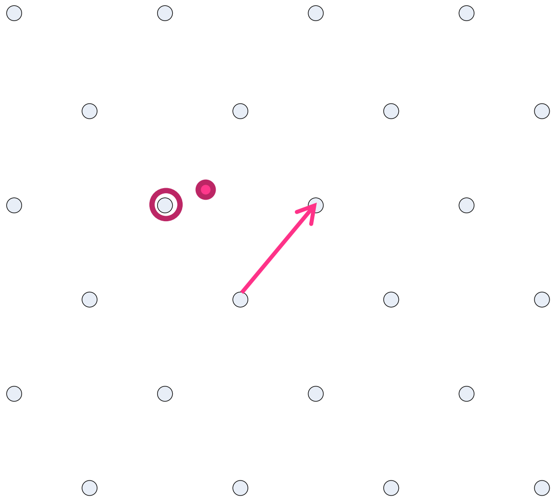
Lattice-based Threshold Cryptography

Rikke Bendlin and Ivan Damgård

Aarhus University

Lattice-based Cryptography

- Popular problems
  - Factoring
  - Discrete logarithms
- Lattice problems
  - SVP
  - CVP
  - approximation variants
- Learning With Errors (LWE)



Lattice-based Cryptography

- Learning With Errors in $\mathbf{Z}_q$

$$<\mathbf{s},\mathbf{a_1}> \approx_\chi b_1$$

$$<\mathbf{s},\mathbf{a_2}> \approx_\chi b_2$$

$$\vdots$$

Find s

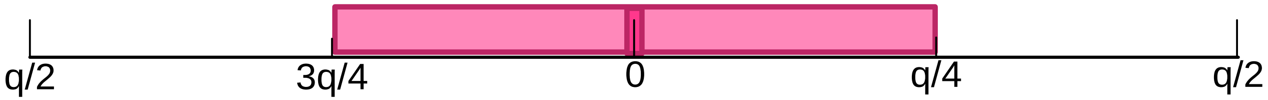
- Reductions to standard lattice problems
  - Quantumly in [Regev 05]
  - Classically in [Peikert et al. 08]

Cryptosystem

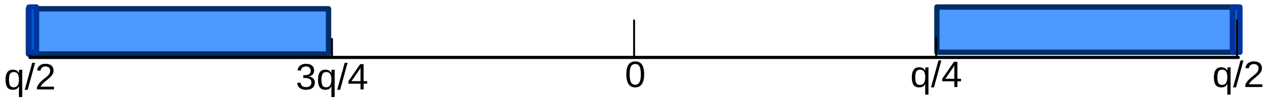
- Based on the cryptosystem in [Regev 05]
  - Security parameter n
  - q = $2^{O(n)}$
- Secret key: **s** (from LWE)
- Public key: linear equations with errors

Cryptosystem

- Encryption: Adding a random subset of the linear equations in the public key to get (**a**,b)
- Decryption: Calculate b - <**a**,**s**>
  - Result = 0

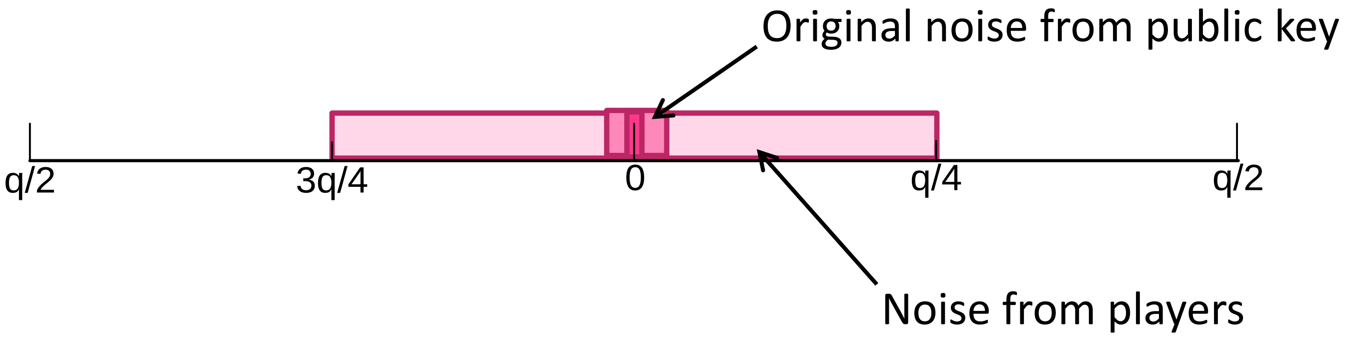


  - Result = 1



Threshold Cryptosystem

- u players
- Secret key: Each entry is secret shared among the players
- Decryption:
  - Each player can compute share of result locally, but adds noise to ensure security



Threshold Cryptosystem

- Pseudorandom secret sharing
  - players can non-interactively share a common value from some interval
  - no communication during decryption other than sending final shares for opening
- Easily made active secure
- Distributed key generation using non-interactive verifiable secret sharing

Upcoming Work

- Zero-knowledge proofs
- Multiparty Computation

Want to know more

Lattice-based Threshold Cryptography

Rikke Bendlin and Ivan Damgård

http://eprint.iacr.org/2009/391.pdf