Key Distribution
and
Oblivious Transfer
à la Merkle

Gilles Brassard, Louis Salvail, Alain Tapp
Université de Montréal

QIP 2009, Santa Fe, 16 January 2009

Ralph Merkle

http://merkle.com/1974

- In the Fall of 1974 I enrolled in CS244, the Computer Security course offered at UC Berkeley and taught by Lance Hoffman.
- I submitted a proposal for what is now known as Public Key Cryptography -- which Hoffman rejected.
- I dropped the course, but kept working on the idea.

Project 2 looks more reasonable, maybe because your description of Project 1 is muddled terribly. Talk to me about these today.

C.S. 244
FALL 1974

Ralph Merkle

Project Proposal

Topic: Establishing secure communications between seperate secure sites over insecure communication lines.

Assumptions: No prior arrangements have been made between the two sites, and it is assumed that any information known at either site is known to the enemy. The sites, however, are now secure, and any new information will not be divulged.

Method 1: Guessing. Both sites guess at keywords. These guesses are one-way encrypted, and transmitted to the other site. If both sites should chance to guess at the same keyword, this fact will be discovered when the encrypted versions are compared, and this keyword will then be used to establish a communications link.

Discussion: No, I am not joking. If the keyword space is of size N, then the probability that both sites will guess at a common keyword rapidly approaches one after the number of guesses exceeds sqrt(N). Anyone listening in on the line must examine all N possibilities. In more concrete terms, if the two sites can process 1000 guesses per second, and desire to establish a link in roughly 10 seconds, then they can use a keword space of size $N=10{,}000^2=10^8$. If the enemy is presumed to have a comprable technology, i.e., 1000 guesses/sec, then he can consider all 10^8 possibilities in $10^8/10^3$ seconds, or 10^5 seconds, which is about one day. As the

It's getting there, but not good enough yet — see comments

Project Proposal

Method 1: Guessing. Both sites guess at keywords. These guesses are one-way encrypted, and transmitted to the other site. If both sites should chance to guess at the same keyword, this fact will be discovered when the encrypted versions are compared, and this keyword will then be used to establish a communications link.

Discussion: No, I am not joking.

$$f : \{1,2,\ldots N\} \rightarrow \{1,2,\ldots N\}$$

Random black-box permutation

$$f : \{1,2,\ldots N\} \to \{1,2,\ldots N\}$$

Alice		Bob
$f(x_1)$		$f(z_1)$
$f(x_2)$	$\Longrightarrow$	$f(z_2)$
$f(x_3)$		$\vdots$
$\vdots$	$\Longleftarrow$	$f(z_i)$
$f(x_t)$		

Shared secret key is $x_3 = z_i$

If $t = N^{1/2}$ then $i \approx N^{1/2}$: legitimate work $\approx t$

Classical eavesdropper's work $\approx N/2 \approx t^2$

Is this any good in practice?

- Assume Alice and Bob are willing to spend one second each.
- It takes one millisecond to compute *f*.
- Eve's expected effort: roughly 8 minutes.
- *Not great!*

Is this any good in practice?

- Assume Alice and Bob are willing to spend one second each.
- It takes one microsecond to compute *f*.
- Eve's expected effort: almost 6 days.
- *Better!*

Is this any good in practice?

- Assume Alice and Bob are willing to spend one second each.
- It takes one nanosecond to compute *f*.
- Eve's expected effort: over 15 years.
- *Wow!*

$$f : \{1,2,\ldots N\} \to \{1,2,\ldots N\}$$

Alice	Bob
$f(x_1)$	$f(z_1)$
$f(x_2)$ $\Longrightarrow$	$f(z_2)$
$f(x_3)$	$\vdots$
$\vdots$ $\Longleftarrow$	$f(z_i)$
$f(x_t)$

Shared secret key is $x_3 = z_i$

If $t = N^{1/2}$ then $i \approx N^{1/2}$: legitimate work $\approx t$

Classical eavesdropper's work $\approx N/2 \approx t^2$

Can we do better than quadratic eavesdropping effort?

NO!

Merkle Puzzles are Optimal

Boaz Barak[*] Mohammad Mahmoody-Ghidary[†]

February 5, 2008

Abstract

We prove that every key exchange protocol in the random oracle model in which the honest users make at most n queries to the oracle can be broken by an adversary making $O(n^2)$ queries to the oracle. This improves on the previous $\tilde{\Omega}(n^6)$ query attack given by Impagliazzo and Rudich (STOC' 89). Our bound is optimal up to a constant factor since Merkle (CACM '78) gave an n query key exchange protocol in this model that cannot be broken by an adversary making $o(n^2)$ queries.

Our result extends to an $O(n^2)$ query attack in the random permutation model, improving on the pervious $\tilde{\Omega}(n^{12})$ attack of Impagliazzo and Rudich. This bound again is optimal up to a constant factor since Merkle's protocol can be adapted to this model as well.

Can we do better
than quadratic
eavesdropping effort?
NO!
How about in a
quantum world?

$$f : \{1,2,\ldots N\} \rightarrow \{1,2,\ldots N\}$$

Alice	Bob
$f(x_1)$	$f(z_1)$
$f(x_2)$	$f(z_2)$
$f(x_3)$	$\vdots$
$\vdots$	$f(z_i)$
$f(x_t)$	

COMPLETE QUANTUM BREAK!

Shared secret key is $x_3 = z_i$

If $t = N^{1/2}$ then $i \approx N^{1/2}$: legitimate work $\approx t$

Quantum eavesdropper's work $\approx N^{1/2} \approx t$ (Grover)

$$f : \{1,2,\ldots N\} \rightarrow \{1,2,\ldots N\}$$

Alice		Bob
$f(x_1)$		$f(z_1)$
$f(x_2)$	$\Longrightarrow$	$f(z_2)$
$f(x_3)$		$\vdots$
$\vdots$	$\Longleftarrow$	$f(z_i)$
$f(x_t)$		

CAN IT BE REPAIRED?

Shared secret key is $x_3 = z_i$

If $t = N^{1/2}$ then $i \approx N^{1/2}$: legitimate work $\approx t$

Quantum eavesdropper's work $\approx N^{1/2} \approx t$ (Grover)

$$f : \{1,2,\ldots N\} \rightarrow \{1,2,\ldots N\}$$

Alice | **Bob**

$f(x_1)$

$f(x_2)$

$f(x_3)$

$\vdots$

$f(x_t)$

$\Longrightarrow$

$Z = \{f(x_i) \mid 1 \leq i \leq t\}$

$g : \{1,2,\ldots N\} \rightarrow \{0,1\}$

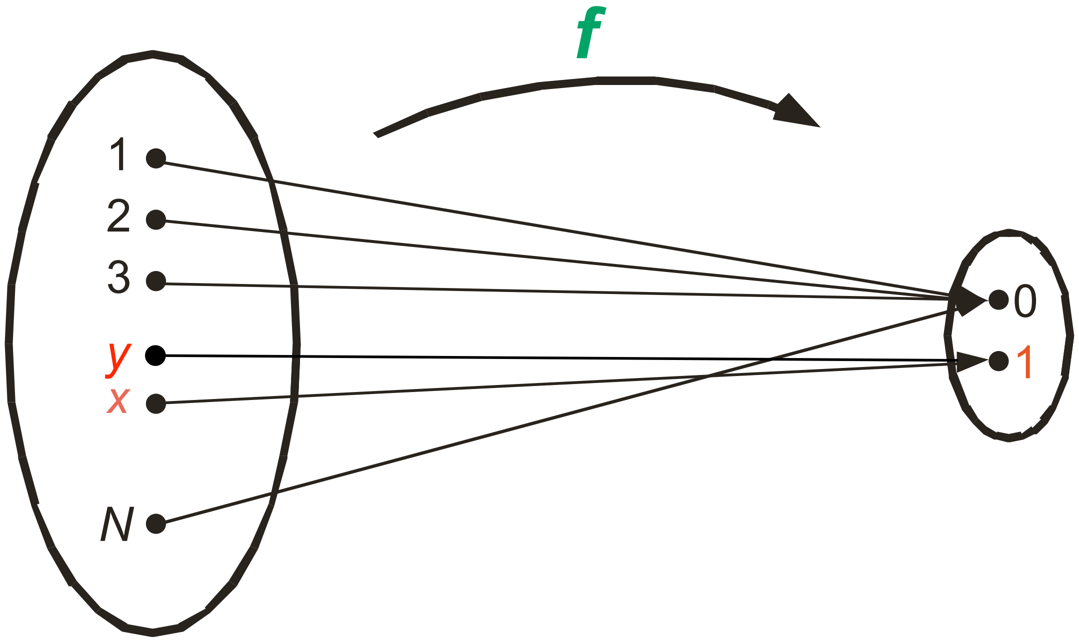
$g(z) = 1 \Leftrightarrow f(z) \in Z$

Grover search for z such that $g(z) = 1$

$\Longleftarrow$ $f(z)$

Shared secret key is z

Grover's Algorithm



Problem: find some x such that $f(x)=1$

Best Classical Algorithm: $\approx N/(t+1)$ queries

Grover's Algorithm: $\approx \sqrt{N/t}$ queries

if there are t solutions

Time needed for Grover

- There are $\#Z = t$ solutions
- Grover makes $\approx (N / t)^{1/2}$ queries
- If $t = N^{1/3}$, this is

$$(N / N^{1/3})^{1/2} = (N^{2/3})^{1/2} = N^{1/3} = t \text{ queries}$$

$$f : \{1,2,\ldots N\} \to \{1,2,\ldots N\}$$

Alice | **Bob**

$f(x_1)$

$f(x_2)$

$f(x_3)$

$\vdots$

$f(x_t)$

$\Longrightarrow$

$Z = \{f(x_i) \mid 1 \le i \le t\}$

$g : \{1,2,\ldots N\} \to \{0,1\}$

$g(z) = 1 \Leftrightarrow f(z) \in Z$

Grover search for z *such that* $g(z) = 1$

$\Longleftarrow$ $f(z)$

Shared secret key is z

If $t = N^{1/3}$ then legitimate work $\approx t$

Quantum eavesdropper's work $\approx N^{1/2} \approx t^{3/2}$

Summary for Key Distribution

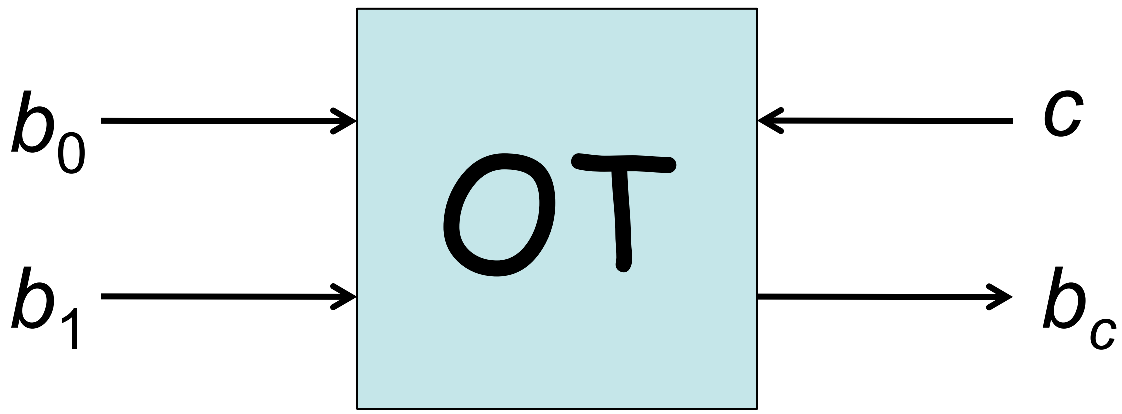
- Legitimate effort ≈ t
- Eavesdropping effort:

		Eavesdropper	
		Classical	Quantum
Alice & Bob	Classical	t^2	t
	Quantum	t^3	$t^{3/2}$

Oblivious Transfer

Alice

Bob



c ?

$b_{1\text{-}c}$?

Oblivious Transfer

- Powerful cryptographic primitive
- Invented by Stephen Wiesner (1970)
- Unconditional security impossible (even quantum mechanically)
- Computational security possible?

YES!

at least polynomially

(assuming one-way permutations)

$$f:\{1,2,\ldots N\}\rightarrow\{1,2,\ldots N\}$$

Alice

Bob

$$\begin{array}{cc} f(x_1) & f(y_1) \\ f(x_2) & f(y_2) \\ f(x_3) & f(y_3) \\ \vdots & \vdots \\ f(x_t) & f(y_t) \end{array} \quad \Longrightarrow \quad \begin{array}{c} f(z_1) \\ f(z_2) \\ \vdots \\ f(z_i) \end{array}$$

$c=0$

$$f : \{1,2,\ldots N\} \to \{1,2,\ldots N\}$$

Alice

Bob

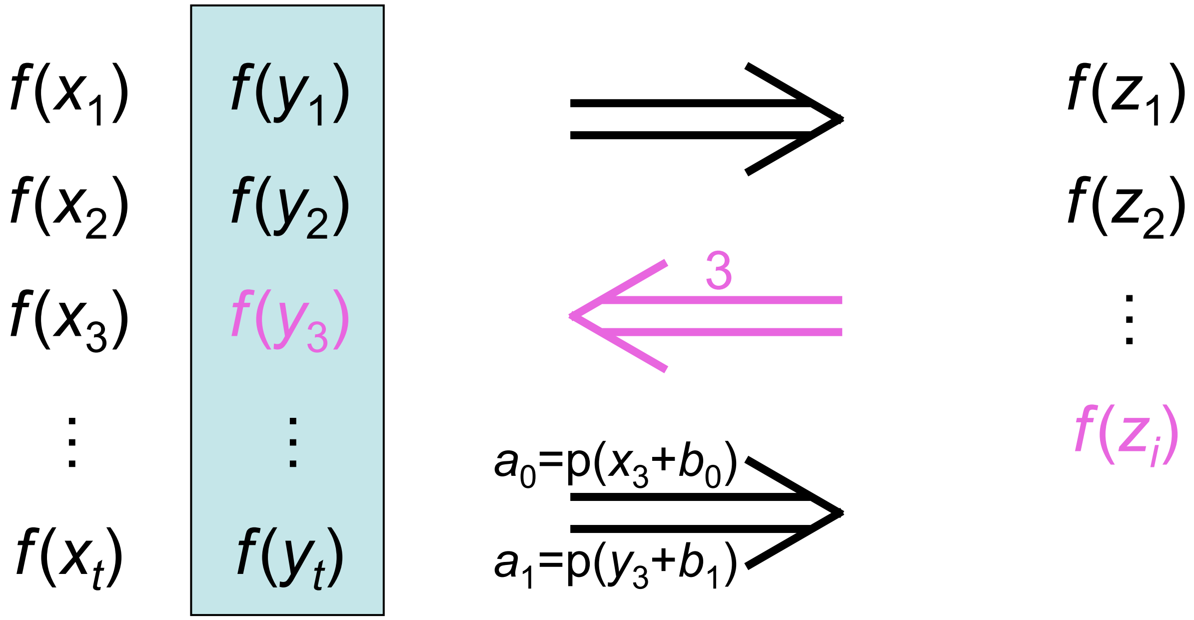
$$\begin{array}{cc} f(x_1) & \boxed{\begin{array}{c} f(y_1) \\ f(y_2) \\ f(y_3) \\ \vdots \\ f(y_t) \end{array}} \\ f(x_2) & \\ f(x_3) & \\ \vdots & \\ f(x_t) & \end{array} \quad \Longrightarrow \quad \begin{array}{c} f(z_1) \\ f(z_2) \\ \vdots \\ f(z_i) \end{array}$$

$c=1$

$$f : \{1,2,\ldots N\} \rightarrow \{1,2,\ldots N\}$$

Alice

Bob



Bob Computes parity$(a_c+z_i) = b_c$

If $t = N^{1/2}$ then $i \approx N^{1/2}$: legitimate work $\approx t$

$$f : \{1,2,\ldots N\} \to \{1,2,\ldots N\}$$

Alice **Bob**

$f(x_1)$ $f(y_1)$ $f(z_1)$

$f(x_2)$ $f(y_2)$ $f(z_2)$

$\boxed{f(x_3) \quad f(y_3)}$ 3 $\vdots$

$\vdots$ $\vdots$ $f(z_i)$

$a_0 = \mathrm{p}(x_3 + b_0)$

$a_1 = \mathrm{p}(y_3 + b_1)$ $\vdots$

$f(x_t)$ $f(y_t)$ $f(z_j)$

Bob Computes $\mathrm{parity}(a_0 + z_j) = b_0$ and $\mathrm{parity}(a_1 + z_i) = b_1$

If $t = N^{1/2}$ then $i \approx N^{1/2}$: legitimate work $\approx t$

Optimal classical *cheating* work $\approx t^{3/2}$

$$f : \{1,2,\ldots N\} \rightarrow \{1,2,\ldots N\}$$

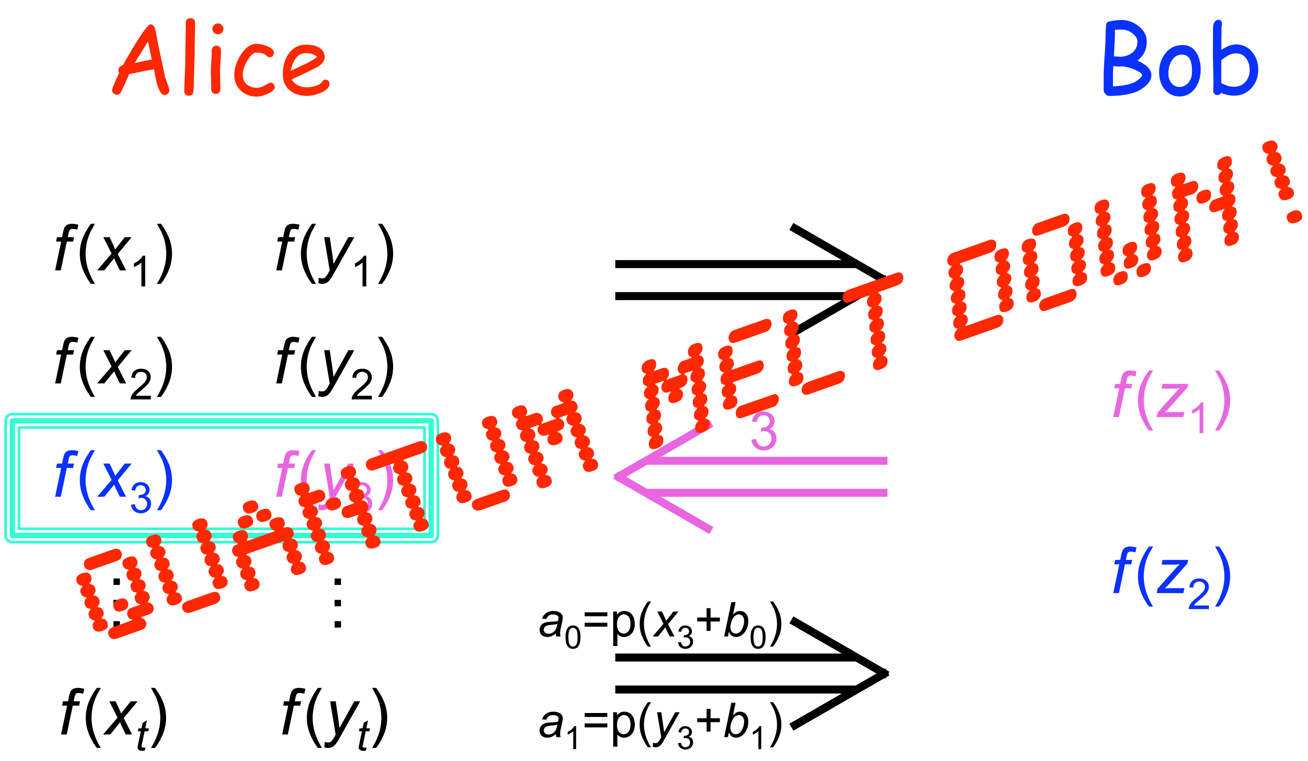
Alice			Bob
$f(x_1)$	$f(y_1)$	$\Longrightarrow$	
$f(x_2)$	$f(y_2)$		$f(z_1)$
$\boxed{f(x_3) \quad f(y_3)}$		$\xleftarrow{3}$	
$\vdots$	$\vdots$		$f(z_2)$
$f(x_t)$	$f(y_t)$	$\xRightarrow[a_1=\mathrm{p}(y_3+b_1)]{a_0=\mathrm{p}(x_3+b_0)}$	

Bob Computes parity$(a_0+z_2) = b_0$ and parity$(a_1+z_1) = b_1$

If $t = N^{1/2}$ then $i \approx N^{1/2}$: legitimate work $\approx t$

Obvious quantum *cheating* work $\approx N^{1/2} \approx t$ (Grover)

$$f : \{1,2,\ldots N\} \rightarrow \{1,2,\ldots N\}$$

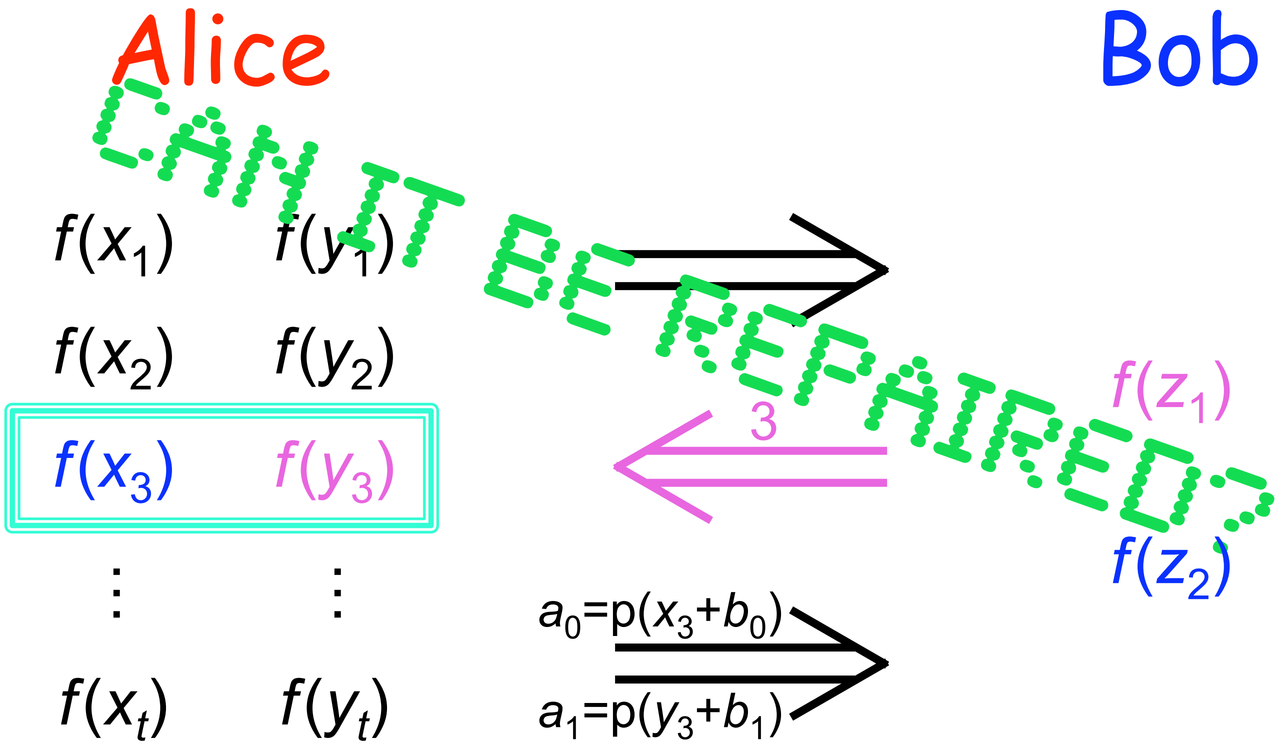


Bob Computes $\mathrm{parity}(a_0 + z_2) = b_0$ and $\mathrm{parity}(a_1 + z_1) = b_1$

If $t = N^{1/2}$ then $i \approx N^{1/2}$: legitimate work $\approx t$

Better quantum *cheating* work $\approx t^{5/6}$

$$f : \{1,2,\ldots N\} \rightarrow \{1,2,\ldots N\}$$



Bob Computes parity$(a_0 + z_2) = b_0$ and parity$(a_1 + z_1) = b_1$

If $t = N^{1/2}$ then $i \approx N^{1/2}$: legitimate work $\approx t$

Better quantum *cheating* work $\approx t^{5/6}$

$$f : \{1,2,\ldots N\} \rightarrow \{1,2,\ldots N\}$$

Alice **Bob**

$f(x_1)$	$f(y_1)$
$f(x_2)$	$f(y_2)$
$f(x_3)$	$f(y_3)$
$\vdots$	$\vdots$
$f(x_t)$	$f(y_t)$

$i=3$

$a_0=\mathrm{p}(x_i+b_0)$

$a_1=\mathrm{p}(y_i+b_1)$

Grover search for z such that $\exists i$ s.t $f(z) = f(y_i)$

Bob Computes parity$(a_c+z) = b_c$

If $t = N^{1/3}$ then legitimate work $\approx (N/t)^{1/2} \approx N^{1/3} \approx t$

$$f : \{1,2,\ldots N\} \rightarrow \{1,2,\ldots N\}$$

Alice | **Bob**

$f(x_1)$ $f(y_1)$ $\Longrightarrow$

$f(x_2)$ $f(y_2)$

$\boxed{f(x_3) \quad f(y_3)}$ $\xleftarrow{i=3}$

Quantum search for i, z_1 & z_2 such that $f(z_1) = f(y_i)$ & $f(z_2) = f(x_i)$

$\vdots$ $\vdots$

$f(x_t)$ $f(y_t)$ $\Longrightarrow$ $a_0 = \mathrm{p}(x_i + b_0)$, $a_1 = \mathrm{p}(y_i + b_1)$

Bob Computes $\mathrm{parity}(a_0 + z_2) = b_0$ and $\mathrm{parity}(a_1 + z_1) = b_1$

If $t = N^{1/3}$ then legitimate work $\approx (N/t)^{1/2} \approx N^{1/3} \approx t$

Best *known* quantum cheating work $\approx t^{4/3}$

Summary for Oblivious Transfer

- Legitimate effort ≈ t
- Eavesdropping effort:

		Eavesdropper: Classical	Eavesdropper: Quantum
Alice & Bob	Classical	$t^{3/2}$	$t^{5/6}$
	Quantum	$t^{5/2}$	$t^{4/3}$

Conclusion

- Classical channel between Alice and Bob.
- No prior entanglement.
- IS QUANTUM MECHANICS A HINDRANCE to classical-channel cryptography?
- What a contrast with *Quantum Cryptography* !

Summary for Key Distribution

- Legitimate effort ≈ t
- Eavesdropping effort:

		Eavesdropper: Classical	Eavesdropper: Quantum
Alice & Bob	Classical	t^2	
	Quantum		$t^{3/2}$

Fully Classical Versus Quantum Merkle

Summary for Oblivious Transfer

- Legitimate effort ≈ t
- Eavesdropping effort:

		Eavesdropper: Classical	Eavesdropper: Quantum
Alice & Bob	Classical	$t^{3/2}$	
	Quantum		$t^{4/3}$

Fully Classical Versus Quantum OT

Open Questions

- The classical t^2 bound is tight for key distribution. How about the quantum $t^{3/2}$?
- Is our $t^{4/3}$ quantum attack against our quantum OT protocol best possible?
- Does a better quantum OT protocol exist?
- Can we design fully classical protocols that remain polynomially secure against quantum attacks?

Thanks!

Questions?

CENTRE DE RECHERCHES MATHÉMATIQUES

Quantum Information Theme Semester

Fall of 2011

CENTRE DE RECHERCHES MATHÉMATIQUES

Bid to host QIP 2012… probably in December 2011

Recall: QIP 2000 was held in Montréal in December 1999, sponsored by CRM

Centre de recherches mathématiques

As part of the Theme Year 1999-2000

QIP 2000
Third Workshop on
Quantum Information Processing

6-11 December 1999

Organizers
Gilles Brassard (Universite de Montreal)
Richard Cleve (University of Calgary)