abstract.docx” in the same folder.

**Reference**

1. Elliot Williams, Quantum Computing Kills Encryption, https://hackaday.com/2015/09/29/quantum-computing-kills-encryption/, Hackaday, 2015
2. Amy Nordrum, https://spectrum.ieee.org/tech-talk/computing/hardware/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment, IEEE Spectrum, 2016
3. Hugo Miller, Quantum Computing Would Make Today’s Encryption Obsolete, https://www.bloomberg.com/news/articles/2017-07-20/quantum-computing-would-make-today-s-encryption-obsolete, Bloomberg, 2017
4. Tom Foremski , IBM warns of instant breaking of encryption by quantum computers: 'Move your data today', https://www.zdnet.com/article/ibm-warns-of-instant-breaking-of-encryption-by-quantum-computers-move-your-data-today/, ZDNet, 2018
5. Peter, Experts say quantum computing could defeat all forms of encryption soon, https://community.spiceworks.com/topic/2136423-experts-say-quantum-computing-could-defeat-all-forms-of-encryption-soon, Spiceworks, 2018
6. Linus Chang, How secure is today's encryption against quantum computers?, https://betanews.com/2017/10/13/current-encryption-vs-quantum-computers/, betanews, 2017
7. Zak Burkley, The Teachings of a Quantum Cat: Quantum Computers and Communication, https://www.lindau-nobel.org/the-teachings-of-a-quantum-cat-quantum-computers-and-communication-part-1/, Lindau Nobel Laureate Meetings, 2016
8. Karen Martin, Waiting for quantum computing: Why encryption has nothing to worry about, https://techbeacon.com/waiting-quantum-computing-why-encryption-has-nothing-worry-about, TechBeacon, 2018
9. Elaine Barker, and Allen Roginsky. "Transitions: Recommendation for transitioning the use of cryptographic algorithms and key lengths." NIST Special Publication 800 (2011): 131A.
10. Lov K. Grover, "A fast quantum mechanical algorithm for database search." Proceedings of the 28th annual ACM symposium on Theory of computing. ACM, 1996.
11. Peter W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM review 41.2 (1999): 303-332.
12. William Whyte, Lee Wilson, Quantum Safety in Certified Cryptographic Modules, NTRU Innovation, 2017
13. Daniel J. Bernstein, et al. "Post-quantum RSA." International Workshop on Post-Quantum Cryptography. Springer, Cham, 2017.
14. Mark H. Kim, Why Quantum Computers Might Not Break Cryptography, https://www.quantamagazine.org/why-quantum-computers-might-not-break-cryptography-20170515/, Quantamagazine, 2017
15. Cliff Saran, Microsoft predicts five-year wait for quantum computing in Azure, https://www.computerweekly.com/news/252440763/Microsoft-predicts-five-year-wait-for-quantum-computing-in-Azure, ComputerWeekly, 2018
16. NIST, Post-Quantum Cryptography Round 1 Submissions, https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions, 2018
17. Julian Kelly, A Preview of Bristlecone, Google’s New Quantum Processor, https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html, Google AI Blog, 2018
18. Peter W. Shor, "Scheme for reducing decoherence in quantum computer memory." Physical review A52.4 (1995): R2493.
19. Swamit S. Tannu, and Moinuddin K. Qureshi. "A Case for Variability-Aware Policies for NISQ-Era Quantum Computers." arXiv preprint arXiv:1805.10224 (2018).
20. Aharonov, Dorit, et al. "Interactive proofs for quantum computations." arXiv preprint arXiv:1704.04487 (2017).
21. Robert J. Mceliece, "A public-key cryptosystem based on algebraic." Coding Thv 4244 (1978): 114-116.
22. Hang Dinh, Cristopher Moore, and Alexander Russell. "McEliece and Niederreiter cryptosystems that resist quantum Fourier sampling attacks." Annual Cryptology Conference. Springer, Berlin, Heidelberg, 2011.
23. Urmila Mahadev, "Classical homomorphic encryption for quantum circuits." arXiv preprint arXiv:1708.02130 (2017).
24. Oded Regev, "On lattices, learning with errors, random linear codes, and cryptography." Journal of the ACM (JACM) 56.6 (2009): 34.
25. Tobias Oder and Tim Güneysu. Implementing the newhope-simple key exchange on low- cost fpgas. In Progress in Cryptology - LATINCRYPT 2017 - 6th International Conference on Cryptology and Information Security in Latin America, Cuba, Sepŋtemŋber 20-22, 2017, Proceedings, 2017.
26. Sujoy Sinha Roy, Frederik Vercauteren, Nele Mentens, Donald Donglong Chen, and Ingrid Verbauwhede. Compact ring-lwe cryptoprocessor. In Cryptographic Hardware and Embedded Systems - CHES 2014 - 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings, pages 371–391, 2014.
27. Thomas Pöppelmann and Tim Güneysu. Towards practical lattice-based public-key encryp- tion on reconfigurable hardware. In Selected Areas in Cryptography - SAC 2013 - 20th In- ternational Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers, pages 68–85, 2013.
28. James Howe, Ciara Moore, Máire O’Neill, Francesco Regazzoni, Tim Güneysu, and K. Bee- den. Standard lattices in hardware. In Proceedings of the 53rd Annual Design Automation Conference, DAC 2016, Austin, TX, USA, June 5-9, 2016, pages 162:1–162:6, 2016.
29. Bingxin Liu and HuapengWu. Efficient multiplication architecture over truncated polynomial ring for ntruencrypt system. In IEEE International Symposium on Circuits and Systems, ISCAS 2016, Montréal, QC, Canada, May 22-25, 2016, pages 1174–1177, 2016.
30. Po-Chun Kuo, et al. High Performance Post-Quantum Key Exchange on FPGAs. Cryptology ePrint Archive, Report 2017/690.(2017). https://eprint. iacr. org/2017/690, 2017.
31. Sujoy Sinha Roy, et al. "Compact ring-LWE cryptoprocessor." International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2014.

**Appendix**

**Vulnerabilities of RSA Systems**