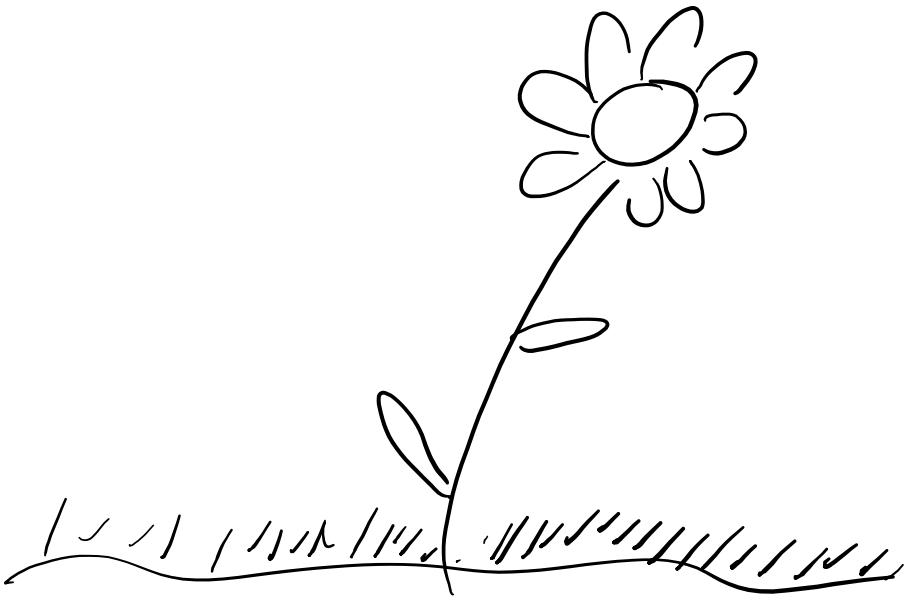

Quantum Random Oracles

- Idealization of hash
- Hash function modeled as random function
- RO heuristic: If proto is secure with random fun, then proto is secure using real hash
- Unsound in general, but good in practice

Formally: RO is a randomly chosen function H.
All algorithms (incl. adv) have oracle access to H.

Example: Full Domain Hash Signatures
Assume: trapdoor OWP f

Example: full-domain hash

Assume: trapdoor OWP f

To sign m: $Sig(m) = f^{-1}(H(m))$

$Verify(\sigma, m)$: $f(\sigma) \stackrel{?}{=} H(m)$

Security proof (unforgeability)

- $A^{Sig, H}$ creates forgery (σ, m)
- Want to translate A into inverter B for f

Algo B

- Input: $f(x)$ for unknown x
- Runs A, provides simulated $\widetilde{Sig}$, $\widetilde{H}$

lazy sampling:

$\widetilde{H}(y)$: - Pick r_y, return $\widetilde{H}(y) := f(r_y)$
- Except on one query: $\widetilde{H}(y_0) := f(x)$

$\widetilde{Sig}(m)$: Return $r_m = f^{-1}(\widetilde{H}(m))$

Indistinguishable!

If A produces forgery: (m, σ).

with some prob: $m = y_0$

$\Rightarrow f(\sigma) = H(m) = H(y_0) = f(x)$ ↯

Quantum RO

1. try The RO is random func.
   A has access to class. oracle H

   $\Rightarrow$ Bad idea. Need superpos. access to H

   (eg. Fischlin's scheme)

2. try The RO is random fun H.
   ... access to oracle

2. try The RO is random.

A has access to oracle

$|x, y\rangle \mapsto |x, y \oplus H(x)\rangle$

Observation: Optimality of Grover $\Rightarrow$ H is OWF

But can we prove anything else?

"Lazy sampling" does not work:

A can query $\sum_x |x\rangle|0\rangle \mapsto \sum_x |x\rangle|H(x)\rangle$

Lost techniques: (2011)

- Adaptive programming (slightly recovered)
- Extracting (only extreme cases)
- Efficient simulation of RO (yes)
- Rewinding with reprogramming (?) (Fiat Shamir)

FDH in Q-ROM

Classical

- Runs A, provides sim

$\tilde{H}(y)$: - Pick r_y, return $\tilde{H}(y) := f(r_y)$

- Except on one query: $\tilde{H}(y_0) := f(x)$

$\sim$

Quantum:

- Pick random fun T

$\tilde{H}(y) := f(T(y))$

Given circuit for T, can build $\tilde{H}$

Needs the "challenge output"

Given circuit for T, can build circuit for $\widetilde{H}$ | "challenge ourp

- Pick a set $S \subseteq \mathrm{dom}\,\widetilde{H}$, density λ
- $\widetilde{H}(y) := \begin{cases} f(T(y)) & \text{if } y \notin S \\ f(x) & \text{if } y \in S \end{cases}$

Zhandry $\Rightarrow$ A random function, with an output fixed in λ-many places, looks somewhat random

---

Another example:

$E(pk, m) := (f_{pk}(r),\ H(r) \oplus m)$

Oneway-To-Hiding Lemma:

(a) $r \to B^H \leftarrow H(r)$ $\quad \overset{\varepsilon}{\simeq}$ (b) $r, y \to B^H$

$\varepsilon \sim R$[when measuring H-query in (b) at random point: get r]

$B^H(r, y)$ runs A with $E = (f_{pk}(r),\ y \oplus m)$ $\quad \to$ no attack

$\Big\}\Big\}\ \varepsilon$

$B^H(r, H(x))$ runs A with $E = (f_{pk}(r),\ H(r) \oplus m)$ $\quad \to$ orig setting

$\varepsilon \sim R$[get r when running A with $E = (f_{pk}(r),\ y \oplus m)$]

= negl. because of OWF

=> no attack in orig. setting.

[Note: No claim at completeness is made. This is a quick collection of literature that comes to my mind.]

Literature for rewinding lecture

Dominique Unruh, CROSSING winter school 2016

The rewinding technique that can be used for quantum zero-knowledge was presented in [Wat09]. See also [Unr12] for a more precise and general formulation of the zero-knowledge properties that are needed (section "zero knowledge', only in the full version).

For a different quantum rewinding technique, see [Unr12]. That one is used in cases where one needs to extract several values from the adversary by running it several times and measuring some value in each run. (It is incomparable with the other technique.)

Impossibility results for rewinding (such as the fact that the classical commitment definition is not suitable for the quantum setting) were given in [ARU14]. Some more impossibilities relating to commitments are given in [Unr16].

Rewinding in the style of [Unr12], but in the presence of computationally-binding commitments is studied in [Unr16]. (One needs a way to get around the fact that classical commitment definitions are not good for the quantum case.)

Literature for random oracle lecture

The quantum random oracle was first explicitly studied in [BDF+11] where they argued that the quantum random oracle needs to be queried in superposition (and showed the security of various signature and encryption schemes).

[Zha12b] analyses Full Domain Hash and for this purpose introduces the technique of replacing a fraction of the random oracle values by the same value ("semi-constant distributions"). A result that might be more powerful than the semi-constant distributions might be the "small-range distributions" [Zha12a] basically says that we only use a small number of values in the whole random oracle.

The one-way-to-hiding lemma was shown in [Unr15b] (but implicitly present in a special case already in [BDF+11]). It was generalized to allow different degrees of adaptive programming in [Unr14, Unr15a].

The fact that the random oracle is a one-way function is well-known, I don't know an original reference. Collision resistance of the random oracle is shown in [Zha15].

It is shown in [ARU14] that the Fiat-Shamir transform [FS87] and Fischlin's proofs with online extractors [Fis05] are not secure in general (w.r.t. to specific oracles in addition to the random oracle). (But it is open whether those schemes are secure using slightly stronger assumptions.) The original classical proof of security from [Fis05] goes through easily using a classical random oracle but a quantum adversary (warning: I have not checked this claim carefully).

Extraction from queries in the quantum random oracle model is used in [Unr15a] for non-interactive ZK proofs and [TU15] for the Fujisaki-Okamoto transform and OAEP.

References

[ARU14] Andris Ambainis, Ansis Rosmanis, and Dominique Unruh. Quantum attacks on classical proof systems (the hardness of quantum rewinding). In *FOCS 2014*, pages 474–483. IEEE, 2014. Preprint on IACR ePrint 2014/296.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In *Asiacrypt 2011*, pages 41–69, Berlin, Heidelberg, 2011. Springer-Verlag.

[Fis05] Marc Fischlin. Communication-efficient non-interactive proofs of knowledge with online extractors. In *Crypto 2005*, volume 3621 of *LNCS*, pages 152–168. Springer, 2005.

[FS87] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *CRYPTO 86*, volume 263 of *LNCS*, pages 186–194. Springer, 1987.

[TU15] Ehsan Ebrahimi Targhi and Dominique Unruh. Quantum security of the fujisaki-okamoto and oaep transforms, 2015. Preprint on IACR ePrint 2015/1210.

[Unr12] Dominique Unruh. Quantum proofs of knowledge. In *Eurocrypt 2012*, volume 7237 of *LNCS*, pages 135–152. Springer, April 2012. Preprint on IACR ePrint 2010/212.

[Unr14] Dominique Unruh. Quantum position verification in the random oracle model. In *Crypto 2014*, volume 8617 of *LNCS*, pages 1–18. Springer, 2014.

[Unr15a] Dominique Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In *Eurocrypt 2015*, volume 9057, pages 755–784, 2015. Preprint on IACR ePrint 2014/587.

[Unr15b] Dominique Unruh. Revocable quantum timed-release encryption. *Journal of the ACM*, 62(6):49:1–76, 2015. Preprint on IACR ePrint 2013/606.

[Unr16] Dominique Unruh. Computationally binding quantum commitments. In *Eurocrypt 2016*, 2016. To appear. Preprint on IACR ePrint 2015/361.

[Wat09] John Watrous. Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009. Online available at `https://cs.uwaterloo.ca/~watrous/Papers/ZeroKnowledgeAgainstQuantum.pdf`.

[Zha12a] Mark Zhandry. How to construct quantum random functions. In *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012*, pages 679–687. IEEE Computer Society, 2012.

[Zha12b] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In *Crypto 2012*, volume 7417 of *LNCS*, pages 758–775. Springer, 2012. Long version on IACR ePrint 2012/076.

[Zha15] Mark Zhandry. A note on the quantum collision and set equality problems. *Quantum Information & Computation*, 15(7&8):557–567, 2015.