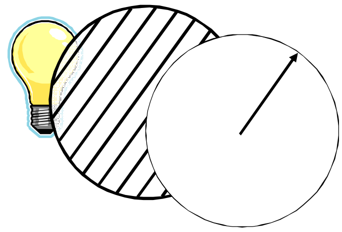
Secure Identification Using Quantum Communication

Serge Fehr, Christian Schaffner *(CWI Amsterdam, NL)*

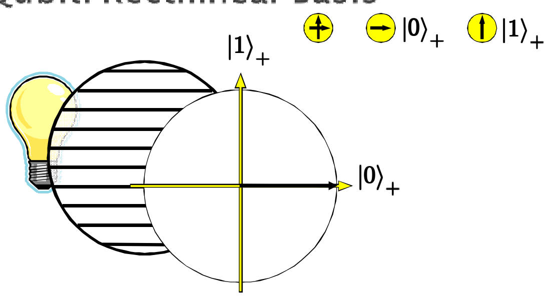
Ivan Damgård, Louis Salvail *(University of Århus, DK)*

Workshop: Practical Applications of New Research in Cryptography
Sabanci University, Turkey
Friday, April 18, 2008

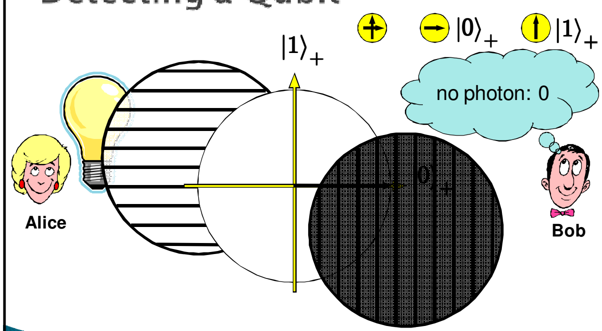
Quantum Bit: Polarization of a Photon



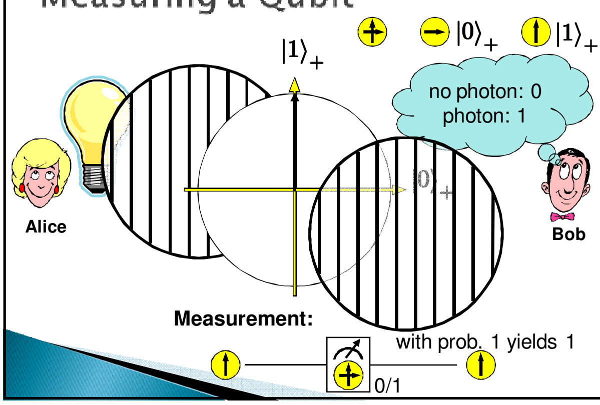
Qubit: Rectilinear Basis



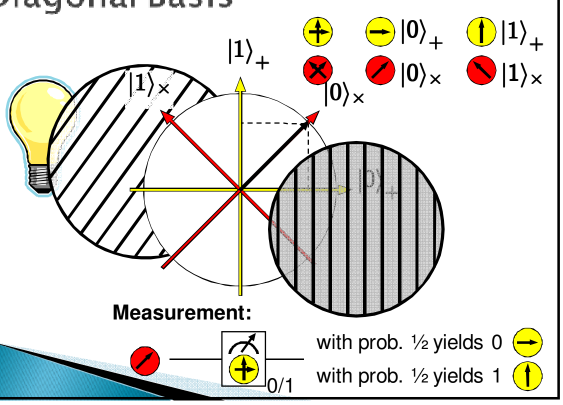
Detecting a Qubit



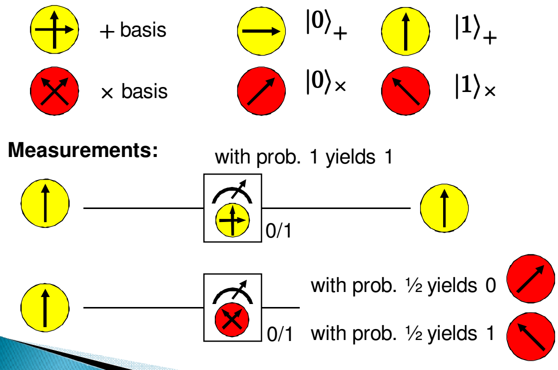
Measuring a Qubit



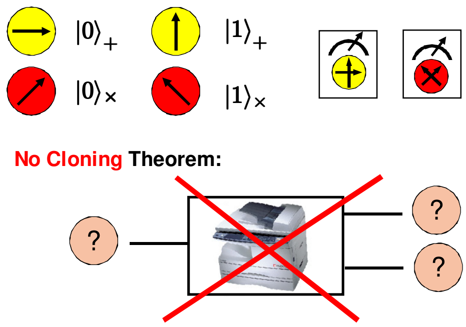
Diagonal Basis



Quantum Mechanics



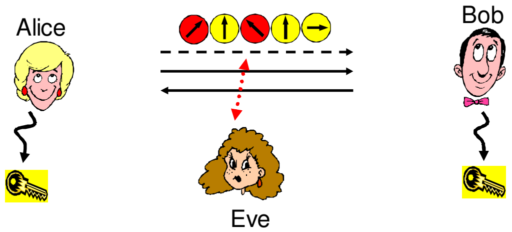
Non-Classical Properties



Outline

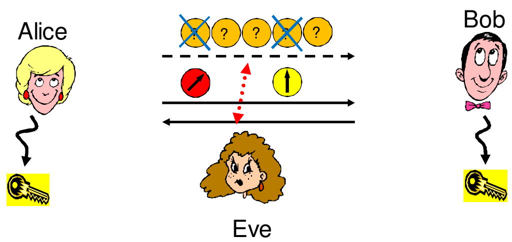
- ✓ Quantum Mechanics
- Quantum Key Distribution
- Two-Party Setting
- Secure Identification
- Conclusion

Quantum Key Distribution (QKD)



- most-studied in quantum cryptography
- 3-party scenario
- unconditional security against unrestricted eavesdroppers

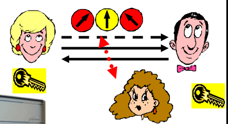
QKD: Intuition



- quantum states are unknown to Eve, cannot copy them
- honest players can check whether Eve interfered
- then amplify their advantage

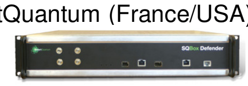
Commercial QKD-Products

- MagicQ (USA)



- idQuantique (Switzerland)

- SmartQuantum (France/USA)

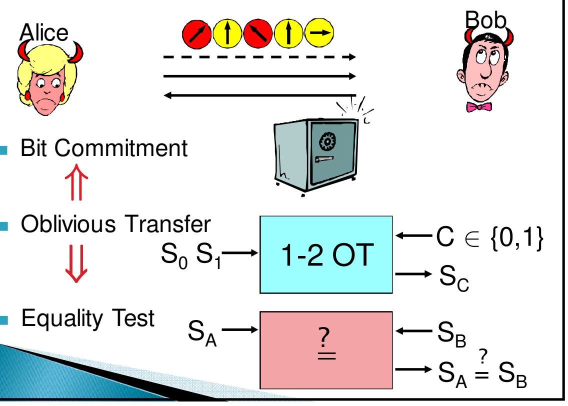


only quantum communication,
no quantum storage
nor quantum computation required

Outline

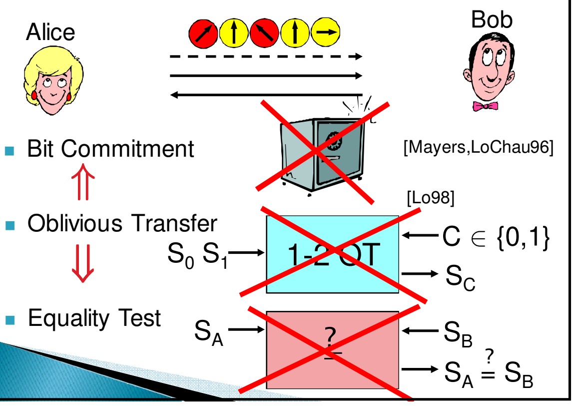
- ✓ Quantum Mechanics
- ✓ Quantum Key Distribution
- **Two-Party Setting**
- Secure Identification
- Conclusion

Two-Party Setting?



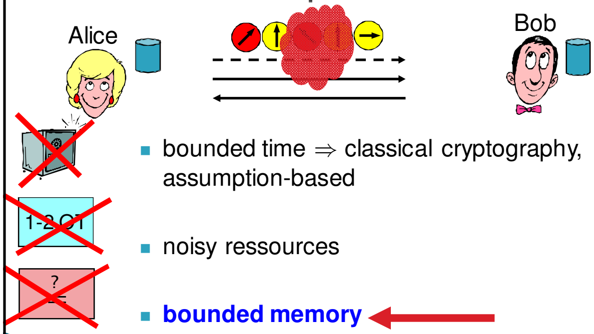
- Bit Commitment ⇑
- Oblivious Transfer ⇓
- Equality Test

Impossibility Results



- Bit Commitment ⇑
- Oblivious Transfer ⇓
- Equality Test

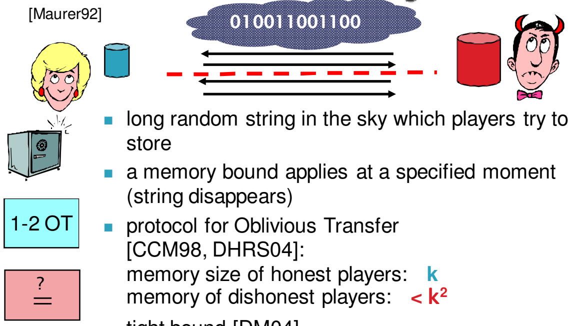
Possible Assumptions



- bounded time ⇒ classical cryptography, assumption-based
- noisy ressources
- **bounded memory**

Classical Bounded-Storage Model

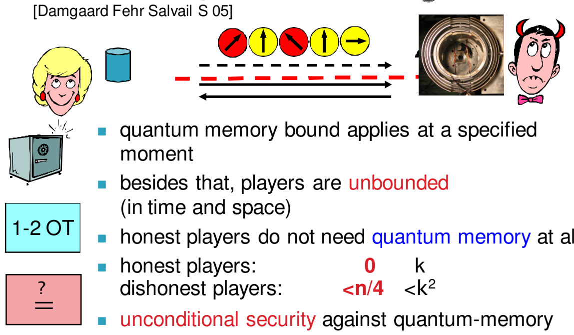
[Maurer92]



- long random string in the sky which players try to store
- a memory bound applies at a specified moment (string disappears)
- protocol for Oblivious Transfer [CCM98, DHRS04]:
  memory size of honest players: k
  memory of dishonest players: $< k^2$
- tight bound [DM04]

Bounded-Quantum-Storage Model

[Damgaard Fehr Salvail S 05]

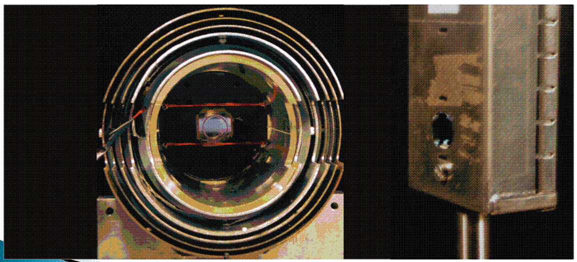


- quantum memory bound applies at a specified moment
- besides that, players are unbounded (in time and space)
- honest players do not need quantum memory at all
- honest players: 0 k
  dishonest players: $<n/4$ $<k^2$
- unconditional security against quantum-memory bounded adversaries

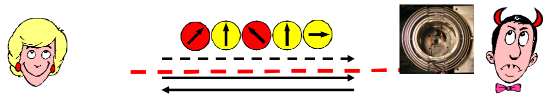
Quantum Memory

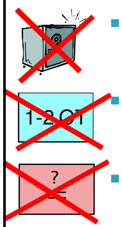
[physics group of Eugene Polzik, Copenhagen (DK)]

- 70% fidelity, few milliseconds, …
- technically very challenging



A Bit of History



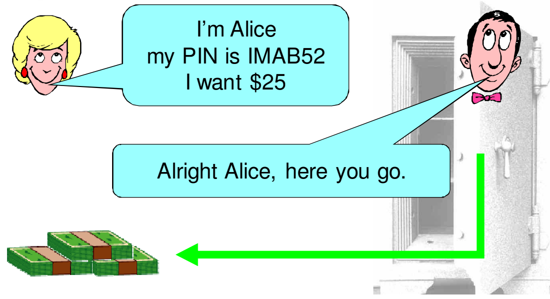


- [Damgaard Fehr Salvail S 05] Rabin-OT and Bit Commitment
- [Damgaard Fehr Renner Salvail S 07] 1-2 Oblivious Transfer
- [Damgaard Fehr Salvail S 07] Secure Identification

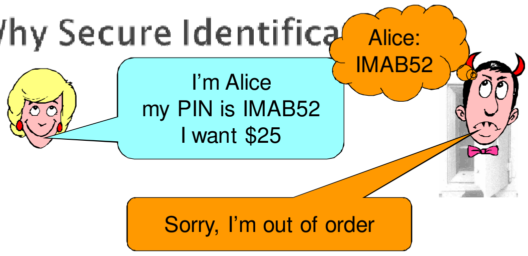
Outline

- ✓ Quantum Mechanics
- ✓ Quantum Key Distribution
- ✓ Two-Party Setting
- Secure Identification
- Conclusion

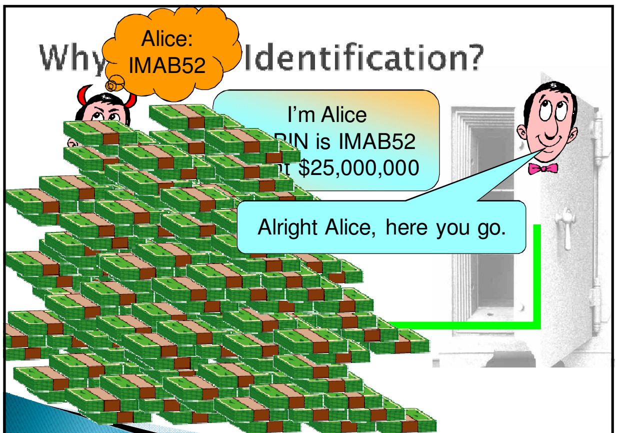
Why Secure Identification?

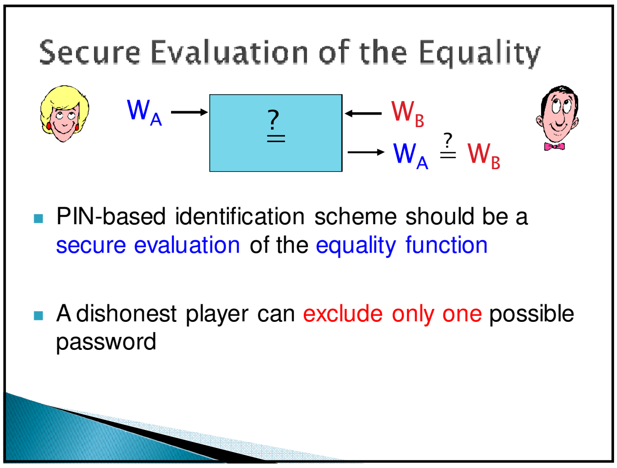


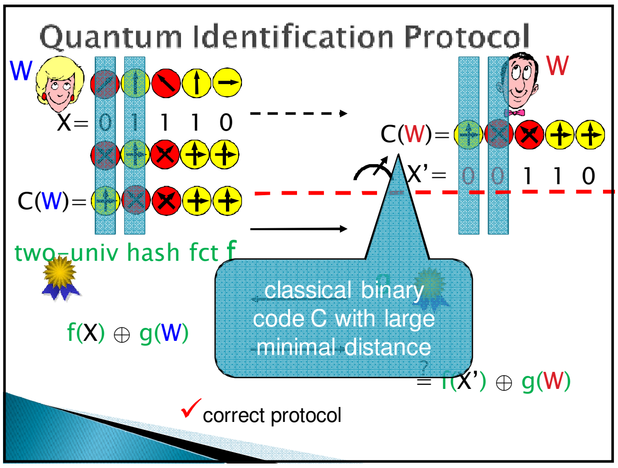
Why Secure Identification?

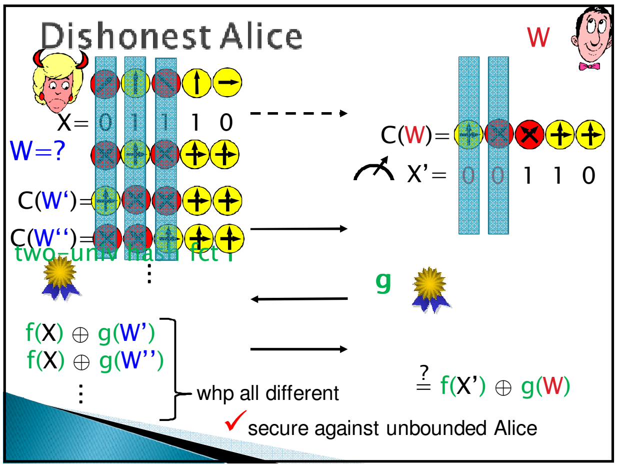


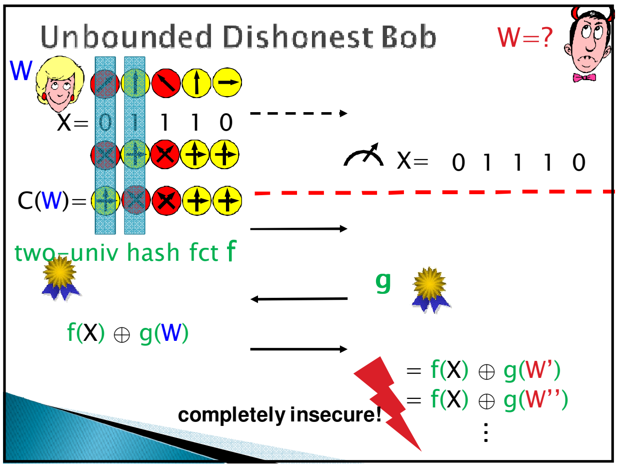
Why Secure Identification?

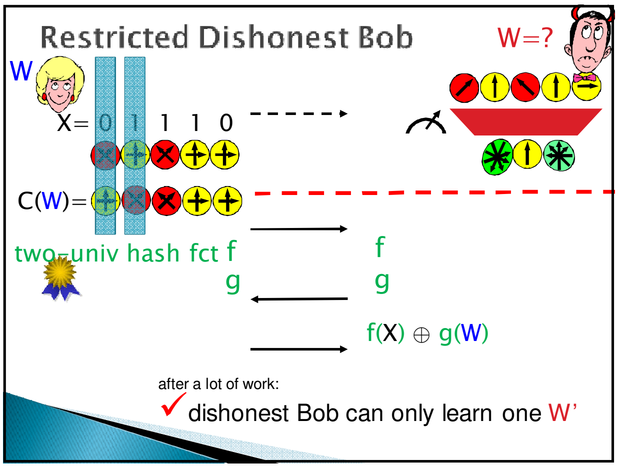


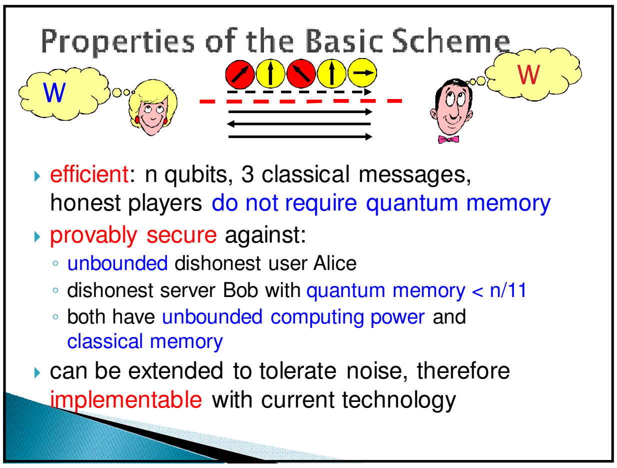

Secure Evaluation of the Equality
W_A
W_B
W_A =? W_B
PIN-based identification scheme should be a secure evaluation of the equality function
A dishonest player can exclude only one possible password

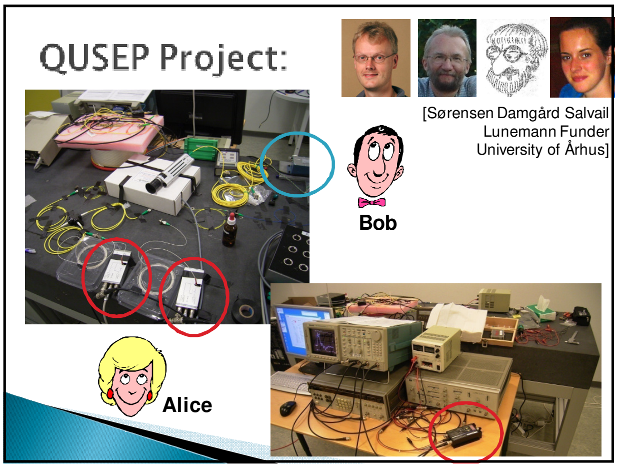

Quantum Identification Protocol
W
W
X= 0 1 1 1 0
C(W)=
C(W)=
X'= 0 0 1 1 0
two-univ hash fct f
classical binary code C with large minimal distance
f(X) ⊕ g(W)
=? f(X') ⊕ g(W)
correct protocol

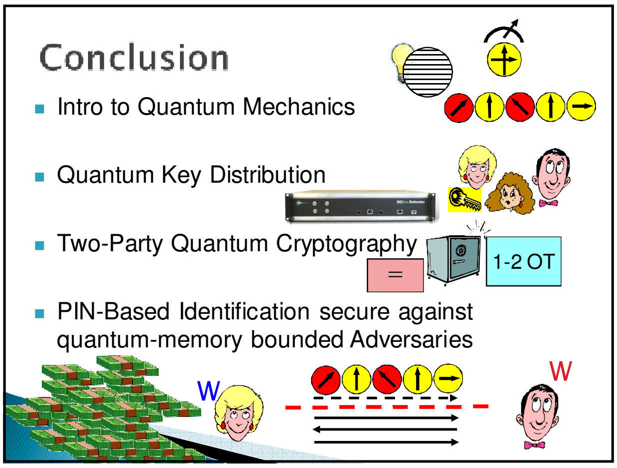

Dishonest Alice
W
X= 0 1 1 1 0
W=?
C(W')=
C(W'')=
C(W)=
X'= 0 0 1 1 0
two-univ hash fct f
g
f(X) ⊕ g(W')
f(X) ⊕ g(W'')
whp all different
=? f(X') ⊕ g(W)
secure against unbounded Alice


Unbounded Dishonest Bob
W=?
W
X= 0 1 1 1 0
C(W)=
X= 0 1 1 1 0
two-univ hash fct f
g
f(X) ⊕ g(W)
= f(X) ⊕ g(W')
= f(X) ⊕ g(W'')
completely insecure!


Restricted Dishonest Bob
W=?
W
X= 0 1 1 1 0
C(W)=
two-univ hash fct f
f
g
g
f(X) ⊕ g(W)
after a lot of work:
dishonest Bob can only learn one W'


Properties of the Basic Scheme
W
W
efficient: n qubits, 3 classical messages, honest players do not require quantum memory
provably secure against:
unbounded dishonest user Alice
dishonest server Bob with quantum memory < n/11
both have unbounded computing power and classical memory
can be extended to tolerate noise, therefore implementable with current technology


QUSEP Project:
[Sørensen Damgård Salvail
Lunemann Funder
University of Århus]
Bob
Alice


Conclusion
Intro to Quantum Mechanics
Quantum Key Distribution
Two-Party Quantum Cryptography
=
1-2 OT
PIN-Based Identification secure against
quantum-memory bounded Adversaries
W
W


Conclusion
Quantum Cryptography is
practical !!
(at least more than you thought)
Thanks to
you!
DAIMI
CWI
SECOQC
QAIP
NWO