Lecture 13: Quantum Cryptography II

slides: http://www.francoislegall.com/courses/iqc12/

Contents:

1. Quantum Key Distribution (continued)

2. Other Tasks in Quantum Cryptography (bit commitment)

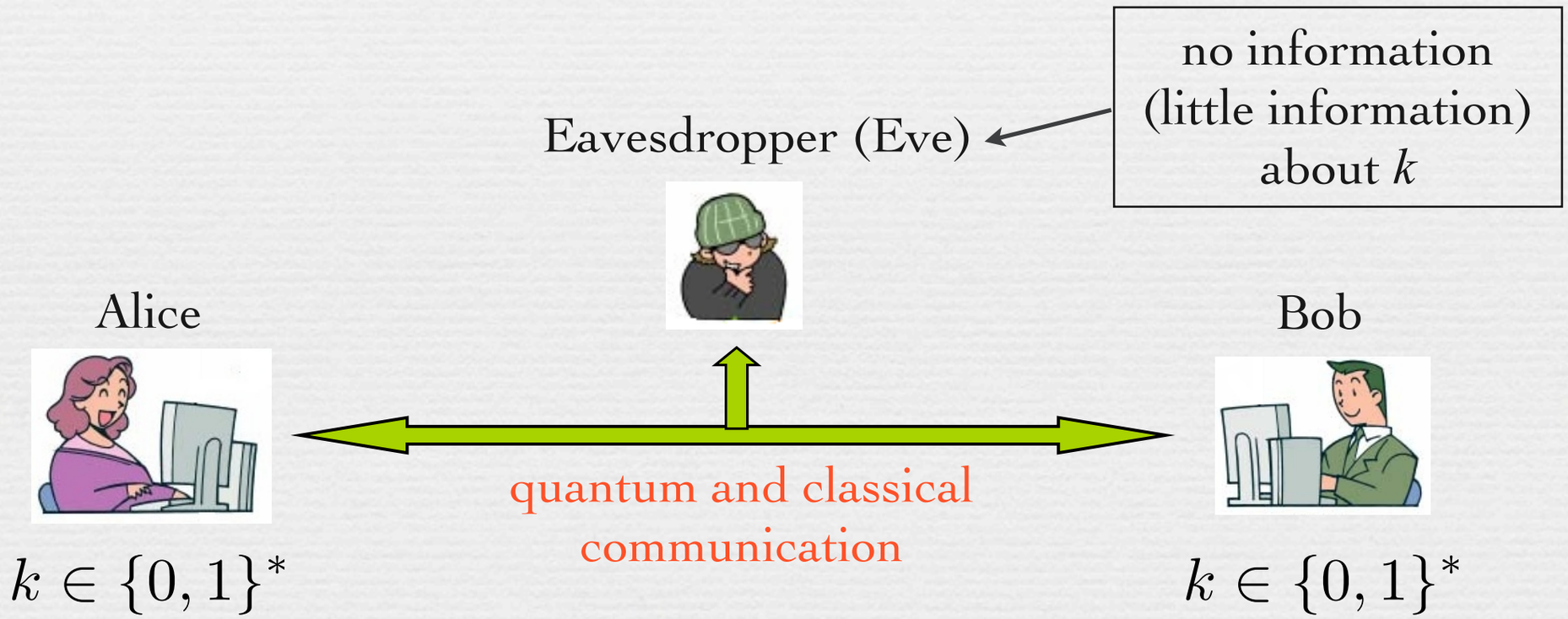
3. Fault-Tolerant Quantum Computation

4. Implementation of Quantum Computers

1. Quantum Key Distribution (continued)

QKD-based Quantum Cryptography (main idea)

Phase 1: Quantum Key Distribution



Phase 2: classical private key cryptosystem using k

BB84 QKD Protocol (last lecture)

Alice

Bob

$|\psi_i\rangle = H^{b_i}|a_i\rangle$

b

c

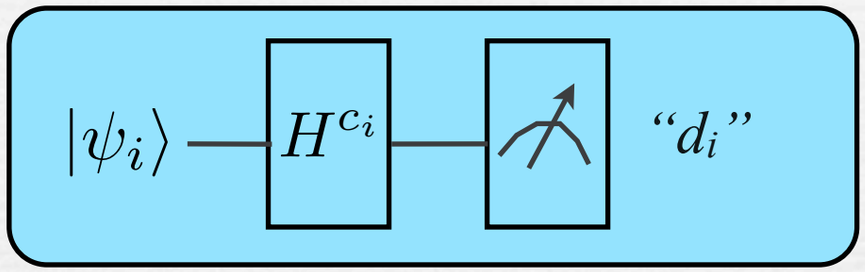
$a, b \in \{0,1\}^n$

$c \in \{0,1\}^n$

$d \in \{0,1\}^n$

key: a_i for i s.t. $b_i = c_i$

key: d_i for i s.t. $b_i = c_i$

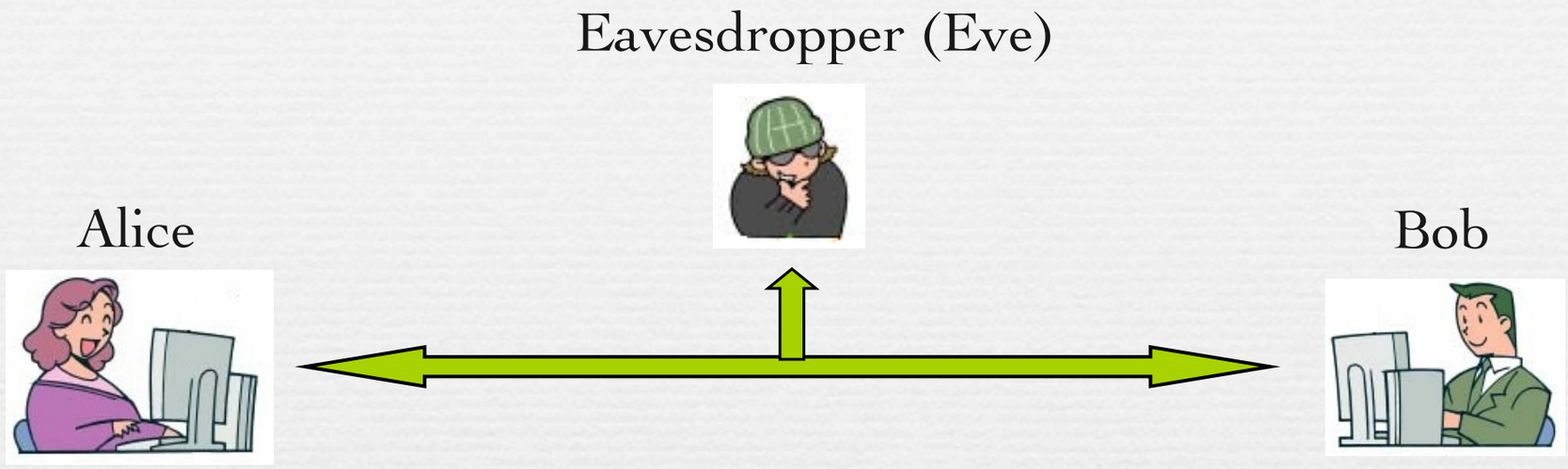


Property: $a_i = d_i$ when $b_i = c_i$

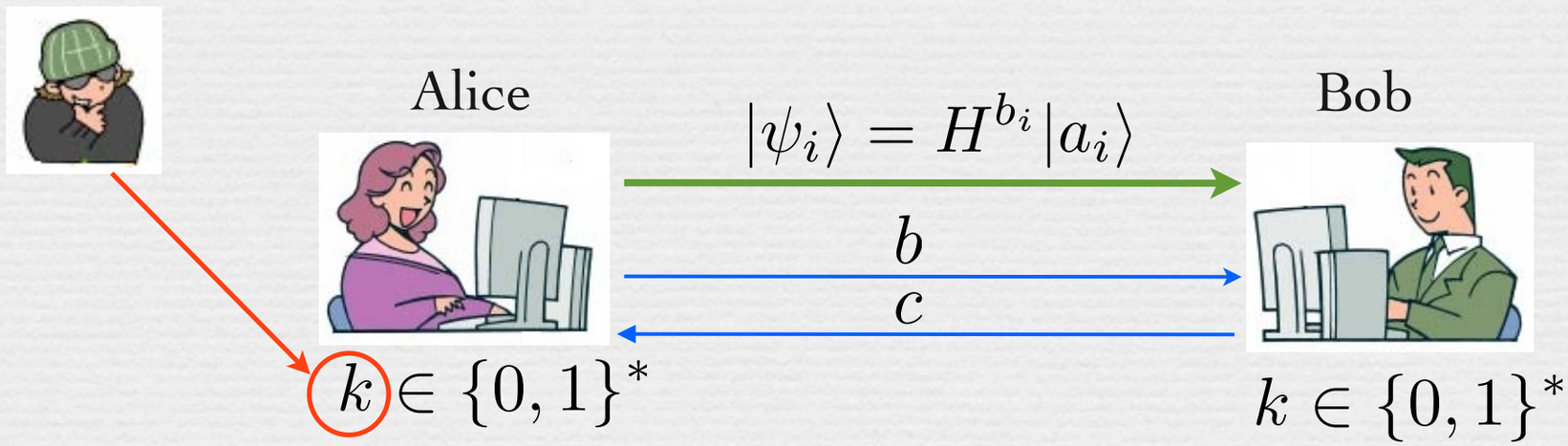
$a =$	a_1	a_2	a_3	a_4	a_5	a_6	a_7
$b =$	0	1	1	1	0	1	0
$c =$	1	1	0	1	0	0	0
$d =$	×	a_2	×	a_4	a_5	×	a_7

- Alice and Bob keep all the bits $a_i = d_i$ such that $b_i = c_i$
- This gives a shared raw key of expected length $n/2$

Security against Eavesdroppers

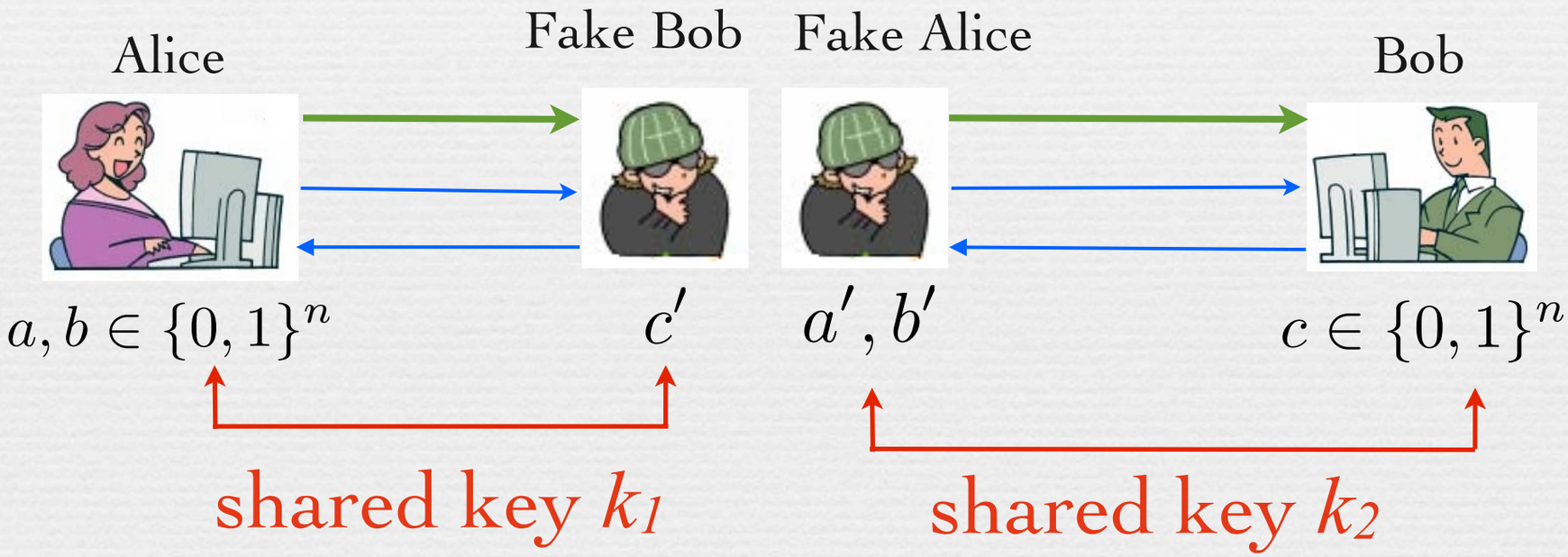


Direct Eavesdropping of Alice's or Bob's devices



Security against Eavesdroppers

Man-in-the-middle attack

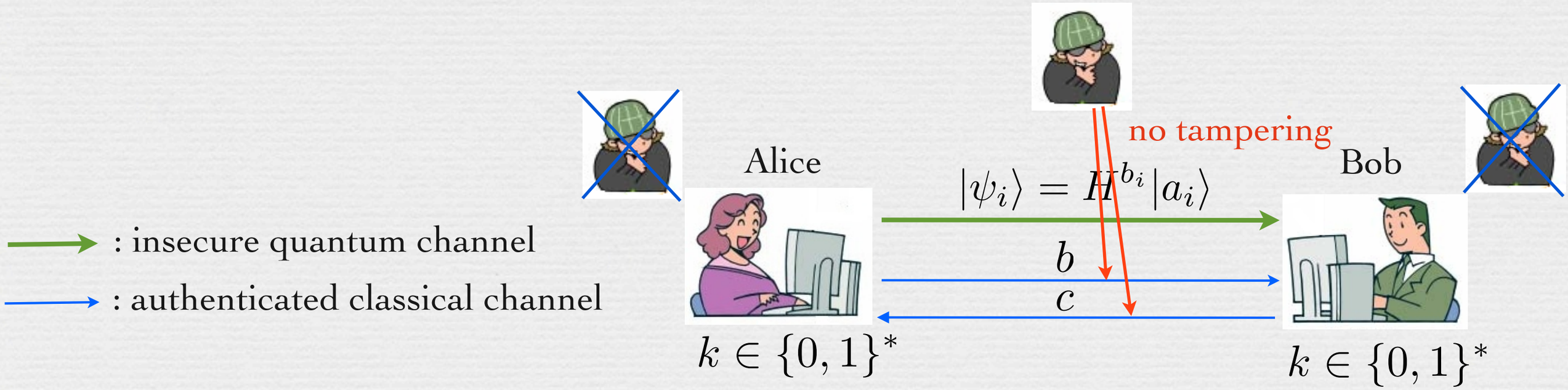


ASSUMPTIONS ARE NEEDED TO PROVE THE SECURITY OF BB84

Security Assumptions

- The eavesdropper cannot access Alice and Bob's encoding/decoding devices

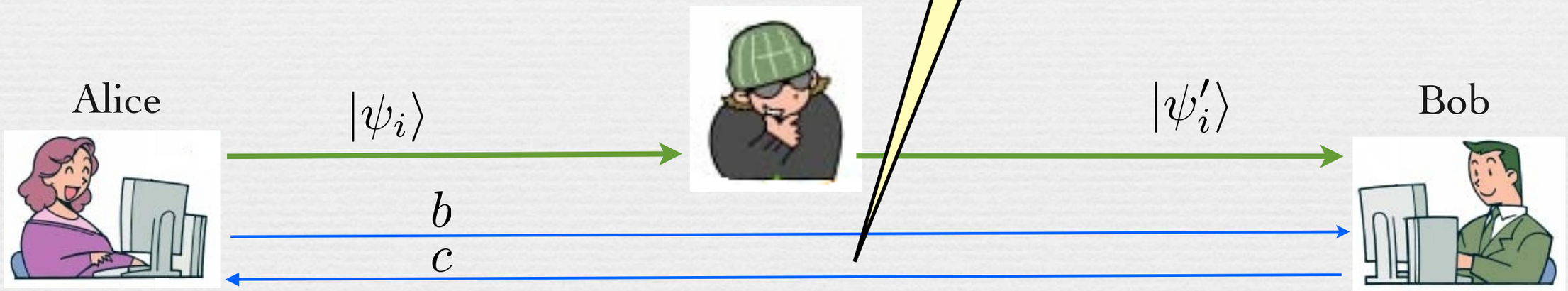
- The eavesdropper can read the classical channel but cannot modify its contents
  - authenticated classical channel
  - usually implemented using an unconditionally secure authentication scheme (typically using the Carter-Wegman scheme)



Security of BB84

- Proving the security of BB84 is not an easy task (finally proved in 1998 by Lo-Chau and Mayers), but it can be theoretically secure ("unconditionally s

- The basic idea is that Eve can only do an intercept-and-resend attack

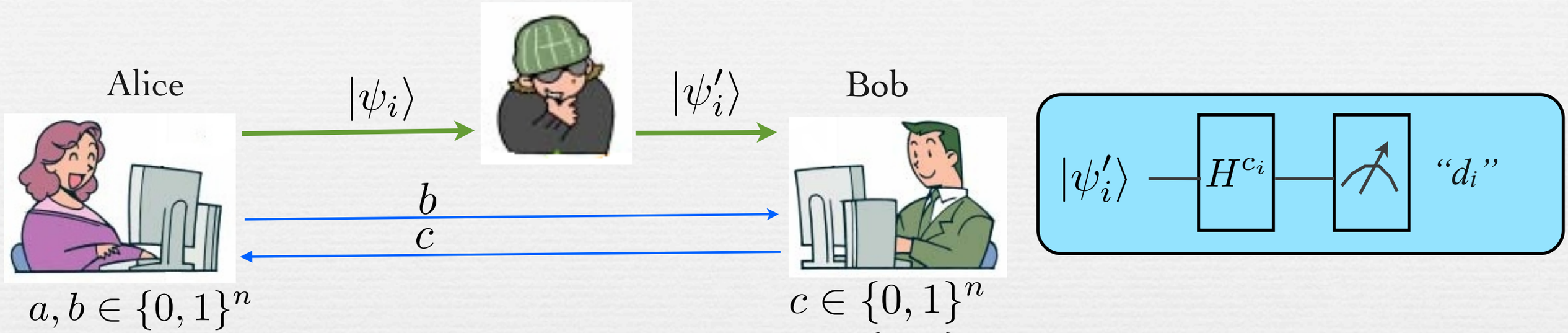


b and *c* are sent at the end of the protocol

- Key idea #1: Eve cannot copy $|\psi_i\rangle$, from the non-cloning theorem

- Key idea #2: Eve must measure $|\psi_i\rangle$ to obtain some information, which perturbs the state, so that $|\psi_i\rangle$ and $|\psi_i'\rangle$ differ

Security of BB84 (idea)



Property: $a_i = d_i$ when $b_i = c_i$

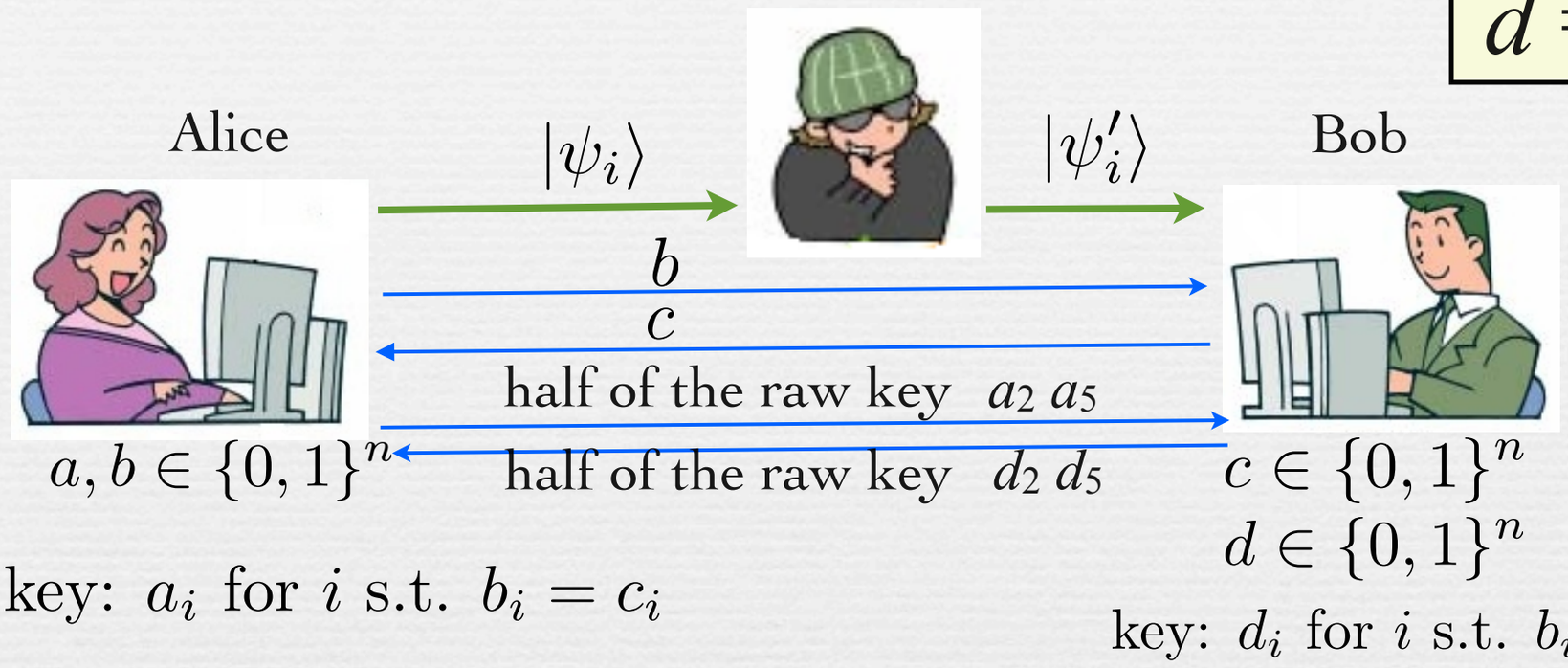
This is not always true if $|\psi_i\rangle$ and $|\psi'_i\rangle$ differ

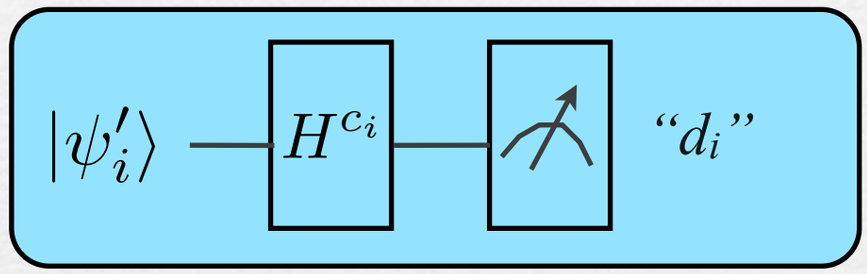
Eavesdropping is detected by checking if the property holds

tradeoff between the amount of information Eve gets and the disturbance induced by the measurements

Complete BB84 Protocol

$$
\begin{array}{lccccccc}
a = & a_1 & \cancel{a_2} & a_3 & a_4 & \cancel{a_5} & a_6 & a_7 \\
b = & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\
c = & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
d = & \times & \cancel{d_2} & \times & d_4 & \cancel{d_5} & \times & d_7
\end{array}
$$





Alice and Bob estimate the eavesdropping rate
(the expected length of the remaining key is $n/4$)

- if it is too large, they abort
- if it is small enough, they proceed to an error correction and privacy amplification step (the expected length of the final shared key is, say, $n/16$)

Quantum Key Distribution: Final Remarks

- Security is information-theoretic and relies only on the laws of quantum mechanics

- Noisy channels: dealt with by assuming that the noise is due to Eve's eavesdropping

- Implementation issues (since single photon laser is an ideal model) solved by variants of BB84

- There exist several other protocols for QKD: BB92,E91,S09... based on similar principles

Quantum Cryptography: reference

Electronic Colloquium on Computational Complexity, Revision 2 of Report No. 146 (2005)

ECCC

Quantum Cryptography: A Survey*

Dagmar Bruß† Gábor Erdélyi‡ Tim Meyer† Tobias Riege‡ Jörg Rothe‡
Heinrich-Heine-Universität Düsseldorf
40225 Düsseldorf, Germany

September 1, 2006

Abstract

We survey some results in quantum cryptography. After a brief introduction to classical cryptography, we provide the quantum-mechanical background needed to present some fundamental protocols from quantum cryptography. In particular, we review quantum key distribution via the BB84 protocol and its security proof, as well as the related quantum bit commitment protocol and its proof of insecurity.

http://eccc.hpi-web.de/report/2005/146/

2. Other Tasks in Quantum Cryptography (bit commitment)

Bit Commitment

commit phase: Alice chooses a bit *b*, and sends a message to Bob

reveal phase: Alice sends a message to Bob so that he can obtain *b*

hiding requirement : Bob cannot obtain *b* before the reveal phase

biding requirement : Alice cannot modify the value *b* after the commit phase

commit

reveal

Bit Commitment

- Bit commitment is a fundamental cryptographic primitive (applications: coin flipping, secure computation...)
- Bit commitment both biding and hiding in an information-theoretical sense cannot exist in the classical setting (but computational biding and computational hiding are possible)
- Quantum bit commitment protocols proposed in the early 90's
  [Brassard, Crépeau, Jozsa, Langlois, 93] [Yao 95]
- Even in the quantum setting, perfectly biding and hiding protocols cannot exist [Mayers 96] but:
  - approximate binding and hiding are possible
  - perfect binding and hiding are achievable in the bounded-storage model [Damgaard,Fehr, Salvail, Schaffner 05]

3. Fault-Tolerant Quantum Computation

Fault-Tolerant Quantum Computation

(Fictional) discussion between a believer and a skeptic, around 1994

B.: Wow! We now know how to break RSA with a quantum computer!

S.: Maybe, but you still need to build a large-scale quantum computer.

B.: Well, it is a technological problem, so it should be doable.

S.: Not sure. You'll have to deal with noise, decoherence and hardware errors.

B.: The same problems appeared when constructing the first classical computer, so this should be OK.

S.: But for quantum computation you need to deal with superpositions, measurements,... The same error-correction techniques as in classical. computation probably cannot be used, so I expect that you will need to build quantum gates with extremely high precision, which is unrealistic.

B.: Um...

Software-Based Error-correction for Classical Computers

- Idea: use error-correcting codes

<u>example:</u>

$$0 \xrightarrow{\text{encoding}} 000 \quad \overset{\text{bit flip}}{010} \xrightarrow{\text{decoding}} 0$$

$$1 \longrightarrow 111 \quad 110 \longrightarrow 1$$

simple error model: each bit is flipped with probability p

two bits (or more) are flipped with probability $<3p^2$
the majority-value of the three bits is unchanged with probability $>1-3p^2$

- Better error-correcting codes are used to obtain better performance

Error-correction for Quantum Computers: Problems

- Repeating a state does not work due to the non-cloning theorem
- In the classical world there are only bit-flip errors. In the quantum world everything is continuous!
- Measurements of a quantum state to check if an error occurred can modify the state

Error-correction for Quantum Computers: Solutions

Shor's 9-qubits code (1995)

logical qubit → physical qubit

$$|0\rangle \longrightarrow |\bar{0}\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$|1\rangle \longrightarrow |\bar{1}\rangle = \frac{1}{\sqrt{8}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

This code corrects all one-qubit errors!

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Idea: it is enough to correct bit-flip errors and phase-flip errors and their product

Error-correction for Quantum Computers: Solutions

- Many quantum error-correcting codes have been constructed (stabilizer codes, CSS codes...)
- The shortest code that encodes one logical qubit and protects against one error has size 5
- As in the classical setting, it is possible to construct codes protecting against an arbitrary number of errors

Fault-Tolerant Quantum Computation

- Quantum error-correcting codes are not enough!
- We need to perform operations (apply unitary transformations, measurements) directly on the encoded qubits.
- Many issues arise: for example applying a CNOT gate can spread the error from the control qubit to the target qubit

Theorem of fault-tolerant quantum computation (1996~)

If the basic error rate of each gate is below some threshold, then we can do arbitrary long quantum computation.

currently about 10^{-4}

can possibly be reduced to a few percents

Fault-Tolerant Quantum Computation

(Fictional) discussion between a believer and a skeptic, around 1996

B.: Wow! We now know how to break RSA with a quantum computer!

S.: Maybe, but you still need to build a large-scale quantum computer.

B.: Well, it is a technological problem, so it should be doable.

S.: Not sure. You'll have to deal with noise, decoherence and hardware errors.

B.: The same problems appeared when constructing the first classical computer, so this should be OK.

S.: But for quantum computation you need to deal with superpositions, measurements,... The same error-correction techniques as in classical computation probably cannot be used, so I expect that you will need to build quantum gates with extremely high precision, which is unrealistic.

B.: We know that we only need to build quantum gates with, say, 99% precision.

S.: Then this may be possible!

Quantum Computers: Implementation

qubit

- photon
- ion
- electron
- nucleus
- superconducting junction
- quantum dot

computation model

- Turing machine
- circuit model
- one-way quantum computing
- topological computing
- adiabatic quantum computing