On the Power of Public-key Encryption in Secure Computation

Abstract

We show that there is a computational primitive which can be used (in a blackbox manner) to securely implement certain 3-party SFE tasks which do not have secure protocols otherwise, but is "useless" for *any* finite, deterministic 2-party SFE: that is, the only finite, deterministic 2-party SFE that have a secure protocol using this primitive are those which have a secure protocol unconditionally.

This leads to a qualitative separation between computational complexity *assumptions* inherent to 2-party secure function evaluation (SFE) and those inherent to 3-party SFE. More precisely, consider the universe of assumptions of the form "f has a semi-honest secure protocol" (in the PPT setting, over a public discussion model); we show that this universe of assumptions corresponding to 3-party functions is strictly larger than that corresponding to 2-party functions (when the elements of this universe are considered distinct unless they are black-box reducible to each other). This answers an open question of Maji et al. (ITCS'10).

Technically, we show that there is an oracle with respect to which public-key encryption (PKE) exists, but is useless for all semi-honest 2-party finite, deterministic SFE tasks. This subsumes a result of Gertner et al. (FOCS'00) which showed that PKE is useless for Oblivious Transfer (and hence, for any complete SFE task). This builds on a recent result by the authors [MMP12] which showed that random oracles (with respect to which PKE does not exist either) are useless for such 2-party SFE. As in [MMP12], this extends to security against active adversaries (in which case PKE is only as useful as being given access to the commitment functionality).

Apart from our main results, this work significantly advances (and conceptually simplifies) several state-of-the-art techniques in the field of black-box separations:

1. We introduce a general *common-information learning* algorithm (CIL) which extends the "eavesdroppers" in prior work [IR89, BM09, HOZ13], to protocols whose messages can depend on information gathered by the CIL so far.

2. With the help of this CIL, we show that in a secure 2-party protocol using an idealized PKE oracle, surprisingly, decryption queries are useless.

3. The idealized PKE oracle with its decryption facility removed can be modeled as an *image-testable random-oracle*. We extend the analysis approaches of prior work on random oracles [IR89, BM09, DLMM11, MMP12, HOZ13] to apply to this class of oracles; this shows that these oracles are useless for semi-honest 2-party SFE (as well as for key-agreement).

Keywords: 2-party Deterministic Secure Function Evaluation, Key-agreement Protocols, Public-key Encryption, Black-box Separation, Common Information Learner

(Joint work with Mohammad Mahmoody and Manoj Prabhakaran.)

References

[BM09] Boaz Barak and Mohammad Mahmoody. Merkle puzzles are optimal - an $O(n^2)$-query attack on any key exchange from a random oracle. In Shai Halevi, editor, *CRYPTO*, volume 5677 of *Lecture Notes in Computer Science*, pages 374–390. Springer, 2009. 1

[DLMM11] Dana Dachman-Soled, Yehuda Lindell, Mohammad Mahmoody, and Tal Malkin. On black-box complexity of optimally-fair coin-tossing. In *Theory of Cryptography Conference - TCC 2011*, 2011. 1

[HOZ13] Iftach Haitner, Eran Omri, and Hila Zarosim. Limits on the usefulness of random oracles. *Theory of Cryptography Conference (TCC, to appear)*, 2013. 1

[IR89] Russell Impagliazzo and Steven Rudich. Limits on the provable consequences of one-way permutations. In David S. Johnson, editor, *STOC*, pages 44–61. ACM, 1989. 1

[MMP12] Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran. Limits of random oracles in secure computation. *CoRR*, abs/1205.3554, 2012. 1