Post-Quantum Cryptography & Privacy
Andreas Hülsing
Privacy?

... the Panopticon must not be understood as a dream building: it is the diagram of a mechanism of power reduced to its ideal form.

Michel Foucault, Discipline and Punish, 1977
Too abstract?
How to achieve privacy?
Under the hood...

Public-key crypto
- ECC
- RSA
- DSA

Secret-key crypto
- AES
- SHA2
- SHA1
- ...

Combination of both needed!
Secret-key cryptography
Main (Secret-key) primitives

• Block- / Stream Cipher
  • Encryption of data
  • Provides Secrecy

• Massage authentication code
  • Authentication of data
  • Provides authenticity

• Hash function
  • Cryptographic checksum
  • Allows efficient comparison
Public-key cryptography
Main (public-key) primitives

• Digital signature
  • Proof of authorship
  • Provides:
    • Authentication
    • Non-repudiation

• Public-key encryption / key exchange
  • Establishment of commonly known secret key
  • Provides secrecy
Applications

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

• Communication security (Signatures, PKE / KEX)
  • 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
We need secret- and public-key crypto to achieve privacy!
How to build PKC

(Computationally) hard problem

RSA  DL  QR  DDH

PKC Scheme

RSA-OAEP  ECDSA  DH-KE
Quantum Computing
Quantum Computing

“Quantum computing studies theoretical computation systems (quantum computers) that make direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data.”

-- Wikipedia
Qubits

• Qubit state: $\alpha_0 \ket{0} + \alpha_1 \ket{1}$ with $\alpha_i \in \mathbb{C}$ such that $|\alpha_0|^2 + |\alpha_1|^2 = 1$

• Ket: $\ket{0} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\ket{1} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

• Qubit can be in state $\frac{\ket{0} + \ket{1}}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

• Computing with 0 and 1 at the same time!
Quantum computers are not almighty

• To learn outcome one has to measure.
  • Collapses state
  • 1 qubit leads 1 classical bit of information
  • Randomized process

• Only invertible computation.

• Impossible to clone (copy) quantum state.
The Quantum Threat
Shor’s algorithm (1994)

- Quantum computers can do FFT very efficiently
- Can be used to find period of a function
- This can be exploited to factor efficiently (RSA)
- Shor also shows how to solve discrete log efficiently (DSA, DH, ECDSA, ECDH)
Grover’s algorithm (1996)

- Quantum computers can search $N$ entry DB in $\Theta(\sqrt{N})$
- Application to symmetric crypto
- Nice: Grover is provably optimal (For random function)
- Double security parameter.
To sum up

• All asymmetric crypto is broken by QC
  • No more digital signatures
  • No more public key encryption
  • No more key exchange

• No secure shopping for tea...
Quantum Cryptography
Why not beat ‘em with their own weapons?

• QKD: Quantum Key distribution.
  • Based on some nice quantum properties: entanglement & collapsing measurements
  • Information theoretic security (at least in theory) -> Great!
  • For sale today!

• So why don’t we use this?
• Only short distance, point-to-point connections!
  • Internet? No way!

• Longer distances require „trusted-repeaters“ 😊
  • We all know where this leads...
PQCRYPTO to the rescue
Quantum-secure problems

No provably quantum resistant problems

We must look here

Bounded-Error Quantum Polynomial-Time

NP-complete

NP

Factoring

BQP

P

Credits: Buchmann, Bindel 2015
Conjectured quantum-secure problems

- Solving multivariate quadratic equations (MQ-problem)
  -> Multivariate Crypto
- Bounded-distance decoding (BDD)
  -> 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
MQ-Problem

Let \( x = (x_1, ..., x_n) \in \mathbb{F}_q^n \) 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 \( \mathbb{F}_q \):

\[
\text{MQ}(n, m, \mathbb{F}_q) = \left\{ F(x) = (f_1(x), ..., f_m(x)) \mid f_s(x) = \sum_{i,j} a_{i,j} x_i x_j + \sum_i b_i x_i, \quad s \in [1, m] \right\}
\]

The MQ Problem \( \text{MQ}(F, \nu) \) is defined as given \( \nu \in \mathbb{F}_q^m \) find, if any, \( s \in \mathbb{F}_q^n \) such that \( F(s) = \nu \).

Decisional version is NP-complete [Garey, Johnson´79]
Multivariate Signatures (trad. approach)

\[ P: \mathbb{F}^n \rightarrow \mathbb{F}^m, \text{ easily invertible non-linear} \]

\[ S: \mathbb{F}^n \rightarrow \mathbb{F}^n, \ T: \mathbb{F}^m \rightarrow \mathbb{F}^m, \text{ affine linear} \]

Public key: \[ G = S \circ P \circ T, \] hard to invert

Secret Key: \[ S, P, T \text{ allows to find } G^{-1} \]

\[ G^{-1} = T^{-1} \circ P^{-1} \circ S^{-1} \]

Signing: \[ s = T^{-1} \circ P^{-1} \circ S^{-1}(m) \]

Verifying: \[ G(s) = ? m \]

Forging signature: Solve \[ G(s) - m = 0 \]

Fast

Large keys:
100 kBit for 100 bit security
Compared to
1776 bit
RSA modulus

- UOV, Goubin et al., 1999
- Rainbow, Ding, et al. 2005
- pFlash, Cheng, 2007
- Gui, Ding, Petzoldt, 2015

Credits: Buchmann, Bindel 2015
Multivariate Cryptography

• Breaking scheme $\iff$ Solving random MQ-instance
  -> NP-complete is a worst-case notion
    (there might be – and there are for MQ -- easy instances)
  -> Not a random instance

Many broken proposals
-> Oil-and-Vinegar, SFLASH, MQQ-Sig, (Enhanced) TTS, Enhanced STS.
-> Security somewhat unclear

• Only signatures
  -> (new proposal for encryption exists but too recent)

• Really large keys

• New proposal with security reduction, small keys, but large signatures.
Coding-based cryptography - BDD

Given:
- Linear code $C \subseteq F_2^n$
- $y \in F_2^n$
- $t \in \mathbb{N}$

Find:
- $x \in C$: $\text{dist}(x, y) \leq t$

BDD is NP-complete (Berlekamp et al. 1978) (Decisional version)

Credits: Buchmann, Bindel 2015
McEliece PKE (1978)

$S, G, P$ matrices over $F$

$G$ generator matrix for Goppa code

Public key: $G' = S \circ G \circ P, t$

Secret Key: $P, S, G$

Encryption: $c = mG' + z \in F^n$

Decryption: $x = cP^{-1} = mSG + zP^{-1}$

solve BDD to get $y = mSG$

decode to obtain $m$

Allows to solve BDD

Fast

Large public keys!

500 kBits for 100 bit security

Compared to 1776 bit RSA modulus

IND-CPA secure version

Credits: Buchmann, Bindel 2015
Code-based cryptography

• Breaking scheme ⇔ Solving BDD
  -> NP-complete is a worst-case notion
    (there might be – and there are for BDD -- easy instances)
  -> Not a random instance
  However, McEliece with binary Goppa codes survived for almost 40 years (similar situation as for e.g. AES)

• Using more compact codes often leads to break
• So far, no practical signature scheme

• Really large public keys
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 $\alpha$SVP)
(Average-case) Lattice Problems
Short Integer Solution (SIS)

\[ \mathbb{Z}_p^n \text{ = n-dim. vectors with entries mod } p \ (\approx n^3) \]

Goal:
Given \( A = (a_1, a_2, \ldots, a_m) \in \mathbb{Z}_p^{n \times m} \)
Find "small" \( s = (s_1, \ldots, s_m) \in \mathbb{Z}^m \) such that

\[ As = 0 \text{ mod } p \]

Reduction from worst-case \( \alpha \text{SVP}. \)
Hash function

Set \( m > n \log p \) and define \( f_A: \{0,1\}^m \rightarrow \mathbb{Z}_p^n \) as

\[
f_A(x) = Ax \mod p
\]

**Collision-resistance:** Given short \( x_1, x_2 \) with \( Ax_1 = Ax_2 \) we can find a short solution as

\[
Ax_1 = Ax_2 \Rightarrow Ax_1 - Ax_2 = 0
\]

\[
A(x_1 - x_2) = 0
\]

So, \( z = x_1 - x_2 \) is a solution and it is short as \( x_1, x_2 \) are short.
Lattice-based crypto

- SIS: Allows to construct signature schemes, hash functions, ... , basically minicrypt.
- For more advanced applications: Learning with errors (LWE)
  - Allows to build PKE, IBE, FHE,...
- Performance: Sizes can almost reach those of RSA (just small const. factor), really fast (for lattices defined using polynomials).
- BUT: Exact security not well accessed, yet. Especially, no good estimate for quantum computer aided attacks.
Hash-based Signature Schemes

[Mer89]

- Post quantum
- Only secure hash function
- Security well understood
- Fast
RSA – DSA – EC-DSA...

Intractability Assumption

Cryptographic hash function

Digital signature scheme

RSA, DH, SVP, MQ, ...

19-3-2018
Merkle’s Hash-based Signatures

SIG = (i=2, PK, SK, 〇, 〇, 〇, 〇)
Hash-based signatures

• Only signatures
• Minimal security assumptions
• Well understood
• Fast & compact (2kB, few ms), but stateful, or
• Stateless, bigger and slower (41kB, several ms).

• Two Internet drafts (drafts for RFCs), one in „RFC Editor queue“
NIST Competition

POST-QUANTUM CRYPTOGRAPHY PROJECT

NEWS -- December 15, 2016: The National Institute of Standards and Technology (NIST) is now accepting submissions for quantum-resistant public-key cryptographic algorithms. The deadline for submission is November 30, 2017. Please see the Post-Quantum Cryptography Standardization menu at left for the complete submission requirements and evaluation criteria.

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise...
Resources

• PQ Summer School: https://2017.pqcrypto.org/school/index.html
• NIST PQC Standardization Project: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
• Master Math (Selected Areas in Cryptology): https://elo.mastermath.nl/
Thank you!
Questions?