Post Quantum Cryptography

By Ankit Chandra

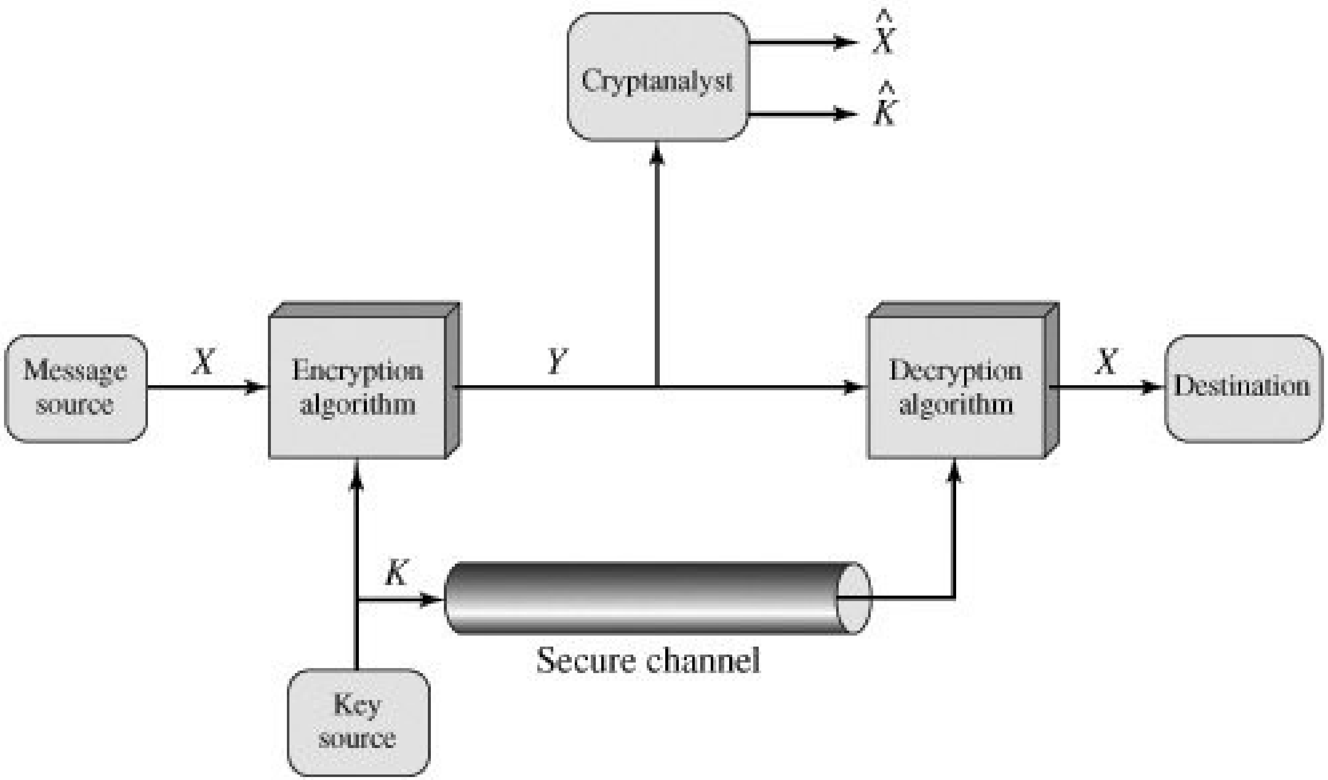
Introduction

Cryptography is the science of keeping private information from unauthorized access, of ensuring data integrity and authentication.

Classical Cryptography

Two parties, Alice(Sender) and Bob(Recipient), wish to exchange messages via some insecure channel in a way that protects their messages from eavesdropping.

Classical Cryptography



Impact of Quantum Computers on current encryption techniques

- Current Encryption techniques can been broken using quantum computers.
- Eg Shor’s algorithm when run on quantum computer can be used to break public key cryptography schemes like RSA, Elgamal.

Post Quantum cryptography(PQC)

Post-quantum cryptography refers to research on cryptographic primitives (usually public-key cryptosystems) that are not breakable using quantum computers.

- This work is popularized by the PQCrypto conference series since 2006

Need to study PQC

- In a predictive sense, quantum computers may become a technological reality; it is therefore important to study cryptographic schemes that are (supposedly) secure even against adversaries with access to a quantum computer.

Approaches in PQC

Presently there are four approaches in post quantum cryptography

- **Lattice-based cryptography** such as NTRU and GGH
- **Hash-based signatures** such as Lamport signatures and Merkle signature scheme
- **Multivariate cryptography**
- **Code-based cryptography** that relies on error-correcting codes, such as McEliece encryption and Niederreiter signatures

Lattice based cryptography:

- Lattice-based cryptography is the generic term for asymmetric cryptographic primitives based on lattices.
- A lattice *L* is a set of points in the *n*- dimentional Euclidean space $\mathbf{R}^n$ with a strong periodicity property
- Lattices were first studied by mathematicians Joseph Louis Lagrange and Carl Friedrich Gauss.
- Lattices have been used recently in computer algorithms and in cryptanalysis.

Multivariate cryptography:

Multivariate cryptography is the generic term for asymmetric cryptographic primitives based on multivariate polynomials over finite fields

- Solving systems of multivariate polynomial equations is proven to be NP-Hard or NP-Complete.
- Hence these schemes are often considered to be good candidates for post-quantum cryptography, once quantum computers can break the current schemes.
- Today multivariate quadratics could be used only to build signatures. All attempts to build a secure encryption scheme have so far failed

Hash based cryptography:

- Hash-based digital signature schemes use a cryptographic hash function. Their security relies on the collision resistance of that hash function
- Hash-based signature schemes are the most important post-quantum signature candidates. Although there is no proof of their quantum computer resistance, their security requirements are minimal.
- Each new cryptographic hash function yields a new hash-based signature scheme. So the construction of secure signature schemes is independent of hard algorithmic problems in number

Code based Cryptography:

- It is the cryptosystems in which the algorithmic primitive (the underlying one-way function) uses an error correcting code C. This primitive may consist in adding an error to a word of C or in computing a syndrome relatively to a parity check matrix of C.
- The first of those systems is a public key encryption scheme and it was proposed by Robert J. McEliece in 1978.Not much of research has been on this topic
- But no attack is known to represent a serious threat on the system, even on a quantum computer.

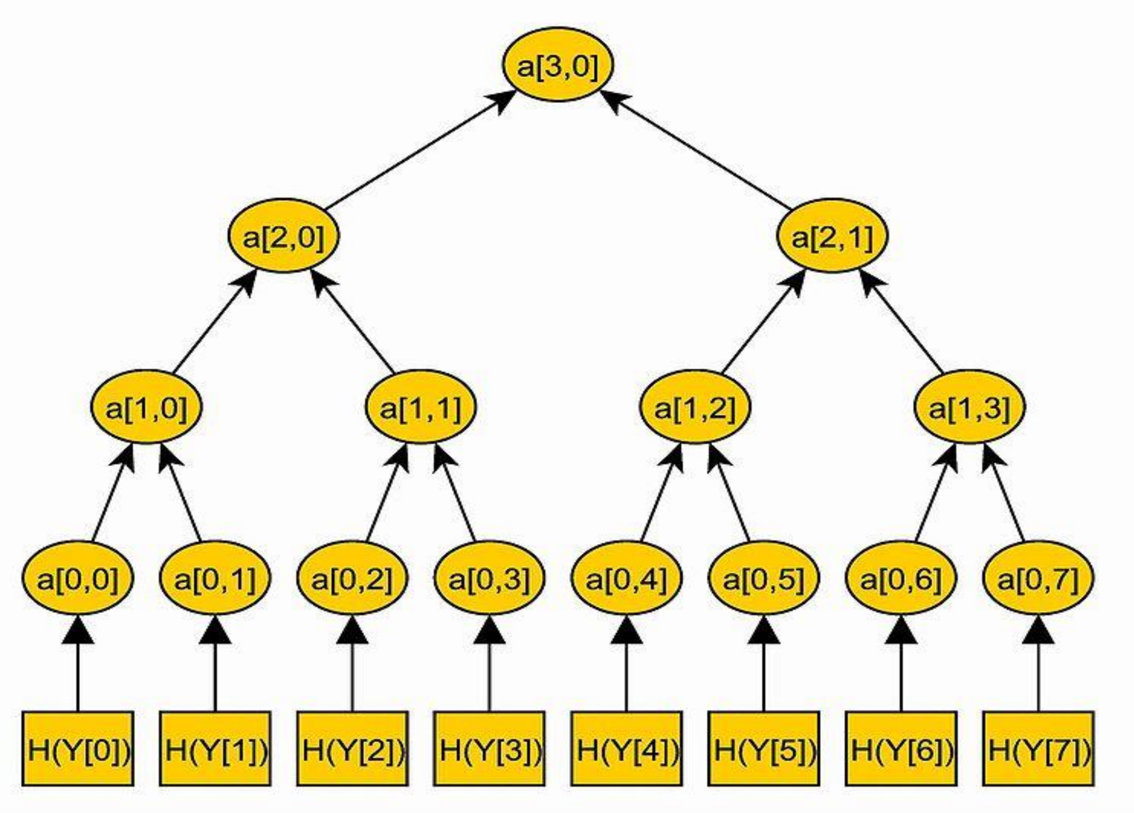
Hash based signature scheme

Merkle signature scheme:

This scheme was invented by Ralph Merkle.

- The idea of Merkle to use a hash tree that reduces the validity of many one-time verification keys (the leaves of the hash tree) to the validity of one public key (the root of the hash tree).

Merkle hash tree



Merkle signature scheme

- Key generation

The number of possible messages must be a power of two, so that we denote the possible number of messages as $N=2^n$.

- Generate public keys X_i and private keys Y_i where i denotes the messages.
- Calculate hash values $h_i = H(X_i)$.
- Each node is denoted by $a_{i,j}$ where i-level no
  j-position of node in that level
- h_i are stored in leaves and intermediate nodes are hash values of their respective child.
- Hence root is public key of the scheme

Signature generation

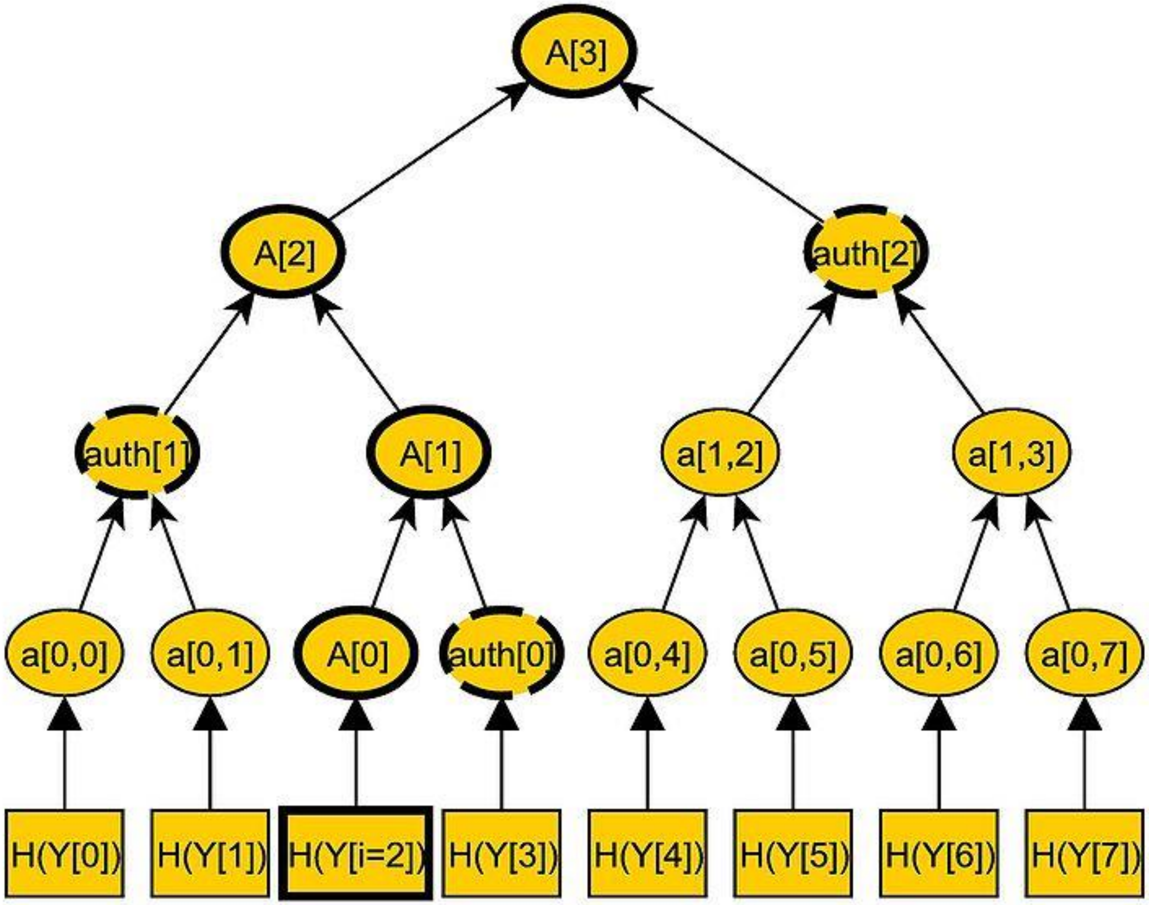
- Path from leaf to root node is used in generating the signature
- the message M is signed with a one-time signature scheme, resulting in a signature sig', first. This is done, by using one of the public and private key pairs (X_i , Y_i).
- The nodes, plus the one-time signature sig' of message M is the signature $sig = H(sig' \,||auth0\, ||auth1\, ||\, \ldots ||authn - 1)$ where $auth_i$ is hash value of intermediate nodes.

Signature verification:

The receiver knows the public key pub, the message M, and the signature

$sig = (sig' \,||auth_0 \,||auth_1 \,|| \ldots ||auth_{n-1})$

Hence is the signature matches it is considered valid.


A[3]
A[2]
auth[2]
auth[1]
A[1]
a[1,2]
a[1,3]
a[0,0]
a[0,1]
A[0]
auth[0]
a[0,4]
a[0,5]
a[0,6]
a[0,7]
H(Y[0])
H(Y[1])
H(Y[i=2])
H(Y[3])
H(Y[4])
H(Y[5])
H(Y[6])
H(Y[7])

Lattice based cryptography

Lattice based cryptography has an encryption system called NTRUEncrypt system

NTRUEncrypt system

Operations are based on objects in a truncated polynomial ring with convolution multiplication and all polynomials in the ring as integer coefficients and degree at most *N*-1

- Each system is specified by three integer parameters (*N*, *p*, *q*) which represent the maximal degree N-1 for all polynomials in the truncated ring *R*, a small modulus and a large modulus, respectively, where it is assumed that *N* is prime, *q* is always larger than *p*, and *p* and *q* are coprime
- Four sets of polynomials L_f, L_g, L_m and L_r (a polynomial part of the private key, a polynomial for generation of the public key, the message and a blinding value, respectively), all of degree at most N-1

Key generation

- To generate the key pair two polynomials **f** and **g**, with coefficients much smaller than q, with degree at most N-1 and with coefficients in {-1, 0, 1}
- Polynomial $f \ \in Lf$ must be taken such that $f\,.fp = 1\ (mod\ p)$ and $f\,.fq = 1\ (mod\ p)$ must hold

The public key **h** is generated computing the quantity

$$h = fq.g\ (mod\ q)$$

Encryption

Sender puts message in the form of a polynomial m with coefficients {-1, 0, 1}.

- With Bob's public key **h** the encrypted message **e** is computed:

$$e = pr.h + m \ (mod \ q)$$

Decryption

- The ciphertext can be decrypted using the following formula

$$a = e\ (mod\ q)$$

This can be explained by following steps

$a = f.e\ (mod\ q)$

$a = f.(r.ph + m)(mod\ q)$

$a = f.(r.p(fq).\ g + m)(mod\ q)$

$a = p(r.g) + f.m\ (mod\ q)$

$b = a\ (mod\ p)$

$b = f.m\ (mod\ p)$ (because $pr.g\ (mod\ p) = 0$)

$c = fp.b = fp.f.m\ (mod\ p)$

$c = m\ (mod\ p)$ (since $f.fp = 1\ (mod\ p)$ was required for fp)

Attacks possible on NTRUEncrypt

1. Ciphertext only attack
2. Lattice based reduction attack

Disadvantages of NTRUEncrypt is it is considered as slow

Challenges of PQC

Three important reasons that parts of the cryptographic community are already starting to focus attention on post quantum cryptography

1. Efficiency
2. Confidentiality
3. Usability

Conclusion

- Long term confidential documents will be readable once quantum computer is build. E.g. military secrets, Electronic signatures on long-term commitments can be forged once quantum computers are available.
- Need to research and implement this system is very important for future security purpose.

References

1. Daniel J. Bernstein (2009). "Introduction to post-quantum cryptography"
2. Peter W. Shor (1995-08-30). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer"
3. Multivariate Cryptography. http://en.wikipedia.org/wiki/Multivariate_cryptography
4. Lattice Based Cryptography. http://en.wikipedia.org/wiki/Lattice-based_cryptography
5. Lattice based problems. http://en.wikipedia.org/wiki/Lattice_problems#cite_note-ajtai-18
6. Merkle Signature scheme. http://en.wikipedia.org/wiki/Merkle_signature_scheme
7. Ralph Merkle. "Secrecy, authentication and public key systems / A certified digital signature". Ph.D. dissertation, Dept. of Electrical Engineering, Stanford University, 1979.
8. NTRUEncrypt Algorithm. http://en.wikipedia.org/wiki/NTRUEncrypt

Thank you