Automated Proof for Formal Indistinguishability and Its Applications (work in progress)

Long Ngo, Colin Boyd , and Juan González Nieto

Information Security Institute

Queensland University of Technology

GPO Box 2434, Brisbane QLD 4001, Australia

Bana *et al.* proposed the relation *formal indistinguishability* (FIR), i.e. an equivalence between two terms built from an abstract algebra [BMS07]. Later Ene *et al.* extended it to cover active adversaries and random oracles [ELN10]. This notion enables a framework to verify computational indistinguishability while still offering the simplicity and formality of symbolic methods.

We are in the process of making an automated tool for checking FIR between two terms. First, we extend the work by Ene *et al.* [ELN10] further, by covering ordered sorts and simplifying the way to cope with random oracles. Second, we investigate the possibility of combining algebras together, since it makes the tool scalable and able to cover a wide class of cryptographic schemes. Specifically, we show that the combined algebra is still computationally sound, as long as each algebra is sound. Third, we design some proving strategies and implement the tool. Basically, the strategies allow us to find a sequence of intermediate terms, which are formally indistinguishable, between two given terms. FIR between the two given terms is then guaranteed by the transitivity of FIR. Finally, we show applications of the work, e.g. on key exchanges and encryption schemes. In the future, the tool should be extended easily to cover many schemes.

This work continues previous research of ours on use of compilers to aid in automated proofs for key exchange [NBN10, NBN11].

References

[BMS07] G. Bana, P. Mohassel, and T. Stegers. Computational soundness of formal indistinguishability and static equivalence. *Advances in Computer Science-ASIAN 2006. Secure Software and Related Issues*, pages 182–196, 2007.

[ELN10] C. Ene, Y. Lakhnech, and V. Ngo. Formal indistinguishability extended to the random oracle model. *Computer Security–ESORICS 2009*, pages 555–570, 2010.

[NBN10] L. Ngo, C. Boyd, and J. Nieto. Automating computational proofs for public-key-based key exchange. *Provable Security*, pages 53–69, 2010.

[NBN11] L. Ngo, C. Boyd, and J. Nieto. Automated proofs for Diffie–Hellman–based key exchanges. In *Proceedings of the 24th IEEE Computer Security Foundations Symposium*, June 2011. To appear.