Black-Box Separations for Differentially Private Protocols

Abstract

We study the maximal achievable accuracy of distributed differentially private protocols for a large natural class of boolean functions, in the computational setting.

In the information theoretic model, McGregor et al. [FOCS 2010] and Goyal et al. [CRYPTO 2013] have demonstrated several functionalities whose differentially private computation results in much lower accuracies in the distributed setting, as compared to the client-server setting.

We explore lower bounds on the computational assumptions under which this particular accuracy gap can possibly be reduced for general two-party boolean output functions. In the distributed setting, it is possible to achieve optimal accuracy, i.e. the maximal achievable accuracy in the client-server setting, for any function, if a semi-honest secure protocol for oblivious transfer exists. However, we show the following strong impossibility results for the distributed setting:

- For *any* boolean function and fixed level of privacy, the maximal achievable accuracy of any (fully) black-box construction based on existence of key-agreement protocols is at least a constant smaller than optimal achievable accuracy. Since key-agreement protocols imply the existence of one-way functions, this separation also extends to one-way functions.
- Our results are tight for the AND and XOR functions. For AND, there exists an accuracy threshold such that any accuracy up to the threshold can be information theoretically achieved; while no (fully) black-box construction based on existence of key-agreement can achieve accuracy beyond this threshold. An analogous statement is also true for XOR (albeit with a different accuracy threshold).

Our results build on recent developments in black-box separation techniques for functions with private input [BM09, HOZ13, MMP14a, MMP14b]; and consequently translate information theoretic impossibilities into black-box separation results.

Keywords: Differentially Private Protocols, Computational Complexity, Random Oracle, Key-agreement Protocols, Black-box Separation.

(Joint work with Dakshita Khurana and Amit Sahai.)

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

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

[MMP14a] Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran. Limits of random oracles in secure computation. In *ITCS*, 2014. 1

[MMP14b] Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran. On the power of public-key encryption in secure computation. In *TCC*, 2014. 1