Daniele Micciancio (UCSD)

Homomorphic Encryption Workshop – March 2018
Security Panel

Historical Perspective

Lattice Cryptoanalysis: 1980-1995

1982: LLL Algorithm

- Polynomial running time
- Worst-case approximation factor exp(c*n)
- Performs much better in practice
- Often used as an "oracle" to find exact solutions

Pravailing attitude within cryptanalysts:

"Lattices should never be used for cryptography"

Turning point: 1996

1996: SIS worst-case average-case connection

- If lattice problems are hard at all, then we know how to used them for cryptography
- SIS: Short Integer Solution problem

1998: The Shortest Vector Problem is NP-hard

Applications

- One-way functions
- Collision resistant hashing

1996: NTRU Cryptosystem:

- Lattices cryptography can be efficient in practice

Bridging theory and practice

2002: Worst-case average-case connection for "cyclic" lattices / RingSIS

- Similar to those used by NTRU, but with security guarantees
- Quasilinear running time using FFT

Still ….

- Only simple applications (one-way functions)
- No serious cryptanalsys efforts

Effectiveness of theory

- Several versions of NTRU signatures proposed and broken
- NTRU encrypt resists, but poorly understood

Lattice cryptography: prime time

2004: LWE problem

Injective version of SIS. (2009: RingLWE – injective RingSIS)

Amazing number of (theoretical) applications

"10 years of lattice cryptography"

Public Key Encryption, ID-based encryption, ...,

Fully Homomorphic Encryption

Worst-case average-case reductions

+ Qualitative validation of cryptographic design

– Not very useful to assess security in practice

Security of lattice cryptography

How to test lattice assumptions? (2007: LLL+25)

1. Worst-case challenge: Cryptographers are charged with the task of finding the “hardest possible” challenge
2. Reverse challenge: cryptanalysts make worst-case claims, the challenge is to find lattices that falsify the claims
3. **Direct cryptanalysis:** Estimate concrete security of average case problems (Ring)SIS, (Ring)LWE.

Cryptanalsys

2008: Predicting Lattice Reduction

Exponential behavior of LLL observed “in practice”

Lattice cryptography is secure, let’s measure it!

Summary

Lattice Algorithms and Cryptanalysis

Active research area for over 30 years

Theoretical Foundation

We know what problems to focus on

Ring Lattices

Used and studied in cryptography for ~20 years

Security estimates

Much work in the last 10 years

Still active research area, but not major surprises expected

E.g., bit security of decision problems = $\log(T/\varepsilon^2)$ [Eurocrypt'18]

Table 1: dim=32768, log q = 478: bit security: 256 → 251