./xenia.jpg

# Post-Quantum Secure Cryptographic Algorithms

**Dipl. Math. Xenia Bogomolec, X4pi UG**
**Dr. Jochen Gerhard, BearingPoint Software Solutions GmbH**

indigomind@protonmail.ch
jochen.gerhard@bearingpoint.com

./jochen.jpg

## Introduction

The expected dawn of a new technological era has certainly begun when IBM offered their first commercially available 20-Qubit Quantum Computers November 2017. While it was still discussed if it was necessary to take quantum technology into account in the IT industry during the last year, the estimations about their capability evolvement become much more specific now.

Luckily scientific researchers have specialized in the examinations of 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. Since 2010, they take place in another town of the world every year. The following article gives an overview of current developments in algorithmic solutions answering the upcoming threats posed by quantum computers as well as unsolved problems in the classical IT landscape.

### Quantum Technologies

Quantum-mechanical phenomena, such as superposition and entanglement, are used for communication, computing, sensing and simulation. While communication, sensing and simulation have been realized in publicly announced projects or products, quantum computing was only a matter of research until last november. 49 qubit processors mark quantum supremacy, the potential ability of quantum computing devices to solve problems that classical computers practically cannot solve. IBM has announced to have built a 50 qubit prototype, Google participates in the race with their new record-breaking 72-qubit quantum processor Bristlecone.

### 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. China has built a 2000km quantum communication channel between Beijing and Shanghai for banks, the Xinhua News Agency and the government, whose nodes receive keys from their quantum communication satellite. Last year they denoted feasible distances up to 1200 km.

In the future quantum computers with enough stable qubits are expected to be able to help building complex materials as well as solve medical and environmental problems amongst other things.

### Threats

It is long known that the security of currently used cryptographic algorithms relying on the hardness of integer factorization will expire with potent enough quantum computers. All public parameters like public keys from asymmetric key pairs and collected key exchanges with the following exchanged data can be used to decrypt data which is meant to be secret.

## Solutions

**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. So 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). Disadvantages for widespread practical usage are limited distances between communication partners and the need of expensive hardware.
Rarely mentioned is the fact that message source authentication does not come with QKD genuinely. Man in the middle attacks are also possible if the communication parties do not agree on an authentication protocol beforehand.

## Post-Quantum Cryptography

The alternative to QKD are algorithms whose security rely on mathematical properties, like hardness of computing the inversion of a one way function even with a quantum computer. There are four mathematical areas which offer solutions for encryption, key exchanges and signatures. Some of them are still in the middle of the research process, others have been observed and challenged for years. The advantages of post-quantum cryptography are that they run effectively on currently used devices such as smart phones, desktops and IoTs and they can be enabled by simple software updates.

**Code-Based**
Syndrome decoding of linear error-correcting codes are NP-complete considered as a decision problem if the number of errors are unbounded. On the other hand, some classes of linear codes have very fast decoding algorithms. The basic idea of a code-based crypto system is to choose a linear code with fast decoding algorithm and disguise it as a general linear code. Then the attacker has to use syndrome decoding for decrypting the message while the message receiver, 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 $P$

$$G' = SGP$$

where $S$, a $(k \times k)$ matrix, functions as a scrambler and $P$ is a $(n \times n)$ permutation matrix. Parameters proposed by MCELIECE [1] 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 [2] 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 [3]:

1) Choose a hash function $h$ and compute the hash value $h(d)$ of the document $d$ which has to be be signed
2) Decrypt the hash value $h(d)$ as if it was 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 to the signature and compares it to the hash value of the document.

Another simple, secure and efficient code-based key exchange protocol is OUROBOROS [4]. The encryption algorithm uses Quasi-Cyclic Codes in Hamming metric, efficient decoding is achieved through BitFlipping. Encryption and decryption are faster than RSA for comparative benchmarks (https://bench.cr.yp.to). Ouroboros' integration into the OpenSSL/TLS library is planned and it is proposed as post-quantum secure algorithm at the NIST.

**Hash-Based**
This domain is limited to digital signatures 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, same as it is known from 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. 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 PRNG and has the size of 256 bits as well. Hereby, the number of possibilities for such signatures are all possible combinations of the simple one-time signatures within the tree structure. This procedure considerously enhances the security of the scheme against brute force attacks.

The latest performance improved hash-based signature scheme is SPHINCS$^+$[5], the advanced SPHINCS [6] scheme which was presented at EUROCRYPT 2015. Unlike its predecessors, XMSS and LMS, it is stateless, meaning that signing doesn't require updating the secret key. It is a so called few-times scheme, where "few" means as much as $2^{64}$. Its signature sizes range from 8kb for NIST security level 1 to 30kb for NIST security level 5.

**Multivariate**

### Isogeny-Based

**To do** Good Idea as outlook! (1) One of the latest and most challenging pq crypto ideas is the application of Isogeny based encryption schemes. There are alread first applications, as e.g. Microsofts VPN-client. **To do** (2)

### 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 approximate adequates have been solved with NP-hard algorithms only. Given they are one of the longest known public key crypto systems, **To do** (3) they can be fairly seen as the most promising post quantum crypto approaches. However, due to their significantly bigger key sizes **To do** (4) they've not been as thoroughly researched and applied as RSA or EL GAMAL. [7] Most used and implemented methods so far - mostly used is NTRU. NewHope seems to be a very interesting thing... Potentially the first one was knapsack or subsetsum by Merkle and Hellman using superincreasing list of integers obfuscated by modulo - can be formulated and broken as finding smallest vector in a lattice. see silverman page 359 NTRU seems to be the first successful and still out there algorithm.

Have to speak about NTRU (Silverman), GGH, NTRU prime and new hope! and mention LLL −> BKZ which came out in 1982 (see silverman 406)
**To do** rewrite section (5)

## To do. . .

## References

[1] R. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory, *DSN Progress Report 42-44*, 1978.

[2] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory, *Problems of Control and Information Theory*, 1886.

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

[4] .... ..., ..., ....

[5] J. Rijneveld , S. Kölbl. The SPHINCS$^+$ reference code, *https://github.com/sphincs/sphincsplus*.

[6] D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, Z. Wilcox-O'Hearn. SPHINCS: practical stateless hash-based signatures, *Springer, Advances in Cryptology - EUROCRYPT 2015*.

[7] J. Hoffstein, J. Pipher, and J. H. Silverman. An Introduction to Mathematical Cryptography, *Springer Science+Business Media*, 2008.