

Random Oracles in a Quantum World



TECHNISCHE
UNIVERSITÄT
DARMSTADT



Cryptoplexity

Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

ISG Research Seminars 2011/2012

Özgür Dagdelen, Marc Fischlin (TU Darmstadt)

Dan Boneh, Mark Zhandry (Stanford University)

Anja Lehmann (IBM Zurich)

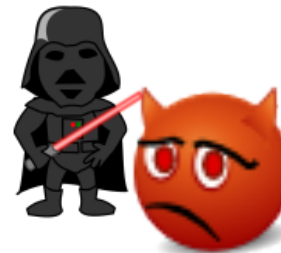
Christian Schaffner (CWI)



Cryptography in Real World



(All) Cryptosystems based on Factorization and Discrete Logarithm Problem are **easy** against classical computers

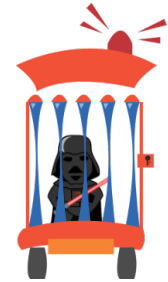


Post Quantum Cryptography

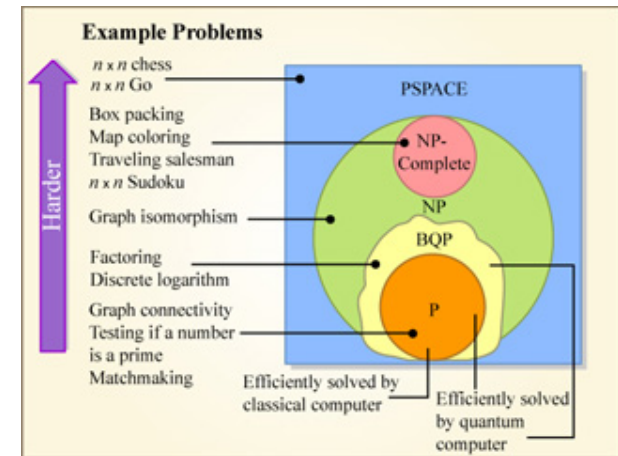


Not all (number-theoretic) problems are *easy* for quantum computers

- *Hash-based Cryptography* (e.g. Merkle's hash-trees signatures)
- *Code-based Cryptography* (e.g. McEliece, Niederreiter)
- *Lattice-based Cryptography* (e.g. NTRU)
- *Multi-variate-quadratic-equations Cryptography*

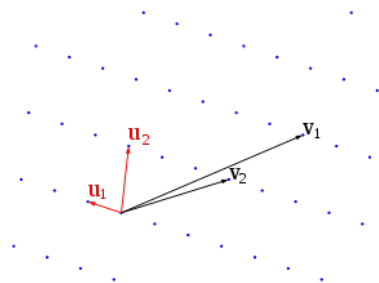


Cryptographic systems that run on conventional computers, are secure against attacks with conventional computers, and remain secure under attacks with quantum computers are called **post-quantum cryptosystems**.



Source: Quantum Complexity Theory, Lecture Notes Fall 2010

Quantum-Resistant Primitives ... with RO?



quantum-resistant
primitive / protocol

+



random oracle

=



quantum adversary

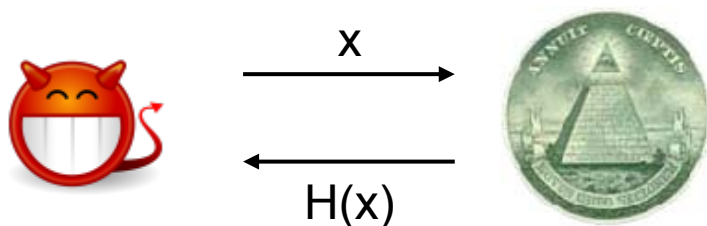
???

Examples:

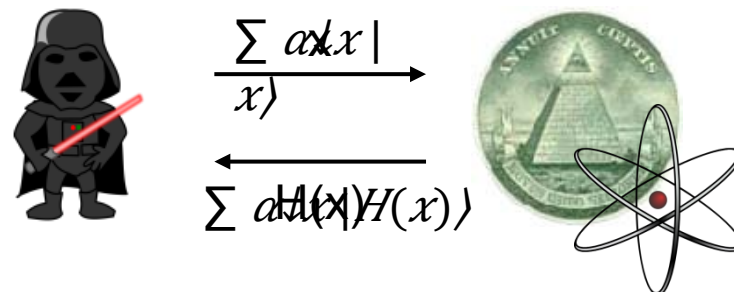
- Signatures [GPV08,GKV10,BF11]
- Encryptions [GPV08]
- Identification Schemes [CLRS10]

Quantum-Accessible Random Oracles

Classical



Quantum



Idea:
Instantiate Random Oracle
by “strong implementation”

minimal requirement:
quantum adversary may query RO
about quantum states

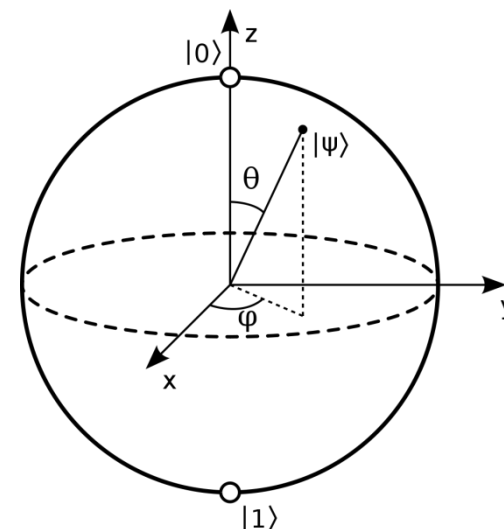
Outline

(1) Introduction to Quantum Theory

(2) Separation Result

(3) Positive Examples

(4) Open Problems



Introduction to Quantum Theory

Transmission of Entropie

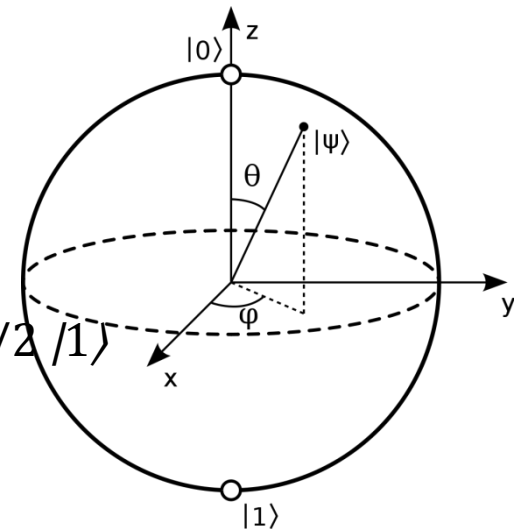
Today:

Qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ classical channel

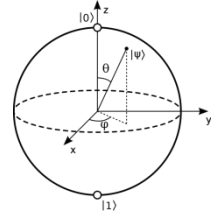
$\alpha, \beta \in \mathbb{C}$ are probability amplitudes

- i.e., $|\alpha|^2 + |\beta|^2 = 1$

alternative: $|\psi\rangle = \sin(\theta/2)e^{-i\phi/2}|0\rangle + \cos(\theta/2)e^{i\phi/2}|1\rangle$



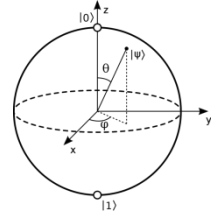
Quantum Computations



Quantum System A

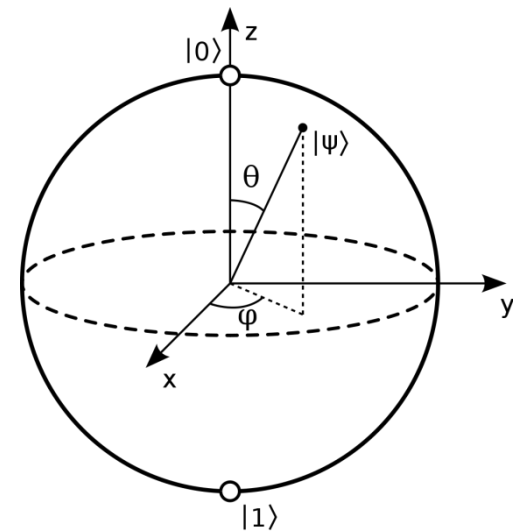
- complex Hilbert space H_A with inner product $\langle \cdot | \cdot \rangle$
- quantum state $|\varphi\rangle \in H_A$ with $\langle \varphi | \varphi \rangle = 1$
- joint quantum system $H_A \otimes H_B$
- $|\varphi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$ with $\sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1$

Quantum Computations

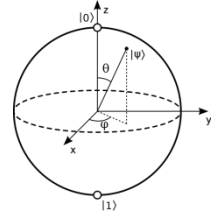


Transformations

- only unitary transformations U
 - $U^\dagger U = I_n$
 - $\det(U) = \pm 1$
- physically seen:
only **rotations** are allowed



Quantum Computations



Measurements $M = \{M_i\}$

- Q-system collapses to classical state
- positive semi-definite operator M_i s.t. $\sum_i M_i = I_n$
- outcome i with prob $p_i = \langle \varphi | M_i | \varphi \rangle$
- partial measurements possible

Toy Example

$$|\psi_{11}\rangle = \alpha_{11}|0\rangle + \beta_{11}|1\rangle$$

$$|\psi_{12}\rangle = \alpha_{12}|0\rangle + \beta_{12}|1\rangle$$

joint

$$|\psi_{11}, \psi_{12}\rangle = \alpha_{11}\alpha_{12}|00\rangle + \alpha_{11}\beta_{12}|01\rangle + \beta_{11}\alpha_{12}|10\rangle + \beta_{11}\beta_{12}|11\rangle$$

measure first qubit

$$|\psi\rangle = \frac{\alpha_{11}\alpha_{12}}{\sqrt{|\alpha_{11}\alpha_{12}|^2 + |\alpha_{11}\beta_{12}|^2}}|\tau_2\rangle|0\rangle + \frac{\alpha_{11}\beta_{12}}{\sqrt{|\alpha_{11}\alpha_{12}|^2 + |\alpha_{11}\beta_{12}|^2}}|\tau_2\rangle|1\rangle$$

result 0

Output:

- 0 with prob. $\frac{|\alpha_{11}\alpha_{12}|^2}{|\alpha_{11}\alpha_{12}|^2 + |\alpha_{11}\beta_{12}|^2}$
- 1 with prob. $\frac{|\alpha_{11}\beta_{12}|^2}{|\alpha_{11}\alpha_{12}|^2 + |\alpha_{11}\beta_{12}|^2}$

Power of Quantum Computing

$$|x, y\rangle \xrightarrow{O} |x, y \oplus \uparrow_{\#} O(x)\rangle$$

Problem I: Given an integer N , find its prime factors.

Classical Solution: General Number Field Sieve needs time $O(e^{\sqrt{3} \log N} (\log \log N)^2)$

Quantum Solution: *Shor's Algorithm* solves in $O((\log N)^3)$ running time

Exponential Speed up

Problem II: Search in an unstructured database with N entries

Classical Solution: requires $\Omega(N)$ look up queries

Quantum Solution: *Grover's Algorithm* needs only $O(\sqrt{2N})$ queries

Quadratic Speed up

Problem III: Collision Search for function f (r -to-1) with domain size N

Classical Solution: requires $\Theta(\sqrt{N/r})$ executions of f

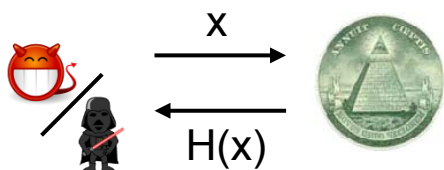
Quantum Solution: *Brassard et al.'s Algorithm* needs only $O(\sqrt{3N/r})$

Quadratic Speed up

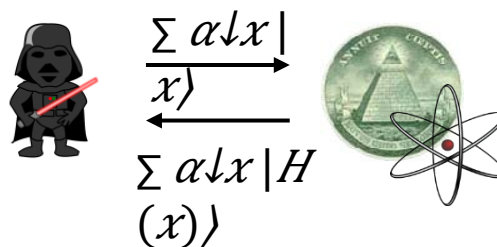
Separation (RO vs QRO)

Is there any difference? **Absolutely !!**

We present a cryptosystem which is



secure
in **classical** ROM



insecure
in **quantum** ROM



insecure
under any
instantiation



Separation

Identification Protocol P^* :

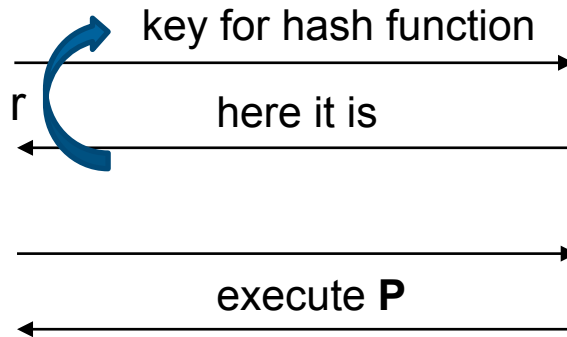
- (Informal Definition) Prover 'convinces' a Verifier that it knows something
- based on quantum-immune ID protocol P

Verifier



pk

Let ctr be the number of
succ. collision within time t



Prover



(sk, pk)

Search for collision

accept if $ctr > r/4$ or P accepts

Security of ID – Protocol P*

Recall:



Problem III: Collision Search for function f (r -to-1) with domain size N

Classical Solution: requires $\Theta(\sqrt{N/r})$ executions of f

Quantum Solution: Brassard et al.'s Algorithm needs only $O(\sqrt{3N/r})$

Idea:

Define t in \mathbf{P}^* exactly between $\sqrt{N/r}$ and $\sqrt{3N/r}$ executions of hash function

\Rightarrow Classical adversaries are too slow (win only when sk is known )
 \Rightarrow Quantum adversaries are fast enough (succeed w/o knowing sk )

Security in classical RO

Theorem: \mathbf{P}^* is secure against any efficient adversary in the classical random oracle model.

Proof sketch: $\Pr[\text{Adv breaks } \mathbf{P}^*] \leq \Pr[\text{ctr} > r/4] + \Pr[\text{Adv breaks } \mathbf{P}]$

Let r be the number of collision rounds.

Let l be the bit size of the digest / random oracle

and n the security parameter. We choose $l = \log n$.

Probability of Adv outputting collision with $q = \alpha \sqrt{3} \cdot 2^{l/2}$ queries is $\frac{q(q-1)}{2N} \leq \frac{\alpha^2}{2} \cdot \frac{2^{l/2}}{\sqrt{3} \cdot 2^{l/2}} \leq \frac{\alpha^2}{2} \cdot \frac{1}{\sqrt{3} \cdot n}$

→ Chernoff-bound $\Pr[\text{ctr} > r/4] \leq \exp(-r \frac{\alpha^2}{2} \cdot \frac{1}{\sqrt{3} \cdot n}) = \exp(-\frac{r \alpha^2}{2 \sqrt{3} \cdot n})$
 $\frac{1}{4} \leq \exp(-\frac{r \alpha^2}{2 \sqrt{3} \cdot n})$

Security against Q-adversaries

Theorem: The protocol \mathbf{P}^* is **insecure** in quantum-accessible RO model.

Proof sketch: $\Pr[\text{Adv breaks } \mathbf{P}^*] \leq \Pr[\text{ctr} > r/4] + \Pr[\text{Adv breaks } \mathbf{P}]$

Let r be the number of collision rounds. Let l be the bit size of the digest / random oracle and n the security parameter. We choose $l = \log n$.

Probability of Adv outputting collision with $q = \sqrt{3} \cdot 2^{l/2}$ queries is $\geq 1/2$ (Brassard et al.)

→ Chernoff-bound → $\Pr[\text{ctr} < r/4] \leq \exp(-r/2 \cdot (1/2)^2 \cdot 1/2) \leq \exp(-r/16) \leq 0.94^{r/16}$

Thus, Adv makes V^* accept with prob $\geq 1 - \Pr[\text{ctr} < r/4]$ which is non-negligible.

Consequences

All Post-Quantum Cryptosystems proven in the Random Oracle Model needs to be revisited.



We prove security for a class of cryptosystems *against quantum adversaries* in the *Quantum Random Oracle* model.

- Digital Signature Schemes
- Encryption Schemes

Revisiting Security of Signature Schemes

Definition:

Let A be a classical PPT adversary against signature scheme S . If there exists PPT adversary B against hard problem P , then S has a history-free reduction from hard problem P .

B is defined by the following algorithms: Let x be an instance of P

- **START**(x) \rightarrow (pk, z)
- **INSTANCE**(pk) $\rightarrow x$
 - distribution of INSTANCE is negl. close to distribution of Game_P
- **RAND** ^{O_c} (r, z) simulates $O(r)$
 - for fix z : $|x, y\rangle \rightarrow |x, y \oplus \text{RAND} \uparrow O \downarrow c(x, z)\rangle$ is indis. from random oracle
- **SIGN** ^{O_c} (m, z) simulates $S(sk, m)$
 - either aborts or distribution of SIGN is negl. close to S
 - probability that none of the queries aborts is non-negligible
- **FINISH** ^{O_c} (m, σ, z) \rightarrow solution to x .
 - with non-negl. probability

Security by History-free Reduction

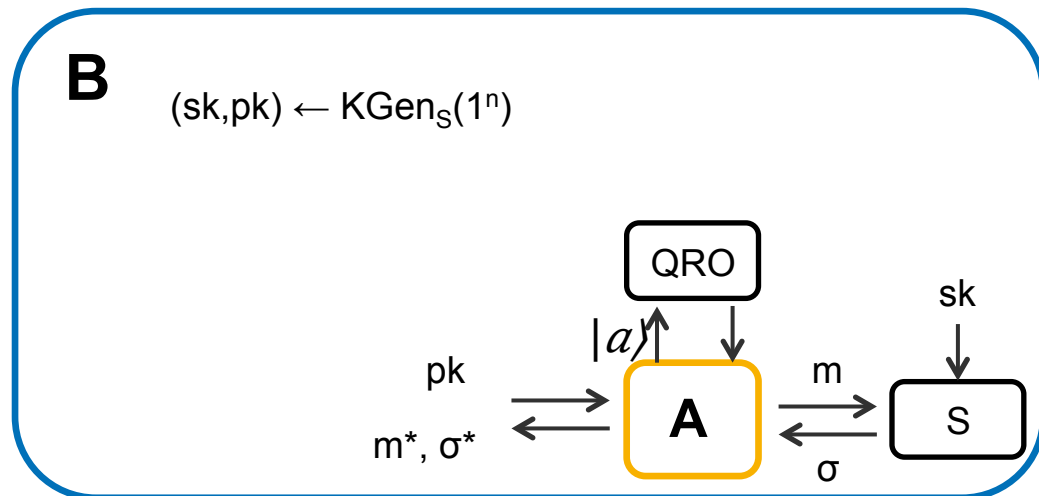
Theorem 1. *Let $\mathcal{S} = (G, S, V)$ be a signature scheme. Suppose that there is a history-free reduction that uses a classical PPT adversary A for \mathcal{S} to construct a PPT algorithm B for a problem P . Further, assume that P is hard for polynomial-time quantum computers, and that quantum-accessible pseudorandom functions exist. Then \mathcal{S} is secure in the quantum-accessible random oracle model.*

Proof Sketch:

Game 0:

Standard quantum signature Game

Assume A has non-negligible advantage



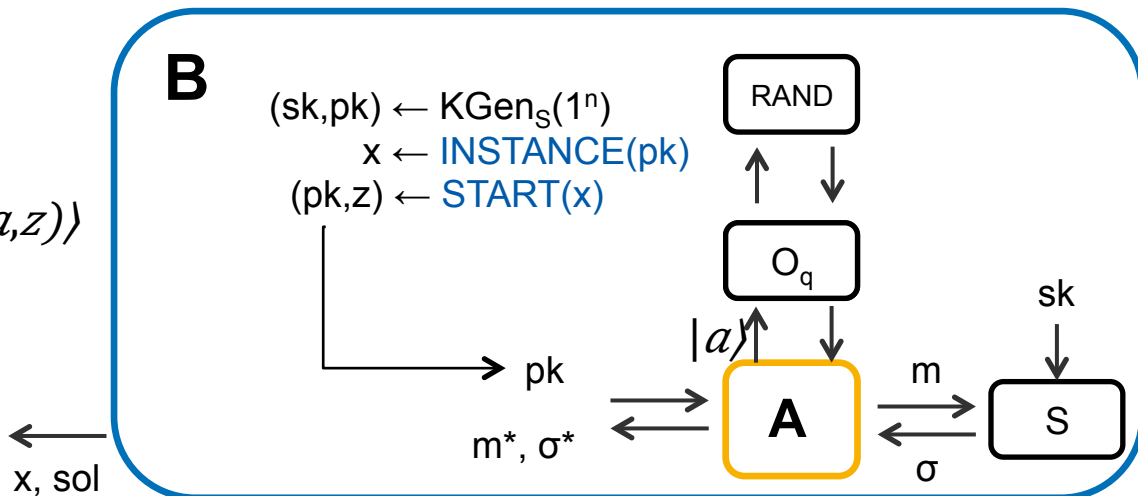
Security by History-free Reduction

Theorem 1. *Let $\mathcal{S} = (G, S, V)$ be a signature scheme. Suppose that there is a history-free reduction that uses a classical PPT adversary A for \mathcal{S} to construct a PPT algorithm B for a problem P . Further, assume that P is hard for polynomial-time quantum computers, and that quantum-accessible pseudorandom functions exist. Then \mathcal{S} is secure in the quantum-accessible random oracle model.*

Proof Sketch:

Game 1:

- $O_q: |a, b\rangle \mapsto |a, b \oplus RAND \uparrow O \downarrow c(a, z)\rangle$
- history-freeness of RAND guarantees $\{O_q\} \approx \{QRO\}$



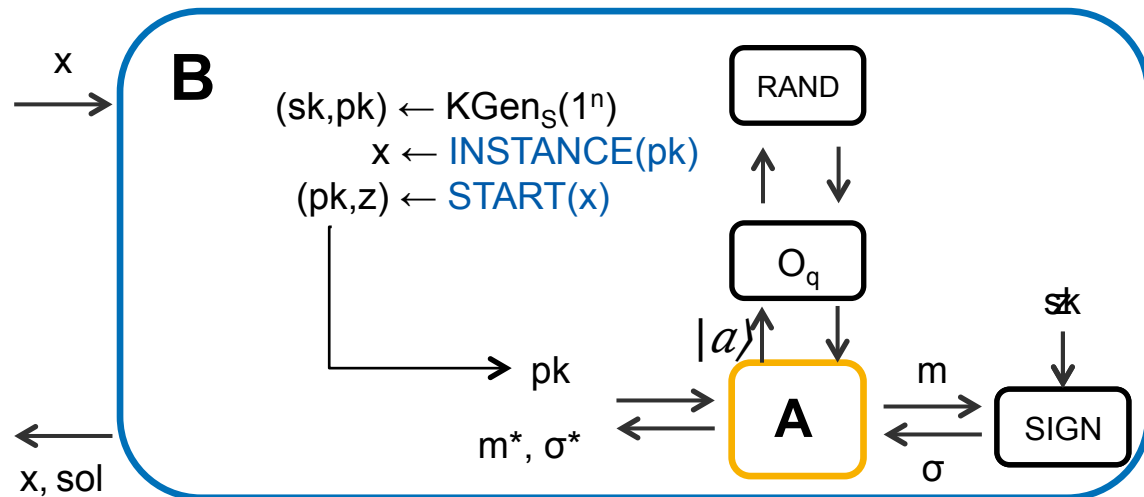
Security by History-free Reduction

Theorem 1. *Let $\mathcal{S} = (G, S, V)$ be a signature scheme. Suppose that there is a history-free reduction that uses a classical PPT adversary A for \mathcal{S} to construct a PPT algorithm B for a problem P . Further, assume that P is hard for polynomial-time quantum computers, and that quantum-accessible pseudorandom functions exist. Then \mathcal{S} is secure in the quantum-accessible random oracle model.*

Proof Sketch:

Game 2:

- distribution generated by INSTANCE is negligibly close to the one from Game_P
- probability that SIGN^{OC}(m,z) does not abort to any query is non-negligible



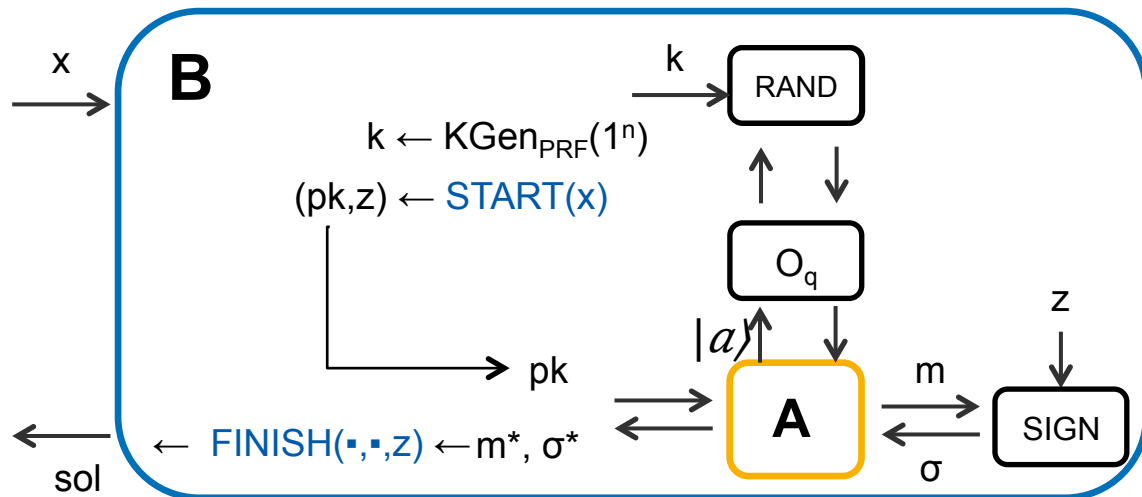
Security by History-free Reduction

Theorem 1. *Let $\mathcal{S} = (G, S, V)$ be a signature scheme. Suppose that there is a history-free reduction that uses a classical PPT adversary A for \mathcal{S} to construct a PPT algorithm B for a problem P . Further, assume that P is hard for polynomial-time quantum computers, and that quantum-accessible pseudorandom functions exist. Then \mathcal{S} is secure in the quantum-accessible random oracle model.*

Proof Sketch:

Game 3:

- PRF: quantum-accessible pseudorandom function



Signatures secure in QRO Model

We show history-free reductions for signatures from

- Preimage Sampleable Trapdoor Functions [Gentry, Peikert, Vaikuntanathan 08]
- Claw-Free Permutations [Goldwasser, Micali, Rivest 88]
- Full-Domain-Hash variant [Katz, Wang 03]

Definiton Full Domain Hash:

Let $F = (G \downarrow f, f, f \uparrow^{-1})$ be a trapdoor permutation, and O a hash function whose range is the same as the range of f . The full domain has signature scheme is $\mathcal{S} = (G, S, V)$

History-Free Reduction:

- $START(pk) := (pk, pk)$
- $INSTANCE(pk) := (pk, sk, O(m))$
- $RAND(pk, m) := (pk, Sample(m), \sigma)$
- $SIGN^{Oc}(m, pk) := Sample(1^n; O_c(m))$
- $FINISH^{Oc}(m, \sigma, pk) := (Sample(1^n; O_c(m)), \sigma)$

PSF $F = (G \downarrow f, Sample, f, f \uparrow^{-1})$

Let $X \downarrow pk$ be domain of $f(pk, \cdot)$.

$Sample(pk, \cdot)$ samples $x \leftarrow \mathcal{X} \downarrow pk$

s.t. $f(pk, x)$ is uniform in $\{f$

$(pk, y): y \in \mathcal{X}\}$

Encryption Schemes in QRO

f: injective trapdoor function

O: Random Oracle

I want securely
sent gift M to the
well-behaved boy

gawway Encryption Scheme [BR93]



C



(pk, sk)

choose r randomly

$$C = (f(pk, r), O(r) \oplus M)$$

$$c \downarrow 1, c \downarrow 2 \leftarrow C$$

$$r = f \uparrow^{-1}(sk, c \downarrow 1)$$

$$M = O(r) \oplus c \downarrow 2$$

We show CPA and CCA security in the quantum-accessible random oracle model.

Worrying Observations

- **Adaptive Programmability**
 - adversary could query oracle on exponentially many values right from the beginning
- **Extractability / Preimage Awareness**
 - classical case: simulator knows preimage, image pair
 - quantum case: query is hidden in a superposition
- **Efficient Simulation**
 - lazy-sampling does not carry over to the quantum setting
- **Rewinding / Partial Consistency**
 - Unnoticed changing of hash values difficult

Interesting Questions

▪ Negative Examples

- Are there real-world examples which are supposed to be secure against quantum adversaries but insecure in the quantum-accessible random oracle model ?

▪ Positive Examples

- Security of signatures derived by Fiat-Shamir paradigm
- More encryption examples
- Answers to the aforementioned worrying observations
- Is history-freeness merely sufficient or even necessary

Thank You!

By the way ... I am still looking for an accommodation this night ;-)