Fine Grained Public Key Cryptography

Rio LaVigne and Andrea Lincoln

January 30, 2018

1 Introduction

[Story: fine grained crypto needs all this stuff.] xxx

Fine-grained complexity has helped explain the hardness of a wide variety of problems. The idea of fine-grained one way functions were introduced by Ball et.al. [BRSV17].

Fine-grained cryptography ideally would have all of the following objects listed bellow. Those in bold we have created. Those italicized have been solved previously.

- Plausibly average case hardness assumptions on which to base cryptographic constructions.
  - *Worst case to average case reductions to show hardness for problems.* [BRSV17]
  - Showing problems hard from satisfiability.
  - **Using plausible average case hypotheses.**
  - Assumptions that have a fine-grained implications for quantum computers as well.
- "Symmetric" Fine-grained Cryptography
  - **Fine-grained one way functions (FGOWFs)**
  - **FGOWFs with hardcore bits**
  - Fine-grained pseudo-random generators (FGPRGs)
- "Asymmetric" Fine-grained Cryptography
  - Fine-grained trap-door functions
  - **Fine-grained key transfer**
  - Fine-grained public key cryptography
  - Fine-grained identity based encryption
- Advanced constructions
  - Oblivious transfer
  - Homomorphic encryption

References

[BRSV17] Marshall Ball, Alon Rosen, Manuel Sabin, and Prashant Nalini Vasudevan. Average-case fine-grained hardness. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 483–496, 2017.