NISTIR[1] 8105

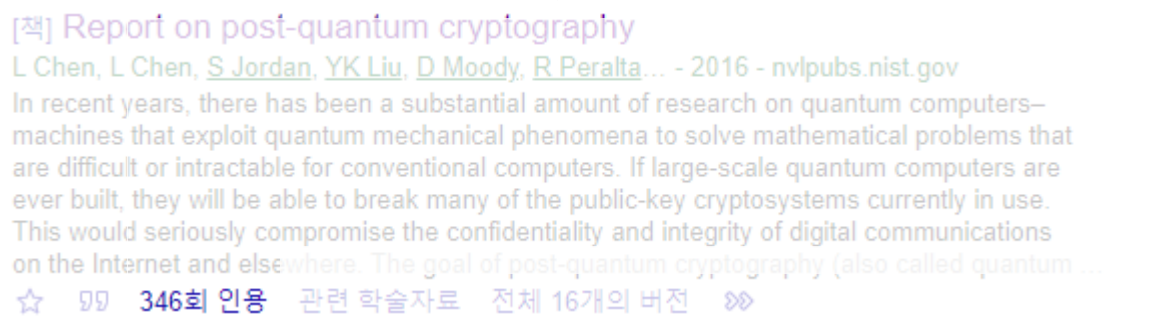
Report on Post-Quantum Cryptography

Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone, 2016

2020. 12. 16

Sungmin Lee

Captured on 20.12.15



1) National Institute of Standards and Technology's Internal Report

Contents

Introduction (1/3)

- Public key cryptography has become an indispensable component of our digital infrastructure
  - In such a connected world, the ability of secure communitation is of the utmost importance
- Our most crucial communication protocols rely principally on three core cryptographic functionalities
  - public key encryption, digital signatures, and key exchange
  - Depends on the difficulty of certain number theoretic problems
    - Integer Factorization, Discrete Log Problem
- In 1994, Peter Shor of Bell Laboratories showed that quantum computers can solve above problems
  - All public key cryptosystems based on such assumptions impotent [1]
- Researchers are working on these questions
  - Is quantum complexity fundamentally different from classical complexity?
  - When will large-scale quantum computers be built?
  - Is there a way to resist both a quantum and a classical computing adversary?

[1] P. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM, 1994

Introduction (2/3)

- In the twenty years since Shor's discovery, the theory of quantum algorithms has developed significantly
  - Quantum algorithms achieving exponential speedup have been discovered for several problems
    - Relating to physics simulation, number theory, and topology
  - Nevertheless, the list of problems admitting exponential speedup remains relatively small
- In contrast, more modest speedups have been developed for broad classes of problems
  - Related to searching, collision finding, and evaluation of Boolean formulae
  - In particular, Grover's search algorithm proffers a quadratic speedup on unstructured search problems
    - Can have the effect of requiring larger key sizes

Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

- Table 1 shows the impact of large-scale quantum computers on common cryptographic algorithms

Introduction (3/3)

- When a large-scale quantum computer will be built is complicated and contentious
  - But, many scientists now believe it to be merely a significant engineering challenge
  - Some experts even predict that within the next 20 or so years
    - sufficiently large quantum computers will be built to break all public key schemes currently in use [2]
- It will take significant effort to ensure a smooth and secure migration from the current widely used cryptosystems to their quantum computing resistant counterparts
  - Regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin to prepare our information security systems to be able to resist quantum computing
- In the academic world, this new science bears the name “Post-Quantum Cryptography”
  - EU projects PQCrypto(Since 2006) and SAFEcrypto, and the CREST Crypto-Math project in Japan
- NIST has a unique role to play in standardizing post-quantum cryptography like AES
  - NIST standards to be endorsed by industry and other standards organizations around the world

[2] Michele Mosca, Cybersecurity in an era with quantum computers: will we be ready?, IACR, 2015

Overview of Quantum-Resistant Cryptography (1/2)

- The impact on symmetric key systems will not be as drastic
  - Grover's algorithm provides a quadratic speed-up for quantum search algorithms in comparison with search algorithms on classical computers then Doubling the key size will be sufficient to preserve security
  - an exponential speed up for search algorithms is impossible then symmetric algorithms and hash functions should be usable in a quantum era [3]
- The algorithms resistant from both classical and quantum has focused on public key algorithms like,
  - Lattice-based cryptography : based on two NP-hard problems SVP[2)] and CVP[3)]
    - Pros : key establishment is relatively simple, efficient and highly parallelizable
    - Cons : Difficult to give precise estimates of the security even known cryptanalysis techniques
  - Code-based cryptography : In 1978, the McEliece cryptosystem was first proposed
    - Pros & Cons : Quite fast but very large key sizes
    - some proposals for code-based signatures, but more success with encryption schemes

2) Shortest vector problem
3) Closest vector problem

[3] Charles H. Bennett, Strengths and Weaknesses of Quantum Computing, SIAM 2006

Overview of Quantum-Resistant Cryptography (2/2)

- The algorithms resistant from both classical and quantum has focused on public key algorithms like, (cont')
  - Multivariate polynomial cryptography : based on the difficulty of multivariate polynomials over finite fields
    - Several multivariate crypto have been proposed and many having been broken [4]
    - some proposals for encryption, but historically more successful as signatures
- Improbable to be a drop-in replacement for waht is in use today
  - Need to overcome that quantum-resistant algorithms have larger key sizes
    - This may result changing various Internet protocols such as TLS or IKE
  - None of the above proposals have been shown to guarantee security against all quantum attacks
    - A new quantum algorithm may be discovered which breaks some of these schemes
    - However, this is similar to the state today that the lack of known attacks is used to justify the security
  - NIST believes that more research and analysis are needed before any of recommendation
    - One exception is hash-based signatures could potentially be standardized in the next few years

[4] V. Dubois et al, Practical cryptanalysis of SFLASH, Advances in Cryptology, CRYPTO 2007

Progress in Quantum Computing Hardware

- Building large-scale quantum computers began after the Peter Shor's discovery but it was unclear
  - Quantum states were too fragile and subject to the accumulation of error for large-scale computation
- In the late 1990, quantum error correcting codes and threshold theorems developed [5]
  - A reliable and fault-tolerant manner by error-correction steps throughout the computation
- Over the years, experimentalists have developed improved hardware with ever lower error rates
  - Simultaneously, theorists have developed new quantum error correction procedures
  - In 2001, IBM calculated 15 = 3 x 5 as Shor's quantum algorithm using nuclear magnetic resonance [6]
  - In 2014, universal quantum gates below fault-tolerance thresholds (around 1 %) have demonstrated [7]
  - In 2019, Google declared quantum supremacy using 53-qubit superconducting processor [8]
- Special purpose analog quantum computers are not believed to be of relevance to cryptanalysis
  - D-wave, Quantum annealer(up to 2,048 qubit with D-Wave 2000Q)

[5] J. Preskill, Reliable Quantum Computers, Proc. Roy. Soc, 1998
[6] Lieven M. K. Vandersypen et al, Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance, Nature, 2001
[7] R. Barends et al, Superconducting quantum circuits at the surface code threshold for fault tolerance, Nature 2014
[8] Frank Arute et al, Quantum supremacy using a programmable superconducting processor, Nature 2019

The Path Forward (1/2)

- The need for stronger cryptography is driven by advances in both classical and quantum computing
  - To provide security against quantum attacks, NIST will have to facilitate a more difficult transition, to new post quantum cryptosystems
- It is unclear when scalable quantum computers will be available, however
  - Researchers have estimated that breaking 2000-bit RSA in hours could be built by 2030 [9]
- Comparing the cost of breaking cryptosystems using classical computers is useful
  - 80 bits of security or less which were phased out in 2013, broken at a cost 100 M$
  - 112 bits of security are likely to remain secure because it may breakable at 1 B$ in 30 years
- Transitioning from 112 to 128 (or higher) bits of security is perhaps less urgent
  - 2016, NIST recommended that 80-bit security level is no longer and 112-bit be phased out by 2031[10]
  - 2020, NIST disallowed that <112-bit security level for applying protection [11]

[9] M. Mariantoni et al, Building a Superconducting Quantum Computer, PQCrypto 2014
[10] NIST, Special Publication (SP) 800-57 Part 1 Revision 4, Recommendation for Key Management – Part 1, 2016
[11] NIST, SP 800-57 Part 1 Rev. 5 Recommendation for Key Management: Part 1 – Genereral, 2020

The Path Forward (2/2)

- Previous cryptography transitions have been based on the bits-of-security paradigm
  - Measures the security based on the time-complexity of attack with a classical computer
  - This does not take into account the security of algorithms against quantum cryptanalysis
- There is not yet a consensus on what will provide acceptable levels of security against quantum attacks
  - For symmetric key systems, one simple heuristic is to double the key lengths to compensate for the quadratic speedup achieved by Grover's algorithm
    - This does not take into account the possibility of more sophisticated quantum attacks
- The development of standards for post-quantum cryptography will require significant resources to analyze candidate quantum-resistant schemes
  - NIST is preparing for the transition to quantum-resistant cryptography
  - Until new quantum-resistant algorithms are standardized, maintaining crypto agility is imperative

Summary

- In recent years, there has been a substantial amount of research on quantum computers to solve mathematical problems that are difficult or intractable for conventional computers.
  - If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use
- The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers
  - and can interoperate with existing communications protocols and networks
- This Internal Report shares NIST's current understanding and initial plan to post-quantum cryptography
  - and emphasizes the need to focus on crypto agility
- In Jul 2020, NIST announced the third-round finalist algorithms out of 69 candidates [12]
  - public-key encryption and key-establishment(4) : Classic McEliece, CRYSTALS-KYBER, NTRU, SABER
  - Digital signature(3) : CRYSTALS-DILITHIUM, FALCON, Rainbow

[12] NISTIR 8309, Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process

Thanks :)

Question?

You can see my direct translation of this report on https://www.sungmin.net/2020/07/nist-report-on-post-quantum-cryptography.html