Post-quantum Secure Cryptographic Algorithms

Xenia Bogomolec and Jochen Gerhard

1 Introduction

The following article gives an overview of current developments in algorithmic solutions, and addresses the upcoming threats posed by quantum computers as well as unsolved problems in the classical IT landscape. It is an update of our 2018 publication in Computeralgebra-Rundbrief (Bogomolec und Gerhard 2018) and contains some new developments. However, the mathematics described are of course still the same. We thank the Fachgruppe Computeralgebra for their support.

The expected dawn of a new technological era certainly began when IBM offered its first commercially available 20-qubit quantum computers in November 2017. While, over the past year, it has still been discussed whether it is necessary to take quantum technology into account in the IT industry, the estimations about its capability evolution have become much more specific now.

X. Bogomolec (✉)
Quant-X Security & Coding GmbH, Hannover, Germany
e-mail: xb@quant-x-sec.com

J. Gerhard
Hofheim am Taunus, Germany
e-mail: jochen.gerhard@commerzbank.com

V. Liermann and C. Stegmann (eds.), *The Digital Journey of Banking and Insurance, Volume II*, https://doi.org/10.1007/978-3-030-78829-2_11

On the other hand, quantum algorithms, which are described in quantum theory and various mathematical areas such as complex linear algebra or category theory, offer more efficient solutions to known problems. In terms of cryptography, those alternative solutions to known mathematical problems, which are the basis for the security of cryptographical algorithms, are called quantum cryptanalyses.

Fortunately, scientific researchers have specialized in examining the various resulting challenges and questions since the beginning of this century. A series of conferences about post-quantum cryptography, the PQCrypto, started in 2006. They have taken place in a different city every year since 2010.

1.1 Quantum Technologies

Quantum–mechanical phenomena, such as superposition and entanglement, are used for communication, imaging, computing, simulation, sensing and metrology. While communication, sensing and simulation have been realized in publicly announced projects or products, universal quantum computing was only a matter of research until November 2017. The first quantum computing processors were introduced to the industry by (D-Wave Systems kein Datum) much earlier. They are so-called quantum annealers, devices which come close to the realization of the theory of adiabatic quantum computing and suitable for a restricted class of problems, such as optimization and machine learning.

With the advent of 65-qubit universal processors, quantum supremacy lies within reach, i.e. the potential of quantum computing devices to solve problems that classical computers practically cannot solve (Hsu kein Datum; Kelly 2018). IBM has announced that it is going to build a 1000-qubit prototype by 2023; Google is participating in the race with its record-breaking quantum processors Bristlecone (72 qb) and Sycamore (54 qb). A public overview of quantum processors and their architecture can be found on Wikipedia kein Datum.

1.2 Benefits

Quantum technologies offer and promise major benefits. So-called adiabatic quantum computers, e.g. the D-Wave 2000Q with 2048 qubits from D-Wave Systems in Canada, are able to solve optimization problems that would overburden a classical computer. Photon-based quantum key distribution devices from ID Quantique in Switzerland are used by the government in Geneva, DARPA and other institutions. China has built the 2000-km quantum communication channel QUESS between Beijing and Shanghai for banks, the Xinhua News Agency and the government, whose nodes receive keys from their quantum communication satellite. In 2017 they recorded feasible distances of up to 1200 km. In the future, quantum computers with enough stable qubits are expected to be able to help build complex materials as well as solve medical and environmental problems, among other things.

1.3 Threats

It has long been known that the security of the currently used cryptographic algorithms relying on the hardness of integer factorization and finding discrete logarithms (DLOG 1 systems) (Shor 1997) will expire with potent enough quantum computers. All public parameters like public keys from asymmetric key pairs can then be used to compute the corresponding private keys. With the knowledge of these private keys, encrypted data collected and assigned to the relevant key exchanges will no longer remain secret. For technologies like public distributed ledgers, where encrypted data is publicly available, this threat is even more serious.

2 Solutions

2.1 Quantum Key Distribution

QKD is an implemented cryptographic protocol for key distribution involving components of quantum mechanics. The security of encryption that uses quantum key distribution relies on the foundations of quantum mechanics. In this context, the process of measuring a quantum system in general disturbs the system itself. Therefore, any third party trying to gain knowledge of the key would be detected by the original communication parties.

Quantum key distribution networks have already been established in China (QUESS), Austria (SECQC), Japan (Tokyo QKD Network), Switzerland (SwissQuantum) and the USA (DARPA). The disadvantages for widespread practical usage are limited distances between communication partners and the need for expensive hardware. The fact that message source authentication does not come with QKD by default is rarely mentioned. Man in the middle attacks are also possible if the communication parties do not agree on an authentication protocol beforehand.

3 Post-Quantum Cryptography

The alternative to QKD are algorithms whose security relies on mathematical properties, like hardness of computing the inversion of a one-way function, even with a quantum computer. Hardness means that the computation takes an unrealistic amount of time, e.g. a billion years. There are four mathematical areas which offer solutions for post-quantum secure encryption, key exchanges and signatures. Some of them are still in the research process, others have been observed and challenged for decades. The advantages of post-quantum cryptography are that it can run effectively on devices currently used, such as smartphones, desktops and IoTs, and they can be established by pure software updates.

3.1 Code-Based

Syndrome decoding of linear error-correcting codes are NP-complete if they are considered as a decision problem with unbounded number of errors. This means that this problem cannot be efficiently solved by a deterministic computer (including all classical computers). On the other hand, some classes of linear codes have very fast decoding algorithms. The basic idea behind a code-based crypto system is to choose a linear code with a fast decoding algorithm and disguise it as a general linear code. Then the attacker has to use syndrome decoding to decrypt the message, while the message recipient, who also set up the system, can remove the disguise and use the fast decoding algorithm.

McEliece and the Niederreiter cryptosystems are two basic encryption schemes built on this setup. McEliece was the first scheme using randomization in the encryption process. Both systems consist of three algorithms:

1. Probabilistic key generation algorithm producing an asymmetric key pair
2. Probabilistic encryption algorithm
3. Deterministic decryption algorithm.

The private key is an *(n; k)*-linear error-correcting code represented by a generator matrix *G*, with a known efficient decoding algorithm. Originally, binary Goppa codes with the Patterson decoding algorithm were used. The public key is the generator matrix *G* perturbated by two randomly chosen invertible matrices S and P

$$G' = SGP$$

Equation 1: Generator matrix

where S, a $(k \times k)$ matrix, functions as a scrambler and P is a $(n \times n)$ permutation matrix. Parameters proposed by McEliece (1978) result in a public key of 2^{16} bytes size. The most effective attacks on McEliece use information-set decoding. To resist those in a quantum computing context, key sizes have to be increased by a factor of 4.

The Niederreiter scheme (Niederreiter 1986) applies the same idea to a parity check matrix H of a linear code. The encryption is about ten times faster than McEliece. McEliece was originally believed not to be usable for authentication or signature schemes because the encryption algorithm is not one-to-one and the total algorithm is truly asymmetric, meaning encryption and decryption do not commute. However, a one-time signature scheme based on McEliece and Niederreiter was proposed at the Asiacrypt in 2001 (Courtois et al. 2001):

1. Choose a hash function *h* and compute the hash value *h(d)* of the document *d* which has to be signed
2. Decrypt the hash value *h(d)* as if it were an instance of the ciphertext
3. Append the decrypted hash value to the document as a signature.

As the second step in the signature scheme almost always fails, the system additionally specifies a deterministic way of tweaking *d* until a hash value *h(d)* is found which can be decrypted. Verification then applies the public encryption function to the signature and compares it to the hash value of the document.

The most recently published code-based key exchange protocol is Ouroboros (Deneuveville et al. 2017). This uses quasi-cyclic codes in Hamming metric in the encryption algorithm; efficient decoding is achieved through bit flipping in the Random Oracle Model. Encryption and decryption are faster than RSA for comparative benchmarks (https://bench.cr.yp.to).

Ouroboros was proposed as a post-quantum secure cryptographic algorithm at the NIST, but removed from Round 2 in favor of the Classic McEliece scheme, which is one of the four Round 3 finalists for public-key encryption and key-establishment algorithms.

3.2 Hash-Based

This domain is limited to digital signature schemes which rely exclusively on the security of the underlying hash functions so far. The signatures themselves reveal a part of the signing key and can only be used for one message, the same as with one-time pads, such as visual cryptography shares.

Merkle tree signature schemes, introduced in 1979, combine a one-time signature scheme with a Merkle tree structure. The building blocks of the Merkle trees are one-time signature key pairs, with the node at the top being the global public key. This typically 256-bit large key can be verified with the path to another given public one-time key in the tree using a sequence of tree nodes, called the authentication path. The global private key is usually derived from a seed generated by a pseudo-random number generator and has the size of 256 bits as well. Therefore, the number of possibilities for such signatures is all possible combinations of the simple one-time signatures within the tree structure. This procedure considerably enhances the security of the scheme against brute force attacks.

The latest performance-improved hash-based signature scheme is Sphincs + (Rijneveld und Kölbl kein Datum), the advanced Sphincs (Bernstein et al. 2015) scheme presented at Eurocrypt 2015. Unlike its predecessors, XMSS and LMS, it is stateless, meaning that signing does not require an updating of the secret key. It is a so-called few-times scheme, where "few-times" means that after 264 signatures it is necessary to reinitiate the complete scheme. Its signature sizes range from 8 kb for NIST security level 1 to 30 kb for NIST security level 5. Sphincs + succeeded in passing Round 2 of the NIST standardization and is now proposed as an alternative candidate to the Round 3 finalists for digital signature algorithms: Crystals-Dilithium (algebraic lattice), Falcon (Fast Fourier lattice) and Rainbow (multivariate).

3.3 Lattice-Based

Lattice-based codes come with the challenge of finding the nearest lattice point or a shortest basis for a given lattice. Both problems and their approximations have been solved with NP-hard algorithms only. Given they are one of the longest known public key crypto systems, they can be fairly seen as the most promising post-quantum crypto approaches. Low memory requirements and high-speed computations let them run effectively on all currently and widely used devices. However, due to their significantly bigger key sizes they have not been as thoroughly researched and applied as RSA, EL Gamal (Hoffstein et al., An Introduction to Mathematical Cryptography 2008) or

DLOG systems. NTRU was the first successful lattice-based asymmetric cryptosystem. It was proposed and patented in 1996 (Hoffstein et al., NTRU: A Ring-Based Public Key Cryptosystem 1998). With the expiration of the patent in 2016, NTRU Prime (Bernstein et al. 2017), an improvement by eliminating worrisome algebraic structure, could be published. Their security relies on the interaction of a polynomial mixing system with the independence of reduction modulo to relatively prime integers p and q (gcd(p,q) = 1). That means: at various stages of encryption and decryption the coefficients of the polynomials are reduced modulo q and/or modulo p. In particular, reduction modulo p and reduction modulo q do not commute with one another.

Another popular ingredient of lattice-based algorithms is the Learning with Errors (LWE) problem. This was used in BCNS (Bos et al. 2013), which phrased Peikert's key encapsulation algorithm as a key exchange protocol. BCNS was the first lattice-based algorithm integrated into the OpenSSL library.

With New Hope (Alkim et al. 2015), an improvement was achieved by choosing more efficient parameters and shifting from LWE to Ring Learning with Errors (RLWE). The New Hope protocol allows man in the middle attacks; message authentication must be implemented additionally. Google ran an experiment by using New Hope embedded in an ECC procedure for a certain number of connections between the Chrome browser and its own servers in 2016. Since 2017, Infineon has worked on the first generation of contactless post-quantum chips with Pöppelmann, one of the authors of the New Hope paper.

Dilithium (Ducas et al. 2017), a module-lattice-based signature scheme, was designed with the intention to be easy to implement against side-channel attacks, while offering efficiency comparable to previously developed lattice-based signature schemes. The key innovation is the replacement of Gaussian sampling by uniformly random sampling over a bounded domain. Furthermore, the public key sizes are reduced by more than a factor of 2.

All these algorithms except BCNS were submitted to the NIST post-quantum cryptography standardization process. The lattice-based Round 3 finalists are: NTRU and Crystals-Kyber (algebraic lattice) for public-key encryption and key-establishment algorithms, and Crystals-Dilithium (algebraic lattice), Falcon (Fast Fourier lattice) for digital signature algorithms.

3.4 Multivariate

The proven NP-hardness and NP-completeness of solving multivariate polynomial equations over a finite field F are the reasons why schemes with those asymmetric cryptographic primitives are considered good candidates for post-quantum security. Most of the published schemes use multivariate quadratics, namely polynomials of degree two.

The basic scheme consists of two affine transformations

$$S : F^n \rightarrow F^n$$

Equation 2: Affine transformation 1

$$T : F^m \rightarrow F^m$$

Equation 3: Affine transformation 2

and an easy-to-invert quadratic map

$$P' : F^m \rightarrow F^n$$

Equation 4: Quadratic map

The trapdoor $(S^{-1}, P'^{-1}, T^{-1})$ represents the private key, without which the public key $P = S \circ P' \circ T$ is assumed to be hard to invert. A first multivariate quadratic scheme, C^* (Matsumoto und Imai 1988), was presented at the Eurocrypt Conference 1988. After it was broken (Patarin, Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt ‘88 1995), the general principle was used for stronger schemes, such as Hidden Field Equations (Patarin, Hidden Field Equations and Isomorphisms of Polynomials: Two New Families of Asymmetric Algorithms 1996) and Quad (Berbain et al. 2006).

Multivariate signature schemes provide the shortest signatures among post-quantum algorithms (GUI [Mohamed und Petzoldt 2015] 129 bit over GF(2) for a quantum security level of 80 bit). The signature x of a message m is created by hashing m into a vector $y \in F^n$ and computing $x = P^{-1}(y) = T^{-1}\big(P'\big(S^{-1}(y)\big)\big)$. The receiver can simply compute the hash y and check if $P(x) = y$.

Medium Field Signature Schemes (Petzoldt et al. 2017) with fewer equations and variables in the public key offer a further reduction in key sizes, greater efficiency and scalable levels of security. It is the basis for the multivariate short signature system GEMSS (Casanova et al. kein Datum), which is an alternative candidate for the Round 3 finalists for NIST standardization.

The multivariate system Rainbow (Chen et al. kein Datum) has been chosen as one of three Round 3 finalists.

3.5 Isogeny-Based

One of the latest and most challenging post-quantum crypto ideas is the application of isogeny-based encryption schemes like Supersingular Isogeny Diffiehellmann (SIDH). With 2688-bit public keys at a 128-bit quantum security level, this scheme uses the smallest keys among post-quantum key exchanges. Additionally, it supports perfect forward secrecy, a property which preserves the confidentiality of old communication sessions even if long-term keys have been compromised.

Although not as thoroughly researched as the previously mentioned schemes, Microsoft published an experimental VPN library with a Supersingular Isogeny Key Encapsulation algorithm (SIKE) based on SIDH among an LWE key exchange and a signature algorithm using symmetric-key primitives and non-interactive zero-knowledge proofs (Microsoft Research Security and Cryptography Group kein Datum). SIKE has also been submitted to the NIST standardization process of post-quantum cryptography schemes. It has been chosen as one of five alternative public-key encryption and key-establishment algorithms for the final round.

In a YouTube video of a Microsoft research session where SIKE is presented to other researchers by Christophe Petit, he states at the end: “I wouldn’t bet national security on it”. On the other hand, SIDH was also described as “the hottest thing we have” in the keynote of the pqcrypto conference 2017.

4 Summary

Post-quantum cryptographic algorithm designers also work with other NP-hard problems from mathematical areas besides the ones we mentioned. We have, for example, Saber (Team SABER kein Datum), a secure key encapsulation mechanism (KEM) whose security relies on the hardness of the Module Learning with Rounding problem (MLWR) as NIST Round 3 finalist for public-key encryption and key-establishment algorithms.

In general, parameter choices are much more delicate for post-quantum cryptographic schemes than they are for classical ones. Furthermore, classical asymmetric schemes mostly rely on number theory, a topic studied in early university courses, whereas post-quantum algorithms tend to include mathematics from courses usually taught at later stages of study.

It will not only be a challenge to distinguish and weigh the complex influences on security of post-quantum encryption schemes; there will also be an increased need for cooperation between mathematicians, computer scientists and programmers to mitigate flaws in implementations, configurations and applications.

For someone who is not familiar with the concept of a mathematical conjecture, it is hard to understand the ground on which the security of cryptography is built and what time can do to it, with or without regard to emerging technologies. Who can say for sure that no one has been generating one RSA key pair after another for decades and storing them in a huge database, where they can simply assign a private key to its public key if it is in their collection? How many distinctive usable key pairs can even be expected within the range of a 4096-bit integer?

Literature

Alkim, E., L. Ducas, T. Pöppelmann, and P. Schwabe. 2015. "Post-Quantum Key Exchange—A New Hope." *IEEE Security and Privacy.*

Berbain, C., H. Gilbert, and J. Patarin. 2006. "A Practical Stream Cipher with Provable Security." *Springer Advances in Cryptology—Eurocrypt.*

Bernstein, D., C. Chuengsatiansup, T. Lange, and C. van Vredendaal. 2017. "NTRU Prime: Reducing Attack Surface at Low Cost." *Cryptology ePrint Archive.*

Bernstein, D. J., D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, and Z. Wilcox-O'Hearn. 2015. "SPHINCS: Practical Stateless Hash-Based Signatures." *Springer, Advances in Cryptology—EUROCRYPT.*

Bogomolec, X., and J. Gerhard. 2018. "Post-Quantum Secure Cryptographic Algorithms." *Computeralgebra-Rundbrief 63.*

Bos, J. W., C. Costello, M. Naehrig, and A. D. Stebila. 2013. "Post-Quantum Key Exchange for the TLS Protocol from the Ring Learning with Errors Problem." *Proceedings of the 45th Annual ACM Symposium on Theory of Computing.*

Casanova, A., J.-C. Faugere, G. Macario-Rat, J. Patarin, L. Perret, and J. Ryckeghem. n.d. "GeMSS: A Great Multivariate Short Signature." https://wwwpolsys.lip6.fr/Links/NIST/GeMSS_specification.pdf.

Chen, M.-S., J. Ding, M. Kannwischer, J. Patarin, A. Petzoldt, D. Schmidt, and B. Y. Yang. n.d. "Rainbow Signature." https://www.pqcrainbow.org/.

Courtois, N. T., M. Finiasz, and N. Sendrier. 2001. "How to Achieve a McEliece-Based Digital Signature Scheme." *Asiacrypt.*

Deneuveville, J. C., P. Gaborit, and G. Zémor. 2017. *A Simple, Secure and Efficient Key Exchange Protocol Based on Coding Theory.* https://ouroboros.rocks/docs/overview.

D-Wave Systems. n.d. *The First and Only Quantum Computer Built for Business.* https://www.dwavesys.com/.

Ducas, L., T. Lepoint, V. Lyubashevsky, P. Schwabe , G. Seiler, and D. Stehlé. 2017. "CRYSTALS—Dilithium: Digital Signatures from Module Lattices." *Cryptology ePrint Archive.*

Hoffstein, J., J. Pipher, and J. H. Silverman. 1998. "NTRU: A Ring-Based Public Key Cryptosystem." *SpringerLink International Number Theory Symposium.*

———. 2008. *An Introduction to Mathematical Cryptography.* Springer Science + Business Media.

Hsu, J. n.d. *Spectrum IEEE Tech Talk*, January 9, 2018. https://spectrum.ieee.org/techtalk/computing/hardware/intels-49qubit-chip-aims-for-quantum-supremacy.

Kelly, J. 2018. *Google AI Blog.* https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html.

Matsumoto, T., and H. Imai. 1988. "Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption." *Springer Eurocrypt.*

McEliece, R. 1978. "A Public-Key Cryptosystem Based on Algebraic Coding Theory." *DSN Progress Report 42–44.*

Microsoft Research Security and Cryptography Group. n.d. *Microsoft PQCrypto VPN.* https://github.com/Microsoft/PQCrypto-VPN.

Mohamed, M. S. E., and A. Petzoldt. 2015. *The Shortest Signatures Ever.* TU Darmstadt (Germany), Kyushu University (Japan).

Niederreiter, H. 1986. "Knapsack-Type Cryptosystems and Algebraic Coding Theory." *Problems of Control and Information Theory.*

Patarin, J. 1995. "Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt '88." *Springer CRYPTO .*

———. 1996. "Hidden Field Equations and Isomorphisms of Polynomials: Two New Families of Asymmetric Algorithms." *Eurocrypt.*

Petzoldt, A., M.-S. Chen, J. Ding, and B.-Y. Yang. 2017. *HMFEv—An Efficient Multivariate Signature Scheme*. Post-Quantum Cryptography: Springer.

Rijneveld, J., and S. Kölbl. n.d. *The SPHINCS+ Reference Code.* https://github.com/sphincs/sphincsplus.

Shor, P. W. 1997. "Polynomial Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer." *SIAM Jouranl on Computing*, 26 ed.: 1484–1509.

Team SABER. n.d. "MLWR Based KEM." *SABER.* https://www.esat.kuleuven.be/cosic/pqcrypto/saber/.

Wikipedia. n.d. *List of Quantum Processors.* https://en.wikipedia.org/wiki/List_of_quantum_processors.