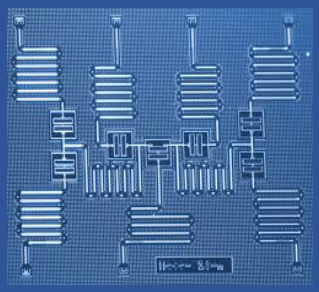
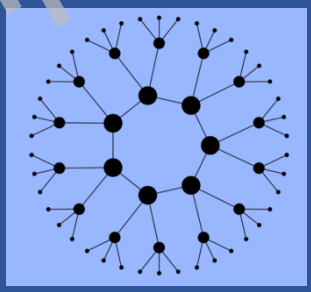
IBM Research
Security Subscription Service

Quantum Safe Cryptography

A series of guides to the impact of quantum technology on cryptography today, and the journey to making systems quantum safe.



Document: 2019 Q2 Security Subscription : Outline for initial report
Contact: securityreport@zurich.ibm.com
Version: 1.0

About IBM Research Security Subscription Service

Welcome to the IBM Research Security Subscription service that provides fact-based strategic insights for security professionals and executives on the topic of migrating to the new generation of quantum safe cryptography. The service includes quarterly reports and a seat at quantum security seminars, where possible collocated with IBM Q Network events. The insights are based on findings from analysis of our own primary research activities in the area of quantum safe cryptography and our own efforts at migrating systems and solutions to become quantum safe. Reports are planned quarterly and cover topics that include:

- The quantum algorithms that threaten today's cryptography
- The quantum impact on the security of IT systems
- Baselining the quantum risk within organizations
- Discovering and prioritizing cryptography vulnerabilities
- Quantum safe cryptographic algorithms
- The state of quantum safe standardization at different standards organizations
- Cryptographic agility as a vehicle for quantum migration
- Cloud migration as a vehicle for cryptographic agility
- Building skills in quantum safe cryptography
- Quantum safe open source activities

For more information and to suggest relevant topics, please contact IBM Research at securityreport@zurich.ibm.com

This document is the 2019 2nd Quarter security report that is the first report in the series.

IBM Corporation
New Orchard Road
Armonk, NY 10504
Produced in the United States of America February 2019

Table of Contents

1 Executive Summary 3
2 Related security topics 4
2.1 Quantum Safe Cryptography 4
2.2 Quantum Key Distribution 4
2.3 Quantum AI 4
2.4 Quantum Sensing 4
2.5 Quantum Random Number Generators 5
3 The security impact of quantum technology 6
3.1 Impacts on classical cryptography 6
3.2 Security Strength 6
3.3 Quantum Algorithms 6
3.4 Symmetric Cryptography 7
3.5 Public Key Cryptography 7
3.6 Impacts on higher level protocols 8
3.7 Impact on PKI 9
Impact on Hardware 9
3.8 Blockchain and long-term ledgers 9
3.9 Internet of Things (IoT) 10
4 Quantum Safe Cryptographic Standardisation 11
4.1 NIST PQC Process 11
4.2 ETSI 11
4.3 ISO/IEC 11
4.4 ANSI X9 12
4.5 IEEE 12
4.6 IETF and IRTF 12
5 Conclusion and look forward to the next report 13
6 Quantum Safe Workshops and conferences 2019 14
7 Glossary 15
8 Bibliography 16

List of Tables

Table 1: Hardness of Classical Public Key Algorithms 6
Table 2: The effective security of different algorithms in a quantum world. 7
Table 3: Quantum resource estimates for Grover's algorithm to attack AES 7
Table 4: Number of qubits required for attacking RSA and ECC 7
Table 5: NIST PQC Process Timeline 11

1 Executive Summary

Quantum computing is a system based on a completely different foundation to the logic underpinning current computers. Today's computers rely on bits, which are embodied as switches that can be set to zero or one. In quantum computing there is the concept of a quantum bit or qubit that can hold several values at the same time, a condition known as superposition. Combined with a quantum mechanical property called entanglement, quantum computers are able to create states that scale exponentially with the number of qubits. Quantum computers promise advantages in solving computationally complex problems that today's classical computers cannot solve.

First proposed by Nobel laureate Richard Feynman in 1982 as a tool to simulate quantum systems, it triggered a series of theoretical research efforts that led to the publication of Peter Shor's factoring algorithm in 1994 [1]. Shor's proposal for a quantum algorithm that can efficiently solve integer factorization and discrete logarithm problems undermines the hard-mathematical problem that is the basis of many of today's asymmetric cryptographic algorithms. A second algorithm [2] created by Les Grover theoretically weakens the security of symmetric cryptographic algorithms. For many years the threat to cryptography was considered theoretical since quantum computers had not been developed that could be used to demonstrate in practice that algorithms indeed worked. This has changed with recent advances in the field of quantum computing. Shor's algorithm has been demonstrated for small numbers meaning that the threat to cryptography has become far more tangible. Predictions that further significant progress in the development of quantum computers could be expected within fifteen years, has created a flurry of activities in the research community, standardization bodies and major industries. The US Government's call for quantum safe cryptography [3] in 2015 is an example of the newly perceived urgency.

Cryptography allows users and machines to establish private and authenticated, confidential communication channels, and to interact securely. It allows systems that are found to contain software vulnerabilities to be securely updated. It underpins the trust that we have in e-commerce, blockchains and crypto-currencies. Without cryptography we would not have the level of digitalization that we have today and simply put, our society depends on it. Developments in quantum computing have given much of the cryptography that we use today an end-of-shelf life, and as such it needs to be replaced with alternatives that are secure against quantum attacks. Unfortunately, it is a common misnomer to think that we can wait until a large quantum computer is built before doing anything. The unfortunate term "Post Quantum Cryptography" reinforces the misunderstanding by suggesting that the solution is something for a post quantum world. This is simply not the case. One cannot wait until a large enough quantum computer appears before starting to act. Regulation often mandates that data needs to remain confidential and secure for long periods of time. The risk that data harvested today and revealed in the future can be a danger to governments, organizations and individuals alike. The future unauthorized release of sensitive medical records, financial transactions, security research, legal proceedings and state secrets can all have serious consequences. Consequently, it is an imperative that the cryptography that we use to protect data today remains secure in the coming decades. The same applies to the cryptography that we use to protect applications and systems. Public key cryptography is used to secure code updates, authenticate users and systems, validate the legitimacy of transactions and transfer assets on blockchains. Systems and applications that we introduce today that will exist into the quantum future must be prepared for the quantum theat.

It is clear that we need to prepare for migration to quantum safe cryptographic schemes. For sensitive data and systems with long operational lives, that journey needs to begin earlier rather than later. That journey should not wait for quantum safe standards to finalized. Experience has shown that changing the cryptography that we use is practice is very difficult. In fact, the current state of cryptographic use within the IT industry is a major source of cyber-insecurity. Cryptography is often buried deep within systems and applications, is complex, and often bugged with implementation errors. This makes it difficult even to find the cryptography that needs replacing. Once found we often find that applications and systems are adapted to characteristics of the cryptography used. This makes it complicated to change from one cryptographic scheme to another. This lack of agility has hampered previous attempts to transition from end-of life cryptography to new safer schemes. A good example is the TLS Heartbleed vulnerability discovered in 2014. It is considered to have cost industry over 500 million dollars and even today many websites are still not fixed.

The necessity to migrate to quantum safe cryptography offers a unique opportunity to correct the current situation and at the same time to improve our cybersecurity posture. This involves stepping back to review how we consume cryptography in a more agile way and using the opportunity to consolidate the sprawl of different cryptographic technologies within our organizations. This set of security reports are designed to facilitate this discussion and to support organizations in grasping the opportunity.

5 Conclusion and look forward to the next report

Why the time to act is now

It would be simple for industry to wait for the NIST standard to be published however this turns out to be a major problem. The TLS standard that underpins most of the internet's security, has just been updated from version 1.2 to version 1.3. Implementing TLS 1.3 is a massive undertaking. Initial testing has shown that packet fragmentation can be a significant cause of problems. Those quantum safe schemes that produce larger cipher artifacts would cause packet fragmentation which questions their suitability as replacements. The prospect of having to integrate new quantum safe cipher suites within a relatively short time is problematic. Many real world applications have implemented inflexible memory management schemes targeting todays commonly used cryptographic schemes and key lengths. The story is the same for many new security frameworks, protocols and standards being developed for smarter transport infrastructures, blockchains, e-Government, critical infrastructures and Industry 4.0. The systems and infrastructures that we are designing and building today need to be secure for the coming decades. To do so requires that industry be prepared for the new generation of cryptography. A typical new car may take 7 years to design and have a road life of 25 years. Medical data in some countries need to be kept secure for 100 years. The US National Academies of Sciences, Engineering, and Medicine Foundation released a survey of quantum technology and a series of key findings. The most important of these was the finding:

"Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, the hazard of such a machine is high enough—and the time frame for transitioning to a new security protocol is sufficiently long and uncertain—that prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster." [31]

Agile Cryptography

The worst outcome of a migration to quantum safe cryptography is that we do not address the lack of cryptographic agility and the associated cyber security challenges. It is expected that quantum safe implementations will need to mature and the ability to locate and patch these schemes will be essential. Addressing cryptographic agility first will simplify the migration to quantum safe schemes and reduce the cybersecurity risk of both classical and quantum safe systems. The Q3 report will contain an introduction to the key dimensions of cryptographic agility.

NIST 2nd PQC Conference

The major event in Q3 is the 2nd NIST PQC conference in August. The Q3 report will provide an analysis of the NIST PQC process with a perspective on the algorithms that are still in contention.

6 Quantum Safe Workshops and conferences 2019

1. International Conference on Post-Quantum Cryptography
   www.waset.org/conference/2019/04/istanbul/ICPQC
   Instanbul, Turkey

2. The Tenth International Conference on Post-Quantum Cryptography (PQCrypto 2019)
   Scientific conference organized by the IACR (International Association of Cryptographers)
   www.pqcrypto2019.org
   Chongqing, China
   Event: May 8 — May 10

3. International Cryptographic Module Conference
   www.icmconference.org
   Track on post quantum crypto
   Vancouver, Canada
   Event May 14-17

4. Crypto 2019 (Crypto)
   Scientific conference organized by the IACR (International Association of Cryptographers)
   www.crypto.iacr.org/2019/
   Santa Barbara, USA
   Event: Aug 18 — Aug 22

5. Second NIST PQC Conference
   International standardization conference organized by NIST
   Co-located with the above Crypto 2019 conference
   www.csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline
   Santa Barbara, USA.
   Event: Aug 18 — Aug 22

6. ETSI 2019 PQC Meeting
   International standardization conference organized by ETSI
   Seattle, USA
   Event: November 5-7

7 Glossary

ABE	Attribute Based Encryption
ANN	Artificial Neural Network
API	Application Programing Interface
BLISS	Bimodal Lattice Signature Schemes
CI	Continuous Integration
CSIT	The Centre for Secure Information Technologies
CSPRNG	Cryptographically Secure Pseudorandom Number Generator
Decoherence	The process of the loss of quantum information through interaction with an. environment.
IBE	Identity Based Encryption
IPC	Interprocess communication
IPsec	Internet Protocol Security
KAT	Known Answer Test
KEM	Key Encapsulation Mechanism
Module LWE	Module Learning with Errors
NISQ	Noisy Intermediate-Scale Quantum
NIST	National Institute of Standards and Technology
NTT	Number Theoretic Transform
OpenSSL	An open source project that provides a toolkit for the TLS and SSL protocols
PRNG	Pseudorandom Number Generator
Ring-TESLA	An ideal-lattice-based version of Tightly secure, Efficient Signatures from Standard Lattices
R-LWE	Ring Learning With Errors
SAD	Software Architecture Document
SAFEcrypto	Secure Architectures of Future Emerging Cryptography SRS Software Requirements Specification
SIS	Short Integer Solution
SSL	Secure Sockets Layer
strongSWAN	An open-source IPsec-based VPN solution
TLS	Transport Layer Security
TRNG	True Random Number Generator
QRNG	Quantum Random Number Generator
VPN	Virtual Private Network

8 Bibliography

[1] S. Peter, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, 1994.

[2] Grover, "A fast quantum mechanical algorithm for database search," ACM, 1996, pp. 212-219.

[3] N. S. Agency, "Commercial National Security Algorithm Suite," NSA Information Assurance, August 2015. [Online]. Available: https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm.

[4] R. Bedington, "Progress in satellite quantum key distribution," *Quantum Information,* vol. 3, 2017.

[5] C. M. D. G. D. B. Francesco Tacchino, "An Artificial Neuron Implemented on an Actual Quantum Processor," arXiv:1811.02266 [quant-ph], 2018.

[6] MIT, "Review of Modern Physics : Quantum Sensing," MIT, 2017.

[7] Nature, "Fluctuations in vacuum energy measured through homodyne detection," *Nature Photonics volume,* vol. 4, pp. 711-715, 2010.

[8] IDQuantique, "Quantis Raadom Number Generator," 2018. [Online]. Available: https://www.idquantique.com/random-number-generation/products/quantis-random-number-generator/. [Accessed 1 10 2018].

[9] D. H.-S. a. J. Hernandez-Castro, "Bias in a Family of Quantum Random Number Generators ,," 2018. [Online]. Available: https://eprint.iacr.org/2017/842.pdf.

[10] NIST, "NIST QRNG Beacon Service," 06 2018. [Online]. Available: https://beacon.nist.gov/home. [Accessed 09 2018].

[11] G. L. Karthikeyan Bhargavan, "Sweet32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN," INRIA, [Online]. Available: https://sweet32.info. [Accessed March 2019].

[12] M. S. G. B. C. S. Y. M. H. S. &. I. L. C. Lieven M. K. Vandersypen, "Letter | Published: 20 December 2001 Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," *Nature,* no. 414, pp. 883-887, 2001.

[13] C. Z. John Proos, "Shor's discrete logarithm quantum algorithm for elliptic curves," *Quantum Information & Computation,* vol. 3, pp. 317-344, 2003.

[14] G. e. Al., "Applying Grover's algorithm to AES: quantum resource estimates," 2015.

[15] Z. C. Pross John, "Shor's discrete logarithm quantum algorithm for elliptic curves," in *arXiv:quant-ph/0301141v2*, 2004.

[16] NSA, "Quantum computing is a major threat to crypto, says the NSA," 2015. [Online]. Available: https://www.digitaltrends.com/computing/quantum-computing-is-a-major-threat-to-crypto-says-the-nsa/. [Accessed 2019].

[17] IBM Research GmbH, "Identity Mixer," IBM Research GmbH, 2018. [Online]. Available: https://www.zurich.ibm.com/identity_mixer/. [Accessed 2019].

[18] Linux Foundation, "Hyperledger Fabric," 2018. [Online]. Available: https://www.hyperledger.org/projects/fabric. [Accessed 2018].

[19] "ZCash," 2018. [Online]. [Accessed 2018].

[20] B. e. Al, "Bulletproofs: Short Proofs for Confidential Transactions and More," 2018. [Online]. Available: https://eprint.iacr.org/2017/1066.pdf. [Accessed 2018].

[21] Monero, "Monero," 2018. [Online]. Available: https://www.getmonero.org. [Accessed 2018].

[22] B.-S. e. Al, "Scalable, transparent, and post-quantum secure computational integrity," March 2018. [Online]. Available: https://eprint.iacr.org/2018/046.pdf. [Accessed 2018].

[23] Google, "Experimenting with Post-Quantum Cryptography," 7 July 2016. [Online]. Available: https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html. [Accessed 11 1 2019].

[24] "NewHope - Post Quantum Key Encapsulation," 2017. [Online]. Available: https://newhopecrypto.org. [Accessed Nov 2018].

[25] Google, "Post-quantum confidentiality for TLS," Google, 11 April 2018. [Online]. Available: https://www.imperialviolet.org/2018/04/11/pqconftls.html. [Accessed Nov 2018].

[26] IETF, "Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH)," July 2017. [Online]. Available: https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html#MFQ-U-OO-815099-15.

[27] IETF, "RFC 7919 : Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)," IETF, 2016.

[28] IETF, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1," Feb 2003. [Online]. Available: https://tools.ietf.org/html/rfc3447#appendix-A.1. [Accessed 1 2019].

[29] F. T. Consortium, "FutureTPM," Future TPM consortium, 2019. [Online]. Available: https://futuretpm.eu. [Accessed 2019].

[30] C. a. L. R. a. P. A. a. T. T. Cheng, "Securing the Internet of Things in a Quantum World," *IEEE Communications Magazine,* pp. 116-120, 02 2017.

[31] National Sciene Foundation, "Quantum Computing Progress and Prospects 2018," National Academies of Science, Engineering, Medicines, 2018.

[32] W. M. Niederhagen Ruben, "Practical Post-Quantum Cryptography," Fraunhofer Institute for Secure Information Technology SIT, Darmstadt, 2017.

[33] A. M., "Generating Hard Instances of Lattice Problems," *ACM Symposium on Theory of Computing,* vol. STOC 96, pp. 99-108.

[34] N. H., "Knapsack-type cryptosystems and algebraic coding theory," *Problems of Control and Information Theory,* pp. 19-34, 1986.

[35] B.-S. e. AL, "Scalable, transparent, and post-quantum secure computational integrity," 2018.

[36] S. R. Devoret M.H., "Superconducting Circuits for Quantum Information: An Outlook,," [Online]. Available: http://qulab.eng.yale.edu/documents/papers/Superconducting%20Circuits%20for%20Quantum%20Information%20-%20An%20Outlook.pdf. [Accessed 10 11 2018].

[37] BSI Germany, " Entwicklungsstand Quantencomputer," 05 2018. [Online]. [Accessed 11 2018].

[38] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," NASA, 1978.

[39] BCG, "The Next Decade in Quantum Computing—and How to Play," BCG, 2018.

[40] IDQuantique, 2018. [Online]. Available: https://www.idquantique.com/chinas-growing-investment-in-quantum-computing/ .

[41] A. Aspuru-Guzik, "Algorithms for Quantum Computers," Scientific American, Sept 2018. [Online]. [Accessed 01 2019].

[42] IBM, *Internal Discussion on Error Correction,* 2019.

[43] H. GROUP, 2017. [Online]. Available: https://www.herjavecgroup.com/wp-content/uploads/2018/07/HG-and-CV-The-Cybersecurity-Jobs-Report-2017.pdf.

[44] E. B. K. a. d. G. P. Luiijf, "Nineteen national cyber security strategies',," *Internation Journal onCritical Infrastructures, ,* vol. 9, pp. 3-31, 2013.

[45] J. Preskill, "Quantum Computing in the NISQ era and beyond," *Quantum,* vol. 2, no. 79, 2018.

[46] "SPHINCS".

[47] Lamport, "Constructing Digital Signatures from a One Way Function," 1979.

[48] J. D. E. a. A. H. Buchmann, "XMSS-a practical forward secure signature scheme based on minimal security assumptions," Springer, Berlin, 2011.

[49] R. Merkle, "Secrecy, authentication and public key systems / A certified digital signature," Stanford, 1979.

[50] IETF - Crypto Forum Research Group, "Hash-Based Signatures, draft-mcgrew-hash-sigs-15," 2015.

[51] L. J. D. P. J. De Feo, "Towards quantum-resistant cryptosystems from su- persingular elliptic curve isogenies," *Crypt,* pp. 209-247, 2014.

[52] F. e. al, "Supersingular Isogeny Diffie–Hellman Authenticated Key Exchange," 20. [Online]. Available: https://eprint.iacr.org/2018/730.pdf. [Accessed 2019].

[53] T. M. a. H. Imai., "Public quadratic polynominal-tuples for efficient signature-verification and message-encryption. ,," in *Advances in Cryptology - EUROCRYPT '88*, Davos, 88.

[54] UK Government, "UK National Quantum Technologies Program," [Online]. Available: http://uknqt.epsrc.ac.uk. [Accessed 2019].

[55] "Quantum Flagship Program," [Online]. Available: https://qt.eu. [Accessed 2019].

[56] NIST, "NIST Risk Management Framework Overview," NIST.

[57] S. consortium, "Safecrypto," 2018. [Online]. Available: https://www.safecrypto.eu.

[58] NIST, "Cryptographic Module Validation Program," NIST, 2018. [Online]. Available: https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards. [Accessed nov 2018].

[59] Common Criteia Organisation, "The Common Criteria," 2018. [Online]. Available: https://www.commoncriteriaportal.org. [Accessed 2018].

[60] T. L. Dan Berstein, "The year in post quantum crypto," 2018. [Online]. Available: https://media.ccc.de/v/35c3-9926-the_year_in_post-quantum_crypto. [Accessed 2018].

[61] T. L. Dan Berstein, "PQCrypto," 10 2018. [Online]. Available: https://pqcrypto.org. [Accessed 11 2018].

[62] Lyubashevsky et Al, " Proceedings of the 29th Annual international conference on Theory and Applications of Cryptographic Techniques," in *EUROCRYPT'10*.

[63] H. Niederreiter, *Problems of Control and Information Theory,* vol. 15, pp. 19-34, 1986.

[64] IBM Research, "IBM Q Network," IBM, 2019. [Online]. Available: https://www.research.ibm.com/ibm-q/network/. [Accessed 22 01 2019].

[65] M. Dyakonov, "The Case Against Quantum Computing," IEEE , 2018.

New Orchard Road
Armonk, NY 10504
Produced in the United States of America July 2019