Towards Higher-Order Cryptography

Raphaëlle Crubillé Ugo Dal Lago

1 Modern Cryptography and Higher-Order Computation

Modern cryptography [4] is at the heart of most privacy and authentication methodologies, and is based around notions like pseudorandomness and computational indistinguishability. Its object of study are functions between binary strings which can be computed by (possibly randomized) algorithms working in polynomial time. As such, it is essentially a theory of *first-order* functions. In an ongoing study, the authors are investigating whether the aforementioned concepts can have an *higher-order* counterpart, and, in case the answer is positive, *which* form could it take. If one looks, e.g., at how a pseudorandom function [4] *of rank 2* could look like, he or she would immediately realizes that for this notion *not* to be vacuous, severe limitations must be placed at the way the function and the adversary interact, thus influencing the definition.

2 Probabilistic Game Semantics and Security Proofs

In [1], Danos and Harmer adapted the setting of game semantics to probabilistic games. On the other hand, Ferée noticed [2] that game semantics offers the right playground when talking about complexity of higher-order programs. Finally, it is well known that Bounded Linear Logic [3] is a powerful, modular account of polynomial time computation. Our work show how these three ingredients, together, provide what is needed to head towards higher-order cryptography.

We consider two models. Our first model is one where we consider polytime memory-free agents with access to a state, from which they can read and write, and that can decide probabilistically of their next move. In our second model, agents are deterministic, stateless, and not memory-free, but can call a probabilistic oracle. We will show these two models to be equivalent under some assumptions, and we will illustrate each of them by expressing in these frameworks some well known (and basic) security proofs.

References

[1] V. Danos and R. Harmer. Probabilistic game semantics. *ACM Trans. Comput. Log.*, 3(3):359–382, 2002.

[2] H. Férée. Game semantics approach to higher-order complexity. *J. Comput. Syst. Sci.*, 87:1–15, 2017.

[3] J. Girard, A. Scedrov, and P. J. Scott. Bounded linear logic: A modular approach to polynomial-time computability. *Theor. Comput. Sci.*, 97(1):1–66, 1992.

[4] J. Katz and Y. Lindell. *Introduction to Modern Cryptography.* Chapman & Hall/CRC, 2007.