Instructions

Individual project. The goal is to go beyond what we can cover in class in two possible ways: 1) some of the results in class are given without careful discussion, and the literature may not be precise or complete (e.g., considered "folklore"). You can choose to work out the details and write up a self-contained note. It will benefit peer students as well as researchers. 2) explore recent developments and new topics not covered in class. This could end up in a survry report, or even better you might identify new research questions and make your contribution. In the latter case, you need to clearly formulate the problem, and demonstrate your approaches and partial results. You do not have to completely solve a problem (big congrats should you do!).

Specs

- **Proposal**: read the suggested project ideas and discuss with the instructors. Then submit a proposal of 1-2 pages consisting of 1) the topic, background, context, motivation; 2) brief summary of the relevant works and core papers to be studied; and 3) a goal you intend to achieve and a plan.
- **Oral presentation**: you will have a full lecture to present your project. You presentation should demonstrate both *breath* and *depth*: you should aim for a clear introdution of your topic with sufficient background and motivation that would **interest** the audience; and then you may choose to explain 1-2 techincal ideas in some detail. Board talk and slides are both accepted.
- **Final report**: in the end, you need to write up a report in the format of a research paper, which includes: 1) a short abstract; 2) an introduction that motivates the topic/problem and gives an overview of the entire paper; 3) details including proper preliminary materials (e.g., notations & defintions), explaning some main technical results; and finally 4) further discussion (e.g., open questions).
- **Report format**: single-column, single-space (between lines) format on letter-size paper. LaTeX and BibTeX are highly recommended.

Timeline

- **Week 6 & 7**: discussing and proposing project ideas.
- **Week 13-14**: in-class presentations.
- **December 7**: final report due.

Suggested Topics

Feel free to pursue a project not on this list. Good venues to look for inspirations: Crypto, Eurocrypt, TCC, Asiacrypt, Qcrypt PQCrypt, and more general Quantum and TCS conferences (e.g., STOC, FOCS, QIP).

More about Quantum Random Oracle and superposition attacks

- **Fijisaki-Okamoto** transformation. The state-of-art?
  - [JZC+18] *IND-CCA-secure Key Encapsulation Mechanism in the Quantum Random Oracle Model, Revisited* by Haodong Jiang and Zhenfeng Zhang and Long Chen and Hong Wang and Zhi Ma.
  - [Z18] *How to Record Quantum Queries, and Applications to Quantum Indifferentiability* by Mark Zhandry.
- **Security of other primitives against superposition attacks**
  - [Z13] *Quantum-Secure Message Authentication Codes* by Dan Boneh and Mark Zhandry.
  - [BZ13] *Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World* by Dan Boneh and Mark Zhandry.

Quantum proof techniques

- **Classical proof techniques for indistinguishability** Can we adapt them in the presence of quantum attacks?
  - (**H-coefficient**) [CS14] *Tight security bounds for key-alternating ciphers* by Shan Chen, John Steinberger.
  - (**Chi-squared**) [DHT17] *Information-theoretic Indistinguishability via the Chi-squared Method* by Wei Dai and Viet Tung Hoang and Stefano Tessaro.
- **(Cryptographic) adversarial method** Another central technique for proving quantum query lower bound. How to make it more applicable to cryptography?
  - [A00] *Quantum lower bounds by quantum arguments* by Andris Ambainis.
  - [BBH+17] *Provably secure key establishment against quantum adversaries* by Aleksandrs Belovs, Gilles Brassard, Peter Hoyer, Marc Kaplan, Sophie Laplante, Louis Salvail.

Quantum side information

- **Quantum rewinding**. Refine Watrous's rewinding lemma to be truly rewinding (i.e., resume to initial state), by some further observation on oblivious amplitute amplification.
  - [Watrous09] *Zero-knowledge against quantum attacks* by John Watrous.
  - [BCCKS14] *Exponential improvement in precision for simulating sparse Hamiltonians* Dominic W. Berry, Andrew M. Childs, Richard Cleve, Robin Kothari, Rolando D. Somma. (See the part on oblivious amplitute amplification.)
- **Proof of knowledge**
  - [Unruh12] *Quantum Proofs of Knowledge* by Dominique Unruh.
- **Quantum-safe randomness extractors** Quantum side information can break some classical construction of randomness extractors, a central primitive in algorithm design, cryptography and complexity theory. How to design extractors that are quantum-proof?
  - [DPVR12] *Trevisan's extractor in the presence of quantum side information* by Anindya De, Christopher Portmann, Thomas Vidick, Renato Renner.

Quantum algorithms and PQC candidates

- **Quantum attacks on t-wise indep. hash** We discussed in class some pairwise independent hash can be broken. How about t and how general is this?
  - [CvDHE16] *Optimal quantum algorithm for polynomial interpolation* by Andrew M. Childs, Wim van Dam, Shih-Han Hung, Igor E. Shparlinski.
- **PQC candidate problems and their hardness** There are a few popular proposals for building cryptography against quantum attacks. How hard are these problems? What are the best algorithms (classical or quantum) for solving these problems? The literature is enormous and the references given below are just some recent work to get you started.
  - **Lattice-based**. [Ducas18] *Advances on quantum cryptanalysis of ideal lattices* by Leo Ducas.
  - **Isogeny-based**. [GV17] *Computational problems in supersingular elliptic curve isogenies* by Steven D. Galbraith and Frederik Vercauteren.
  - **Code-based**. [Kir18] *Improved Quantum Information Set Decoding* by Elena Kirshanova.
  - **Multivariate-based**. [DP18] *Current State of Multivariate Cryptography* by Jintai Ding and Albrecht Petzoldt. (Available via TAMU library or download PDF here.)