Post-Quantum Cryptography

a talk about problems... problems... problems

Andreas Hülsing

TU Eindhoven
The Problem
Public-key cryptography
Main (public-key) primitives

- Digital signature (DSIG)
  - Proof of authorship
  - Provides:
    - Authentication
    - Non-repudiation

- Public-key encryption (PKE) / Key exchange (KEX) / Key encapsulation mechanism (KEM)
  - Establishment of commonly known secret key
  - Provides secrecy
Applications

• Code signing (DSIG)
  • Software updates
  • Software distribution
  • Mobile code

• Communication security (DSIG, PKE / KEX /KEM)
  • TLS, SSH, IPSec, ...
  • eCommerce, online banking, eGovernment, ...
  • Private online communication
Connection security (simplified)

Hi

pk, Cert(pk belongs to shop)

PKC to establish shared secret sk

SKC secured communication using sk
How to build PKC

(Computationally) hard problem

PKC Scheme

RSA - OAEP
ECDSA
DH-KE
The problem

• Large (few thousand logical qubits) quantum computers can solve previously used problems (Factoring & DLog)
• All previous public key schemes are broken
• No KEX, KEM, PKE, and DSIG

• Symmetric key primitives generally remain secure!
This is a problem that QKD cannot solve!
But post-quantum cryptography can!
Early post-quantum crypto

„Cryptography based on problems that are conjectured to be hard even for quantum computers.“

Lattice-based: SVP / CVP

Hash-based: CR / SPR / ...

Code-based: SD

Multivariate: MQ

\[
y_1 = x_1^2 + x_1x_2 + x_1x_4 + x_3
\]

\[
y_2 = x_3^2 + x_2x_3 + x_2x_4 + x_1 + 1
\]

\[
y_3 = ...
\]
Modern post-quantum crypto

„Users using cryptography on conventional computers facing quantum adversaries“

Adds questions like
- How to argue security?
- Are our security models sound?
- What is the complexity of actual quantum attacks?
The computational complexity approach

- Public key cryptography cannot be information theoretically secure
- We need to base it on hardness of computational problems
- Cryptanalysis needed to determine complexity of solving problems aka breaking systems
  - Needed to select parameters.
Conjectured quantum-hard problems

• Solving multivariate quadratic equations (MQ-problem) -> Multivariate Crypto

• Syndrom decoding problem (SD) -> Code-based crypto

• Short(est) and close(st) vector problem (SVP, CVP) -> Lattice-based crypto

• Breaking security of symmetric primitives (SHAx-, AES-, Keccak-,... problem) -> Hash-based signatures / symmetric crypto

• (Finding isogenies between supersingular elliptic curves -> SIDH)
“We see our role as managing a process of achieving community consensus in a transparent and timely manner” NIST’s Dustin Moody 2018
Status of the competition

- Nov 2017 Submissions collected
- Dec 2017 Complete & Proper proposals published
  - -> Starts round 1 (of 2 or 3 rounds)
- 2022 – 2024 Draft standards exist
### Submissions
(69 complete & proper)

<table>
<thead>
<tr>
<th>Type</th>
<th>PKE/KEM</th>
<th>Signature</th>
<th>Signature &amp; PKE/KEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lattice</td>
<td>21 (-1 due to merge)</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Code-based</td>
<td>18 (-1 withdrawn)</td>
<td>3 (-1 withdrawn)</td>
<td></td>
</tr>
<tr>
<td>Hash-based</td>
<td></td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Multivariate</td>
<td>2</td>
<td>7</td>
<td>2 (-1 withdrawn)</td>
</tr>
<tr>
<td>Braid group</td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Supersingular Elliptic Curve Isogeny</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Satirical submission</td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Other</td>
<td>4 (-2 withdrawn)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
First evaluation results

Submissions

• Submissions generally follow a few previously known theoretic constructions.
• Submissions differ in how the theoretical construction is implemented

Attacks

• 11 attacks on 10 schemes published.
• No “big surprises” (aka efficient solution to one of the underlying hard problems)
• Attacks either break those schemes that are “fundamentally new” or exploit implementation decisions
The computational problems
MQ-Problem

Let \( x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n \) and \( \text{MQ}(n, m, \mathbb{F}_q) \) denote the family of vectorial functions \( F: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m \) of degree 2 over \( \mathbb{F}_q \):

\[
\text{MQ}(n, m, \mathbb{F}_q) = \left\{ F(x) = (f_1(x), \ldots, f_m(x)) \mid f_s(x) = \sum_{i,j} a_{i,j} x_i x_j + \sum_i b_i x_i \right\},
\]
Multivariate Cryptography

• First proposal 1988
• Only signatures
  -> (new proposal for encryption exists but very recent)
• Cryptanalysis tasks:
  • Hardness of solving random MQ-instance
  • Hardness of solving “special” MQ-instances
• Known quantum attacks:
  • “Quantization” of classical algorithms (Bernstein & Yang ‘17, Faugère, Horan, Kahunobaei, Kaplan, Kashefi & Perret ‘17)
    • Cost $\mathcal{O}(2^{cn})$, $c = 0.457$ for $m=n$ and $q=2$
Syndrom Decoding Problem

Given a matrix $G \in \mathbb{F}_q^{k \times n}$ of rank $k$, the set $C := \{mG : m \in \mathbb{F}_q^k\}$ is called a linear code with generator matrix $G$. If $C = \{c \in \mathbb{F}_q^n : Hc^t = 0\}$ we call $H$ the parity check matrix.

Syndrom Decoding Problem

Given:

- Linear Code $C \subseteq \mathbb{F}_q^n$,
- Syndrom $s \subseteq \mathbb{F}_q^k$,
- and error bound $b \in \mathbb{N}$

Return:

- $e \in \mathbb{F}_q^n$ of weight $\leq b$ such that $He^t = s$

Decision version is NP-hard (Berlekamp, McEliece & v.Tilborg ’78; Barg ’94)
Code-based cryptography

• First proposal 1978: McEliece with binary Goppa codes
• Until recently, practical proposals only known for KEM
• Either huge keys or structured codes (QC-MDPC)
• Cryptanalysis tasks:
  • Hardness of solving random SD-instance
  • Hardness of solving SD for specific codes (QC-MDPC, Goppa)
• Known quantum attacks:
  • “Quantization” of classical algorithms (Kachigar & Tillich '17)
  • Cost $O(2^{cn})$, $c = 0.058$ worst-case
Lattice-based cryptography

Basis: $B = (b_1, b_2) \in \mathbb{Z}^{2 \times 2}; b_1, b_2 \in \mathbb{Z}^2$

Lattice: $\Lambda(B) = \{x = By \mid y \in \mathbb{Z}^2\}$
Shortest vector problem (SVP)
(Worst-case) Lattice Problems

- **SVP**: Find shortest vector in lattice, given random basis. NP-hard (Ajtai’96)
- **Approximate SVP (αSVP)**: Find short vector (norm $< \alpha$ times norm of shortest vector). Hardness depends on $\alpha$ (for $\alpha$ used in crypto not NP-hard).
- **CVP**: Given random point in underlying vectorspace (e.g. $\mathbb{Z}^n$), find the closest lattice point. (Generalization of SVP, reduction from SVP)
- **Approximate CVP (αCVP)**: Find a „close“ lattice point. (Generalization of αSVP)
Lattice-based crypto

• First proposal GGH (proposed 1995, published 1997) or Ajtai (1996)?
• Signatures & KEM / KEX
• Either huge keys and/or sigs or structured lattices (Ideal / module lattices)
• Cryptanalysis tasks:
  • Hardness of solving $\alpha$SVP for random lattices
  • Hardness of solving $\alpha$SVP for structured lattices (Ideal-, Module lattices)
• Known quantum attacks:
  • “Quantization” of classical algorithms (Laarhoven, Mosca & v.d.Pol ‘15; Aono, Nguyen & Shen '18)
  • Cost $2^{cn+o(n)}$, $c = 0.268$ (heuristically)
(Hash) function families

- $H_n := \{h_k : \{0,1\}^{m(n)} \rightarrow \{0,1\}^n\}$
- $m(n) \geq n$
- „efficient“
Preimage resistance (PRE)

\[ H_n := \{ h_k : \{0,1\}^{m(n)} \to \{0,1\}^n \} \]

\[ h_k \leftarrow H_n \]
\[ x \leftarrow \{0,1\}^{m(n)} \]
\[ y_c \leftarrow h_k(x) \]

Success if \( h_k(x^*) = y_c \)
Collision resistance (CR)

\[ H_n := \{ h_k : \{0,1\}^m(\text{n}) \rightarrow \{0,1\}^n \} \]

\[ h_k \leftarrow H_n \]

Success if

\[ h_k(x_1^*) = h_k(x_2^*) \text{ and } x_1^* \neq x_2^* \]
Second-preimage resistance (SPR)

\[ H_n := \{ h_k : \{0,1\}^{m(n)} \to \{0,1\}^n \} \]

\[ h_k \leftarrow H_n \]
\[ x_c \leftarrow \{0,1\}^{m(n)} \]

Success if
\[ h_k(x_c) = h_k(x^*) \text{ and } x_c \neq x^* \]
Hash-based signatures

• First proposal Lamport (1979)
• Only signatures
• Fast & compact (2kB, few ms), but stateful, or
• Stateless, bigger and slower (41kB, several ms).
• Cryptanalysis tasks:
  • Solving PRE, SPR, CR,... for random function families
  • Solving PRE, SPR, CR,... for specific hash function (SHA2, SHA3)
• Quantum attacks:
  • Upper & lower bounds for generic attacks (Zhandry ‘15, Huelsing, Song & Rijneveld ‘16)
    • PRE, SPR: $\Theta\left(\frac{q^2}{2^n}\right)$, CR: $\Theta\left(\frac{q^3}{2^n}\right)$
  • Costs in more realistic models are worse (e.g. Bernstein & Souza Banegas ‘17)
Quantum cryptanalysis?

All known algorithms improve conventional algorithms by less than a square root factor!
Conclusion

• We need more actual quantum cryptanalysis!
• Skipped due to time: There are a lot of open questions beyond selecting new DSIG / KEM / PKE schemes:
  • What are the right models when proving security?
    • See notion of collapsing [Unruh ‘16], or the ongoing discussion about indifferentiability [Zhandry ‘18, Carstens, Ebrahimi, Tabia & Unruh ‘18]
  • How do we proof security in these models?
    • Real-Ideal: We often do not even know quantum complexity in ideal setting
Resources

• PQ Summer School: https://2017.pqcrypto.org/school/index.html

• NIST PQC Standardization Project: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
Thank you!
Questions?