Post-quantum cryptography

Post-quantum cryptography (sometimes referred to as **quantum-proof**, **quantum-safe** or **quantum-resistant**) refers to cryptographic algorithms (usually public-key algorithms) that are thought to be secure against an attack by a quantum computer. As of 2018, this is not true for the most popular public-key algorithms, which can be efficiently broken by a sufficiently strong hypothetical quantum computer. The problem with currently popular algorithms is that their security relies on one of three hard mathematical problems: the integer factorization problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem. All of these problems can be easily solved on a sufficiently powerful quantum computer running Shor's algorithm.[1][2] Even though current, publicly known, experimental quantum computers lack processing power to break any real cryptographic algorithm,[3] many cryptographers are designing new algorithms to prepare for a time when quantum computing becomes a threat. This work has gained greater attention from academics and industry through the PQCrypto conference series since 2006 and more recently by several workshops on Quantum Safe Cryptography hosted by the European Telecommunications Standards Institute (ETSI) and the Institute for Quantum Computing.[4][5][6]

In contrast to the threat quantum computing poses to current public-key algorithms, most current symmetric cryptographic algorithms and hash functions are considered to be relatively secure against attacks by quantum computers.[2][7] While the quantum Grover's algorithm does speed up attacks against symmetric ciphers, doubling the key size can effectively block these attacks.[8] Thus post-quantum symmetric cryptography does not need to differ significantly from current symmetric cryptography. See section on symmetric-key approach below.

Contents

Algorithms

Currently post-quantum cryptography research is mostly focused on six different approaches:[2][5]

Lattice-based cryptography

This approach includes cryptographic systems such as learning with errors, ring learning with errors (ring-LWE),[9][10][11] the ring learning with errors key exchange and the ring learning with errors signature, the older NTRU or GGH encryption schemes, and the newer NTRU signature and BLISS signatures.[12] Some of these schemes like NTRU encryption have been studied for many years without anyone finding a feasible attack. Others like the ring-LWE algorithms have proofs that their security reduces to a worst-case problem.[13] The Post Quantum Cryptography Study Group sponsored by the European Commission suggested that the Stehle–Steinfeld variant of NTRU be studied for standardization rather than the NTRU algorithm.[14][15] At that time, NTRU was still patented. Studies have indicated that NTRU may have more secure properties than other lattice based algorithms [16].

Multivariate cryptography

This includes cryptographic systems such as the Rainbow (Unbalanced Oil and Vinegar) scheme which is based on the difficulty of solving systems of multivariate equations. Various attempts to build secure multivariate equation encryption schemes have failed. However, multivariate signature schemes like Rainbow could provide the basis for a quantum secure digital signature.[17] There is a patent on the Rainbow Signature Scheme.

Hash-based cryptography

This includes cryptographic systems such as Lamport signatures and the Merkle signature scheme and the newer XMSS[18] and SPHINCS[19] schemes. Hash based digital signatures were invented in the late 1970s by Ralph Merkle and have been studied ever since as an interesting alternative to number-theoretic digital signatures like RSA and DSA. Their primary drawback is that for any hash-based public key, there is a limit on the number of signatures that can be signed using the corresponding set of private keys. This fact had reduced interest in these signatures until interest was revived due to the desire for cryptography that was resistant to attack by quantum computers. There appear to be no patents on the Merkle signature scheme and there exist many non-patented hash functions that could be used with these schemes.

The stateful hash-based signature scheme XMSS is described in RFC 8391.[20] Note that all the above schemes are one-time or bounded-time signatures, Moni Naor and Moti Yung invented UOWHF hashing in 1989 and designed a signature based on hashing (the Naor-Yung scheme)[21] which can be unlimited-time in use (the first such signature that does not require trapdoor properties).

Code-based cryptography

This includes cryptographic systems which rely on error-correcting codes, such as the McEliece and Niederreiter encryption algorithms and the related Courtois, Finiasz and Sendrier Signature scheme. The original McEliece signature using random Goppa codes has withstood scrutiny for over 30 years. However, many variants of the McEliece scheme, which seek to introduce more structure into the code used in order to reduce the size of the keys, have been shown to be insecure.[22] The Post Quantum Cryptography Study Group sponsored by the European Commission has recommended the McEliece public key encryption system as a candidate for long term protection against attacks by quantum computers.[14]

Supersingular elliptic curve isogeny cryptography

This cryptographic system relies on the properties of supersingular elliptic curves and supersingular isogeny graphs to create a Diffie-Hellman replacement with forward secrecy.[23] This cryptographic system uses the well studied mathematics of supersingular elliptic curves to create a Diffie-Hellman like key exchange that can serve as a straightforward quantum computing resistant replacement for the Diffie-Hellman and elliptic curve Diffie–Hellman key exchange methods that are in widespread use today. Because it works much like existing Diffie–Hellman implementations, it offers forward secrecy which is viewed as important both to prevent mass surveillance by governments but also to protect against the compromise of long term keys through failures.[24] In 2012, researchers Sun, Tian and Wang of the Chinese State Key Lab for Integrated Service Networks and Xidian University, extended the work of De Feo, Jao, and Plut to create quantum secure digital signatures based on supersingular elliptic curve isogenies.[25] There are no patents covering this cryptographic system.

Symmetric key quantum resistance

Provided one uses sufficiently large key sizes, the symmetric key cryptographic systems like AES and SNOW 3G are already resistant to attack by a quantum computer.[26] Further, key management systems and protocols that use symmetric key cryptography instead of public key cryptography like Kerberos and the 3GPP Mobile Network Authentication Structure are also inherently secure against attack by a quantum computer. Given its widespread deployment in the world already, some researchers recommend expanded use of Kerberos-like symmetric key management as an efficient and effective way to get Post Quantum cryptography today.[27]

Security reductions

In cryptography research, it is desirable to prove the equivalence of a cryptographic algorithm and a known hard mathematical problem. These proofs are often called "security reductions", and are used to demonstrate the difficulty of cracking the encryption algorithm. In other words, the security of a given cryptographic algorithm is reduced to the security of a known hard problem. Researchers are actively looking for security reductions in the prospects for post quantum cryptography. Current results are given here:

Lattice-based cryptography – Ring-LWE Signature

In some versions of Ring-LWE there is a security reduction to the shortest-vector problem (SVP) in a lattice as a lower bound on the security. The SVP is known to be NP-hard.[28] Specific ring-LWE systems that have provable security reductions include a variant of Lyubashevsky's ring-LWE signatures defined in a paper by Güneysu, Lyubashevsky, and Pöppelmann.[10] The GLYPH signature scheme is a variant of the Güneysu, Lyubashevsky, and Pöppelmann (GLP) signature which takes into account research results that have come after the publication of the GLP signature in 2012. Another Ring-LWE signature is Ring-TESLA.[29]

Lattice-based cryptography – NTRU, BLISS

The security of the NTRU encryption scheme and the BLISS[12] signature is believed to be related to, but not provably reducible to, the Closest Vector Problem (CVP) in a Lattice. The CVP is known to be NP-hard. The Post Quantum Cryptography Study Group sponsored by the European Commission suggested that the Stehle–Steinfeld variant of NTRU **which does** have a security reduction be studied for long term use instead of the original NTRU algorithm.[14]

Multivariate cryptography – Rainbow

The Rainbow Multivariate Equation Signature Scheme is a member of a class of multivariate quadratic equation cryptosystems called "Unbalanced Oil and Vinegar Cryptosystems" (UOV Cryptosystems) Bulygin, Petzoldt and Buchmann have shown a reduction of generic multivariate quadratic UOV systems to the NP-Hard Multivariate Quadratic Equation Solving problem.[30]

Hash-based cryptography – Merkle signature scheme

In 2005, Luis Garcia proved that there was a security reduction of Merkle Hash Tree signatures to the security of the underlying hash function. Garcia showed in his paper that if computationally one-way hash functions exist then the Merkle Hash Tree signature is provably secure.[31]

Therefore, if one used a hash function with a provable reduction of security to a known hard problem one would have a provable security reduction of the Merkle tree signature to that known hard problem. [32]

The Post Quantum Cryptography Study Group sponsored by the European Commission has recommended use of Merkle signature scheme for long term security protection against quantum computers.[14]

Code-based cryptography – McEliece

The McEliece Encryption System has a security reduction to the Syndrome Decoding Problem (SDP). The SDP is known to be NP-hard[33] The Post Quantum Cryptography Study Group sponsored by the European Commission has recommended the use of this cryptography for long term protection against attack by a quantum computer.[14]

Code-based cryptography – RLCE

In 2016, Wang proposed a random linear code encryption scheme RLCE [34] which is based on McEliece schemes. RLCE scheme can be constructed using any linear code such as Reed-Solomon code by inserting random columns in the underlying linear code generator matrix.

Supersingular elliptic curve isogeny cryptography

Security is related to the problem of constructing an isogeny between two supersingular curves with the same number of points. The most recent investigation of the difficulty of this problem is by Delfs and Galbraith indicates that this problem is as hard as the inventors of the key exchange suggest that it is.[35] There is no security reduction to a known NP-hard problem.

Comparison

One common characteristic of many post-quantum cryptography algorithms is that they require larger key sizes than commonly used "pre-quantum" public key algorithms. There are often tradeoffs to be made in key size, computational efficiency and ciphertext or signature size. The table lists some values for different schemes at a 128 bit post-quantum security level.

Algorithm	Type	Public Key	Private Key	Signature
NTRU Encrypt[36]	Lattice	6130 B	6743 B	
Streamlined NTRU Prime	Lattice	1232 B		
Rainbow[37]	Multivariate	124 KB	95 KB	
SPHINCS[19]	Hash Signature	1 KB	1 KB	41 KB
SPHINCS+[38]	Hash Signature	32 B	64 B	8 KB
BLISS-II	Lattice	7 KB	2 KB	5 KB
GLP-Variant GLYPH Signature[10][39]	Ring-LWE	2 KB	0.4 KB	1.8 KB
New Hope[40]	Ring-LWE	2 KB	2 KB	
Goppa-based McEliece[14]	Code-based	1 MB	11.5 KB	
Random Linear Code based encryption[41]	RLCE	115 KB	3 KB	
Quasi-cyclic MDPC-based McEliece[42]	Code-based	1232 B	2464 B	
SIDH[43]	Isogeny	751 B	48 B	
SIDH (compressed keys)[44]	Isogeny	564 B	48 B	
3072-bit Discrete Log	**not PQC**	384 B	32 B	96 B
256-bit Elliptic Curve	**not PQC**	32 B	32 B	65 B

A practical consideration on a choice among post-quantum cryptographic algorithms is the effort required to send public keys over the internet. From this point of view, the Ring-LWE, NTRU, and SIDH algorithms provide key sizes conveniently under 1KB, hash-signature public keys come in under 5KB, and MDPC-based McEliece takes about 1KB. On the other hand, Rainbow schemes require about 125KB and Goppa-based McEliece requires a nearly 1MB key.

Lattice-based cryptography – LWE key exchange and Ring-LWE key exchange

The fundamental idea of using LWE and Ring LWE for key exchange was proposed and filed at the University of Cincinnati in 2011 by Jintai Ding. The basic idea comes from the associativity of matrix multiplications, and the errors are used to provide the security. The paper[45] appeared in 2012 after a provisional patent application was filed in 2012.

In 2014, Peikert[46] presented a key transport scheme following the same basic idea of Ding's, where the new idea of sending additional 1 bit signal for rounding in Ding's construction is also utilized. For somewhat greater than 128 bits of security, Singh presents a set of parameters which have 6956-bit public keys for the Peikert's scheme.[47] The corresponding private key would be roughly 14,000 bits.

In 2015, an authenticated key exchange with provable forward security following the same basic idea of Ding's was presented at Eurocrypt 2015,[48] which is an extension of the HMQV[49] construction in Crypto2005. The parameters for different security levels from 80 bits to 350 bits, along with the corresponding key sizes are provided in the paper.[48]

Lattice-based Cryptography – NTRU encryption

For 128 bits of security in NTRU, Hirschhorn, Hoffstein, Howgrave-Graham and Whyte, recommend using a public key represented as a degree 613 polynomial with coefficients $\mod (2^{10})$. This results in a public key of 6130 bits. The corresponding private key would be 6743 bits.[36]

Multivariate cryptography – Rainbow signature

For 128 bits of security and the smallest signature size in a Rainbow multivariate quadratic equation signature scheme, Petzoldt, Bulygin and Buchmann, recommend using equations in $\mathbb{F}_{31}$ with a public key size of just over 991,000 bits, a private key of just over 740,000 bits and digital signatures which are 424 bits in length.[37]

Hash-based cryptography – Merkle signature scheme

In order to get 128 bits of security for hash based signatures to sign 1 million messages using the fractal Merkle tree method of Naor Shenhav and Wool the public and private key sizes are roughly 36,000 bits in length.[50]

Code-based cryptography – McEliece

For 128 bits of security in a McEliece scheme, The European Commissions Post Quantum Cryptography Study group recommends using a binary Goppa code of length at least $n = 6960$ and dimension at least $k = 5413$, and capable of correcting $t = 119$ errors. With these parameters the public key for the McEliece system will be a systematic generator matrix whose non-identity part takes $k \times (n - k) = 8373911$ bits. The corresponding private key, which consists of the code support with $n = 6960$ elements from $GF(2^{13})$ and a generator polynomial of with $t = 119$ coefficients from $GF(2^{13})$, will be 92,027 bits in length[14]

The group is also investigating the use of Quasi-cyclic MDPC codes of length at least $n = 2^{16} + 6 = 65542$ and dimension at least $k = 2^{15} + 3 = 32771$, and capable of correcting $t = 264$ errors. With these parameters the public key for the McEliece system will be the first row of a systematic generator matrix whose non-identity part takes $k = 32771$ bits. The

private key, a quasi-cyclic parity-check matrix with $d = 274$ nonzero entries on a column (or twice as much on a row), takes no more than $d \times 16 = 4384$ bits when represented as the coordinates of the nonzero entries on the first row.

Barreto et al. recommend using a binary Goppa code of length at least $n = 3307$ and dimension at least $k = 2515$, and capable of correcting $t = 66$ errors. With these parameters the public key for the McEliece system will be a systematic generator matrix whose non-identity part takes $k \times (n - k) = 1991880$ bits.[51] The corresponding private key, which consists of the code support with $n = 3307$ elements from $GF(2^{12})$ and a generator polynomial of with $t = 66$ coefficients from $GF(2^{12})$, will be 40,476 bits in length.

Supersingular elliptic curve isogeny cryptography

For 128 bits of security in the supersingular isogeny Diffie-Hellman (SIDH) method, De Feo, Jao and Plut recommend using a supersingular curve modulo a 768-bit prime. If one uses elliptic curve point compression the public key will need to be no more than 8x768 or 6144 bits in length.[52] A March 2016 paper by authors Azarderakhsh, Jao, Kalach, Koziel, and Leonardi showed how to cut the number of bits transmitted in half, which was further improved by authors Costello, Jao, Longa, Naehrig, Renes and Urbanik resulting in a compressed-key version of the SIDH protocol with public keys only 2640 bits in size.[44] This makes the number of bits transmitted roughly equivalent to the non-quantum secure RSA and Diffie-Hellman at the same classical security level.[53]

Symmetric–key-based cryptography

As a general rule, for 128 bits of security in a symmetric-key-based system, one can safely use key sizes of 256 bits. The best quantum attack against generic symmetric-key systems is an application of Grover's algorithm, which requires work proportional to the square root of the size of the key space. To transmit an encrypted key to a device that possesses the symmetric key necessary to decrypt that key requires roughly 256 bits as well. It is clear that symmetric-key systems offer the smallest key sizes for post-quantum cryptography.

Forward secrecy

A public-key system demonstrates a property referred to as perfect forward secrecy when it generates random public keys per session for the purposes of key agreement. This means that the compromise of one message cannot lead to the compromise of others, and also that there is not a single secret value which can lead to the compromise of multiple messages. Security experts recommend using cryptographic algorithms that support forward secrecy over those that do not.[54] The reason for this is that forward secrecy can protect against the compromise of long term private keys associated with public/private key pairs. This is viewed as a means of preventing mass surveillance by intelligence agencies.

Both the Ring-LWE key exchange and supersingular isogeny Diffie-Hellman (SIDH) key exchange can support forward secrecy in one exchange with the other party. Both the Ring-LWE and SIDH can also be used without forward secrecy by creating a variant of the classic ElGamal encryption variant of Diffie-Hellman.

The other algorithms in this article, such as NTRU, do not support forward secrecy as is.

Any authenticated public key encryption system can be used to build a key exchange with forward secrecy.[55]

Open Quantum Safe project

Open Quantum Safe[56][57] **(OQS)** project was started in late 2016 and has the goal of developing and prototyping quantum-resistant cryptography. It aims to integrate current post-quantum schemes in one library: **liboqs**.[58] **liboqs** is an open source C library for quantum-resistant cryptographic algorithms. liboqs initially focuses on key exchange algorithms. liboqs provides a common API suitable for post-quantum key exchange algorithms, and will collect together various implementations. liboqs will also include a test harness and benchmarking routines to compare performance of post-quantum implementations. Furthermore, OQS also provides integration of liboqs into OpenSSL.[59]

As of April 2017, the following key exchange algorithms are supported:[56]

Algorithm	Type
BCNS15[60]	Ring learning with errors key exchange
NewHope[61][40]	Ring learning with errors key exchange
Frodo[62]	Learning with errors
NTRU[63]	Lattice-based cryptography
SIDH[64][65]	Supersingular isogeny key exchange
McBits[66]	Error-correcting codes

Implementation

One of the main challenges in post-quantum cryptography is considered to be the implementation of potentially quantum safe algorithms into existing systems. There are tests done, for example by Microsoft Research implementing PICNIC in a PKI using Hardware security modules.[67] Test implementations for Google's NewHope algorithm have also been done by HSM vendors.

See also

- Ideal lattice cryptography (ring-learning with errors is one example of ideal lattice cryptography)
- Post-Quantum Cryptography Standardization by NIST
- Quantum cryptography, for cryptography based on quantum mechanics; likely to be implemented in quantum computers.

References

1. Peter W. Shor (1997). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". *SIAM Journal on Computing*. **26** (5): 1484–1509. arXiv:quant-ph/9508027 (https://arxiv.org/abs/quant-ph/9508027). doi:10.1137/S0097539795293172 (https://doi.org/10.1137%2FS0097539795293172).
2. Daniel J. Bernstein (2009). "Introduction to post-quantum cryptography" (http://www.pqcrypto.org/www.springer.com/cda/content/document/cda_downloaddocument/9783540887010-c1.pdf) (PDF). *(Introductory Chapter to Book "Post-quantum Cryptography")*.
3. "New qubit control bodes well for future of quantum computing" (http://phys.org/news/2013-01-qubit-bodes-future-quantum.html). *phys.org*.

4. "Cryptographers Take On Quantum Computers" (http://spectrum.ieee.org/computing/software/cryptographers-take-on-quantum-computers). IEEE Spectrum. 2009-01-01.
5. "Q&A With Post-Quantum Computing Cryptography Researcher Jintai Ding" (http://spectrum.ieee.org/computing/networks/qa-with-postquantum-computing-cryptography-researcher-jintai-ding). IEEE Spectrum. 2008-11-01.
6. "ETSI Quantum Safe Cryptography Workshop" (http://www.etsi.org/news-events/events/770-etsi-crypto-workshop-2014?highlight=YTozOntpOjA7czo3OiJxdWFudHVtIjtpOjE7czo0OiJzYWZlIjtpOjI7czoxMjoicXVhbnR1bSBzYWZlIjt9). *ETSI Quantum Safe Cryptography Workshop*. ETSI. October 2014. Retrieved 24 February 2015.
7. Daniel J. Bernstein (2009-05-17). "Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?" (http://cr.yp.to/hash/collisioncost-20090823.pdf) (PDF).
8. Daniel J. Bernstein (2010-03-03). "Grover vs. McEliece" (http://cr.yp.to/codes/grovercode-20100303.pdf) (PDF).
9. Peikert, Chris (2014). "Lattice Cryptography for the Internet" (http://eprint.iacr.org). IACR. Archived from the original (http://eprint.iacr.org/2014/070.pdf) (PDF) on 31 January 2014. Retrieved 10 May 2014.
10. Güneysu, Tim; Lyubashevsky, Vadim; Pöppelmann, Thomas (2012). "Practical Lattice-Based Cryptography: A Signature Scheme for Embedded Systems" (http://emsec.rub.de/media/sh/veroeffentlichungen/2014/06/12/lattice_signature.pdf) (PDF). INRIA. Retrieved 12 May 2014.
11. Zhang, jiang (2014). "Authenticated Key Exchange from Ideal Lattices" (http://eprint.iacr.org/). *iacr.org*. IACR. Archived from the original (http://eprint.iacr.org/2014/589.pdf) (PDF) on 17 August 2014. Retrieved 7 September 2014.
12. Ducas, Léo; Durmus, Alain; Lepoint, Tancrède; Lyubashevsky, Vadim (2013). "Lattice Signatures and Bimodal Gaussians" (http://eprint.iacr.org/2013/383). Retrieved 2015-04-18.
13. Lyubashevsky, Vadim; =Peikert; Regev (2013). "On Ideal Lattices and Learning with Errors Over Rings" (http://eprint.iacr.org). IACR. Archived from the original (http://eprint.iacr.org/2012/230.pdf) (PDF) on 22 July 2013. Retrieved 14 May 2013.
14. Augot, Daniel (7 September 2015). "Initial recommendations of long-term secure post-quantum systems" (http://pqcrypto.eu.org/docs/initial-recommendations.pdf) (PDF). *PQCRYPTO*. Retrieved 13 September 2015.
15. Stehlé, Damien; Steinfeld, Ron (2013-01-01). "Making NTRUEncrypt and NTRUSign as Secure as Standard Worst-Case Problems over Ideal Lattices" (http://eprint.iacr.org/2013/004).
16. Easttom, Chuck (2019-02-01). "An Analysis of Leading Lattice-Based Asymmetric Cryptographic Primitivess" (https://ieeexplore.ieee.org/abstract/document/8666459).
17. Ding, Jintai; Schmidt (7 June 2005). Ioannidis, John (ed.). *Rainbow, a New Multivariable Polynomial Signature Scheme*. *Third International Conference, ACNS 2005, New York, NY, USA, June 7–10, 2005. Proceedings*. Lecture Notes in Computer Science. **3531**. pp. 64–175. doi:10.1007/11496137_12 (https://doi.org/10.1007%2F11496137_12). ISBN 978-3-540-26223-7.
18. Buchmann, Johannes; Dahmen, Erik; Hülsing, Andreas (2011). "XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions". *Lecture Notes in Computer Science*. **7071** (Post-Quantum Cryptography. PQCrypto 2011): 117–129. CiteSeerX 10.1.1.400.6086 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.400.6086). doi:10.1007/978-3-642-25405-5_8 (https://doi.org/10.1007%2F978-3-642-25405-5_8). ISSN 0302-9743 (https://www.worldcat.org/issn/0302-9743).
19. Bernstein, Daniel J.; Hopwood, Daira; Hülsing, Andreas; Lange, Tanja; Niederhagen, Ruben; Papachristodoulou, Louiza; Schneider, Michael; Schwabe, Peter; Wilcox-O'Hearn, Zooko (2015). Oswald, Elisabeth; Fischlin, Marc (eds.). *SPHINCS: practical stateless hash-based signatures*. *Lecture Notes in Computer Science*. **9056**. Springer Berlin Heidelberg. pp. 368–397. CiteSeerX 10.1.1.690.6403 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.690.6403). doi:10.1007/978-3-662-46800-5_15 (https://doi.org/10.1007%2F978-3-662-46800-5_15). ISBN 9783662467992.
20. "RFC 8391 - XMSS: eXtended Merkle Signature Scheme" (https://tools.ietf.org/html/rfc8391). *tools.ietf.org*.
21. *Moni Naor, Moti Yung: Universal One-Way Hash Functions and their Cryptographic Applications .STOC 1989: 33-43*
22. Overbeck, Raphael; Sendrier (2009). Bernstein, Daniel (ed.). *Code-based cryptography*. *Post-Quantum*

Cryptography. pp. 95–145. doi:10.1007/978-3-540-88702-7_4 (https://doi.org/10.1007%2F978-3-540-88702-7_4). ISBN 978-3-540-88701-0.

23. De Feo, Luca; Jao; Plut (2011). "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies" (http://eprint.iacr.org/2011/506.pdf) (PDF). *PQCrypto 2011*. Retrieved 14 May 2014.
24. Higgins, Peter (2013). "Pushing for Perfect Forward Secrecy, an Important Web Privacy Protection" (https://www.eff.org/deeplinks/2013/08/pushing-perfect-forward-secrecy-important-web-privacy-protection). Electronic Frontier Foundation. Retrieved 15 May 2014.
25. Sun, Xi; Tian; Wang (19–21 Sep 2012). *Browse Conference Publications > Intelligent Networking and Co … Help Working with Abstracts Toward Quantum-Resistant Strong Designated Verifier Signature from Isogenies*. *Intelligent Networking and Collaborative Systems (INCoS), 2012 4th International Conference on*. pp. 292–296. doi:10.1109/iNCoS.2012.70 (https://doi.org/10.1109%2FiNCoS.2012.70). ISBN 978-1-4673-2281-2.
26. Perlner, Ray; Cooper (2009). "Quantum Resistant Public Key Cryptography: A Survey" (https://www.nist.gov/manuscript-publication-search.cfm?pub_id=901595). NIST. Retrieved 23 Apr 2015.
27. Campagna, Matt; Hardjono; Pintsov; Romansky; Yu (2013). "Kerberos Revisited Quantum-Safe Authentication" (http://docbox.etsi.org/Workshop/2013/201309_CRYPTO/S03_INDUSTRY_SESSION/PITNEYBOWES_PINTSOV.pdf) (PDF). ETSI.
28. Lyubashevsky, Vadim; Peikert; Regev (25 June 2013). "On Ideal Lattices and Learning with Errors Over Rings" (https://web.eecs.umich.edu/~cpeikert/pubs/ideal-lwe.pdf) (PDF). Springer. Retrieved 19 June 2014.
29. Akleylek, Sedat; Bindel, Nina; Buchmann, Johannes; Krämer, Juliane; Marson, Giorgia Azzurra (2016). "An Efficient Lattice-Based Signature Scheme with Provably Secure Instantiation" (https://eprint.iacr.org/2016/030).
30. Bulygin, Stanislav; Petzoldt; Buchmann (2010). *Towards Provable Security of the Unbalanced Oil and Vinegar Signature Scheme under Direct Attacks*. *Progress in Cryptology – INDOCRYPT 2010*. Lecture Notes in Computer Science. **6498**. pp. 17–32. CiteSeerX 10.1.1.294.3105 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.294.3105). doi:10.1007/978-3-642-17401-8_3 (https://doi.org/10.1007%2F978-3-642-17401-8_3). ISBN 978-3-642-17400-1.
31. Pereira, Geovandro; Puodzius, Cassius; Barreto, Paulo (2016). "Shorter hash-based signatures". *Journal of Systems and Software*. **116**: 95–100. doi:10.1016/j.jss.2015.07.007 (https://doi.org/10.1016%2Fj.jss.2015.07.007).
32. Garcia, Luis. "On the security and the efficiency of the Merkle signature scheme" (http://eprint.iacr.org/2005/192.pdf) (PDF). *Cryptology ePrint Archive*. IACR. Retrieved 19 June 2013.
33. Blaum, Mario; Farrell; Tilborg (31 May 2002). *Information, Coding and Mathematics*. Springer. ISBN 978-1-4757-3585-7.
34. Wang, Yongge (2016). "Quantum resistant random linear code based public key encryption scheme RLCE". *Proceedings of Information Theory (ISIT)*. IEEE ISIT: 2519–2523. arXiv:1512.08454 (https://arxiv.org/abs/1512.08454).
35. Delfs, Christina; Galbraith (2013). "Computing isogenies between supersingular elliptic curves over F_p". arXiv:1310.7789 (https://arxiv.org/abs/1310.7789) [math.NT (https://arxiv.org/archive/math.NT)].
36. Hirschborrn, P; Hoffstein; Howgrave-Graham; Whyte. "Choosing NTRUEncrypt Parameters in Light of Combined Lattice Reduction and MITM Approaches" (https://www.securityinnovation.com/uploads/Crypto/params.pdf) (PDF). NTRU. Retrieved 12 May 2014.
37. Petzoldt, Albrecht; Bulygin; Buchmann (2010). "Selecting Parameters for the Rainbow Signature Scheme – Extended Version -" (http://eprint.iacr.org). Archived from the original (http://eprint.iacr.org/2010/437.pdf) (PDF) on 11 Aug 2010. Retrieved 12 May 2014.
38. "SPHINCS+: Submission to the NIST post-quantum project" (https://sphincs.org/data/sphincs+-specification.pdf) (PDF).
39. Chopra, Arjun (2017). "GLYPH: A New Insantiation of the GLP Digital Signature Scheme" (https://eprint.iacr.org/2017/766).
40. Alkim, Erdem; Ducas, Léo; Pöppelmann, Thomas; Schwabe, Peter (2015). "Post-quantum key exchange - a new

hope" (http://eprint.iacr.org/2015/1092) (PDF). Cryptology ePrint Archive, Report 2015/1092. Retrieved 1 September 2017.

41. Wang, Yongge (2017). "Revised Quantum Resistant Public Key Encryption Scheme RLCE and IND-CCA2 Security for McEliece Schemes" (https://eprint.iacr.org/2017/206).
42. Misoczki, R.; Tillich, J. P.; Sendrier, N.; Barreto, P. S. L. M. (2013). *MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes*. *2013 IEEE International Symposium on Information Theory*. pp. 2069–2073. CiteSeerX 10.1.1.259.9109 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.259.9109). doi:10.1109/ISIT.2013.6620590 (https://doi.org/10.1109%2FISIT.2013.6620590). ISBN 978-1-4799-0446-4.
43. Costello, Craig; Longa, Patrick; Naehrig, Michael (2016). "Efficient algorithms for supersingular isogeny Diffie-Hellman" (http://eprint.iacr.org/2016/413.pdf) (PDF). *Advances in Cryptology*.
44. Costello, Craig; Jao; Longa; Naehrig; Renes; Urbanik. "Efficient Compression of SIDH public keys" (https://eprint.iacr.org/2016/963). Retrieved 8 October 2016.
45. Lin, Jintai Ding, Xiang Xie, Xiaodong (2012-01-01). "A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem" (http://eprint.iacr.org/2012/688).
46. Peikert, Chris (2014-01-01). "Lattice Cryptography for the Internet" (http://eprint.iacr.org/2014/070).
47. Singh, Vikram (2015). "A Practical Key Exchange for the Internet using Lattice Cryptography" (http://eprint.iacr.org/2015/138). Retrieved 2015-04-18.
48. Zhang, Jiang; Zhang, Zhenfeng; Ding, Jintai; Snook, Michael; Dagdelen, Özgür (2015-04-26). Oswald, Elisabeth; Fischlin, Marc (eds.). *Authenticated Key Exchange from Ideal Lattices*. Lecture Notes in Computer Science. Springer Berlin Heidelberg. pp. 719–751. CiteSeerX 10.1.1.649.1864 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.649.1864). doi:10.1007/978-3-662-46803-6_24 (https://doi.org/10.1007%2F978-3-662-46803-6_24). ISBN 978-3-662-46802-9.
49. Krawczyk, Hugo (2005-08-14). "HMQV: A High-Performance Secure Diffie-Hellman Protocol". In Shoup, Victor (ed.). *Advances in Cryptology – CRYPTO 2005*. Lecture Notes in Computer Science. **3621**. Springer Berlin Heidelberg. pp. 546–566. doi:10.1007/11535218_33 (https://doi.org/10.1007%2F11535218_33). ISBN 978-3-540-28114-6.
50. Naor, Dalit; Shenhav; Wool (2006). "One-Time Signatures Revisited: Practical Fast Signatures Using Fractal Merkle Tree Traversal" (http://www.eng.tau.ac.il/~yash/Naor_Shenhav_Wool.pdf) (PDF). IEEE. Retrieved 13 May 2014.
51. Barreto, Paulo S. L. M.; Biasi, Felipe Piazza; Dahab, Ricardo; López-Hernández, Julio César; Morais, Eduardo M. de; Oliveira, Ana D. Salina de; Pereira, Geovandro C. C. F.; Ricardini, Jefferson E. (2014). Koç, Çetin Kaya (ed.). *A Panorama of Post-quantum Cryptography*. Springer International Publishing. pp. 387–439. doi:10.1007/978-3-319-10683-0_16 (https://doi.org/10.1007%2F978-3-319-10683-0_16). ISBN 978-3-319-10682-3.
52. De Feo, Luca; Jao; Plut (2011). "Towards Quantum-Resistant Cryptosystems From Supersingular Elliptic Curve Isogenies" (http://eprint.iacr.org). Archived from the original (http://eprint.iacr.org/2011/506.pdf) (PDF) on October 2011. Retrieved 12 May 2014.
53. "Cryptology ePrint Archive: Report 2016/229" (http://eprint.iacr.org/2016/229). *eprint.iacr.org*. Retrieved 2016-03-02.
54. Ristic, Ivan (2013-06-25). "Deploying Forward Secrecy" (https://community.qualys.com/blogs/securitylabs/2013/06/25/ssl-labs-deploying-forward-secrecy). SSL Labs. Retrieved 14 June 2014.
55. "Does NTRU provide Perfect Forward Secrecy?" (http://crypto.stackexchange.com/a/19115/12089). *crypto.stackexchange.com*.
56. "Open Quantum Safe" (https://openquantumsafe.org/). *openquantumsafe.org*.
57. Stebila, Douglas; Mosca, Michele. "Post-Quantum Key Exchange for the Internet and the Open Quantum Safe Project" (http://eprint.iacr.org/2016/1017). *Cryptology ePrint Archive, Report 2016/1017, 2016*. Retrieved 9 April 2017.
58. "liboqs: C library for quantum-resistant cryptographic algorithms" (https://github.com/open-quantum-safe/liboqs). 26 November 2017 – via GitHub.
59. "openssl: Fork of OpenSSL that includes quantum-resistant algorithms and ciphersuites based on liboqs" (https://github.com/open-quantum-safe/openssl). 9 November 2017 – via GitHub.

60. Stebila, Douglas (26 Mar 2018). "liboqs nist-branch algorithm datasheet: kem_newhopenist" (https://github.com/open-quantum-safe/liboqs/blob/7cc365a363a05cdb233b9d72d0164c123d7b0b65/docs/algorithms/kem_newhopenist.md). *GitHub*. Retrieved 27 September 2018.
61. "Lattice Cryptography Library" (https://www.microsoft.com/en-us/research/project/lattice-cryptography-library/). *Microsoft Research*. 19 Apr 2016. Retrieved 27 September 2018.
62. Bos, Joppe; Costello, Craig; Ducas, Léo; Mironov, Ilya; Naehrig, Michael; Nikolaenko, Valeria; Raghunathan, Ananth; Stebila, Douglas (2016-01-01). "Frodo: Take off the ring! Practical, Quantum-Secure Key Exchange from LWE" (http://eprint.iacr.org/2016/659).
63. "NTRUOpenSourceProject/NTRUEncrypt" (https://github.com/NTRUOpenSourceProject/NTRUEncrypt). *GitHub*. Retrieved 2017-04-10.
64. "SIDH Library - Microsoft Research" (https://www.microsoft.com/en-us/research/project/sidh-library/). *Microsoft Research*. Retrieved 2017-04-10.
65. Feo, Luca De; Jao, David; Plût, Jérôme (2011-01-01). "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies" (https://web.archive.org/web/20140503190338/http://eprint.iacr.org/2011/506). Archived from the original (https://eprint.iacr.org/2011/506) on 2014-05-03.
66. Bernstein, Daniel J.; Chou, Tung; Schwabe, Peter (2015-01-01). "McBits: fast constant-time code-based cryptography" (https://eprint.iacr.org/2015/610).
67. "Microsoft/Picnic" (https://github.com/Microsoft/Picnic/blob/master/spec/design-v1.0.pdf) (PDF). *GitHub*. Retrieved 2018-06-27.

Further reading

- *Post-Quantum Cryptography* (https://www.springer.com/mathematics/numbers/book/978-3-540-88701-0). Springer. 2008. p. 245. ISBN 978-3-540-88701-0.
- Isogenies in a Quantum World (http://ecc2011.loria.fr/slides/jao.pdf)
- On Ideal Lattices and Learning With Errors Over Rings (http://www.di.ens.fr/~pnguyen/LCD/LCD_Vadim.pdf)
- Kerberos Revisited: Quantum-Safe Authentication (http://docbox.etsi.org/Workshop/2013/201309_CRYPTO/S03_INDUSTRY_SESSION/PITNEYBOWES_PINTSOV.pdf)
- The picnic signature scheme (https://github.com/Microsoft/Picnic/blob/master/spec/design-v1.0.pdf)

External links

- PQCrypto, the post-quantum cryptography conference (http://www.pqcrypto.org/)
- ETSI Quantum Secure Standards Effort (http://www.etsi.org/news-events/news/947-2015-03-news-etsi-launches-quantum-safe-cryptography-specification-group)
- NIST's Post-Quantum crypto Project (http://csrc.nist.gov/groups/ST/post-quantum-crypto/)
- PQCrypto Usage & Deployment (https://ianix.com/pqcrypto/pqcrypto-deployment.html)
