Merkle Puzzles in a Quantum World

Kassem Kalach

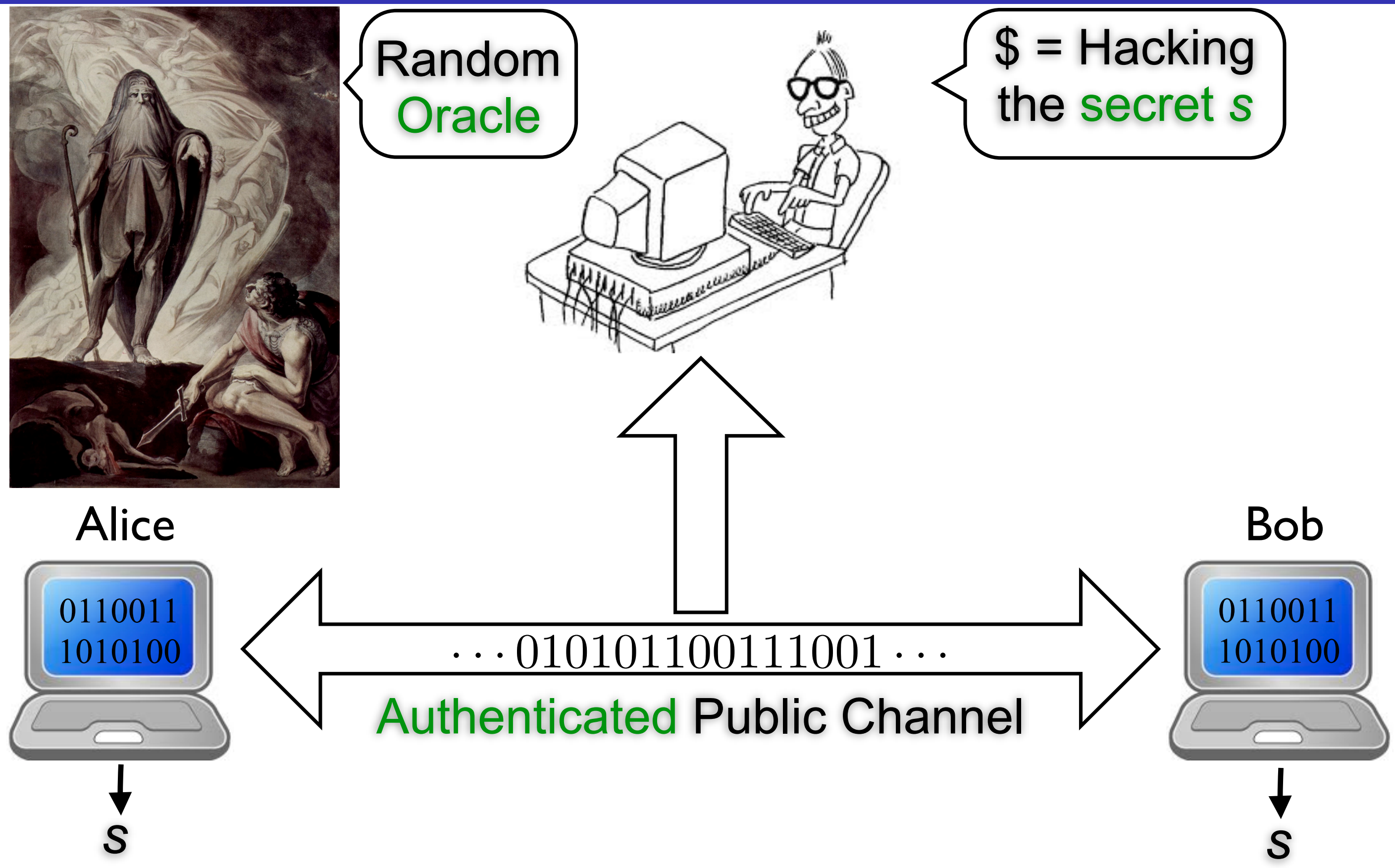
LITQ, DIRO
Université de Montréal

Joint work with

Gilles Brassard	Université de Montréal
Peter Høyer	University of Calgary
Marc Kaplan	Université de Montréal
Sophie Laplante	Université Paris-Sud
Louis Salvail	Université de Montréal

QCrypt 2011
ETH, Zurich, Swiss
12 September 2011

Key Establishment/Distribution Problem



Challenge

Make the eavesdropping effort grow as much as possible in the legitimate effort (query complexity).

The First Seminal Solution [Merkle74]

- By Ralph Merkle in 1974, as a project proposal in a course on computer security (CS244) at UC Berkeley.
- Rejected by the Professor, but Merkle continued working on it.
- Eventually published in 1978 by *Communications of the ACM,* it was initially rejected because:

Ms. Susan L. Graham
Computer Science Division-EECS
University of California, Berkeley
Berkeley, California 94720

CACM Editor

Dear Ms. Graham,

Thank you very kindly of your communication of October 7 with the enclosed paper on "Secure Communications over Insecure Channels". I am sorry to have to inform you that the paper is not in the main stream of present cryptography thinking and I would not recommend that it be published in the Communications of the ACM, for the following reasons:

http://merkle.com/1974

The First Seminal Solution [Merkle74] (...)

- Based on the birthday paradox.

Nice Property

Merkle scheme is provably secure in the random oracle model in contrast with schemes based on the assumed difficulty of some mathematical problems (such as RSA and Diffie-Hellman).

Definition of Security

A protocol is secure if the eavesdropping effort grows super-linearly with the legitimate effort.

Merkle's Scheme [Merkle74]

Alice

X	Y
x_1	$f(x_1)$
$\vdots$	$\vdots$
x_i	$f(x_i)$
$\vdots$	$\vdots$
x_N	$f(x_N)$

$$x \rightarrow \boxed{N^2} \rightarrow f(x)$$

$$\xrightarrow{f(x_1), \ldots, f(x_i), \ldots, f(x_N)}$$

Bob

Find one element of *X*:

$s \in_R \mathrm{Dom}(f)$

$f(s) \in Y?$ No!

Merkle's Scheme [Merkle74]

Alice

X	Y
x_1	$f(x_1)$
$\vdots$	$\vdots$
x_i	$f(x_i)$
$\vdots$	$\vdots$
x_N	$f(x_N)$

$$x \rightarrow \boxed{N^2} \rightarrow f(x)$$

$$\xrightarrow{f(x_1), \ldots, f(x_i), \ldots, f(x_N)}$$

Bob

Find one element of *X*:

$s \in_R \mathrm{Dom}(f)$

$f(s) \in Y?$ No!

Merkle’s Scheme [Merkle74]

Alice

X	Y
x_1	$f(x_1)$
$\vdots$	$\vdots$
x_i	$f(x_i)$
$\vdots$	$\vdots$
x_N	$f(x_N)$

x

N^2

$f(x)$

$$f(x_1), \ldots, f(x_i), \ldots, f(x_N) \longrightarrow$$

$$\xleftarrow{\quad f(s) \quad}$$

Bob

Find one element of X:

$s \in_R \mathrm{Dom}(f)$

$f(s) \in Y$? Yes!

Achieved in $O(N)$ queries, based on the birthday paradox.

s

Merkle's Scheme [Merkle74]

Alice

$x \to N^2 \to f(x)$

Bob

$$f(x_1), \ldots, f(x_i), \ldots, f(x_N) \longrightarrow$$

X	Y
x_1	$f(x_1)$
$\vdots$	$\vdots$
x_i	$f(x_i)$
$\vdots$	$\vdots$
x_N	$f(x_N)$

$\longleftarrow \stackrel{?}{=} f(s)$

Yes!

Find one element of X:

$s \in_R \mathrm{Dom}(f)$

$f(s) \in Y?$ Yes!

Achieved in $O(N)$ queries, based on the birthday paradox.

$$\xleftarrow{\quad f(s) \quad}$$

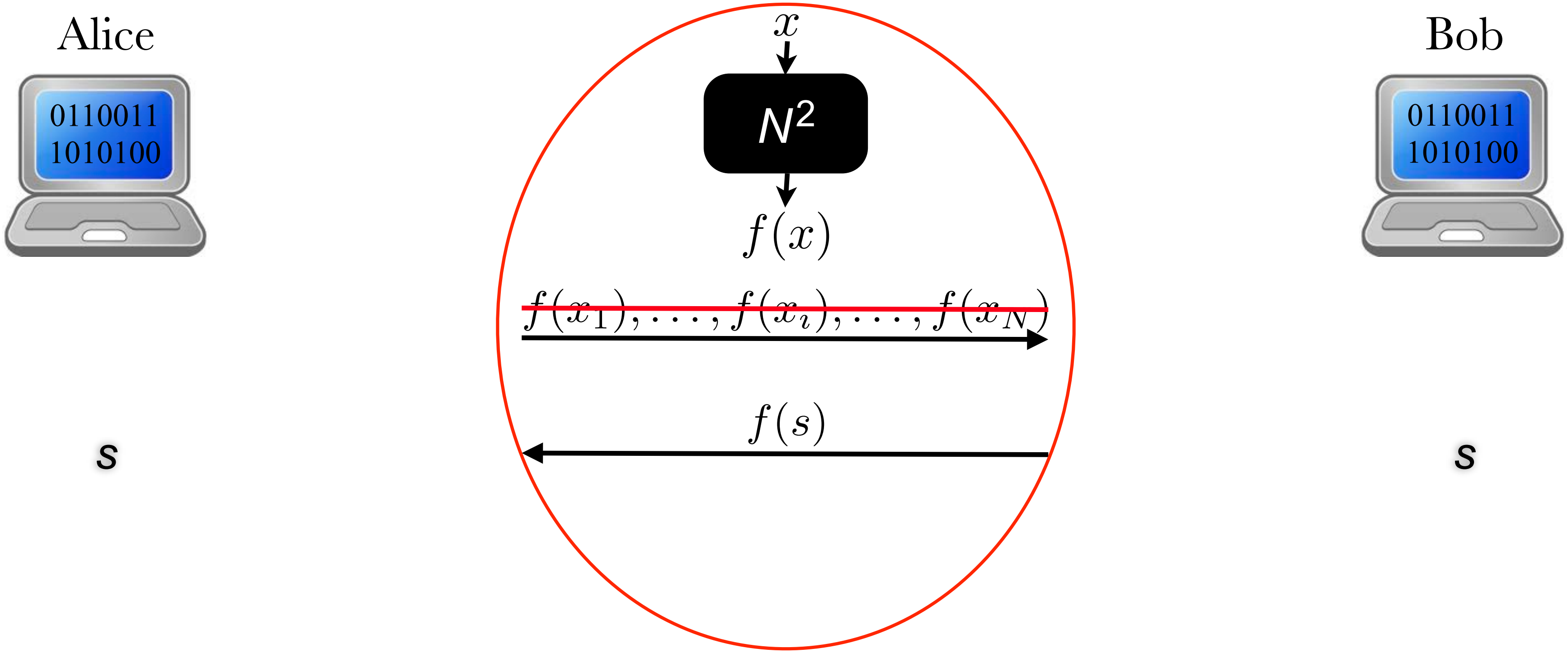
Given $f(s)$, use the table to find s.

$\downarrow$ s

Alice and Bob agree on a secret s with $O(N)$ queries

$\downarrow$ s

Security of Merkle's Scheme



Eavesdropper
needs $\Omega(N^2)$ queries to find s

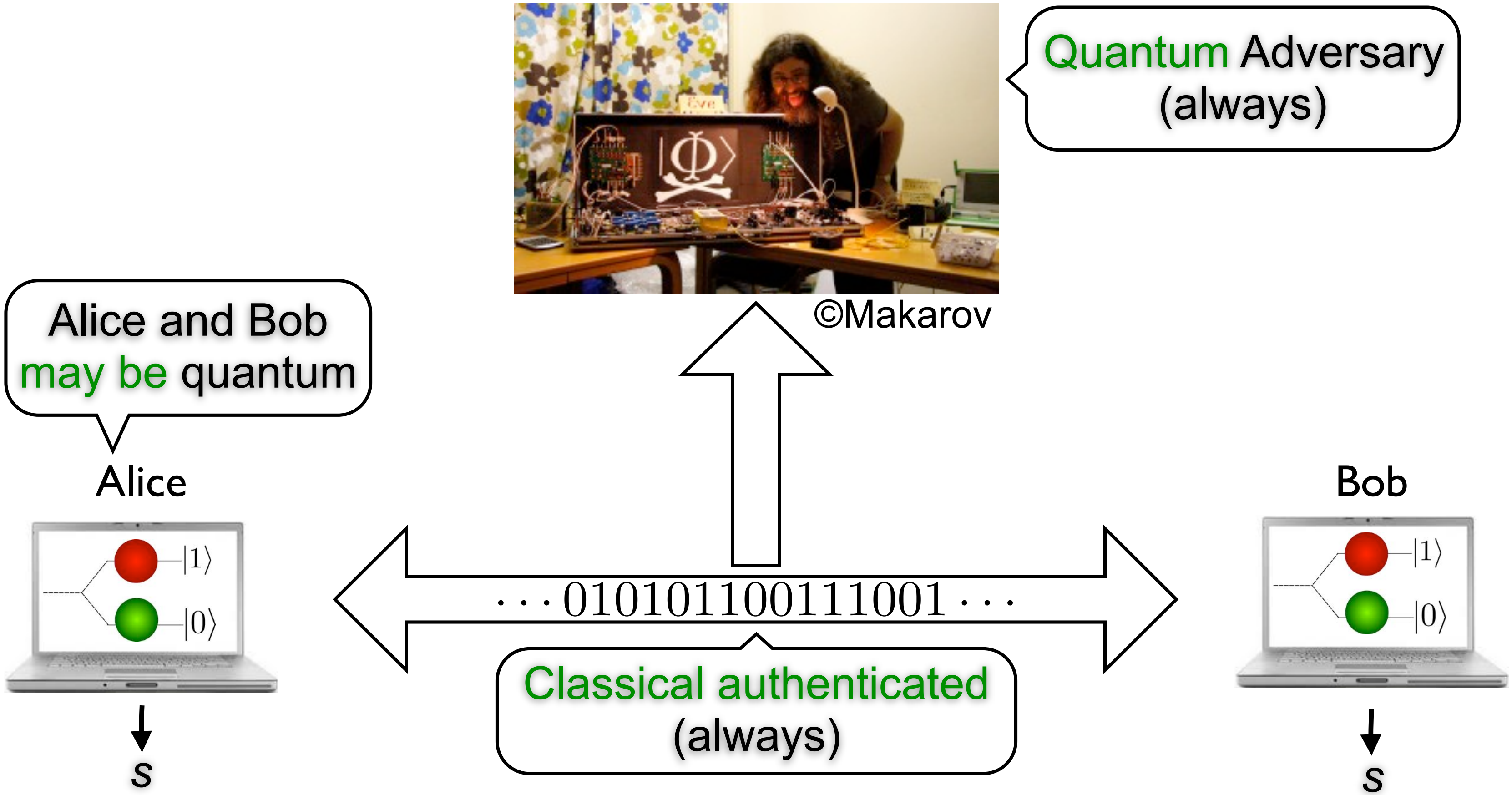
Can we do better?

No!
Every key exchange protocol in the random oracle model can be broken in $O(N^2)$ queries.

[Barak, Mahmoody 08].

Problem solved: $\Theta(N^2)$ is best possible

Key Agreement à la Merkle in a Quantum World



Preliminary: Grover's Algorithm & its Generalization (BBHT)

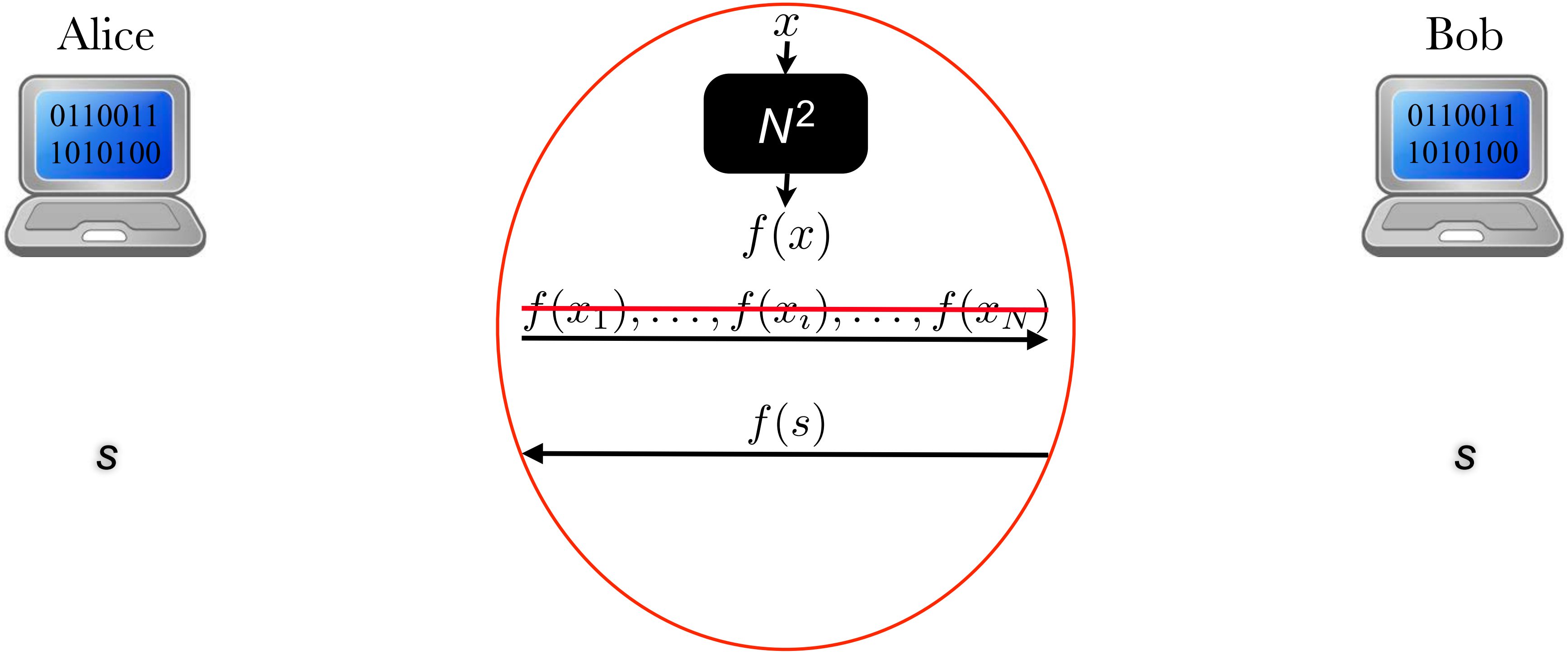
- Grover [Grover 96]
- BBHT [Boyer, Brassard, Høyer, Tapp 96].

Unstructured search problem

Consider a black-box function of domain of size N, and $t > 0$ distinct images of this function. The problem is to invert one of them.

- BBHT's algorithm solves this problem after about $\sqrt{N/t}$ quantum queries.
- To invert a specific image ($t = 1$), Grover's algorithm finds the solution after about $\sqrt{N}$ quantum queries.
- This is optimal [Bennett, Bernstein, Brassard, Vazirani 97 and Zalka 99].

Security of Merkle's Scheme in a Quantum World



Eavesdropper

finds s in $O(\sqrt{N^2}) = O(N)$ queries using Grover.

Motivating Questions

1. Can the quadratic security of Merkle's scheme be restored if legitimate parties make use of quantum powers as well?

2. Can every key exchange protocol in the random oracle model be broken in $O(N)$ quantum queries when legitimate parties are classical?

Quantum Merkle Puzzles [Brassard, Salvail 08]

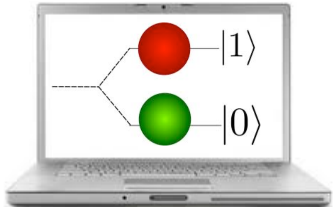
Alice

X	Y
x_1	$f(x_1)$
$\vdots$	$\vdots$
x_i	$f(x_i)$
$\vdots$	$\vdots$
x_N	$f(x_N)$

$$x \rightarrow \boxed{N^3} \rightarrow f(x)$$

$$f(x_1), \ldots, f(x_i), \ldots, f(x_N)$$

Bob



Find one element of X.

Quantum Merkle Puzzles [Brassard, Salvail 08]

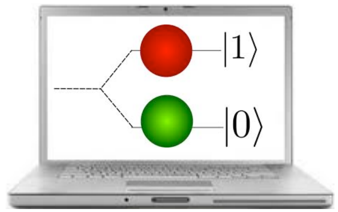
Alice

x

N^3

$f(x)$

Bob



X	Y
x_1	$f(x_1)$
$\vdots$	$\vdots$
x_i	$f(x_i)$
$\vdots$	$\vdots$
x_N	$f(x_N)$

$\leftarrow \stackrel{?}{=} f(s)$

$$\xrightarrow{f(x_1), \ldots, f(x_i), \ldots, f(x_N)}$$

Find one element of *X*.

Using BBHT, this can be done in

$$O\left(\sqrt{\frac{N^3}{N}}\right) = O(N)$$

quantum queries.

Yes!

$$\xleftarrow{f(s)}$$

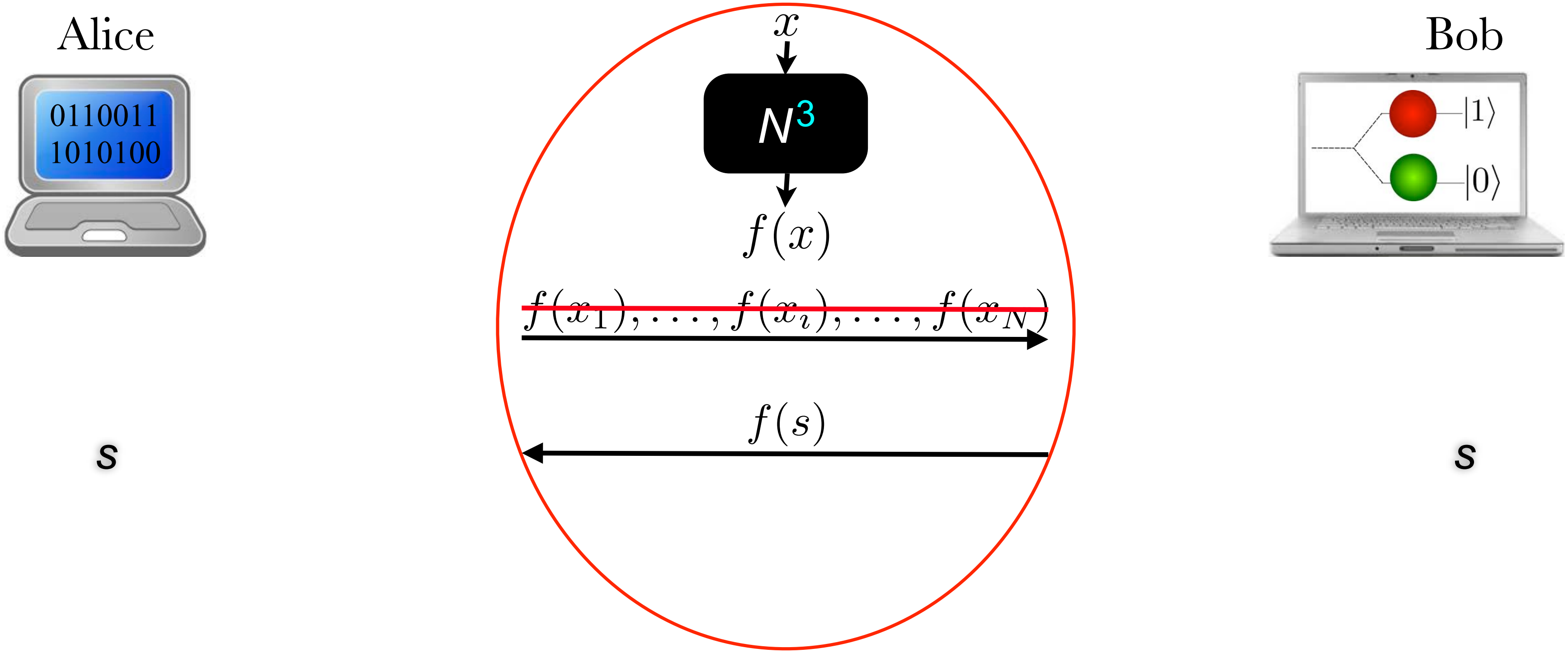
Given $f(s)$, use the table to find *s*.

$\downarrow$ *s*

Alice and Bob agree on a secret *s* in *O*(*N*) queries

$\downarrow$ *s*

Security of Quantum Merkle Puzzles



Eavesdropper
finds s in $O(\sqrt{N^3}) = O(N^{3/2})$
using Grover. This is optimal.

Our First Contribution

Can we do better?

Yes! We devised a quantum protocol and proved its security of

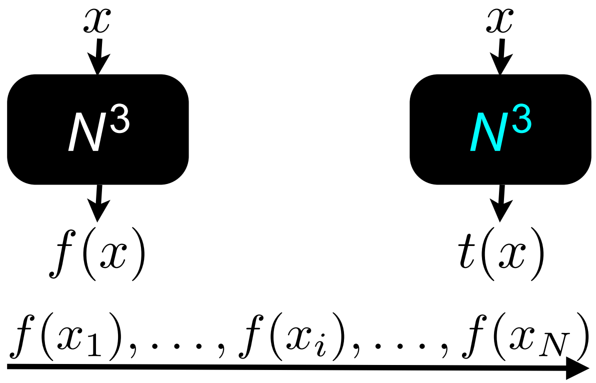
$$\Omega(N^{5/3})$$

queries.

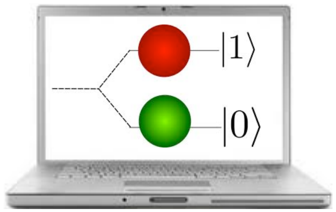
Improved Quantum Merkle Protocol [Our 1st Contribution]

Alice

X	Y
x_1	$f(x_1)$
$\vdots$	$\vdots$
x_i	$f(x_i)$
$\vdots$	$\vdots$
x_N	$f(x_N)$



Bob



Find two elements of X.

Using BBHT, this can be done in

$$O\left(\sqrt{\frac{N^3}{N}}\right) = O(N)$$

quantum queries.

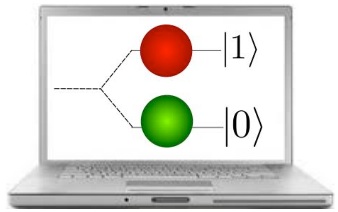
(s, s')

Improved Quantum Merkle Protocol [Our 1st Contribution]

Alice

$$x \downarrow \boxed{N^3} \downarrow f(x) \qquad x \downarrow \boxed{N^3} \downarrow t(x)$$

Bob



X	Y	Z
x_1	$f(x_1)$	$t(x_1)$
$\vdots$	$\vdots$	$\vdots$
x_i	$f(x_i)$	$t(x_i)$
$\vdots$	$\vdots$	$\vdots$
x_N	$f(x_N)$	$t(x_N)$

$$f(x_1), \ldots, f(x_i), \ldots, f(x_N) \longrightarrow$$

Find two elements of X.

Using BBHT, this can be done in

$$O\left(\sqrt{\frac{N^3}{N}}\right) = O(N)$$

quantum queries.

$$\longleftarrow w = t(s) \oplus t(s')$$

Given w, use table and bitwise XOR to find the secret.

$\downarrow$ (s, s')

Alice and Bob agree on a secret in $O(N)$ queries

$\downarrow$ (s, s')

Security Proof of Our 1st Contribution

1. We devised an $O(N^{5/3})$-query quantum attack.
2. We proved a matching $\Omega(N^{5/3})$-query lower bound.

Optimal Quantum Attack

- Based on quantum walks in a Johnson graph.
- Adaptation of Ambainis' algorithm for the element distinctness problem [Ambainis 03], which is optimal [Aaronson, Shi 04].

The Element Distinctness Problem (ED)

Given a black-box function *c*, decide if $c(x_i) = c(x_j)$ for some distinct elements x_i, x_j.

Solved in $\Theta(N^{2/3})$ quantum queries, for a domain of size *N*.

The XOR Problem

Given a black-box function *t*, decide if $t(x_i) \oplus t(x_j) = w$ for some distinct elements x_i, x_j.

Solved in $\Theta(N^{2/3})$ quantum queries, for a domain of size *N*.

For the upper bound, we used Ambainis's algorithm for ED.
For the lower bound, we reduced ED to the XOR problem.

Optimal Quantum Attack (...)

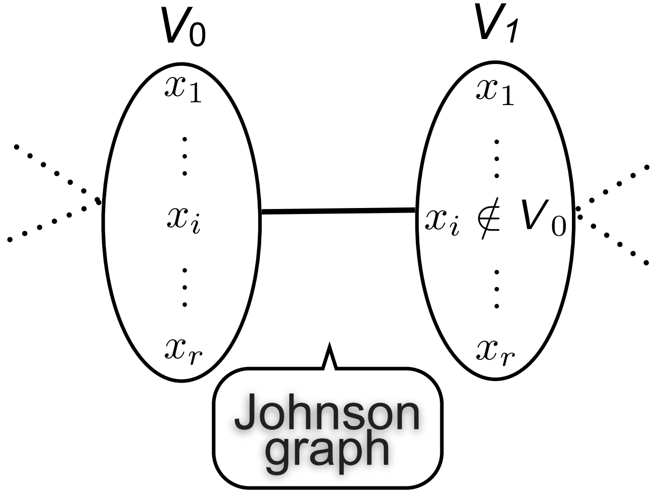
Why do we get $O(N \cdot N^{2/3}) = O(N^{5/3})$?

- The domain of t is X of size N.
- X is embedded randomly in N^3 elements.
- Each query to t requires $\Theta(N)$ queries to f using BBHT.

$$\Theta\left(\sqrt{N^3/N}\right)$$

Walking on Johnson Graph

- Undirected graph in which each vertex contains r entries ($r < N$).
  Each x_i is in X and $t(x_i)$ is kept in the node.
  Connected nodes differ by 2 elements.
- Problem: find a vertex (marked)containing two distinct (x_i, x_j) elements $t(x_i) \oplus t(x_j)$ such $= w$



- <u>S</u>etup phase requires r queries to t and $\Theta(rN)$ queries to f.
- <u>U</u>pdate phase (“walking”) requires one query to t and $\Theta(N)$ queries to f .
- <u>C</u>hecking if a vertex is marked requires no queries.

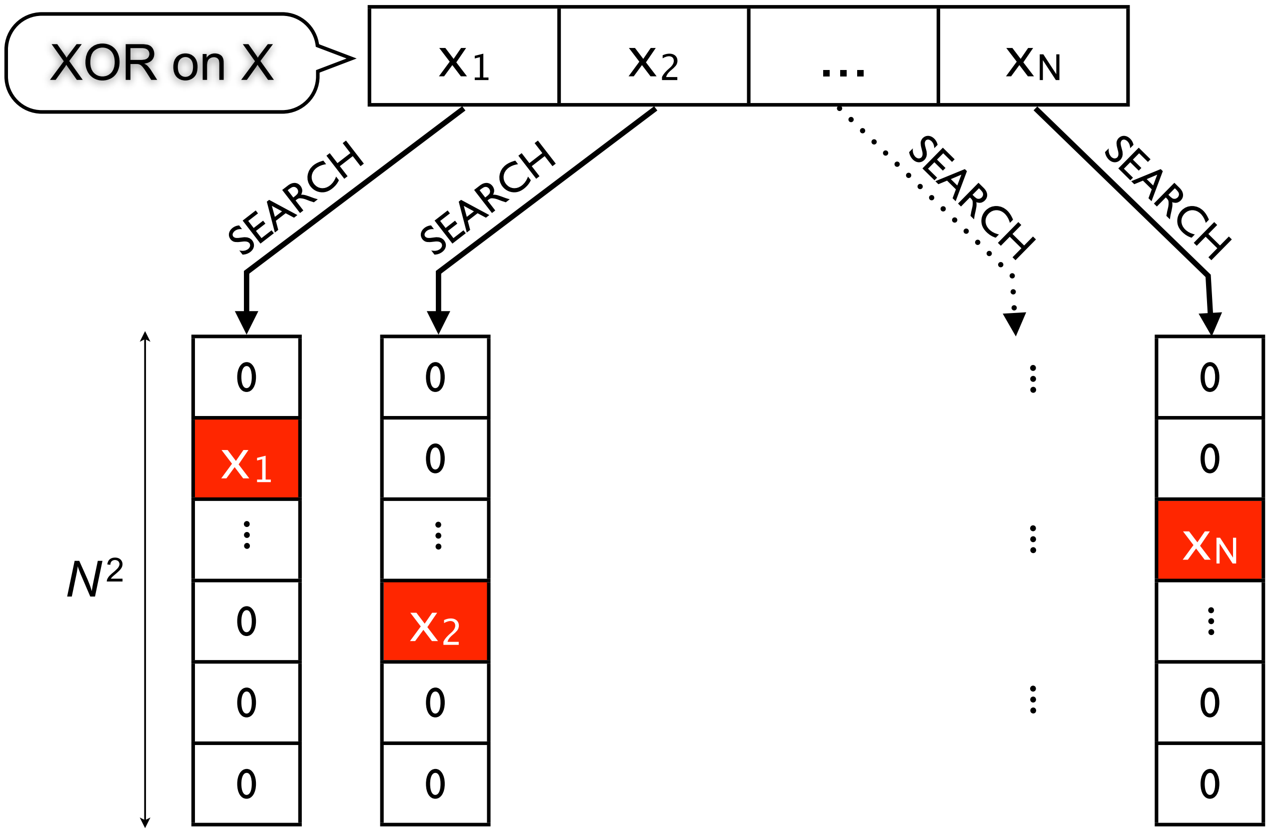
- Solved in $S + O(\frac{N}{r}(\sqrt{r}\,U + C))$ expected queries.
- Taking $r = N^{2/3}$ (optimal), we get $O(N^{5/3})$ queries to f and $O(N^{2/3})$ queries to t .

Lower Bound Proof Sketch

1. We defined a search problem related to XOR problem;
2. We proved $\Omega(N^{5/3})$ lower bound for this search problem; and
3. We reduced this search problem to the eavesdropping strategy against our protocol.

Lower Bound Proof Sketch (...)

- Given N "buckets" of size N^2.
- Each bucket contains one element of X, and zero elsewhere.
- Problem: find two distinct elements such that $t(x_i) \oplus t(x_j) = w$.



Lower Bound Proof Sketch (...)

Crucial observation

The defined search problem is the composition of the XOR problem on N elements, with SEARCHing each element in a set of size N^2.

- One would like to apply the composition theorem due to
  - Høyer, Lee and Špalek [2007] and
  - Lee, Mittal, Reichardt and Špalek [2010].
- Not applicable in our case because it requires the inner function (SEARCH) to be Boolean!
- We proved a new composition theorem using similar techniques; in particular the quantum eavesdropping effort is in:

$$\Omega(\underbrace{N^{2/3}}_{\text{XOR}} \cdot \underbrace{N}_{\text{SEARCH}}) = \Omega(N^{5/3})$$

Lower Bound Proof Sketch (...)

✓ 1. We defined a search problem related to the XOR problem;

✓ 2. We proved $\Omega(N^{5/3})$ lower bound for this search problem; and

3. We reduced an equivalent (randomized) search problem to the eavesdropping strategy against our protocol.

Short of time, we have to skip step 3.

Our Second Contribution

Question (more challenging!)

Can every key exchange protocol in the random oracle model be broken in $O(N)$ quantum queries when legitimate parties are classical?

No!!!

We devised a classical protocol and proved its security of

$$\Theta(N^{7/6})$$

Classical Protocol Secure Against a Quantum Adversary [2nd Contr.]

Alice

X	Y
x_1	$f(x_1)$
$\vdots$	$\vdots$
x_i	$f(x_i)$
$\vdots$	$\vdots$
x_N	$f(x_N)$

$$x \rightarrow \boxed{N^2} \rightarrow f(x)$$

$$x \rightarrow \boxed{N^2} \rightarrow t(x)$$

$$\xrightarrow{f(x_1), \ldots, f(x_i), \ldots, f(x_N)}$$

Bob

Find two elements of X.

Achieved in $O(N)$ queries, based on the birthday paradox.

$$\downarrow$$
$$(s, s')$$

Classical Protocol Secure Against a Quantum Adversary [2nd Contr.]

Alice

$x \downarrow$ $\boxed{N^2}$ $\downarrow f(x)$

$x \downarrow$ $\boxed{N^2}$ $\downarrow t(x)$

Bob

X	Y	Z
x_1	$f(x_1)$	$t(x_1)$
$\vdots$	$\vdots$	$\vdots$
x_i	$f(x_i)$	$t(x_i)$
$\vdots$	$\vdots$	$\vdots$
x_N	$f(x_N)$	$t(x_N)$

$\xrightarrow{f(x_1), \ldots, f(x_i), \ldots, f(x_N)}$

Find two elements of X.

Achieved in $O(N)$ queries, based on the birthday paradox.

$\xleftarrow{w = t(s) \oplus t(s')}$

Given w, use table and bitwise XOR to find the secret.

$\downarrow$

(s, s')

Quantum eavesdropper finds the secret in $\Theta(N^{7/6})$ queries.
(Same attack and lower bound techniques)

$\downarrow$

(s, s')

Conclusion, Conjectures and Open Questions

	Alice/Bob	**Quantum** Eve
Merkle's	Classical	$\Theta(N)$
Our classical protocol		$\Theta(N^{7/6})$
Brassard & Salvail's	Quantum	$\Theta(N^{3/2})$
Our quantum protocol		$\Theta(N^{5/3})$

Classical Eve needs $\Theta(N^2)$

Compared to our two protocols on http://arxiv.org/abs/1108.2316

- This classical protocol improves over the $\Theta(N^{13/12})$ protocol.
- This quantum protocol is new, but with the same security.

Bonus...

We proved a new composition theorem for quantum query complexity.

Conclusion, Conjectures and Open Questions (...)

First open question

Are our two protocols optimal?

We conjecture they are not!

- We discovered a sequence of quantum protocols in which our most efficient quantum attack against the k^{th} protocol requires a number of queriers in

$$\Omega\left(N^{1+\frac{k}{k+1}}\right)$$

- We discovered a sequence of classical protocols in which our most efficient quantum attack against the k^{th} protocol requires a number of queriers in

$$\Omega\left(N^{\frac{1}{2}+\frac{k}{k+1}}\right)$$

Are these attacks optimal?

Conclusion, Conjectures and Open Questions (...)

Other open questions

1. Is there a quantum protocol that exactly achieves quadratic security?
2. Is there a quantum protocol that achieves better than quadratic security?!!!
3. What is the optimal classical protocol?

Thanks!