Course Title: Quantum Information and Cryptography

1 Objective of the course

Objective of the course is to build quantum-preparedness for post quantum era. Due to Grover [1], Shor [2] and Simon [3] algorithms classical private and public key cryptographic security might be compromized totally or partially. By Post Quantum Cryptography, we generally mean the Public Key Cryptography which are resistant against quantum adversary, an adversary having unbounded power of computation. NIST has already started this effort [4]. Another avenue is Quantum Cryptography. In this direction, to provide the students an overview about this paradigm, we organize the syllabus as follows.

1. Introduction to Quantum Information
   (a) States, Operators, Measurements
   (b) Quantum Entanglement: Quantum Teleportation, Super-dense coding
   (c) Quantum gates and circuits
2. Quantum Algorithms: Deutsch-Jozsa, Simon, Grover, Shor, and their cryptanalytic implications
   (a) Implication of Grover's and Simon's algorithms towards classical symmetric key cryptosystems
   (b) Implication of Shor's algorithm towards factorization and Discrete Logarithm based classical public key cryptosystems
3. Quantum True Random Number Generators (QTRNG)
   (a) Detailed design and issues of quantumness
   (b) Commercial products and applications
4. Quantum key distribution (QKD)
   (a) BB84, Ekert, Semi-Quantum QKD protocols and their variations
   (b) Issues of Device Independence

(c) Commercial products

5. Other cryptologic issues, such as Quantum secret sharing and multiparty computation
6. Introductory topics in Post-Quantum Cryptography

2 Learning Outcome

The following are expected from the students after completion of the course.

- Basic understanding about Quantum Information and Computation.
- Students should write and run program(s) in IBM quantum computers.
- Students should understand how to implement Grover key recovery attack on classical symmetric ciphers.
- Getting an overall understanding about Quantum Key Distribution and Secret Sharing protocols.
- To obtain the flavour of quantum supremacy over classical computation.

References

[1] L. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of 28th Annual Symposium on the Theory of Computing (STOC)*, May 1996, pages 212–219. Available at `http://xxx.lanl.gov/abs/quant-ph/9605043`

[2] P. W. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Foundations of Computer Science (FOCS) 1994, page 124–134, IEEE Computer Society Press.

[3] D. R. Simon. On the power of quantum computation. SIAM journal on computing. 1997 Oct; 26(5): 1474-83.

[4] `https://csrc.nist.gov/projects/post-quantum-cryptography`

Quantum Information and Cryptography

- Syllabus
  1. Introduction to Quantum Information
     (a) States, Operators, Measurements
     (b) Quantum Entanglement: Quantum Teleportation, Super-dense coding
     (c) Quantum gates and circuits
  2. Quantum Algorithms: Deutsch-Jozsa, Simon, Grover, Shor, and their cryptanalytic implications
     (a) Implication of Grover's and Simon's algorithms towards classical symmetric key cryptosystems
     (b) Implication of Shor's algorithm towards factorization and Discrete Logarithm based classical public key cryptosystems
  3. Quantum True Random Number Generators (QTRNG)
     (a) Detailed design and issues of quantumness
     (b) Commercial products and applications
  4. Quantum key distribution (QKD)
     (a) BB84, Ekert, Semi-Quantum QKD protocols and their variations
     (b) Issues of Device Independence
     (c) Commercial products
  5. Other cryptologic issues, such as Quantum secret sharing and multiparty computation
  6. Introductory topics in Post-Quantum Cryptography
- Recommended Texts
  1. M. A. Nielsen and I. L. Chuang: Quantum Computation and Quantum Information, Cambridge University Press
  2. P. Kaye, R. Laflamme, and M. Mosca: An Introduction to Quantum Computing, Oxford University Press, New York
  3. Presskil Lecture notes: Available online: `http://www.theory.caltech.edu/~preskill/ph229/`
  4. N. David Mermin: Quantum Computer Science, Cambridge University Press
  5. D. Unruh: Quantum Cryptography, Available online: `https://courses.cs.ut.ee/all/MTAT.07.024/2017_fall/uploads/`
  6. NIST Post Quantum Cryptography, Available online: `https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions`