Approaches, models, and challenges in the analysis of cryptographic algorithms and protocols in the context of the Quantum Threat

Vitaly Kiryukhin,
Anton Naumenko,
Andrey Shcherbachenko

LLC “SFB Lab”, JSC “InfoTeCS”

CTCrypt 2025
4 June 2025

Disclaimer

СФБ ЛАБ

1. The presentation does NOT contain:
   - predictions about the timeframe
     for creating an efficient quantum computer;
   - in-depth details of quantum computing.

Disclaimer

СФБ ЛАБ

1. The presentation does NOT contain:
   - predictions about the timeframe
     for creating an efficient quantum computer;
   - in-depth details of quantum computing.
2. We talk mostly about provable security, less about constructive cryptanalysis, and a little about common sense.

Disclaimer

СФБ ЛАБ

1. The presentation does NOT contain:
   - predictions about the timeframe for creating an efficient quantum computer;
   - in-depth details of quantum computing.
2. We talk mostly about provable security, less about constructive cryptanalysis, and a little about common sense.
3. Almost all the results presented are essentially well known and do not claim any novelty.

Well-known or well-recognised statements

СФБ ЛАБ

It is commonly believed that by using Shor's algorithm and an efficient quantum computer, it is possible to break existing asymmetric algorithms: RSA, ECDSA, GOST 34.10, Diffi-Hellman etc.

Well-known or well-recognised statements

СФБ ЛАБ

It is commonly believed that by using Shor's algorithm and an efficient quantum computer, it is possible to break existing asymmetric algorithms: RSA, ECDSA, GOST 34.10, Diffi-Hellman etc.

We will not discuss this, but try to answer the following questions:

- What about other cryptoalgorithms and protocols?
- How to prove security?

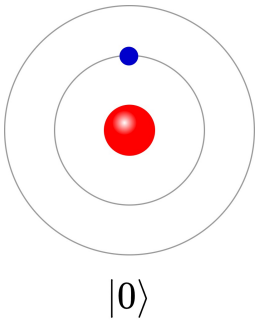
Basic information about quantum computing

Qubit (quantum bit)

- **Qubit** is a two-level quantum system
- Element of 2D complex space
- Like the classical bit, has two distinguished basis states (e.g., $|0\rangle = (1\,0)^\top$ and $|1\rangle = (0\,1)^\top$)
- **Unlike** the classical bit, can be “both” at the same time (superposition):

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,,$$

where α and β are complex w.r.t. normalization constraint $|\alpha|^2 + |\beta|^2 = 1$

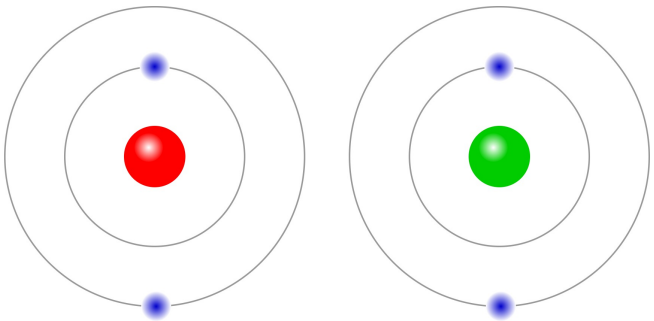


Many-qubit systems

- n-qubit system is a tensor product of the spaces of its individual qubits
- A state of the system is

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

- Has 2^n basis states – the growth is exponential
- Any linear transformation acts on all 2^n states in superposition ("quantum parallelism")



$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

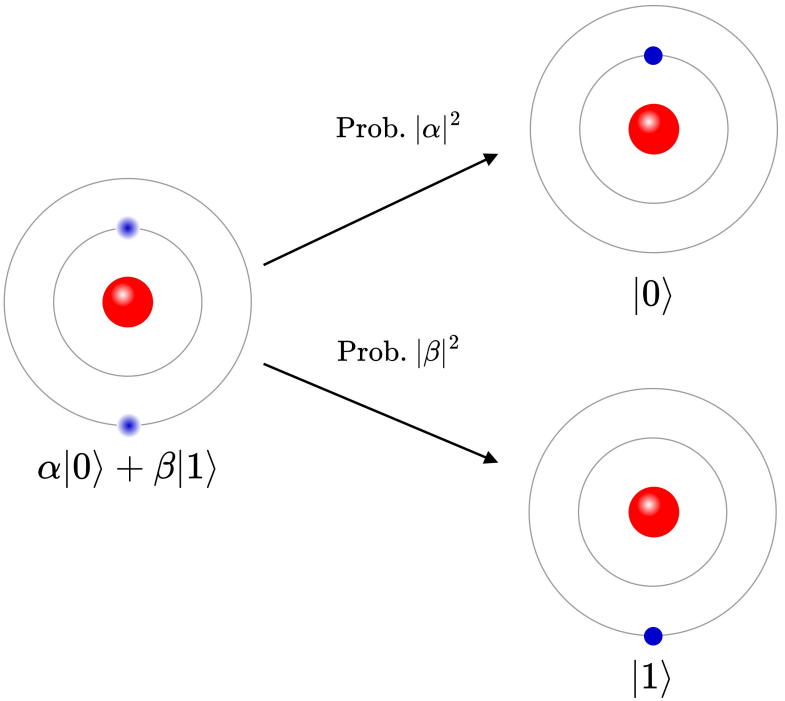
Transformations

СФБ ЛАБ

- Transformations of qubits are unitary operators (“gates”)
- 1-qubit gates:
  - Pauli’s group: I, X, Z, Y;
  - Hadamard H, etc.
- 2-qubit gates: $CNOT$ – controlled bit-flip (XOR), CZ, $SWAP$, etc.
- 3-qubit gates:
  - Toffoli – controlled $CNOT$ (AND+XOR);
  - Fredkin – controlled $SWAP$, etc.
- To construct any n-qubit gate with arbitrary precision, we need a smaller set of 1-/2-/3-qubit gates (“universal set”)

Measurement

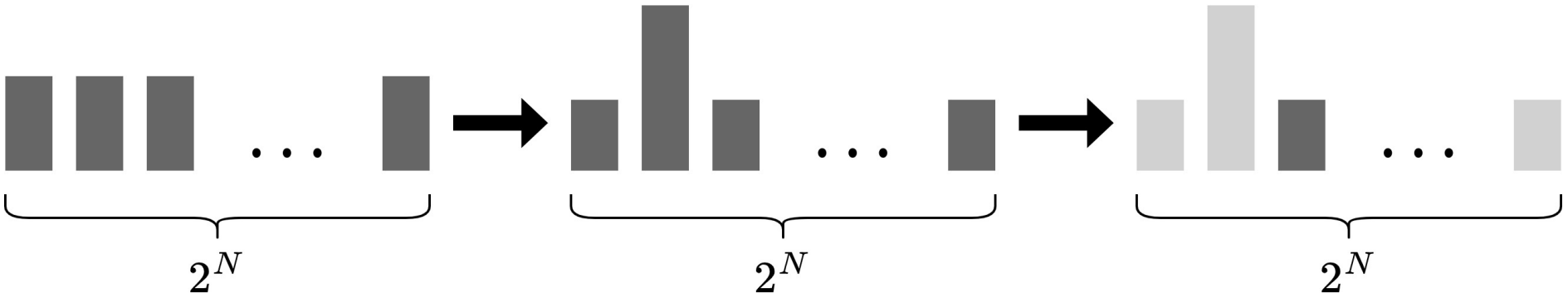
- **Measurement** is a special (non-unitary) type of transformation
- It makes qubit to probabilistically collapse into one of the basis states, destroying superposition



$|\alpha|^2$ (and $|\beta|^2$) are probabilities to find qubit in $|0\rangle$ (and $|1\rangle$) state after measurement

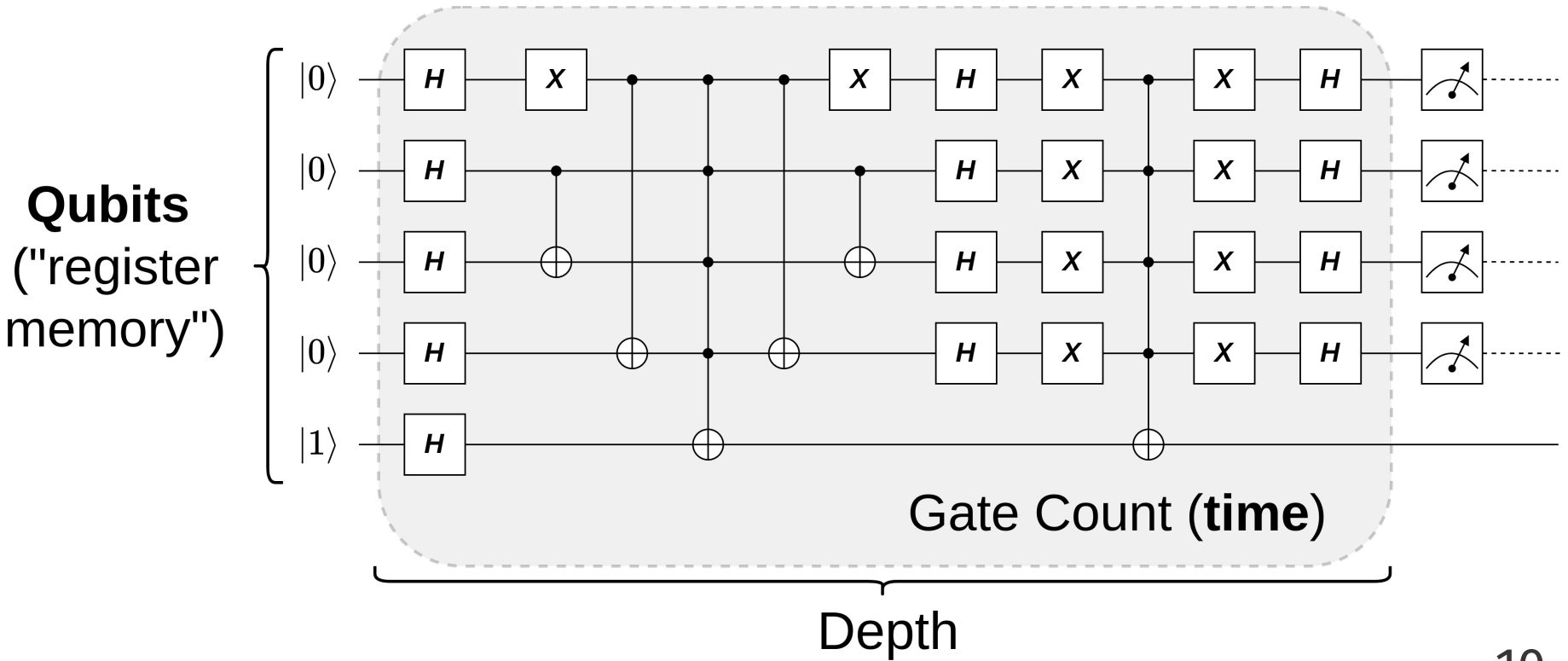
Simplifying analogy from the classical world

superposition of N qubits	**distribution** over 2^N bitstrings
transformation	distribution **change**
measurement	**sampling** from distribution



Gate model

- Gate model: computations are represented as circuits
- We can think of:
  - logical ***qubits*** as "***register memory***"
  - ***gates*** as ***time*** (in their total number or in layers)



Three settings: Q0, Q1, Q2

Formal comments

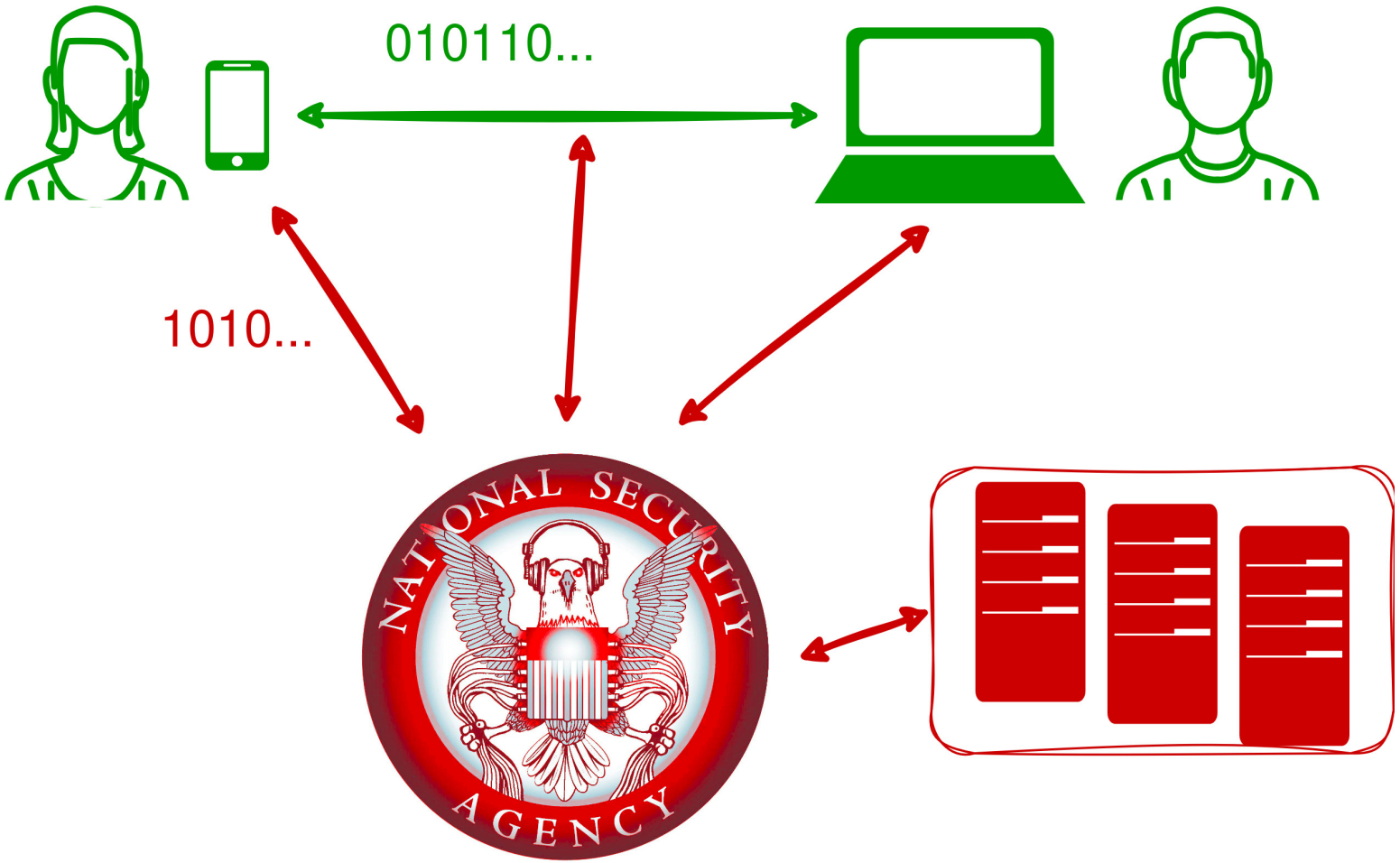
Setting is defined by answers to two questions:

– how does the adversary interact with cryptosystem?

– what kind of computations can the adversary perform?

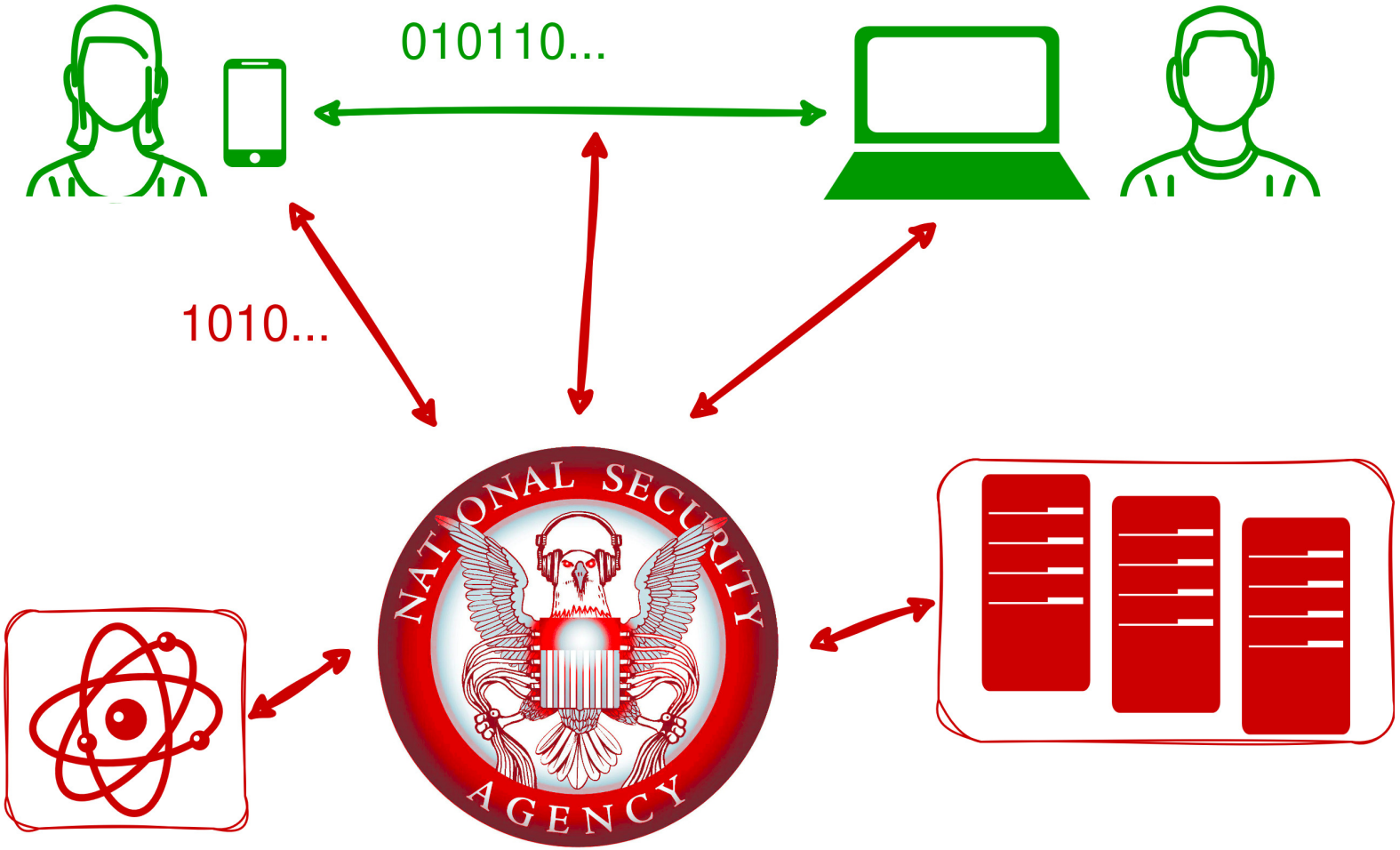
Setting	Interactions	Computations
Q0	Classic	Classic
Q1	Classic	Quantum
Q2	Quantum	Quantum

Q0: CLASSIC INTERACTIONS AND COMPUTATIONS



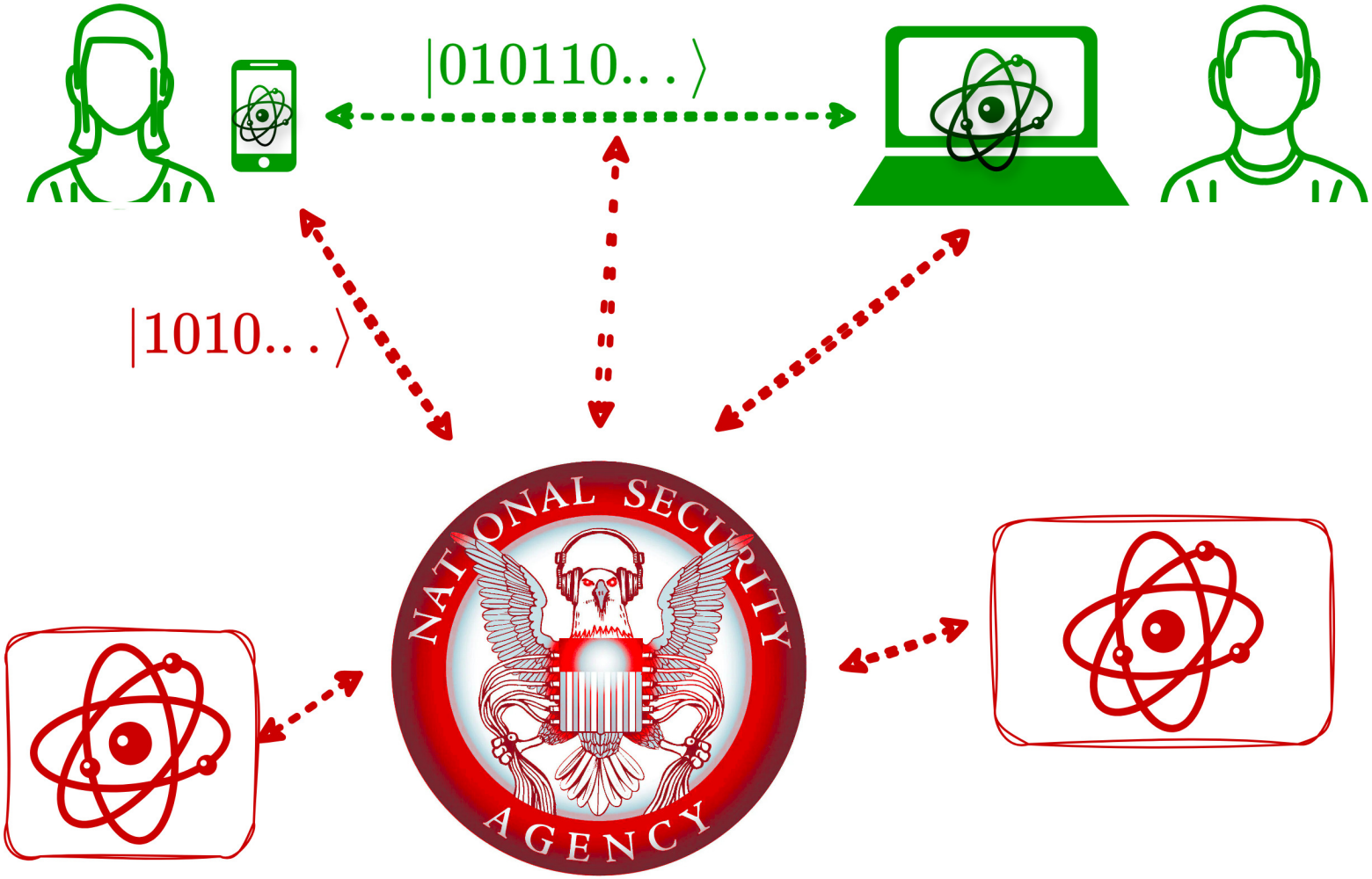
The crypto reality familiar to everyone.

Q1: COMPUTATIONS BECOME QUANTUM



Possible near future.
The adversary will have built an efficient quantum computer.
We probably won't know it right away.

Q2: EVERYTHING BECOMES QUANTUM



We're definitely not here.
We'll definitely be able to detect if we end up here.

Three settings: Q0, Q1, Q2

Cryptographers prefer *stronger* models.

Q1 is stronger than Q0.

Q2, although not realistic now, is the strongest model.

Why not just use it everywhere?

Three settings: Q0, Q1, Q2

СФБ ЛАБ

Cryptographers prefer *stronger* models.

Q1 is stronger than Q0.

Q2, although not realistic now, is the strongest model.

Why not just use it everywhere?

⇒ Many cryptoalgorithms are **insecure in Q2!**

⇒ Many cryptoalgorithms have much **worse security bounds in Q2!**

What is insecure in Q2?

Examples:

- CBC-MAC-like schemes
- AEAD-scheme GCM
- Wegman-Carter MAC (information theoretic secure scheme!)
- SPHINCS+ (postquantum hash-based signature)

Example: attack on Wegman-Carter in Q2

$$Tag = Msg \otimes Key \oplus OneTimeKey$$

$$Tag, Msg, Key, OneTimeKey \in GF(2^n)$$

Example: attack on Wegman-Carter in Q2

$$Tag = Msg \otimes Key \oplus OneTimeKey$$

$$Tag, Msg, Key, OneTimeKey \in GF(2^n)$$

- Query the tag oracle with the superposition of Msg_1 and Msg_2
- Use Deutsch's algorithm to recover i-th secret bit of

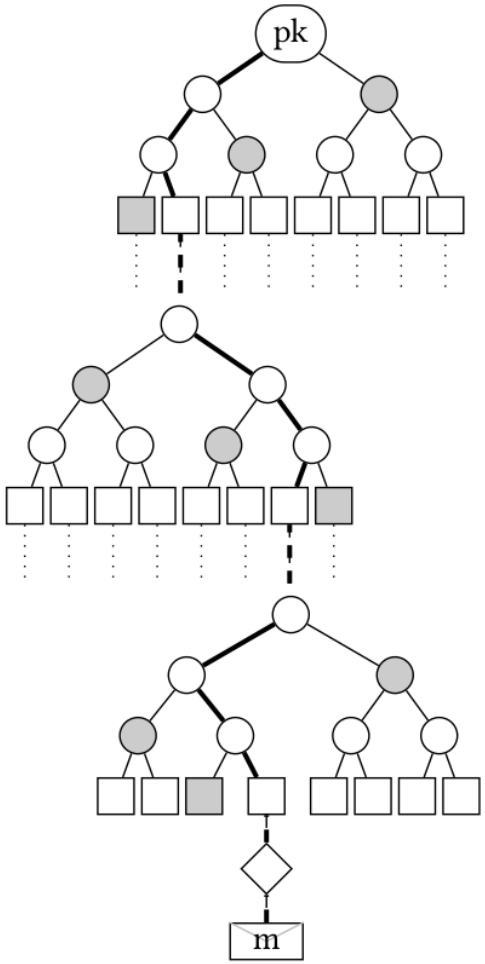
  $Msg_1 \otimes Key \oplus Msg_2 \otimes Key$
- Recover all bits of Key in several queries $\Rightarrow$ universal forgery

Dan Boneh, Mark Zhandry – 2012

Quantum-Secure Message Authentication Codes

Example: attack on SPHINCS/SPHINCS+ in Q2

- Find f messages signed by a single instance of FTS
- Fix index $idx \in \{0,1\}^{64}$ of target FTS
- Search a message with idx by Grover's algorithm and $\approx 2^{32}$ superposition queries to signing oracle
- Repeat f times and make a forgery



Quan Yuan, Mehdi Tibouchi, Masayuki Abe – 2023

Quantum-access Security of Hash-based Signature Schemes

Thesis №1 about models

СФБ ЛАБ

- Q0 is our reality
- Q1
  - realistic
  - possibly “near future”
  - “hard-to-detect”
- Q2
  - interesting and powerful model
  - NOT realistic now and in near future
  - “easy-to-detect”

Next, we talk only about Q1

Two "types" of security proofs

Two "types" of security proofs

СФБ ЛАБ

1. **Standard Model** – reduction of protocol security to the complexity of some problem(s)
2. **Random Oracle Model** – some component (hash, cipher, permutation) is idealised a priori

Logic of proof in Standard Model

Let there exist an arbitrary algorithm **A**

that efficiently attacks a protocol **P**,

then there exists an algorithm **B**

that is equally efficient at solving a hard problem **H**.

But **H** is said to be unsolvable, so **P** cannot be attacked!

Standard model

СФБ ЛАБ

Examples of proofs in Standard Model

- CTR encryption indistinguishability
- CMAC unforgeability
- Merkle-Damgard hash collision and preimage resistance
- SPHINCS signature indistinguishability

Random Oracle Model

СФБ ЛАБ

One of the cryptoprotocol algorithms (e.g. hash function) is immediately replaced by “ideal and incomputable“ Random Oracle.

No real hash function can be a Random Oracle,

no real block cipher can be an “ideal cipher”,

but ROM is useful and gives a simpler proofs and effective protocols.

Random Oracle Model

СФБ ЛАБ

Examples of proofs in ROM

- ECDSA / GOST 34.10 unforgeability
- Sponge-like hash properties
- PBKDF2 time hardness
- Davies-Meyer compression collision/preimage resistance
- Kyber (lattice-based KEM) indistinguishability

Q1 and security proofs in Standard Model

Q1 and proofs in Standard Model

СФБ ЛАБ

Good news

...black-box (reduction) proofs can be adapted

Slightly less good news

...complexity of basic problems should be **re-evaluated** because of the presence of a quantum computer

Q1: Two possible approaches

СФБ ЛАБ

1. All computations are quantum

- An adversary and oracles are ***quantum*** algorithms
- All queries are ***quantum*** (i.e. superpositions)
- Before computing the oracle's response, the query is **measured**
- The response can be computed using only ***classical*** computations

Q1: Two possible approaches

СФБ ЛАБ

1. All computations are quantum

- An adversary and oracles are ***quantum*** algorithms
- All queries are ***quantum*** (i.e. superpositions)
- Before computing the oracle's response, the query is **measured**
- The response can be computed using only ***classical*** computations

⇒ Simple and implicit approach, quantum and classical resources are accounted for together.

Q1: Two possible approaches

СФБ ЛАБ

2. “Magic box”

- An adversary and oracles are *classical* algorithms
- All queries are *classical*
- The adversary gains access to *another oracle*, a “magic box”, a quantum computer *QC*
- QC accepts *classical* queries (programmes), executes them, returns the result
- Each query to the QC implicitly specifies the distribution on the outputs

Formally, all algorithms and oracles are running on Quantum Turing Machines.

Q1: Two possible approaches

СФБ ЛАБ

2. “Magic box”

- An adversary and oracles are *classical* algorithms
- All queries are *classical*
- The adversary gains access to *another oracle*, a “magic box”, a quantum computer *QC*
- QC accepts *classical* queries (programmes), executes them, returns the result
- Each query to the QC implicitly specifies the distribution on the outputs

⇒ Explicit, but more flexible approach.

The resources can be accounted for in more detail.

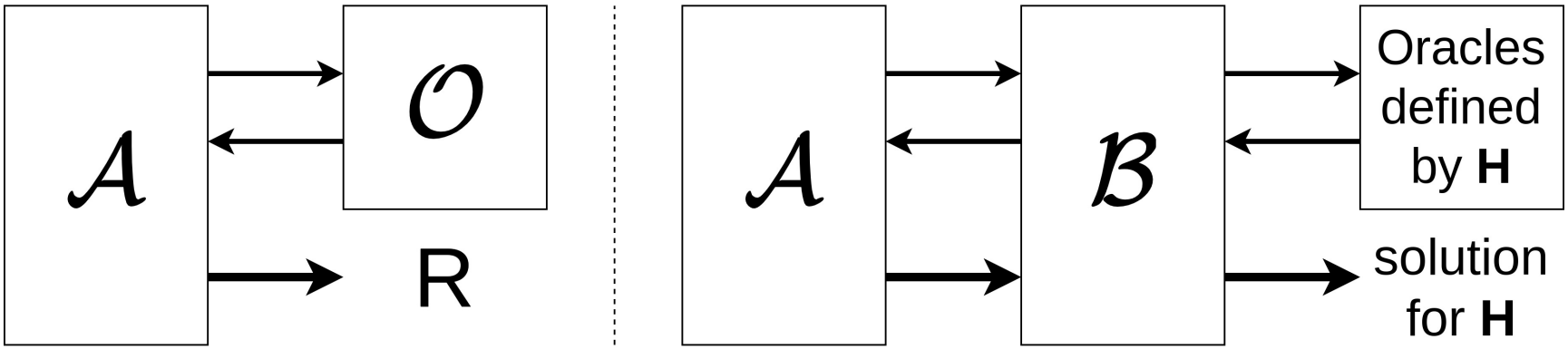
Formally, all algorithms and oracles are running on Quantum Turing Machines.

Idea of proof adaptation with “Magic box”

Classical setting (Q0)

An algorithm **A**, by accessing the oracle **O**, produces the result **R**.

An algorithm **B** that uses **A**, models an oracle **O** for it, and uses **R** to solve some hard problem **H**.



Idea of proof adaptation with "Magic box"

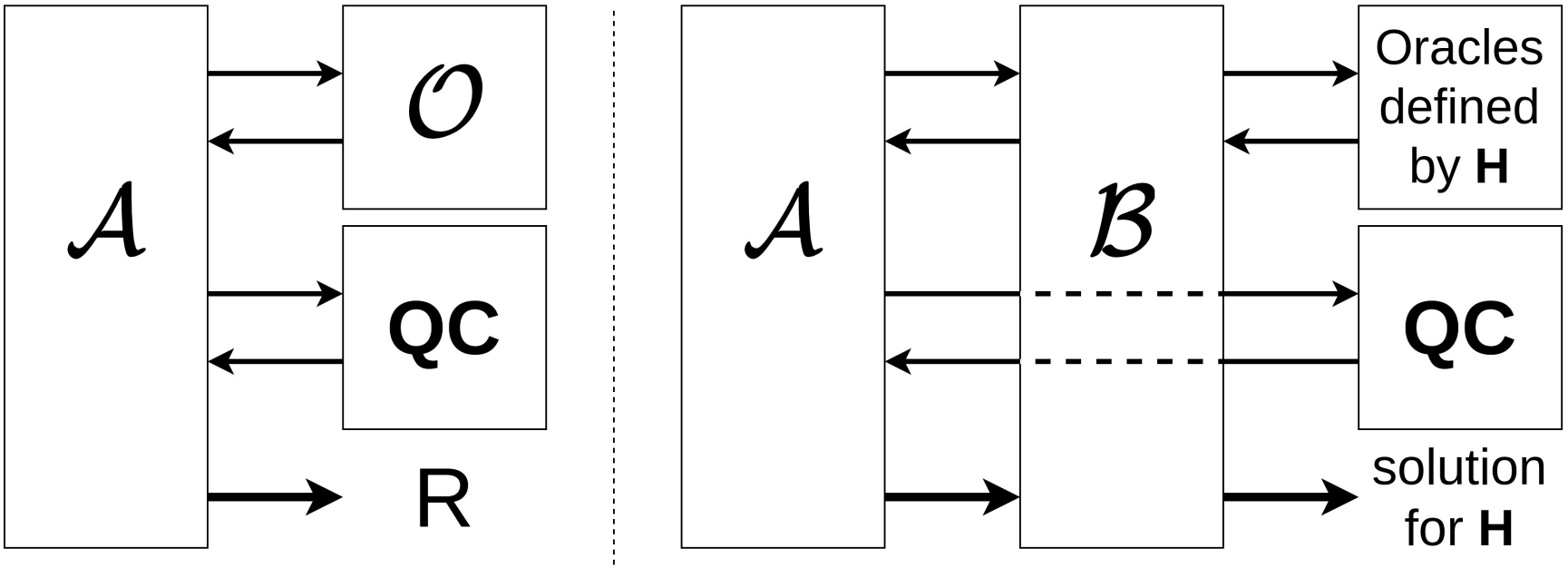
Quantum setting (Q1)

A gains access to **QC**. **B** also gains access to the same **QC**.

B responds to queries from **A** to **O** *in the same way as before* in Q0.

B responds to queries from **A** to **QC** by simple forwarding.

The proof is preserved, but instead of **H**, we have "**H** in Q1".



Basic hard problems in Q1

Although the proof persists,

the basic hard problems may no longer stay as such:

- problem may become easily solvable (e.g. discrete log);
- problem's complexity may be reduced (e.g. block ciphers security).

Example: resources of QC

QC can be implemented in a variety of ways,
including non-universal.

Gate model

- total time
- number of restarts
- number of parallel instances
- number of qubits
- memory size and type
- max depth
- … and so on

The adversary has its own “classical” resources and **QC** resources.
In the simplest case, the running times are t_C and t_Q.

Example: resources of QC

Definitely,

$$\text{“classic operations” } t_C \geq \text{“quantum operations” } t_Q,$$

but now and in near future

$$\text{“classic operations” } t_C \gg \text{“quantum operations” } t_Q.$$

Results

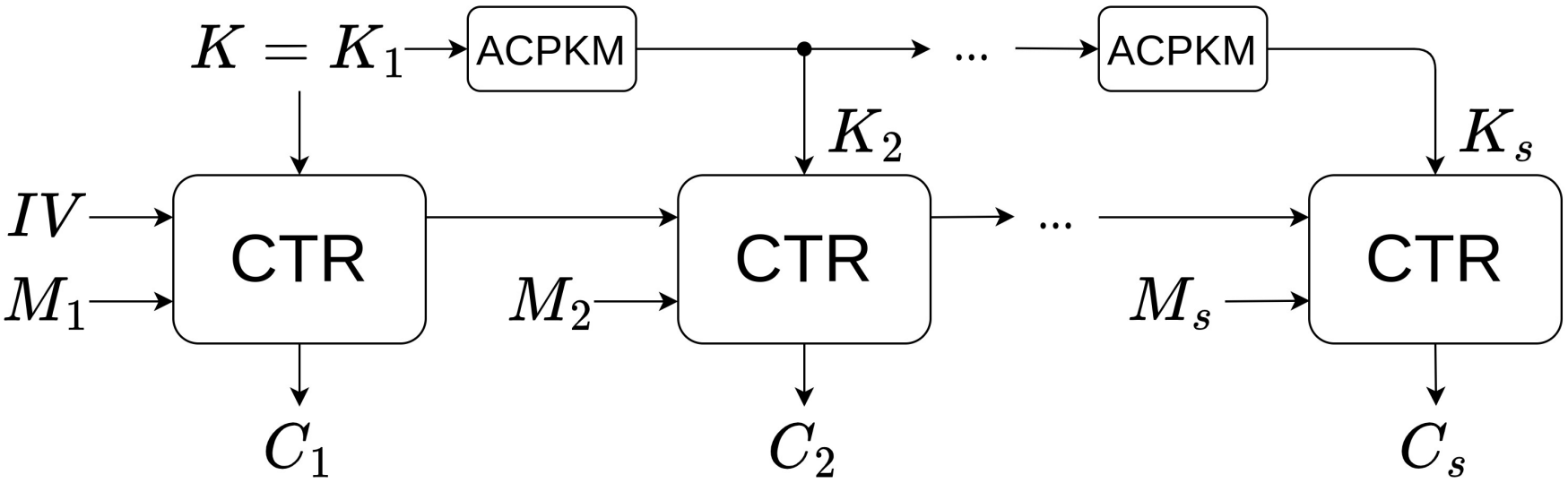
We obtain post-quantum security proofs (Q1) for:

- Encryption modes (CBC, CFB, OFB, CTR, CTR-ACPKM)
- MAC modes (OMAC, OMAC-ACPKM)
- AEAD (MGM)
- Keyed hash (HMAC-Streebog, Streebog-K)
- Unkeyed hash (preimage/collision resistance of Streebog)
- Protocols (CRISP, IPlir, TLS with PSK).

Note

Security models are usually denoted by the suffix/prefix “Q1” or “PQ”.

Example: CTR-ACPKM with block cipher E



s sections of σ n-bit blocks each.

Example: CTR-ACPKM with block cipher E

Theorem (Q0 – classical)

$$\mathrm{Adv}^{\mathit{IND\text{-}CPNA}}_{\text{CTR-ACPKM}}(t_C, s, \sigma) \le s \cdot \mathrm{Adv}^{\mathit{PRP}}_{\mathrm{E}}(t'_C, \sigma) + s \cdot \left(\frac{\sigma^2}{2^{n+1}}\right),$$

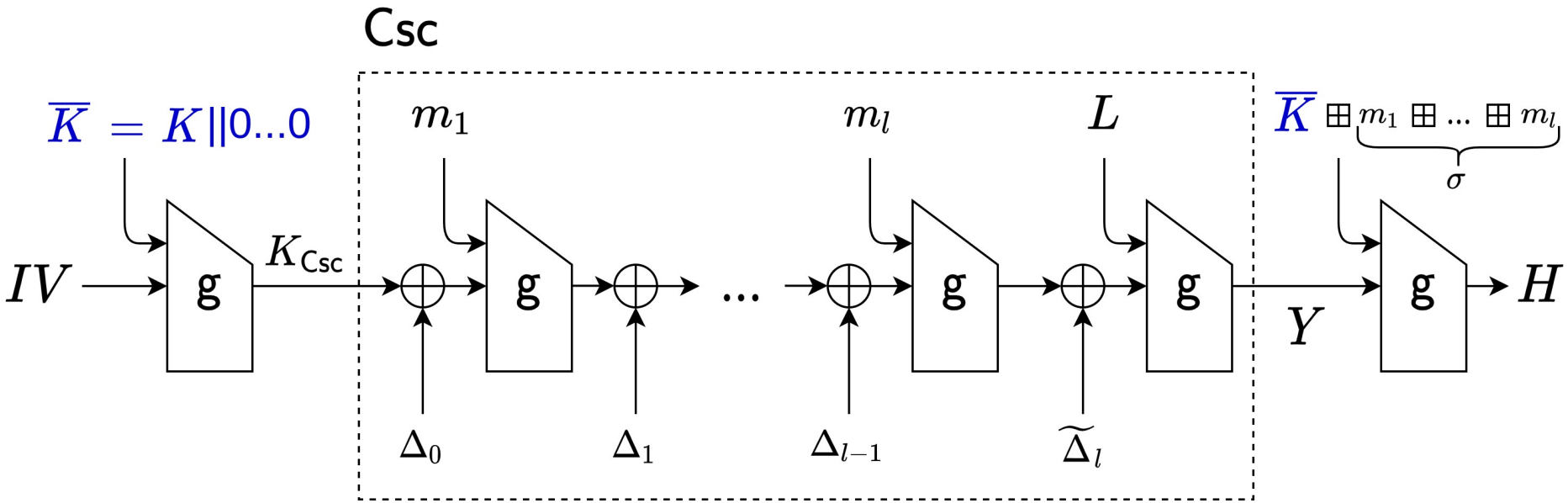
Theorem (Q1 – quantum)

$$\mathrm{Adv}^{\mathit{IND\text{-}CPNA\text{-}Q1}}_{\text{CTR-ACPKM}}(t_C, t_Q, s, \sigma) \le s \cdot \mathrm{Adv}^{\mathit{PRP\text{-}Q1}}_{\mathrm{E}}(t'_C, t_Q, \sigma) + s \cdot \left(\frac{\sigma^2}{2^{n+1}}\right),$$

t_C classical and t_Q quantum computation resources, $t'_C \approx t_C$,

s sections of σ n-bit blocks each.

Example: Keyed Streebog PRF-security



$H = \text{Streebog}(\overline{K}||M)$,

block length $n = 512$ bit,

key length $k \leq n$.

Example: Keyed Streebog PRF-security

СФБ ЛАБ

Theorem (Q0 – classical)

$$\mathrm{Adv}^{PRF}_{\text{Streebog-K}}(t_C, q, l) \leq$$

$$\leq \mathrm{Adv}^{PRF\text{-}RKA_{\boxplus}}_{g^{\triangledown}}(t'_C, q', q', 1) + \ell' \cdot \mathrm{Adv}^{PRF\text{-}RKA_{\oplus}}_{g^{\triangleright}}(t'_C, q) + \frac{q^2+q}{2^{n+1}},$$

Theorem (Q1 – quantum)

$$\mathrm{Adv}^{PRF\text{-}Q1}_{\text{Streebog-K}}(t_C, t_Q, q, l) \leq$$

$$\leq \mathrm{Adv}^{PRF\text{-}RKA_{\boxplus}\text{-}Q1}_{g^{\triangledown}}(t'_C, t_Q, q', q', 1) + \ell' \cdot \mathrm{Adv}^{PRF\text{-}RKA_{\oplus}\text{-}Q1}_{g^{\triangleright}}(t'_C, t_Q, q) + \frac{q^2+q}{2^{n+1}},$$

t_C classical and t_Q quantum computation resources, $(t'_C \approx t_C)$,
q adaptively chosen messages $(q' = q + 1)$, $n = 512$,
ℓ is the maximum length of the message (in n-bit blocks), $\ell' = \ell + 1$.

Thesis №2: security proofs in Standard Model

СФБ ЛАБ

- Security proof in Standard Model can be easily adapted to Q1
- The complexity of basic problems should be re-evaluated

Thesis №2: security proofs in Standard Model

СФБ ЛАБ

- Security proof in Standard Model can be easily adapted to Q1
- The complexity of basic problems should be re-evaluated
- If a post-quantum scheme has classical proof “only through reduction”, then we should care only about underlying basic problems, not about the whole scheme

The complexity of basic problems

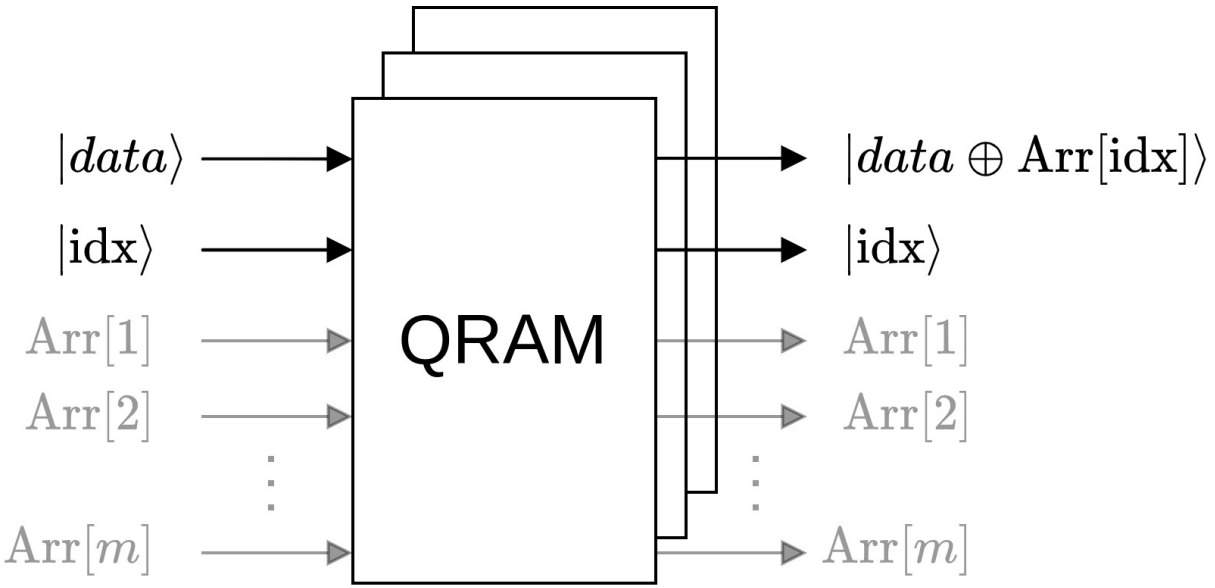
List of basic problems

- PRP-security of Kuznyechik
- PRP-security of Magma
- PRF-security of Streebog compression function (CF)
- Preimage/collision resistance of Streebog CF or Streebog itself
- Syndrome decoding of random linear code
- and many others

Quantum memory (QRAM)

	Interactions	Computations	QRAM
Q0	Classical	Classical	No
Q1	Classical	Quantum	No
			expensive
			cheap
Q2	Quantum	Quantum	

Quantum memory (QRAM)



- Special gate that can be used to address data quantumly
- “One more dimension” in gate-based circuits
- Time cost of access:
  - $O(\sqrt{m})$ (“expensive”)
  - $O(1)$ (“cheap” assumption)

Universal methods

Method	Target	Time	Probability	QRAM
Q0 – Classical				
Bruteforce/guessing	key / preimage	2^k	$t_C/2^k$	–
ρ-Pollard	collision	$2^{n/2}$	$t_C^2/2^n$	–
Q1 – Quantum				
Grover	key / preimage	$2^{k/2}$	$t_Q^2/2^k$	–
Brassard-Høyer-Tapp	collision	$2^{n/3}$	$t_Q^2/2^{\frac{2}{3}n}$	$2^{n/3}$

... and others

PRP-security of Kuznyechik

Q0 – classical

$$\mathrm{Adv}^{PRP}_{\text{Kuznyechik}}(t_C, \sigma) \lessapprox \frac{t_C}{2^k}$$

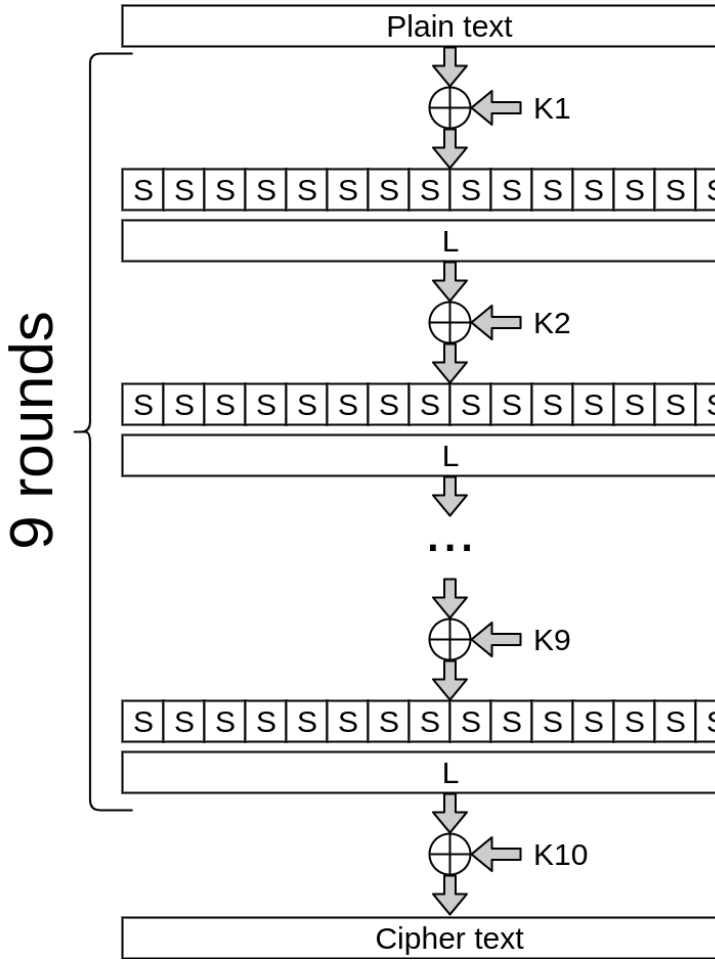
Q1 – quantum

$$\mathrm{Adv}^{PRP\text{-}Q1}_{\text{Kuznyechik}}(t_C, t_Q, \sigma) \lessapprox \frac{t_C}{2^k} + \frac{t_Q^2}{2^k}$$

t_C / t_Q – classical / quantum computation resources,

σ – number of adaptively chosen PT-CT pairs,

$k = 256$ – key bit length.



PRP-security of Magma

Q0 – classical

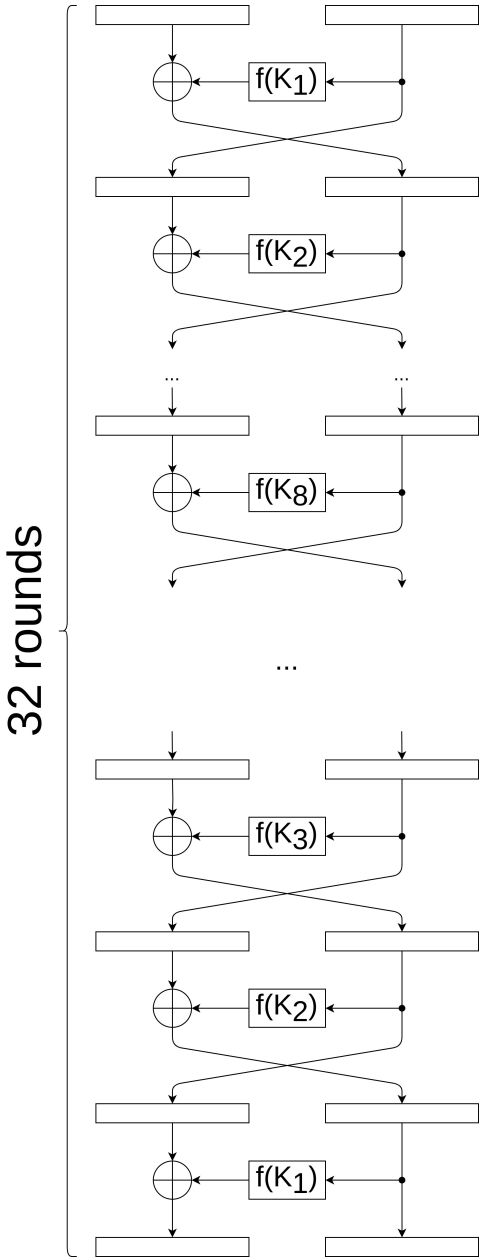
$$\mathrm{Adv}^{PRP}_{\mathrm{Magma}}(t_C, \sigma) \lessapprox \frac{t_C}{2^{192}} + \frac{\sigma}{2^{64}}$$

Q1 – quantum (No QRAM)

$$\mathrm{Adv}^{PRP\text{-}Q1}_{\mathrm{Magma}}(t_C, t_Q, \sigma) \lessapprox \frac{t_C}{2^{192}} + \frac{\sigma}{2^{64}} + \frac{t_Q^2}{2^{256}}$$

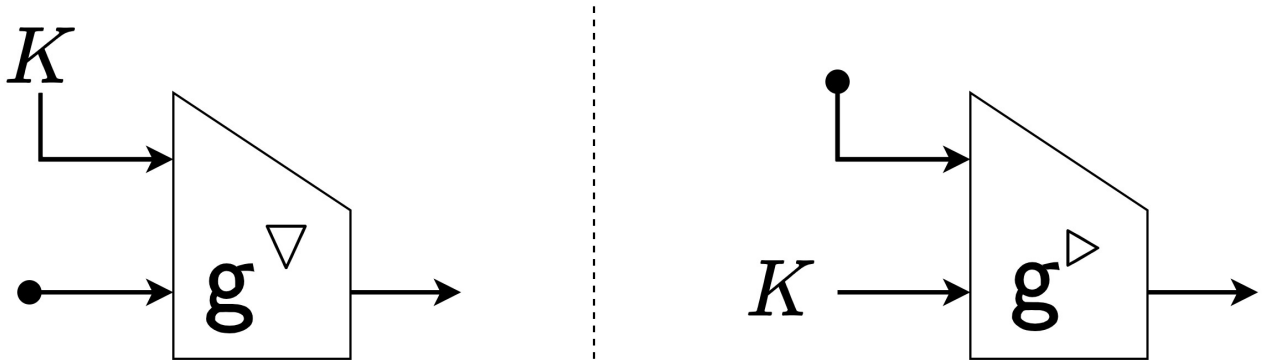
Q1 – quantum (huge cheap QRAM)

$$\mathrm{Adv}^{PRP\text{-}Q1}_{\mathrm{Magma}}(t_C, t_Q, \sigma) \lessapprox \frac{t_C}{2^{192}} + \frac{\sigma}{2^{64}} + \frac{t_Q^2}{2^{224}}$$



X. Dong, B. Dong, X. Wang – 2018
Quantum attacks on some Feistel block ciphers

PRF-security of Streebog compr. function



Q0 – classical

$$\mathrm{Adv}^{PRF}_{g^{\triangledown}}(t_C, \sigma) \lessapprox \frac{t_C}{2^k}, \qquad \mathrm{Adv}^{PRF}_{g^{\triangleright}}(t_C, \sigma) \lessapprox \frac{t_C}{2^k} + \frac{\sigma^2}{2^n},$$

Q1 – quantum

$$\mathrm{Adv}^{PRF\text{-}Q1}_{g^{\triangledown}}(t_C, t_Q, \sigma) \lessapprox \frac{t_C}{2^k} + \frac{t_Q^2}{2^k}, \qquad \mathrm{Adv}^{PRF\text{-}Q1}_{g^{\triangleright}}(t_C, t_Q, \sigma) \lessapprox \frac{t_C}{2^k} + \frac{t_Q^2}{2^k} + \frac{\sigma^2}{2^n},$$

$k \leq n = 512,$

Similar bounds for PRF-RKA (related key attack) notion.

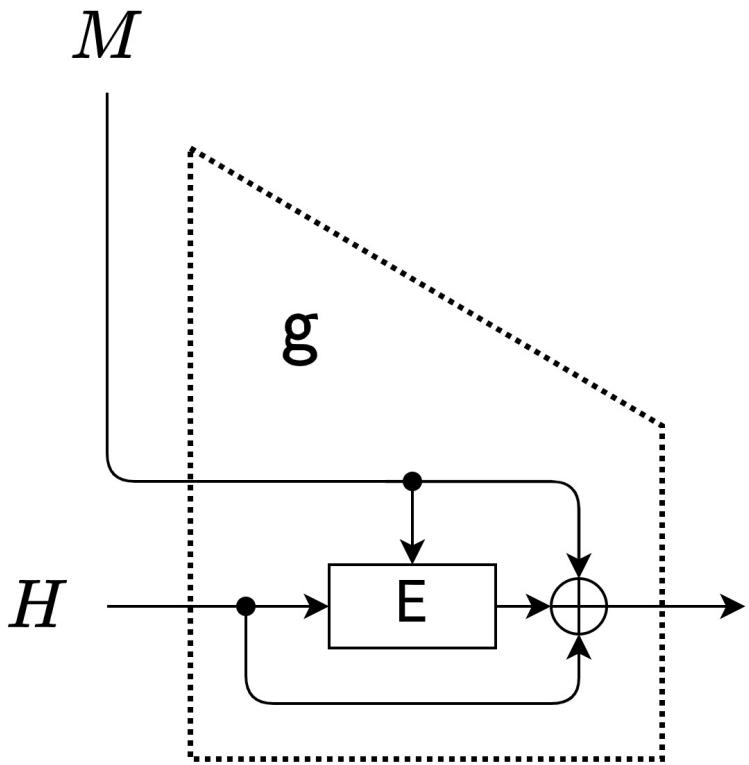
Preimage resistance: Streebog compr. function

Q0 – classical

$$\mathrm{Adv}_{\mathrm{g}}^{PRE}(t_C) \lessapprox \frac{t_C}{2^n}$$

Q1 – quantum

$$\mathrm{Adv}_{\mathrm{g}}^{PRE\text{-}Q1}(t_C, t_Q) \lessapprox \frac{t_C}{2^n} + \frac{t_Q^2}{2^n}$$



Collision resistance: Streebog compr. function

СФБ ЛАБ

Q0 – classical

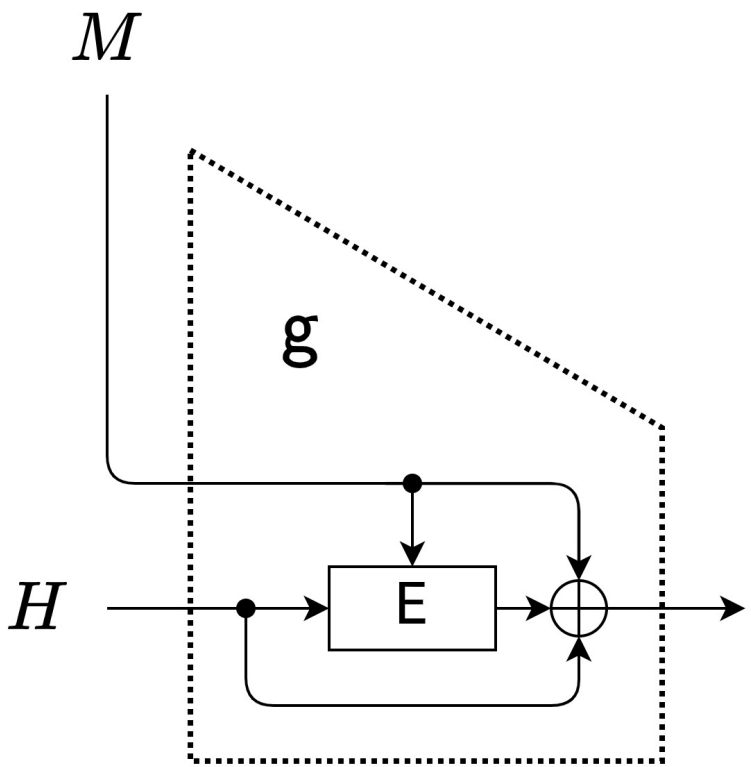
$$\mathrm{Adv}_{\mathrm{g}}^{CR}(t_C) \lessapprox \frac{t_C^2}{2^n}$$

Q1 – quantum (No QRAM)

$$\mathrm{Adv}_{\mathrm{g}}^{CR\text{-}Q1}(t_C, t_Q) \lessapprox \frac{t_C^2}{2^n}$$

Q1 – quantum (huge cheap QRAM)

$$\mathrm{Adv}_{\mathrm{g}}^{CR\text{-}Q1}(t_C, t_Q) \lessapprox \frac{t_C^2}{2^n} + \frac{t_Q^2}{2^{\frac{2n}{3}}}$$



Syndrome decoding of random linear code

Q0 – classical

$$\mathrm{Adv}^{SD}_{n,k,w}(t_C) \lessapprox \frac{t_C}{\binom{n}{w}/\binom{n-k}{w}}$$

Q1 – quantum

$$\mathrm{Adv}^{SD\text{-}Q1}_{n,k,w}(t_C, t_Q) \lessapprox \frac{t_C}{\binom{n}{w}/\binom{n-k}{w}} + \frac{t_Q^2}{\binom{n}{w}/\binom{n-k}{w}}$$

- n, k – code parameters
- w – error vector's weight

(assuming ISD is the best attack – classical due to [Prange, 1962]; quantum due to [Bernstein, 2010])

Special methods in quantum cryptanalysis

Special methods

~~Q0: Is it possible to do better than key guessing?~~

Q1: Is it possible to do better than Grover's algorithm (or other generic attacks)?

Example: AES-256 cryptanalysis in Q0

Rounds	Time	Data	Memory	Method
7	2^{172}	2^{34}	2^{32}	Square, 2000
7	2^{98}	2^{99}	2^{96}	MITM, 2013
8	2^{196}	2^{113}	2^{82}	MITM, 2013
9	2^{203}	2^{117}	2^{202}	MITM, 2020
14	2^{256}	3	–	key guessing

Bonnetain X., Naya-Plasencia M., Schrottenloher A. – FSE 2020

Quantum Security Analysis of AES

Example: AES-256 cryptanalysis in Q1

Rounds	Q. Time	Data	QRAM	Cl. Memory	Method
7	2^{111}	2^{37}	–	2^{36}	Square
7	2^{97}	2^{37}	2^{27}	2^{38}	Square
8	$2^{126.6}$	2^{113}	–	2^{88}	MITM
9	?	?	?	?	?
14	2^{128}	3	–	–	Grover

Bonnetain X., Naya-Plasencia M., Schrottenloher A. – FSE 2020

Quantum Security Analysis of AES

Example: Kuznyechik cryptanalysis in Q0

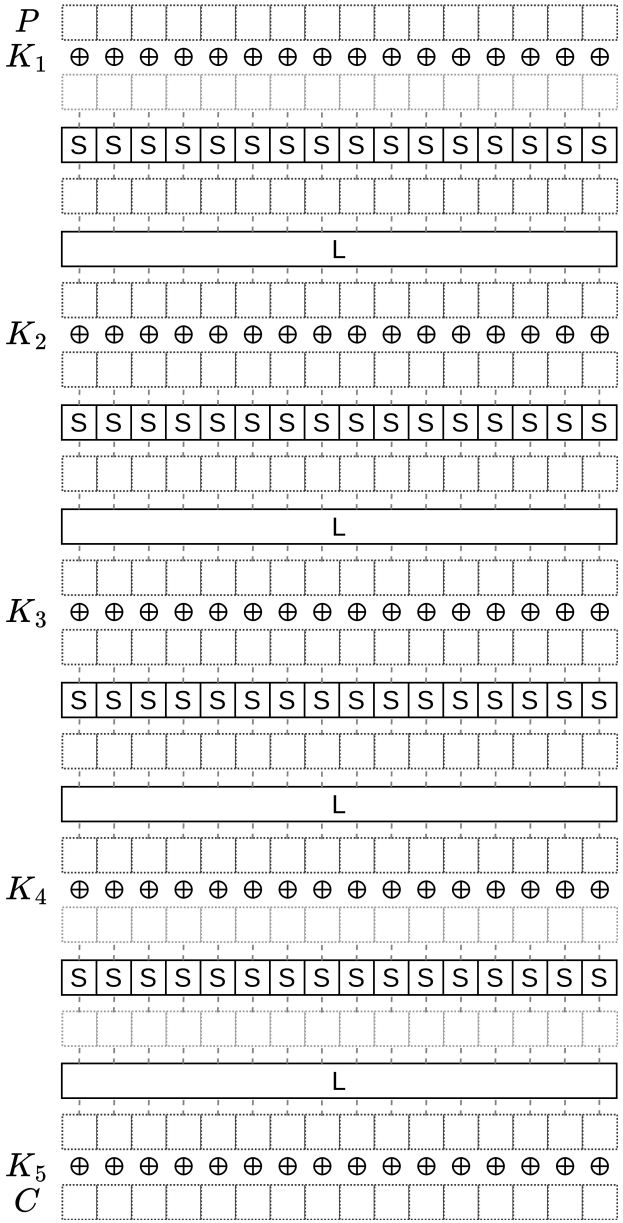
СФБ ЛАБ

Rounds	Time	Data	Memory	Method
4	2^{137}	2^{9}	2^{10}	Integral
4	2^{56}	2^{56}	2^{10}	Multiset-Algebraic
5	2^{120}	2^{120}	2^{10}	Multiset-Algebraic
5	2^{159}	2^{113}	2^{154}	MITM, 2018
6	2^{214}	2^{113}	2^{207}	MITM, 2018
6	2^{141}	2^{120}	2^{132}	Multiset-Algebraic + FFT, 2023
7	2^{148}	2^{128}	2^{140}	Multiset-Algebraic + FFT, 2023
9	2^{256}	3	–	key guessing

Quantum attack on 4-round Kuznyechik

$C = X[K_5]LSX[K_4]LSX[K_3]LSX[K_2]LSX[K_1](P)$

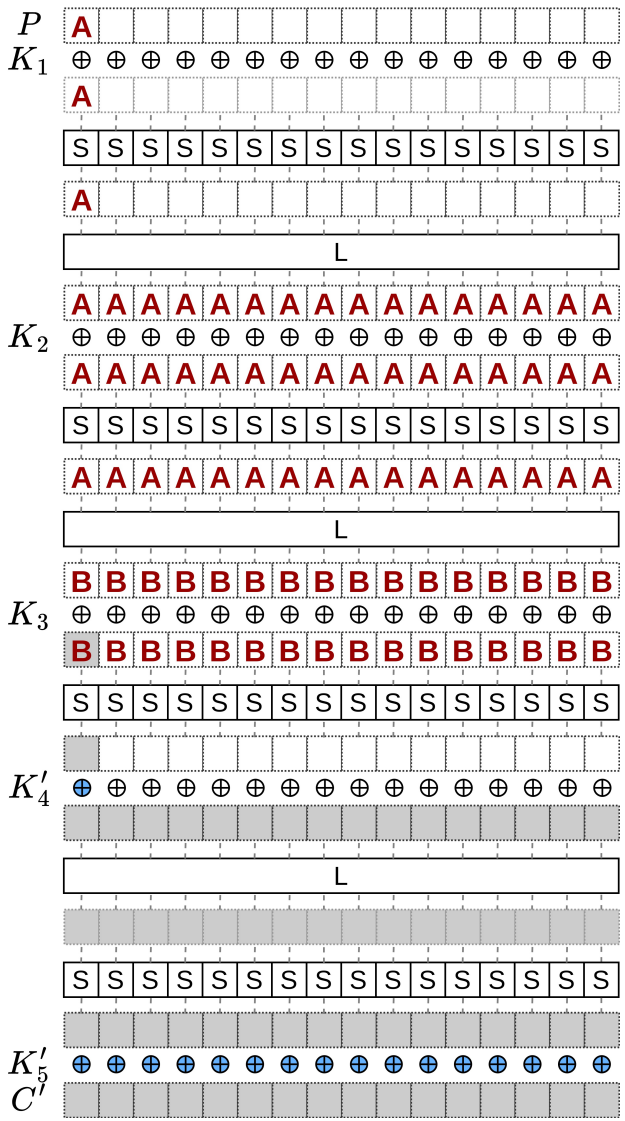
- 4 rounds (5 rounds keys)
- X – XOR with round key
- S – 16 byte S-boxes
- L – MDS matrix



Quantum attack on 4-round Kuznyechik

Classical integral attack:

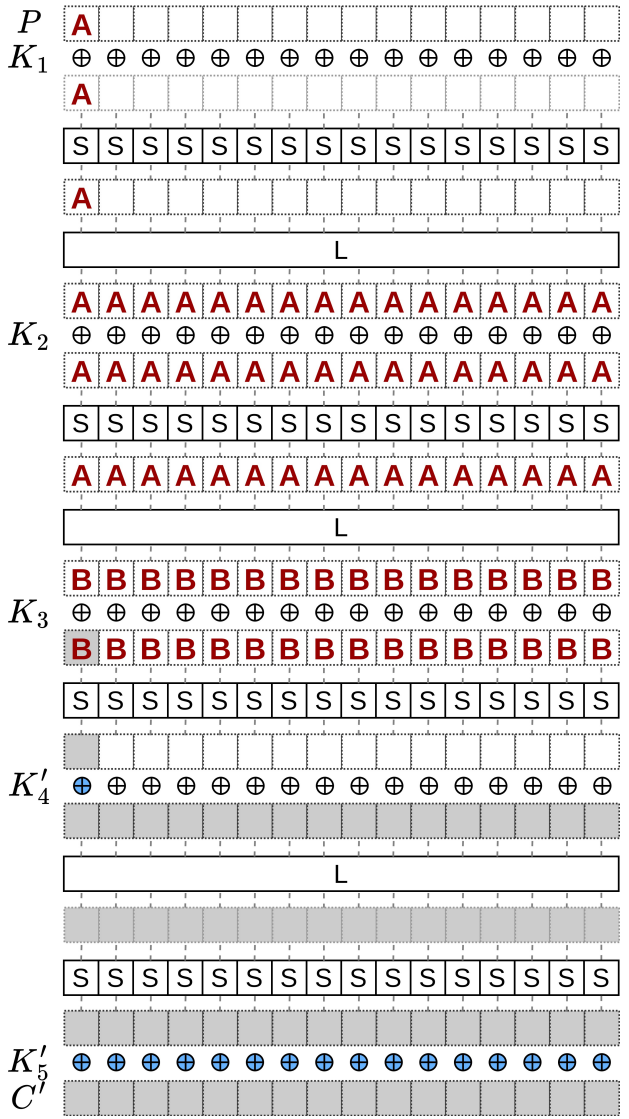
- Choose structure of 256 PT
- First byte in each PT is different (**A**)
- Sum of blocks after 3 round gives zero (**B**)
- Use equivalent representation of the last two rounds (swap X and L)
- Guess 136 bit: all K'_5 and one byte in K'_4
- Decrypt CT and check **B**-property for several structures



Quantum attack on 4-round Kuznyechik

Quantum integral attack:

- Use 18 structures ($256 \cdot 18$ PT)
- Compose an “oracle” F that gets 136 bits of keys and returns **True** if the **B**-property is true for all structures
- Without QRAM “oracle” F uses about $t_Q^F \approx \frac{1}{4} \cdot 256 \cdot 18 \cdot 2$ “encryptions”
- Use Grover’s algorithm for F, about $2^{136/2} = 2^{68}$ iterations
- Totally $t_Q \approx 2^{68} \cdot t_Q^F \approx 2^{79}$ “encryptions”



Quantum attack on 4-round Kuznyechik

"Naive" Grover's application gives $t_Q \approx 2^{128}$.

Classical method $t_C \approx 2^{136}$.

Proposed quantum integral attack $t_Q \approx 2^{80}$.

Open problem

How to attack more rounds of Kuznyechik with QC?

Example: Streebog block cipher cryptanalysis

Secret key setting. Key length = block length = 512 bit.

Rounds	Time	Data	Cl.Memory	QRAM	Method
Q0 – Classical					
6	2^{140}	2^{68}	2^{68}	–	integral
6.75	$2^{399.5}$	2^{483}	2^{349}	–	imp. diff., 2015
7	2^{421}	2^{64}	2^{354}	–	imp. polytopic, 2021
12	2^{512}	2	–	–	key guessing
Q1 – Quantum					
6	2^{104}	2^{68}	2^{68}	–	integral
12	2^{256}	2	–	–	Grover

Example: full-round Magma cryptanalysis

Rounds	Time	Data	Cl. Memory	QRAM	Method
Q0 – Classical					
32	2^{224}	2^{32}	2^{64}	–	Ref. points
32	2^{192}	2^{64}	2^{36}	–	Fix. points
32	2^{256}	5	–	–	key guessing
Q1 – Quantum					
32	2^{112}	2^{64}	2^{64}	2^{64}	Fix. points
32	2^{128}	5	–	–	Grover

X. Dong, B. Dong, X. Wang – 2018

Quantum attacks on some Feistel block ciphers

Thesis №3: quantum cryptanalysis

СФБ ЛАБ

Cryptanalysis in Q1

Non-trivial results can be achieved:

- better than Grover search;
- better than classical methods.

“Rule of thumb”

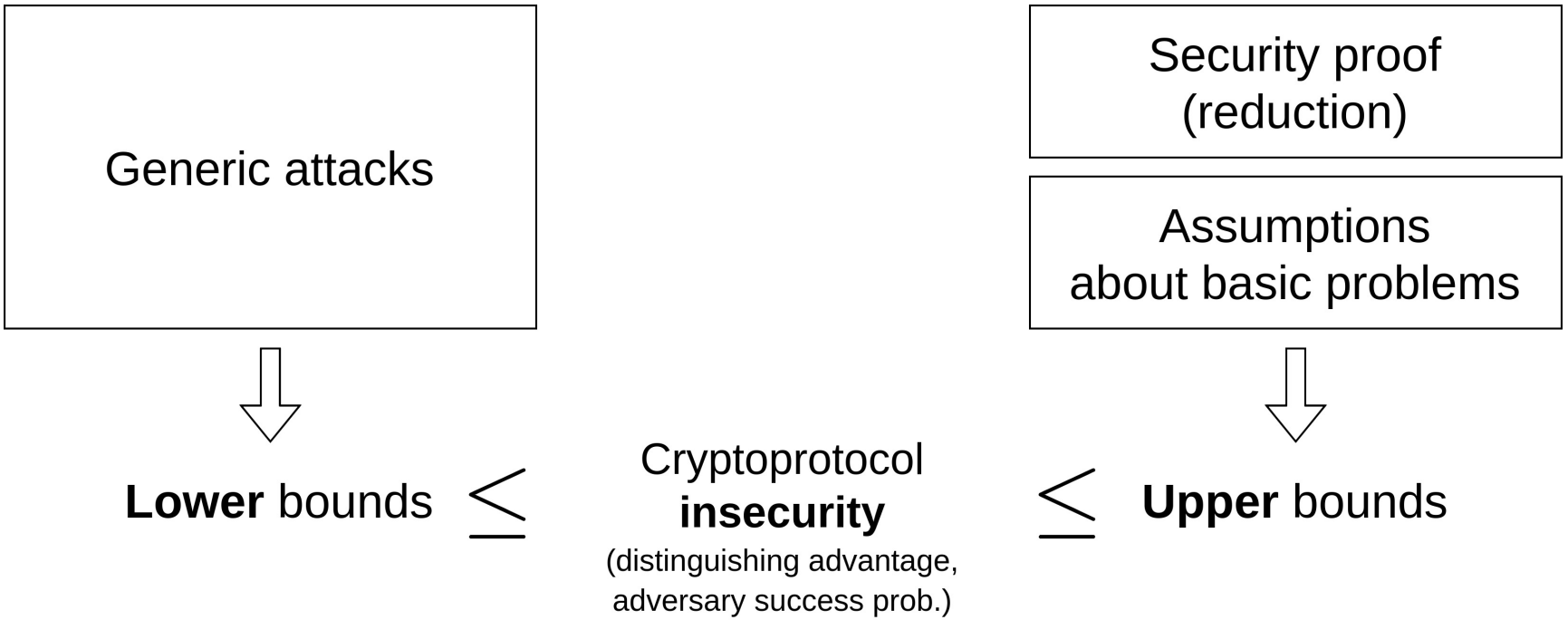
For symmetric cryptoalgorithms in Q1,

“non-trivial quantum attack” is *harder to construct* than

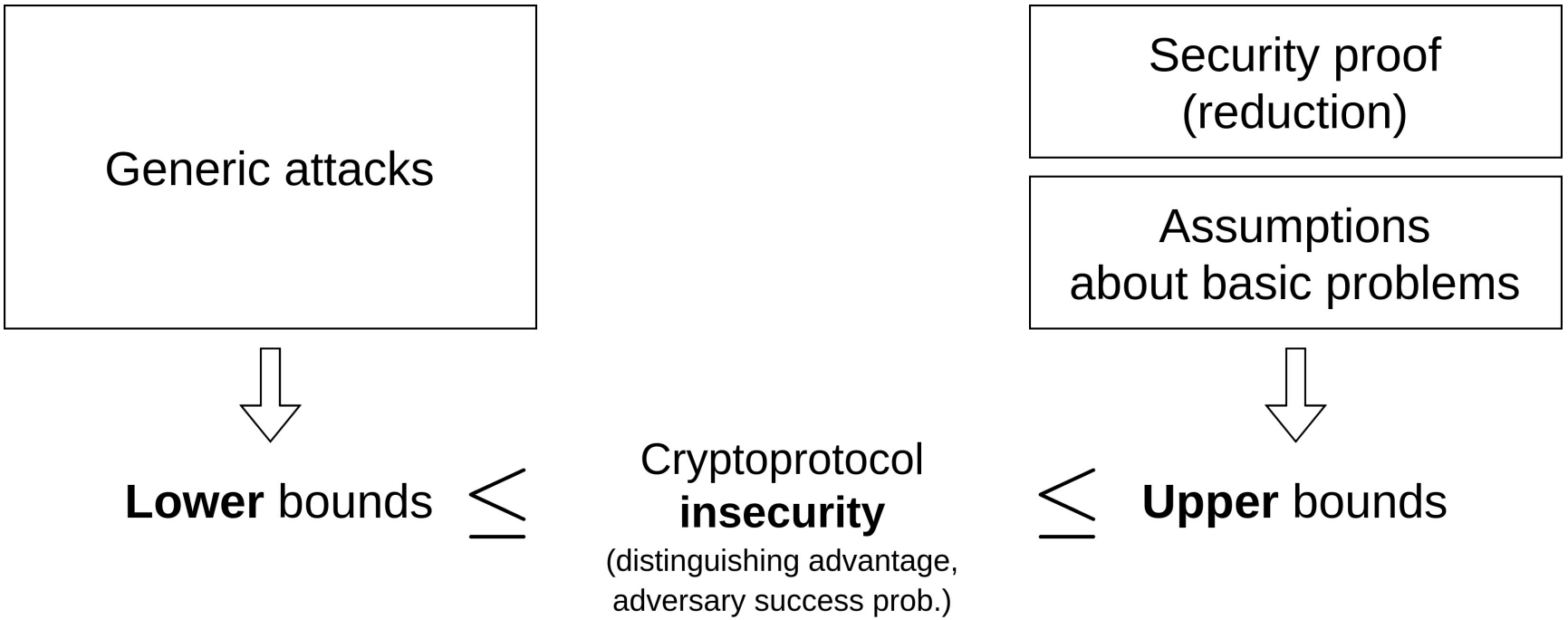
“non-trivial classical attack”.

Numerical estimates and untight bounds

Tightness of the security bounds

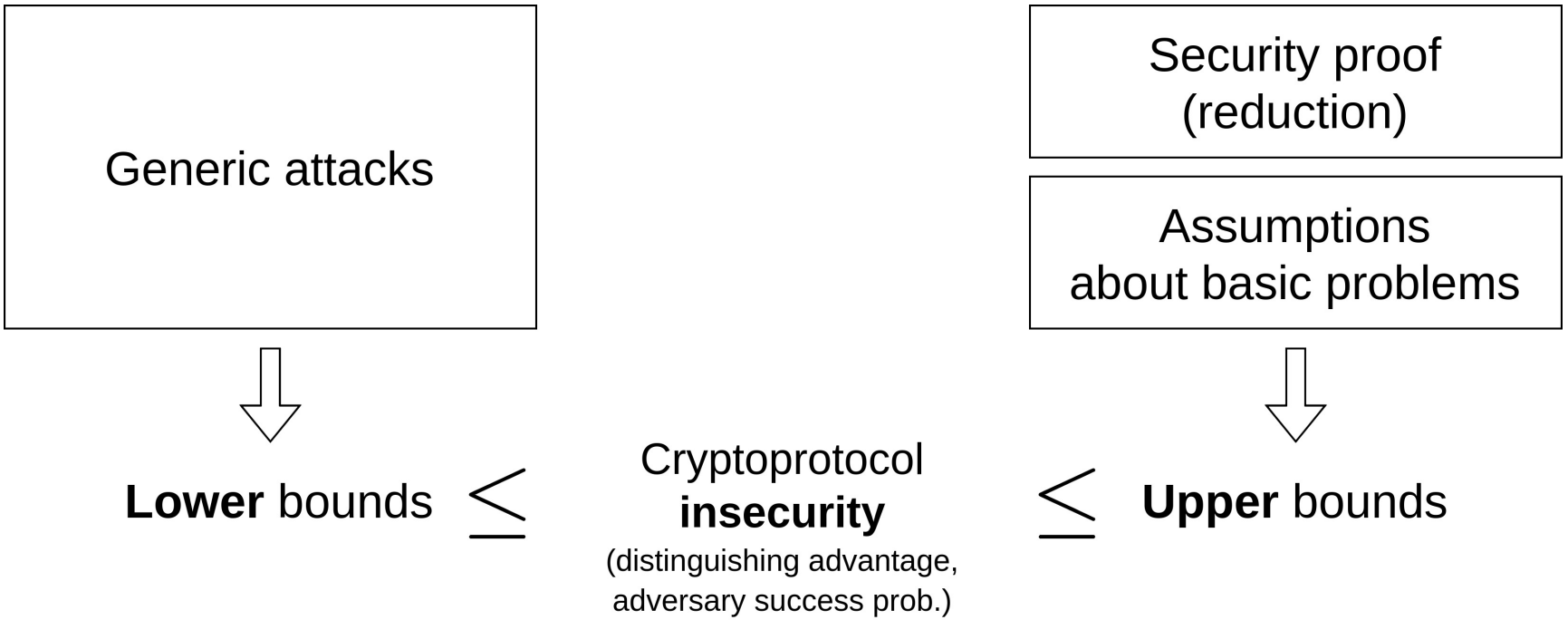


Tightness of the security bounds



Lower bounds ≈ Upper bounds ⇒ tightness

Tightness of the security bounds



Lower bounds ≈ Upper bounds ⇒ tightness

Proof adaptation from Q0 to Q1: tight bounds can become untight

Reason of untightness

The upper bound obtained using the “hybrid argument” (summand $N \cdot Adv(\ldots)$) may not be achieved by the generic multitarget attack.

Multitarget attacks

СФБ ЛАБ

Key recovery

μ independent k-bit secret keys $K_1,\ldots,K_\mu$, μ PT-CT pairs,

$$ciphertext_i = \mathrm{Enc}(K_i, plaintext),\ 1 \le i \le \mu.$$

Find at least one key from $K_1,\ldots,K_\mu$.

Preimage

μ random k-bit hash values $Y_1,\ldots,Y_\mu$.
Find (i, X):

$$\mathrm{Hash}(X) = Y_i,\ 1 \le i \le \mu.$$

Multitarget attacks

Probability of recovery of one (out of μ) keys

Q0	Q1	Q1	Q1
	No QRAM	costly QRAM	cheap QRAM
$\mu \cdot \frac{t_C}{2^k}$	$\frac{t_Q^2}{2^k}$	$\sqrt{\mu} \cdot \frac{t_Q^2}{2^k}$	$\mu \cdot \frac{t_Q^2}{2^k}$

Q0: The success probability is increased ***linearly*** by μ

Q1: It's more complicated and depends on QRAM

Example: CTR-ACPKM with Kuznyechik

Q0 – classical

$$\mathrm{Adv}^{\mathit{IND\text{-}CPNA}}_{\text{CTR-ACPKM}}(t_C, s, \sigma) \lessapprox s \cdot \frac{t_C}{2^k} + s \cdot \left(\frac{\sigma^2}{2^{n+1}}\right),$$

Q1 – quantum

$$\mathrm{Adv}^{\mathit{IND\text{-}CPNA\text{-}Q1}}_{\text{CTR-ACPKM}}(t_C, t_Q, s, \sigma) \lessapprox s \cdot \frac{t_C}{2^k} + s \cdot \frac{{t_Q}^2}{2^k} + s \cdot \frac{\sigma^2}{2^{n+1}},$$

t_C / t_Q – classical / quantum computation resources,

s sections of σ n-bit blocks each,

$k = 256$, $n = 128$.

Example: CTR-ACPKM

Attack	Lower bound	Upper bound
Recovery of one key from ACPKM key-chain	$s \cdot \frac{t_C}{2^k}$	$s \cdot \frac{t_C}{2^k}$
Absence of the birthday paradox in each of s sections	$s \cdot \frac{\sigma^2}{2^{n+1}}$	$s \cdot \frac{\sigma^2}{2^{n+1}}$
Grover's algorithm	$\frac{t_Q^2}{2^k}$	$s \cdot \frac{t_Q^2}{2^k}$

$\Rightarrow$ Tightness in Q0, but not in Q1.

Open problem

Is it possible to accelerate an attack
on the ACPKM keychain using QC even with "cheap QRAM"?

Example: Keyed Streebog

Q0 – classical

$$\mathrm{Adv}^{PRF}_{\text{Streebog-K}}(t_C, q, l) \lessapprox \frac{t_C}{2^k} + \frac{t_C \cdot q \cdot l}{2^{n-1}} + \frac{q^2 + q}{2^{n+1}}$$

Q1 – quantum

$$\mathrm{Adv}^{PRF\text{-}Q1}_{\text{Streebog-K}}(t_C, t_Q, q, l) \lessapprox \frac{t_C}{2^k} + \frac{t_C \cdot q \cdot l}{2^{n-1}} + \frac{q^2 + q}{2^{n+1}} + \frac{{t_Q}^2}{2^k} + \frac{{t_Q}^2 \cdot q \cdot l}{2^{n-1}}$$

t_C / t_Q – classical / quantum computation resources,
q – number of adaptively chosen messages ($q' = q + 1$),
ℓ – maximum length of the message (in n-bit blocks), $\ell' = l + 1$.

Thesis №4: heuristic estimates in Q1

- Due to the “hybrid argument”

  some security bounds become untight after proof adaptation.
- Tightness can be returned by:
  - new proofs (reductions) to other problems;
  - new generic quantum attacks.
- The key capacity estimates mostly remain the same

  (here, as always, we’re not talking

  about side channels and other “off-model” threats).

Q1 AND SECURITY PROOFS IN ROM

Reason for difficulty

Why doesn’t the “as for standard model“ adaptation work?

Example

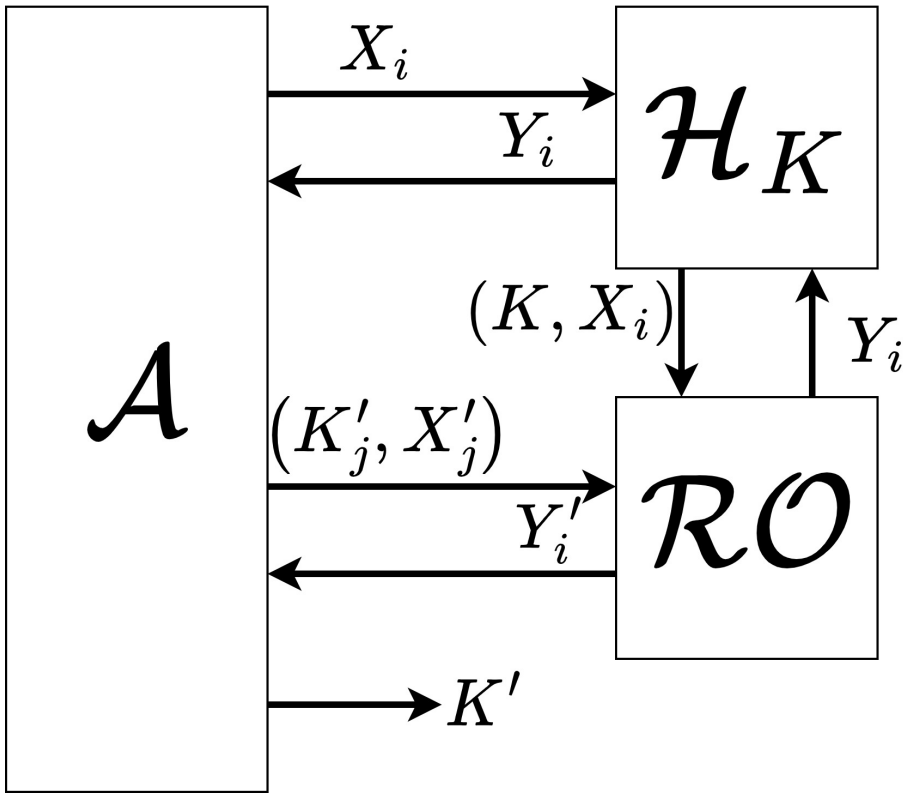
Adversary **A** has access to a keyed hash function $\mathbf{H}_K$ that is modelled as a Random Oracle **RO**.

q queries to $\mathbf{H}_K$.

t queries ("computations") to **RO**.

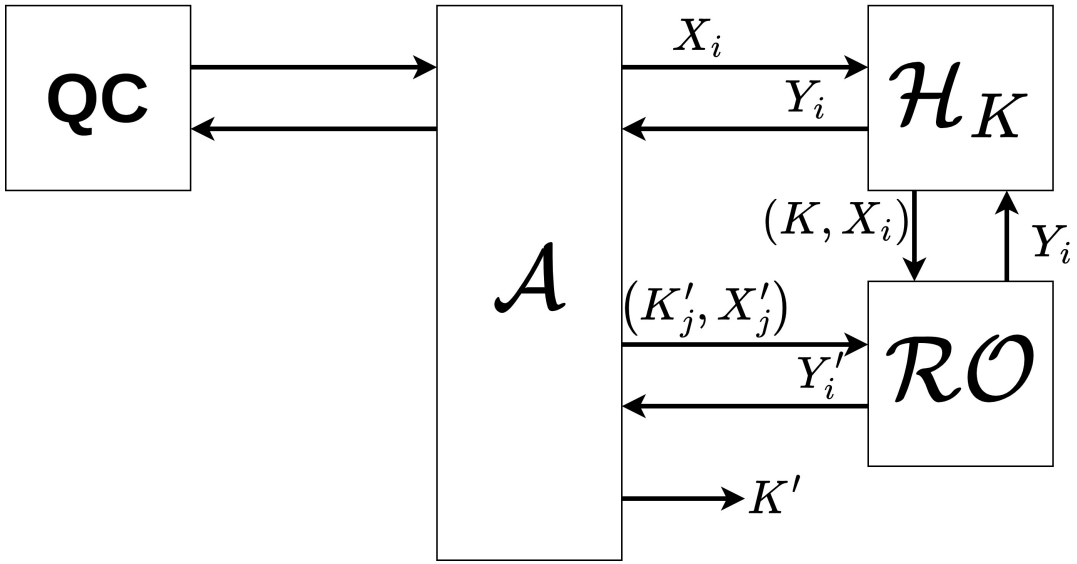
Goal: secret key K.

$$\Pr(K' = K) \leq \frac{t}{2^k}$$



Example

Let's go to quantum setting and give **A** access to **QC**.

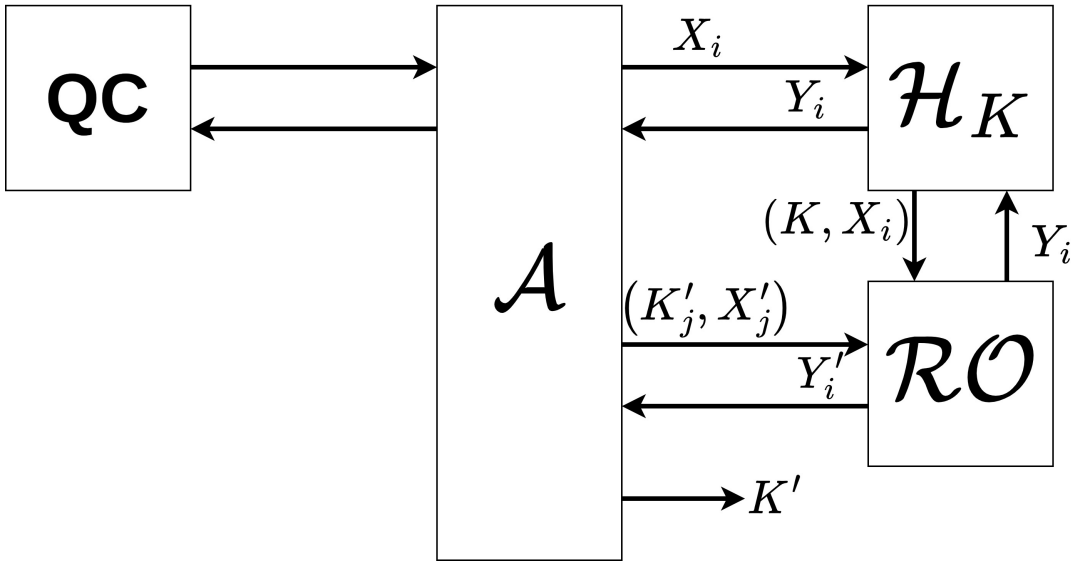


The adversary's probability of success has NOT changed.

The **RO**'s "description" cannot be used in **QC**.

Example

Let's go to quantum setting and give **A** access to **QC**.

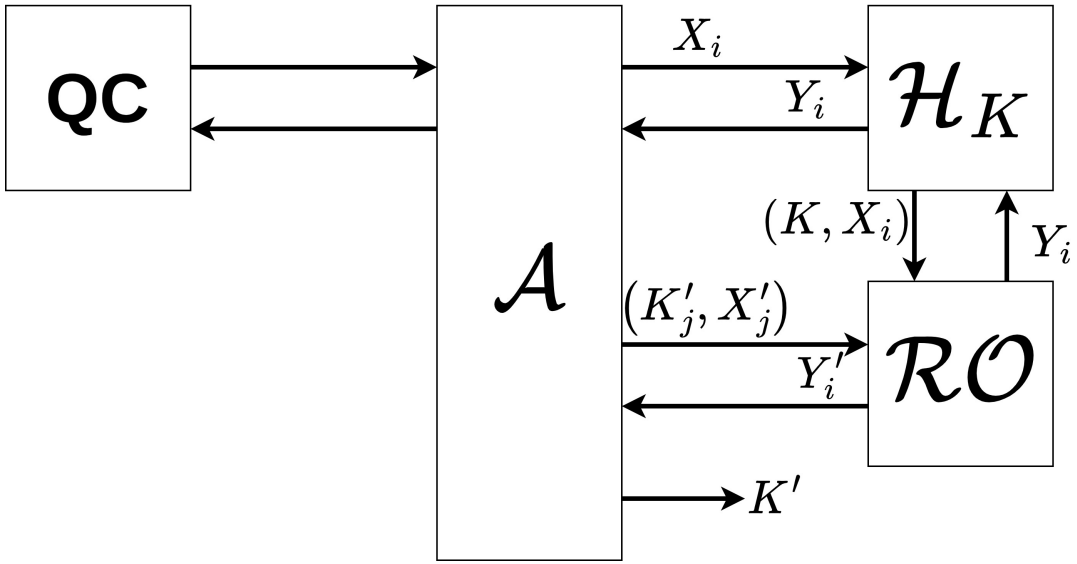


The adversary's probability of success has NOT changed.

The **RO**'s "description" cannot be used in **QC**. But **A** should get a quadratic speed up due to Grover's algorithm...

Example

Let's go to quantum setting and give **A** access to **QC**.



The adversary's probability of success has NOT changed.

The **RO**'s "description" cannot be used in **QC**. But **A** should get a quadratic speed up due to Grover's algorithm...

$\Rightarrow$ ROM is inadequate in Q1.

Security proofs in Random Oracle Model (ROM) can NOT be easily adapted to Q1.

From ROM to QROM

QROM – Quantum Random Oracle Model

Quantum adversary A can make **superposition** queries to **RO**.

Even **all** 2^N outputs can be computed after a *single* N-bit query.

QROM – Quantum Random Oracle Model

Quantum adversary A can make **superposition** queries to **RO**.

Even **all** 2^N outputs can be computed after a *single* N-bit query.

Most of the classical proof methods stop working.

Other special techniques have been developed over the last 15 years, but that's a different broad discussion.

Examples: secure crypto in QROM

СФБ ЛАБ

Fujisaki-Okamoto transform

"Weak" public-key encryption ⇒ secure KEM

K. Hövelmanns, E. Kiltz, S. Schage, D. Unruh. – PKC 2020

Generic Authenticated Key Exchange in the Quantum Random Oracle Model

... and many other papers.

Examples: secure crypto in QROM

СФБ ЛАБ

Fiat-Shamir transform

Three-round interactive proof ⇒ non-interactive proof

J.Don, S.Fehr, C.Majenz, C.Schaffner – CRYPTO 2019

Security of the Fiat-Shamir transformation in the quantum random-oracle model

... and many other papers.

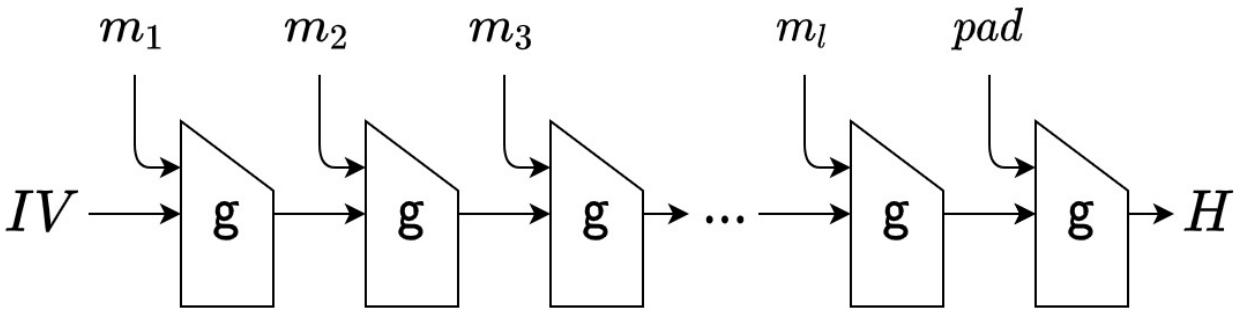
Can a real hash play the role of QROM?

СФБ ЛАБ

No real hash function can essentially implement a (quantum) ROM.

We can hope only on (quantum) ***indifferentiability*** under some other assumptions (“ideal cipher” or “ideal permutation” models).

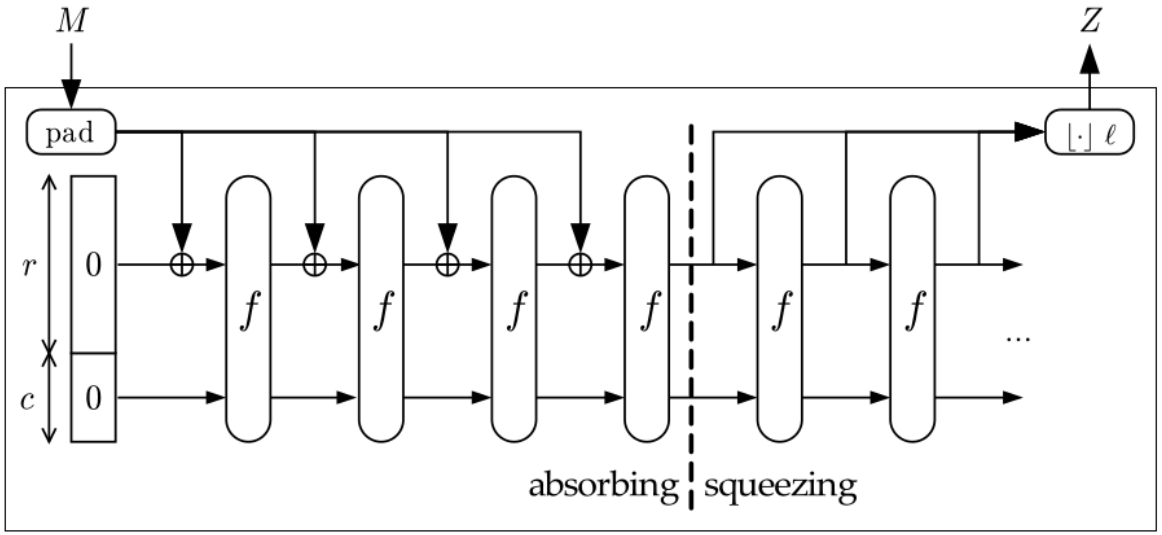
Quantum Indifferentiability: MD



M. Zhandry – CRYPTO 2019

How to Record Quantum Queries, and Applications to Quantum Indifferentiability

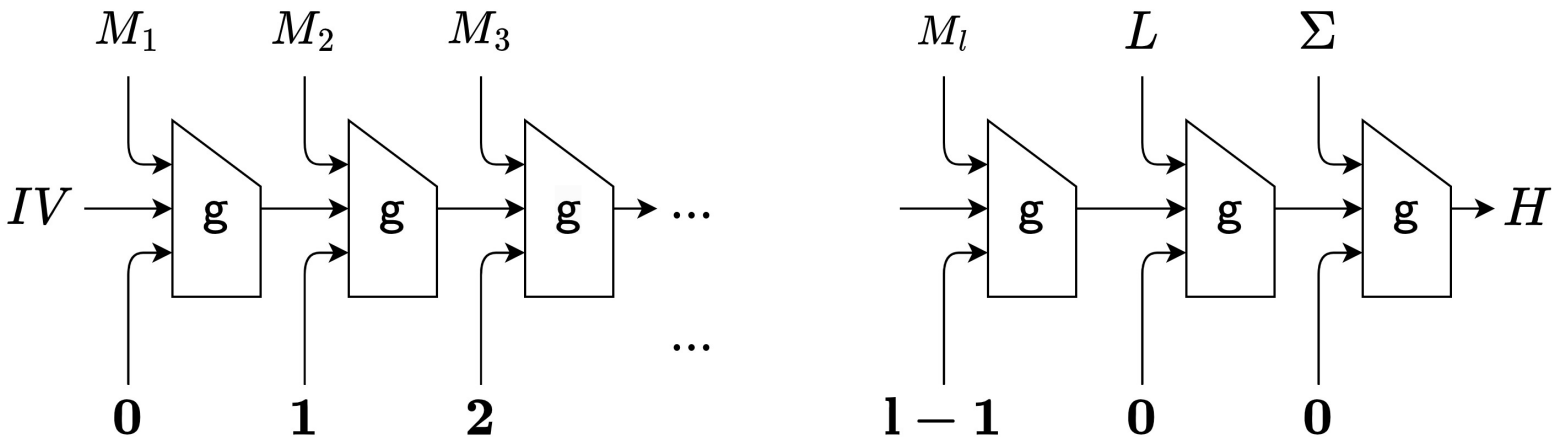
Quantum Indifferentiability: Sponge



G.Alagic, J.Carolan, C.Majenz, S.Tokat – 2025

The Sponge is Quantum Indifferentiable – 2025

Quantum Indifferentiability: Streebog?



Open problem

Streebog is proven to be indifferentiable from ROM under "ideal cipher" assumption [ABB23].
Prove the analogous for the quantum case (QROM).

[ABB23] L. R. Akhmetzyanova, A. A. Babueva, A. A. Bozhko

Streebog as a Random Oracle

CTCrypt 2023

Conclusion

- Q1 in the most adequate setting for “quantum threat”.

Conclusion

СФБ ЛАБ

- Q1 in the most adequate setting for “quantum threat”.
- Existing security proofs of cryptoalgorithms and protocols in the “Standard Model” (only through black-box reductions) can be easily adapted to Q1 setting.

Conclusion

- Q1 in the most adequate setting for “quantum threat”.
- Existing security proofs of cryptoalgorithms and protocols in the “Standard Model” (only through black-box reductions) can be easily adapted to Q1 setting.
- The numerical heuristic complexities of the basic problems should be re-evaluated for Q1.

Conclusion

- Revaluation should take into account both universal (i.e. Grover) and special methods of quantum cryptanalysis.

Conclusion

СФБ ЛАБ

- Revaluation should take into account both universal (i.e. Grover) and special methods of quantum cryptanalysis.
- Quantum cryptanalysis may give non-trivial results, but as “rule of thumb” for symmetric algorithms in Q1: “non-trivial quantum attack” means “non-trivial classical attack”.

Conclusion

- Revaluation should take into account both universal (i.e. Grover) and special methods of quantum cryptanalysis.
- Quantum cryptanalysis may give non-trivial results, but as “rule of thumb” for symmetric algorithms in Q1: “non-trivial quantum attack” means “non-trivial classical attack”.
- The key capacity estimates for protocols and modes mostly remain the same, but some security bounds become untight.

Conclusion

СФБ ЛАБ

- Revaluation should take into account both universal (i.e. Grover) and special methods of quantum cryptanalysis.
- Quantum cryptanalysis may give non-trivial results, but as “rule of thumb” for symmetric algorithms in Q1: “non-trivial quantum attack” means “non-trivial classical attack”.
- The key capacity estimates for protocols and modes mostly remain the same, but some security bounds become untight.
- Existing security results in “Random Oracle Model” should be reformulated from scratch in “Quantum ROM”, but a lot of the results and tools already exist.

Thank you for attention!
Questions?

Vitaly Kiryukhin,
Anton Naumenko,
Andrey Shcherbachenko
LLC “SFB Lab”, JSC “InfoTeCS”

CTCrypt 2025
4 June 2025