Introduction to Post-Quantum Cryptography

Dung H. Duong

Kyushu University

Cybersecurity Workshop, UNSW March 28-29, 2016

Introduction

Widely used public key cryptosystems

- RSA : integer factorization problem
- ECC (Elliptic curve cryptography) : discrete logarithm problem

Widely used public key cryptosystems

- RSA : integer factorization problem
- ECC (Elliptic curve cryptography) : discrete logarithm problem

Threats

- 1994. Shor's quantum algorithm
- growth of computer power

Introduction

Widely used public key cryptosystems

- RSA : integer factorization problem
- ECC (Elliptic curve cryptography) : discrete logarithm problem

Threats

- 1994. Shor's quantum algorithm
- growth of computer power

All public key cryptosystems will be insecure in the era of large-scale quantum computer

Need

Alternative cryptosystems whose underlying mathematical problems are hard for

- powerful classical computers
- large-scale quantum computers

Need

Alternative cryptosystems whose underlying mathematical problems are hard for

- powerful classical computers
- large-scale quantum computers

$\Rightarrow$ Post-quantum (quantum-safe) cryptography

Need

Alternative cryptosystems whose underlying mathematical problems are hard for

- powerful classical computers
- large-scale quantum computers

$\Rightarrow$ Post-quantum (quantum-safe) cryptography

- long-term security, efficient implementation
- high functional: fully homomorphic encryption, multi-linear maps

Post-quantum cryptography

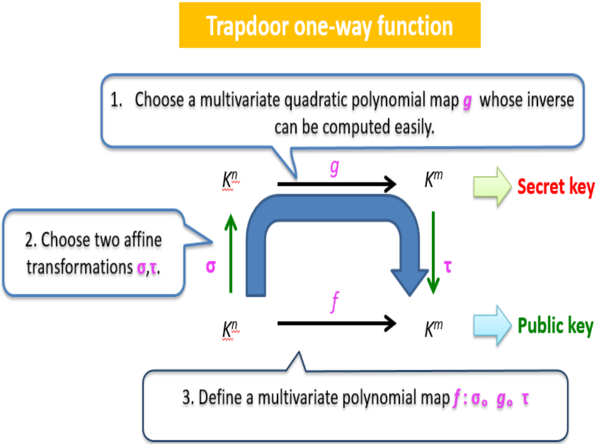
- Lattice-based cryptography (eg. NTRU)
- Code-based cryptography (eg. McEliece-Niederreiter)
- Multivariate cryptography (eg. UOV, Rainbow)
- Hash-based cryptography
- Others (isogeny based cryptography...)

Multivariate public key cryptosystems (MPKC) whose security depends on the difficulty of MQ problem (NP-hard)

MQ problem: find a solution of the system of multivariate equations:

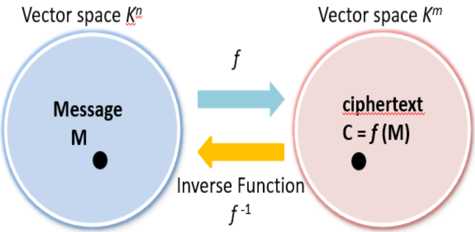
$$\begin{cases} f^{(1)}(x_1, \cdots, x_n) & = \sum_{1 \le i,j \le n} a_{ij}^{(1)} x_i x_j + \sum_{1 \le i \le n} b_i^{(1)} x_i + c^{(1)} = d^{(1)} \\ f^{(2)}(x_1, \cdots, x_n) & = \sum_{1 \le i,j \le n} a_{ij}^{(2)} x_i x_j + \sum_{1 \le i \le n} b_i^{(2)} x_i + c^{(2)} = d^{(2)} \\ \quad \cdots & \\ f^{(m)}(x_1, \cdots, x_n) & = \sum_{1 \le i,j \le n} a_{ij}^{(m)} x_i x_j + \sum_{1 \le i \le n} b_i^{(m)} x_i + c^{(m)} = d^{(m)} \end{cases}$$

MPKC structure



MPKC encryption

$f : K^n \rightarrow K^m$ multivariate polynomial map

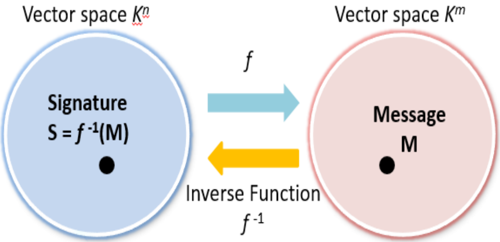


For any cipher text ***C***, there must exist the corresponding plain text uniquely.

⇒ f is injective. ⇒ $n \leq m.$ Ex. Simple Matrix scheme, ZHFE, EFC, SRP

MPKC signature

$f : K^n \to K^m$ multivariate polynomial map



For any message **M**, there must exist the corresponding signature.

⇒ f is surjective. ⇒ $n \geq m$. Ex. UOV, Rainbow, Gui

Recent activities

- January 2015, DIMACS Workshop on The Mathematics of Post-Quantum Cryptography
- April 2015, NIST Workshop on Cybersecurity in a Post-Quantum World
- September 2015, Dagstuhl Seminar on Quantum Cryptanalysis
- November 2015, ESTI Workshop on Quantum-safe Cryptography
- February 2016, PQCrypto 2016, Fukuoka, Japan

- August 2015, **National Security Agency (NSA)** announced preliminary plans for transitioning to quantum resistant algorithms
- 240 participants (USA 70, Europe 60, Asia 110)
- **National Institute of Standards and Technology (NIST)** announced "Post-Quantum Cryptography: NIST's Plan for the Future"

NIST's timeline

Timeline

- Fall 2016 – formal Call For Proposals
- Nov 2017 – Deadline for submissions
- 3–5 years – Analysis phase
  - NIST will report its findings
- 2 years later – Draft standards ready

- Workshops
  - Early 2018 – submitter's presentations
  - One or two during the analysis phase

Big research projects

- Post-quantum cryptography for long-term security: http://pqcrypto.eu.org/
- CROSSING: https://www.crossing.tu-darmstadt.de/
- JST CREST CryptoMath: https://cryptomath-crest.jp/

Laboratory of Mathematical Designs for Advanced Cryptography

- Established: April 1, 2015
- Members:
  - Prof. Tsuyoshi Takagi (head), Assoc. Prof. Masaya Yasuda, Assist. Prof. Dung H. Duong
  - 3 postdocs, 3 PhD students, around 15 master and undergraduate students
- Areas of research
  - Post-quantum cryptography: lattice-based, hash-based, isogeny-based and multivariate cryptography
  - elliptic curve cryptography, pairing, NFS
  - implementation

Thank you!