

Quantum Bit Commitment  
from any  
Quantum One-Way Permutation

Paul Dumais (Université de Montréal)

Dominic Mayers (NEC, Princeton)

Louis Salvail (Århus University, Denmark)

Paul Dumais, Dominic Mayers, Louis Salvail.

Perfectly Concealing Quantum Bit Commitment  
from any Quantum One-Way Permutation.

*Advances in Cryptology:*

**EUROCRYPT 2000: Proceedings,**

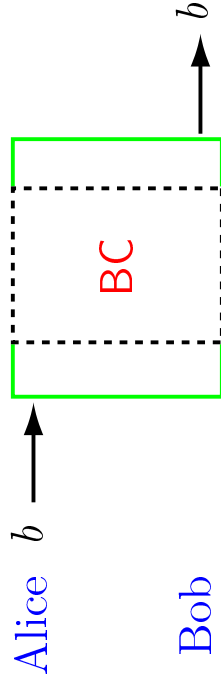
LNCS 1807, pages 300–315, Springer, Berlin, 2000.

## Quantum cryptography

Two trusting parties      Two mistrusting parties

<p>The adversary is a third party</p> <p>Secret key generation</p> <p>Unconditional security for both parties</p> <p>Information theory based</p>	<p>One of the two parties is the adversary</p> <p>Bit commitment</p> <p>Computational assumption needed for one of the parties</p> <p>Computationally based</p>
---	---

## Bit Commitment



Bit Commitment  
commit and unveil

Alice

$b$

$[b]$

Bob

$$b = Q([b], [b])$$

Bit Commitment  
breaking the binding condition

Alice

$\square$

$[0]$

$[1]$

Bob

$$0 = Q(\square, [0])$$

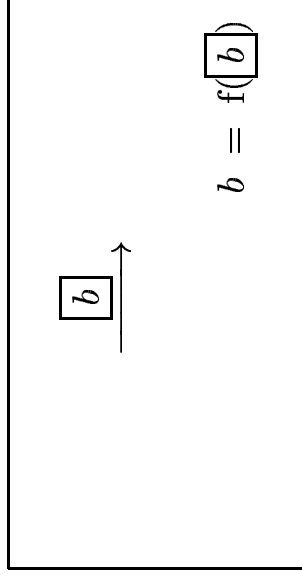
AND

$$1 = Q(\square, [1])$$

**Bit Commitment**  
breaking the **hiding** condition

Alice

Bob



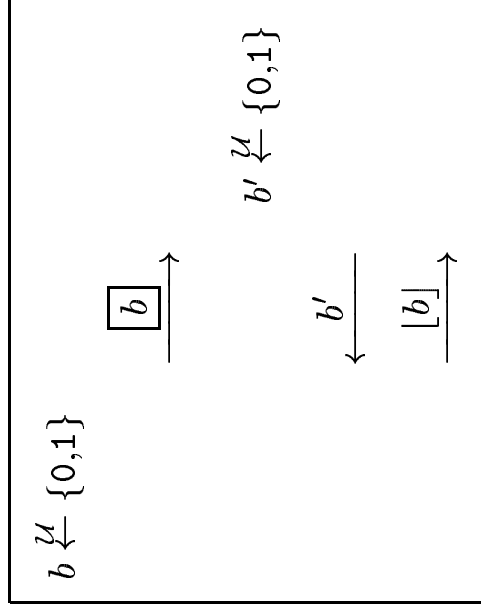
**Bit commitment is useful for...**

- Coin tossing
- Zero-knowledge proofs
- Multipartite computation
  - Voting schemes
  - Submission schemes
- ...

## Coin Toss from Bit Commitment

Alice

Bob



$$c \leftarrow b \oplus b'$$

Quantum bit commitment with unconditional security for both parties is impossible!

H. K. Lo, H. F. Chau.

Is Quantum Bit Commitment Really Possible?  
*Physical Review Letters*,  
vol. 78, no 17, April 1997, pages 3410–3413.

Dominic Mayers.

Unconditionally Secure Quantum Bit Commitment is Impossible.  
*Physical Review Letters*,  
vol. 78, no 17, April 1997, pages 3414–3417.

Quantum bit commitment (with conditional security) is still possible...

Physical assumptions (L. Salvail, 1998):

“Alice cannot perform generalized measurement over  $n$  qubits coherently”

Conditionally binding, unconditionally hiding.

Computational assumptions (this paper):

“Quantum one-way permutations exist.”

Conditionally binding, unconditionally hiding.

Noisy channel assumptions

Etc

One-Way Permutation

$$\pi_k : \{0,1\}^k \xrightarrow{\simeq} \{0,1\}^k$$

$$y \leftarrow \pi(x)$$

### One-Way Permutation

breaking the one-way condition

$$y \xleftarrow{\mathcal{U}} \{0,1\}^k$$

$$x \leftarrow \mathbf{I}(y)$$

$$y = \pi(x)$$

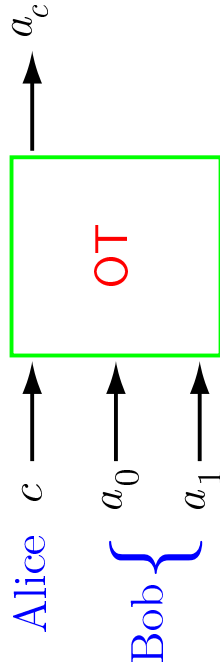
### One-way functions: classical candidates

- Number theory
  - Multiplication (*factoring is hard*)
  - RSA
  - Modular exponentiation (*discrete log is hard*)
  - ...
- Coding theory
- Lattices
- Subset-sum problem
- Elliptic curves
- Polynomials
- ...

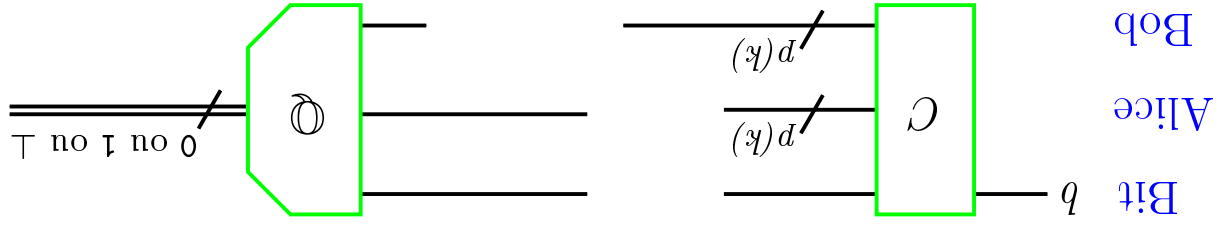
<b>Two trusting parties cryptography</b> (secret key generation)	
Classical	<p>Diffie-Hellmann Key Exchange (W. Diffie, M. E. Hellman, 1976)</p> <p>Computational assumption needed</p>
Quantum	<p>QKD (C. H. Bennett, G. Brassard, 1984)</p> <p>Unconditional security</p>

<b>Two mistrusting parties cryptography</b> (bit commitment)	
Classical	<p>Bit commitment (BC) need not be sufficient for oblivious transfer (OT).</p> <p>BC based on one-way permutations (<math>O(k)</math>) needs <math>O(k)</math> rounds of interaction (M. Naor, R. Ostrovsky, R. Venkatesan, M. Young, 1998).</p>
Quantum	<p>BC is sufficient for OT (C. Crépeau, 1994; A. C. Yao, 1995)</p> <p>BC based on quantum OWH do not need interaction (this paper).</p>

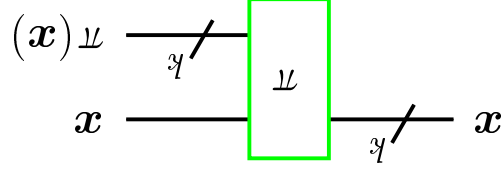
Oblivious Transfer



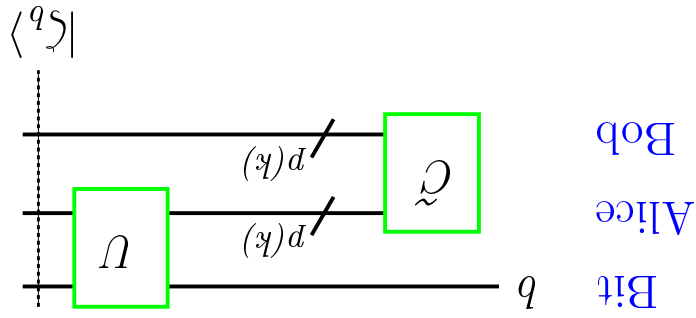
Quantum bit commitment: modelization



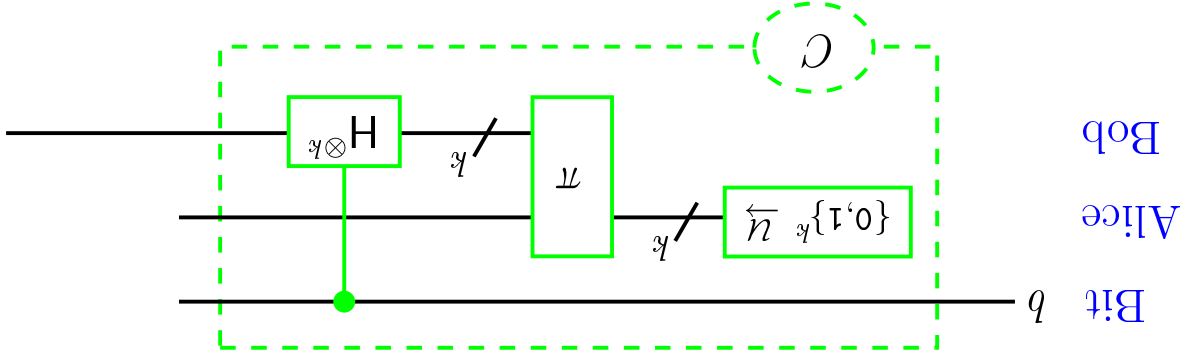
Quantum one-way permutation:  
modelization



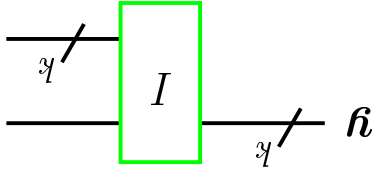
Breaking the binding condition  
of quantum bit commitment:  
modelization



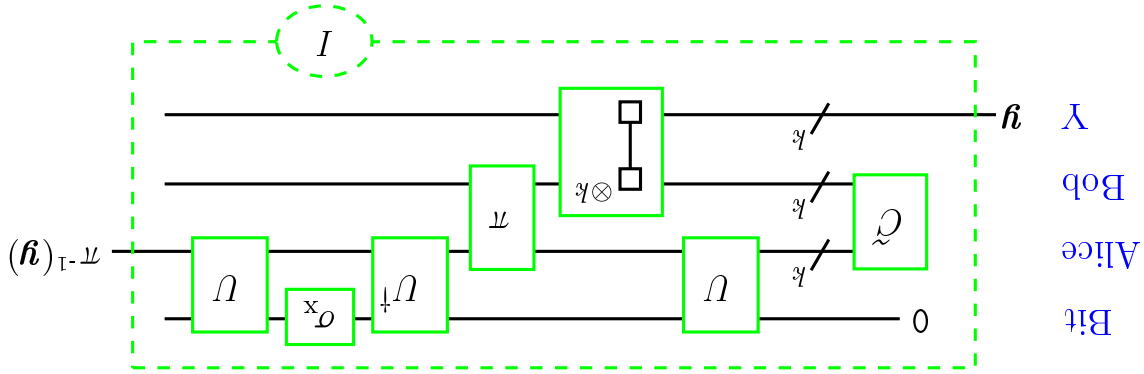
Quantum bit commitment from  
quantum one-way permutation



Breaking quantum one-way  
permutation: modelization



Adversary to quantum one-way permutation  
 from adversary to the binding condition of  
 quantum bit commitment



One-way permutations: quantum candidates

?

What other cryptographic reductions  
may be adapted to a quantum computer?

Computationally based quantum cryptography  
is a rich domain!