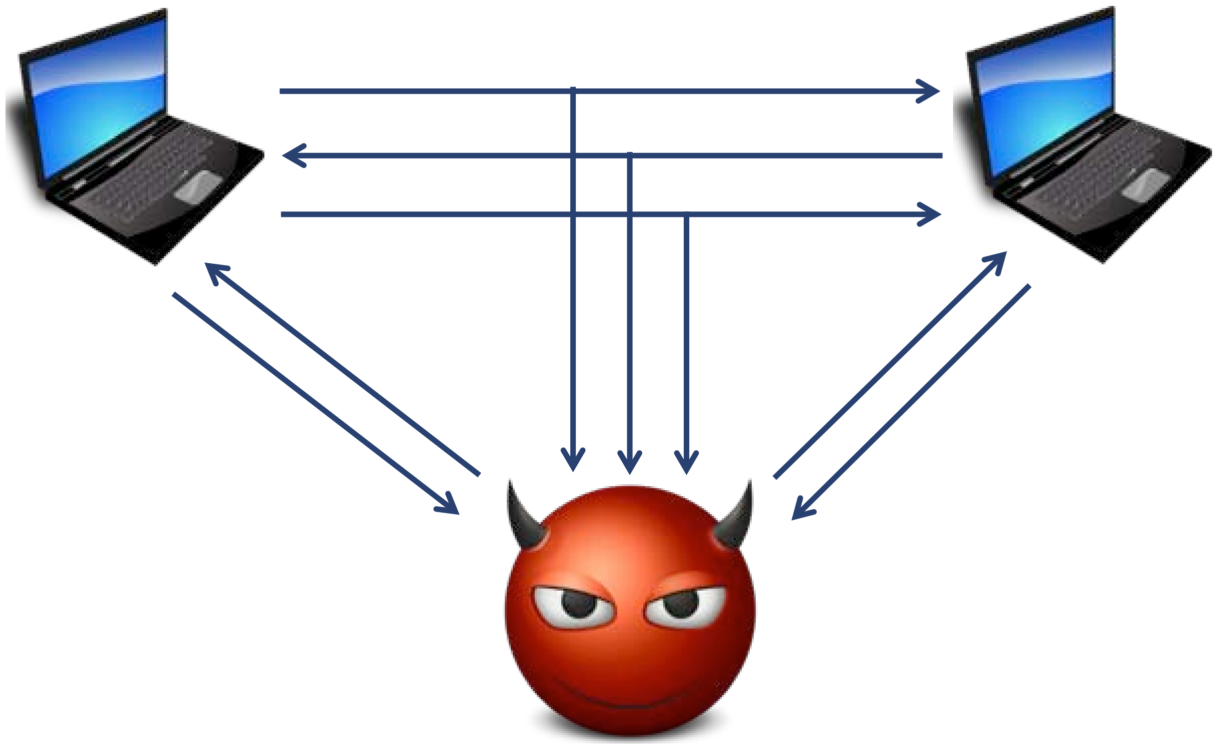
BEYOND POST–QUANTUM CRYPTOGRAPHY

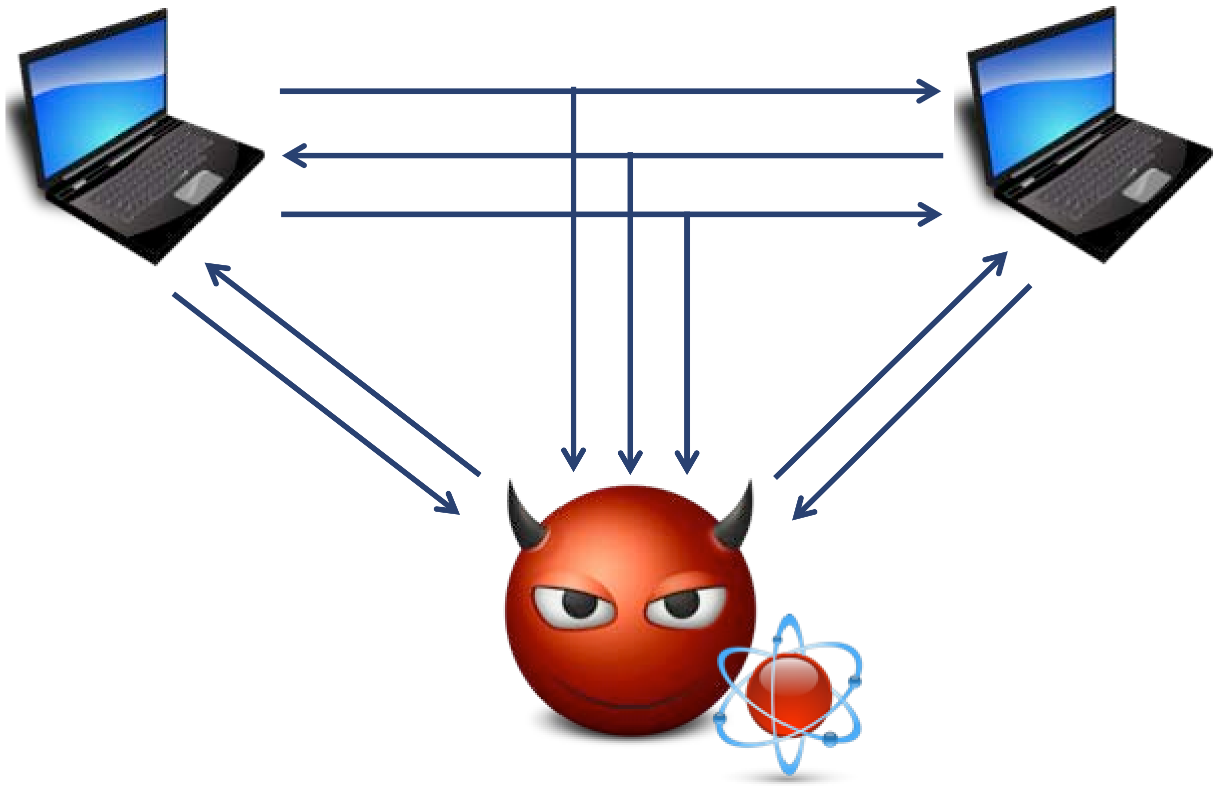
Mark Zhandry – Stanford University

Joint work with Dan Boneh

Classical Cryptography



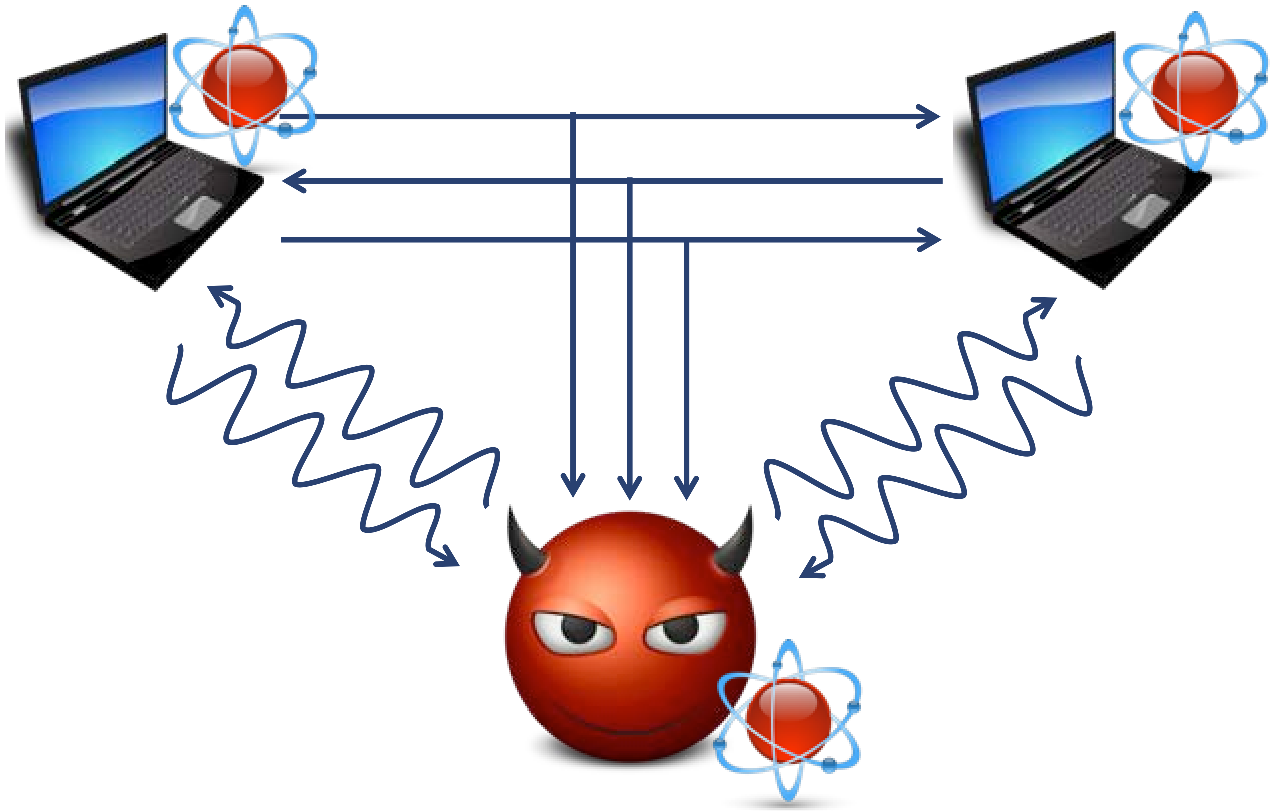
Post-Quantum Cryptography



All communication stays classical

Beyond Post-Quantum Cryptography

Eventually, all computers will be quantum

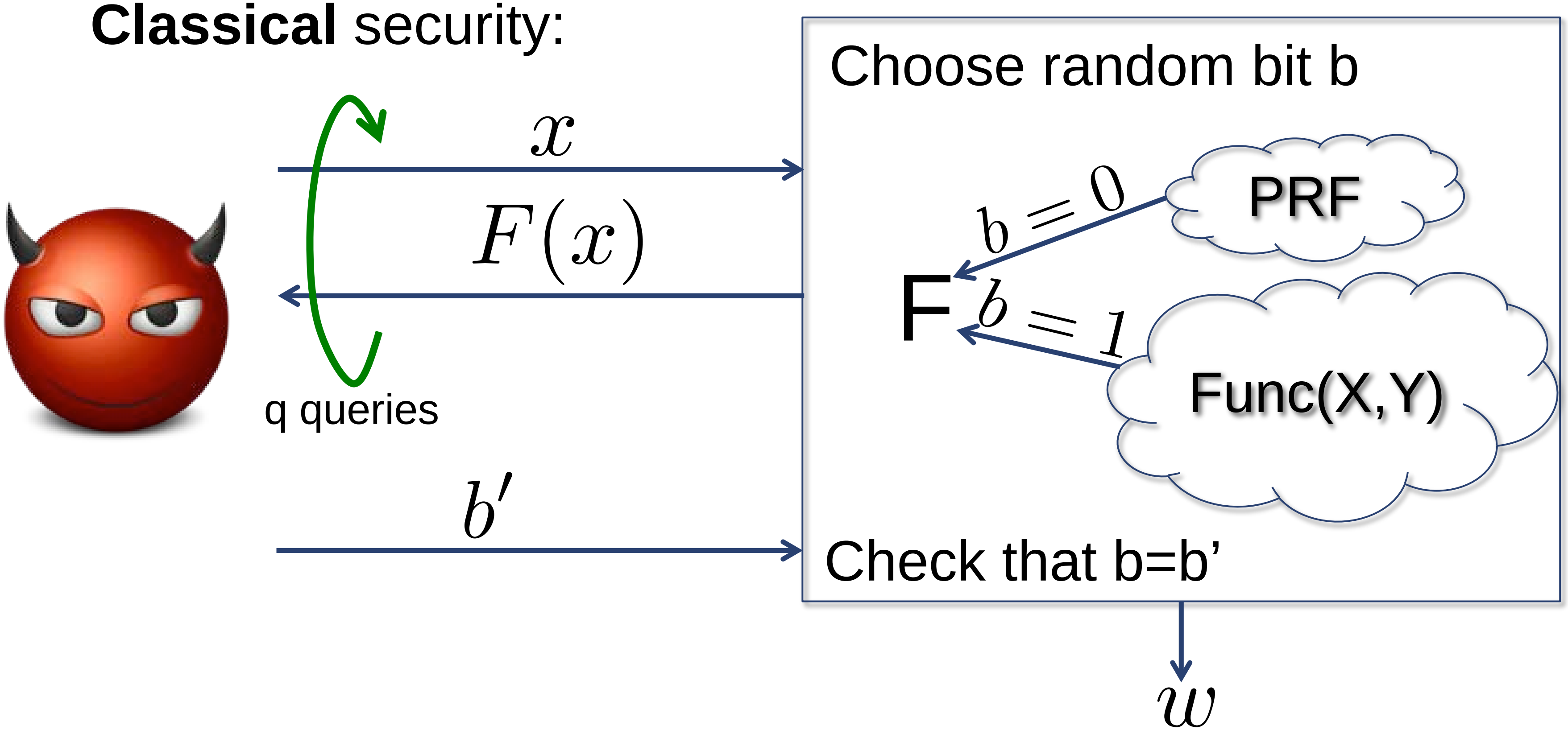


Adversary may use quantum interactions
⟶ need new security definitions

Example: Pseudorandom Functions

[GGM'84]

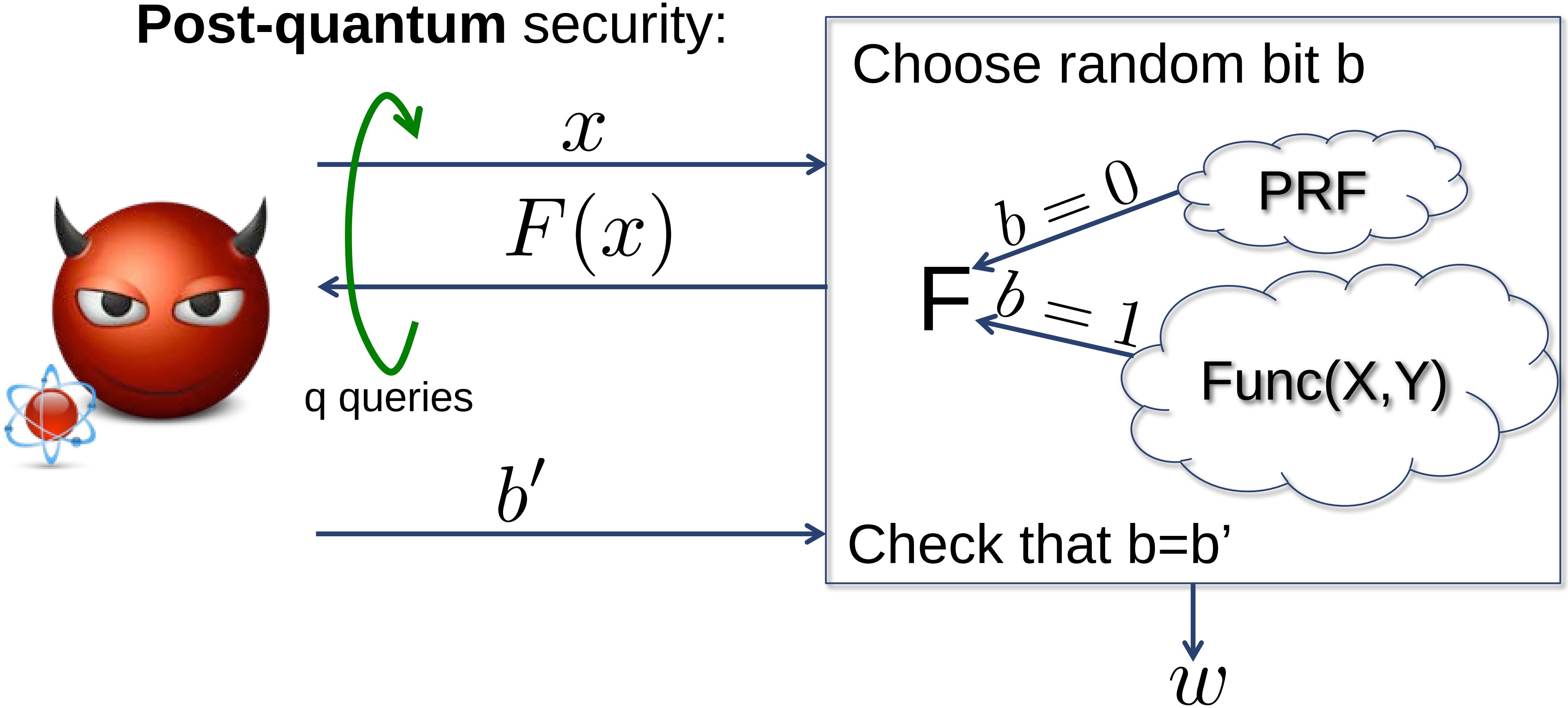
Classical security:



PRF is secure if $\left|\Pr[w=1] - \frac{1}{2}\right| < \mathtt{negl}$

Example: Pseudorandom Functions

Post-quantum security:

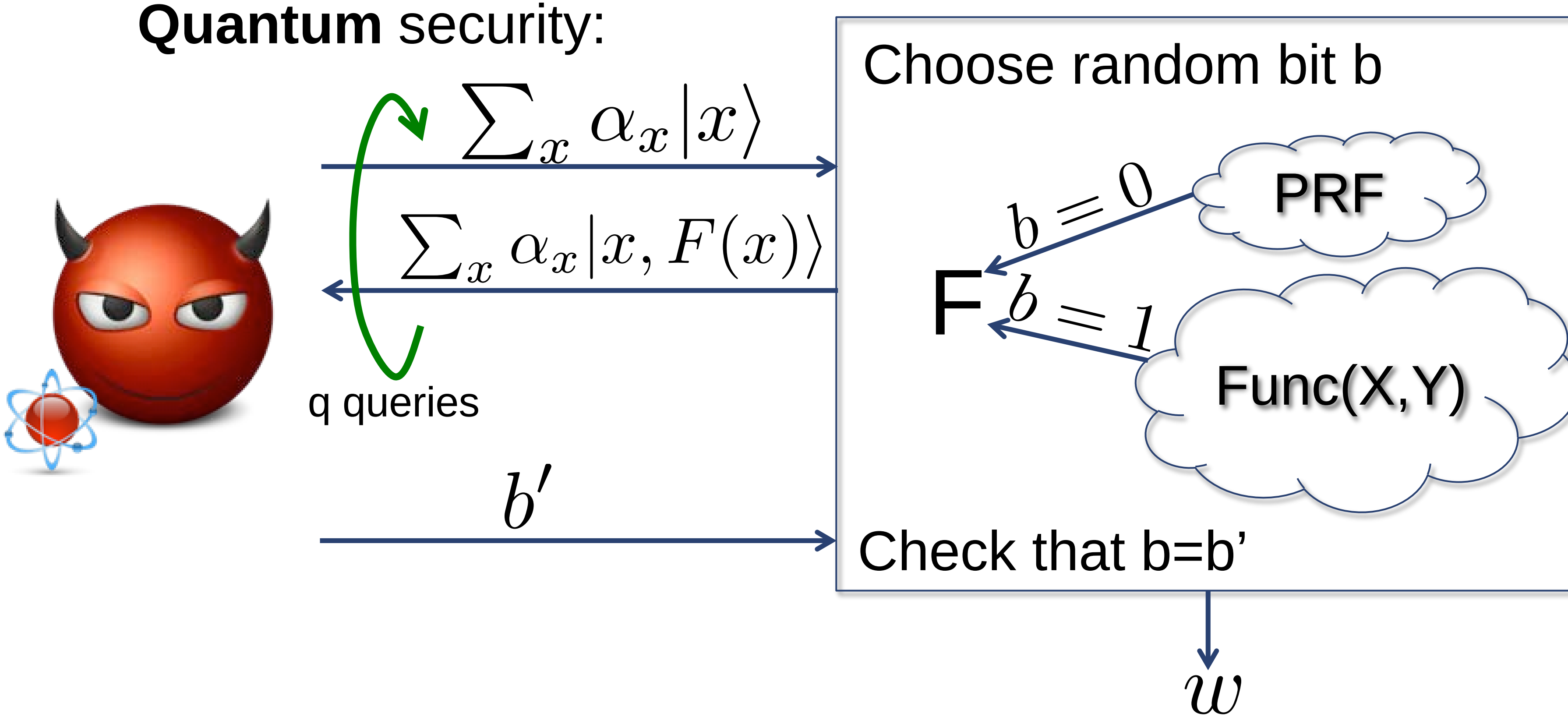


PRF is secure if $\left|\Pr[w=1] - \frac{1}{2}\right| < \texttt{negl}$

Example: Pseudorandom Functions

[Aar'09]

Quantum security:



PRF is secure if $\left|\Pr[w=1] - \frac{1}{2}\right| < \mathtt{negl}$

Post-Quantum vs Full Quantum Security

In post-quantum setting, security games generally don't change, only adversary's computational power

$\longrightarrow$ Can often replace primitives with quantum-immune primitives and have classical proof carry through

For full quantum security, security game itself is quantum

$\longrightarrow$ Now, classical proofs often break down

$\longrightarrow$ Need new tools to prove security

Non-interactive Security Games

If no interaction, security game does not change

$\longrightarrow$ no difference between post-quantum and full quantum security

Examples:

- One-way functions
- Pseudorandom generators
- Collision-resistant hash functions

In these cases, classical proofs often do carry through

- Example:

  quantum-secure OWFs → quantum-secure PRGs

This Talk

A First Step: The Quantum Random Oracle Model

[BDFLSZ'11, Zha'12a]

Full Quantum Security:

- Quantum-secure PRFs (or quantum PRFs) [Zha'12b]
- Quantum-secure MACs [BZ'12]
- Quantum-secure Signatures and Encryption [BZ'13]

Quantum Random Oracle Model

Quantum Random Oracle Model

[BDFLSZ'11]

A first step towards full quantum security

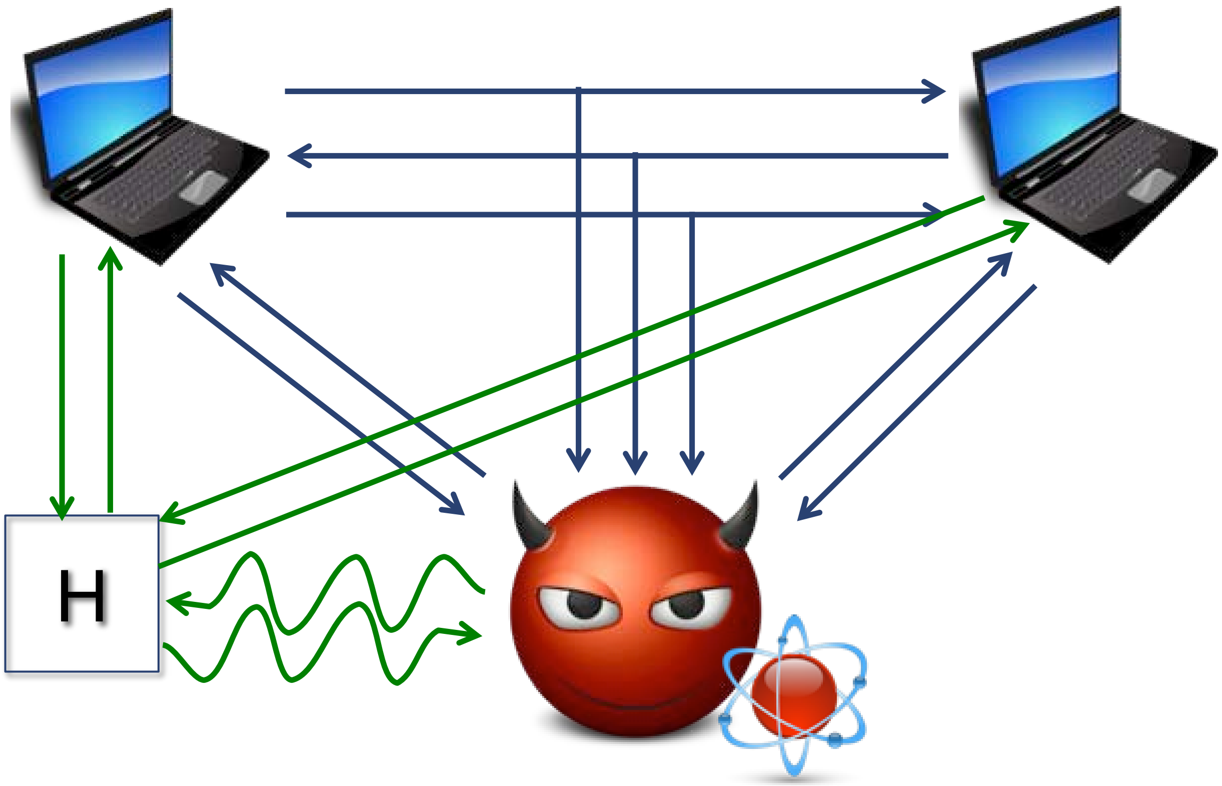
Honest parties still classical (i.e. post-quantum world)

Model hash function as a random oracle that accepts quantum queries

- Captures ability of adversary to evaluate hash function on superposition of inputs

All other interaction remains classical

Quantum Random Oracle Model



Quantum Random Oracle Model

Proven secure [BDFLSZ'11, Zha'12a]

- Several signature schemes (inc. GPV)
- CPA-secure encryption
- GPV identity-based encryption

Not yet proven

- Signatures from identification protocols (Fiat-Shamir)
- CCA Encryption from weaker notions

Full Quantum Security

Quantum-secure PRFs:

- PRFs: building block for most of symmetric crypto
  - PRPs (e.g. Luby-Rankoff), encryption schemes, MACs

Quantum-secure MACs:

- PRF → MAC
- Natural question: quantum PRF → quantum-secure MAC?

Quantum-secure Signatures and Encryption

- From generic assumptions?
- Security of schemes in the literature?

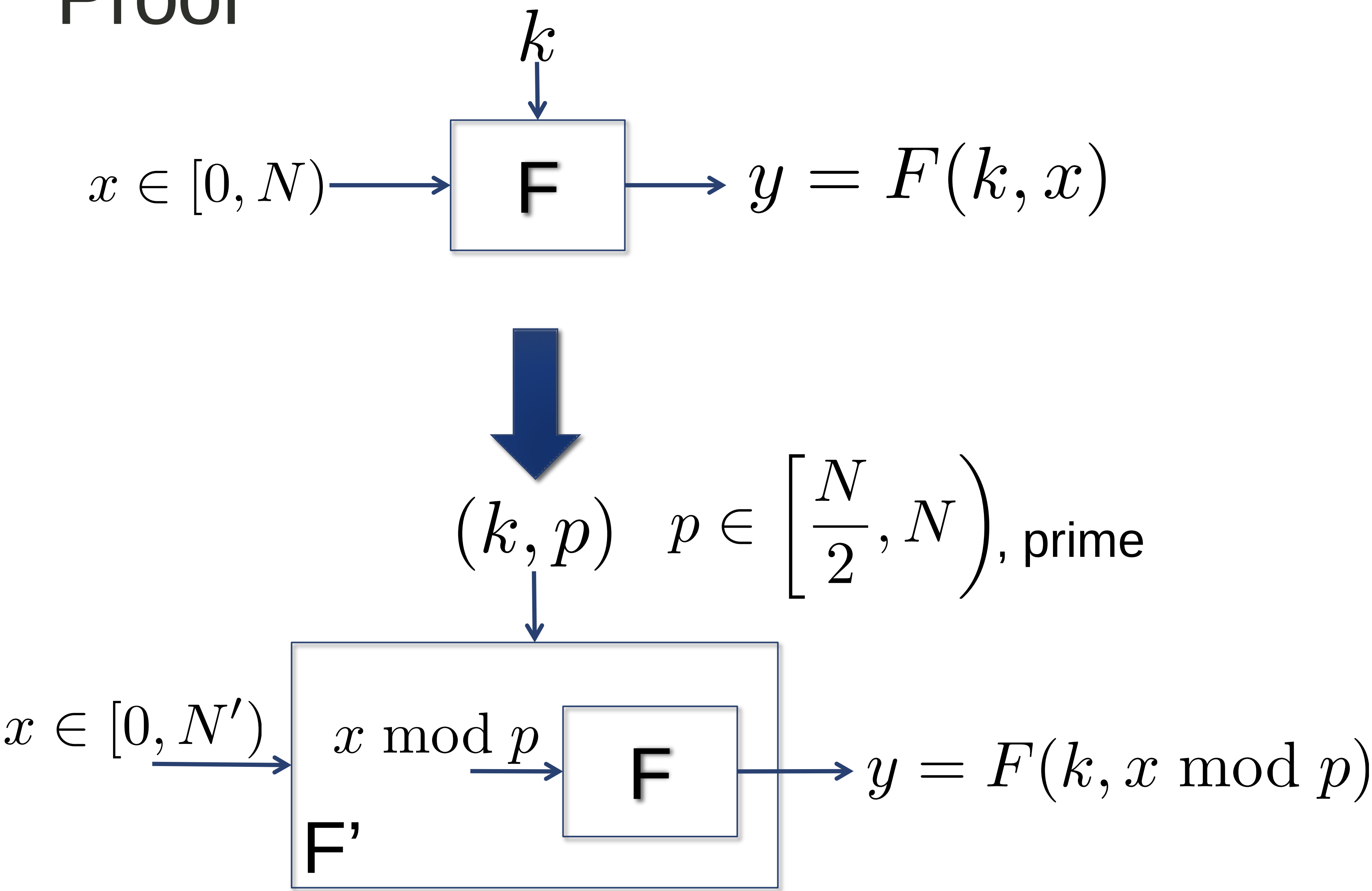
Quantum PRFs [Zha'12b]

Separation

PRF < Quantum PRF

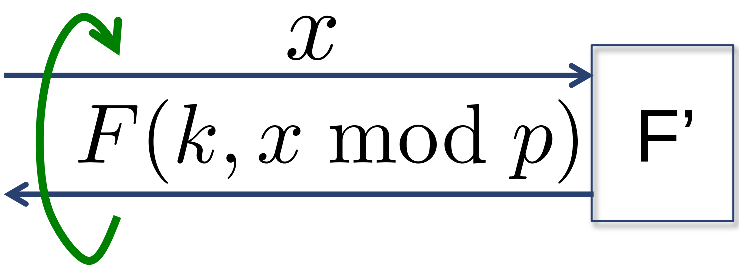
Theorem: If post-quantum PRFs exist, then there are post-quantum PRFs that are not quantum PRFs

Proof

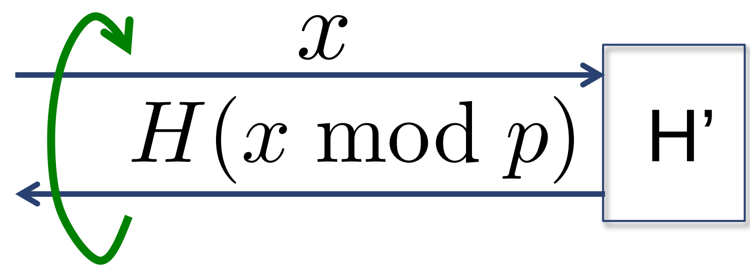

k
$x \in [0, N)$
F
$y = F(k, x)$
(k, p)
$p \in \left[\frac{N}{2}, N\right)$, prime
$x \in [0, N')$
$x \bmod p$
F
F'
$y = F(k, x \bmod p)$

Proof

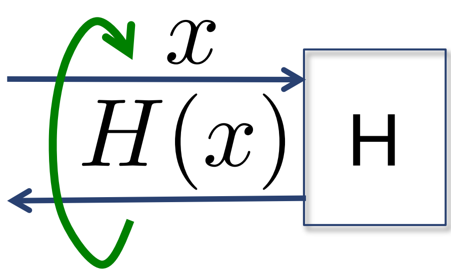
Lemma 1: If F is post-quantum secure, then so is F'.



$\approx_{\mathrm{QP}}$



$\approx_{\mathrm{QP}}$



As long as $x \bmod p \neq x' \bmod p$ for all queries $x \neq x'$, this looks like a random oracle

Probability this fails: $O(q^2(\log N)/N)$

Proof

Lemma 2: Either F or F' are not quantum secure.

F'(x+p) = F'(x) ← Periodic!

Quantum queries can find p [BL'95]

Once we know p, easy to distinguish F' from random

How to Construct Quantum PRFs

Hope that classical PRFs work in quantum world:

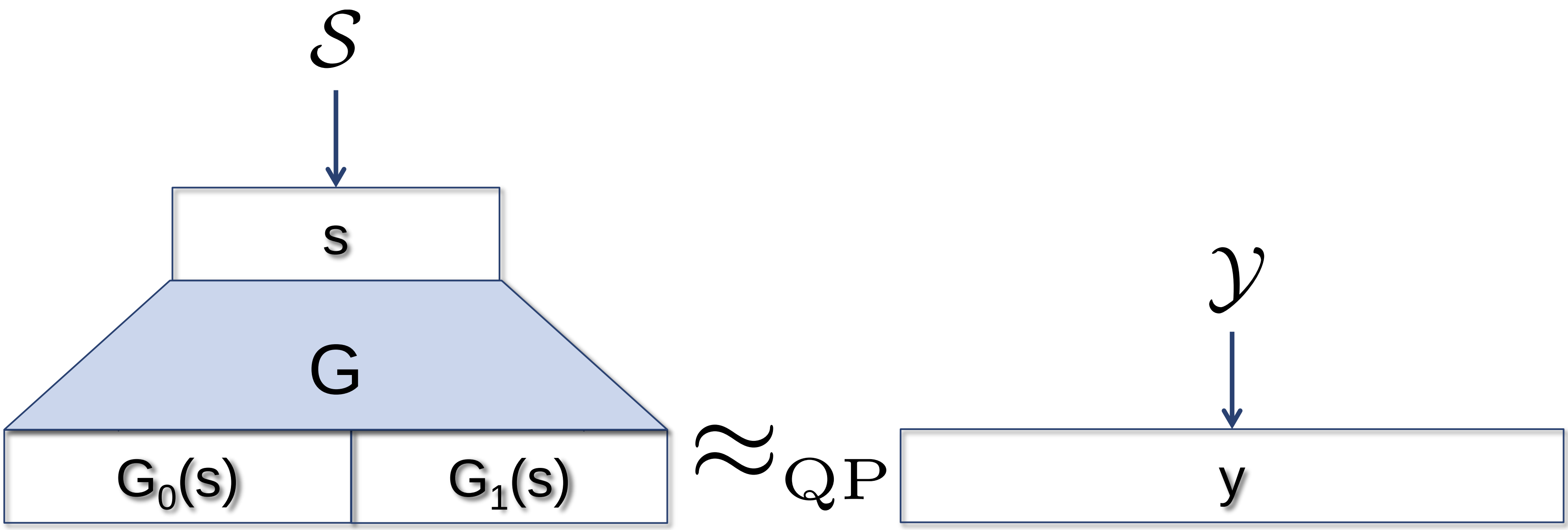
- From quantum-secure pseudorandom generators [GGM'84]
- From quantum-secure pseudorandom synthesizers [NR'95]
- Directly from lattices [BPR'11]

Classical proofs do not carry over into the quantum setting

$\longrightarrow$ Need new proof techniques

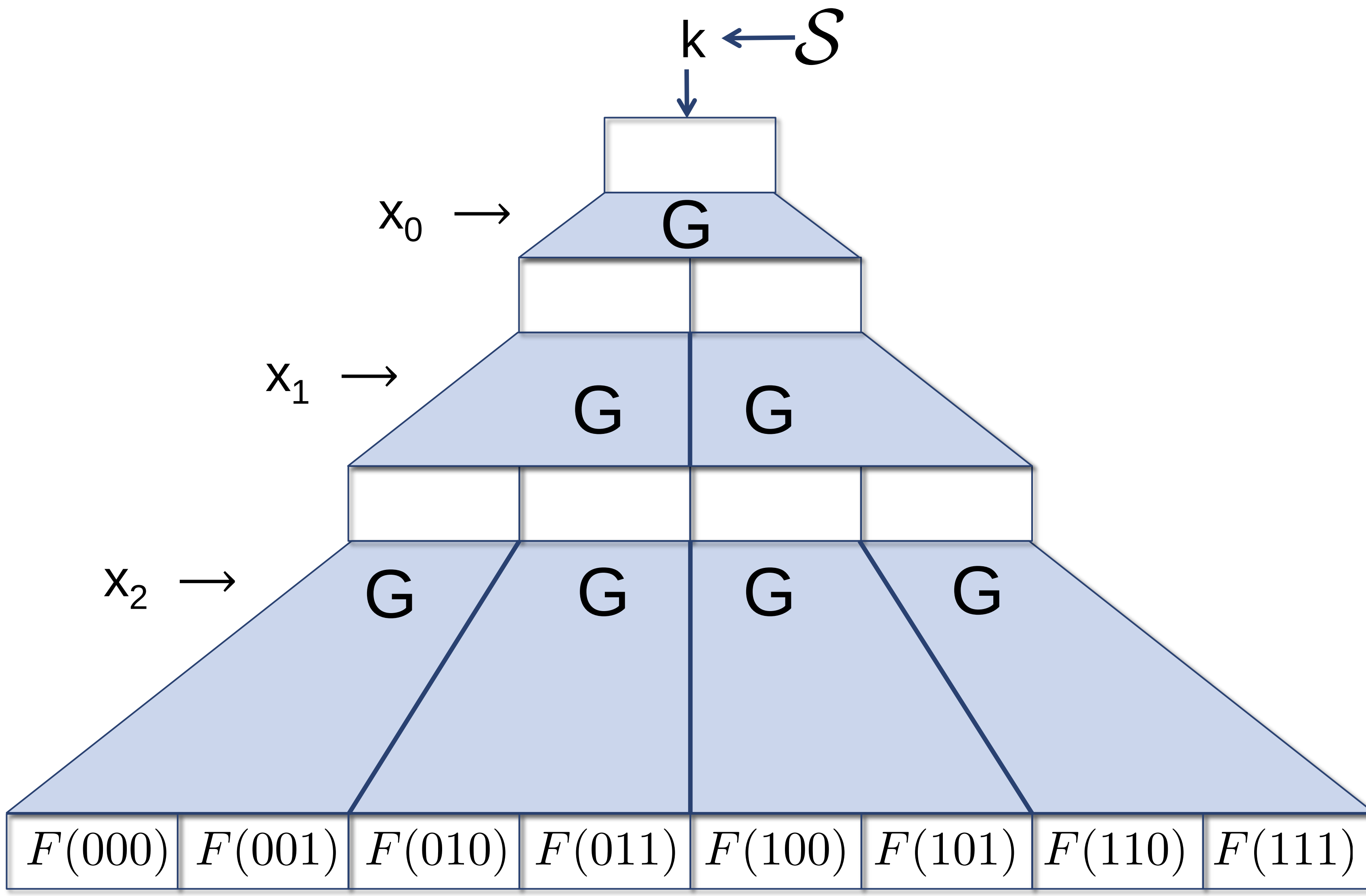
Example: GGM

Pseudorandom Generators



Indistinguishable for Quantum Machines

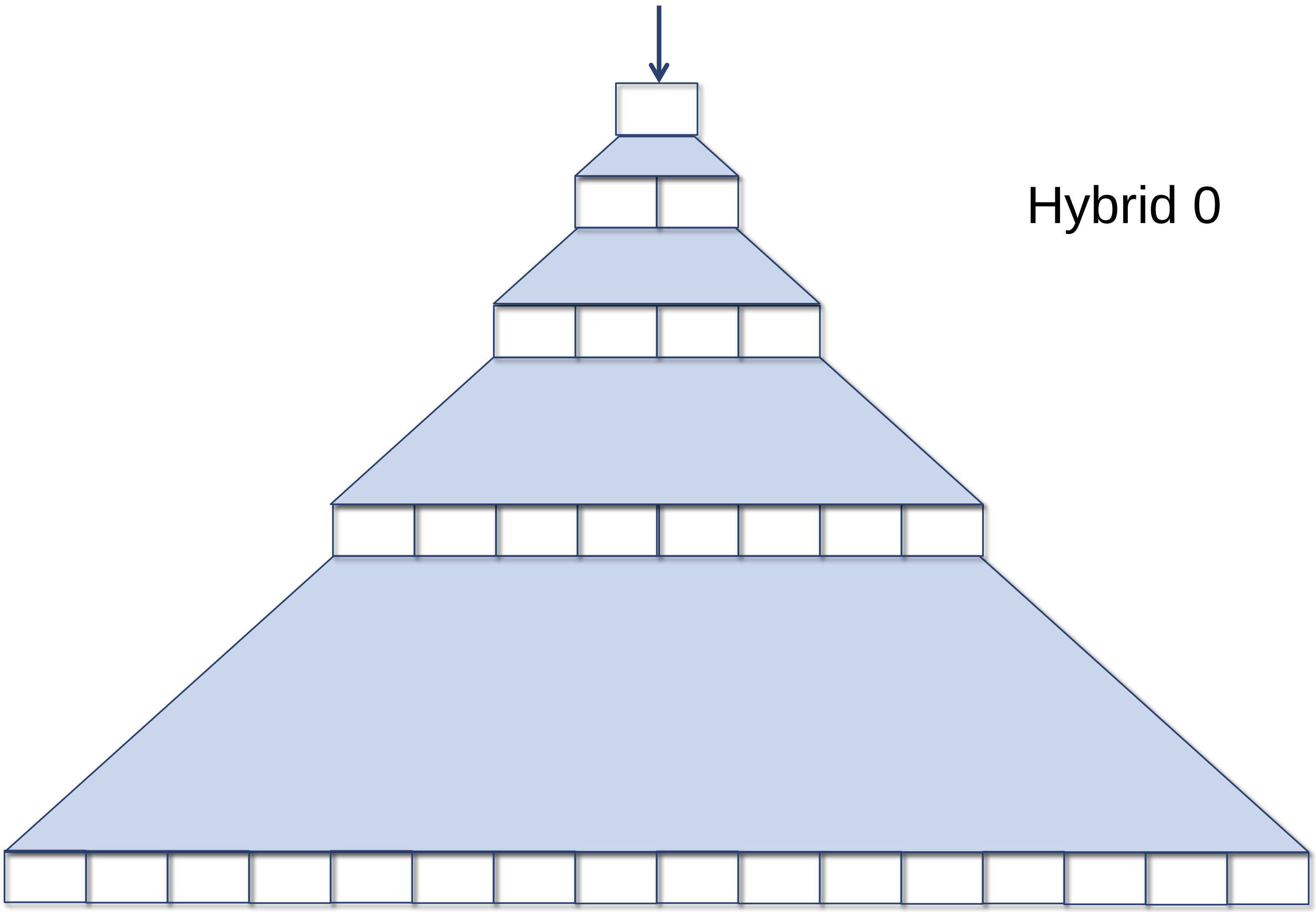
The GGM Construction



Original Security Proof

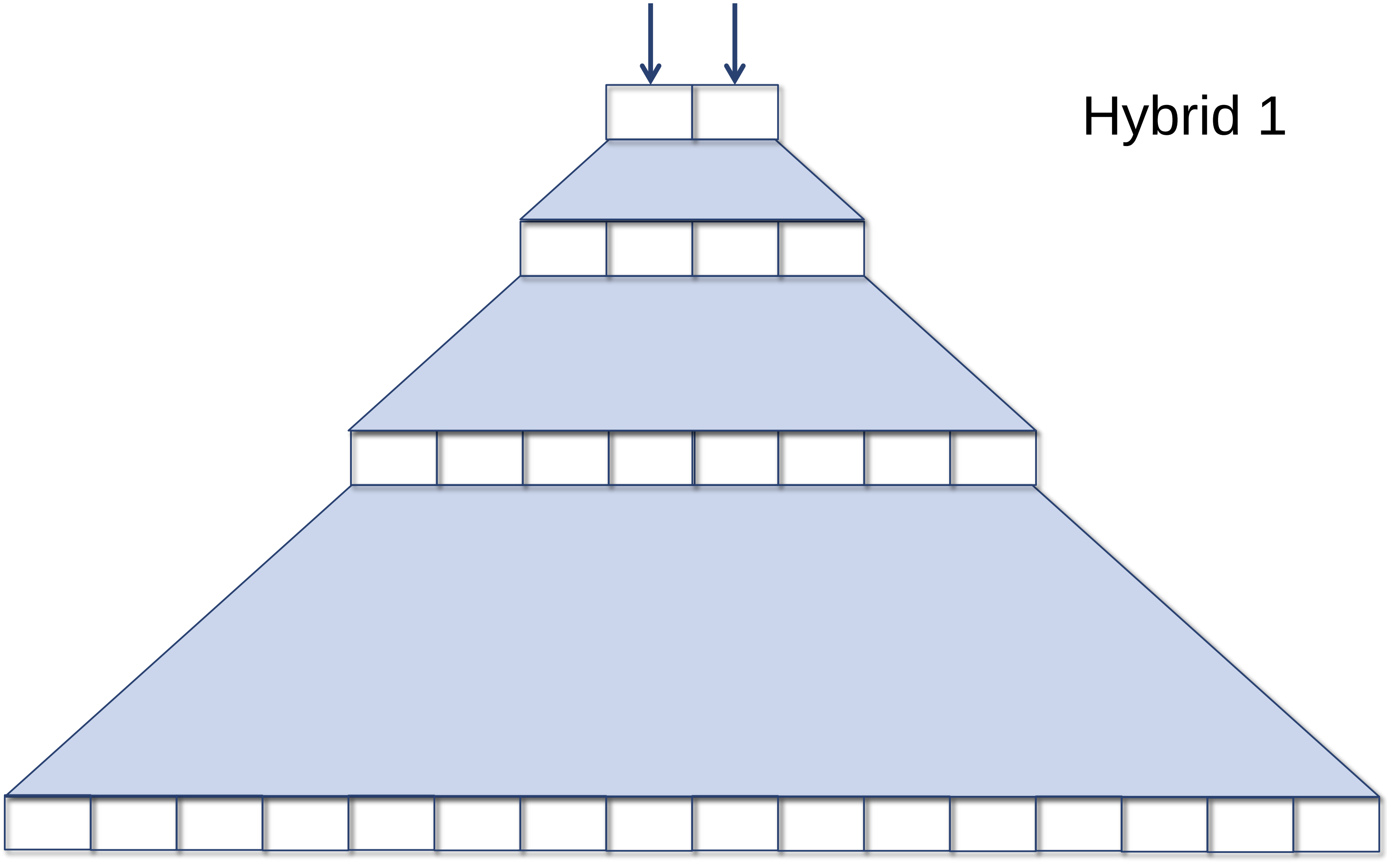
Step 1: Hybridize over levels of tree

Original Security Proof: Step 1



Hybrid 0

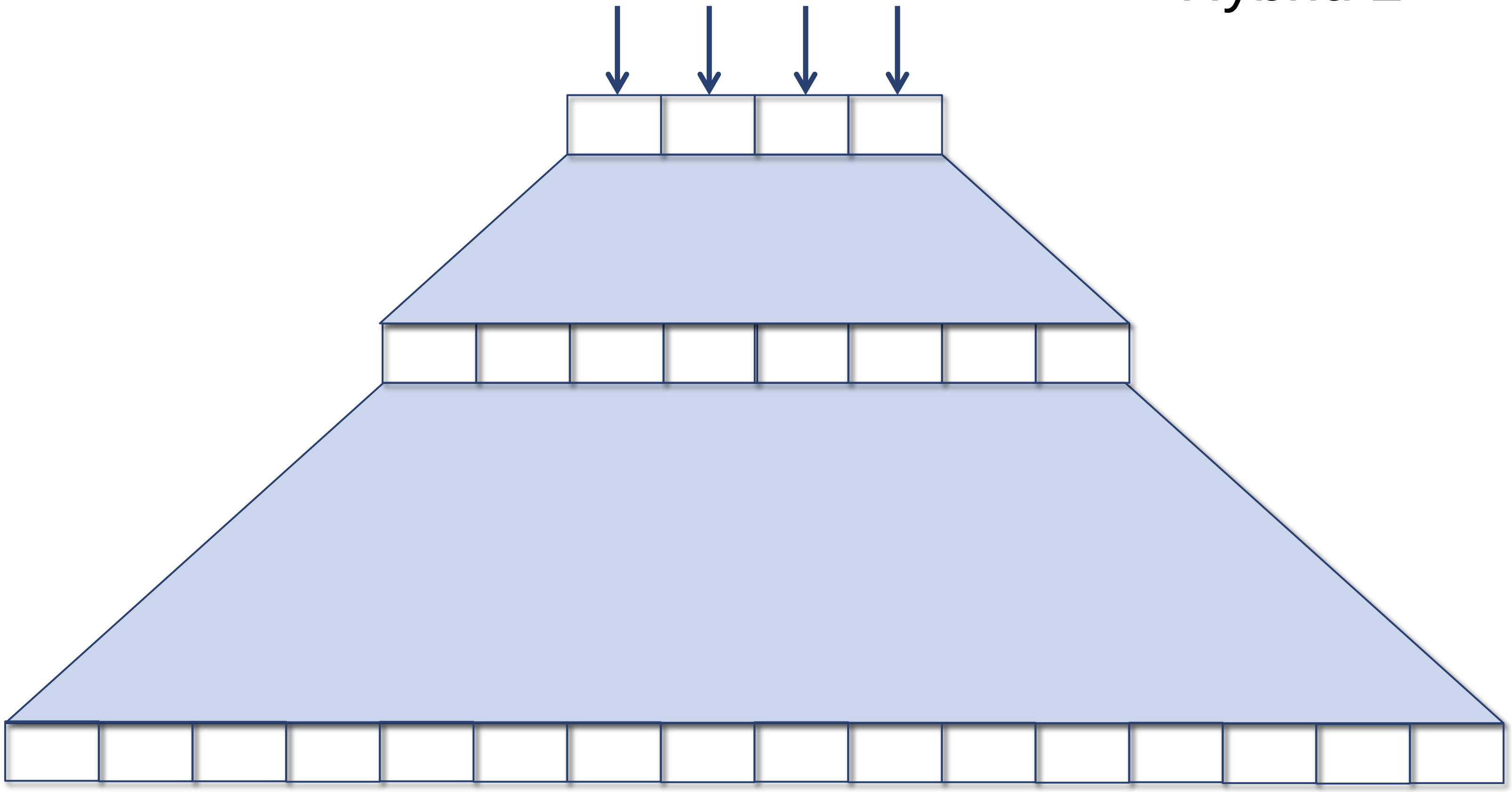
Original Security Proof: Step 1



Hybrid 1

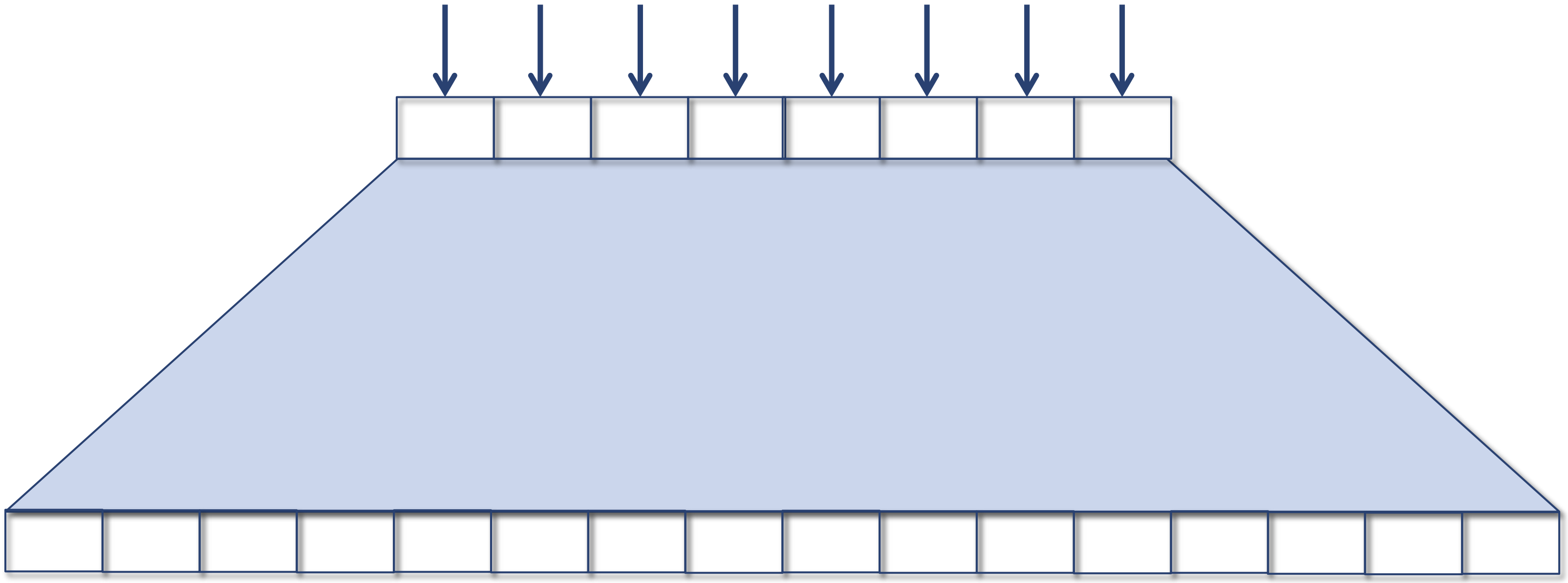
Original Security Proof: Step 1

Hybrid 2



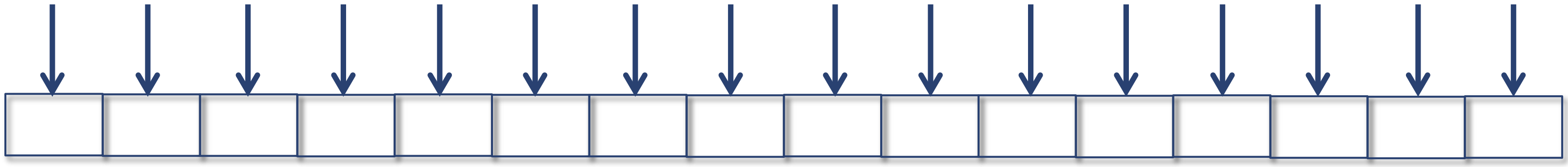
Original Security Proof: Step 1

Hybrid 3



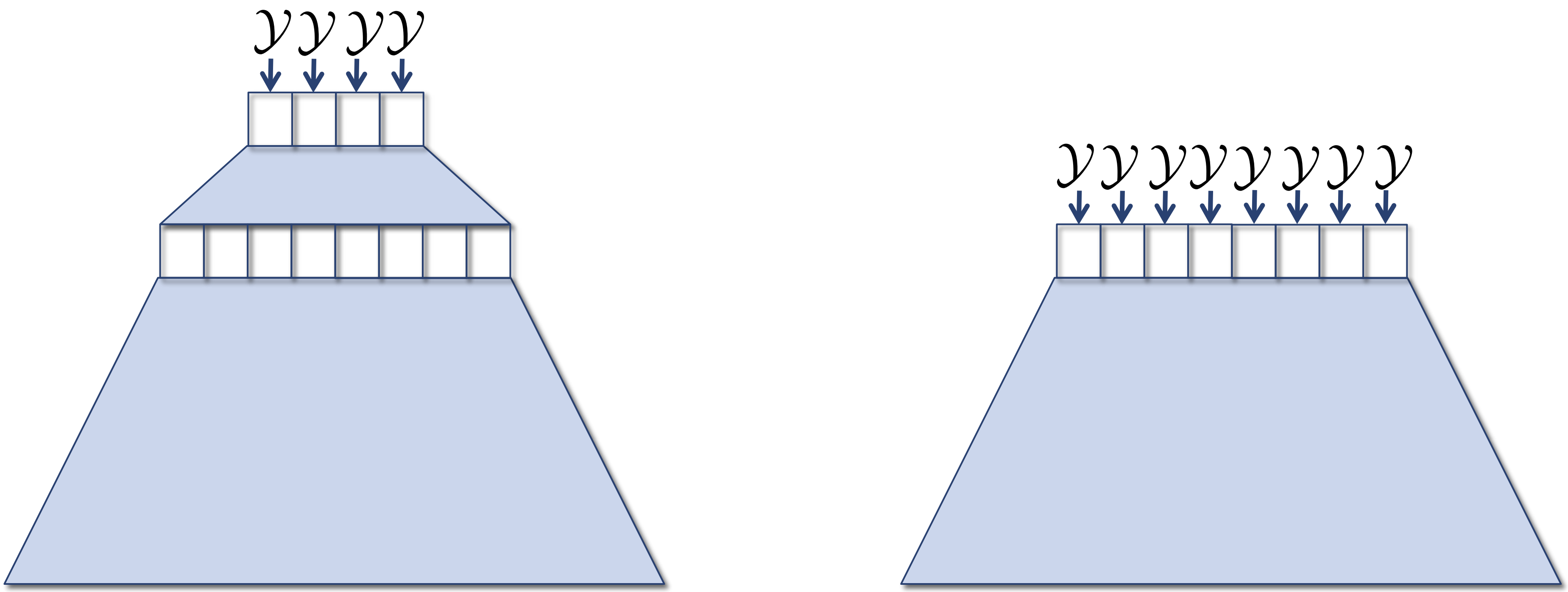
Original Security Proof: Step 1

Hybrid n



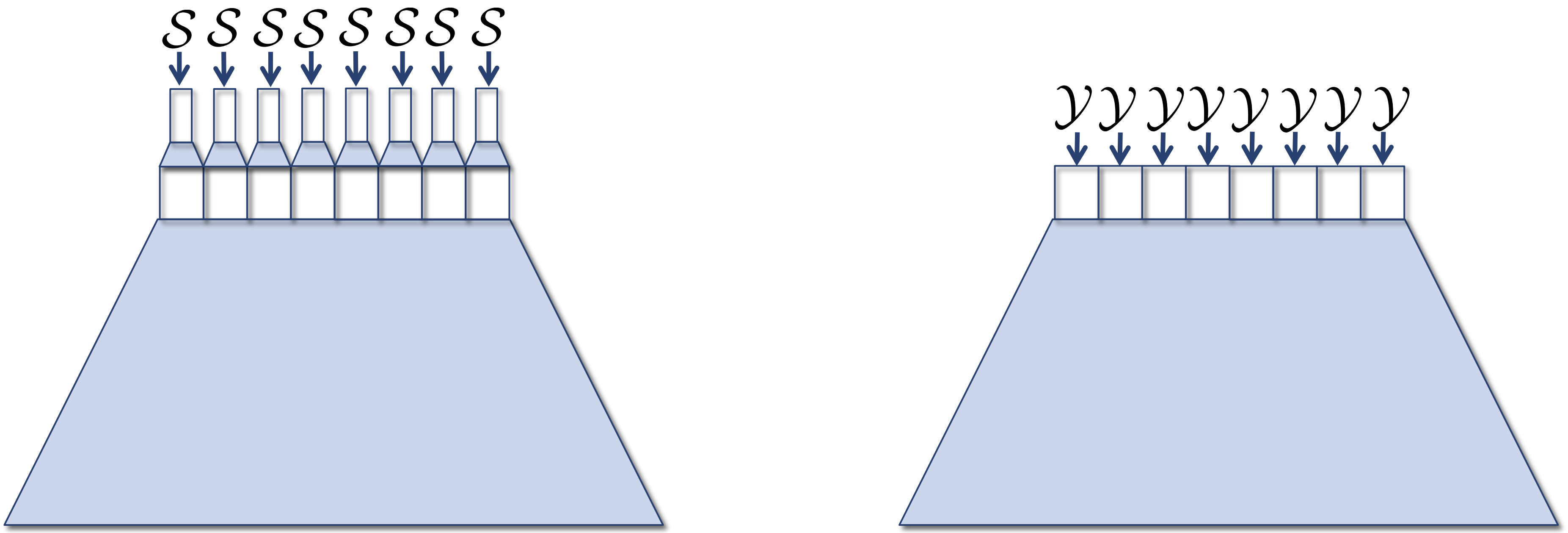
Original Security Proof: Step 1

PRF distinguisher will distinguish two adjacent hybrids



Original Security Proof: Step 1

PRF distinguisher will distinguish two adjacent hybrids

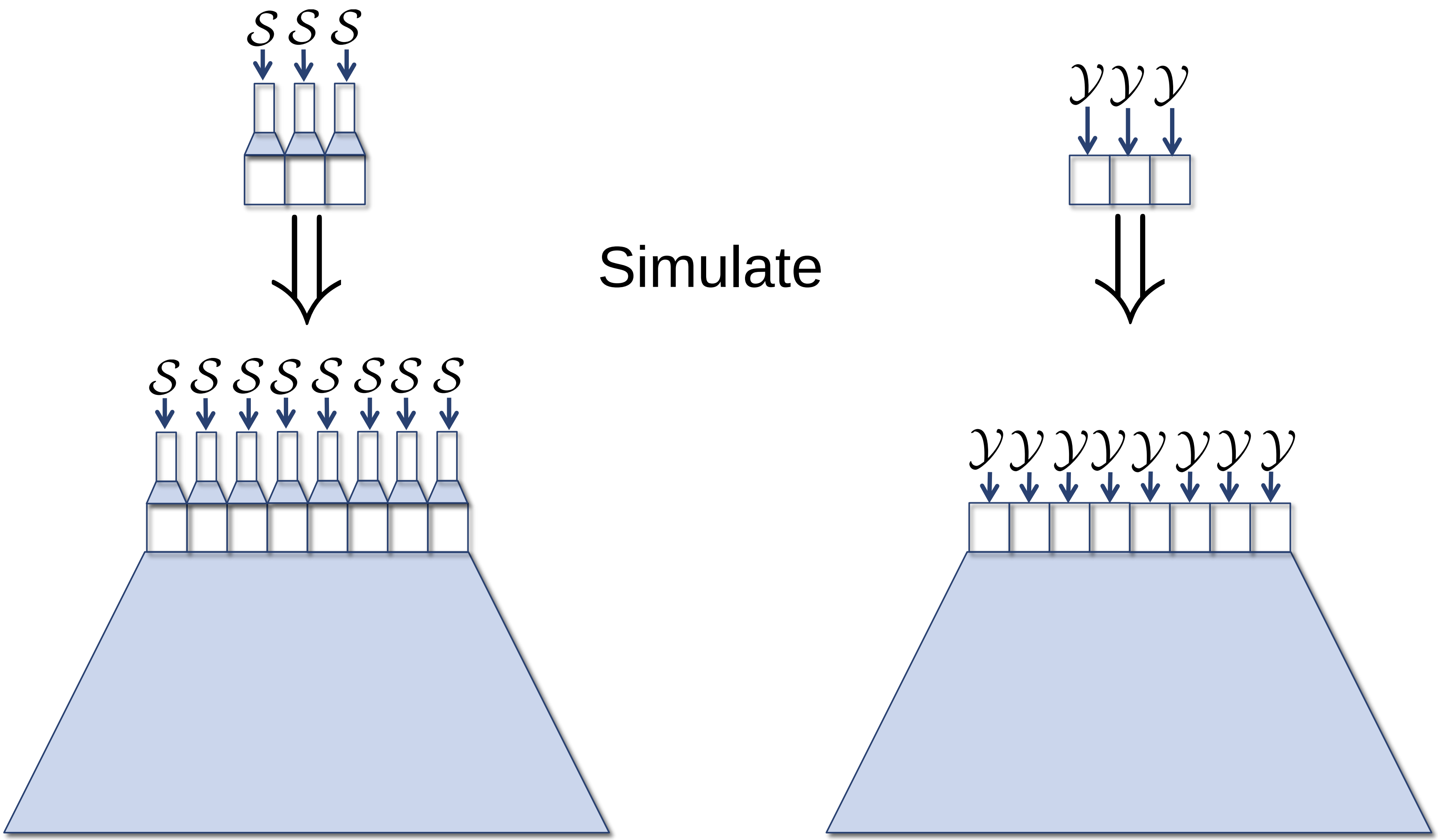


Original Security Proof

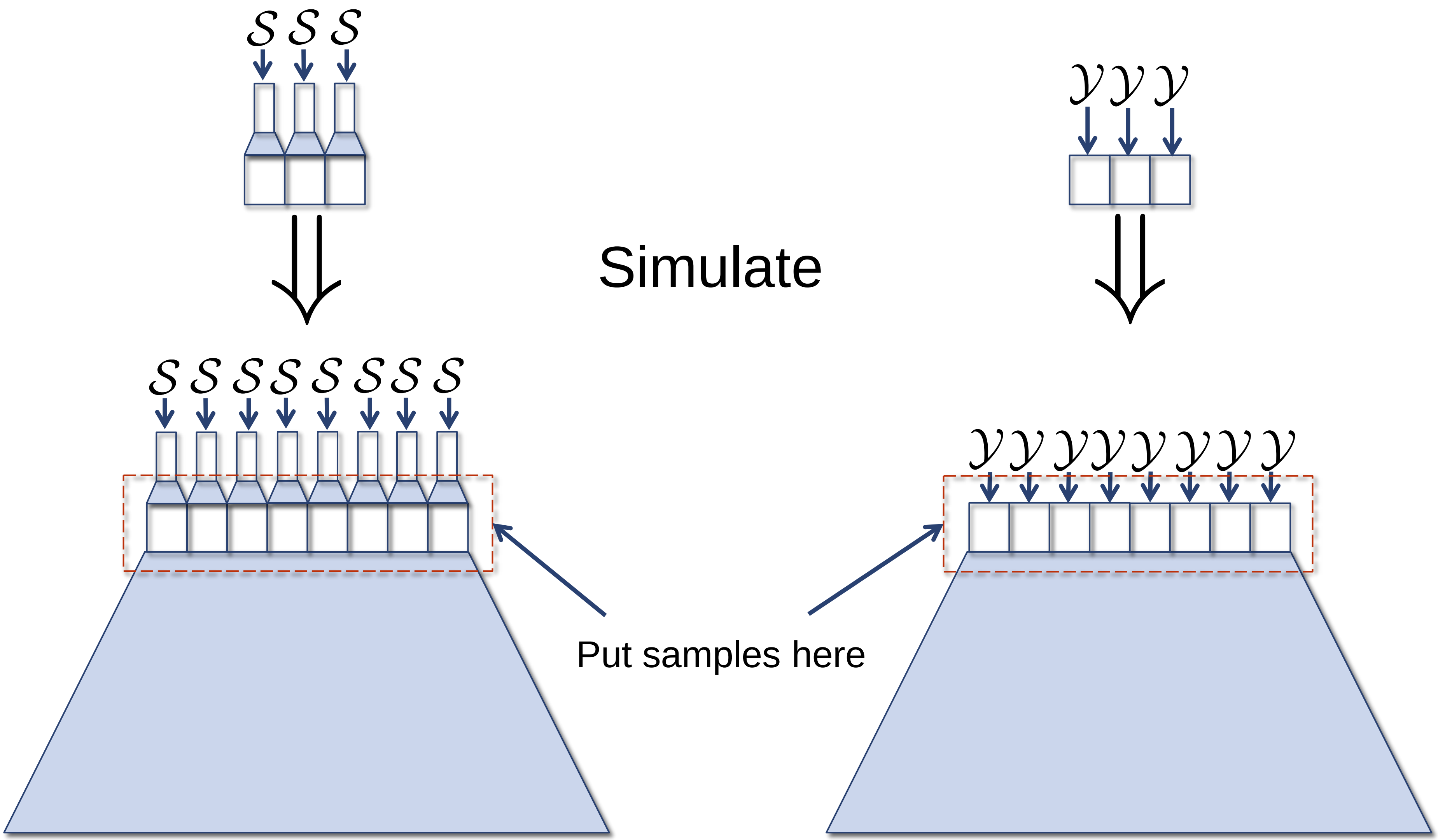
Step 1: Hybridize over levels of tree ✓

Step 2: Simulate hybrids using q samples

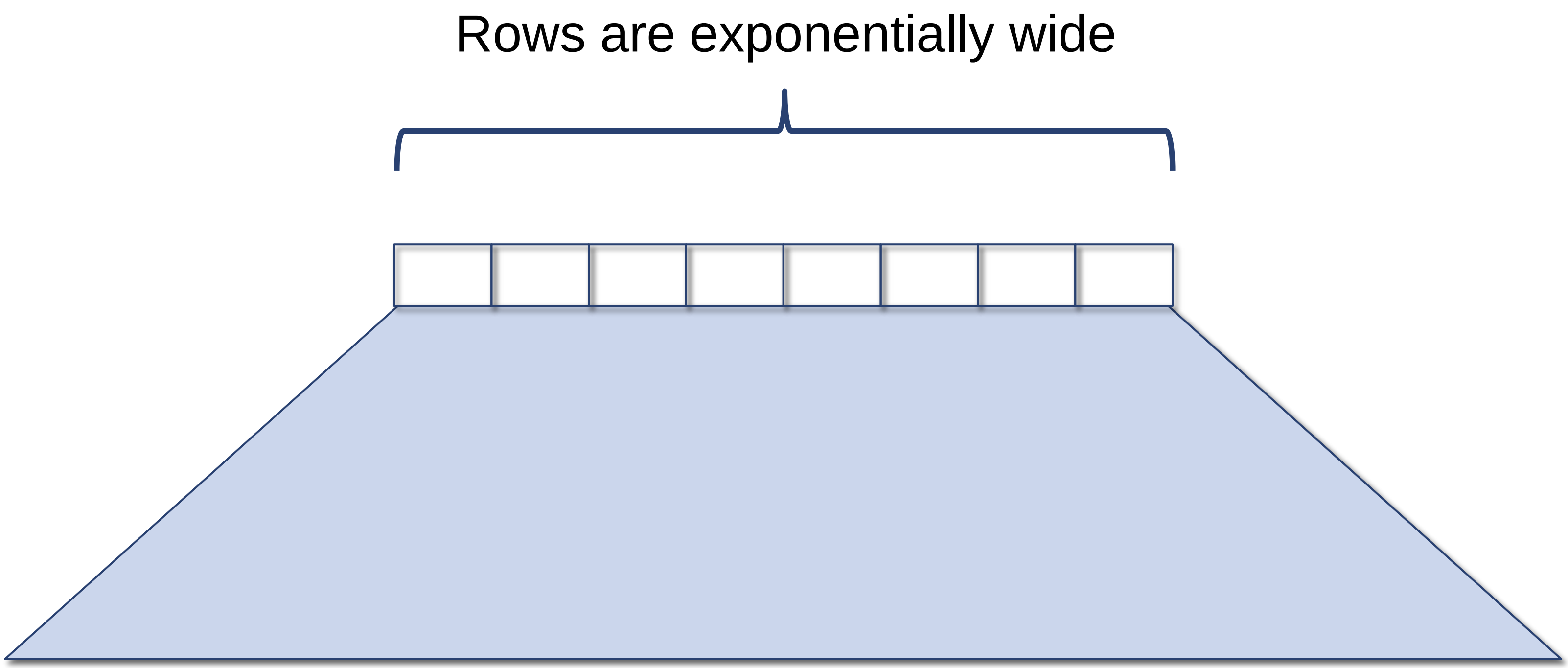
Original Security Proof: Step 2



Original Security Proof: Step 2



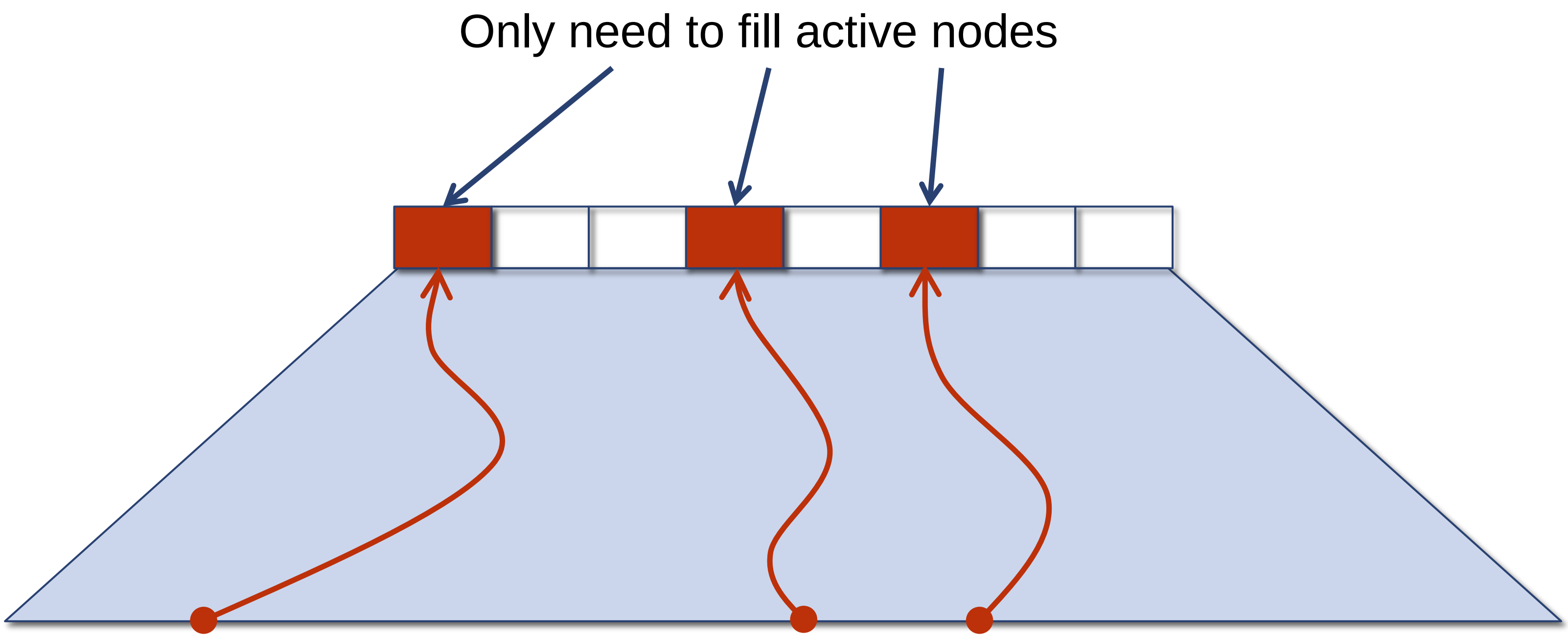
Original Security Proof: Step 2



Problem?

Original Security Proof: Step 2

Active node: value used to answer query



Adversary only queries polynomial number of points

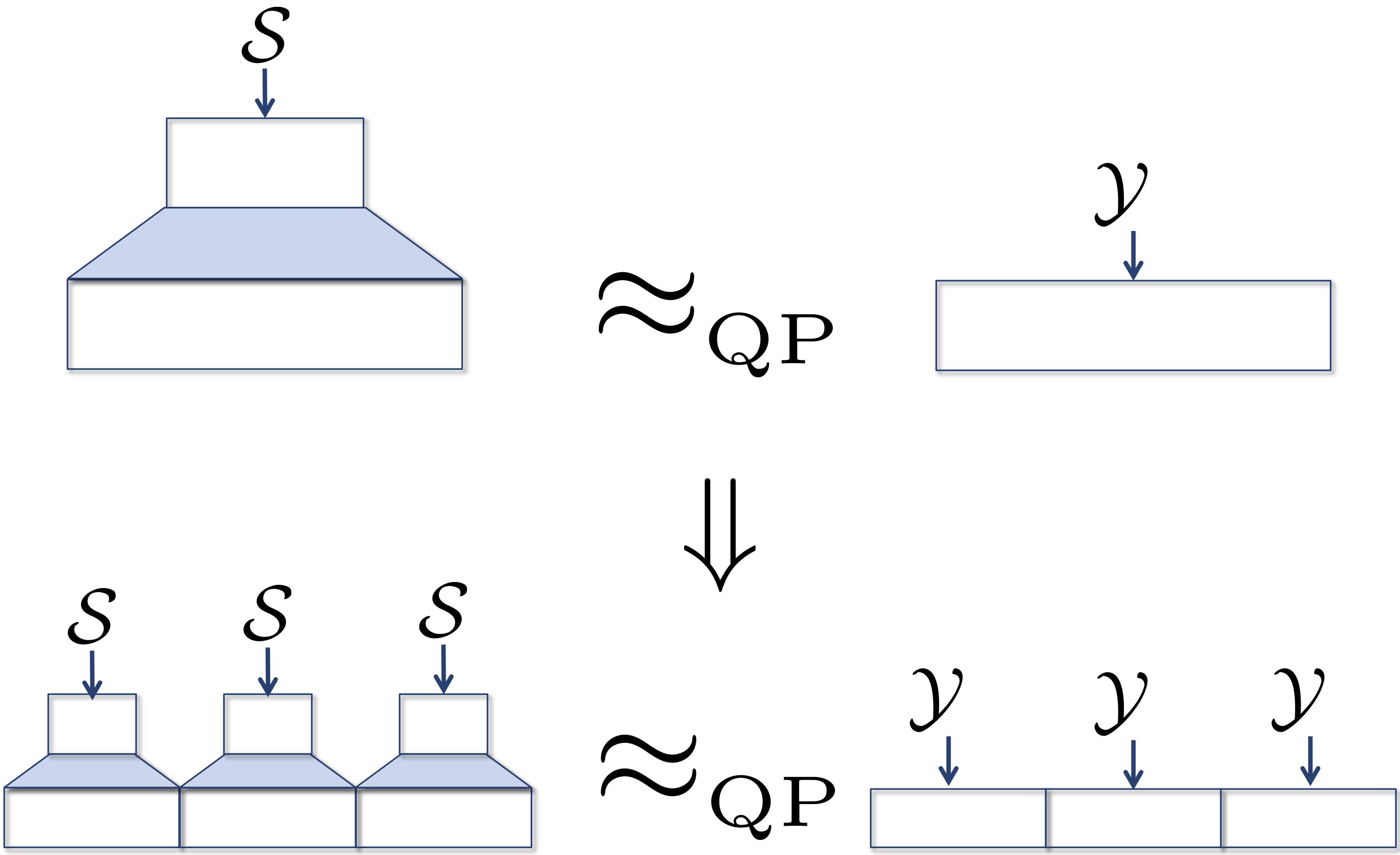
Original Security Proof

Step 1: Hybridize over levels of tree ✓

Step 2: Simulate hybrids using q samples ✓

Step 3: Pseudorandomness of one PRG sample implies pseudorandomness of q samples

Original Security Proof: Step 3



Original Security Proof

Step 1: Hybridize over levels of tree ✓

Step 2: Simulate hybrids using q samples ✓

Step 3: Pseudorandomness of one PRG sample implies pseudorandomness of q samples ✓

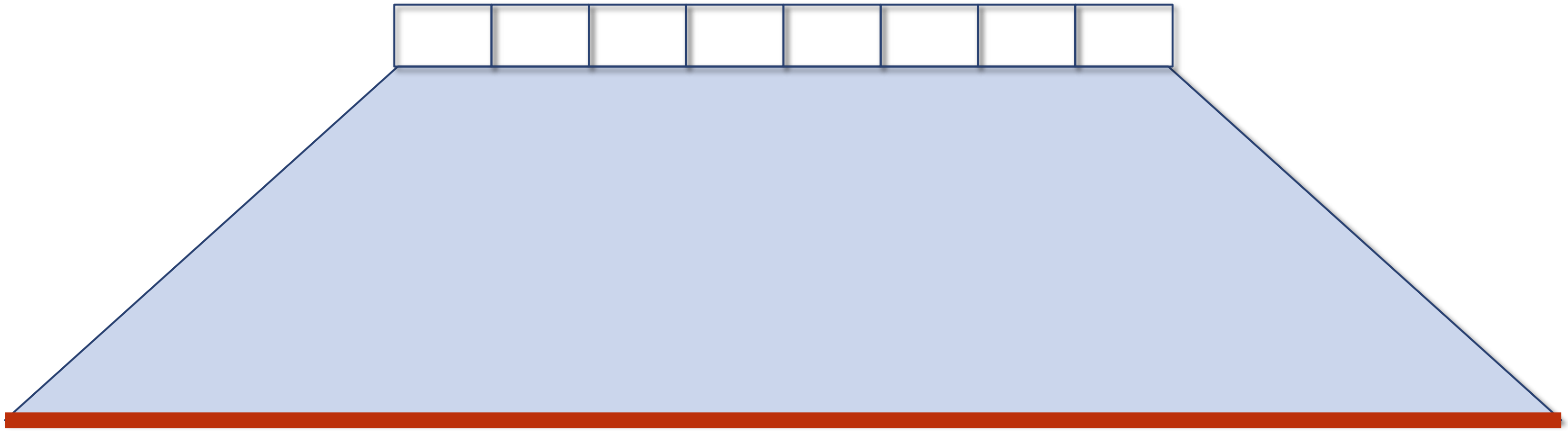
Quantum Security Proof Attempt

Step 1: Hybridize over levels of tree ✓

Step 2: Simulate hybrids using q samples X

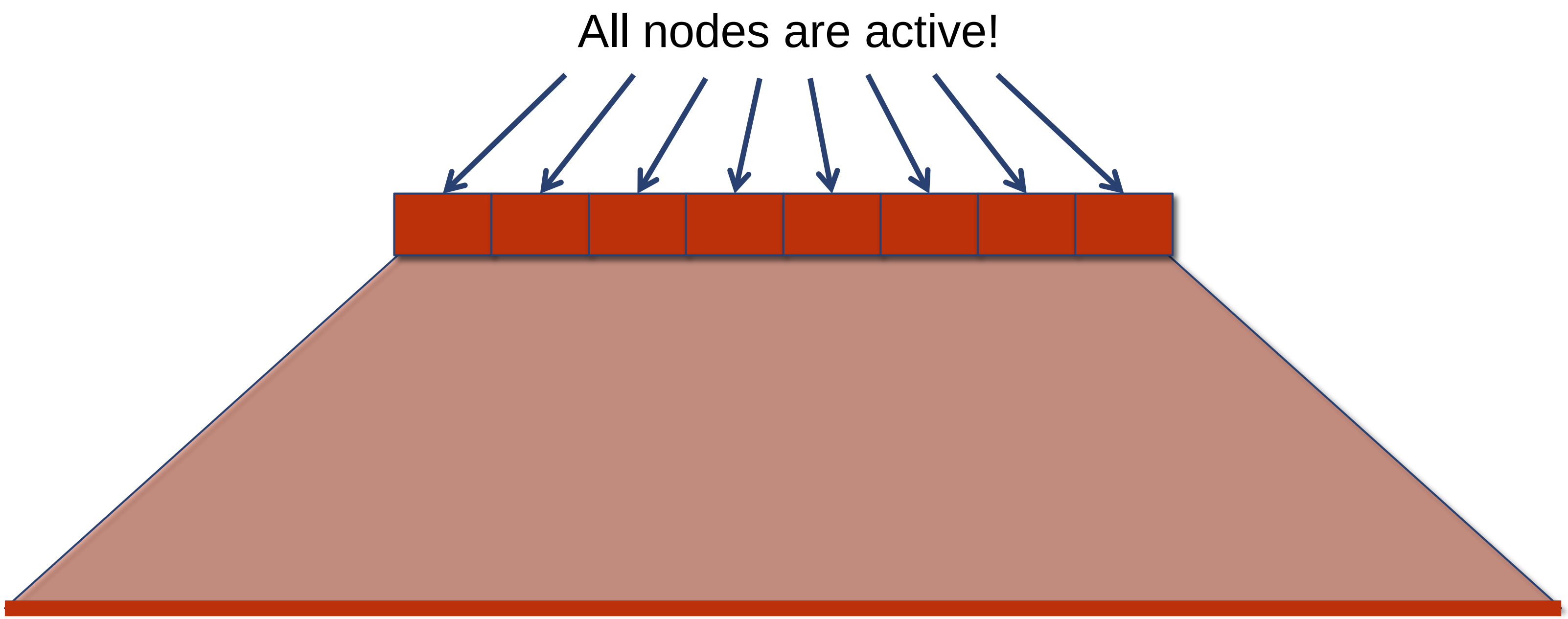
Step 3: Quantum pseudorandomness of one PRG sample implies quantum pseudorandomness of q samples ✓

Difficulty Simulating Hybrids



Adversary can query on all exponentially-many inputs

Difficulty Simulating Hybrids



Exact simulation requires exponentially-many samples

Need new simulation technique

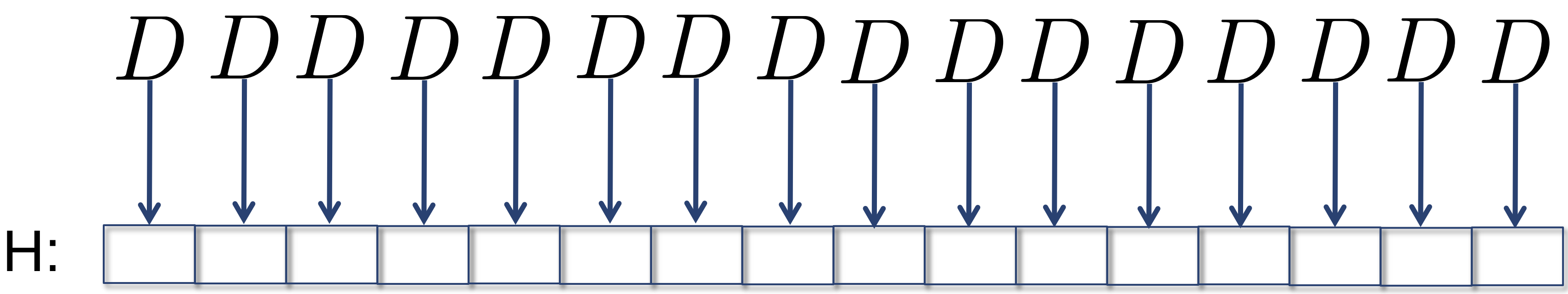
A Distribution to Simulate

Any distribution D on values induces a distribution on functions

For all $x \in \mathcal{X}$

$$y_x \leftarrow D$$

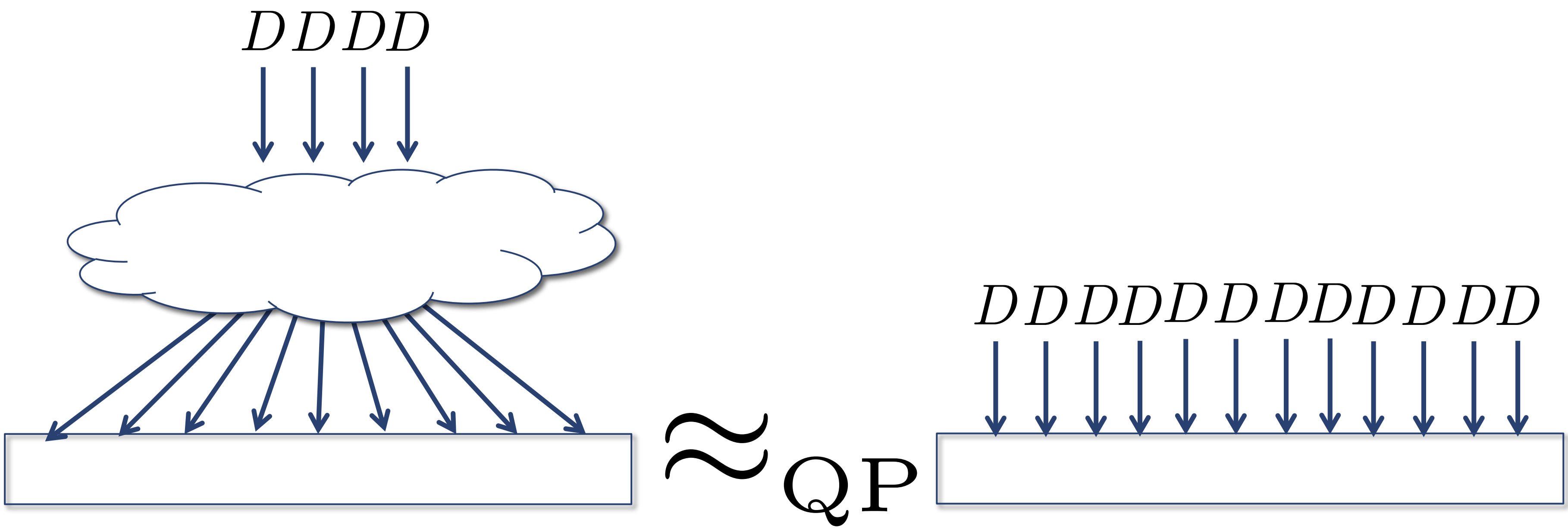
$$H(x) = y_x$$



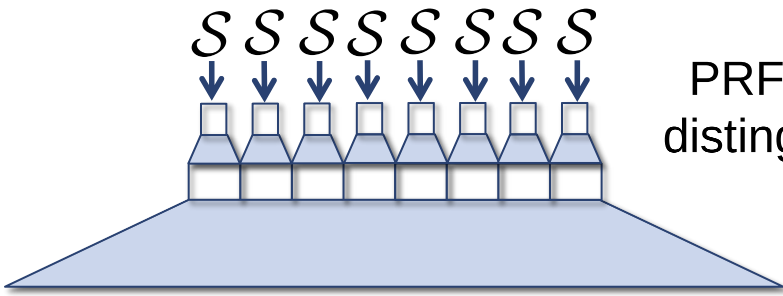
$$D^{\mathcal{X}}$$

A Distribution to Simulate

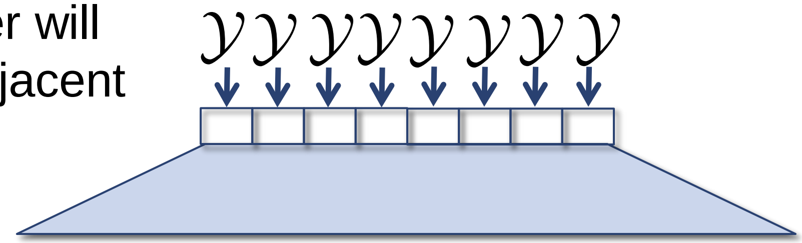
Suppose we could simulate D^X approximately using a polynomial number of samples from D:



Fixing the GGM Proof

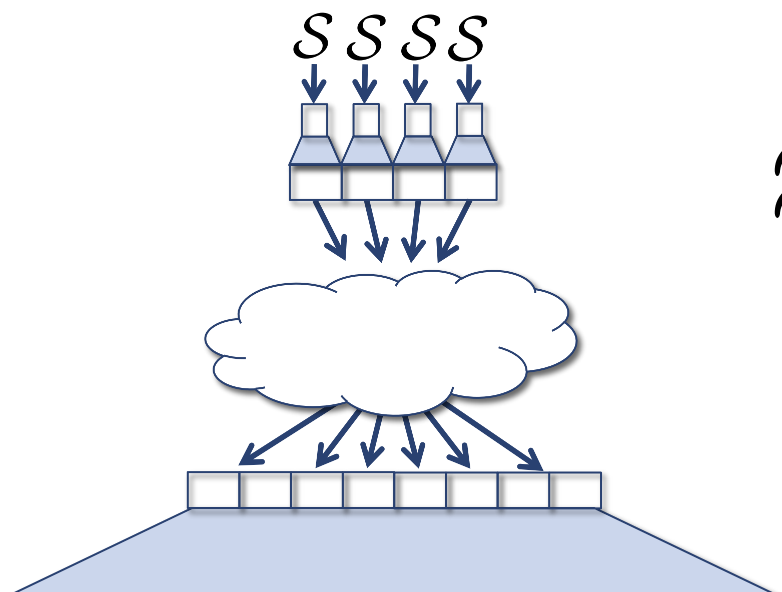


PRF distinguisher will distinguish two adjacent hybrids

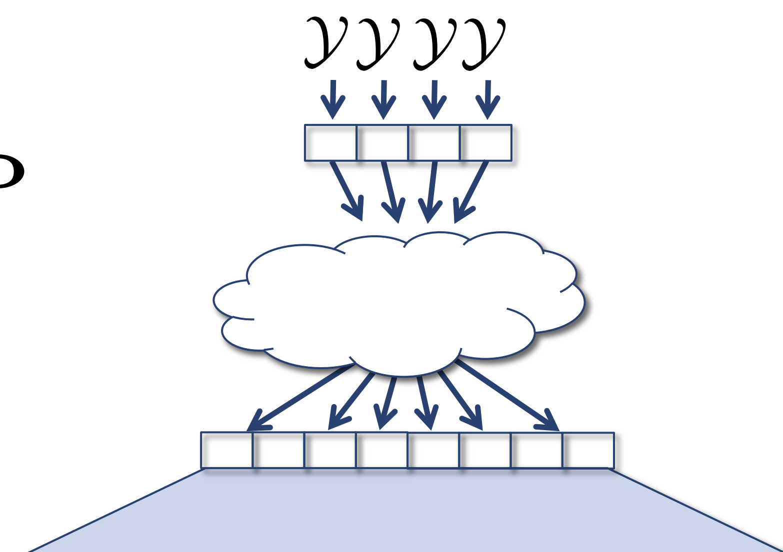


$$\approx_{QP}$$

$$\approx_{QP}$$



$$\approx_{QP}$$



Quantum Security Proof

Step 1: Hybridize over levels of tree ✓

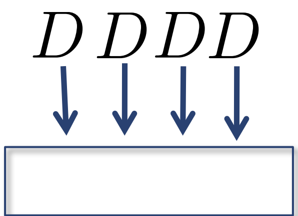
Step 2: Simulate hybrids approximately using polynomially-many samples ?

Step 3: Quantum pseudorandomness of one sample implies quantum pseudorandomness of polynomially-many samples ✓

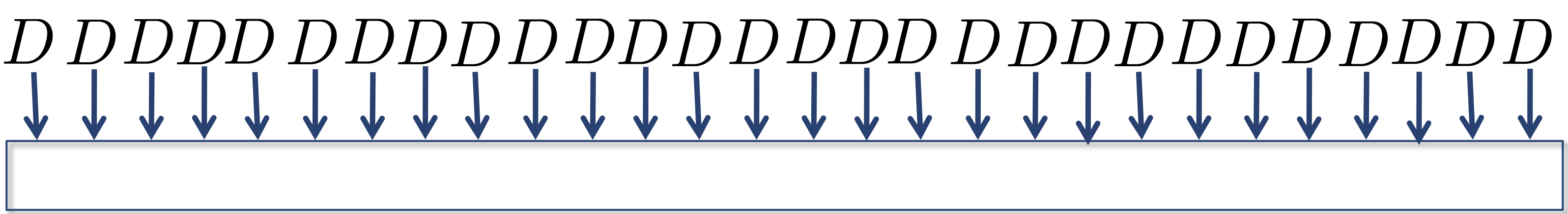
Simulating D^X

We have r samples:

- poly r



Want to simulate:



New Tool: Small Range Distributions

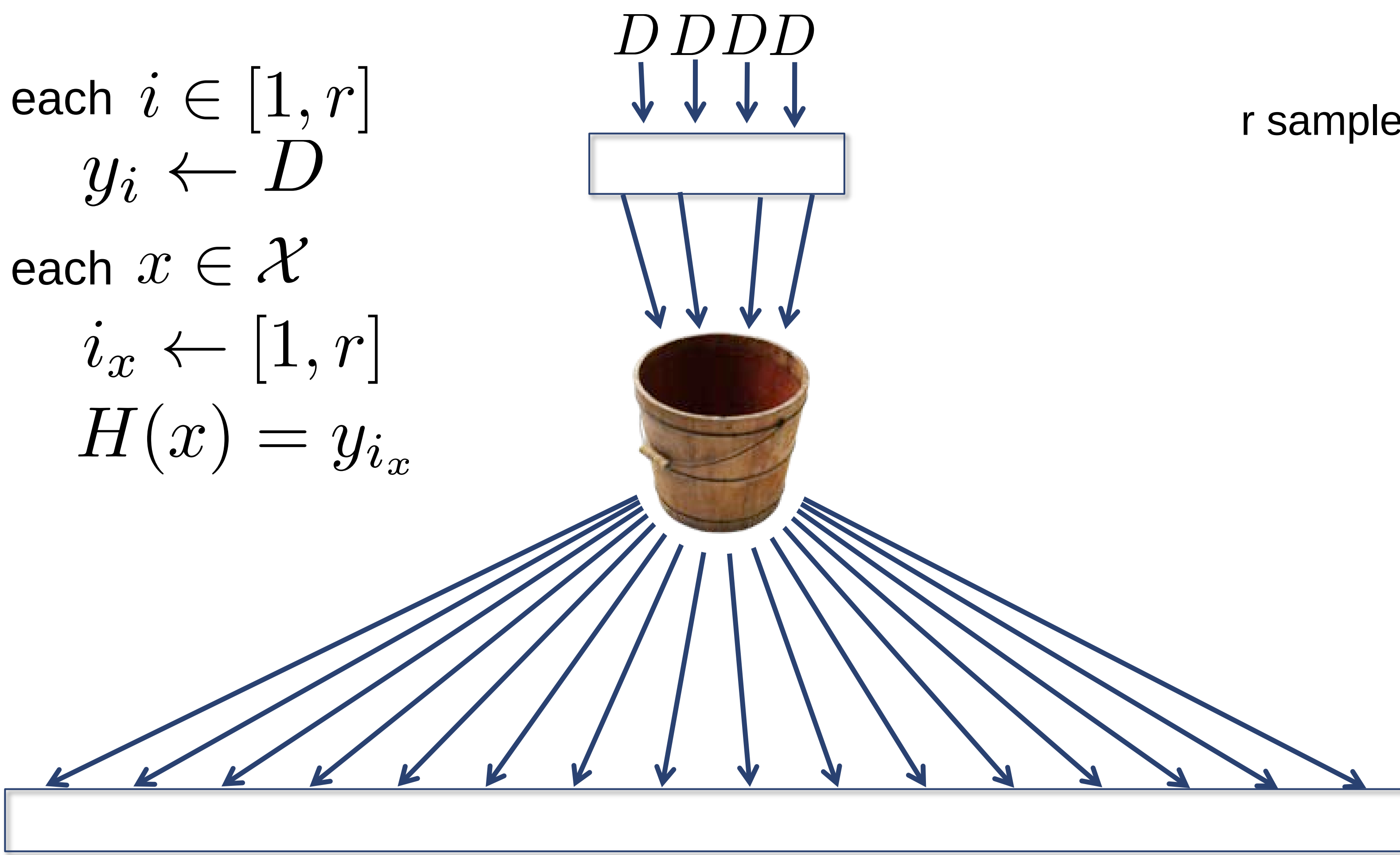
For each $i \in [1, r]$

$$y_i \leftarrow D$$

For each $x \in \mathcal{X}$

$$i_x \leftarrow [1, r]$$

$$H(x) = y_{i_x}$$



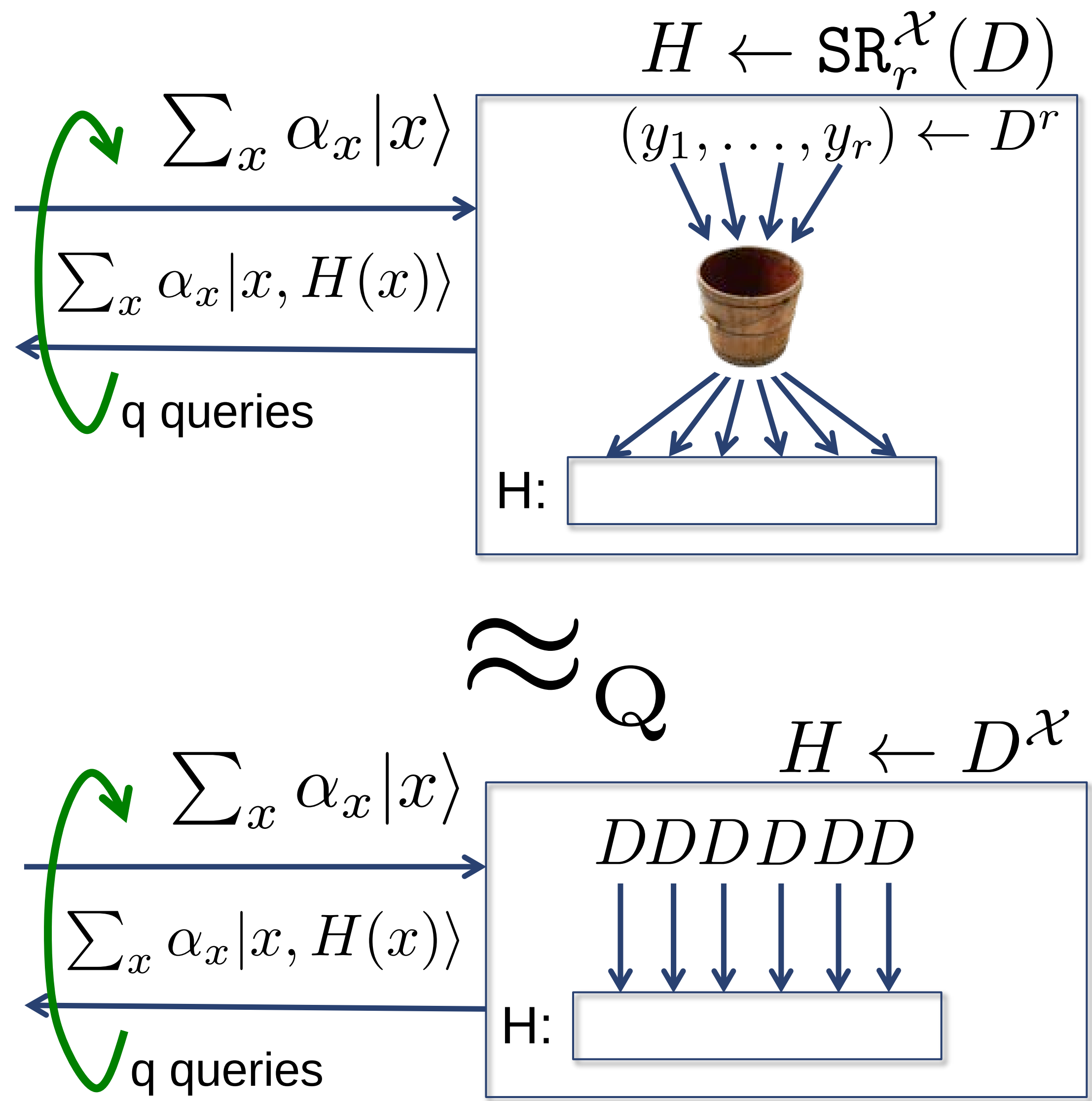
r samples of D

$$\mathrm{SR}_r^{\mathcal{X}}(D)$$

Technical Theorem

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

Not negligible, but good enough for our purposes



Proving the Technical Theorem

Let $p(1/r) = \Pr[A^{SR_r^{\mathcal{X}}(D)}() = 1]$

Observation: $SR_\infty^{\mathcal{X}}(D) = D^{\mathcal{X}}$

Goal: bound $|p(1/r) - p(0)|$

First, we'll need

Lemma: If A makes q quantum queries, then p is a polynomial in 1/r of degree at most 2q

What does this buy us?

Polynomials!

Let λ∈[0,1] parameterize a family of oracle distributions E_λ

Let A be an oracle algorithm, $p(\lambda) = \Pr[A^{E_\lambda}() = 1]$

$$0 \leq p(\lambda) \leq 1 \forall \lambda \in [0,1]$$

What if p(λ) is a polynomial of degree d?

Markov inequality:

$$|p'(\lambda)| \leq d^2 \forall \lambda \in [0,1]$$

Therefore, $|p(\lambda) - p(0)| \leq d^2 \lambda$

Proving the Technical Theorem

Idea: let $E_\lambda = SR_{1/\lambda}^{X}(D)$

$\longrightarrow$ p(λ) has degree 2q

$$\left|\Pr[A^{SR_r^{\mathcal{X}}(D)}() = 1] - \Pr[A^{D^{\mathcal{X}}}() = 1]\right|$$
$$= \left|\Pr[A^{E_{1/r}}() = 1] - \Pr[A^{E_0}() = 1]\right|$$
$$= |p(1/r) - p(0)| \leq (2q)^2/r \text{ ?}$$

Problem: E_λ only a distribution for λ = 1/r (integer r)

$\longrightarrow$ 0 ≤ p(λ) ≤ 1 only for λ = 1/r

$\longrightarrow$ Need replacement for Markov inequality

Replacement for Markov Inequality

Lemma: If $0 \leq p(1/r) \leq 1 \forall r \in \mathbb{Z}^+$
and p is a degree-d polynomial in 1/r, then

$$|p(\lambda) - p(0)| < (\pi^2/6)d^3\lambda$$

for all λ in [0,1]

Proving the Technical Theorem

If $p(1/r) = \Pr[A^{SR_r^{\mathcal{X}}(D)}() = 1]$, then p satisfies the revised Markov inequality with d=2q

$$\left|\Pr[A^{SR_r^{\mathcal{X}}(D)}() = 1] - \Pr[A^{D^{\mathcal{X}}}() = 1]\right|$$
$$= |p(1/r) - p(0)| < (\pi^2/6)(2q)^3/r \checkmark$$

One Final Step

Recall definition of SR distribution:

For each $i \in [1, r]$

$$y_i \leftarrow D$$

For each $x \in \mathcal{X}$

$$i_x \leftarrow [1, r]$$

$$H(x) = y_{i_x}$$

How do we pick the i_x?

- Let R be a drawn from (2q)-wise indep. function family
- i_x = R(x)

Theorem: (2q)-wise independent functions look like random functions to any q-query quantum algorithm

Quantum GGM

Step 1: Hybridize over levels of tree ✓

Step 2: Simulate hybrids approximately using small range distributions and polynomially-many samples ✓

Step 3: Quantum pseudorandomness of one sample implies quantum pseudorandomness of polynomially-many samples ✓

Our PRF Results

Separation: PRFs ≠ quantum PRFs

New tool: small-range distributions

Proofs of quantum security for some classical PRF constructions:

- From quantum-secure pseudorandom generators [GGM'84]
- From quantum-secure pseudorandom synthesizers [NR'95]
- Directly from lattices [BPR'11]

Quantum-secure MACs [BZ'12]

Classical Security

m_i

σ_i

q queries

(m^*, σ^*)

Choose random key k

$\sigma_i \leftarrow S(k, m_i)$

Check:

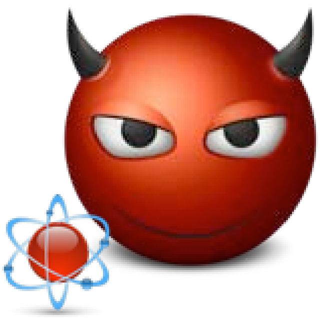
$(m^*, \sigma^*) \neq (m_i, \sigma_i) \forall i$

$V(k, m^*, \sigma^*) = 1$

w

MAC is secure if $\Pr[w = 1] < \texttt{negl}$

Post-Quantum Security



m_i

σ_i

q queries

(m^*, σ^*)

Choose random key k

$\sigma_i \leftarrow S(k, m_i)$

Check:

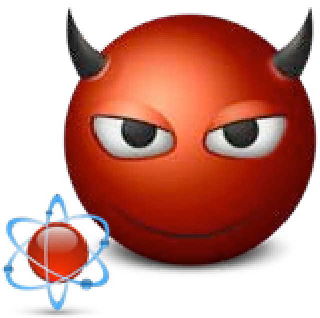
$(m^*, \sigma^*) \neq (m_i, \sigma_i) \forall i$

$V(k, m^*, \sigma^*) = 1$

w

MAC is secure if $\Pr[w = 1] < \mathtt{negl}$

Quantum Security?



$\sum_m \alpha_m |m\rangle$

$\sum_m \alpha_m |m, \sigma_m^{(i)}\rangle$

q queries

(m^*, σ^*)

Choose random key k

Pick random r_i

$\sigma_m^{(i)} = S(k, m; r_i)$

Too restrictive

Check:

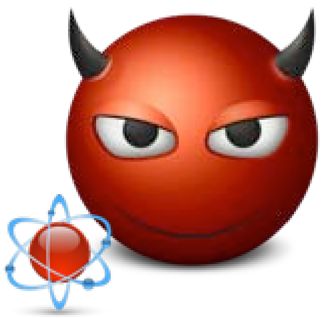
$\cancel{(m^*, \sigma^*) \neq (m, \sigma_m^{(i)}) \forall i, m}$

$V(k, m^*, \sigma^*) = 1$

w

MAC is secure if $\Pr[w = 1] < \mathtt{negl}$

Quantum Security



$\sum_m \alpha_m |m\rangle$

$\sum_m \alpha_m |m, \sigma_m^{(i)}\rangle$

q queries

$(\mathbf{m}, \boldsymbol{\sigma}) \in \mathcal{M}^{q+1} \times \mathcal{S}^{q+1}$

Choose random key k

Pick random r_i

$$\sigma_m^{(i)} = S(k, m; r_i)$$

Check:

$$(m_j, \sigma_j) \neq (m_k, \sigma_k)$$

$$V(k, m_j, \sigma_j) = 1$$

w

MAC is secure if $\Pr[w = 1] < \texttt{negl}$

Separation

MAC $\neq$ Quantum-secure MAC

Theorem: If post-quantum PRFs exist, then there are post-quantum MACs that are not quantum-secure MACs

Carries over immediately from PRF separation

Also have natural examples where underlying PRF is quantum-secure (Carter-Wegman MAC)

A Simple Classical MAC

Let F be a classically secure PRF

F is also a classically-secure MAC:

$S(k,m) = F(k,m)$

$V(k,m,\sigma) = F(k,m)==\sigma?$

Security: Replace F with random oracle

$\longrightarrow$ Adversary can't tell difference

$\longrightarrow$ Forgeries correspond to input/output pairs of oracle

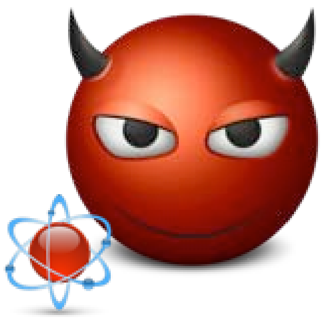
$\longrightarrow$ Impossible to generate new pairs

A Simple Quantum-secure MAC?

Let F be a quantum-secure PRF

Is F also a quantum-secure MAC?

Security of PRF as a MAC



$\sum_m \alpha_m |m\rangle$

$\sum_m \alpha_m |m, F(k,m)\rangle$

q queries

$(\mathbf{m}, \boldsymbol{\sigma}) \in \mathcal{M}^{q+1} \times \mathcal{S}^{q+1}$

Choose random key k

Check:

$(m_j, \sigma_j) \neq (m_k, \sigma_k)$

$\sigma_j = F(k, m_j)$

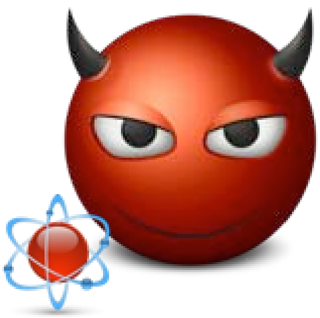
w

Adversary wins with prob ε

Security of PRF as a MAC

Choose random oracle H

$\sum_m \alpha_m |m\rangle$



$\sum_m \alpha_m |m, H(m)\rangle$

q queries

$(\mathbf{m}, \boldsymbol{\sigma}) \in \mathcal{M}^{q+1} \times \mathcal{S}^{q+1}$

Check:

$(m_j, \sigma_j) \neq (m_k, \sigma_k)$

$\sigma_j = H(m_j)$

w

Adversary wins with prob ε-negl

Quantum Oracle Interrogation

Allowed q quantum queries to random oracle H

Goal: produce q+1 input/output pairs

Classical queries: can’t do better than 1/|Y|

$\longrightarrow$ Hard if H outputs super-logarithmically many bits

Quantum queries?

$\longrightarrow$ get to “see” entire oracle with a single query

Single-Bit Outputs

Bad news: If |Y|=2 (i.e. single bit output), the oracle interrogation problem is easy.

Theorem([vD'98]): There is an algorithm that makes q quantum queries to any oracle H:X→{0,1} and produces 1.99q input/output pairs, with probability 1-negl(q)

Are we in trouble?

Arbitrary Output Size

We exactly characterize the difficulty of the oracle interrogation problem:

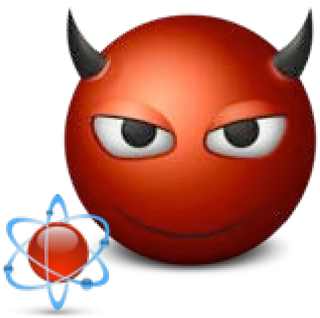
Theorem: Any quantum algorithm making q quantum queries to an oracle H:X→Y solves the oracle interrogation problem with probability at most $1-(1-|Y|^{-1})^{q+1}$.

Moreover, there is a quantum algorithm exactly matching this bound.

Two cases:

- log |Y| ≤ (log q)/2: probability is negligibly close to 1 → Easy
- log |Y| = ω(log q): probability is negligible → Hard ✓

Security of PRF as a MAC



$\sum_m \alpha_m |m\rangle$

$\sum_m \alpha_m |m, H(m)\rangle$

q queries

$(\mathbf{m}, \boldsymbol{\sigma}) \in \mathcal{M}^{q+1} \times \mathcal{S}^{q+1}$

Choose random oracle H

Check:

$(m_j, \sigma_j) \neq (m_k, \sigma_k)$

$\sigma_j = H(m_j)$

w

Must be negligible

$\longrightarrow$ ε is negligible

Adversary wins with prob ε-negl

The Rank Method

Fix q, let $|\psi_H\rangle$ be final state (before measurement) of quantum algorithm after q queries to H

$\{|\psi_H\rangle : H \in \mathcal{H}\}$ spans some subspace of the overall Hilbert space

Let $\mathtt{Rank} = \mathrm{Dim\ Span}\{|\psi_H\rangle : H \in \mathcal{H}\}$

Lemma: For any goal, the probability of success is at most Rank times the probability of success of the best 0-query algorithm

Applying the Rank Method

Goal: output $k=(q+1)$ input/output pairs

Best 0-query algorithm: pick k arbitrary distinct inputs, guess outputs

Success prob: $(|Y|^{-1})^k = |Y|^{-(q+1)}$

Only need to bound the rank of any q-query algorithm

The Rank Method

Lemma: The rank of any algorithm that makes q queries to an oracle H: X→Y is at most

$$\sum_{r=0}^{q} \binom{|\mathcal{X}|}{r} (|\mathcal{Y}|-1)^r$$

Exact

Applying the Rank Method

Prob success of any q-query algorithm

≤ Rank * best success prob of 0-query algs

$$\leq \frac{\sum_{r=0}^{q} \binom{|\mathcal{X}|}{r} (|\mathcal{Y}|-1)^r}{|\mathcal{Y}|^{q+1}} \approx \frac{\binom{|\mathcal{X}|}{q}}{|\mathcal{Y}|}$$

Too big!

Applying the Rank Method

Observation: for any (q+1) inputs, knowing H at other points does not help determine H at these points

$\longrightarrow$ Might as well only query on superpositions of (q+1) points

$$\frac{\sum_{r=0}^{q}\binom{|\mathcal{X}|}{r}(|\mathcal{Y}|-1)^r}{|\mathcal{Y}|^{q+1}}$$

$$\downarrow$$

$$\frac{\sum_{r=0}^{q}\binom{q+1}{r}(|\mathcal{Y}|-1)^r}{|\mathcal{Y}|^{q+1}} = 1-\left(1-\frac{1}{|\mathcal{Y}|}\right)^{q+1} \quad ✓$$

Our MAC Results

Exact characterization of success probability for quantum oracle interrogation

- Developed new general tool: Rank method

Quantum-secure MACs:

- Quantum-secure PRFs are quantum-secure MACs
- A variant of Carter-Wegman is quantum-secure

One-time quantum-secure MACs:

- Pairwise independence is not enough
- 4-wise independence is

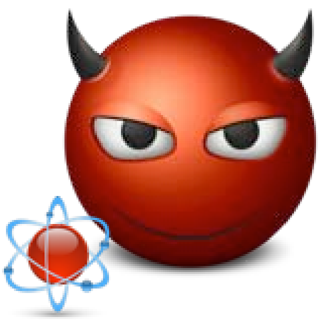
Quantum-Secure Signatures [BZ'13]

Quantum Security

$\mathtt{pk}$

$\sum_m \alpha_m |m\rangle$

$\sum_m \alpha_m |m, \sigma_m^{(i)}\rangle$



q queries

$(\mathbf{m}, \boldsymbol{\sigma}) \in \mathcal{M}^{q+1} \times \mathcal{S}^{q+1}$

$(\mathtt{sk}, \mathtt{pk}) \leftarrow G()$

Pick random r_i

$\sigma_m^{(i)} = S(\mathtt{sk}, m; r_i)$

Check:

$(m_j, \sigma_j) \neq (m_k, \sigma_k)$

$V(\mathtt{pk}, m_j, \sigma_j) = 1$

w

S is secure if $\Pr[w = 1] < \mathtt{negl}$

Separation

Sig $\neq$ Quantum-secure Sig

Theorem: If post-quantum signatures exist, then there are post-quantum signatures that are not quantum-secure signatures

Building Quantum-secure Signatures

Hope that existing constructions can be proven secure:

- Lattice schemes [ABB'10,CHKP'10]
- Generic constructions (Lamport, Merkle)
- RO schemes [GPV'08]

Compilers to boost security?

One-time QROM Conversion

Let (G,S,V) be a classically secure signature scheme

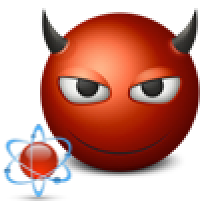
Construct new QROM scheme (G,S',V') where:

$$S'(\mathtt{sk},m) = S(\mathtt{sk},H(m))$$
$$V'(\mathtt{pk},m,\sigma) = V(\mathtt{pk},H(m),\sigma)$$

Theorem: If (G,S,V) is one-time post-quantum secure, then (G,S',V') is one-time quantum secure in the quantum random oracle model.

Proof Sketch

Start with a one-time adversary for S':



$$\sum_m \alpha_m |m\rangle \longrightarrow$$

$$\longleftarrow \sum_m \alpha_m |m, S(\mathtt{sk}, H(m); r)\rangle$$

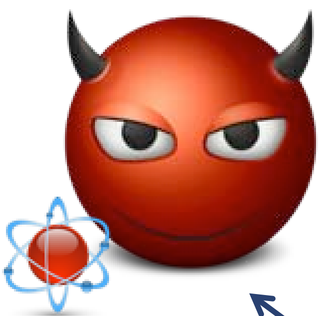
Step 1: Replace H with a SR distribution on t samples.

$\longrightarrow$ S only evaluated on t points

Problem: Adversary only generates 2 signatures!

Proof Sketch

Step 2: Sample H(m)



$$\sum_m \alpha_m |m\rangle$$

$$\sum_m \alpha_m |m, H(m)\rangle$$

measurement

$$\sum_{m:H(m)=h} \alpha_m |m, h\rangle$$

$$\sum_{m:H(m)=h} \alpha_m |m, S(\mathtt{sk}, h)\rangle$$

S only evaluated on 1 input!

$\longrightarrow$ One signature must be forgery

Measurement Lemma

A: $$|\psi_0\rangle \rightarrow |\psi_1\rangle \longrightarrow |\psi_2\rangle \xrightarrow{\text{measurement}} x$$

A': $$|\psi_0\rangle \rightarrow |\psi_1\rangle \xrightarrow[\text{measurement}]{\text{partial}} |\psi'_1\rangle \rightarrow |\psi'_2\rangle \xrightarrow{\text{measurement}} x$$

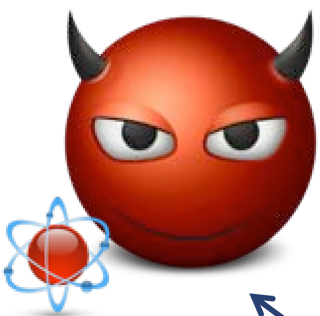
Results in one of k outcomes

Lemma: Pr[x←A'] ≥ Pr[x←A]/k

Proof Sketch

Step 2: Sample H(m)

only reduces adversary's success probability by factor of t



$$\sum_m \alpha_m |m\rangle$$

$$\sum_m \alpha_m |m, H(m)\rangle$$

measurement

$$\sum_{m:H(m)=h} \alpha_m |m, h\rangle$$

$$\sum_{m:H(m)=h} \alpha_m |m, S(\mathtt{sk}, h)\rangle$$

S only evaluated on 1 input!

$\longrightarrow$ One signature must be forgery

Generalizing to Many-time Security

Let $\mathcal{R}$ be a pairwise independent function family.

$$S'(\mathtt{sk}, m) = r \xleftarrow{R} \{0,1\}^\lambda, R \xleftarrow{R} \mathcal{R}$$
$$(r, S(\mathtt{sk}, H(m,r); R(m)))$$

Theorem: If (G,S,V) is classically secure, then (G,S',V') is quantum secure in the quantum random oracle model.

Our Signature Constructions

Two compilers:

- Post-quantum security → Quantum security in the QROM
  - GPV probabilistic full domain hash

- Post-quantum security + chameleon hash → Quantum security
  - CHKP'10 signatures
  - Modification to ABB'10 signatures

GPV in the QROM

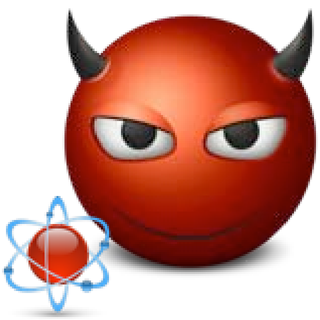
Generalization of Rank theorem

From generic assumptions:

- Lamport signatures + Merkle signatures
- From any hash function

Quantum-Secure Encryption [BZ'13]

Quantum Security



$\mathtt{pk}$

$\sum_c \alpha_c|c\rangle$

$\sum_c \alpha_c|c, D(\mathtt{sk}, c)\rangle$

m_0, m_1

$c^* = E(\mathtt{pk}, m_b)$

$\sum_c \alpha_c|c\rangle$

$\sum_c \alpha_c|c, f(c)\rangle$

b'

$(\mathtt{sk}, \mathtt{pk}) \leftarrow G()$, random b

$$f(c) = \begin{cases} D(\mathtt{sk}, c) & \text{if } c \neq c^* \\ \perp & \text{else} \end{cases}$$

Check b = b'

w

Quantum secure if $\left|\Pr[w=1] - \frac{1}{2}\right| < \mathtt{negl}$

Encryption Results

Classical challenge is required

- Quantum challenge queries lead to unsatisfiable definitions

Separation:

- If classically secure encryption schemes exist, then there are classically secure encryption schemes that are not quantum-secure

Constructions:

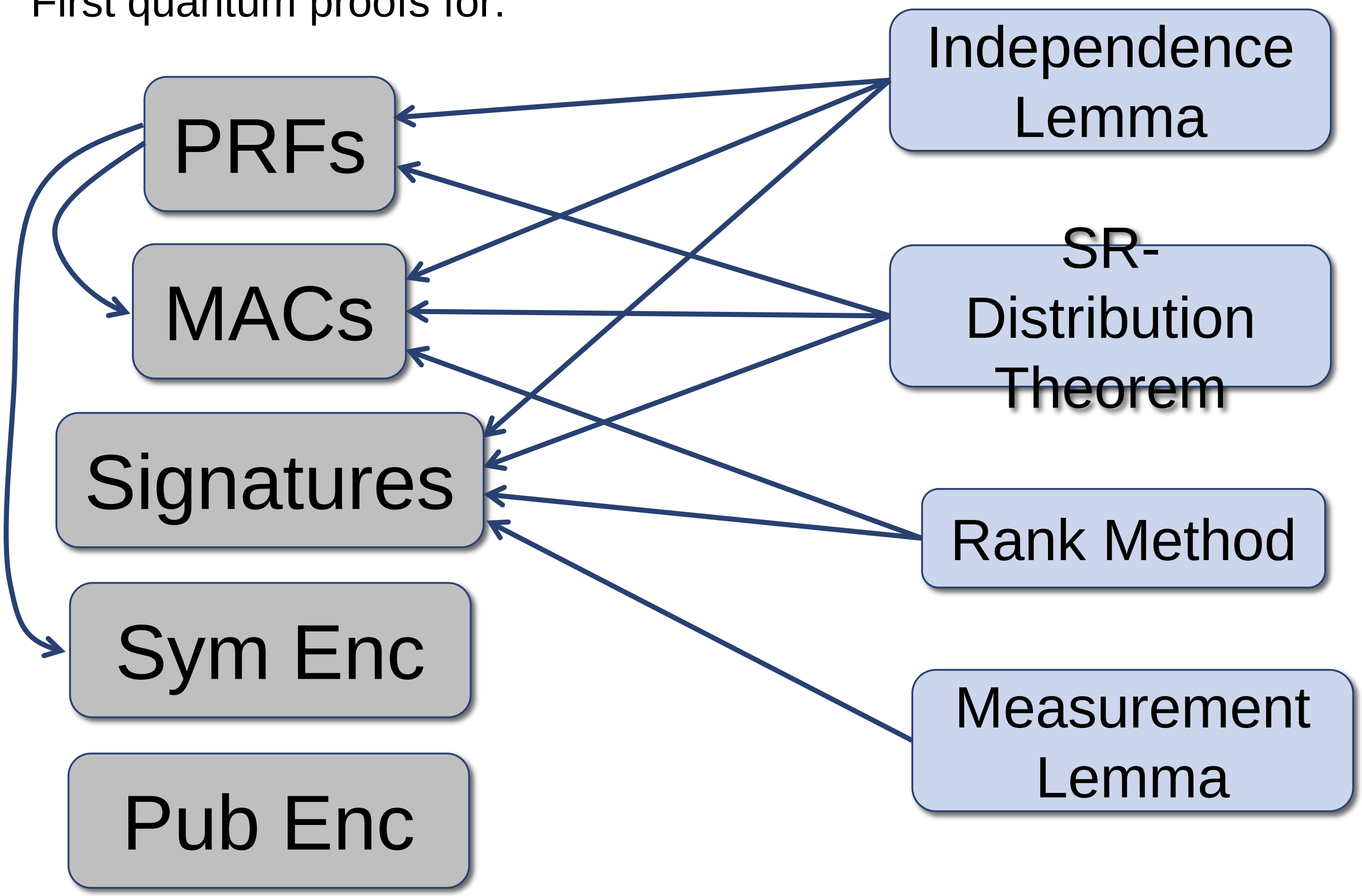
- Symmetric CCA from quantum-secure PRFs
- Public Key CCA from LWE
  - Quantum selectively-secure IBE + generic conversion

Summary of Separation Results

Classical Security:		Quantum Security:
PRF		PRF
MAC	$\neq$	MAC
Sign		Sign
Enc		Enc

Summary of Positive Results

First quantum proofs for:



Future Work

Many natural open questions:

- Quantum PRFs ⇒ Quantum PRPs (Luby-Rackoff)?
- 3-wise independence enough for 1-time MAC?
- Quantum-secure authenticated encryption ⇒ quantum-secure CCA?
- Signatures from one-way functions?

More complicated primitives?

- Adaptively secure (H)IBE?
- Functional encryption?

Thank you!