Quantum Cryptography and Cryptanalysis - Status

5th International Conference on
Public Key Infrastructure and its Applications: PKIA 2024
IEEE CS&IAS Chapter Bangalore
05-06, September 2024

C.E.Veni Madhavan

Department of Computer Science and Automation
Indian Institute of Science, Bangalore
C.R.Rao Advanced Institute of Math., Stats., and Computer Science
Amrita Vishwa Vidyapeetham

6 September 2024

Quantum Cryptography and Cryptanalysis - Current Directions

Design, Analysis: Mathematics, Algorithms, Computations

1. Lattices
2. Codes
3. Curves
4. Equations
5. Congruences
6. Hash Chains

1. Lattices

Design

- CRYSTALS; pqNTRU; FALCON - modules over polynomial rings over finite fields, vector spaces and lattices; easy versus hard instances;
- other finite fields and algebraic structures, other quantum invulnerable trapdoors

Analysis

- approximations, average-cases: SVP, CVP, SIS
- enumeration, sieving, hybrid heuristics
- classical, quantum, hybrid attacks
- lattice problems, LWE problem, decoding problems, integer factoring, discrete lagarithm problems can be related

2. Codes

Design

- many codes (code zoo) - vector spaces, polynomial rings over finite fields, easy versus hard instances of encoding, decoding;
- QC-LDPC, QC-MDPC, BIKE, convolution, algebraic-geometry codes
- Reed-Muller, Reed-Solomon, Mattson-Solomon, Goppa, Gabidulin
- Hamming metric, rank metric
- other finite fields and algebraic structures, other quantum invulnerable trapdoors
- quantum error correcting codes (bit flips, phase flips), approximate QECC

Analysis

- decoding random codes : approximations, average-cases
- information set decoding, list decoding heuristics
- classical, quantum, hybrid attacks

3. Curves

Design

- elliptic curves over finite fields, isogenies, supersingular curves,
- hyperelliptic curves

Analysis

- isogeny cmputations, expander graphs, spectral properties
- index calculus, generic group BSGS
- classical, quantum, hybrid attacks

4. Equations, 5. Congruences

Design

- multivariate quadratic equations (RAINBOW), LWE congruences over finite fields

Analysis

- linearization; GE,Lanczos,Wiedemann methods; Grobner bases; SAT solvers
- classical, quantum, hybrid attacks

6. Hash Chains

Design

- forest of tweakable hash chains over integer rings

Analysis

- determining hash collisions; TMDTO attacks
- classical, quantum, hybrid attacks