CLASSICAL CRYPTOSYSTEMS IN A QUANTUM WORLD

Mark Zhandry – Stanford University

* Joint work with Dan Boneh

But First: My Current Work

Indistinguishability Obfuscation (and variants)

- Multiparty NIKE without trusted setup and with small parameters
- Broadcast encryption with short ciphertexts and secret/public keys
- Traitor tracing with short ciphertexts and secret/public keys
- More to come

Talk at NYU 2:30pm Tomorrow (11/20). Ask me for details

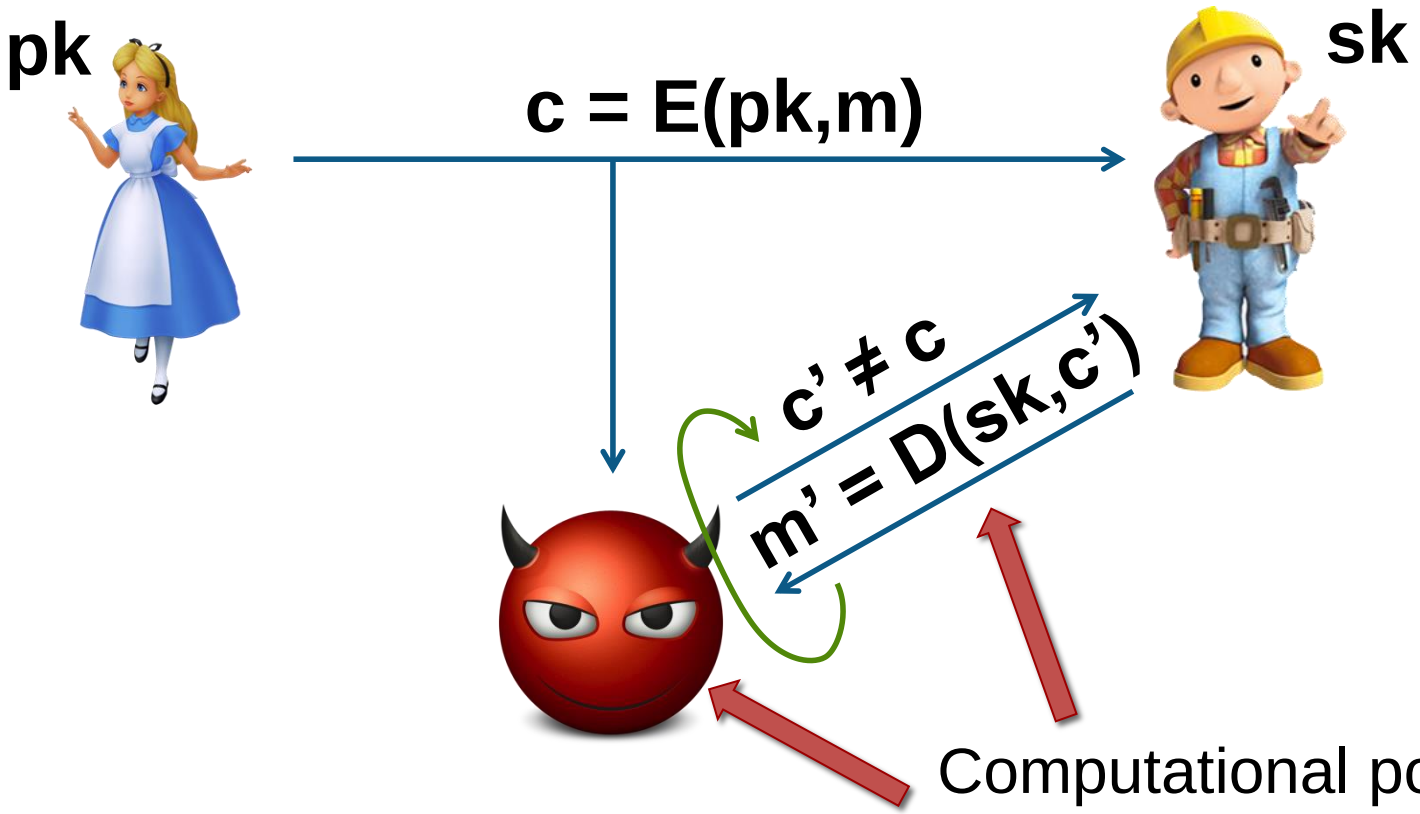
Multilinear Maps

- Can above primitives be built directly from multilinear maps?

Back to Quantum

Classical Crypto

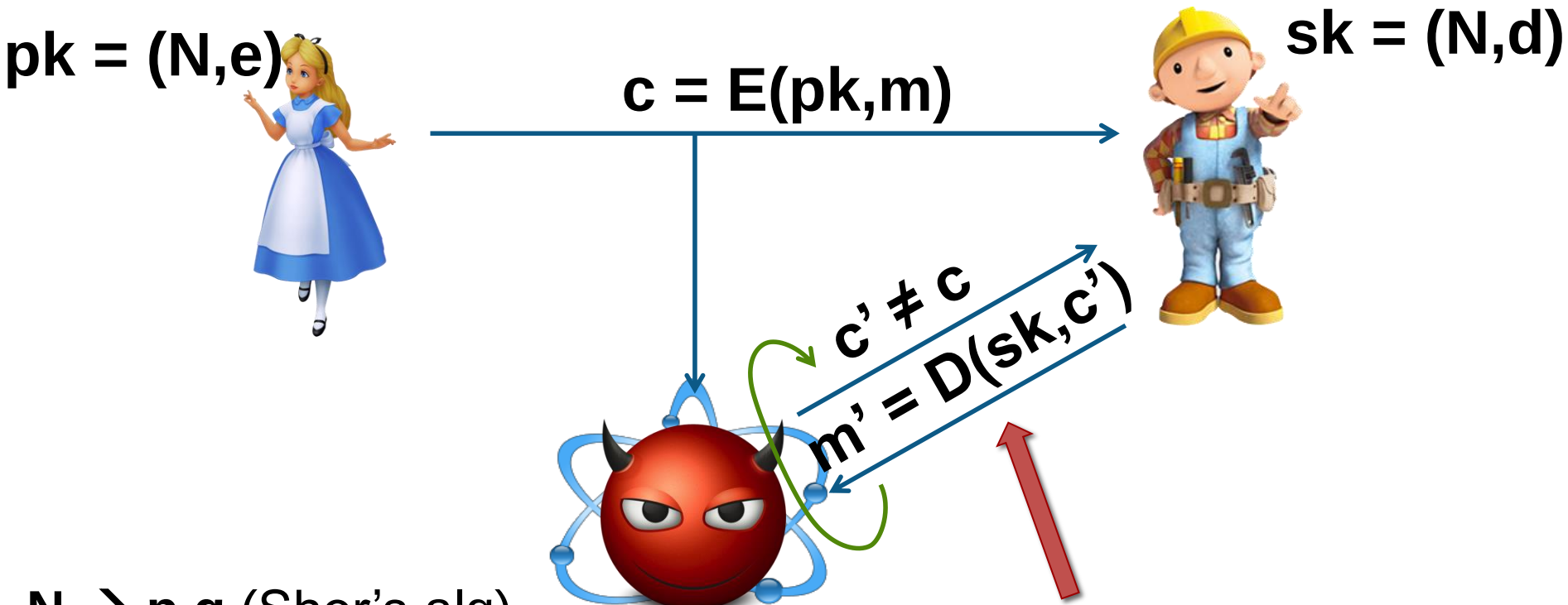
Ex: CCA encryption



Quantum Computing Attack

Aka: Post-quantum crypto

Adversary has quantum computer:



N → p,q (Shor's alg)
$d = e^{-1} \bmod \phi(N)$
m = D(sk,c)

Interactions remain classical

Defending against Quantum Computing Attacks

Need crypto based on hard problems for quantum computers

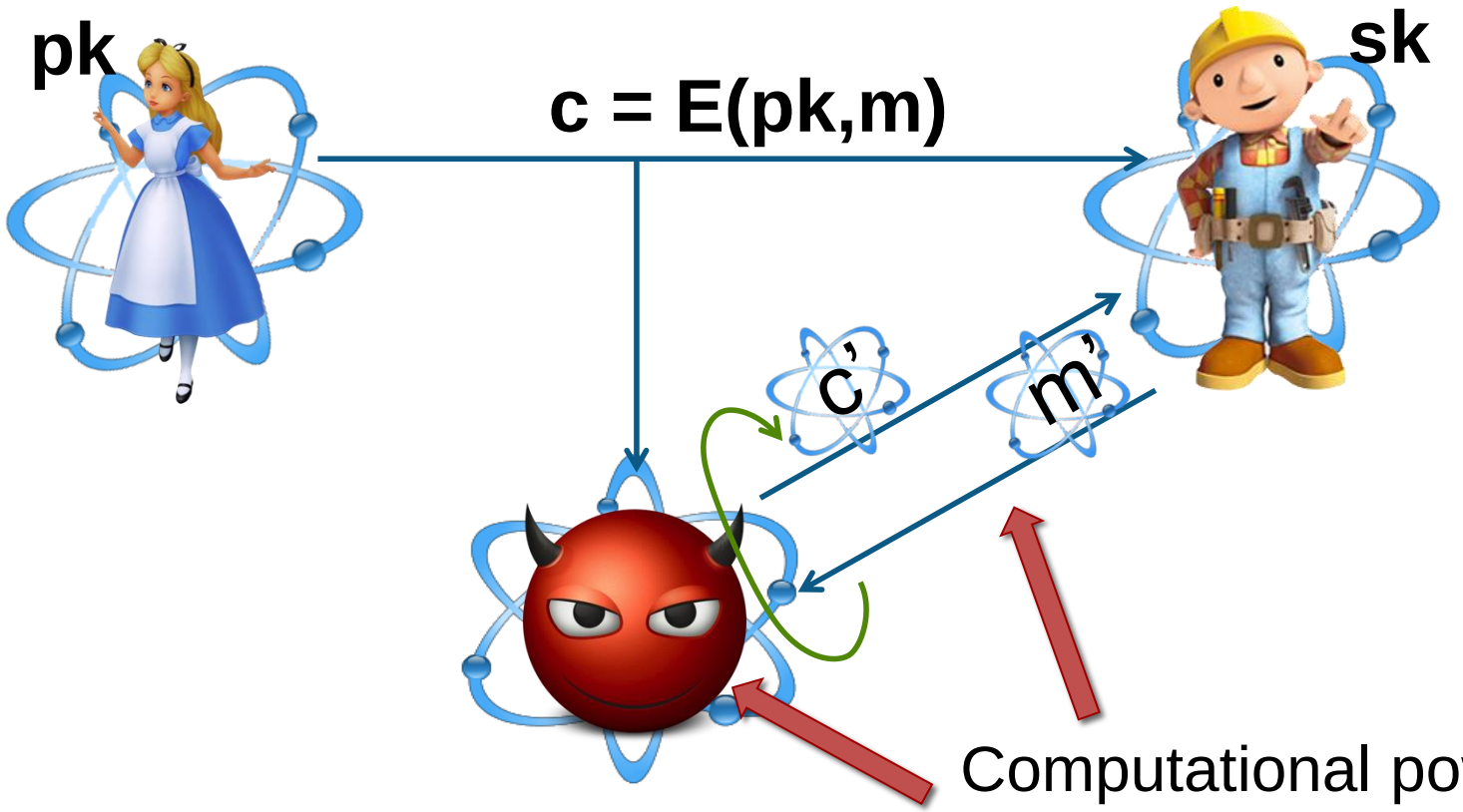
- Ex: lattice problems

Classical security proofs (reductions) often carry through

- Many reductions treat adversary as black box
- Classical interactions → simulate adversary using classical techniques
- Ex: OWF → PRF, IBE → CCA encryption, etc.
- Exception: rewinding

This Talk: Quantum Channel Attacks

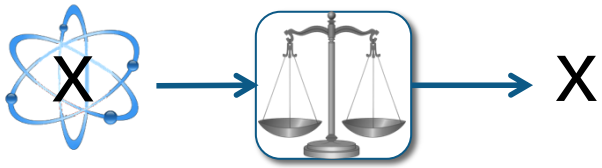
All parties have quantum computers



Quantum Background

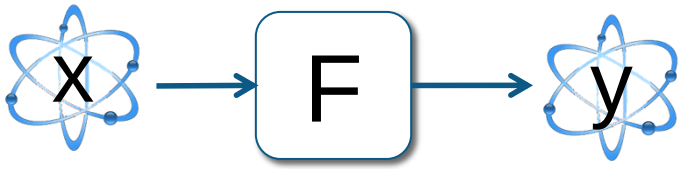
$$= \sum_{x \in \mathcal{X}} \alpha_x |x\rangle \qquad \left(\sum_{x \in \mathcal{X}} |\alpha_x|^2 = 1 \right)$$

Measurement:



(Output **x** with probability $|\alpha_x|^2$)

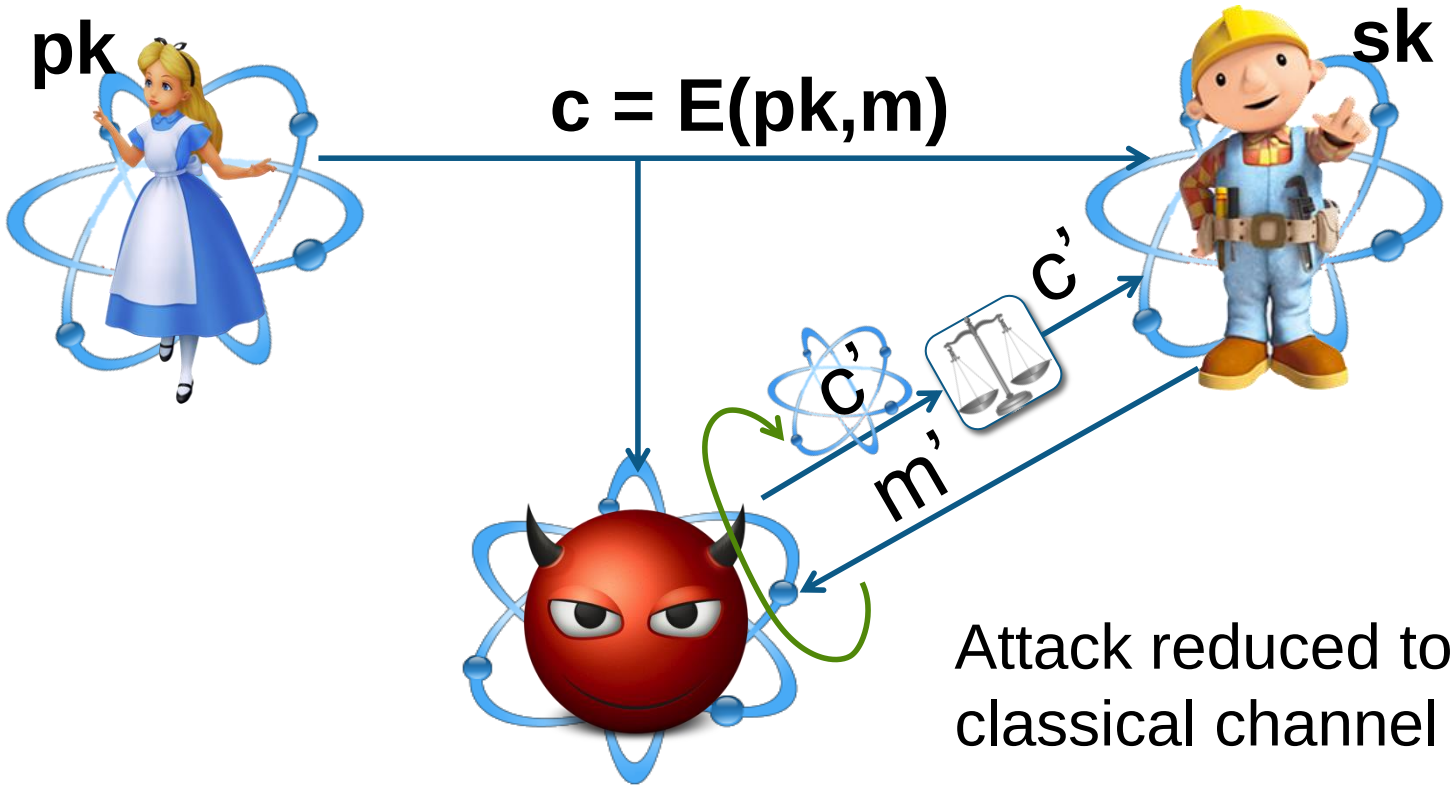
Can perform any classical op:



$$= \sum_{x \in \mathcal{X}} \alpha_x |F(x)\rangle$$

Motivation

Objection: Can always measure incoming query



Attack reduced to classical channel attack

Motivation

Objection: Can always measure incoming query

Answer: Implementing measurement securely is non-trivial

- Measurement is physical – must trust hardware
- What if adversary has access to device?
- Only way to be certain: entangle fully with query
  - Requires quantum storage ≥ total data measured.

Conservative approach to crypto:

Use schemes secure against quantum channel attacks

Proving Quantum Security

Main difficulty: simulation

- Adversary may query on superposition of **all** inputs
- Exact simulation:
  - need an answer at every point
  - Distribution of all answers must be same as real setting

Possible solutions:

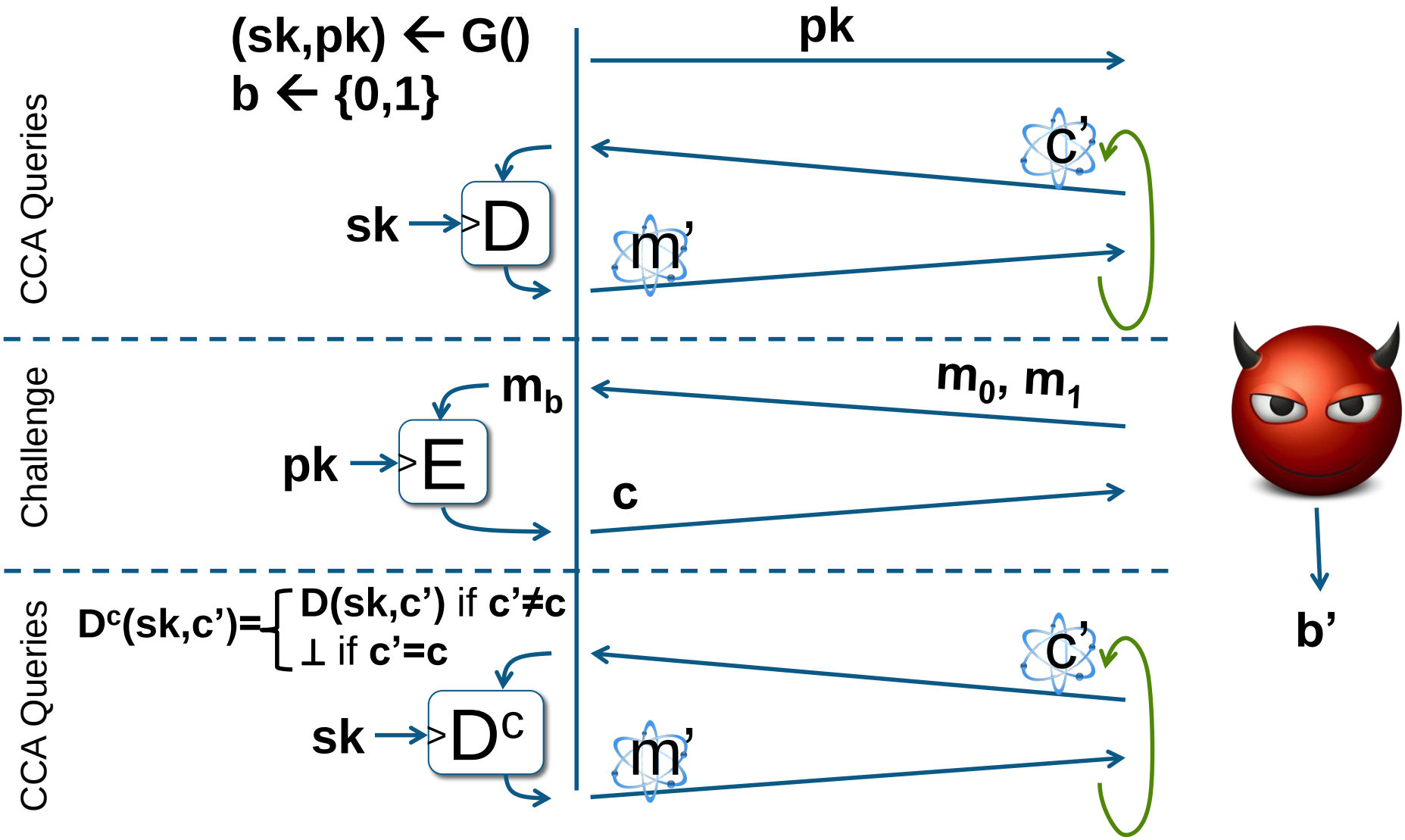
- Find reduction that answers every point correctly
- Distribution of answers indistinguishable from real setting
- Answer incorrectly on some inputs*

What’s to come

- Encryption
- Pseudorandom functions
- Message authentication codes
- Signatures (if time)

Encryption

Quantum CCA Attack



Proving security against quantum CCA

Goal: find reduction that can decrypt all queries except challenge

Reduction can compute all decryption keys except challenge

Example:

ABB'10 selective IBE

+

selective IBE → CCA

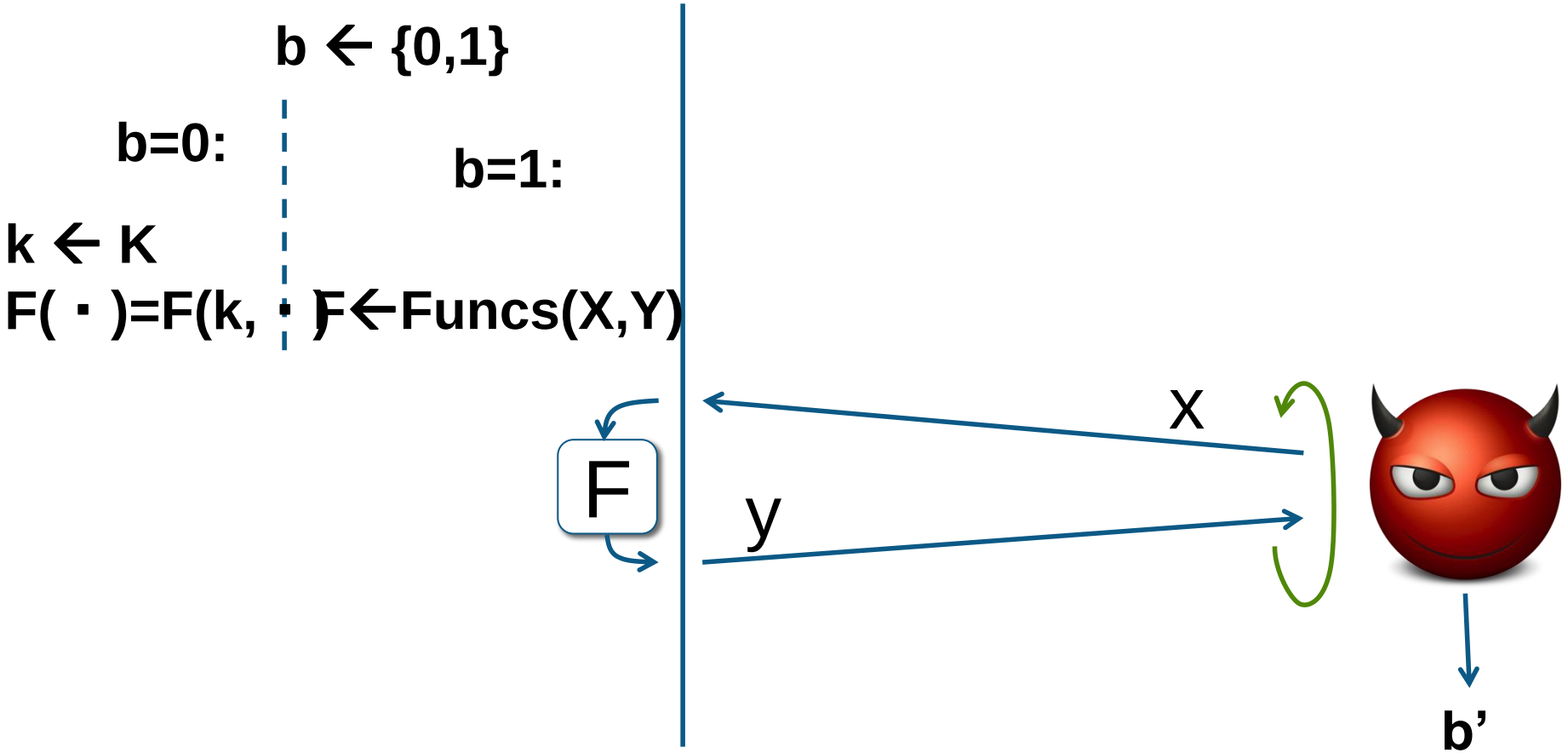
Reduction can decrypt every ciphertext but challenge

- Needs all decryption keys but challenge

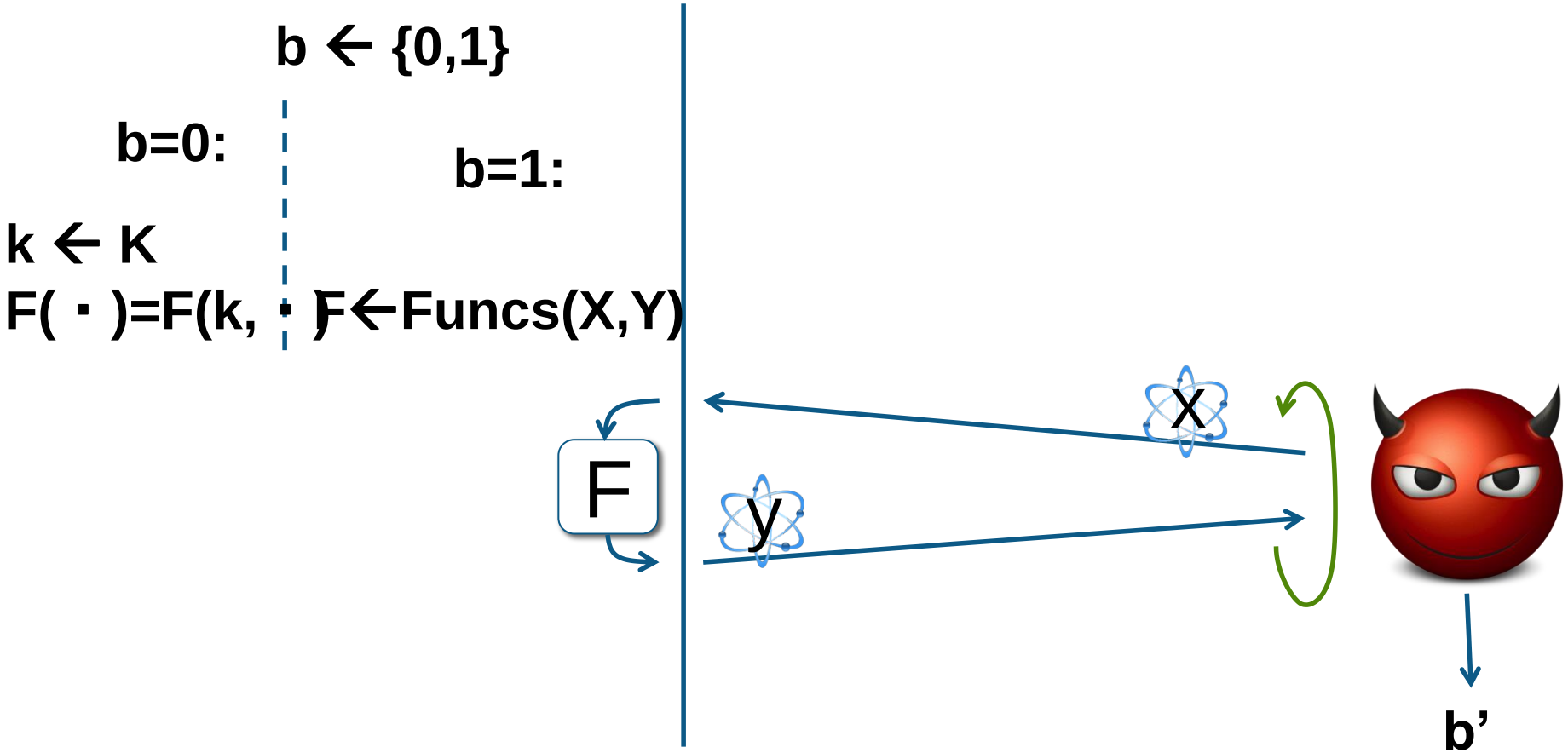
Pseudorandom Functions

Pseudorandom Functions

Recall classical def:

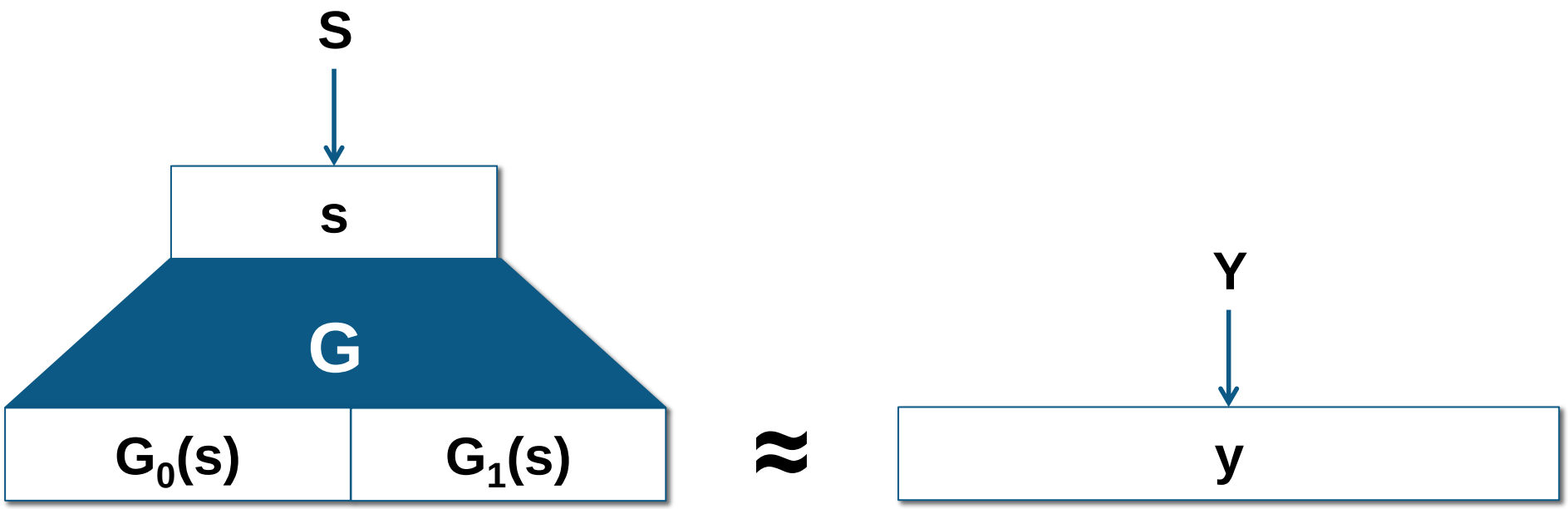


Quantum Security for PRFs

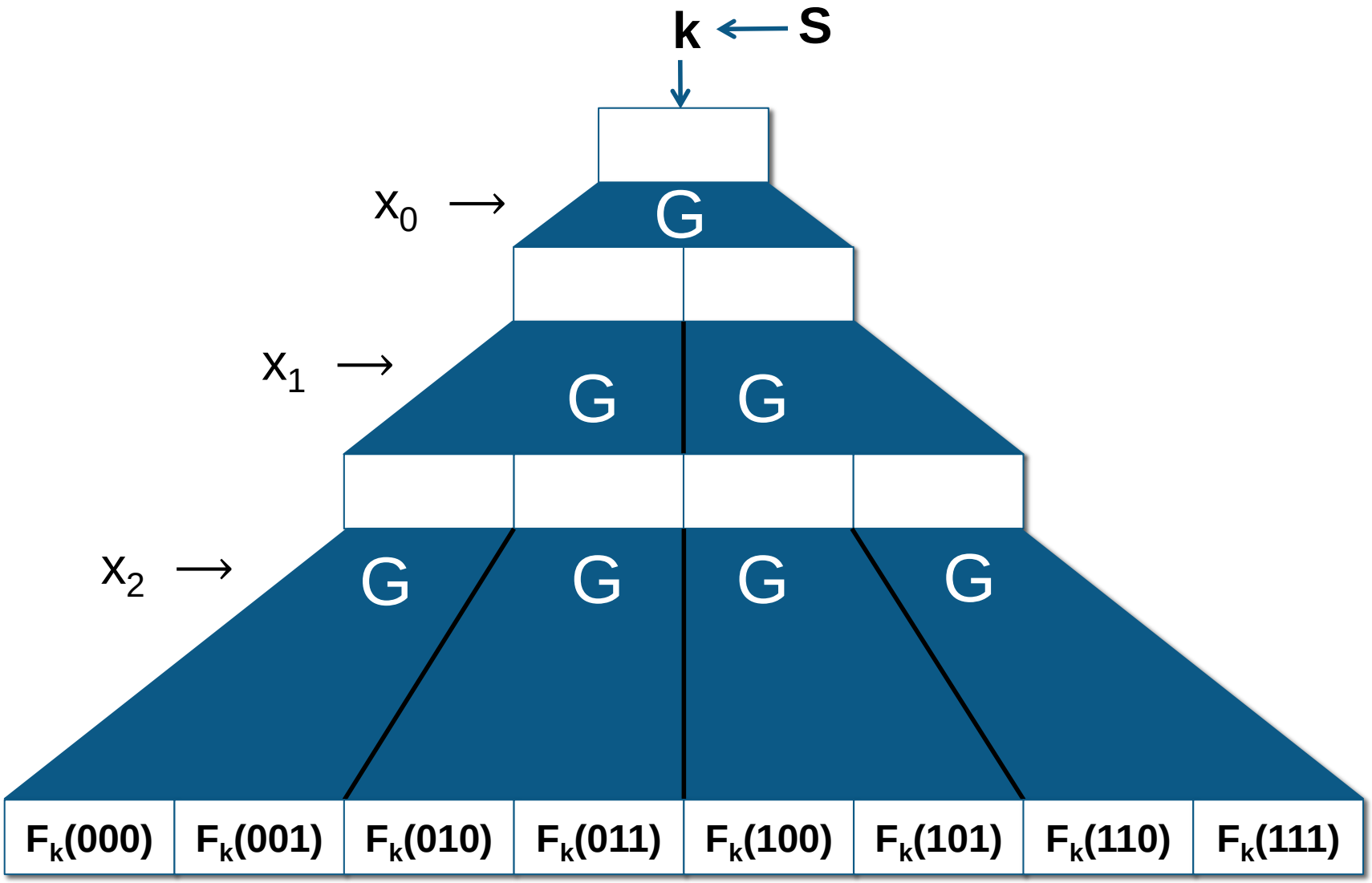


The GGM Construction

Pseudorandom Generators



The GGM Construction

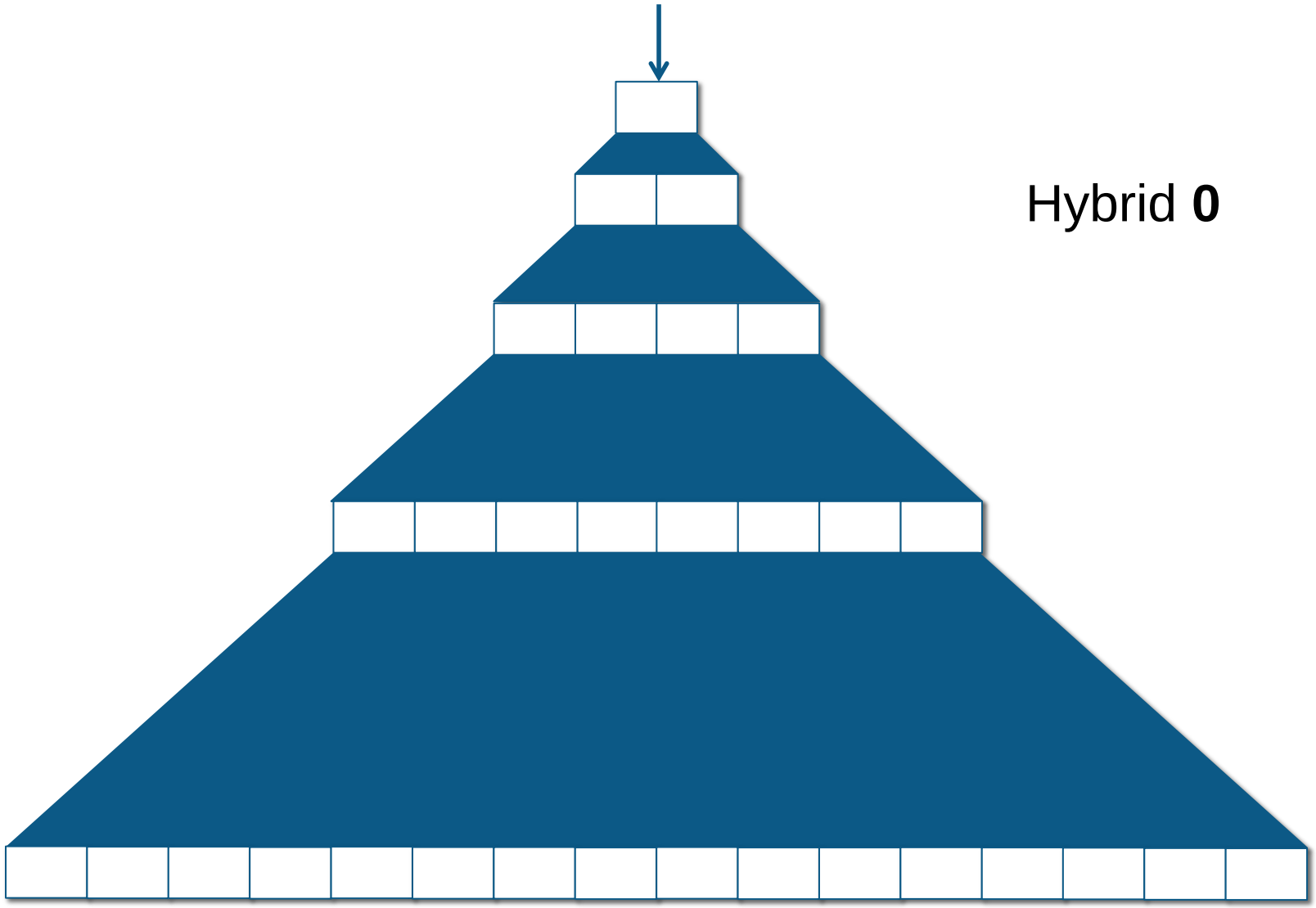


Quantum Security Proof?

Follow classical steps:

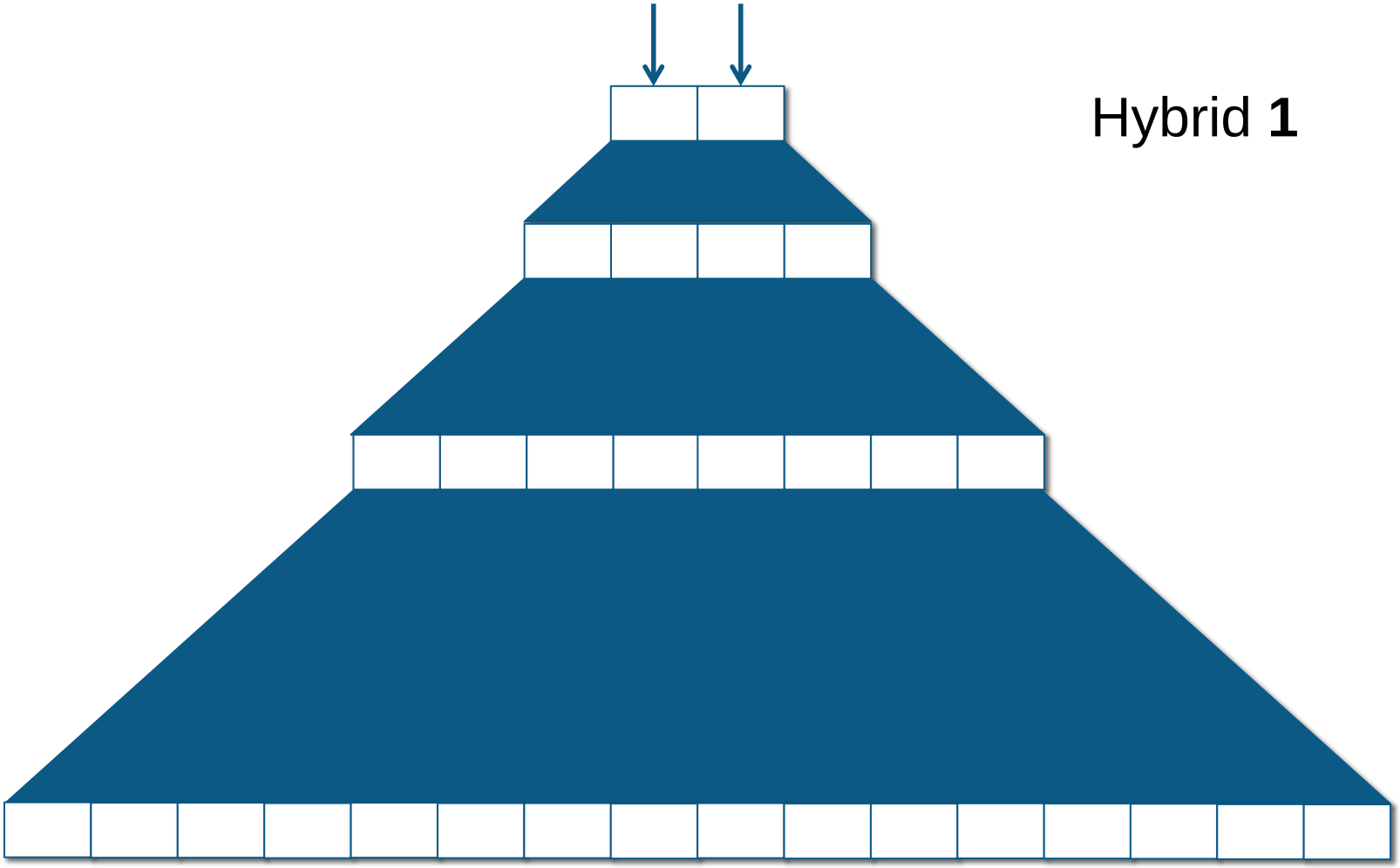
Step 1: Hybridize over levels of tree

Hybridize Over Levels



Hybrid **0**

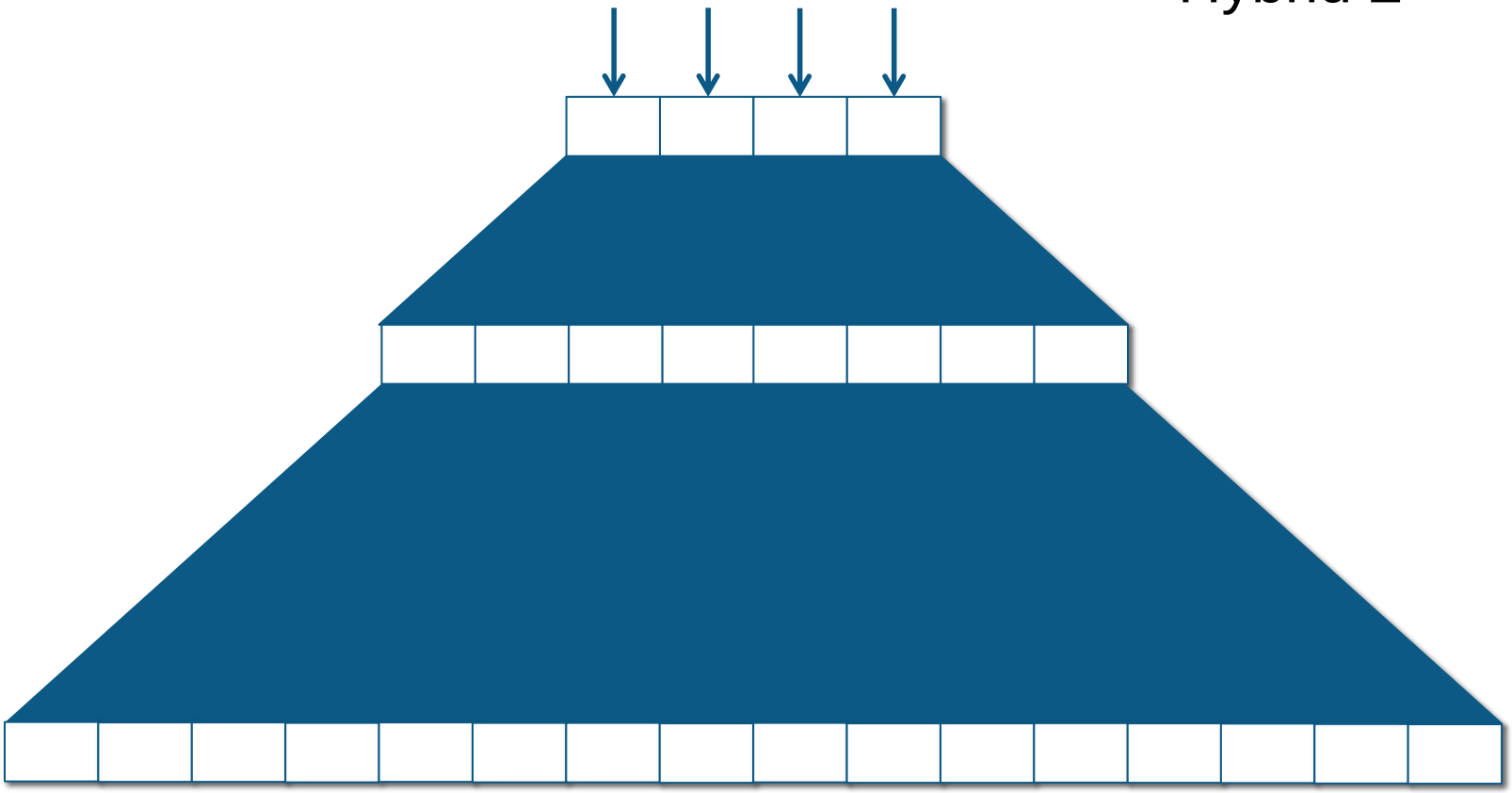
Hybridize Over Levels



Hybrid **1**

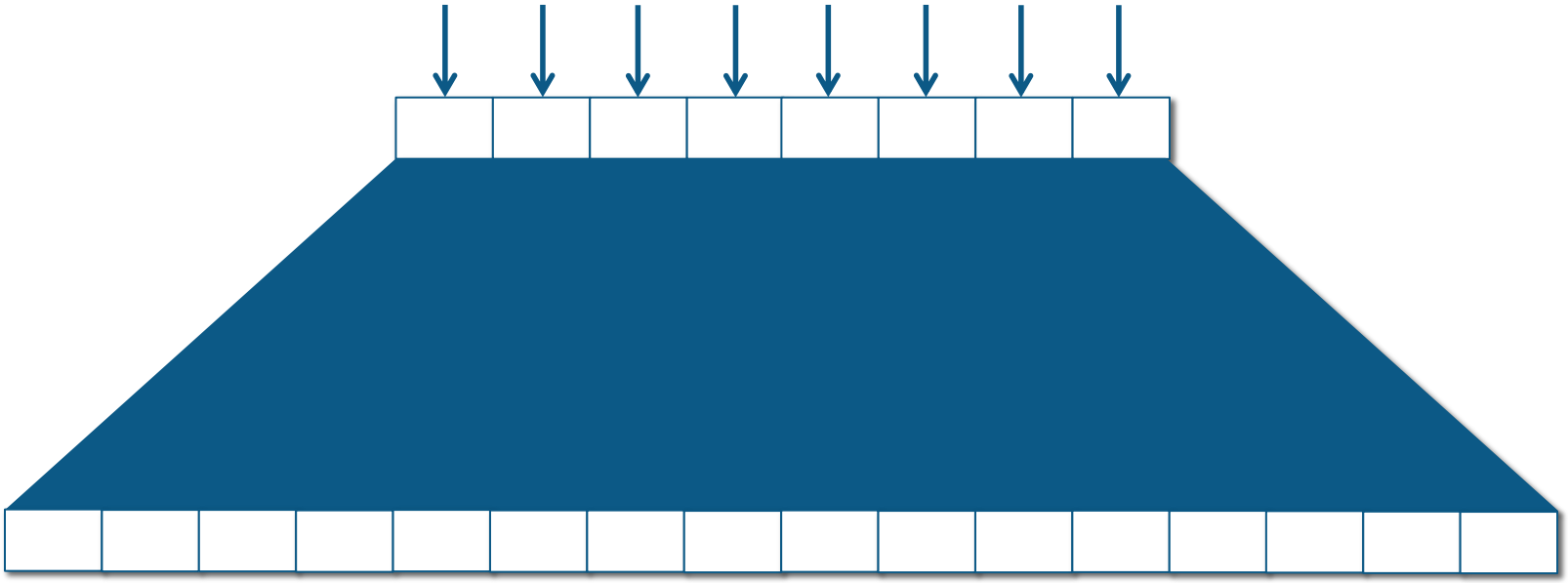
Hybridize Over Levels

Hybrid **2**



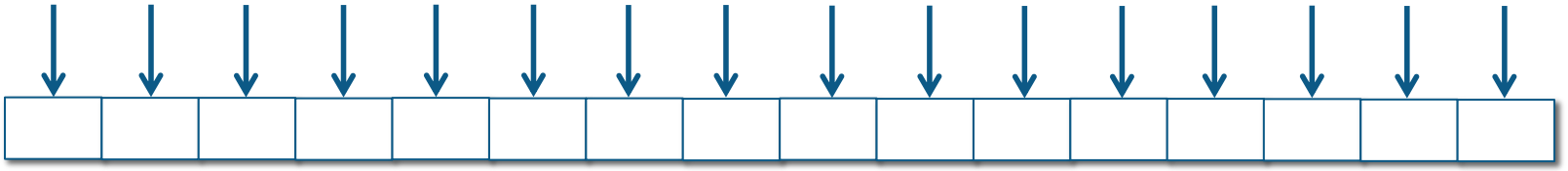
Hybridize Over Levels

Hybrid **3**



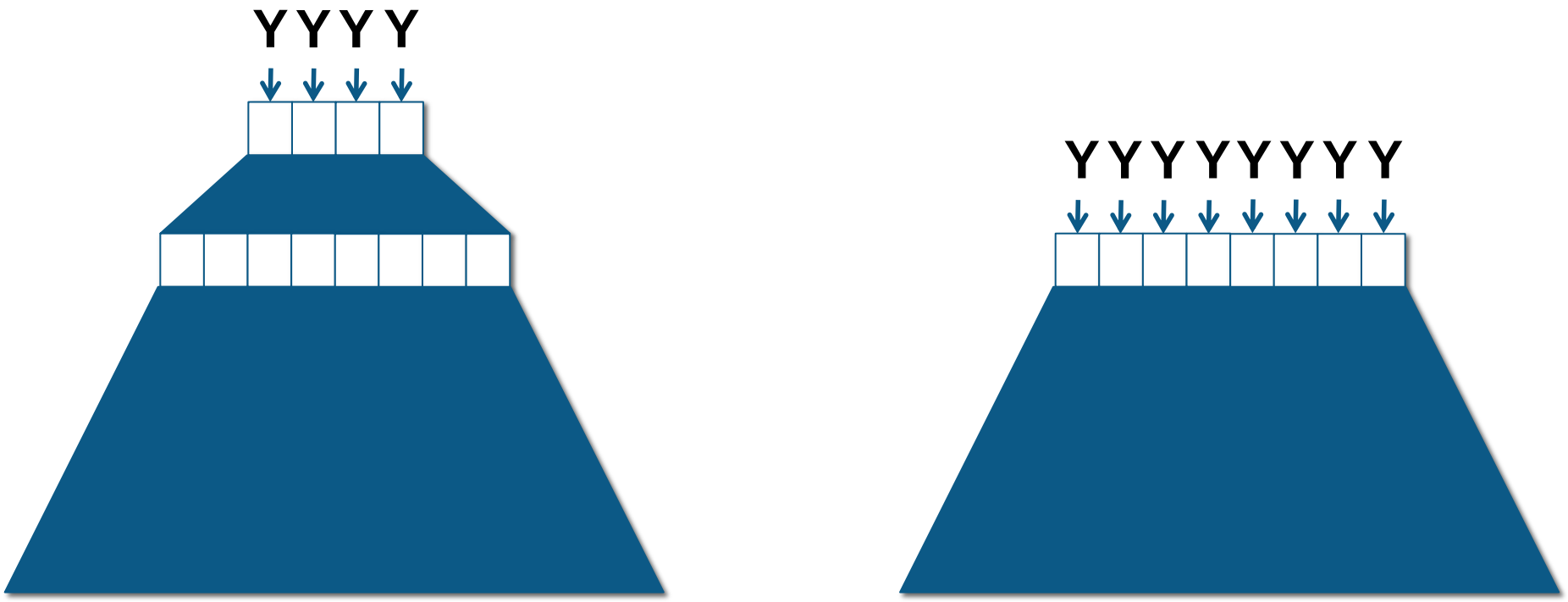
Hybridize Over Levels

Hybrid **n**



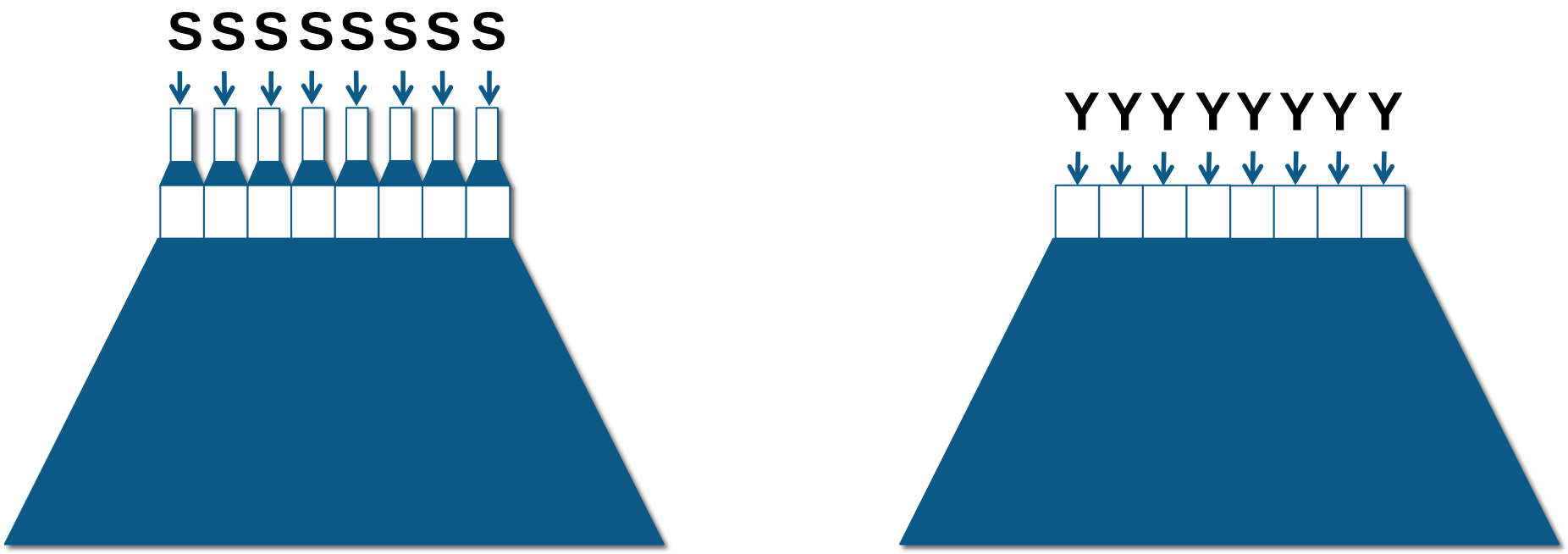
Hybridize Over Levels

PRF distinguisher will distinguish two adjacent hybrids



Hybridize Over Levels

PRF distinguisher will distinguish two adjacent hybrids



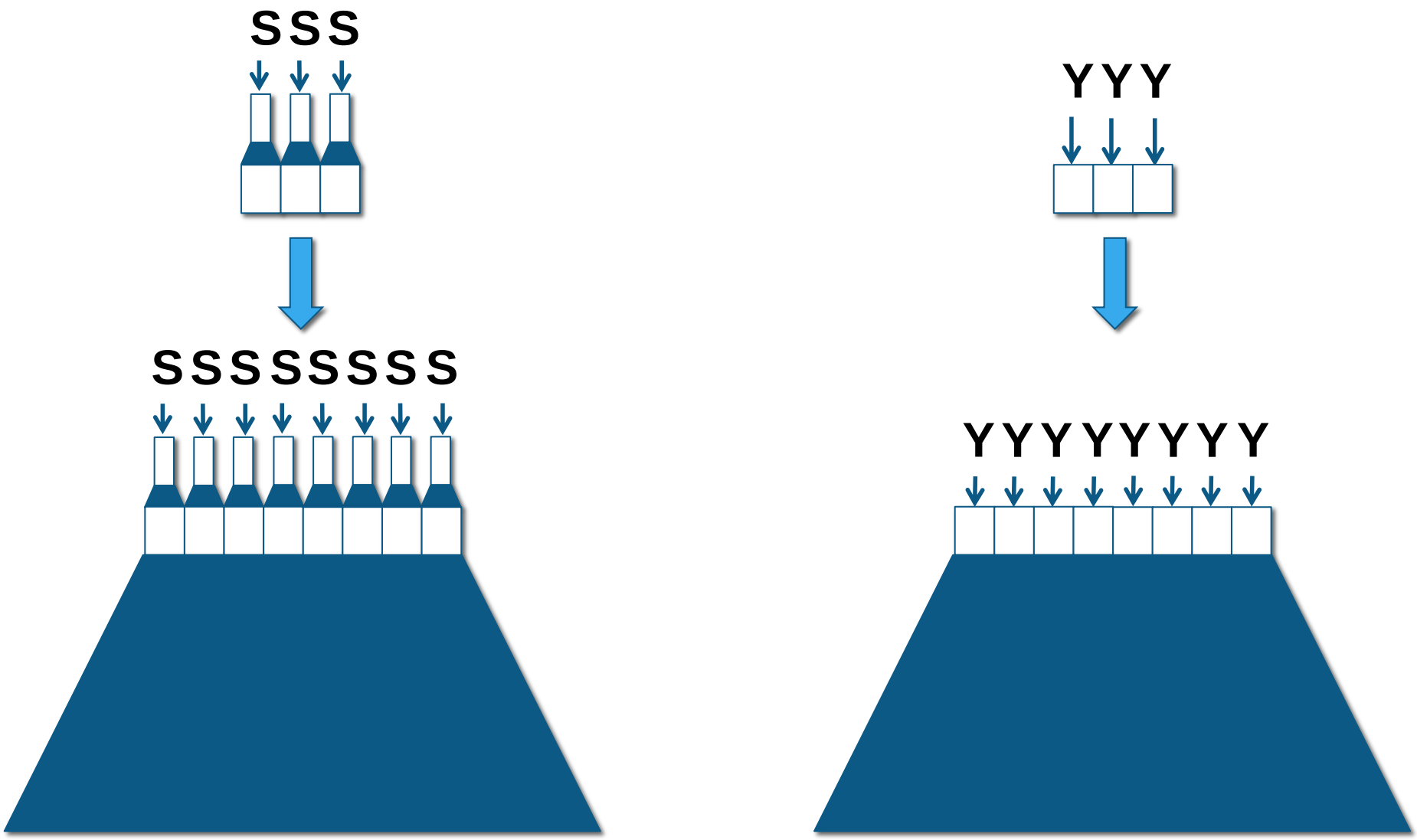
Quantum Security Proof?

Follow classical steps:

Step 1: Hybridize over levels of tree ✓

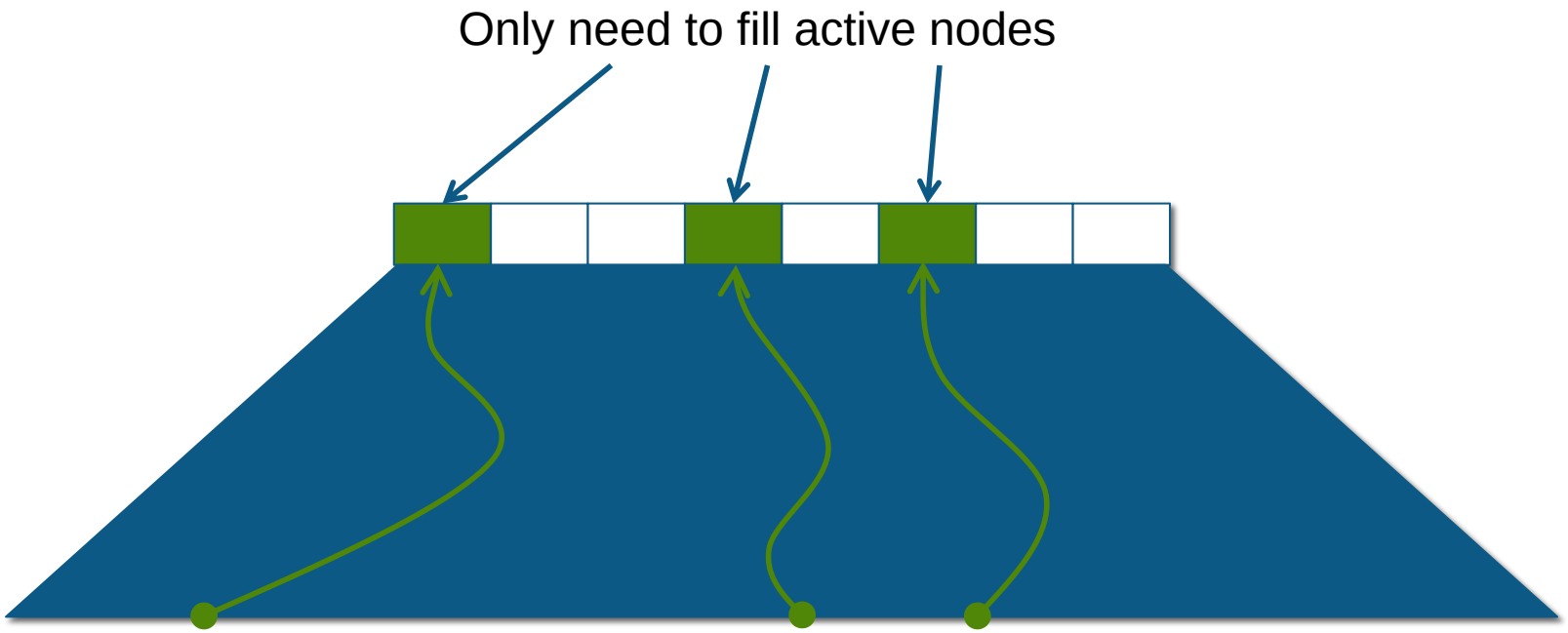
Step 2: Simulate hybrids using PRG/Random samples

Simulating Hybrids



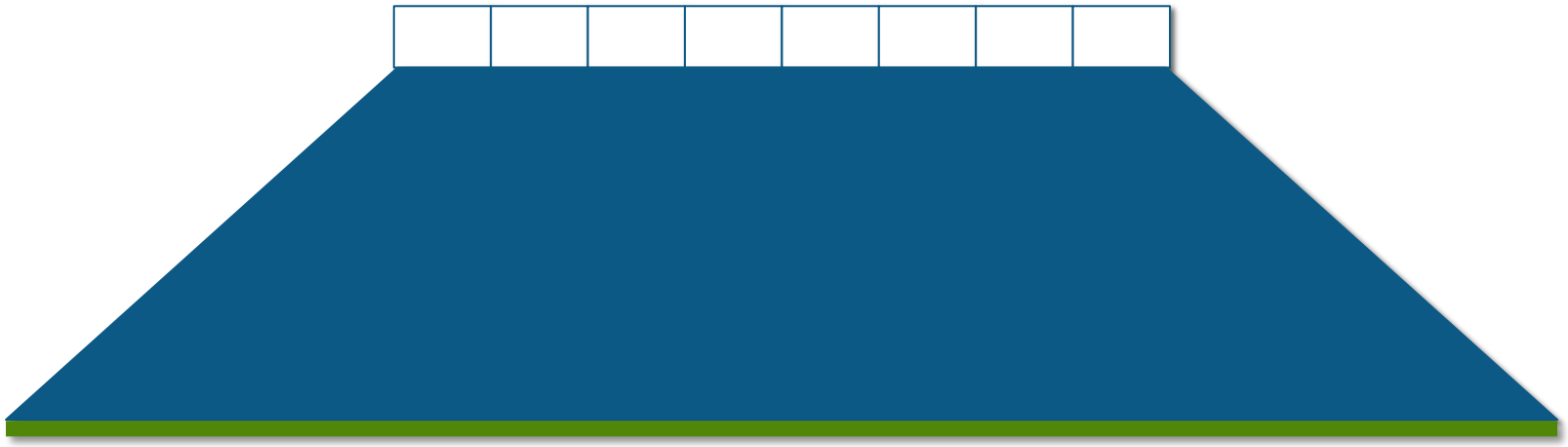
How It Was Done Classically

Active node: value used to answer query



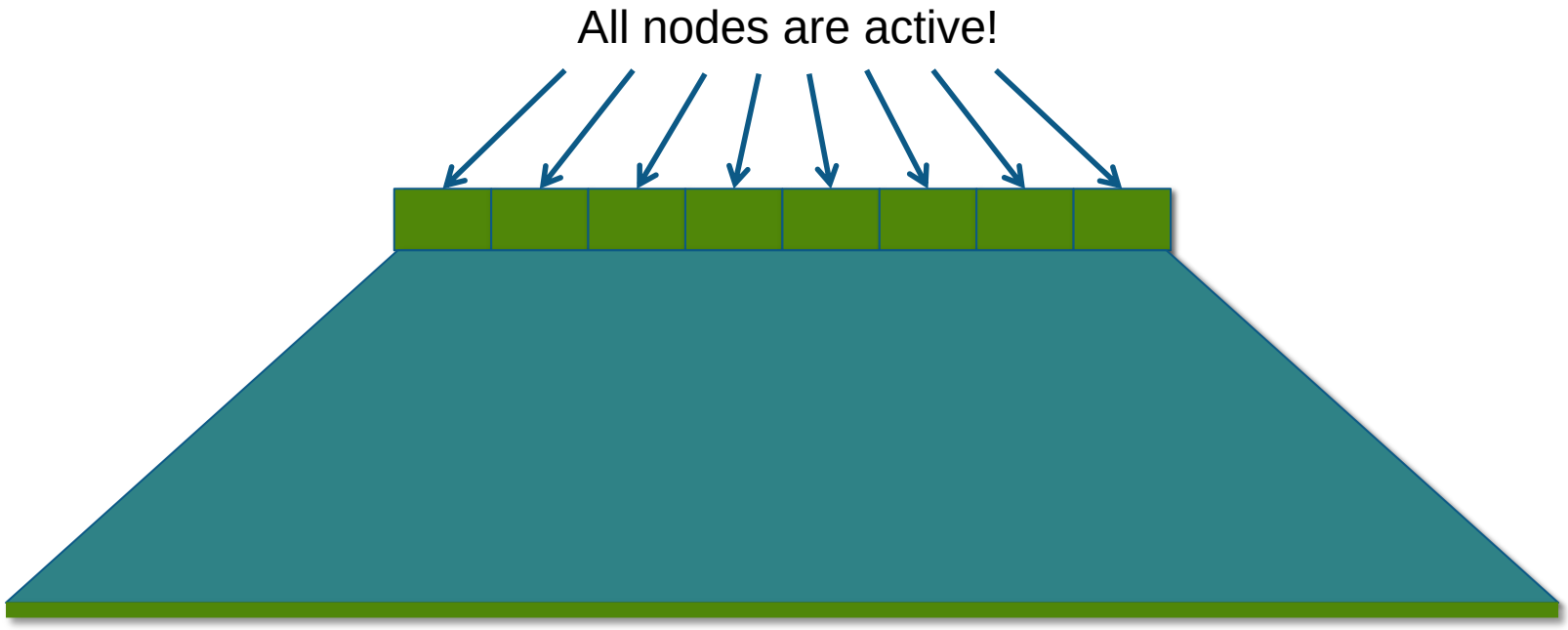
Adversary only queries polynomial number of points

Quantum Simulation?



Adversary can query on all exponentially-many inputs

Quantum Simulation?



Adversary can query on all exponentially-many inputs

Cannot simulate exactly with polynomial samples!

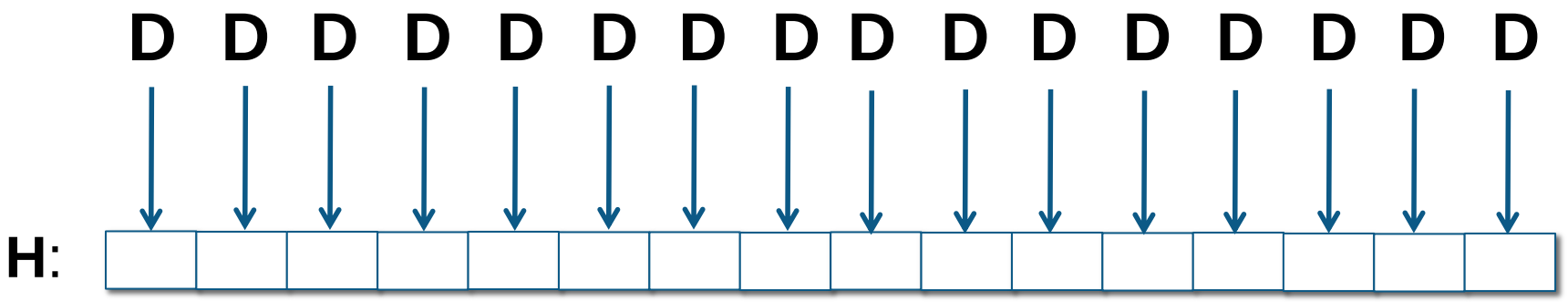
A Distribution to Simulate

Any distribution **D** on values induces a distribution on functions

For all $x \in X$:

$y_x \leftarrow D$

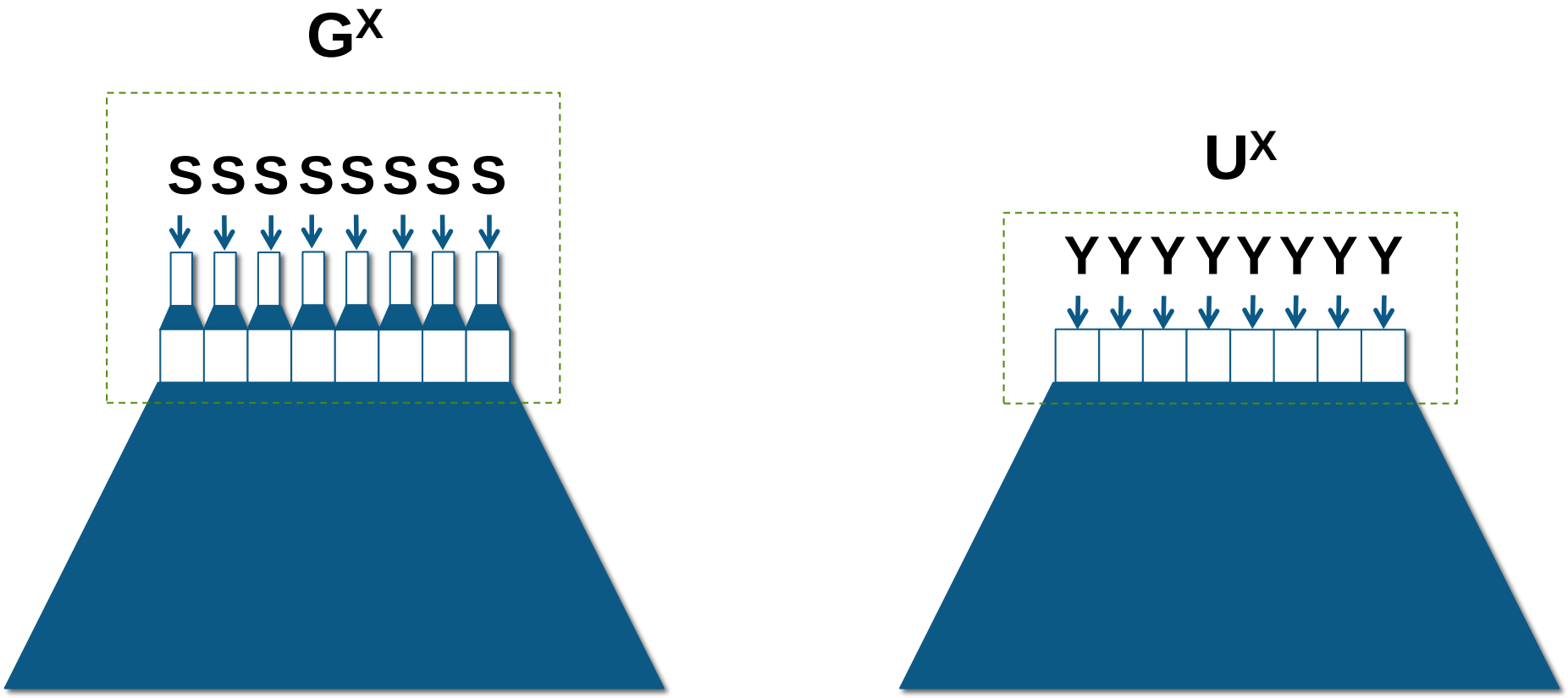
$H(x) = y_x$



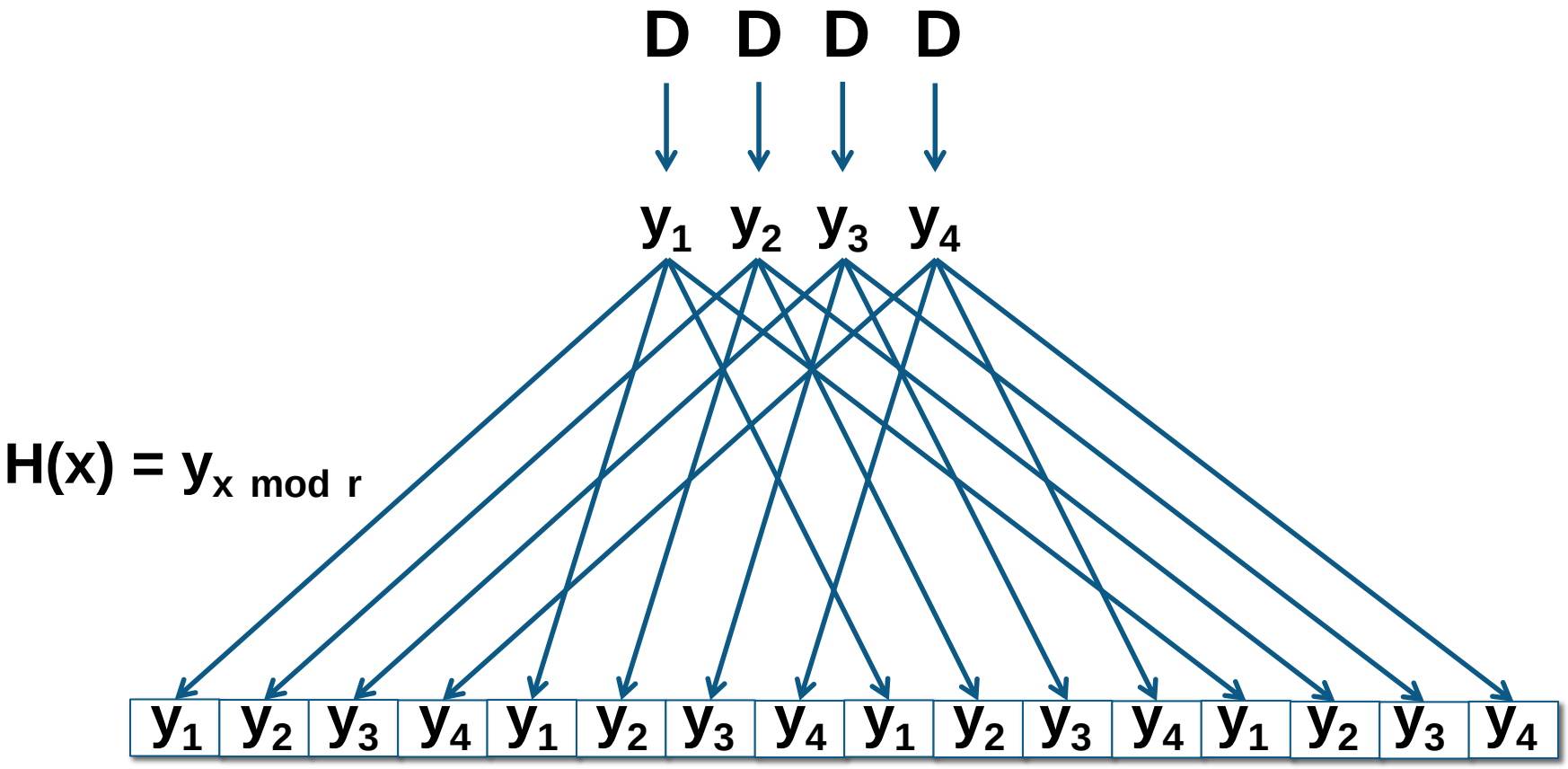
D^X

Simulating Hybrids

Goal: simulate $\mathbf{D}^{\mathbf{X}}$ using poly samples of **D**

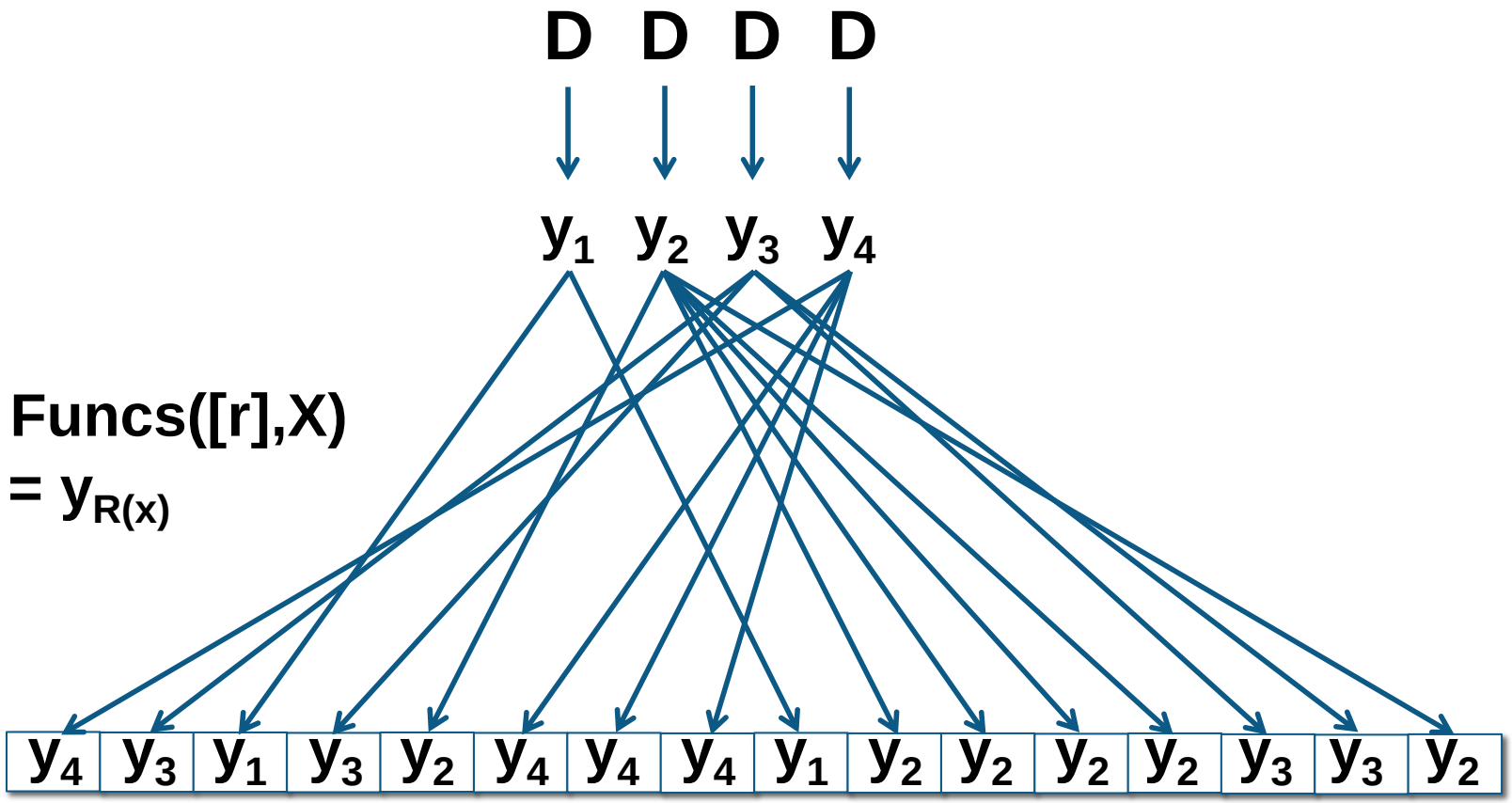


Attempt 1: Systematic



H is periodic → period learnable by quantum algorithms

Attempt 2: Random



R ← Funcs([r],X)
H(x) = $y_{R(x)}$

Called small range distributions, **$SR_r^X(D)$**

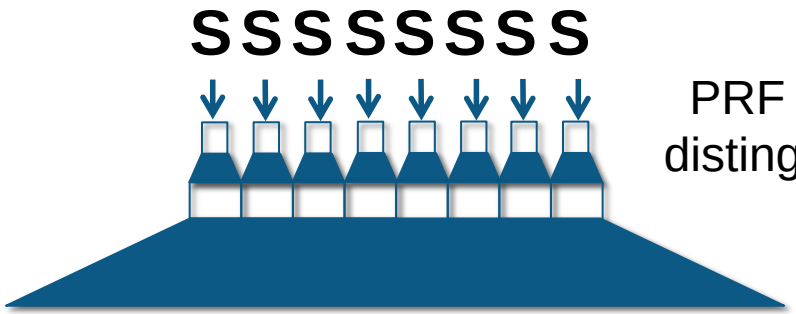
Small Range Distributions

Theorem: $\mathbf{SR_r^X(D)}$ is indistinguishable from $\mathbf{D^X}$ by any **q**-query quantum algorithm, except with probability $\mathbf{O(q^3/r)}$

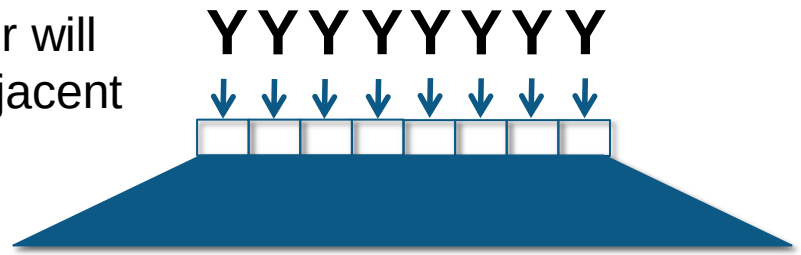
Notes:

- Highly non-trivial
- Distinguishing prob not negligible, but good enough
  - We get to choose **r**
- Random function **R** not efficiently constructible
  - [Zha'12a] Can simulate **R** using **k**-wise independence

Quantum GGM Proof

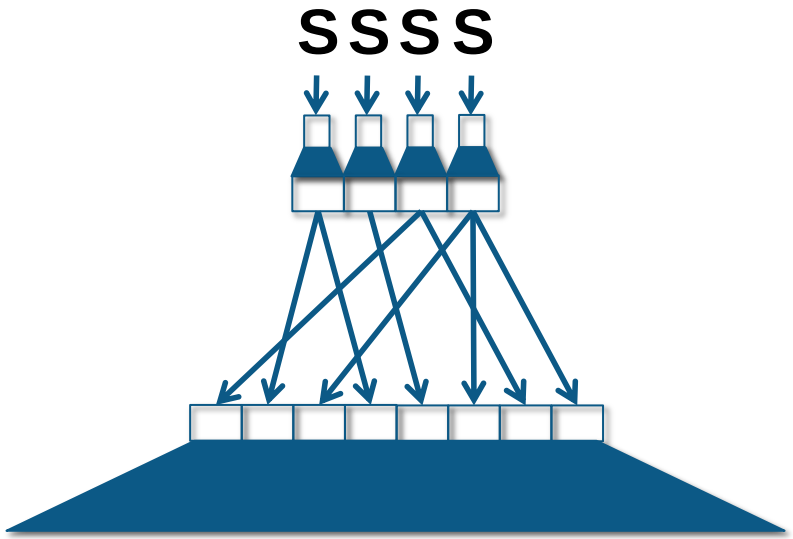


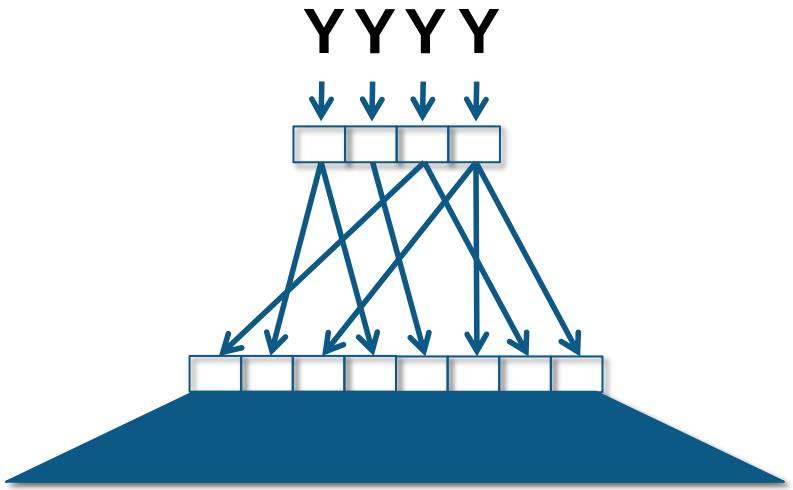
PRF distinguisher will distinguish two adjacent hybrids



≈ (SR distributions)

≈ (SR distributions)





Quantum Security Proof?

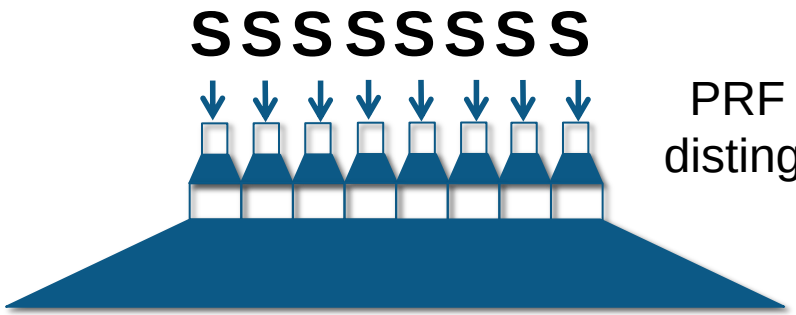
Follow classical steps:

Step 1: Hybridize over levels of tree ✓

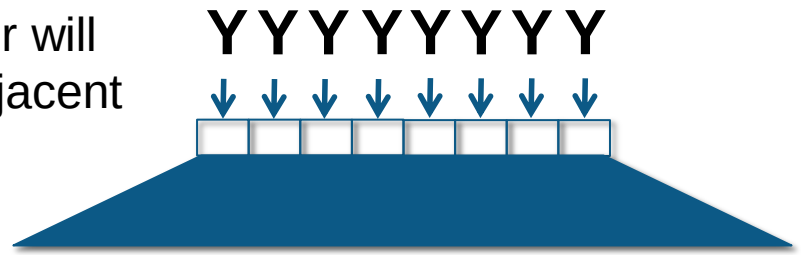
Step 2: Simulate hybrids approximately using PRG/Random samples ✓

Step 3: Hybrid over samples ✓

Quantum GGM Proof

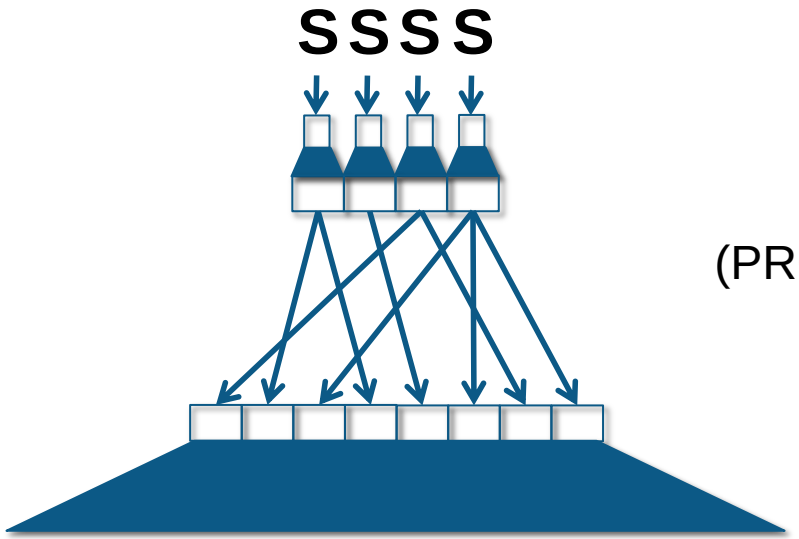


PRF distinguisher will distinguish two adjacent hybrids



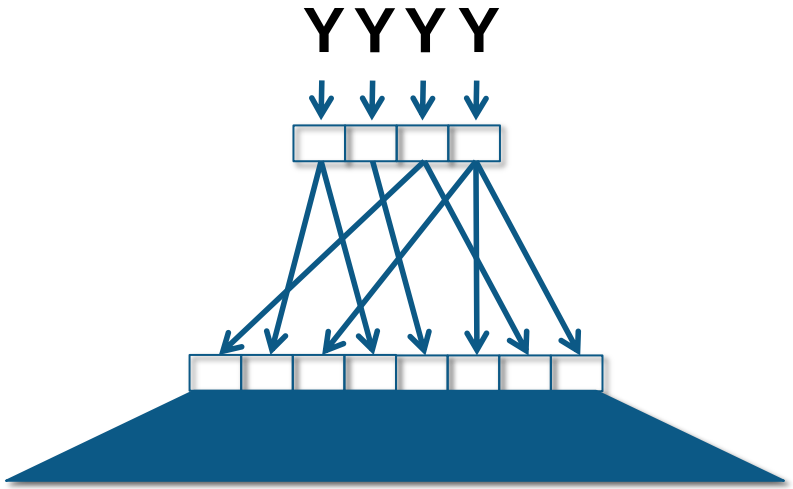
≈ (SR distributions)

≈ (SR distributions)



≈

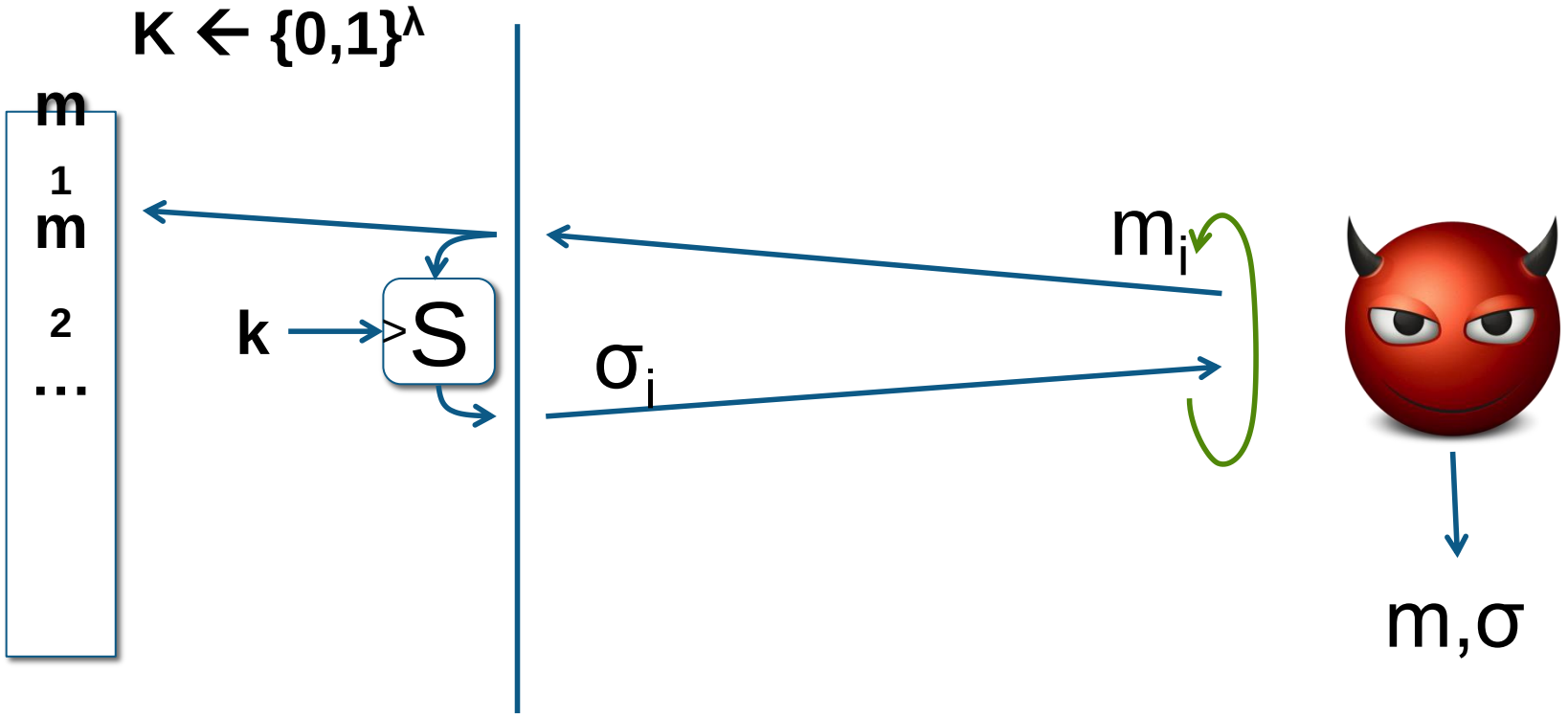
(PRG security)



Message Authentication Codes (MACs)

Message Authentication Codes (MACs)

Recall classical def:

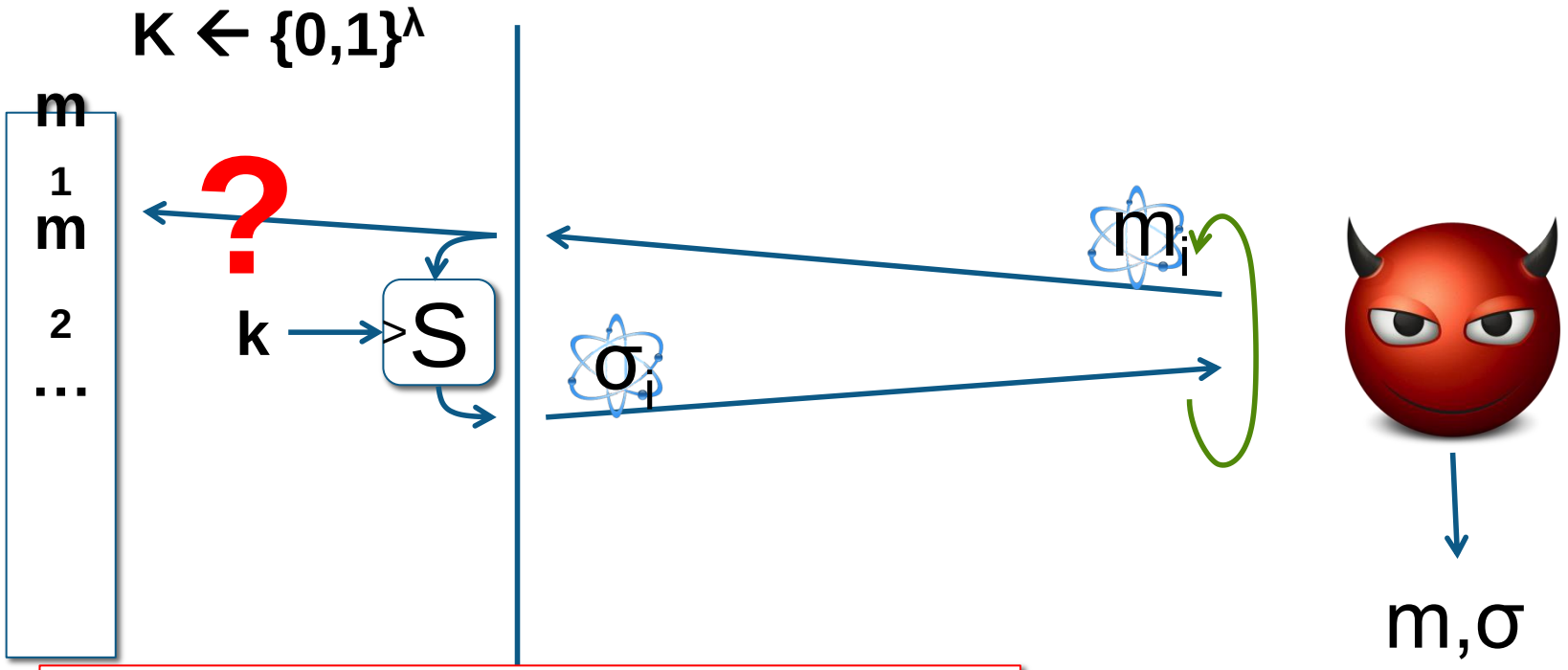


Requirements:

V(k,m,σ) accepts,

m ≠ m$_i$ for any **i**

Quantum Security?



Cannot copy quantum info!

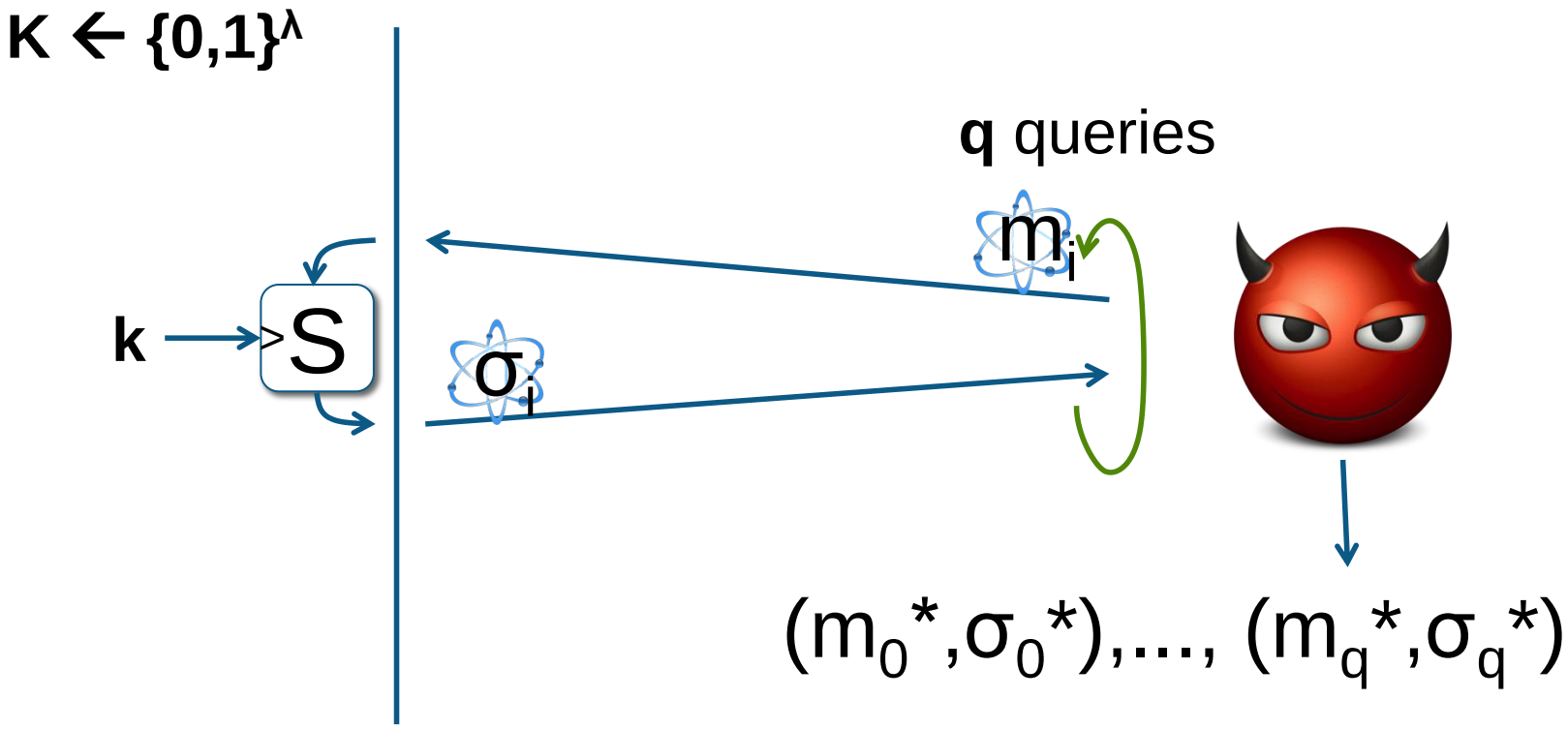
- Must define success without reference to queries

Requirements:

V(k,m,σ) accepts,

m ≠ m$_i$ for any **i**

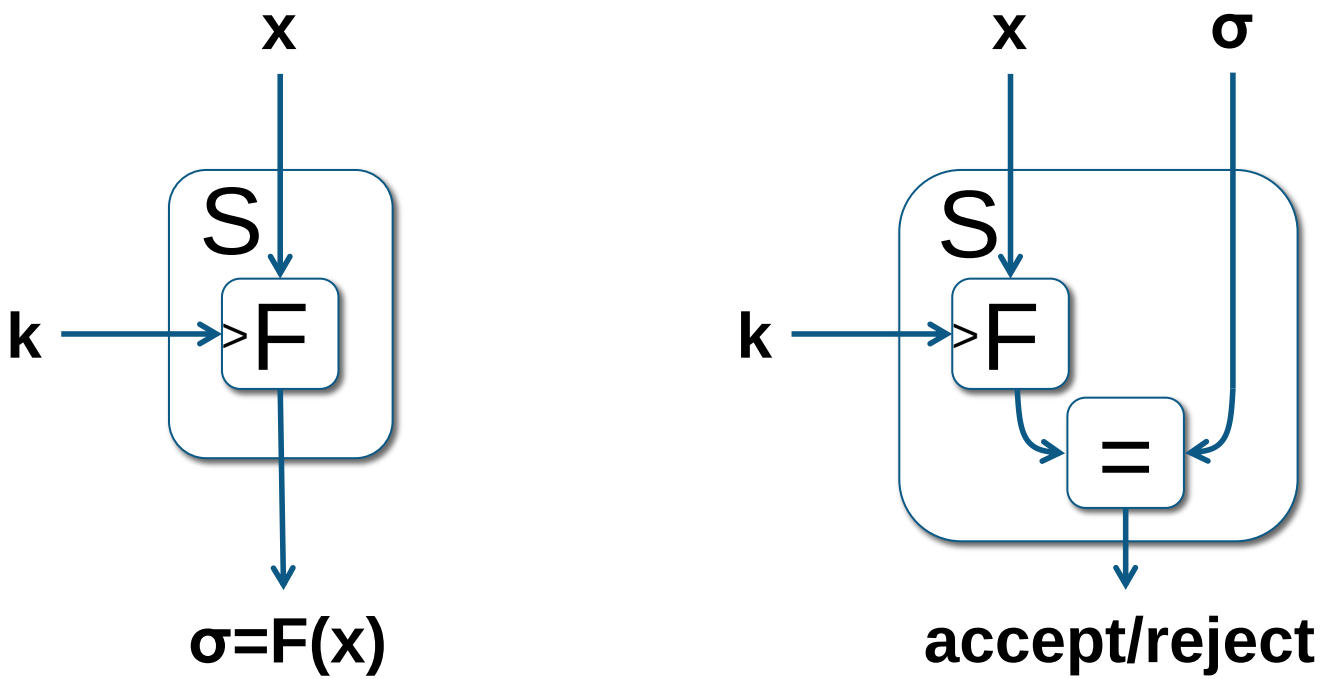
Quantum Security



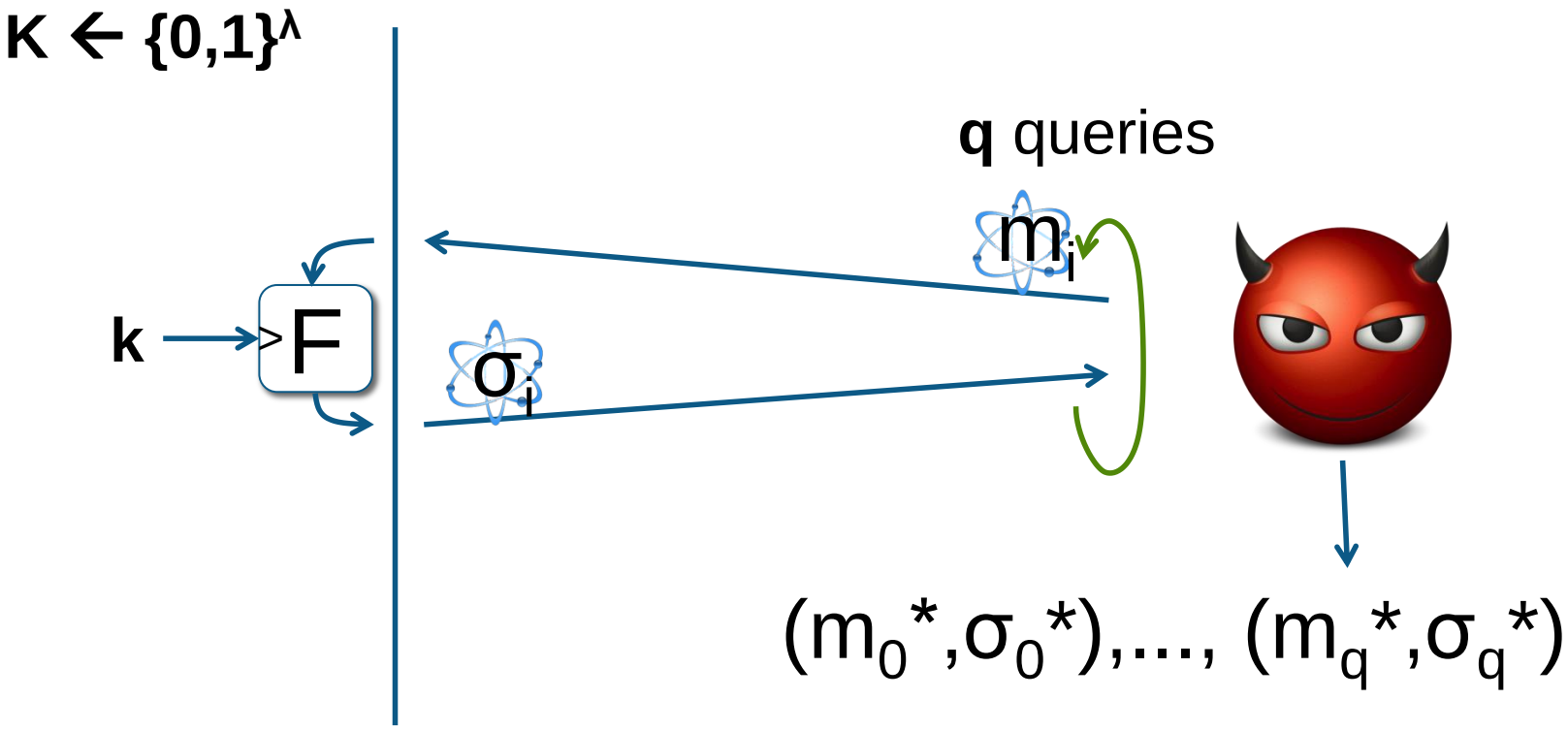
Adversary must produce **q+1** (distinct) forgeries
after making **q** queries

PRF as a MAC

Try classical construction:



Security of PRF as a MAC

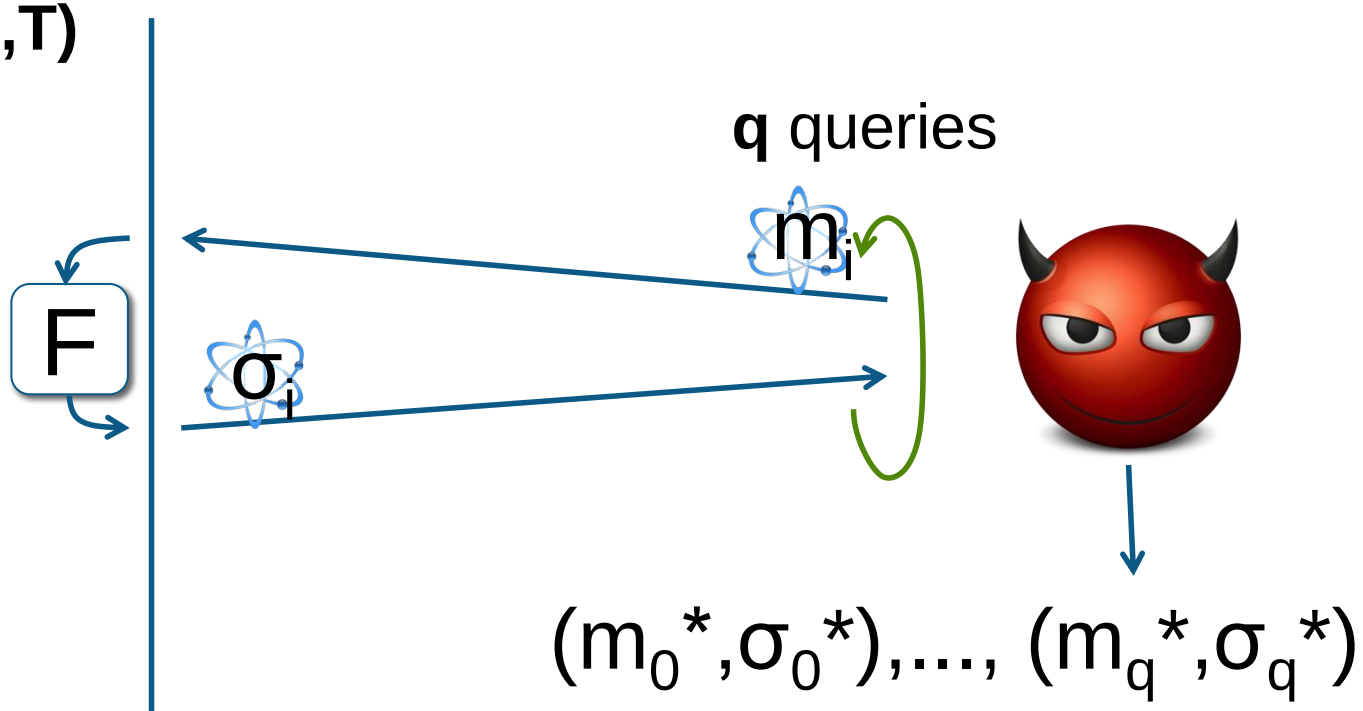


Adversary must produce **q+1** (distinct) input/output pairs of **F** after making **q** queries

Security of PRF as a MAC

Replace **F** with a random function

F ← Funcs(M,T)



Oracle Interrogation:

Adversary must produce **q+1** (distinct) input/output pairs of random function after making **q** queries

Quantum Oracle Interrogation

Classically: hard Adv[**q+1** points]: **1/|T|**

(**1/2^n** for **n**-bit tags)

Quantum: **not so fast**

[vD'98]: random function **F: X → {0,1}**

q quantum queries ⇒ **1.9q** points w.h.p.

Also true for small range size:

ex: random function **F: X → {0,1}^{2}**

q quantum queries ⇒ **1.3q** points w.h.p.

Question: What about large range size?

Quantum Oracle Interrogation

Our result:

Theorem: Random function **F: X → T**

Adv[**q** queries ⇒ **q+1** points] ≤ **(q+1)/|T|**

(only lose factor of **q+1** relative to classical case)

Highly nontrivial

- Invented new quantum impossibility tool: The Rank Method

Takeaway: Quantum Oracle Interrogation easier, but still hard

Back to MAC Security

Classical CMA:

secure PRF ⇒ **secure MAC** (Adv: **1/|T|**)

Quantum CMA:

quantum-secure PRF ⇒ **quantum-secure MAC**

(Adv: **(q+1)/|T|**)

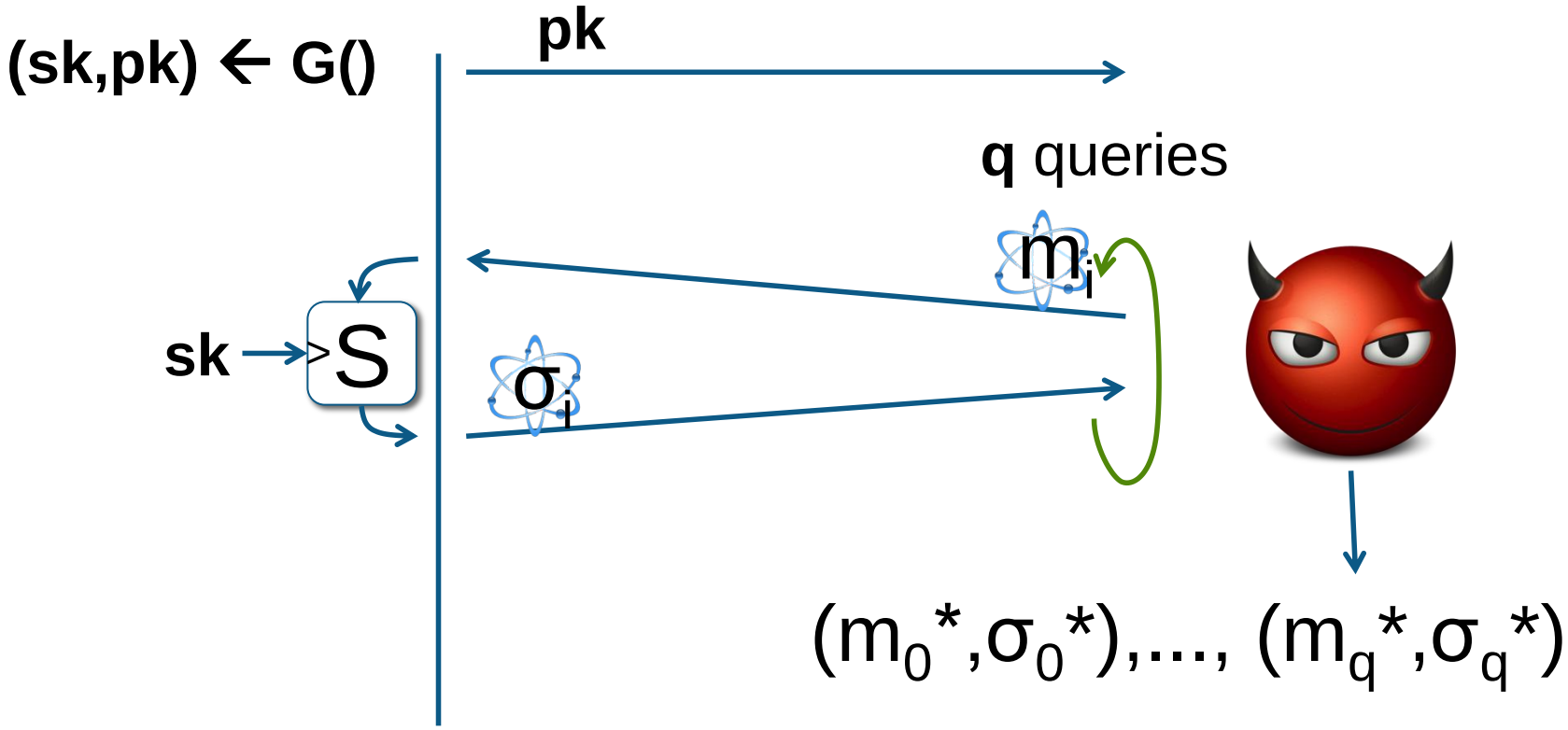
Both cases:

MAC size super-logarithmic ⇒ **MAC is secure**

Signatures

Signatures

Naturally extend MAC definition



Proof Difficulties

Aborts are problematic

- Can’t both abort and continue

Adversary can tell if signatures are invalid

- Need to sign all messages correctly

Previous quantum proof techniques 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?

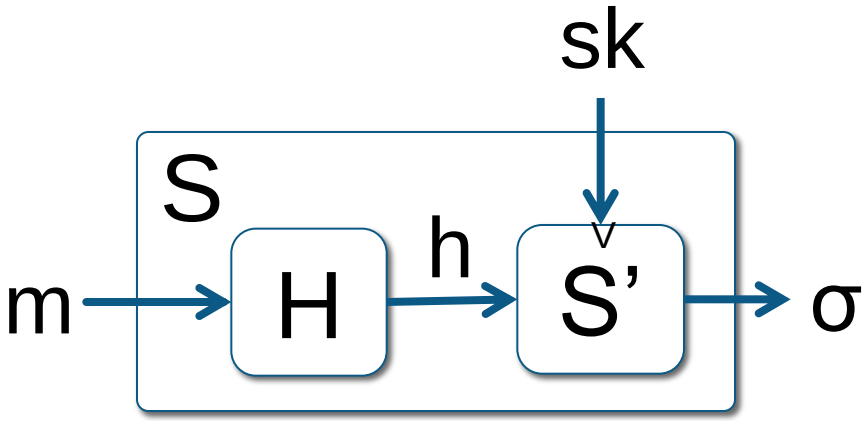
Examples:

- 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:



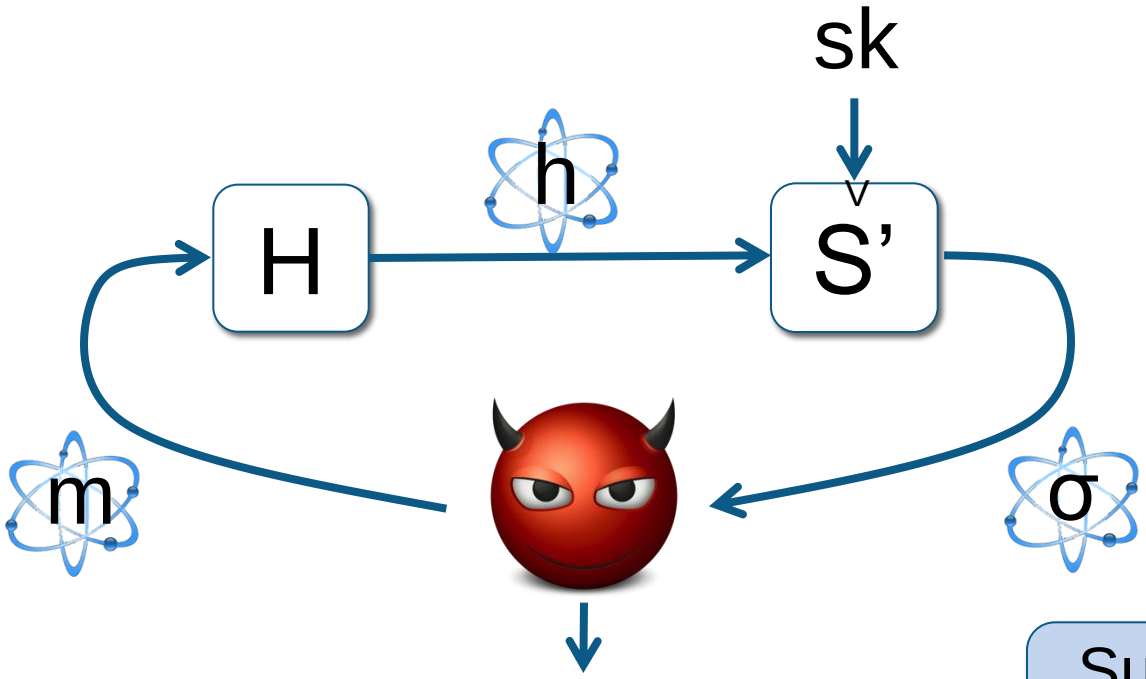
Classical Advantages:

- 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



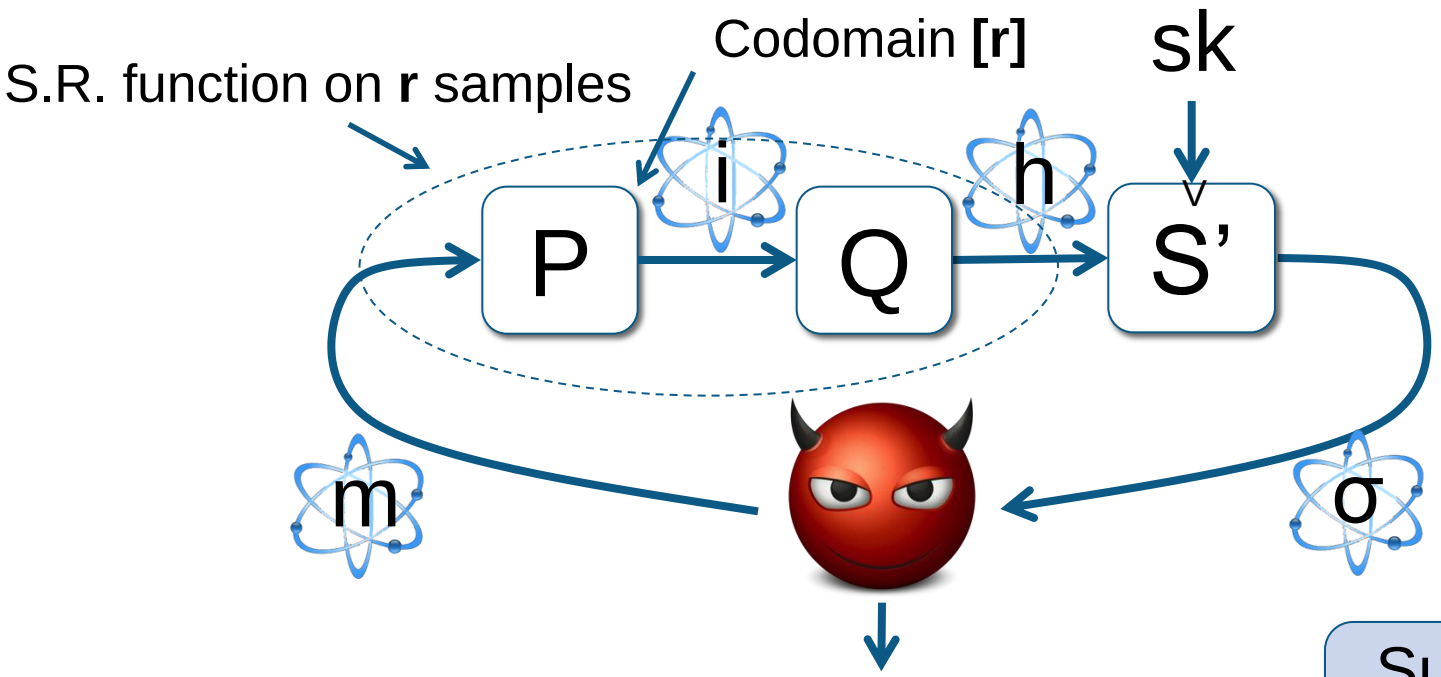
Success prob: ε

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

Problem: exponentially many **h**

→ must query **S'** too many times

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



Success prob: ε/2

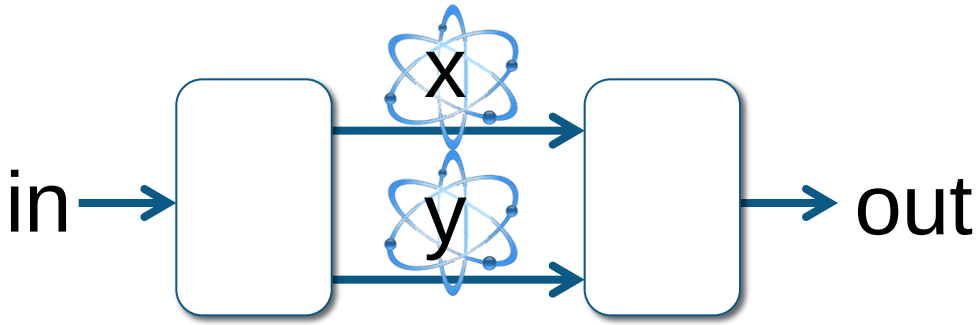
Now **S'** only queried on **r** inputs → Can simulate

Next Step: Use one of the σ_i as a forgery for **S'**

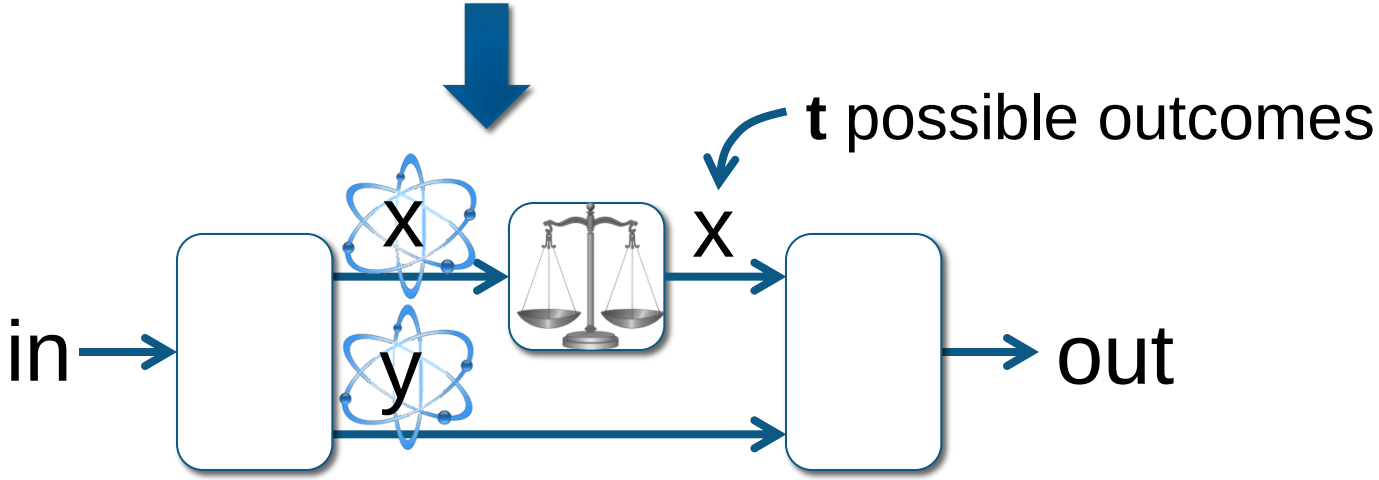
Problem: # of sigs (**q+1**) **<<** # of **S'** queries (**r**)

Intermediate Measurement

New quantum simulation technique:

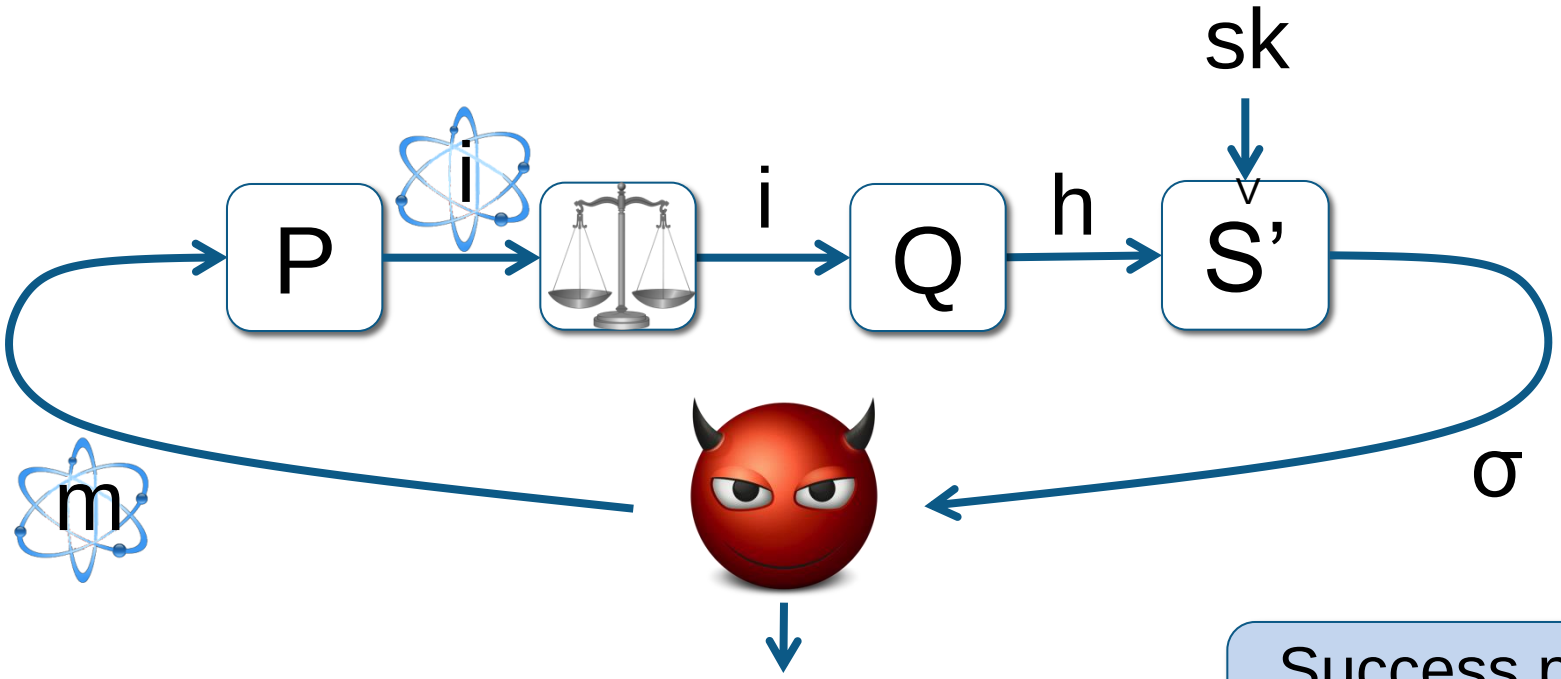


Success prob: **σ**



Theorem: Success prob: ≥**σ/t**

Step 2: Measure Output of **P**



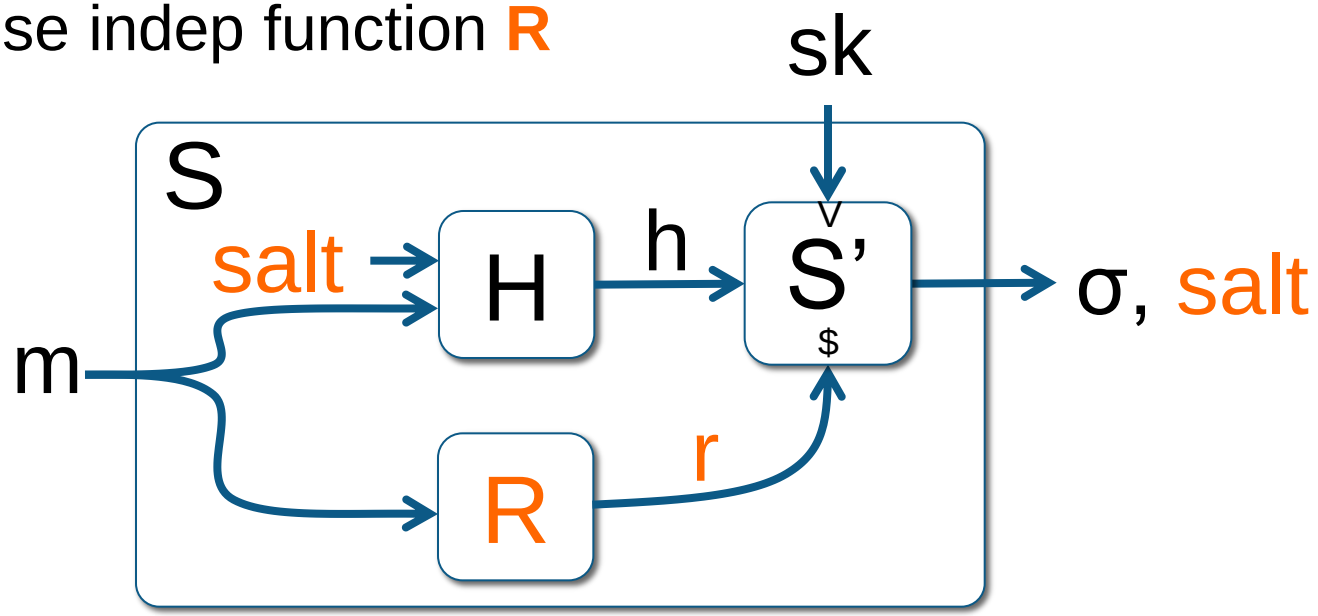
Only **q** queries to **S'** → One of the $\boldsymbol{\sigma}_i$ must be forgery for **S'**

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 ⇒ quantum-secure signatures

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

Result Summary

Quantum CCA Encryption

- One specific example

Quantum PRFs

- From generators [GGM'84], synthesizers [NR'95], or LWE [BPR'11]

Quantum MACs

- PRF as a MAC
- Modification of Carter-Wegmen [WC'81]

Quantum CMA-secure Signatures

- Two generic conversions
- From collision resistance

Open Problems

Prove quantum security for more existing schemes

- CBC-MAC, NMAC, etc.
- Hash and Sign without salting
- …

Improve tightness of reductions

- Most of our security reductions are very loose