Post-Quantum Secure Cryptographic Algorithms

Overview of Developments 2017/2018

Authors

Dr. Math. Jochen Gerhard

and

Dipl. Math. Xenia Bogomolec

with the friendly support of

Institute for Algebraic Geometry Leibniz University Hanover

July 2018

Content

July 12, 2018

1 Abstract **2**

2 Quantum Computing **3**

2.1 Benefits 3

2.2 Threats 3

3 Solutions **9**

3.1 Quantum Key Distribution 9

3.2 Post-Quantum Cryptography 9

3.2.1 Code-Based 12

3.2.1 Hash-Based 12

3.2.2 Isogeny-Based 12

3.2.3 Lattice-Based 9

3.2.4 Multivariate 9

1 Abstract

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.

2 Quantum Technologies

Quantum-mechanical phenomena, such as superposition and entanglement, are used for communication, computing, sensoring and simulation. While communication, sensoring 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.

2.1 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.

2.2 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.

3 Solutions

Science never sleeps and many splendid minds invested their work into the development of new technologies that will resist quantum computer attacks. There are two kind of approaches, physical and mathematical.

3.1 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. 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.

3.2 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.

3.2.1 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 such a system is to take one of those linear codes with fast decoding algorithms and disguise it as a general linear code. Then the attacker has use syndrome decoding for decrypting the message while the message receiver, who set up the system, can remove the disguise and use the fast decoding algorithm.

There are two basic encryption schemes based on this set-up, the McEliece and the Niederreiter cryptosystems. McEliece, introduced in 1978, was the first scheme using randomization in the encryption process. It is based on the choice of an (n, k)-linear code and consists of three algorithms:

1) a probabilistic key generation algorithm producing an asymmetric key pair
2) a probabilistic encryption algorithm
3) a deterministic decryption algorithm.

The private key is an error correcting code with efficient decoding algorithm represented by a generator matrix G. Originally binary Goppa Codes with the Patterson decoding algorithm were used. The public key is a 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 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. This cryptosystem cannot be used for authentication or signature schemes because the encryption algorithm is not one-to-one and the total algorithm is truly asymmetric (encryption and decryption do not commute)

- Wang proposed secure encryption scheme based on any efficient linear code
- encryption and decryption faster than RSA for comparative benchmarks (bench.cr.yp.to)
- rarely used, exceptionally: freenet-like application entropy
- McEliece not IK-CPA but Randomized McEliece IK-CPA

Niederreiter

- variation of McEliece 1986
- applies same idea to parity check matrix H of a linear code
- a signature scheme based on Niederreiter exists
- We proved that the k-repetition paradigm instantiated with Niederreiter is IK-CCA2 in the standard model. (IK = Indistinguishability of keys , means a ciphertext does not leak information about pk.)
- IND-CPA $\nLeftrightarrow$ IK-CPA, IND-CCA $\nLeftrightarrow$ IK-CCA
- IND-CCA2 and IK-CCA2 with k-wise Niederreiter, random padding, one-time signature
- open: more efficient scheme in the standard model?

Ouroboros

A simple, secure and efficient key exchange protocol based on coding theory. MCEliece 1978, Niederreiter 1986, RS,BCH, Goppa, RM 2000. Key exchange as an encryption scheme. Ouroboros is IND-CPA under the 2-DQCSD and 3-DQCSD assumptions.

3.2.2 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$^+$, the advanced SPHINCS 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.

3.2.3 Isogeny-Based

...

3.2.4 Lattice-Based

...

3.2.5 Multivariate

...