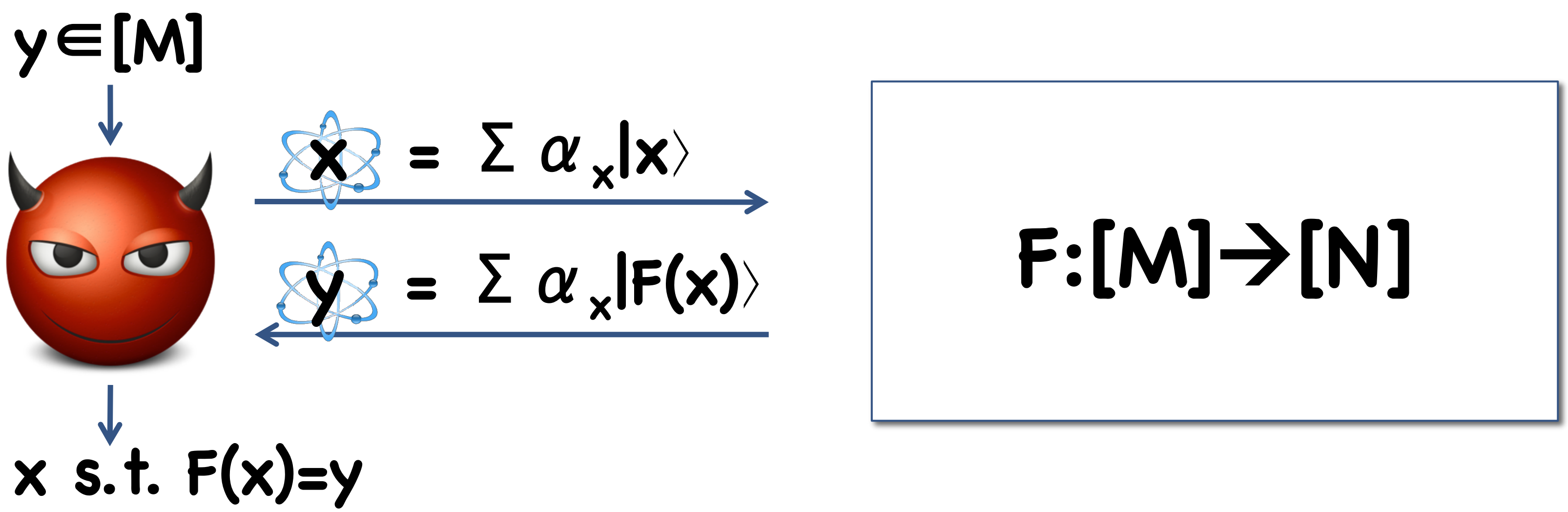
Quantum Query Solvability

Mark Zhandry – Stanford, MIT

Quantum Query Complexity

How many (quantum) queries are required to solve a given oracle task

Ex: Pre-image search



[Gro'96,BBBV'97]: $\Theta(N^{1/2})$ queries required

Quantum Query Complexity Results

General form: "$\Theta(f(M,N))$ quantum queries required to solve with success probability $2/3$"

- $O(f(M,N))$: "upper bound", a.k.a algorithm
- $\Omega(f(M,N))$: "lower bound"

Notes:

- Generally worst case
- Asymptotic in # of queries:
  - "exactly $f(M,N)$ queries required…" very unusual
- Almost always allow for some errors
- $2/3$ sort of arbitrary, as long as constant

Lower Bounds for Cryptographers

Quantum Lower Bounds	What Cryptographers Want
Worst case	Average case • E.g. random function **F**, output **y**
Rule out algorithms with high success probability (say 2/3)	Even success probability **1/log N** is devastating
Asymptotic in # of queries	Asymptotic in success probability OK • Sometimes # of queries is exact
	Often consider different settings

Quantum Query Solvability

Ideal format of results for crypto

General form: "Given $\mathbf{q}$ quantum queries, max success probability is $\Theta(\mathbf{f(q,M,N)})$"

Notes:

- Asymptotic in success prob, exact in # of queries
- Makes sense even for extremely small probabilities

Case Study 1: Pre-Image Search

Quantum Query Complexity: $\Theta(N^{1/2})$ [Gro'96,BBBV'97]

What is the quantum query solvability?

A. $\Theta(q/N^{1/2})$
B. $\Theta(q^2/N^{1/2})$
C. $\Theta(q^2/N)$
D. $\Theta(q^2/N^2)$
E. $\Theta(q^4/N^2)$

Case Study 1: Pre-Image Search

Quantum Query Complexity: $\Theta(N^{1/2})$ [Gro'96,BBBV'97]

What is the quantum query solvability?

Inconsistent with QQC

A. $\Theta(q/N^{1/2})$

B. $\cancel{\Theta(q^2/N^{1/2})}$

C. $\boxed{\Theta(q^2/N)}$

D. $\cancel{\Theta(q^2/N^2)}$

E. $\Theta(q^4/N^2)$

Not hard to show using hybrid method [BBBV'97]

Case Study 2: Quantum Collision Finding

$x = \sum \alpha_x |x\rangle$ $\longrightarrow$

$y = \sum \alpha_x |F(x)\rangle$ $\longleftarrow$

$F:[M] \rightarrow [N]$

$\downarrow$

$x_1 \neq x_2$ s.t. $F(x_1)=F(x_2)$

How many (quantum) queries needed to find collision?

- Relation to other problems (e.g. element distinctness, graph isomorphism)
- "Collision resistant" functions central to crypto
  - Often model such functions as random functions
  - For crypto, almost always want **N << M**
- Query complexity/solvability guides parameter settings

Case Study 2: Quantum Collision Finding

Quantum Query Complexity: $\Theta(N^{1/3})$ [BHT'97,A'01,Shi'01,Zha'15]

What is the quantum query solvability?

A. $\Theta(q/N^{1/3})$

B. $\Theta(q^2/N^{2/3})$

C. $\Theta(q^2/N)$

D. $\Theta(q^3/N)$

E. $\Theta(q^6/N^2)$

Case Study 2: Quantum Collision Finding

Quantum Query Complexity: $\Theta(N^{1/3})$ [BHT'97,A'01,Shi'01,Zha'15]

What is the quantum query solvability?

Inconsistent with QQC

A. $\Theta(q/N^{1/3})$

B. $\Theta(q^2/N^{2/3})$

~~C. $\Theta(q^2/N)$~~

D. $\boxed{\Theta(q^3/N)}$

E. $\Theta(q^6/N^2)$

Who Cares

So what if QQS of collision finding was $\Theta(q/N^{1/3})$ instead of $\Theta(q^3/N)$?

- Interesting natural question

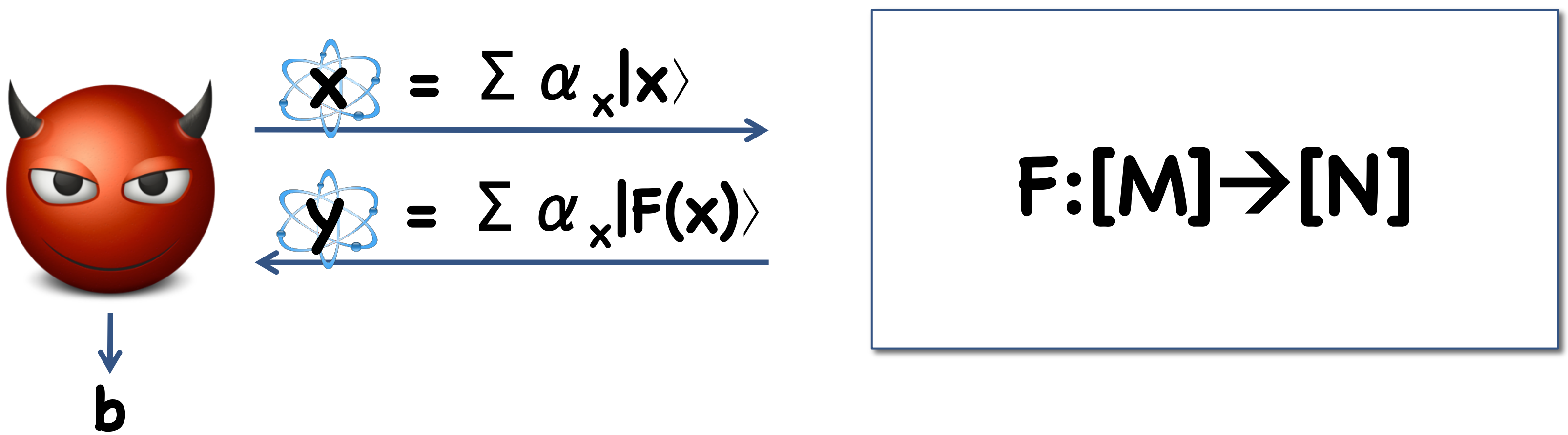
- Affects concrete parameters used for crypto hash functions
  - Adversary can make, say, 2^{80} queries
  - Considered broken if collision can be found with prob $>2^{-80}$
  - $\Theta(q^3/N)$: $N \geq 2^{320}$ (need **320**-bit hashes)
  - $\Theta(q/N^{1/3})$: $N \geq 2^{480}$ (need **480**-bit hashes)

- Can be useful intermediate step for QQC results!

The QQC of Collision Finding

Initial results ([Aar'01,Shi'01,HH'04) prove lower bounds for an **easier** problem:

b=1: F has "many" collisions
b=0: F injective



Quantum Collision *Detection*

Quantum Collision Detection

Thm ([Aar'01,Shi'01,HH'04]): $\Omega(N^{1/3})$ lower bound for worst case collision detection problem when **N≥M**

Cor: $\Omega(N^{1/3})$ lower bound for worst case collision *finding* problem when **N≥M**

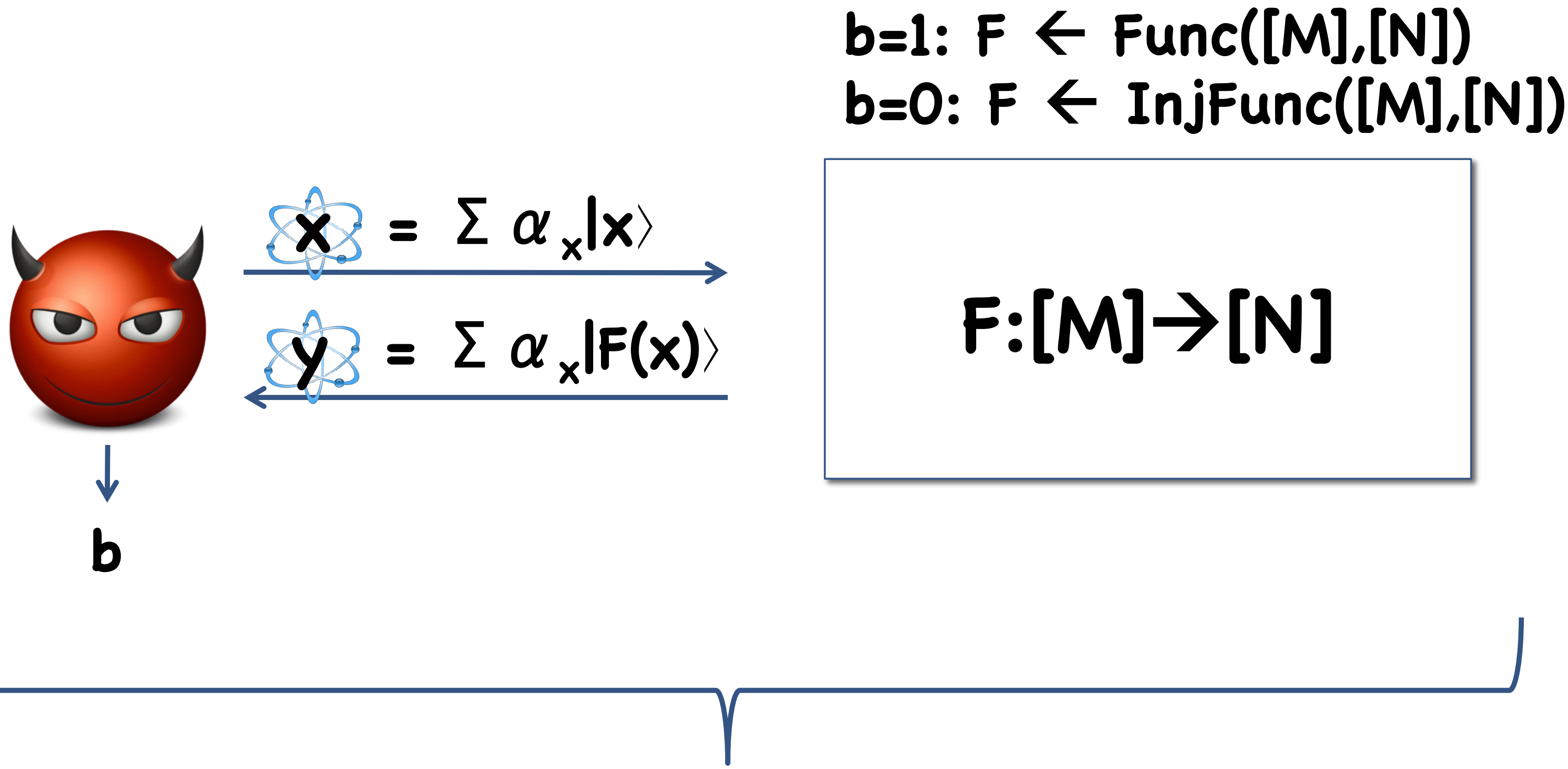
Proof: Injective functions have no collisions

⇒ any collision finding is also a detector

Notes:

- When **N<M**, collisions guaranteed to exist ⇒ detection is easy!
- Worst case: results only apply to **r**-to-**1** functions

Average Case Quantum Collision Detection



Average Case Quantum Collision *Detection*

Step 1: Extend to Average Case

Thm ([Yue'14]): $\boldsymbol{\Omega(N^{1/5})}$ lower bound for average case quantum collision detection problem

Uses adversary method + worst-case collision lower bound

Thm ([Zha'15]): $\boldsymbol{\Omega(N^{1/3})}$ lower bound for average case quantum collision detection problem

Uses "polynomial-like" method from [Zha'12]

Step 2: Extend to Quantum Query Solvability

Actually show something stronger:

Thm ([Zha'15]): $O(q^3/N)$ bound on success probability for average case quantum collision detection problem

Cor 1: $O(q^3/N)$ bound on success probability for average case quantum collision *finding* problem when $N \geq M$

Step 3: Extend QQS to Arbitrary **N,M**

Cor 1: $O(q^3/N)$ bound on success probability for average case quantum collision *finding* problem when **N≥M**

Cor 2: $O(q^3/N)$ bound on success probability for average case quantum collision *finding* problem for arbitrary **N,M**

Proof Idea

$x = \sum \alpha_x |x\rangle$

$y = \sum \alpha_x |F(x)\rangle$

$F:[M] \to [N]$

$x_1 \neq x_2$ s.t. $F(x_1)=F(x_2)$ <u>with prob **p**</u>

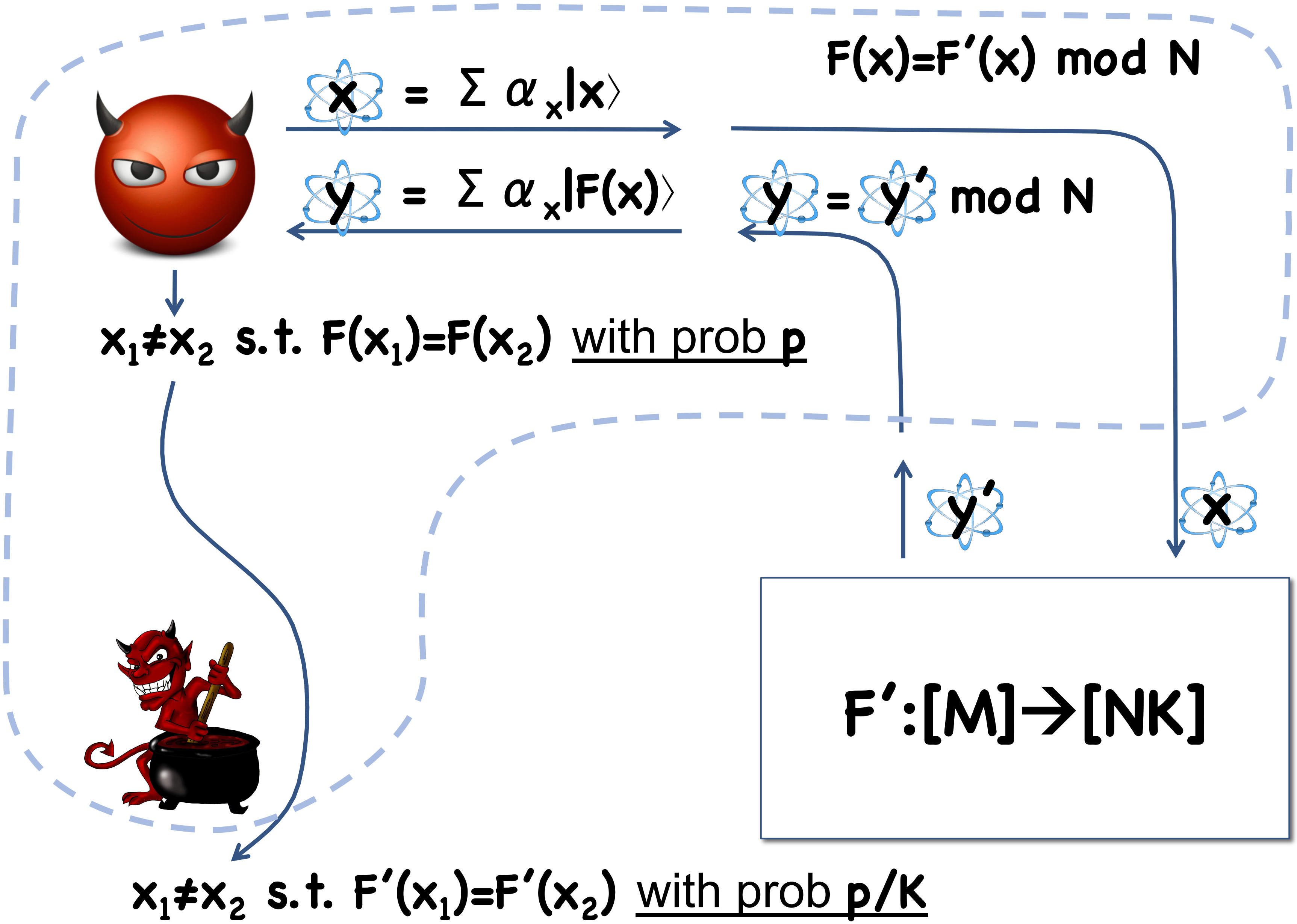
$x = \sum \alpha_x |x\rangle$

$y' = \sum \alpha_x |F'(x)\rangle$

$F':[M] \to [NK]$

$x_1 \neq x_2$ s.t. $F'(x_1)=F'(x_2)$ <u>with prob **p'**</u>

Proof



F(x)=F'(x) mod N
x = Σ α_x|x⟩
y = Σ α_x|F(x)⟩
y = y' mod N
x₁≠x₂ s.t. F(x₁)=F(x₂) with prob p
y'
x
F':[M]→[NK]
x₁≠x₂ s.t. F'(x₁)=F'(x₂) with prob p/K

Proof

Success prob p
on $F:[M] \rightarrow [N]$

Success prob p/K
on $F':[M] \rightarrow [N' = NK]$

Choose K so that $N' = NK \geq M$

$$\Rightarrow \quad p/K = O(q^3/(NK))$$

$$\Rightarrow \quad p = O(q^3/N) \quad ✓$$

Proof Overview

Thm ([Zha'15]): $O(q^3/N)$ bound on success probability for average case quantum collision *detection* problem

Cor 1: $O(q^3/N)$ bound on success probability for average case quantum collision *finding* problem when $N \geq M$

Cor 2: $O(q^3/N)$ bound on success probability for average case quantum collision *finding* problem for *arbitrary* N,M

Cor 3: $\Omega(N^{1/3})$ lower bound for average case quantum collision *finding* problem for arbitrary N,M

Effect of Different Solvabilities

Suppose QQS was $O(q/N^{1/3})$

Success prob p
on $F:[M]\rightarrow[N]$

Success prob p/K
on $F':[M]\rightarrow[N' = NK]$

Choose K so that $N' = NK \geq M$

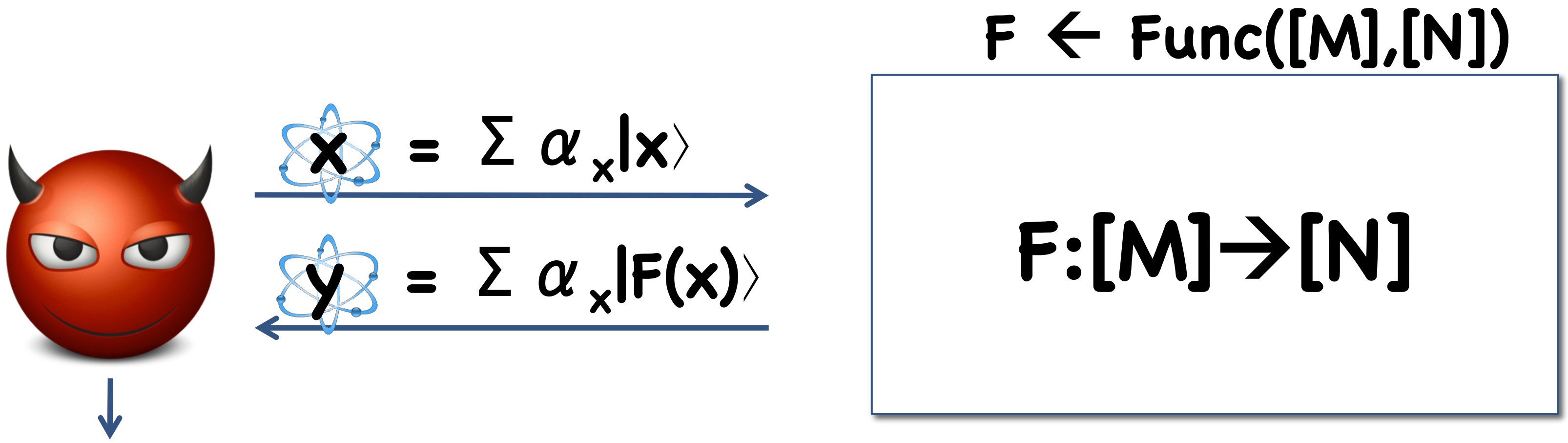
$$\Rightarrow \quad p/K = O(q/(NK)^{1/3})$$

$$\Rightarrow \quad p = O(qK^{2/3}/N^{1/3}) = O(q\ M^{2/3}/N)$$

Quantum query complexity is $\Omega(N/M^{2/3})$

- Meaningless when $N<M^{2/3}$

Case Study 3: Quantum Oracle Interrogation



Distinct $(x_1,F(x_1)),(x_2,F(x_2)),\ldots,(x_k,F(x_k))$

Comes up in quantum resistant MAC/Signature analysis

- **N** exponential
- Want (extremely) low success probability even for **q=k-1**
- Success prob **1** for **q=k** ⇒ Asymptotic query count meaningless

[vD'98]: Query complexity **< 0.501k** for **N=2**

Case Study 3: Quantum Oracle Interrogation

How does [vD'98] generalize to arbitrary **N**?

Open up analysis:

- Success probability $\sum_{r=0}^{q} \binom{k}{r}$
- Generalize algorithm to arbitrary **N**: $C_{k,q,N} := \sum_{r=0}^{q} \binom{k}{r} (N-1)^r$
- Small constant **N**: $q = (1-1/N+\varepsilon)k \Rightarrow$ prob $1-2^{-O(k)}$
  - E.g. $N=4$ (**2** bit outputs), need $q=0.751k$ queries to output k points
- Exponential **N**: even when $q=k-1$, prob is $< (q+1)/N$
  - But is this attack optimal?

Matching Lower Bound?

Existing methods (e.g. adversary, polynomial) don't cut it as is

- Theorem statements asymptotic in *query number*
- Other difficulties in using

[BZ'13]: developed new method – the Rank method

- Relates success prob after **q** queries to prob before *any* query
- Built from the start to give quantum query *solvability* results

Thm ([BZ'15]): $\boldsymbol{C_{k,q,N}}$ is the best possible success probability for quantum oracle interrogation

- [vD'98] and generalization are **exactly** optimal!

Takeaways

QQS useful quantity to study

- Natural
- Reveals important info missed using QQC alone
- Good for cryptographers
- Meaningful in settings where QQC loses meaning
- Can help for proving QQC results
- Better understanding of power of a quantum query?
  - Extra **q** factor?

?