Karlsruhe Institute of Technology

Institut für Theoretische Informatik
Lehrstuhl Prof. Dr. J. Müller-Quade
crypto.iti.kit.edu

Verifiable random oracles

Master's Thesis

The random oracle model (ROM) is a widely used in heuristic in practice. But replacing a random oracle with a hash function does in general not preserve the security, hence the heuristic is flawed. Implementing the ROM via trusted party is possible, but makes protocols **interactive**.

This thesis considers a new model, the VROM. **Verifiable random oracles** extends random oracles by also providing a "proof of correct evaluation". That is, VRO consists of two algorithms:

- $\mathsf{VRO.Hash}(m) = (h, \pi)$, where h is the hash and π is the "proof".
- $\mathsf{VRO.VfyHash}(m, h, \pi)$ checks whether h is the correct hash.

Given a random oracle RO, one can instantiate a VRO by setting $\pi = \bot$ and $\mathsf{VfyHash}(m, h, \pi) = [\mathsf{RO}(m) == h]$. Unlike the ROM, the VROM potentially allows "semi-interactive" protocols: Parties computing $\mathsf{VRO.Hash}$ must query VRO (interactively), but verifiying hashes is possible non-interactively.

Scope of the work

(1) A first **modeling** of the VROM as an "ideal functionality" in a suitable framework (e.g. real-ideal, UC, or CC) and a simple implementation.
(2) Easy(?) applications of VROM: FDH-signature schemes, NIZK via from Σ-protocols via Fiat–Shamir, NIZK-PoK via Fischlin's transformation.[Dam10; Fis05]
(3) Improved implementations. Here, there several possible choices.

Requirements

Following prior knowledge is useful (or must be acquired while working on) the master's thesis.

- Familiarity with advanced cryptography (e.g. suitable lectures or seminars).
- Knowledge in multi-party computation (MPC) and universal composability (UC) or constructive cryptography (CC), especially the real-ideal model for security definitions. See [Lin16] for a short introduction.
- Probability theory/analysis of algorithms (especially the runtime analysis of rewinding-based security reductions is non-trivial).

Contact

In case of interest or for further information, please contact Michael Klooß, michael.klooss@kit.edu.

Literatur

[Dam10] Ivan Damgård. *On Σ-protocols*. 2010. URL: https://cs.au.dk/~ivan/Sigma.pdf.

[Fis05] Marc Fischlin. "Communication-Efficient Non-interactive Proofs of Knowledge with Online Extractors". In: *CRYPTO*. Bd. 3621. Lecture Notes in Computer Science. Springer, 2005, S. 152–168.

[Lin16] Yehuda Lindell. "How To Simulate It - A Tutorial on the Simulation Proof Technique". In: *IACR Cryptol. ePrint Arch.* 2016 (2016), S. 46. URL: http://eprint.iacr.org/2016/046.