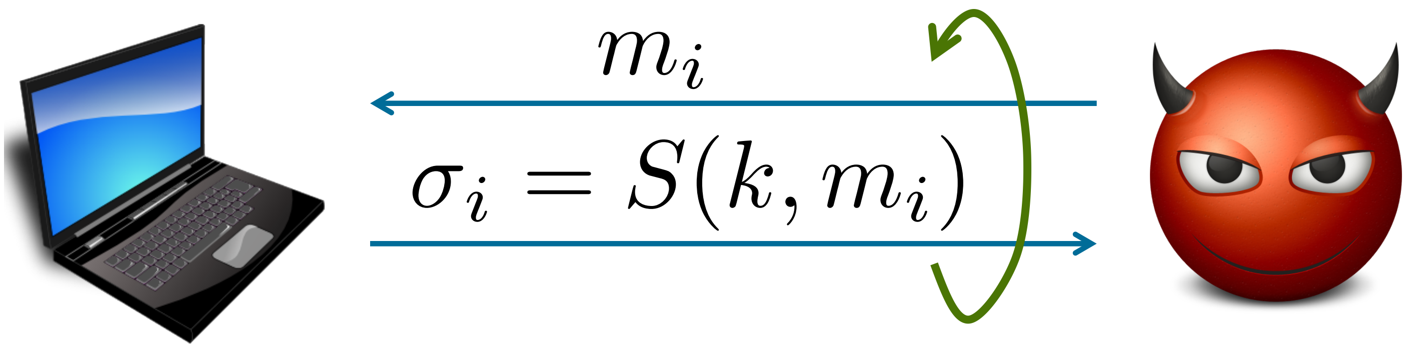
Quantum-Secure Message Authentication Codes

Dan Boneh and Mark Zhandry – Stanford University

Classical Chosen Message Attack (CMA)



Secret key k

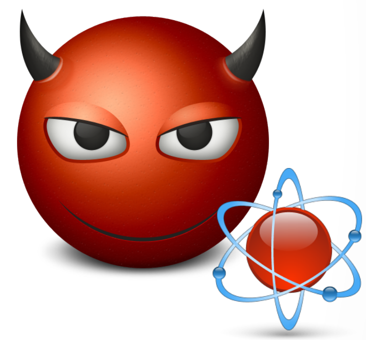
Post-Quantum CMA

Adversary has **quantum** computing power:

Secret key k

$$m_i$$

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

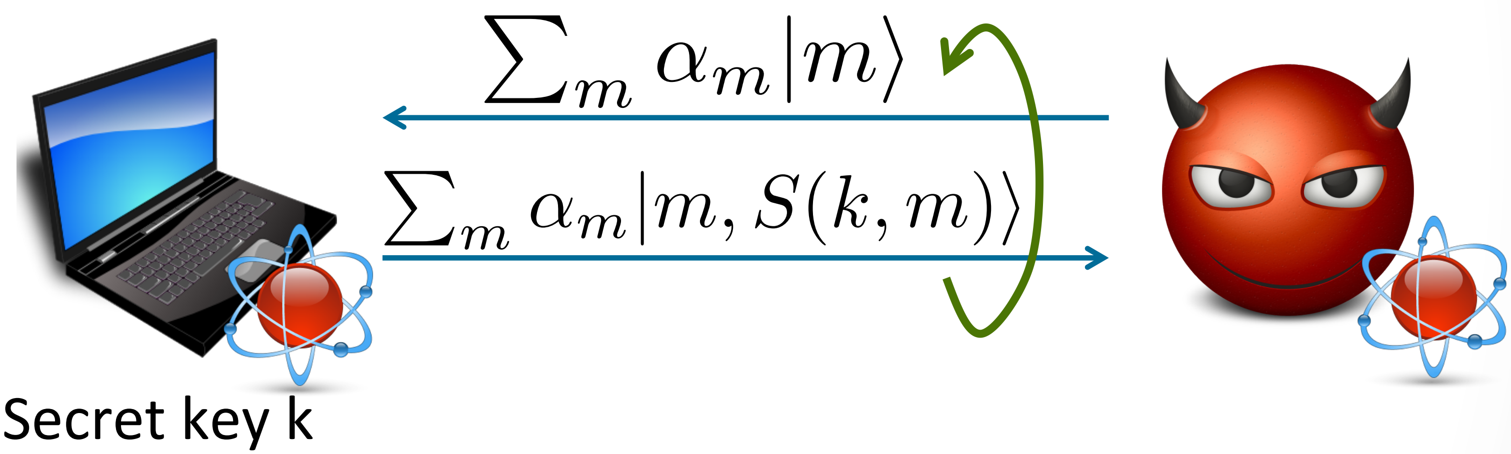


Interactions remain **classical**

$\Rightarrow$ security models **unchanged**

Quantum CMA

Everyone is quantum ⇒ **quantum queries**



Quantum interactions ⇒ **new** security models

Extends [BDFLSZ'11, DFNS'11, Zha'12a, Zha'12b]

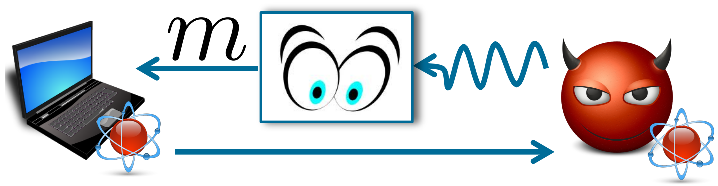
An Emerging Field

Many classical security games have quantum analogs:

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

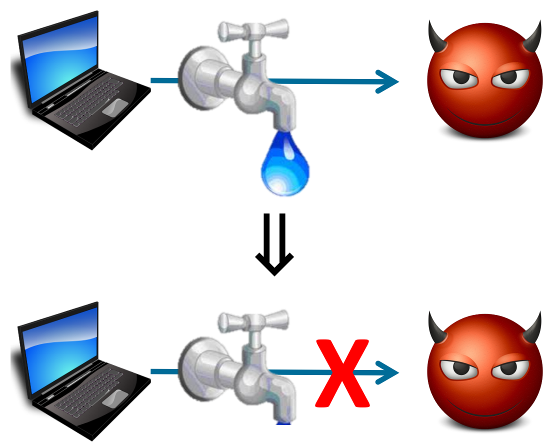
Motivation

Hardware Alternative:
“Classicalize” queries by observing them



Hardware designer – ensure nobody can bypass

Leakage Analog:



Hardware designer – ensure no side-channels

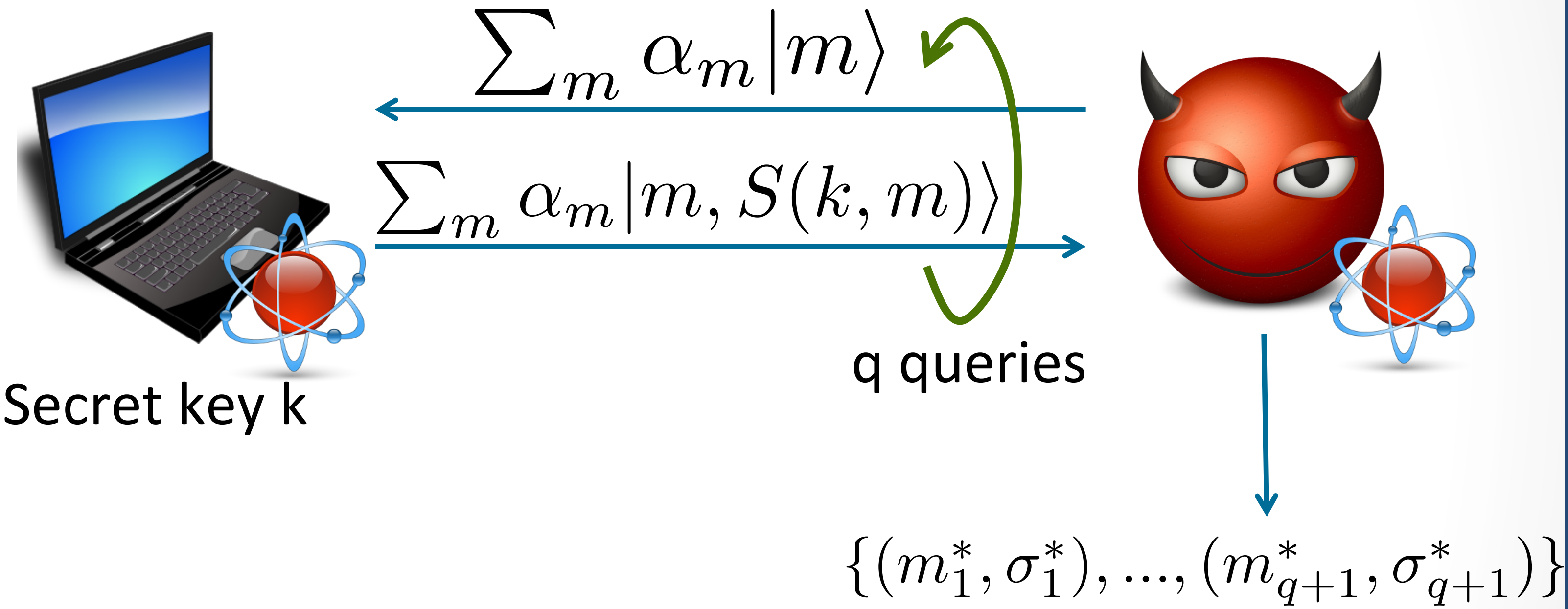
Software Alternative:
Quantum-secure crypto

Hardware designer not worried

Software Alternative:
Leakage-resilient crypto

Hardware designer not worried

Quantum MAC Security: Definitions



Existential forgery:

q quantum queries $\Rightarrow$ **q+1 (distinct) tags**

Building Quantum-Secure MACs

First attempt: do classical constructions work?

Example: **1-time** MAC from **pairwise independence**

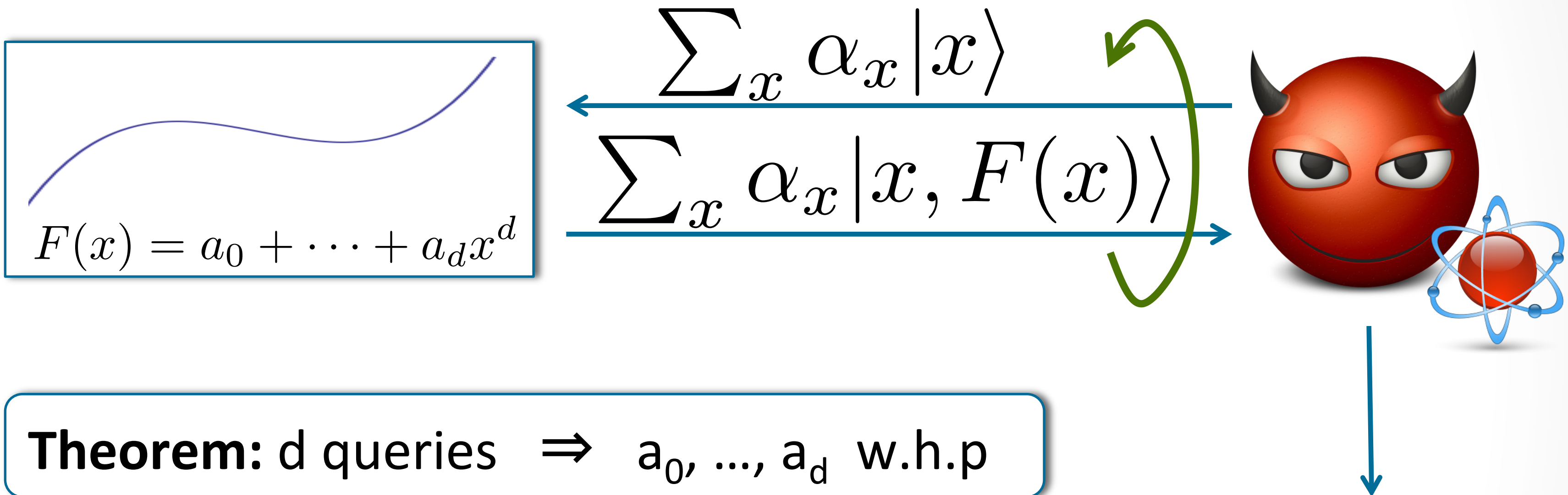
$$S(k,m) = h_k(m)$$

$h_k(m)$ pairwise independent

e.g. $h_k(m) = k_1 m + k_2 \mod p$

One quantum query $\Rightarrow$ **two tags???**

Quantum Polynomial Interpolation



$$(a_0, \cdots, a_d)$$

Theorem: d queries ⇒ $a_0, \ldots, a_d$ w.h.p

Classically, need d+1 queries

Best known lower bound: (d+1)/2 queries

Example: 1 quantum query to $h_k(m) = k_1 m + k_0 \bmod p$ ⇒ k_0, k_1

→ Pairwise independence is **insecure** for one-time MAC

→ Carter Wegman (CW) is **insecure** under quantum CMA

Secure 1-Time MACs

Theorem: Any **4-wise** independent function is a quantum secure one-time MAC

2-wise independence: **insecure**

3-wise independence: **???**

4-wise independence: **secure**

Can also make CW secure with pairwise independence

Quantum-Secure MACs from PRFs

Classical construction:

S(k , m)	=	PRF(k , m)
V(k , m , σ)	=	Check: PRF(k , m) == σ

Classical CMA: **secure**

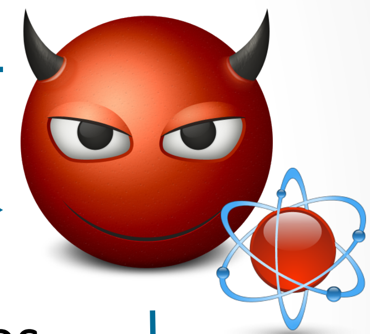
Quantum CMA: **???**

Quantum-Secure MACs from PRFs

Secret key k

$\sum_m \alpha_m |m\rangle$

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



q queries

$\{(m_1^*, \sigma_1^*), \ldots, (m_{q+1}^*, \sigma_{q+1}^*)\}$

Existential forgery:

q quantum queries $\Rightarrow$ **q+1 (distinct) points** of PRF

Quantum-Secure PRFs [Zha'12b]

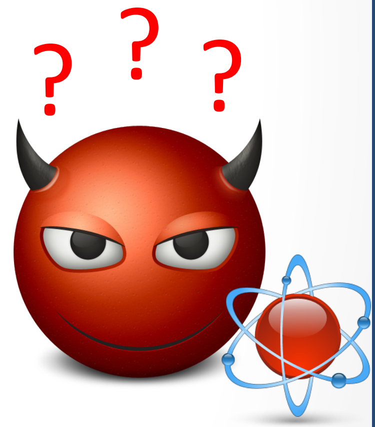
Main tool for building MACs:

Random key k

$F(x) \equiv PRF(k, x)$

$\sum_x \alpha_x |x\rangle$

$\sum_x \alpha_x |x, F(x)\rangle$



vs.

Random function F from $\mathcal{X}$ to $\mathcal{Y}$

$\sum_x \alpha_x |x\rangle$

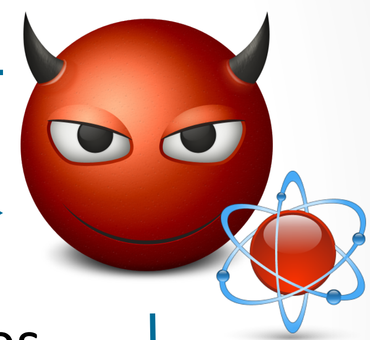
$\sum_x \alpha_x |x, F(x)\rangle$

Quantum Oracle Interrogation

Random function F from $\mathcal{X}$ to $\{0,1\}^n$

$\sum_m \alpha_m |m\rangle$

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



q queries

$\{(m_1^*, \sigma_1^*), \ldots, (m_{q+1}^*, \sigma_{q+1}^*)\}$

Hypothetical MAC forger:

q quantum queries $\Rightarrow$ **q+1 (distinct) points** of F

Question: **Is this hard?**

Quantum Oracle Interrogation

Classically: hard Adv[q+1 points]: $\frac{1}{2^n}$

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

Theorem: Random function F: X → $\{0,1\}^n$

Adv[**q queries** ⇒ **q+1 points**] ≤ $\frac{q+1}{2^n}$

Highly non-trivial

New quantum impossibility tool: The **Rank Method**

Therefore:

- Small range: Adv[**q+1 points**] large
- Large range: Adv[**q+1 points**] small

The Rank Method

Rank: new quantity for quantum oracle algorithms

- Measure of information learned by algorithm

Adv[q queries ⇒ q+1 points]
≤ Rank[q queries] × Adv[0 queries ⇒ q+1 points]

Adv[0 queries ⇒ q+1 points] ≤ $\frac{1}{2^{n(q+1)}}$

Rank[q queries] ≤ $(q+1)2^{nq}$

Adv[q queries ⇒ q+1 points] ≤ $\frac{q+1}{2^n}$

Back to MAC Security

Classical CMA:

secure PRF ⇒ **secure MAC** (Adv: $\frac{1}{2^n}$)

Quantum CMA:

quantum-secure PRF ⇒ **quantum-secure MAC** (Adv: $\frac{q+1}{2^n}$)

Both cases:

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

Summary & Open Problems

Quantum security stronger than classical security

- Pairwise independent functions: **1-time insecure**
- Classical Carter-Wegman: **insecure**

MACs secure against quantum CMA:

- quantum-secure PRF ⇒ **quantum-secure MAC**
- 4-wise independent hash ⇒ **1-time MAC**
- Efficient "Quantum Carter Wegman"

Open Problem:

- CBC-MAC, PMAC, NMAC **quantum secure?**

Thanks!