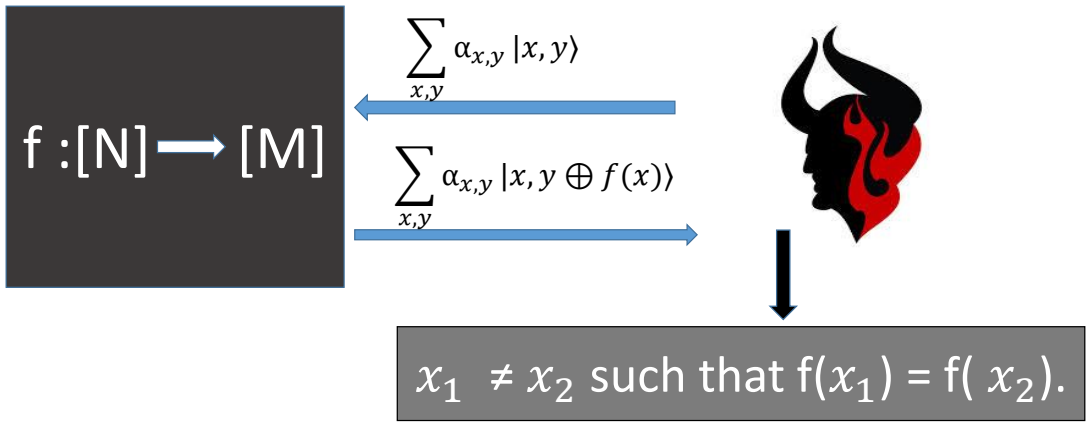
Quantum Collision-Resistance of Non-Uniformly Distributed Functions

Made by:
Ehsan Ebrahimi Targhi

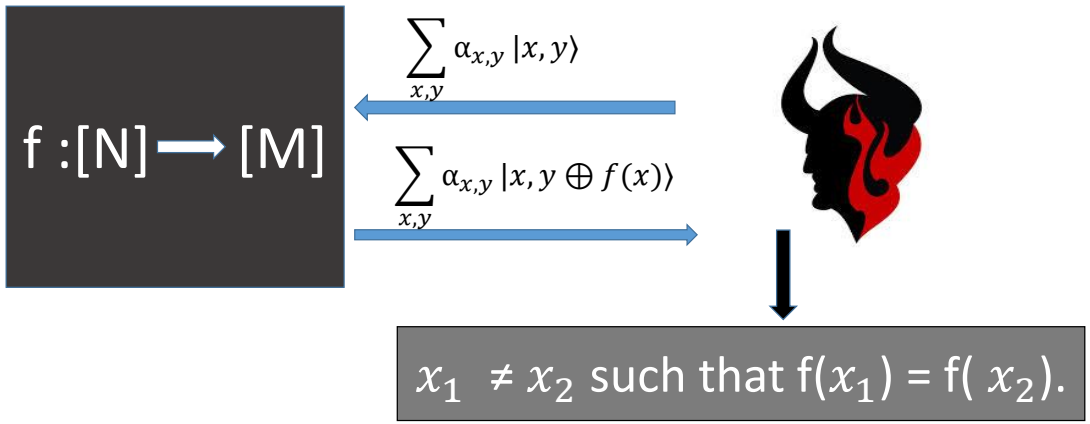
University of Tartu

PQCrypto Conference, Fukuoka, Japan
24 February 2016
Joint work with Dominique Unruh and Gelo Tabia

The problem: (Quantum Collision)



The problem: (Quantum Collision)



Question: How many quantum queries are needed to output a collision? (quantum query complexity point of view)
or
What is the maximum success probability given the specific number of queries? (quantum query solvability (Zhandry))

Why for random function?

Collision-resistant hash functions are fundamental in cryptology.

Why for random function?

Collision-resistant hash functions are fundamental in cryptology.

1. In the random oracle model, they model as random functions.

Why for random function?

Collision-resistant hash functions are fundamental in cryptology.

1. In the random oracle model, they model as random functions.
2. In most cryptographic applications, they need to be compression functions.

Why for random function?

Collision-resistant hash functions are fundamental in cryptology.

1. In the random oracle model, they model as random functions.
2. In most cryptographic applications, they need to be compression functions.

Recall: By birthday attack, the probability of success is roughly $1/2$ when $q = \Theta(M^{1/2})$ for a classical adversary.

Previous result:

Theorem

Let $f : [N] \to [M]$ be a random function. Then any quantum algorithm making q number of queries to f outputs a collision for f with probability at most $\frac{C(q+2)^3}{M}$ where C is a universal constant.[1]

$\Rightarrow \Omega(M^{1/3})$ queries are needed to output a collision.

[1] [Zhandry, Quantum Information & Computation, 2015]

Previous result:

Theorem

Let $f : [N] \to [M]$ be a random function. Then any quantum algorithm making q number of queries to f outputs a collision for f with probability at most $\frac{C(q+2)^3}{M}$ where C is a universal constant.[1]

$\Rightarrow \Omega(M^{1/3})$ queries are needed to output a collision.

Question: What if outputs of function f are chosen according to a non-uniform distribution.

[1] [Zhandry, Quantum Information & Computation, 2015]

Motivation for non-uniform functions:

- In some cryptographic constructions, the combination of a truly random function and encryption function has to be collision-resistant:

Motivation for non-uniform functions:

- In some cryptographic constructions, the combination of a truly random function and encryption function has to be collision-resistant:
  - Fujisaki-Okamoto transform:

$$Enc^{hy}_{pk}(m;\delta) = \left(Enc^{asy}_{pk}\left(\delta; H\left(\delta \| Enc^{sy}_{G(\delta)}(m)\right)\right),\ Enc^{sy}_{G(\delta)}(m)\right).$$

    - $Enc^{asy}_{pk} \circ H$ has to be collision-resistant.

Our contribution:

$$H_\infty(D) = -\log \max_{m \in [M]} \Pr[D(m)]$$

Theorem

Let $f : [N] \to [M]$ be a function whose outputs are chosen according to a distribution with min-entropy k. Then any quantum algorithm A making q queries to f returns a collision for f with probability at most $\frac{C'(q+2)^{9/5}}{2^{k/5}}$ where C' is a universal constant.

$\Rightarrow \Omega(2^{k/9})$ queries are needed to output a collision.

Preliminaries (for proof):

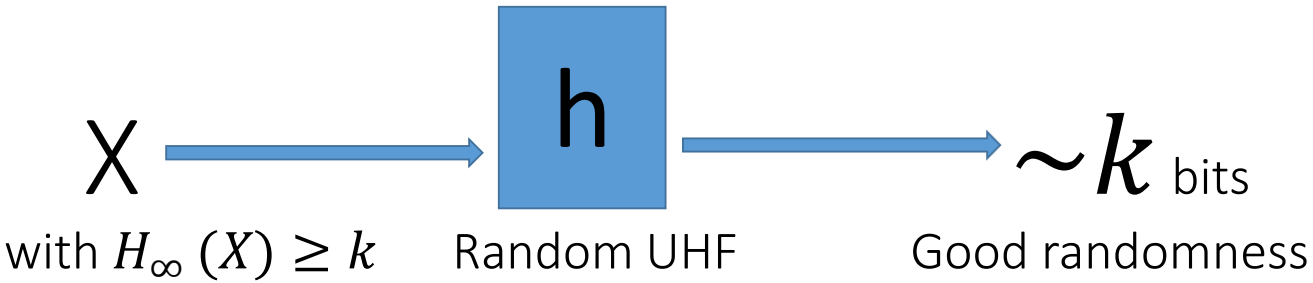
Definition (Universal Hash Function [2])

A family of functions $H = \{h : \{0,1\}^n \to \{0,1\}^m\}$ is called a universal family if for all distinct $x, y \in \{0,1\}^n$:

$$\Pr[h(x) = h(y) : h \xleftarrow{\$} H] \leq 1/2^m.$$

[2] [Larry Carter, Mark N. Wegman, J. Comput. Syst. Sci, 1979]

Preliminaries (Leftover Hash Lemma[3]):



[3] [Johan Håstad, Russell Impagliazzo, Leonid A. Levin, Michael Luby, 1993]

Proof sketch:

$$\Pr[\mathrm{Coll}(f; A_q^f) : f \leftarrow D^X]$$

$$\overset{(1)}{\leq} \Pr[\mathrm{Coll}(h \circ f; A_q^f) : f \leftarrow D^X]$$

$$\overset{(2)}{=} \Pr[\mathrm{Coll}(h \circ f; B_q^{h \circ f}) : f \leftarrow D^X] \text{ (preimages of } f \text{)}$$

$$\overset{(3)}{\approx} \Pr[\mathrm{Coll}(f^*; B_q^{f^*}) : f^* \xleftarrow{\$} \{\}] \text{ (LHL, } (D_1 \cong D_2 \iff D_1^X \cong D_2^X)^4)$$

$$\overset{(4)}{\approx} \text{ hard}$$

We prove that

$$\Pr[\mathrm{Coll}(f; A_q^f) : f \leftarrow D^X] \leq O(\frac{q^{9/5}}{2^{k/5}}).$$

[4] [Zhandry, How to Construct Quantum Random Functions, FOCS, 2012]

Question?

Thank you for listening!