Cryptographic Hardness of Random Local Functions – Survey

Benny Applebaum *

School of Electrical Engineering, Tel-Aviv University
bennyap@post.tau.ac.il

Constant parallel-time cryptography allows performing complex cryptographic tasks at an ultimate level of parallelism, namely, by local functions that each of their output bits depend on a constant number of input bits. The feasibility of such highly efficient cryptographic constructions was widely studied in the last decade via two main research threads.

The first is an encoding-based approach, developed in [1, 2], in which standard cryptographic computations are transformed into local computations via the use of special encoding schemes called *randomized encoding* of functions. The second approach, initiated by Goldreich [3], is more direct and it conjectures that almost all non-trivial local functions have some cryptographic properties.

In this survey we focus on the latter approach. We consider *random local functions* in which each output bit is computed by applying some fixed d-local predicate P to a randomly chosen d-size subset of the input bits. Formally, this can be viewed as selecting a random member from a collection $\mathcal{F}_{P,n,m}$ of d-local functions where each member $f_{G,P} : \{0,1\}^n \to \{0,1\}^m$ is specified by a d-uniform hypergraph G with n nodes and m hyperedges, and the i-th output of $f_{G,P}$ is computed by applying the predicate P to the d inputs that are indexed by the i-th hyperedge.

In this talk, we will investigate the cryptographic hardness of random local functions. In particular, we will survey known attacks and hardness results, discuss different flavors of hardness (one-wayness, pseudorandomness, collision resistance, public-key encryption), and mention applications to other problems in cryptography and computational complexity. We also present some open questions with the hope to develop a systematic study of the cryptographic hardness of local functions.

References

1. B. Applebaum, Y. Ishai, and E. Kushilevitz, *Cryptography in* NC^0, SIAM Journal on Computing, **36(4)** (2006), 845–888.
2. B. Applebaum, Y. Ishai, and E. Kushilevitz, *Computationally private randomizing polynomials and their applications*, Journal of Computational Complexity, **15(2)** (2006), 115–162.
3. O. Goldreich, *Candidate one-way functions based on expander graphs*, Electronic Colloquium on Computational Complexity (ECCC), **7(090)** (2000).

* Supported by Alon Fellowship, ISF grant 1155/11, Israel Ministry of Science and Technology (grant 3-9094), and GIF grant 1152/2011.