(4) two-party Cryptographic Protocols
BIT COMMITMENT

COMMIT

UNVEIL

b, 29 - 41 - 02 - 17
Oblivious Transfer (message multiplexing)

B₀ \quad 1/2-OT \quad Bₜ

B₁ \quad C
Oblivious Transfer

B₀ → 1/2-OT → B₁

B₀ → → B₁

B₁ → → B₀

© Claude Crépeau 2002-2005
Oblivious Transfer
Oblivious Function Evaluation

\[ f(x,y) \quad f,g \quad g(x,y) \]
Mutual Identification

x = y?

x = y?

x = y?

x = y?
Classically

Oblivious Transfer (message multiplexing)

B₀ → B_c

B₁

C

Trapdoor One-way Permutation

BIT COMMITMENT

COMMIT

UNVEIL

x → f(x, y)

y → g(x, y)

One-way Function

Oblivious Function Evaluation

f, g

Classically

One-way Function

Trapdoor One-way Permutation

Oblivious Transfer (message multiplexing)
Quantumly

Oblivious Transfer (message multiplexing)

B₀ → 1/2 × OT → Bₙ

B₁ → C

BIT COMMITMENT

COMMIT

UNVEIL

One-way Function

Oblivious Function Evaluation

x

f(x, y)

f, g

y

g(x, y)
Classically (information theoretical)

Folklore
Quantumly
(information theoretical)

Mayers, Lo-Chau
Non-Locality Box

\[ a \oplus b = x \ll y \]

C: \( 3/4 \)  
Q: \( \cos^2(\pi/8) \approx 85\% \)
Quantumly

Oblivious Transfer
(message multiplexing)

B₀ → ¹/₂-OT → Bₜ

B₁ → C

Woll, Wullschleger

BIT COMMITMENT

COMMIT

UNVEIL

b, 29 - 41 - 02 - 17

Non-Local Box

a ⊕ b = x ∧ y

1) Wolf, Wullschleger
2) Short, Gisin, Popescu
3) Buhrman, Christandl, Unger, Wehner, Winter
Quantum Oblivious Transfer
Oblivious Transfer (message multiplexing)

\[ B_0 \rightarrow 1/2-OT \rightarrow B_c \]

\[ B_1 \rightarrow 1/2-OT \rightarrow C \]
## q-OT

### Setup

- **A:** 0 1 1 0 0 1 0 0 1 1 0 1 0 0 0 1 1 1 0 1 1 0 0 0
- **B:** x x + + x + + + x + + x x x + + x + x + x +

### Round 1

- **A:** x + x + + + x x x + + + + x x x + + + + + x +
- **B:** 0 0 1 0 0 1 0 0 0 1 1 0 0 0 0 1 1 0 0 0

### Round 2

- **B:** 0 0 1 1 0 1 0 1 0 0 0
- **A:** 0 0 1 1 0 1 0 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 0 1

### Round 3

- **B:** 0 0 1 1 0 1 0 1 = 0
- **A:** 0 0 1 1 0 1 0 1 = 0

### Round 4

- **A:** 0 0 1 1 0 1 0 1
- **B:** b₀ = 0

---

**Crépeau-Kilian**
\( Q\text{-OT} \)

\[
A: \begin{array}{cccccccccccccccc}
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\
\times & + & + & + & + & \times & \times & \times & + & + & + & \times & \times & \times & + & + & + & + & \times & + \\
\end{array}
\]

\( b_0, b_1 \)
Q-OT

\[ b_0, b_1 \]

\[
\begin{align*}
A: & \quad 0 1 1 0 0 1 0 0 1 1 0 1 0 0 0 1 1 1 0 1 1 0 0 0 \\
& \quad \times + \times + + + \times \times \times + + + + \times \times \times + + + + \times + \\
B: & \quad \times \times + + \times + + + \times + + \times \times \times + \times \times \times + + \times + + \times + \\
& \quad 0 0 1 0 0 1 0 0 1 0 0 0 0 1 1 1 0 0 0 1 1 0 0 0
\end{align*}
\]
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| B: | × | × | + | + | × | + | + | × | + | + | × | × | × | + | + | × | × | × | + | + | × | + |
|    | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| A: | × | + | × | + | + | × | × | × | + | + | + | × | × | × | + | + | + | + | + | × | + |
| B: | 0 | ☐ | ☐ | 0 | ☐ | 1 | ☐ | ☐ | 1 | ☐ | 0 | ☐ | ☐ | 1 | 0 | ☐ | ☐ | 1 | 0 | 0 | 0 |
Q-OT

A: 0 1 1 0 0 1 0 0 1 1 0 1 0 0 0 1 1 1 0 1 1 0 0 0

B: 0 0 1 1 0 1 0 1 0 0 0

A: 0 0 1 1 0 1 0 1 0 0 0 1 1 0 0 0 1 0 1 1 0 0 0 1 0 1
Oblivious Transfer

C \rightarrow \frac{1}{2}OT \leftarrow C

\rightarrow Bc

C

© Claude Crépeau 2002-2005
\[
\begin{array}{cccccccc}
B: & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
A: & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
B: & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
A: & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
\end{array}
\]
q-OT

B: 0 0 1 1 0 1 0 1 = 0  
A: 0 0 1 1 0 1 0 1 = 0

B: b_0 = 0

A: b_0 = 0

B: b_1 = 0

A: b_1 = 0
Oblivious Transfer

\[ B_0 \quad \rightarrow \quad 1/2-OT \quad \leftarrow \quad B_1 \]

\[ B_0 \quad \rightarrow \quad B_0 \]

\[ B_1 \quad \rightarrow \quad B_1 \]
### Q-OT

#### A: 0 1 1 0 0 1 0 0 1 1 0 1 0 0 0 1 1 1 0 1 1 0 0 0

\[ \times + \times + + + \times \times \times \times + + + + \times \times \times + + + + + \times + + \]

#### B: 0 1 1 0 0 1 0 0 1 1 0 1 0 0 0 1 1 0 1 1 0 0 0

\[ \times + \times + + + \times \times \times \times + + + + \times \times \times + + + + + \times + + \]

\[ \therefore \quad \begin{array}{c}
A: \\
B: 0 0 1 1 0 1 0 1 = 0 \quad 0 = 1 1 0 0 0 1 0 1 \\
A: 0 0 1 1 0 1 0 1 = 0 \quad 0 = 1 1 0 0 0 1 0 1 \\
\end{array}
\]

\[ \begin{array}{c}
A: \\
B: b_0 \quad b_1 \\
\oplus \quad \oplus \\
0 \quad 0 = b_1
\end{array}
\]
Oblivious Transfer

B_0 \rightarrow 1/2-OT \rightarrow B_1

B_0 \leftarrow \rightarrow B_1
**Q-OT**

*from Q-BC*

| A: | 0 1 1 0 0 1 0 0 1 1 0 1 0 0 0 1 1 1 0 1 1 0 0 0 |
| B: | × × + + × + + × + × × × + × × + × + + + |

| A: | 0 0 1 0 0 1 0 0 1 0 0 0 0 1 1 1 0 1 0 0 0 |
| B: | × × + + × + + × + × × × + × × + × + + + |

| A: | 1 0 1 1 1 1 1 0 0 1 1 1 0 0 0 1 1 1 0 0 0 |
| B: | × + + + × × + + + × + + + + + |

| A: | × × + × × + + + × × + + + × |
| B: | × + + × + + + + + × + + + 0 0 0 |
Q-OT
from Q-BC

A: 0 1 1 0 0 1 0 0 1 1 0 1 0 0 0 1 1 1 0 1 1 0 0 0
   x + x + + + x x x x + + + x x x + + + x +

B: x x + + x + + + x + + x x x + x x x + + x + x + +
   0 0 1 0 0 1 0 0 1 0 0 0 0 1 1 1 0 0 0 1 1 0 0 0
Q-OT

from Q-BC

B: \[\times \times + + \times + + + \times + + \times \times \times + \times \times \times + + \times + + \times +\]

0 0 1 0 0 1 0 0 1 0 0 0 0 1 1 1 0 0 0 1 1 0 0 0

A: 

© Claude Crépeau 2002-2005
**Q-OT**

from **Q-BC**

<table>
<thead>
<tr>
<th>A:</th>
<th>B:</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>b₀</td>
<td>×₀</td>
<td>+₀</td>
<td>+₁</td>
<td>×₁</td>
<td>+₁</td>
<td>×₀</td>
<td>×₀</td>
<td>×₁</td>
<td>×₀</td>
<td>×₀</td>
<td>×₁</td>
</tr>
</tbody>
</table>
Q-OT

from Q-BC

A:  ×  ×  +  ×  ×  +  ×  ×  +  ×  ×  +  ×  ×  +  ×  ×  +  ×  ×  +  ×  ×  +

B:  ×  +  ×  +  +  +  +  ×  +  +  +  +  ×  +  +  ×  +  +  ×  +  +  ×  +  +
two provers
Cryptographic Protocols
Classically

BGKW88
Classically

Ben-Or, Goldwasser, Kilian, Wigderson
\[ z = x \quad \text{if } b = 0 \]
\[ z = x \oplus y \quad \text{if } b = 1 \]
\[ x_0 \oplus z = 0 \cdot y = 0 \]
\[ x_1 \oplus z = 1 \cdot y = y \]
\[ x_0 \oplus x_1 = (x_0 \oplus z) \oplus (x_1 \oplus z) = y \]

possible with prob. at most \(2^{-n}\)

Ben-Or, Goldwasser, Kilian, Wigderson
Classically

$$x \oplus z = b \cdot y$$

Ben-Or, Goldwasser, Kilian, Wigderson
Quantumly

or

???
two provers BC
Classically Secure
Quantumly Insecure

(7)
Quantumly

Ben-Or, Goldwasser, Kilian, Wigderson
\[ z = \begin{cases} \ x & \text{if } b = 0 \\ \ x \oplus y & \text{if } b = 1 \end{cases} \]

Ben-Or, Goldwasser, Kilian, Wigderson
Classically

\[ D_H(x \oplus z, b \cdot y) \approx 25\% n > n/5 \]

\[ D_H(x \oplus z, b \cdot y) < n/5? \]

Ben-Or, Goldwasser, Kilian, Wigderson
Quantumly

\[ \approx 85\% \implies D_H(x \oplus z, b \cdot y) \approx 15\% n < n/5 \]

\[ D_H(x \oplus z, b \cdot y) < n/5? \]

Ben-Or, Goldwasser, Kilian, Wigderson
Classically

\[ D_H(x_0 \oplus z, 0 \cdot y) = D_H(x_0 \oplus z, 0) < n/5 \]
\[ D_H(x_1 \oplus z, 1 \cdot y) = D_H(x_1 \oplus z, y) < n/5 \]
\[ D_H(x_0 \oplus x_1, y) = D_H((x_0 \oplus z) \oplus (x_1 \oplus z), y) < 2n/5 < n/2 \]
possible with prob. at most \( c^{-n} \)

75% \( \rightarrow D_H(x \oplus z, b \cdot y) \approx 25\% n > n/5 \)

Ben-Or, Goldwasser, Kilian, Wigderson
Quantumly

Ben-Or, Goldwasser, Kilian, Wigderson
(8)

two provers BC
Classically and
Quantumly Secure
\[ z = x \oplus r_b \]

modified BGKW
Classically

\[ x_0 \oplus z = r_0 \]
\[ x_1 \oplus z = r_1 \]
\[ x_0 \oplus x_1 = (x_0 \oplus z) \oplus (x_1 \oplus z) = r_0 \oplus r_1 \]

possible with prob. at most \(2^{-n}\)
Quantumly

modified BGKW
Quantumly

MAIN THEOREM

Let $Z$ and $O$ be POVMs such that outputs $x_0$ and $x_1$ one could obtain by applying one of them to the state shared among the two provers.

Suppose the success probability of unveiling is $p_0 + p_1 > 1 + \delta$, then the (prediction probability of $y_0 \oplus y_1$) > $\delta$.

This prediction probability is achieved by first applying $Z$ to the shared state followed by $O$ on the leftover system or the other way around.
Imagine that Peggy and Paula would like to be able to unveil a certain instance of $b$ both as 0 and as 1. Our only assumption is that Paula knows nothing about $r_0, r_1$. Let them share an unlimited quantity of entanglement in any form they wish. Without loss of generality to unveil a zero the message of Paula is defined by the outcome $w_0$ of a POVM $\mathcal{Z} = \{Z_1^+, Z_2^+, \cdots, Z_{2^n}^+\}$ and to unveil a 1 by the outcome $w_1$ of a POVM $\mathcal{O} = \{O_1^+, O_1, \cdots, O_{2^n}^+, O_{2^n}\}$.

Each operator in a POVM is a positive matrix and can thus be decomposed into a linear combination of orthogonal projectors with coefficients between 0 and 1.
Let $p_0$ be the probability of successfully unveiling 0 and $p_1$ be the probability of successfully unveiling 1. Suppose there exists a pair of POVMs where $p_0 + p_1 > 1$. We show that any quantum player can then obtain both classical strings $w_0, w_1$ to unveil both values with probability strictly greater than zero. Notice that if we manage to make the probability of getting both strings $w_0, w_1$ greater than $1/2^n$, then Paula can compute $r_0 \oplus r_1 = w_0 \oplus w_1$ better than at random. This implies communication between Peggy and Paula, which is impossible by hypothesis.
The strategy of Paula is simply to perform both measurements, one after the other. Let’s denote her state by $\rho$. Assume the right outcome for unveiling a zero is $w_0$ and the right outcome for unveiling a one is $w_1$.

The probability to obtain $w_0$ if $Z$ is measured is

$$p_0 = Tr(Z_{w_0}^\dagger Z_{w_0} \rho)$$

and the state becomes

$$Z_{w_0} \rho Z_{w_0}^\dagger / p_0.$$ 

The probability to obtain $w_1$ if $O$ is measured is

$$p_1 = Tr(O_{w_1}^\dagger O_{w_1} \rho)$$

and the state becomes

$$O_{w_1} \rho O_{w_1}^\dagger / p_1.$$
If $\mathcal{O}$ is measured after $Z$ the probability to obtain $w_0$ and $w_1$ is given by

$$p_{01} = p_0 Tr[O_{w_1}^\dagger O_{w_1} Z_{w_0} \rho Z_{w_0}^\dagger / p_0] = Tr[O_{w_1}^\dagger O_{w_1} Z_{w_0} \rho Z_{w_0}^\dagger]$$

If $Z$ is measured after $\mathcal{O}$ the probability to obtain $w_1$ and $w_0$ is given by

$$p_{10} = p_1 Tr[Z_{w_1}^\dagger Z_{w_1} O_{w_0} \rho O_{w_0}^\dagger / p_1] = Tr[Z_{w_1}^\dagger Z_{w_1} O_{w_0} \rho O_{w_0}^\dagger]$$

Both $p_{01}$ and $p_{10}$ must be smaller or equal to $1/2^n$ otherwise Paula learns something about $r_0 \oplus r_1 = w_0 \oplus w_1$ (which is impossible without communication).
Having all this in mind, consider the following sequence of implications:

\[ p_{01} + p_{10} \leq 1/2^{n-1} \]

\[ Tr[Z_{w_{1}} O_{w_{1}} Z_{w_{0}} O_{w_{0}} \rho O_{w_{0}}^{\dagger}] \leq 1/2^{n-1} \]

\[ Tr[(I - (I - O_{w_{1}}^{\dagger} O_{w_{1}})) Z_{w_{0}} \rho Z_{w_{0}}^{\dagger}] + Tr[(I - (I - Z_{w_{1}}^{\dagger} Z_{w_{1}})) Z_{w_{0}} \rho O_{w_{0}}^{\dagger}] \leq 1/2^{n-1} \]

\[ Tr[Z_{w_{0}} \rho Z_{w_{0}}^{\dagger}] - Tr[(I - O_{w_{1}}^{\dagger} O_{w_{1}}) Z_{w_{0}} \rho Z_{w_{0}}^{\dagger}] + \]

\[ Tr[Z_{w_{0}} \rho O_{w_{0}}^{\dagger}] - Tr[(I - Z_{w_{1}}^{\dagger} Z_{w_{1}}) O_{w_{0}} \rho O_{w_{0}}^{\dagger}] \leq 1/2^{n-1} \]

Using that \( p_{0} = Tr(Z_{w_{0}}^{\dagger} Z_{w_{0}} \rho) \) and \( p_{1} = Tr(O_{w_{1}}^{\dagger} O_{w_{1}} \rho) \) we get

\[ p_{0} + p_{1} \leq Tr[(I - O_{w_{1}}^{\dagger} O_{w_{1}}) Z_{w_{0}} \rho Z_{w_{0}}^{\dagger}] + Tr[(I - Z_{w_{1}}^{\dagger} Z_{w_{1}}) O_{w_{0}} \rho O_{w_{0}}^{\dagger}] + 1/2^{n-1} \]

\[ p_{0} + p_{1} \leq Tr[I - O_{w_{1}}^{\dagger} O_{w_{1}}] + Tr[I - Z_{w_{1}}^{\dagger} Z_{w_{1}}] + 1/2^{n-1} \]

\[ p_{0} + p_{1} \leq (1 - p_{0}) + (1 - p_{1}) + 1/2^{n-1} \]  
\[ 2(p_{0} + p_{1}) \leq 2 + 1/2^{n-1} \]

\[ p_{0} + p_{1} \leq 1 + 1/2^{n} \]
This last statement means that the probability of cheating the bit commitment scheme is only exponentially little better than in the honest case. This is the best we could hope for because this value is reached by Peggy-Paula acting nearly honestly: Peggy and Paula act honestly except that when Paula unveils if she wish to unveil the opposite bit to Peggy she sends a random string instead of $w$. With probability $1/2^n$ she succeeds in unveiling the opposite bit.
WARNING!

(9)
Oblivious Transfer
(message multiplexing)
Oblivious Transfer (message multiplexing)

Brassard, Crépeau, Mayers, Salvail 97
Mutual Identification

x = y?

y = x?

=,=
Mutual Identification

x = y?

SUCCESS!

y = x?
Mutual Identification

\[ x - y ? \quad =,= \quad x = y ? \]

FAILURE!
(10) Classical Multi-party Computing
Classical Multi-party Computing

- Network of $n$ players
- Each has input $x_i$
- Want to compute $f(x_1,\ldots,x_n)$ for some known function $f$
- E.g. electronic voting
Classical Multi-party Computing

Even if $t$ out of $n$ players try to cheat:

1. Cheaters learn nothing (except output)

2. Cheaters cannot affect output (except by choice of input)
Results

- Classical MPC (without broadcast)
- VSS (without broadcast)
- Classical MPC (with broadcast)
- VSS (with broadcast)

$t = \text{number of cheaters}$

$0 \leq t \leq n/2$

Impossible
(11) Multi-Party Quantum Computing
Multi-party **Quantum** Computing

- Players' inputs are quantum states
  - Possibly entangled
  - No description necessary (protocol is “oblivious”)
- Output is quantum
- Want to evaluate a known quantum circuit \( U \)
- Player \( i \) gets \( i \)-th component of output
Multi-party Quantum Computing

• Players' inputs form an arbitrary state
  \( \rho \) in \( H_1 \otimes H_2 \otimes \ldots \otimes H_n \)

• Player \( i \) holds \( i \)-th component:
  \( \rho_i \)

• Each player gets one output:
  \( \rho_i' = (U\rho U^\dagger)_i \)
Multi-party Quantum Computing

Even if \( t \) out of \( n \) players try to cheat:

1. Cheaters learn nothing (except output)
2. Cheaters cannot affect output (except by choice of inputs)
Results

- $t < n/6$: Any Multi-party Quantum Computation
- $t < n/4$: Verifiable Quantum Secret-Sharing
- $t \geq n/4$: Even (perfect) VQSS is impossible
Results

Classical MPC
(with broadcast)

Classical MPC
(without broadcast)

Verifiable Quantum Secret Sharing
(without broadcast)

Verifiable Quantum Secret Sharing
(with broadcast)

MPQC

$t = \text{number of cheaters}$

IMPOSSIBLE
MPQC and Fault-Tolerant Computing

- MPQC is like FTQC with a different error model...

<table>
<thead>
<tr>
<th></th>
<th>FTQC</th>
<th>MPQC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of errors</td>
<td>randomly spread, independent</td>
<td>maliciously placed, entangled with data</td>
</tr>
<tr>
<td>Error location</td>
<td>Can occur anywhere</td>
<td>At most $t$ positions</td>
</tr>
</tbody>
</table>

- Similar protocol techniques:
  Classical MPC [BGW, CCD] $\rightarrow$ FTQC [AB99] $\rightarrow$ MPQC [CGS]

- Different proof techniques
  (Need different notion of “proximity” to coding subspaces)