Post-quantum security of cryptographic transformations in the random oracle model

Huang, Y.

Stellingen

Behorende bij het proefschrift *"Post-Quantum Security of Cryptographic Transformations in the Random Oracle Model"*

1. Provable security ensures that breaking the considered scheme is at least as difficult as solving a well-studied hard computational problem. However, this guarantee stands and falls with the correctness of the proof. Fiat-Shamir with Aborts (FSwA) — an important design principle for digital signature schemes — was analyzed and "proven" secure in different forms, but prior to our works on the topic, all the claimed proofs suffered from the same subtle flaw. (Chapter 3)

2. Contrary to the belief that the non-resignability (NR) of the BUFF transformation is well-established, it is actully not. Whether NR is achieved by BUFF, or achievable at all, depends on subtle details of its formal definition. (Chapter 4)

3. It is commonly understood that recovering a string x from its hash value $H(x)$ is hard. However, the situation becomes tricky when the target preimage x is chosen dependent on the hash function. Our result (stated below) formally addresses this in the random oracle model.

   Let $\mathcal{A}$ be a query-bounded algorithm given oracle access to a random function H, drawn uniformly with a given domain and co-domain; let x and z be random variables, arbitrarily correlated to each other and H, such that $\mathsf{H}_\infty(x \mid H, z)$ is high. Then the probability that $\mathcal{A}^H(H(x), z) = x$ is small. (Theorem 4.22)

4. Let $\mathcal{A}$ be an oracle algorithm making at most q_1 and q_2 queries to (stateless) oracles O_1 and O_2, respectively. Then, by introducing dummy queries, one easily obtains a functionally equivalent oracle algorithm $\mathcal{B}$ that makes at most $q_1 + q_2$ queries to O_1 and to O_2, such that the choice of which oracle to query at each point in time is pre-determined, i.e. independent of previous query responses. Less obviously, there exists such an oracle algorithm $\mathcal{B}$ that, instead, makes at most $2q_1$ queries to O_1 and $2q_2$ queries to O_2. This provides an improvement when, say, $q_1 \ll q_2$ and the queries to O_1 are more "costly." (Chapter 5)

---

5. In the design of post-quantum cryptographic schemes, replacing computational hard problems (like factoring) with quantum hard problems, while necessary, is not sufficient to achieve security against quantum attacks.

6. Despite the well-known fact that a (seedless) deterministic procedure cannot act as a randomness extractor for general min-entropy sources *in the plain model*, there is still formal justification *in the random oracle model* for the common practice of using a fixed cryptographic hash function (like SHA2 or SHA3) to extract randomness from arbitrary high min-entropy sources.

7. For an (ordinary) algorithm $\mathcal{A}$, there is standard notation to refer to $\mathcal{A}$'s output on input x, namely $\mathcal{A}(x)$. The situation is rather unsatisfactory when it comes to *interactive* algorithms, which interact with one another in order to produce their respective outputs. In this case, there is no commonly accepted notation for the joint output, or the individual outputs, or the transcript of messages exchanged.

8. Let ζ be a primitive 2^{k+1}th root of unity, and $\mathbf{B}$ be a 2×2 invertible matrix over $\mathbb{Q}(\zeta)$, which defines a ($\mathbb{Q}$-linear) norm $\|v\|_{\mathbf{A}} := \sqrt{\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(v^* \mathbf{A} v\right)}$ for $\mathbf{A} := \mathbf{B}^* \mathbf{B}$. Then, given $\mathbf{A}$, when elements in $\mathbb{Q}(\zeta)$ are represented as $\mathbb{Q}$-linear combinations of $\{\zeta, \ldots, \zeta^{2^k}\}$, there is an efficiently computable function ϕ such that for every $v \in \mathbb{Q}(\zeta) \setminus \{0\}^2$, we have $\|\phi(v)\|_{\mathbf{A}} = \|v\|_{\mathbf{A}}$ and $\phi(v) \notin \{\zeta v, \ldots, \zeta^{2^{k+1}} v\}$. This shows that the original assumption used to prove the security of HAWK is false.

9. For any function $f : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ with Fourier transform $\hat{f}$, the Fourier transform of $g(x, y) := f(x + y, y)$ equals $\hat{g}(x, y) = \hat{f}(x, y - x)$. This elementary result from Fourier analysis lies at the core of the compressed-oracle technique, which has had a major impact on proving security in the quantum random oracle model.

---

*

---

10. Introducing client-side surveillance in the context of private communication technology would undermine the trust and security of our modern cryptographic infrastructure.

Yu-Hsuan Huang
Leiden, April 1st, 2026