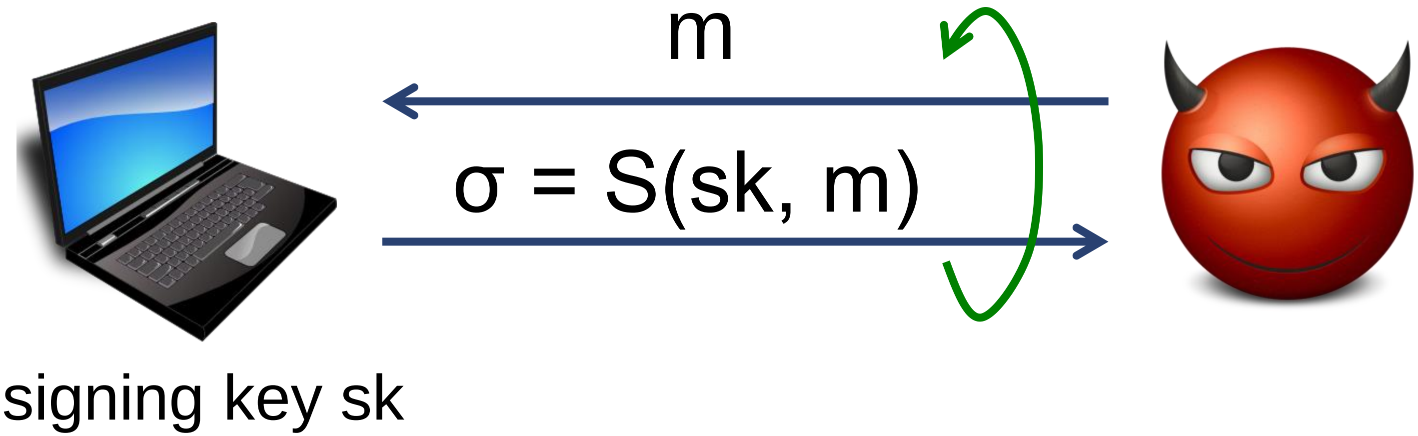
Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World

Dan Boneh and **Mark Zhandry**

Stanford University

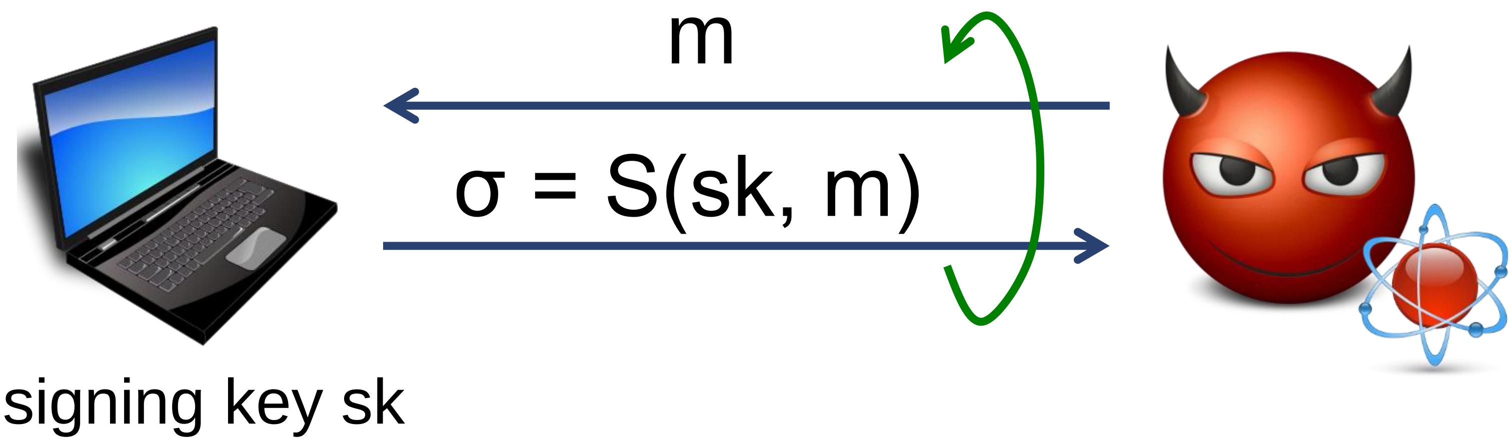
Classical Chosen Message Attack (CMA)



Classical CMA + Quantum Computer

(post-quantum CMA)

Adversary has **quantum** computing power:

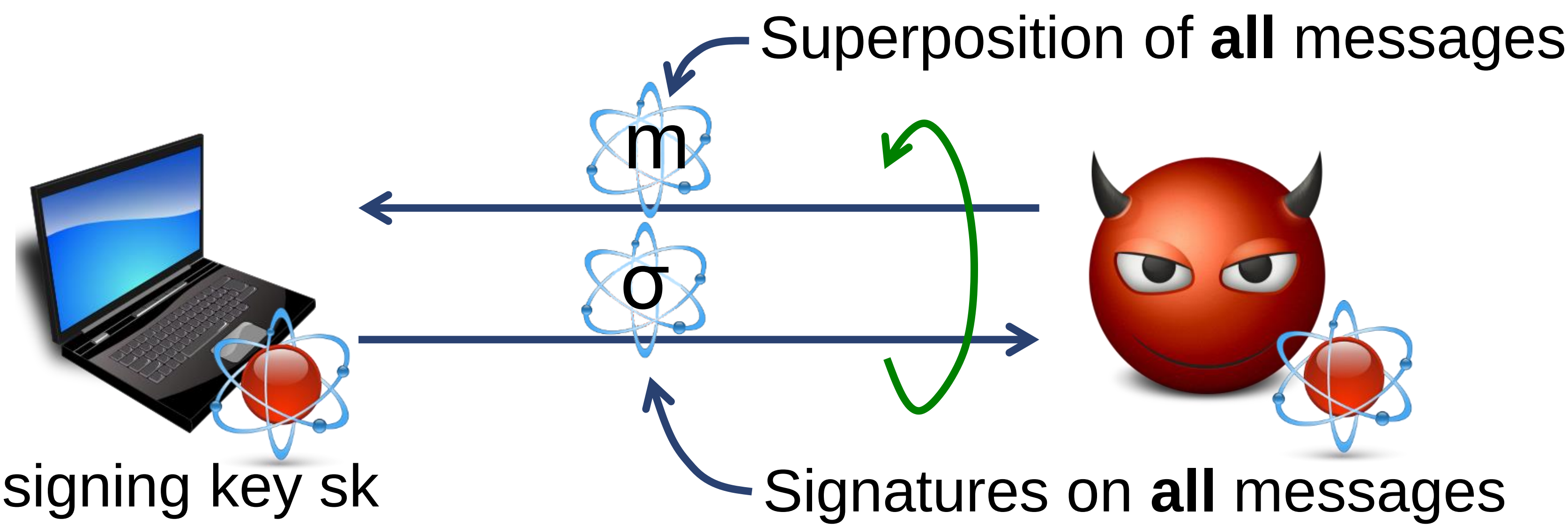


Interactions remain **classical**

⇒ classical proofs often carry through

This Talk: Quantum CMA

Everyone is quantum ⇒ **quantum queries**



Quantum interactions ⇒ need **quantum** proofs

Extends [BDFLSZ'11, DFNS'11, Z'12a, Z'12b, BZ'13a]

An Emerging Field

Many classical security games have quantum analogs:

- Quantum secret sharing, zero knowledge [DFNS'11]
- Quantum-secure PRFs [Z'12b]
- Quantum CMA for MACs [BZ'13a]
- Quantum-secure non-malleable commitments ???
- Quantum-secure IBE, ABE, FE ???
- Quantum-secure identification protocols ???

Motivation

Quantum world ⇒ unforeseen exotic attacks?

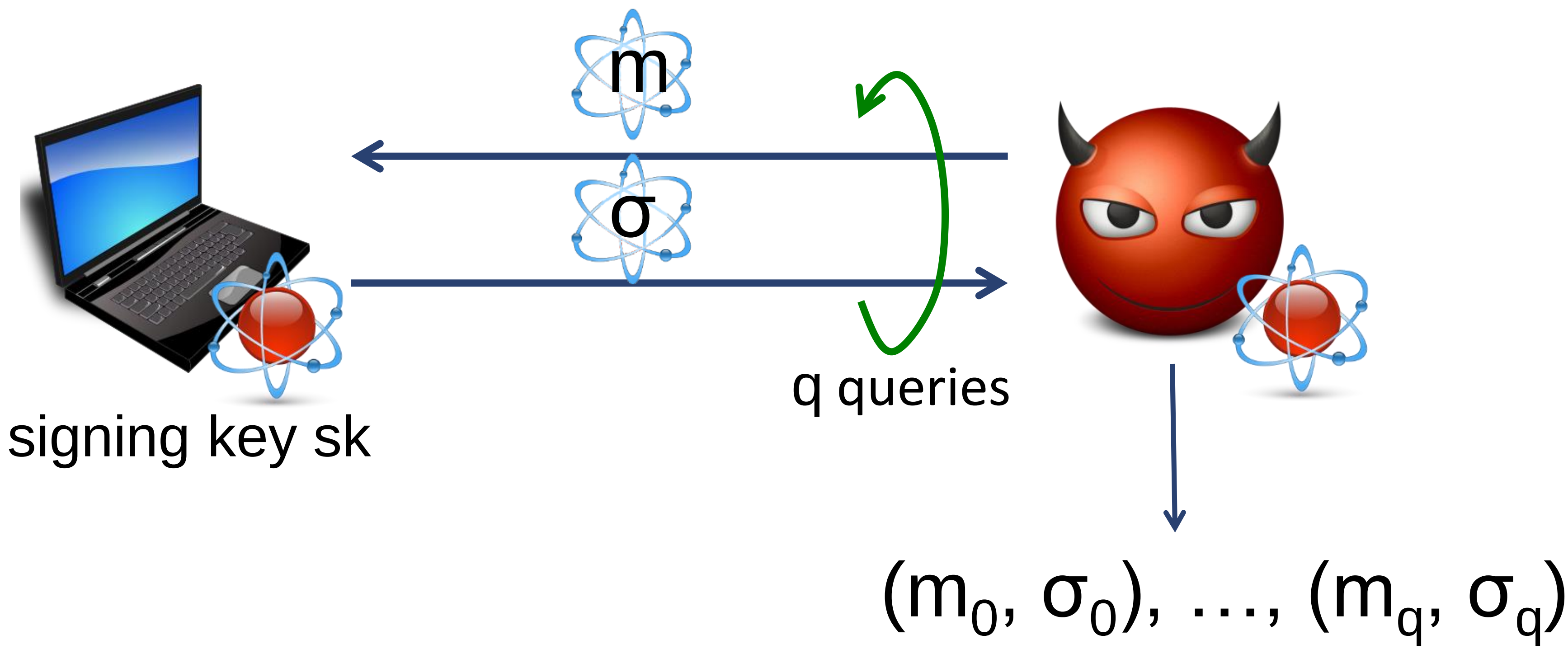
- Use most conservative model

Objection: can always "classicalize" queries

- Burden on hardware designer
- What if adversary can bypass?

Quantum-secure crypto: no need to classicalize

Quantum Security: Signature Definition



Existential forgery:

q quantum queries ⇒ **q+1** (distinct) signatures

Building Quantum-Secure Signatures

Separation:

Theorem: ∃classical CMA secure schemes that are not quantum CMA secure

Difficulties in proving quantum security:

- Aborts seem problematic
- Reduction must sign entire superposition correctly
- Existing proof techniques [Z'12b, BZ'13a] leave query intact
  - Known limitations in quantum setting:
    - MPC [DFNS'11]
    - Fiat-Shamir in QROM [DFG'13]
  - Cannot prove security for unique signatures (Ex: Lamport)

Building Quantum-Secure Signatures

First attempt: do classical constructions work?

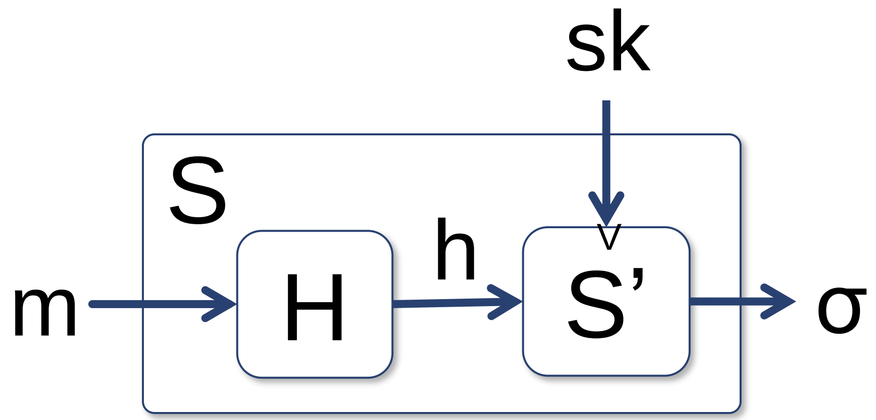
Examples:

- From lattices [CHKP’10, ABB’10]
- Using random oracles [BR’93, GPV’08]
- From generic assumptions [Rom’90]

Short answer: sometimes yes, with small modifications

Hash and Sign

Many classical signature schemes hash before signing:



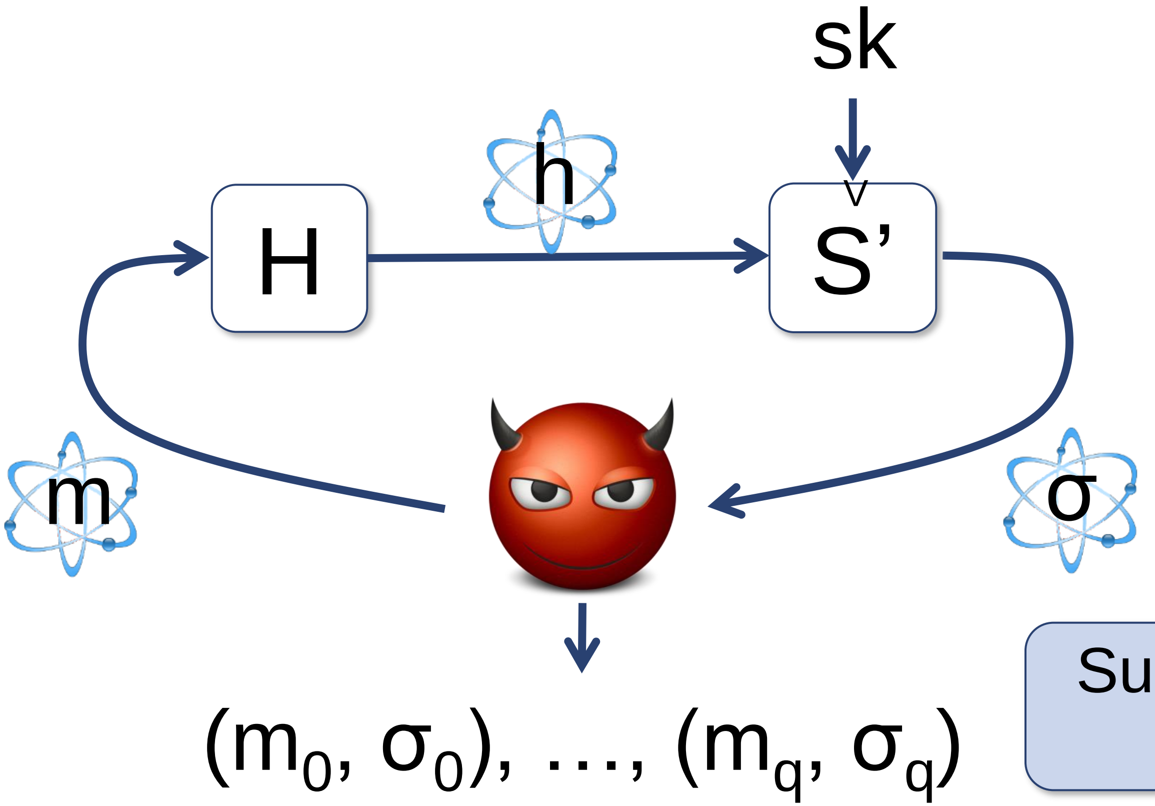
Classical Advantages:

- Only sign small hash → more efficient
- Weak security requirements for **S'** if **H** modeled as random oracle

Our Goal:

- Prove quantum security of **S** assuming only classical security of **S'**

Quantum Security of Hash and Sign



Success prob: ε

First Step: Simulate using only classical queries to **S'**

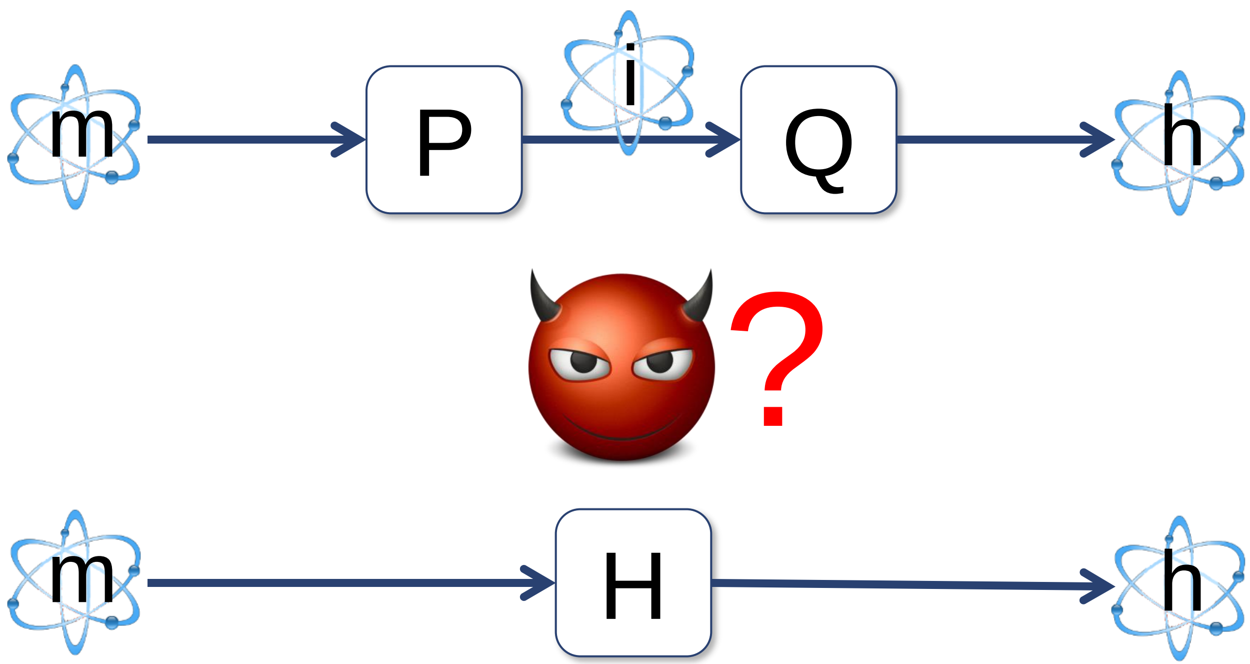
Problem: exponentially many **h**

→ must query **S'** too many times

Small Range Distributions [Z'12b]

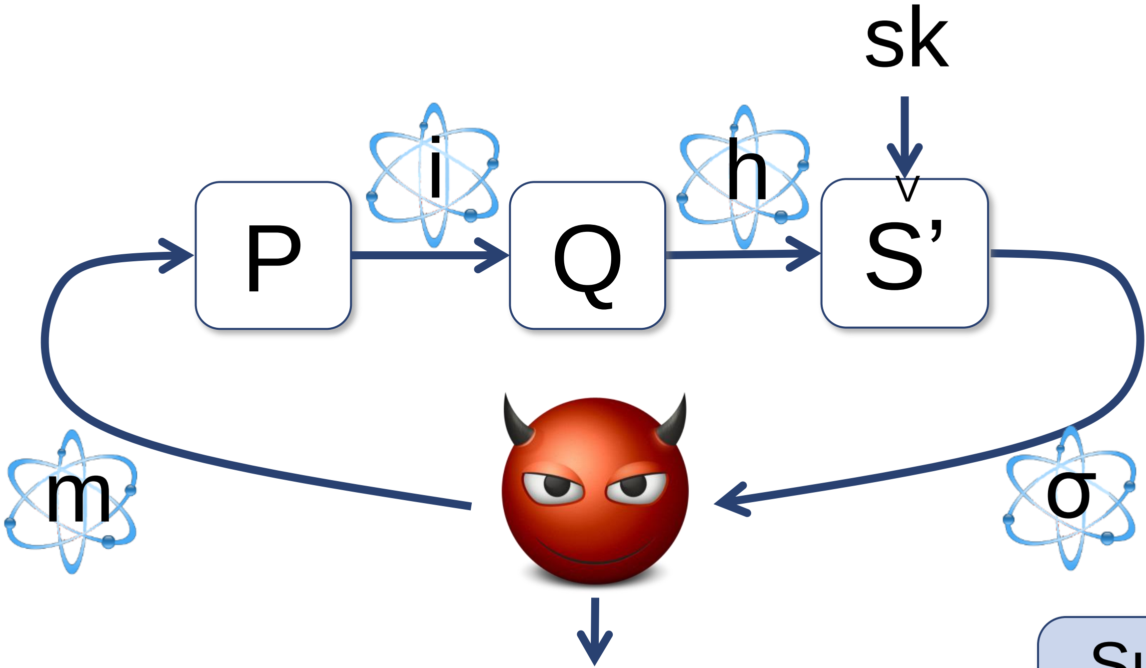
Quantum simulation tool:

Let P: M → [r] , Q: [r] → H be random functions



Theorem [Z'12b]: **Q∘P ≈ H** for large enough (polynomial) **r**

Step 1: Use S.R. Distribution for **H**



$(m_0, \sigma_0), \ldots, (m_q, \sigma_q)$

Success prob: ε/2

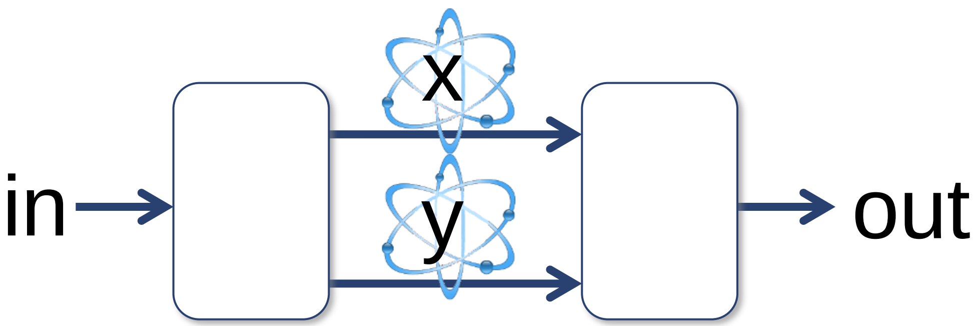
Now **S'** only queried on **r** inputs → Can simulate

Next Step: Use one of the $\boldsymbol{\sigma_i}$ as a forgery for **S'**

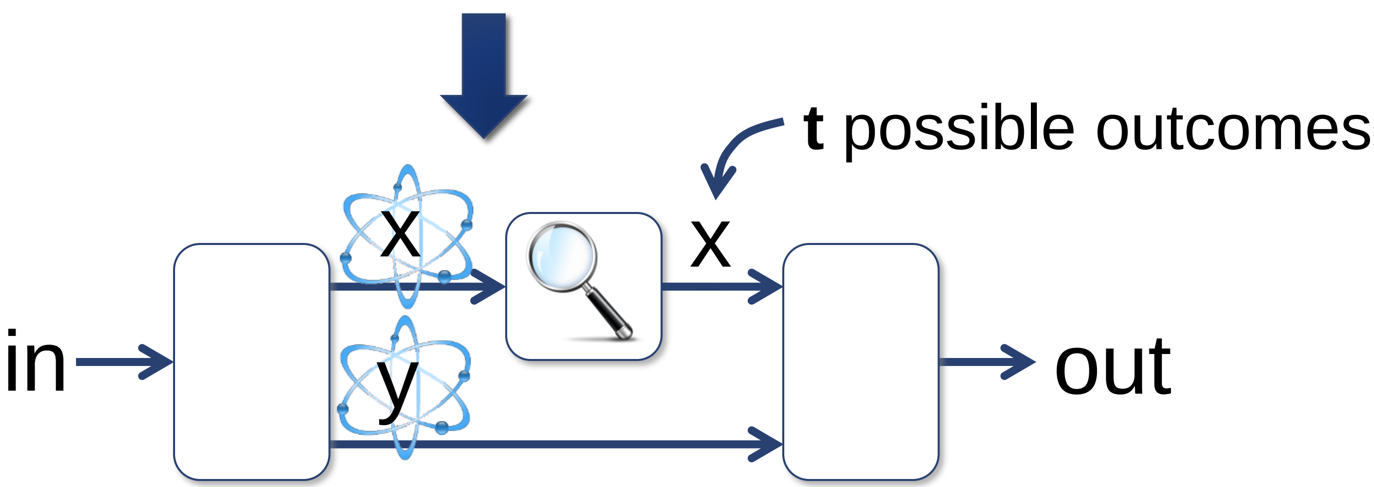
Problem: # of sigs (**q+1**) **<<** # of **S'** queries (**r**)

Intermediate Measurement

New quantum simulation technique:

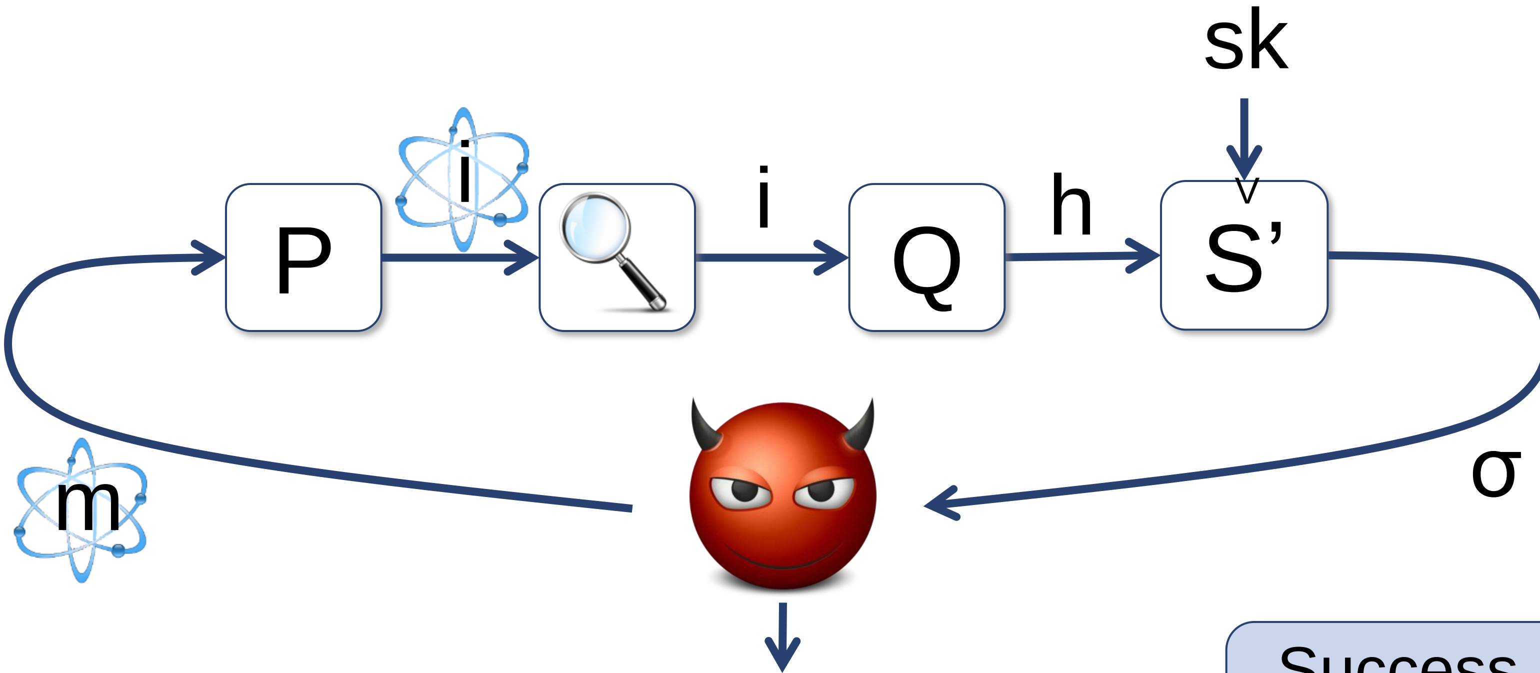


Success prob: **σ**



Theorem: Success prob: **≥σ/t**

Step 2: Measure Output of **P**



$(m_0, \sigma_0), \ldots, (m_q, \sigma_q)$

Success prob:
$\varepsilon/2r^q$

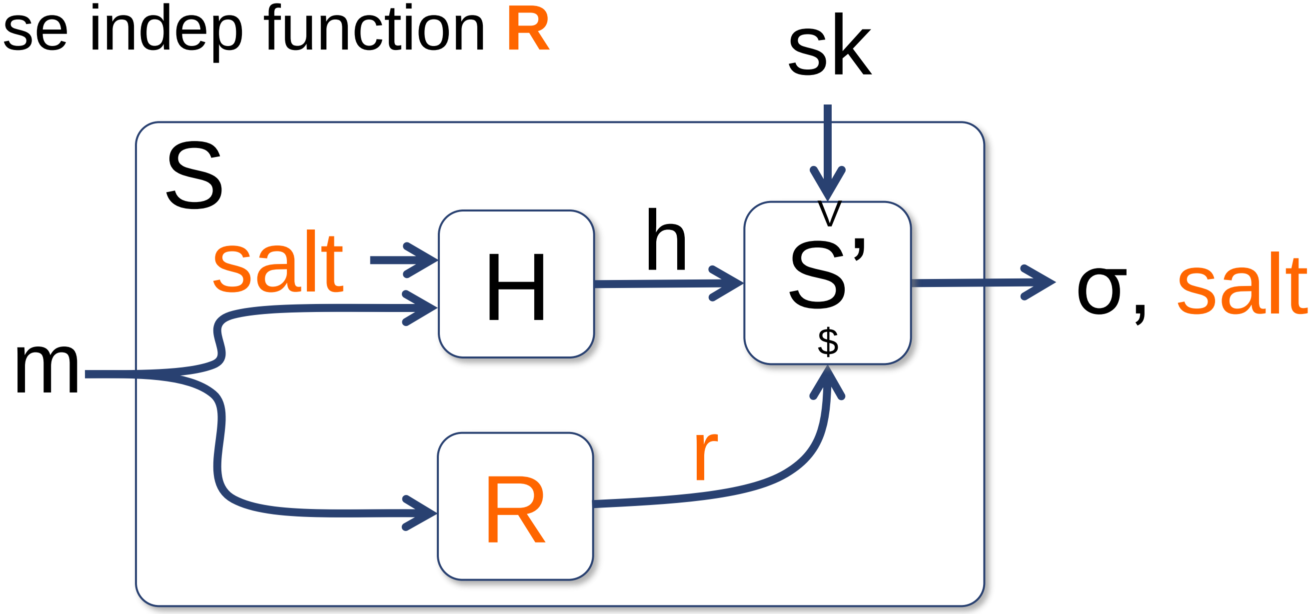
Only **q** queries to **S'** → One of the $\boldsymbol{\sigma_i}$ must be forgery for **S'**

Success probability non-negligible for **constant q**

Many-time Secure Scheme

To sign each message, draw

- A random **salt**
- A pairwise indep function **R**



Theorem: If **S'** is classical many-time secure, then **S** is quantum many-time secure

Other Signature Constructions

Theorem: (Slight variant of) GPV is quantum-secure

- Uses entirely different techniques

Non-Random Oracle Schemes:

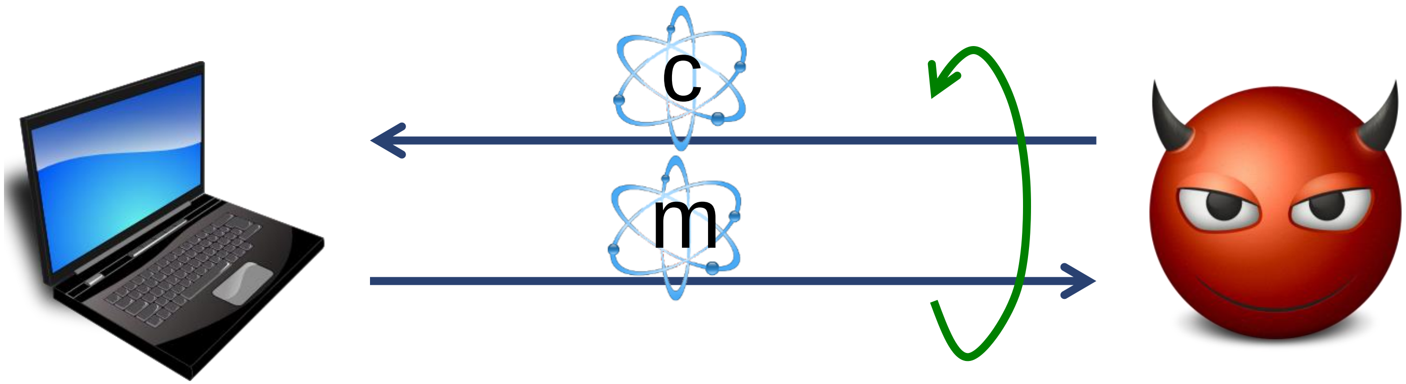
Theorem: Generic conversion using Chameleon hash

Theorem: Collision resistance $\Rightarrow$ quantum-secure signatures

- Follow-up work: signatures from one-way functions

Quantum Chosen Ciphertext Attack

What if adversary can learn decryptions of superpositions of ciphertexts?



decryption key sk

Adversary attempts to break **classical** semantic security

Quantum CCA Encryption

Our results:

Separation:

Theorem: $\exists$classical CCA secure schemes that are not quantum CCA secure

Two constructions:

Theorem: OWF $\Rightarrow$ Symmetric key quantum CCA

Theorem: LWE $\Rightarrow$ Public key quantum CCA

Summary & Open Problems

Classical security does not imply quantum security

Quantum-secure signatures:

- In the (quantum) random oracle model (inc. GPV sigs)
- Using a chameleon hash
- From collision resistance

Quantum CCA encryption: both symmetric and public key

Open Problems:

- Quantum security of Fiat Shamir signatures?
- Quantum security of CBC-MAC, NMAC, PMAC?

Thanks!