Cryptographical Security in the Quantum Random Oracle Model

Tommaso Gagliardoni

Center for Advanced Security Research Darmstadt (CASED) - TU Darmstadt, Germany

June, 21st, 2012

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.

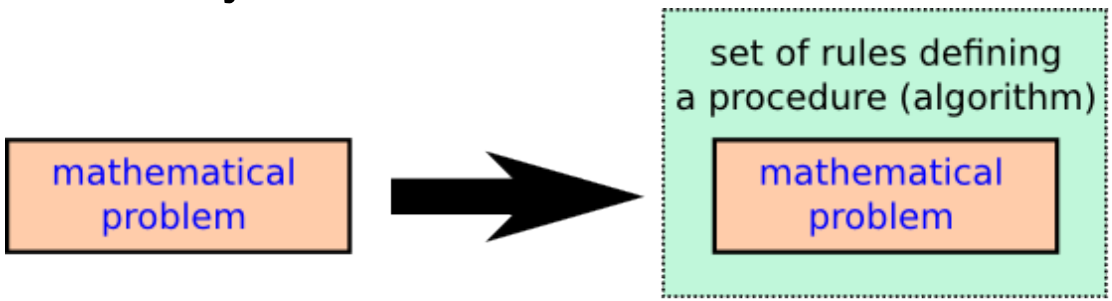
Cryptography

Purposes:

- secrecy of information exchanged via insecure channels
- authentication of entities accessing valuable data
- integrity of messages
- much more (signatures, commitment, zero-knowledge, ...)

Many different classifications (symmetric/asymmetric key, homomorphic, quantum, steganography, ...)

Usually a common construction scheme



Cryptographical Protocol

Example: RSA

Mathematical problem

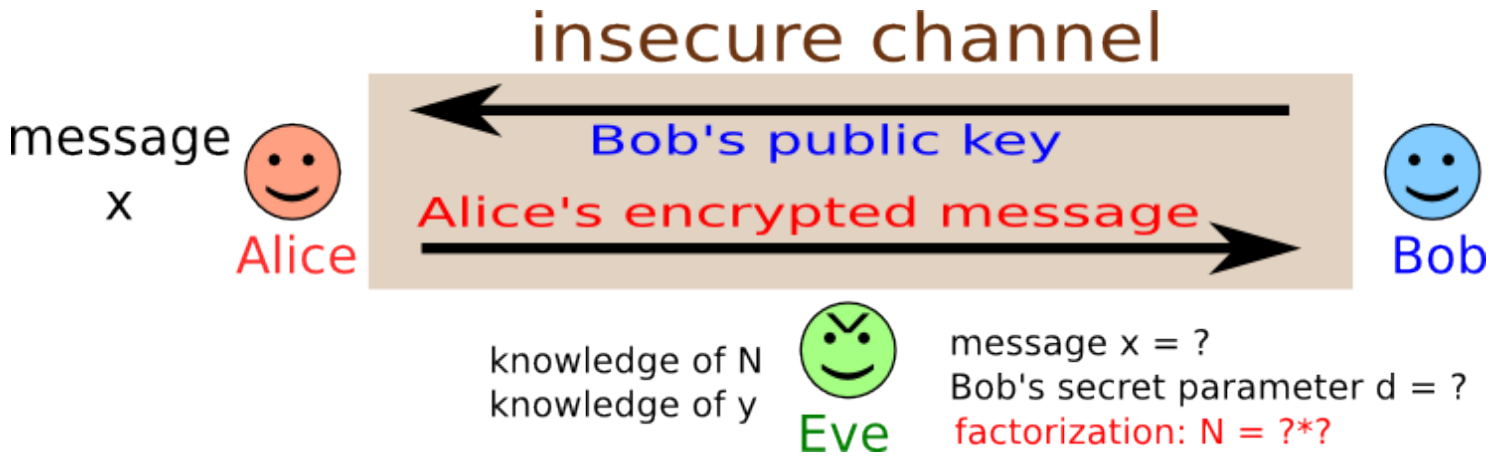
factorization of a number $N = p * q$ which is the product of two large primes

(simplified) RSA encryption scheme

- key generation: generate large primes p, q, set $N = pq$, compute $d = 3^{-1} \mod (p-1)(q-1)$. Public key is the pair $(N, 3)$, private key is the pair (N, d).
- message encryption: to encrypt message $x \in \mathbb{Z}_N$, set cyphertext $y = x^3 \mod N$
- message decryption: to decrypt cyphertext y, perform $x = y^d \mod N$

RSA security

All the operations are 'easy' to compute for honest parties Alice and Bob



NOTICE TWO ASSUMPTIONS:

- Eve is unable to efficiently factorize large integers
- the only way to efficiently recover d is by factoring N

Assumptions in the classical world

Crypto scheme secure $\Rightarrow$ computationally secure $\Rightarrow$
$\Rightarrow$ mathematical problem is (classically) hard to solve

Quantum computer solves efficiently certain problems $\Rightarrow$
$\Rightarrow$ some schemes become insecure

Assumptions in the quantum world

In the Quantum scenario we want problems that are hard to solve even on a quantum computer, and then build quantum-secure crypto schemes from those problems.

Some examples:

- lattice-based problems
- hash-based cryptography
- linear codes
- multivariate cryptography

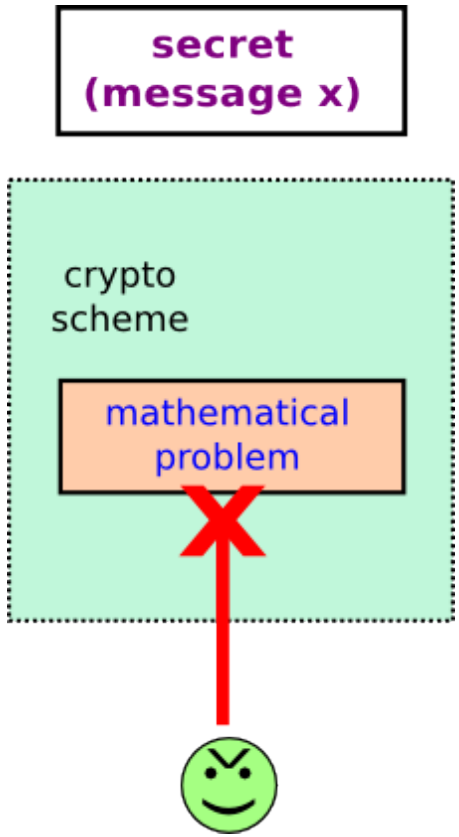
Post-quantum cryptography = classical, quantum-resistant

Computational security

Back to the classical world...

We are assuming that the only way to break the protocol is to solve the difficult underlying problem: the scheme is secure because Eve has not enough computational power.

Security of the mathematical problem $\Rightarrow$ security of the scheme

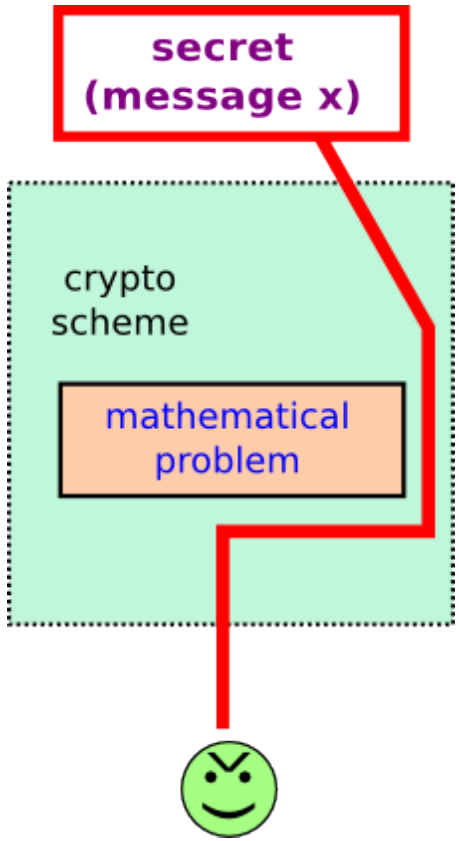


Is this really the case?

Provable security

Not always true!!!

If the scheme itself is not well designed, there could be 'workarounds' allowing an attacker to break the security WITHOUT actually attacking the hard problem.

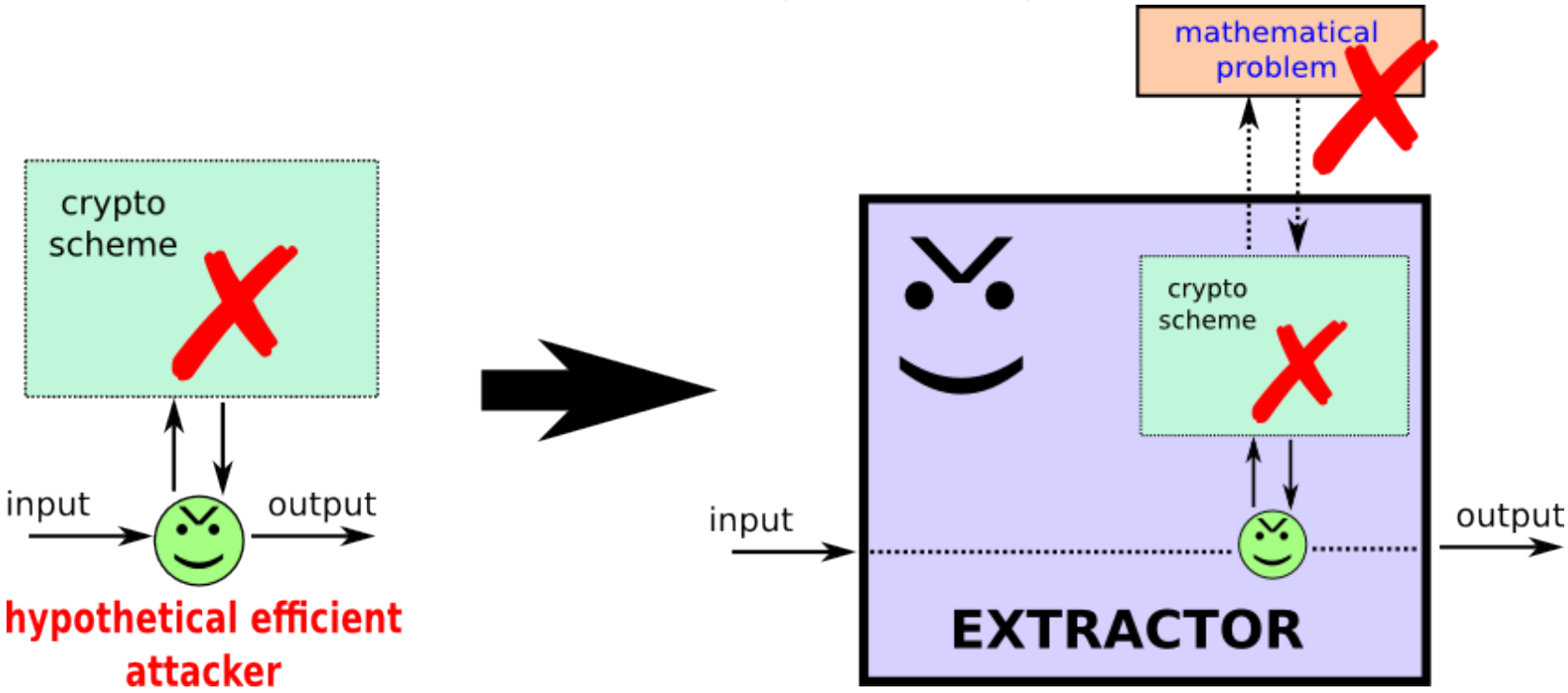


Security of the mathematical problem $\not\Rightarrow$ security of the scheme

PROVABLE SECURITY: formally prove that a scheme is at least as secure as its 'building block'

Reductions

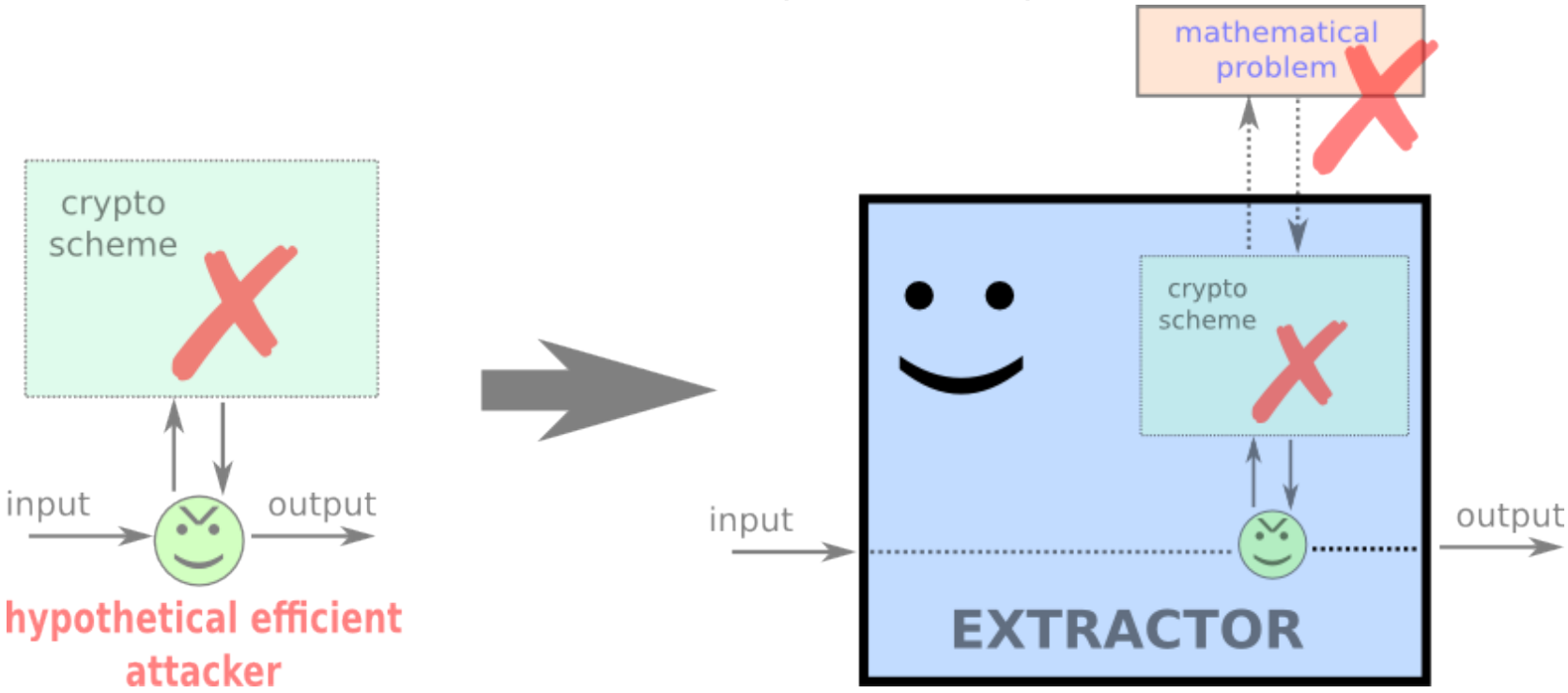
Proving equivalence between scheme and problem via an extractor (simulator)



Scheme is secure (relatively to basic computational hardness assumption) $\iff$ an extractor exists

Reductions

Proving equivalence between scheme and problem via an extractor (simulator)



Notice that the extractor is the good guy!!!
(existence of an extractor = good for the scheme)

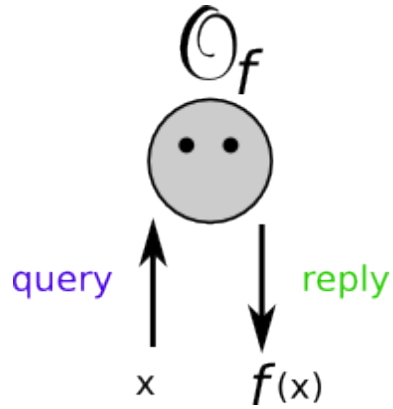
Random Oracle Model (ROM)

Hash function $H : \{0,1\}^n \mapsto \{0,1\}^m$ such that:

- it is easy to compute $H(x), \forall x$
- given y, it is hard to find x such that $H(x) = y$
- it is hard to find x_1, x_2 such that $H(x_1) = H(x_2)$

Random function: f chosen randomly amongst all possible $\{F : \{0,1\}^n \mapsto \{0,1\}^m\} \equiv$ ideal hash function

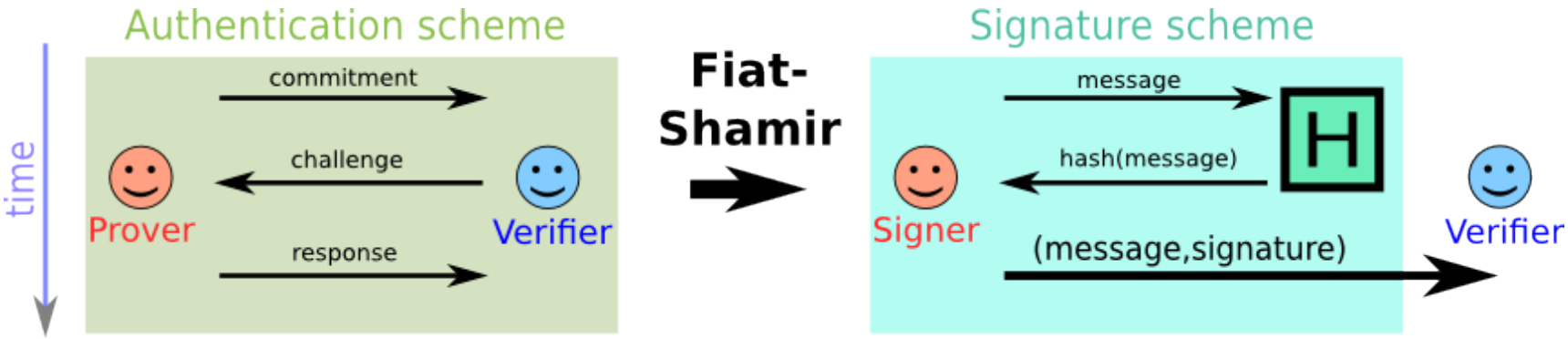
Random oracle: computational oracle for a certain random function



Often used to make extractions easier.
Reasonable model? (instantiation issues)

Example: Fiat-Shamir

Fiat-Shamir heuristics: protocol to transform any 3-steps interactive authentication scheme (Σ-protocol) into a digital signature scheme through the use of an hash function.



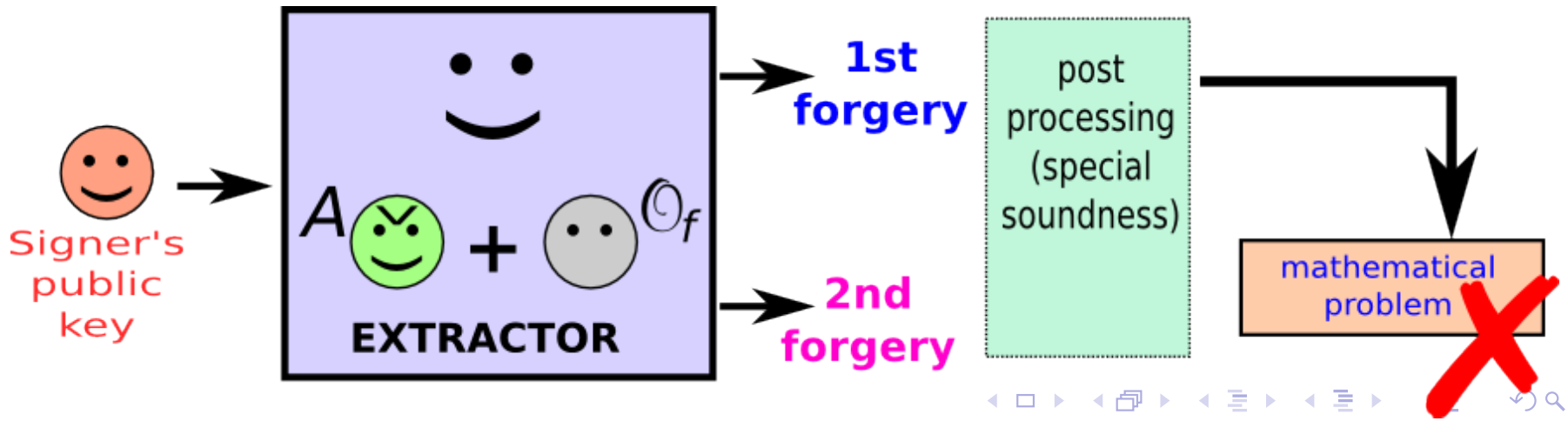
Special soundness

Given two transactions $(com, ch, res), (com, ch', res')$ with $ch \neq ch'$, it is possible to efficiently extract a witness (break the underlying mathematical problem).

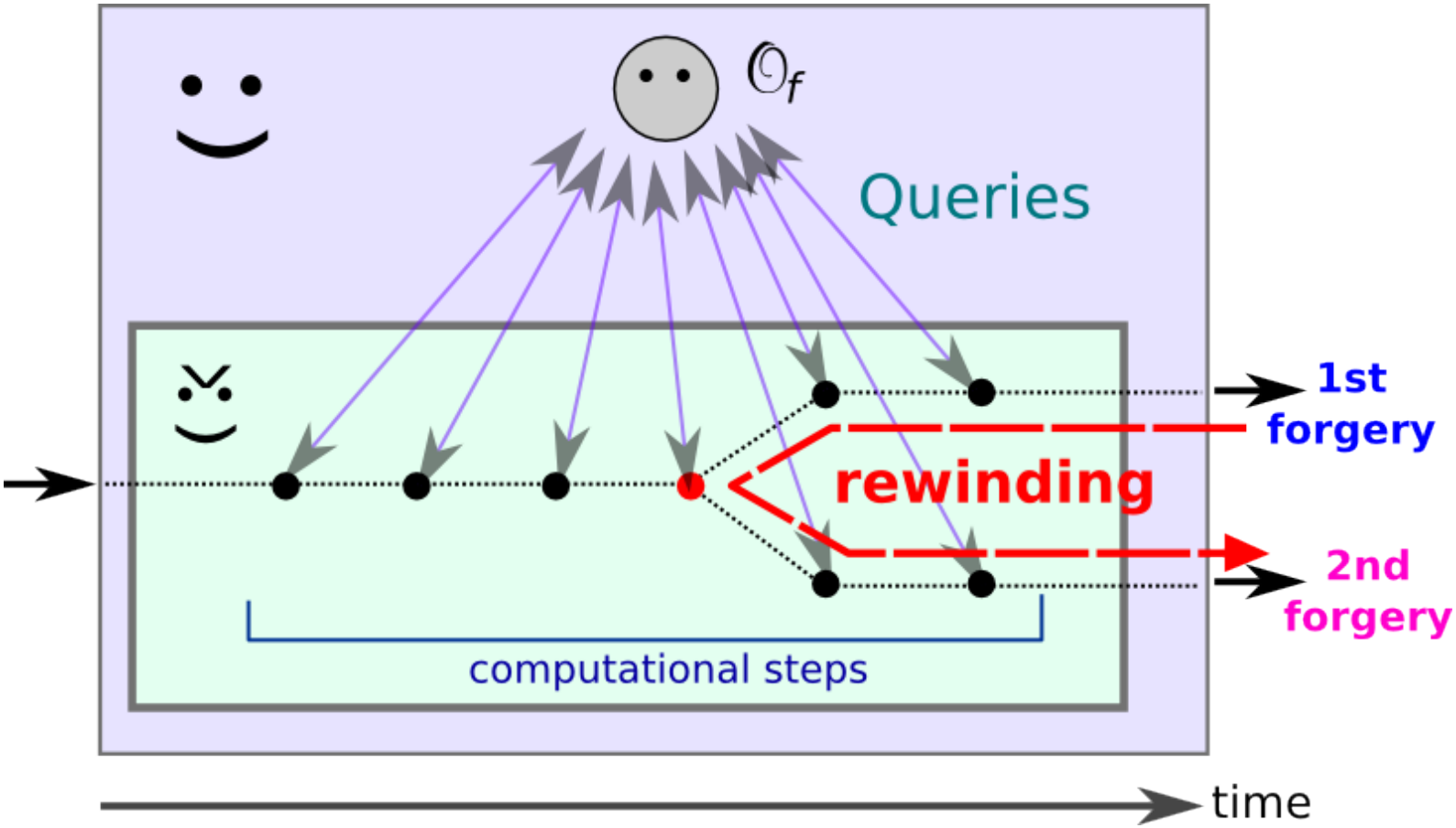
Example: Fiat-Shamir

Let's assume that an efficient attacker A exists for a Fiat-Shamir-based signature scheme. I.e.: given a publick key as an input, A is able to find a forgery for an arbitrary message in polynomial time with high probability.

Proof of security (for the signature scheme): through the use of an extractor which exploits the special soundness in the ROM by finding two different but related signatures for the same message.



Example: Fiat-Shamir

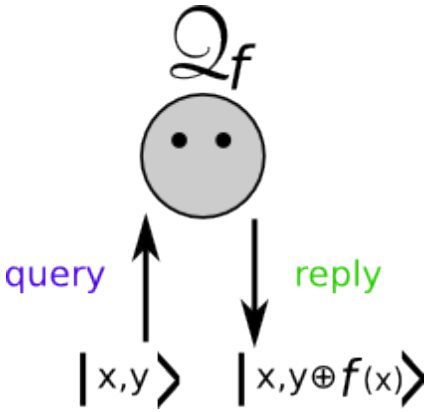


Forking lemma

If A succeeds once, it will probably succeed again with a small time overhead. Furthermore, the two forgeries will be related with good probability.

Quantum Random Oracle Model (QROM)

Quantum Random Oracle



An attacker in the quantum random oracle model (QROM) can ask queries in superposition

Is the attacker more powerful?

Security in the QROM

Problem: in the QROM many of the techniques we use for reduction don't usually work

- 'let's save the current state of the attacker...'
- 'let's perform operation U over two copies of the variable...'
- 'after we got the result, let's rewind the state of the attacker at point...'
- 'query after query, let's build a table with all the outcomes...'

Forking Lemma doesn't work.

Could it be the case that the security model is equivalent but we just don't know the right techniques yet?

Separation results

Classical security proofs do not imply security in the QROM, even if the mathematical problem is quantum resistant

D. Boneh, O. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, M. Zhandry.
Random Oracles in a Quantum World.
arXiv:1008.0931v2

Conclusions

- a cryptographical protocol is built upon a basic mathematical problem
- assumptions on the hardness of the problem are necessary but not sufficient for the security of the scheme
- in order to prove security we need formal proofs: to break the scheme is equivalent to solve the problem (ROM)
- in the quantum world we need new problems to have post-quantum cryptography
- many of the techniques we use for formal proofs in the classical world fail in the quantum world
- there exist examples of schemes which are provably secure in the ROM but unsecure in the QROM

End of this talk

Thanks for the attention!

tommaso[AT]gagliardoni[DOT]net