

# Post-Quantum Cryptography: Introduction and Trends

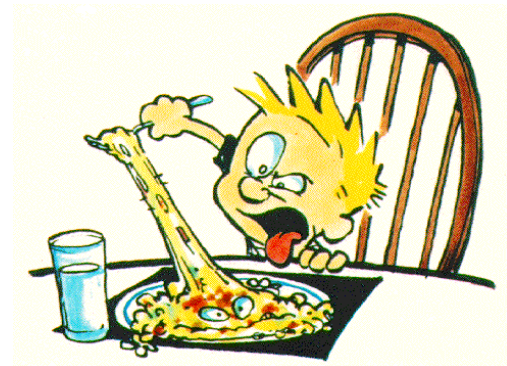


Paulo S. L. M. Barreto

LARC/PCS/EPUSP

# A Preliminary Word

- This talk is an introductory overview, and hence necessarily incomplete.
- The choice of topics is, to a certain extent, a matter of personal taste (shame on me for unfulfilled expectations).



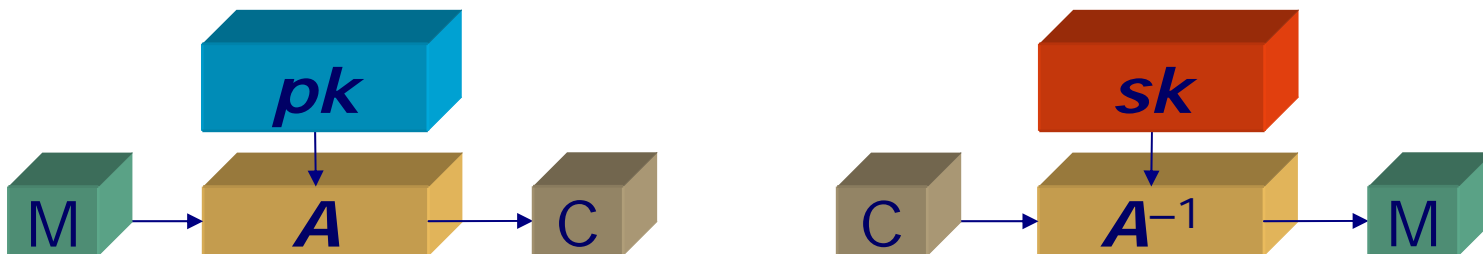
# Asymmetric Cryptography

- Two distinct keys:

- Private (or secret) key  $sk$ .
- Public key  $pk$ .

- Infeasible to compute  $sk$  from  $pk$ .

- Transformations that depend on one of these keys can only be feasibly inverted using the *other* key of the same pair.



# Motivation

- The overwhelming majority of actually deployed public key cryptosystems rest on only *two* intractability assumptions: IFP and DLP.
- Shor's quantum algorithm can efficiently solve (i.e. break) the IFP and the DLP.



# Post-Quantum Cryptosystems

- Entirely classical (plug-in replacements to IFP and DLP based schemes).
- Intractability assumptions apparently beyond the capabilities of quantum computers.

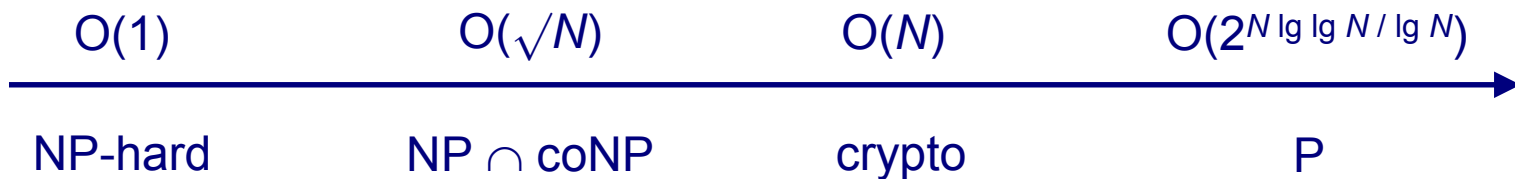


# Is that secure?

- Nobody knows exactly what quantum computers can do ( $BQP$  vs  $NP$ )...
- Nobody knows exactly what *classical* computers can do either ( $P$  vs  $NP$ )...
- IFP and DLP are not even known to be classically intractable (that's why we talk about *security assumptions*).

# Is that secure?

- Post-quantum security assumptions: certain problems are “hard enough” even for quantum computers.
- Possibly not intractable in the most stringent sense (e.g. not NP-hard).



# Effective resistance against quantum attacks

- No known polynomial-cost quantum attacks does not mean no effect at all!
- Quantum shortcuts: Grover search reduces  $O(N)$  to  $O(\sqrt{N})$ , and hence  $O(2^k)$  to  $O(\sqrt{2^k})$ , i.e. still exponential (with smaller basis).
- Keys sizes are  $O(k^c)$  for some small  $c$ , hence an increase by a factor of  $2^c$  addresses this issue.

# Proposed Post-Quantum Families

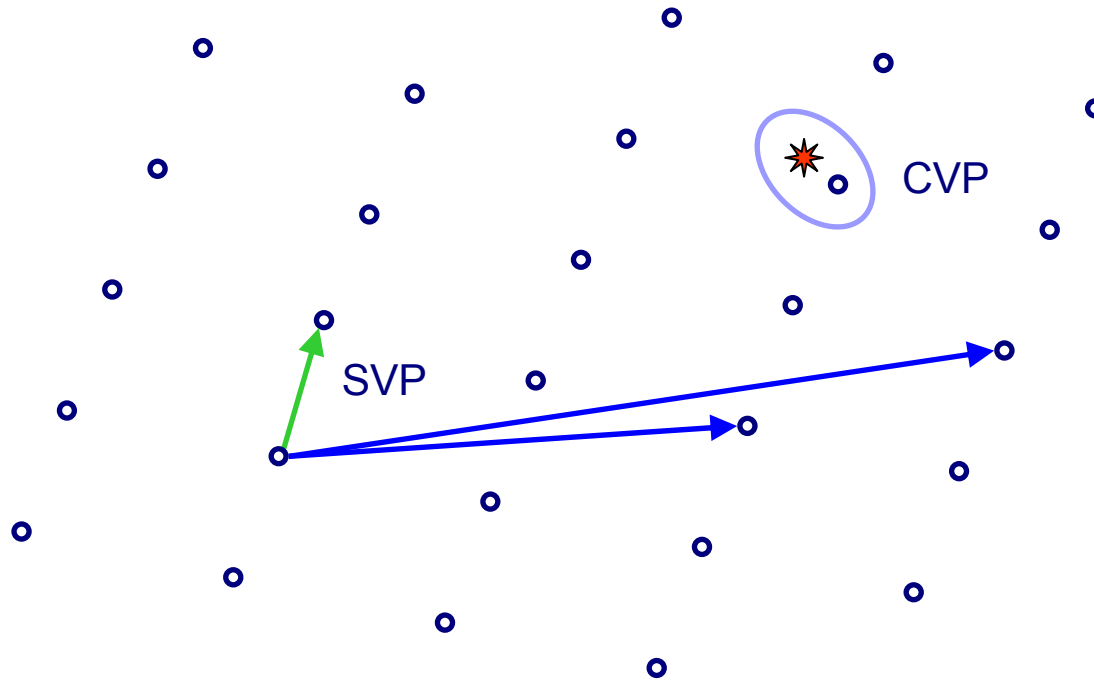
- *Lattices*;
- *Coding theory*;
- *Multivariate quadratic equations (MQE)*;
- Many more: Merkle signatures, permuted kernels and perceptrons, constrained linear equations, distributional matrix representability, **non-Abelian groups**, ...



# The Main Players

- Certain lattice and coding problems bear a striking resemblance.
- Some cryptosystems reflect that similarity as well:
  - McEliece (1978) in Fujisaki-Okamoto mode (1999): codes.
  - Peikert (2008): lattices.
- Relationship between coding-based schemes and MQE.

# Lattice Problems



# Closest Vector in a Lattice

## ■ Input:

- positive integers  $n, k, t$ ;
- generator matrix  $G \in (\mathbb{Z}/q\mathbb{Z})^{k \times n}$  of a modular lattice  $\mathcal{L} \subset (\mathbb{R})^n$ ;
- vector  $c \in (\mathbb{R})^n$ .

- ## ■ Question: $\exists? m \in (\mathbb{Z}/q\mathbb{Z})^k$ such that $e = c$
- $mG$  has Euclidean norm  $\ell_2(e) \leq t$  ?

# Bounded Distance Decoding

## ■ Input:

- positive integers  $n, k, t$ ;
- generator matrix  $G \in (\mathbb{F}_q)^{k \times n}$  of a linear  $[n, k]$ -code  $\mathcal{C} \subset (\mathbb{F}_q)^n$ ;
- vector  $c \in (\mathbb{F}_q)^n$ .

- ## ■ Question:
- $\exists? m \in (\mathbb{F}_q)^k$  such that  $e = c - mG$  has Hamming weight  $\text{wt}(e) \leq t$  ?

# McEliece-FO Cryptosystem

## ■ Key generation:

- Choose a uniformly random  $[n, k]$   $t$ -error correcting Goppa code  $\Gamma(L, g)$ , compute systematic generator  $G \in (\mathbb{F}_2)^{k \times n}$ , and set  $sk \leftarrow (L, g)$ ,  $pk \leftarrow (G, t)$ .

## ■ Encryption of $m \in \{0, 1\}^k$ :

- Choose a uniformly random  $r \in (\mathbb{F}_2)^k$  and compute a  $t$ -error vector  $e \leftarrow \mathcal{H}(r, m) \in (\mathbb{F}_2)^n$ .
- Compute  $c \leftarrow (rG + e, \mathcal{E}(r) \oplus m) \in (\mathbb{F}_2)^n \times \{0, 1\}^k$ .

$$c \leftarrow (rG + e, \mathcal{E}(r) \oplus m)$$

## ■ Decryption of $(u, d) \in (\mathbb{F}_2)^n \times \{0, 1\}^k$ :

- Use  $sk$  to correct the errors in  $u$ , recovering  $r$  and  $e$ .
- Recover  $m \leftarrow \mathcal{E}(r) \oplus d$  and accept iff  $e = \mathcal{H}(r, m)$ .

# Peikert Cryptosystem

## ■ Key generation:

- Choose a full-rank, almost uniformly random matrix  $G \in (\mathbb{Z}_q)^{k \times n}$  and a trapdoor (i.e. “short”) matrix  $D \in \mathbb{Z}^{n \times n}$  such that  $GD = O \pmod{q}$ , and set  $sk \leftarrow D$ ,  $pk \leftarrow G$ .

## ■ Encryption of $m \in \{0, 1\}^t$ :

- Choose a uniformly random  $r \in (\mathbb{Z}_q)^k$  and a normally distributed error vector  $e \in (\mathbb{Z}_q)^n$ .
- Compute  $c \leftarrow (rG + e, \mathcal{E}(r) \oplus m) \in (\mathbb{Z}_q)^n \times \{0, 1\}^t$ .

$$c \leftarrow (rG + e, \mathcal{E}(r) \oplus m)$$

## ■ Decryption of $(u, d) \in (\mathbb{Z}_q)^n \times \{0, 1\}^t$ :

- Use  $sk$  to correct the errors in  $u$ , recovering  $r$ .
- Recover  $m \leftarrow \mathcal{E}(r) \oplus d$ .

# Coding-based schemes vs MQE

- Parity-check matrix:  $H$  such that  $HG^T = O$ .
- Private code:  $H_0G_0^T = O$  for some highly structured  $H_0$ .
- Public code:  $HG^T = O$ , with  $G = G_0P$  for some (private) punctured permutation  $P$ .
- $\therefore H_0PG^T = O$ .
- MQE system in the elements of  $H_0$  and  $P$ .

# Cryptographically-Friendly Problems

- Examples of actual security assumptions:
  - $u$ -SVP hard to approximate to a subquadratic factor in the lattice dimension.
  - permuted Goppa codes hard to decode.
- Usually the best known way to attack these particular assumptions is the same as for more general settings.
  - generic lattice reduction and information set decoding.
- Beware of “assumption proliferation.”

# An Unexpected Side Effect

- Query to a distributed database: how much does a company spend with its payroll?

$$\sum_{p \in P} S_p \times E_p$$

- where:

- $P$  = employee positions in the company,
- $S_p$  = salary associated to position  $p$ ,
- $E_p$  = #employees in position  $p$ .

# An Unexpected Side Effect

- Computations must be distributed.
- Even retrieving information requires decrypting (i.e. Exposing) sensitive data.
- Performing the operations on the ciphertexts yields garbage upon decryption.
- ... Or doesn't it?

# An Unexpected Side Effect

- Fully homomorphic encryption scheme:  
$$\mathcal{E}_k(a \times b + c) = \mathcal{E}_k(a) \times \mathcal{E}_k(b) + \mathcal{E}_k(c).$$
- Bootstrappable: re-encrypt with a new key, without revealing either key.
- First “practical” scheme (Gentry 2009): ideal lattices.
- Complexity:  $O(n^6)$ ; now  $O(n^3)$ .
- Pure side effect of post-quantum scheme.

# Post-Quantum Cryptosystems: Advantages

- Many features of conventional systems are supported (some are even unique, e.g. fully homomorphic encryption).
- Efficient processing as compared to pre-quantum schemes, e.g.  $O(n \log n)$  instead of  $O(n^3)$ .
- Easy to implement, e.g. small integers.

# Post-Quantum Cryptosystems: Challenges

- Not every feature of conventional systems is known to be achievable with existing post-quantum proposals.
- Operational problems (key size, formal security analysis).
- Large-scale migration burden.

# Example

## ■ Digital signatures:

scheme	$ sk $	$ pk $	$ \sigma $
Bonsai	152 701	32 827 383	37 941
Ideal Bonsai	14 639	2 918 052	1 060 162
GPV	84 714	43 419	111
Ideal GPV	5 072	3 857	1 151
<b>CFS</b>	59	737	<b>0.022</b>
<b>QD-CFS</b>	5	174	<b>0.022</b>
Treeless	2	2	6
<b>GG</b>	<b>0.085</b>	<b>0.043</b>	15

Sizes in kB

Sources: Rückert & Schneider,  
PQCrypto'2010; B. et al., Inscrypt'2010

# Example

## ■ Encryption:

scheme	$ sk $	$ pk $	$ ct / pt $
LWE	34 019	17 435	79
Multibit LWE	71	1 366	~1
McEliece	4	192	1.3
Multibit Ring LWE	1	18	2
QD McEliece	0.7	4	2

## ■ See NTRU talk ☺

Sizes in kB

Sources: Rückert & Schneider,  
PQCrypto'2010; Misoczki & B. SAC'2009

# Summarizing

- PQC is a purely classical alternative to quantum cryptography.
- Post-quantum security assumptions mimic the *modus vivendi* of pre-quantum schemes.
- Several pros over traditional systems, cons being currently addressed.
- Popularity trend: lattices, codes, MQE.



Questions?

Thank You!