Random Oracles in a Quantum World

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 **hard** against classical computers

are **easy** with quantum computers

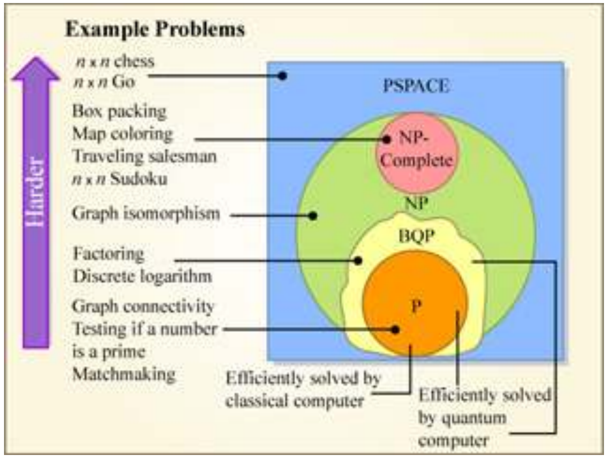
TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity

Post Quantum Cryptography

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

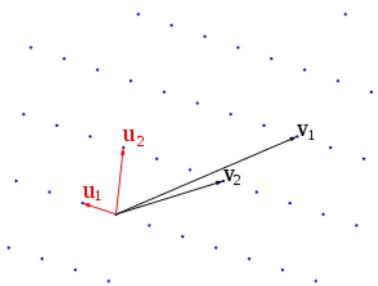
- *Hash-based Cryptography (e.g. Merkle's hash-trees signatures)*
- *Code-based Cryptography (e.g. McEliece, Niederreiter)*
- *Lattice-based Cryptography (e.g. NTRU)*
- *Multi-variate-quadratic-equations Cryptography*

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**.



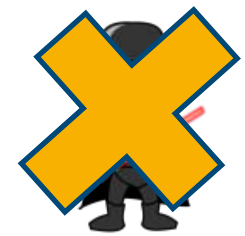
Source: Quantum Complexity Theory, Lecture Notes Fall 2010

Quantum-Resistant Primitives … with RO?



+

=



???

quantum-resistant primitive / protocol

random oracle

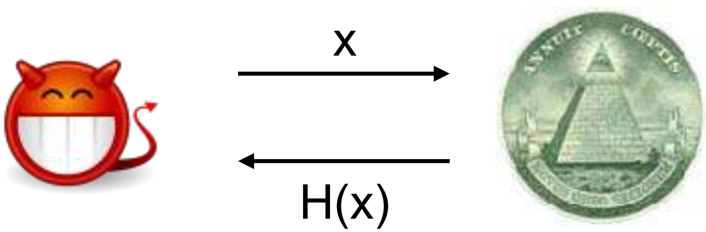
quantum adversary

Examples:

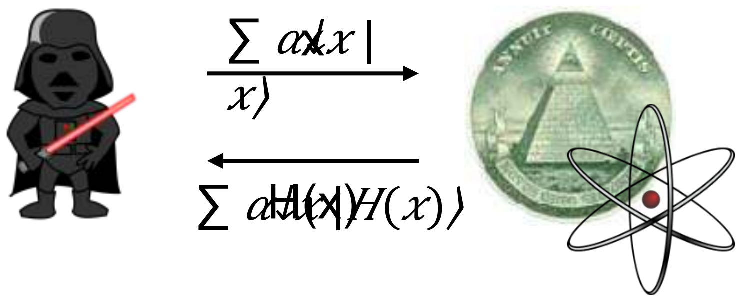
- Signatures [GPV08,GKV10,BF11]
- Encryptions [GPV08]
- Identification Schemes [CLRS10]

Quantum-Accessible Random Oracles

Classical



Quantum



Idea:
Instantiate Random Oracle
by “strong implementation”

minimal requirement:
quantum adversary may query RO
about quantum states

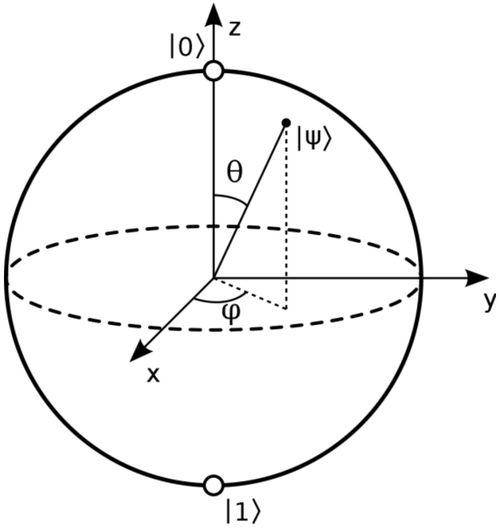
Outline

(1) Introduction to Quantum Theory

(2) Separation Result

(3) Positive Examples

(4) Open Problems



Introduction to Quantum Theory

Transmission of Entropie

Today:

Bit 0/1 classical channel

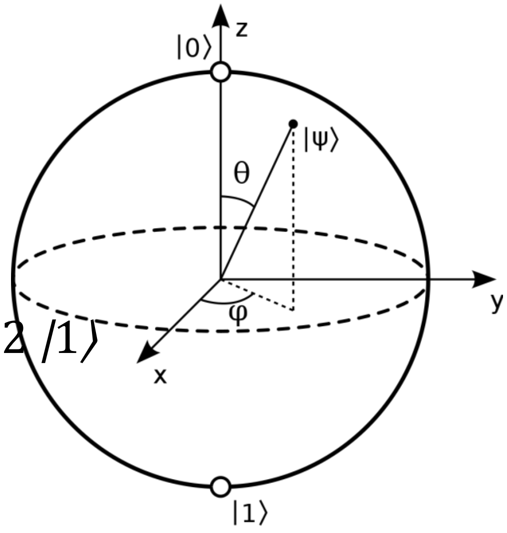
Future:

Qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ quantum channel

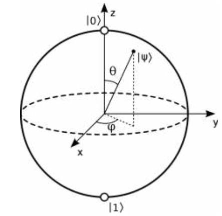
$\alpha, \beta \in \mathbb{C}$ are probability amplitudes

- 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



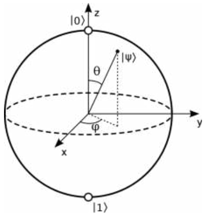
Quantum System A

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

TECHNISCHE UNIVERSITÄT DARMSTADT

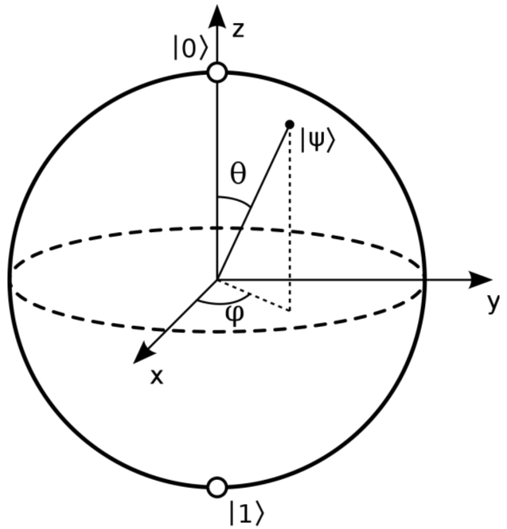
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Quantum Computations

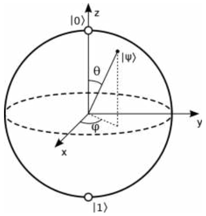


Transformations

- only unitary transformations U
  - $U^{*} U = I_n$
  - $\det(U) = \pm 1$
- 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 $p_i=\varphi M_i \varphi$
- partial measurements possible

Toy Example

$$|\psi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle$$

$$|\psi_2\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle$$

joint

$$|\psi_1, \psi_2\rangle = \alpha_1 \alpha_2 |00\rangle + \alpha_1 \beta_2 |01\rangle + \beta_1 \alpha_2 |10\rangle + \beta_1 \beta_2 |11\rangle$$

measure first qubit

Output:

- 0 with prob. $|\alpha_1 \alpha_2|^2 + |\alpha_1 \beta_2|$
- 1 with prob. $|\beta_1 \alpha_2|^2 + |\beta_1 \beta_2|$

result 0

$$|\psi\rangle = \alpha_1 \alpha_2 / \sqrt{|\alpha_1 \alpha_2|^2 + |\alpha_1 \beta_2|^2}\, |0\rangle + \alpha_1 \beta_2 / \sqrt{|\alpha_1 \alpha_2|^2 + |\alpha_1 \beta_2|^2}\, |1\rangle$$

Power of Quantum Computing

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

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

Classical Solution: General Number Field Sieve needs time $O(e^{\sqrt[3]{7\log N(\log\log N)^2}})$

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 $O(\sqrt{N})$ 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

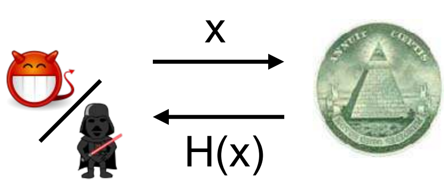
Quantum Solution: *Brassard et al.'s Algorithm* needs only $O(\sqrt[3]{N/r})$

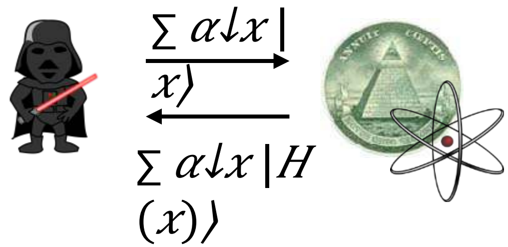
Quadratic Speed up

Separation (RO vs QRO)

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

We present a cryptosystem which is

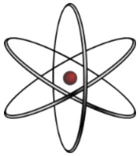




secure
in **classical** ROM

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 | *Prover*

pk

(sk,pk)

key for hash function →

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

r

← here it is

Search for collision

→

execute **P**

←

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 $O(\sqrt[3]{N/r})$

Idea:

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

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

Security in classical RO

Theorem: **P*** is secure against any efficient adversary in the classical random oracle model.

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

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 $\mathrm{l} = \log n$.

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

$\xrightarrow{Chernoff-bound} \Pr[ctr > r/4] \le \exp\left(-r\frac{\alpha^2}{2\sqrt[3]{n}}\left(\frac{\sqrt[3]{n}-2\alpha^2}{2\alpha^2}\right)^2 \frac{1}{4}\right) \le \exp\left(-\frac{r\sqrt[3]{n}}{32\alpha^2}\right)$

Security against Q-adversaries

Theorem: The protocol **P*** is insecure in quantum-accessible RO model.

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

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 $\mathrm{l} = \log n$.

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

$\rightarrow \mathit{Chernoff-bound}{:}\quad \Pr[ctr < r/4] \leq \exp(-r/2\ (1/2)^2\ 1/2) \leq \exp(-r/16) \leq 0.94^r$

Thus, Adv makes V* accept with prob $\geq 1 - \Pr[ctr < r/4]$ 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**

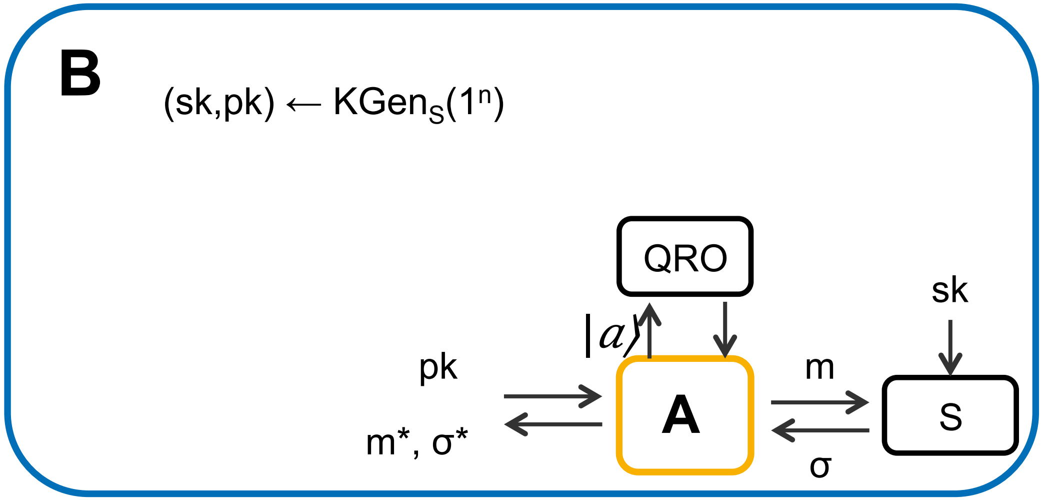
- **START(x)** → (pk,z)
- **INSTANCE(pk)** → x
  - distribution of INSTANCE is negl. close to distribution of $\text{Game}_{\mathbf{P}}$
- $\mathbf{RAND}^{\mathbf{O_c}}\mathbf{(r,z)}$ simulates O(r)
  - for fix z: $|x,y\rangle \rightarrow |x, y \oplus RAND^{O_c}(x,z)\rangle$ is indis. from random oracle
- $\mathbf{SIGN}^{\mathbf{O_c}}\mathbf{(m,z)}$ 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
- $\mathbf{FINISH}^{\mathbf{O_c}}\mathbf{(m,\sigma,z)}$ → 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



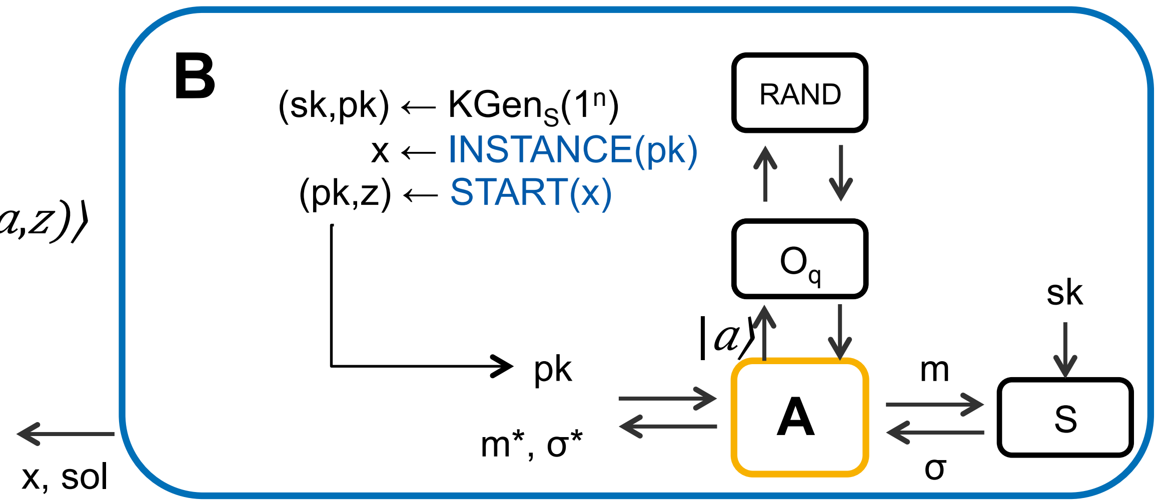
Security by History-free Reduction

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 $\{O_q\} \approx \{QRO\}$



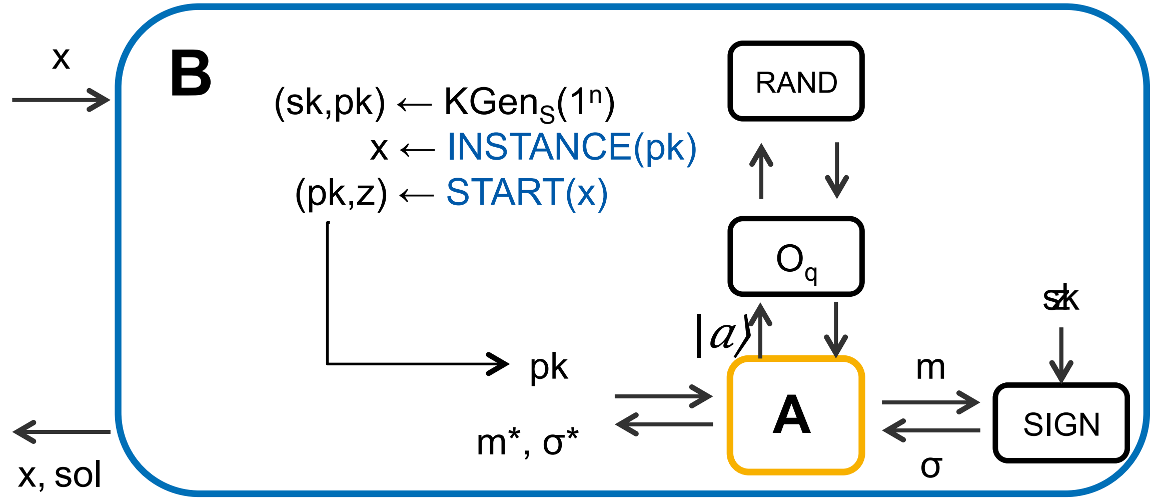
Security by History-free Reduction

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 negliglbly close to the one from $\text{Game}_{\mathbf{P}}$
- probability that $\text{SIGN}^{O_c}(m,z)$ does not abort to any query is non-negligible



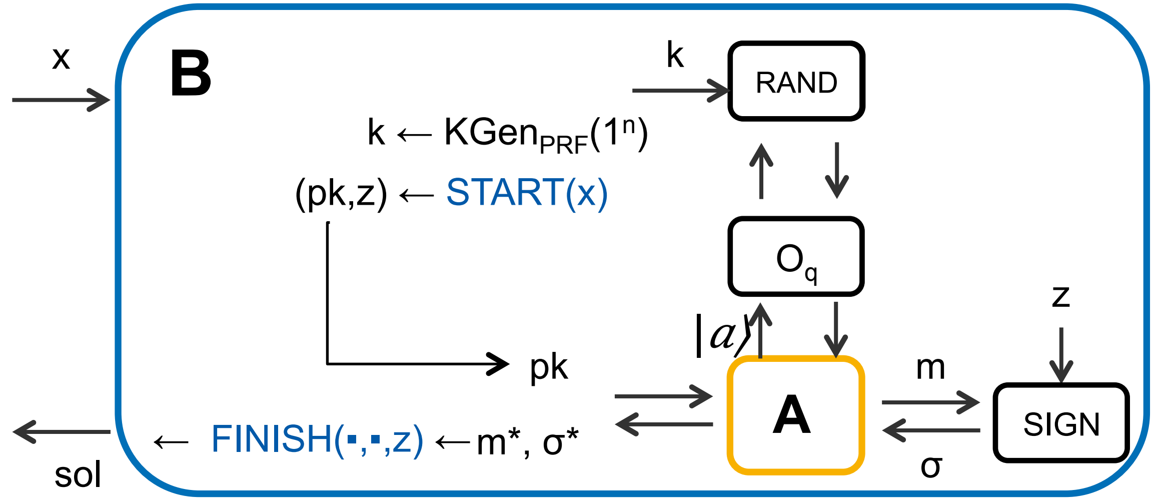
Security by History-free Reduction

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 $\boldsymbol{F}=(G_f, f, f^{-1})$ 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 $\boldsymbol{S}=(G,S,V)$ where:

- $G=G_f$
- $S(sk,m)=f^{-1}(sk,O(m))$
- $V(pk,m,\sigma)=\{1 \text{ if } O(m)=f(pk,\sigma)$

History-Free Reduction:

- START(pk) := (pk,pk)
- INSTANCE(pk) := pk
- RAND^{O_c}(r,pk) := f(pk, *Sample*(1^n;O_c(r)))
- SIGN^{O_c}(m,pk) := *Sample*(1^n;O_c(m))
- FINISH^{O_c}(m,σ,pk) := (*Sample*(1^n;O_c(m)), σ)

PSF $F=(G_f, Sample, f, f^{-1})$
Let X_{pk} be domain of $f(pk,\cdot)$.
$Sample(pk,\cdot)$ samples $x \xleftarrow{\$} X_{pk}$
s.t. $f(pk,x)$ is uniform in $\{f(pk,y): y\in X\}$

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity

Encryption Schemes in QRO

f: injective trapdoor function
O: Random Oracle

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

E ... gaway Encryption Scheme [BR93]

C

(pk,sk)

choose *r* randomly

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

$c_1, c_2 \leftarrow \perp C$

$r = f^{-1}(sk, c_1)$

$\boldsymbol{M} = O(r) \oplus c_2$

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 ;-)