UNIVERSITY OF WATERLOO

QIC 710 / CS 768 / PH 767 / CO 681 / AM 871 / PM 871 Fall 2020

Introduction to
Quantum Information Processing

Richard Cleve

Institute for Quantum Computing

and

Cheriton School of Computer Science

a primer for beginners
quantum algorithms
quantum information theory

Part 4: quantum cryptography

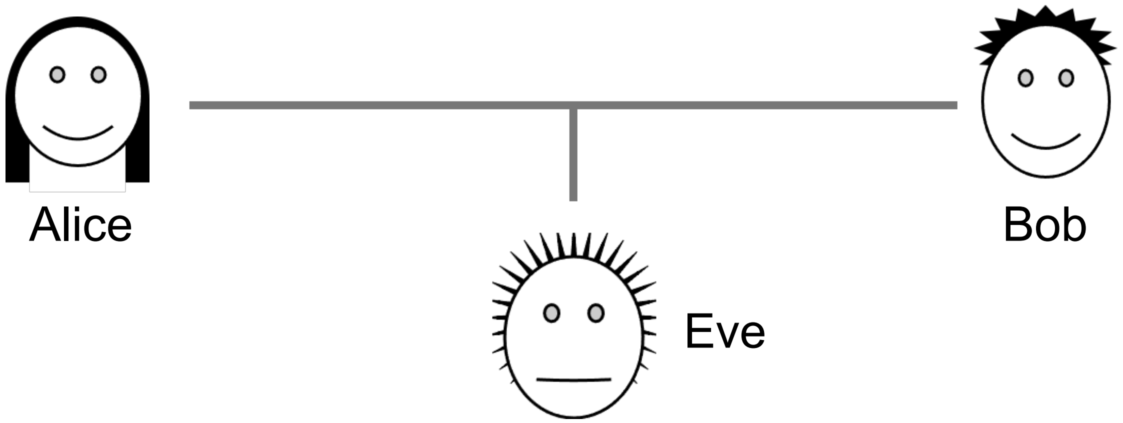
Lecture 23

The BB84 key distribution scheme

Private communication

Goal: for Alice and Bob to communicate privately in the presence of an eavesdropper Eve

message $m \in \{0,1\}^n$



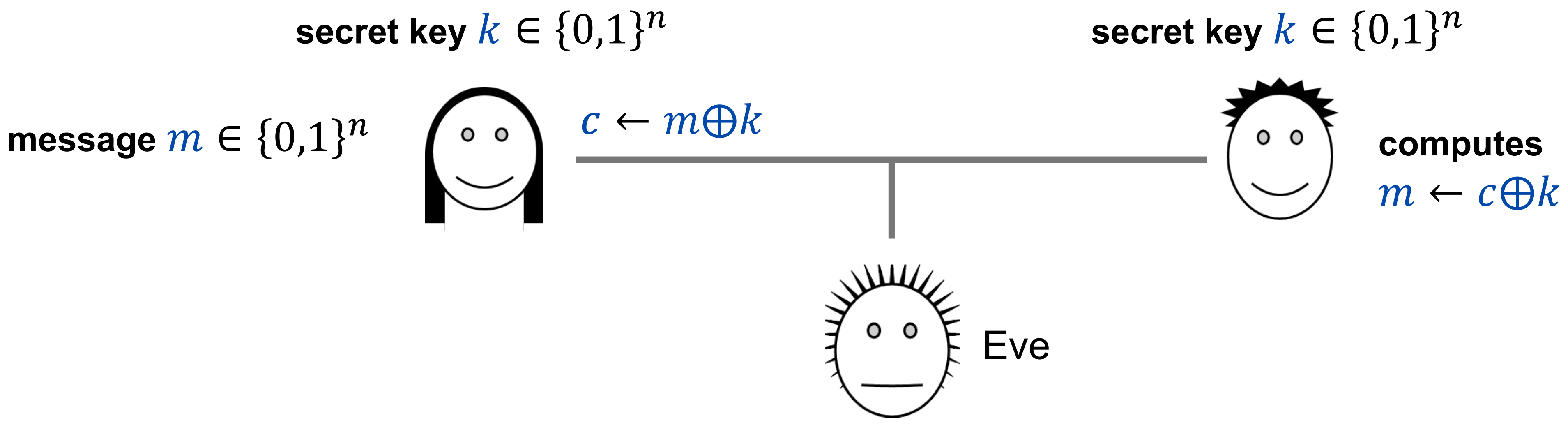
learns m

learns nothing about m

Definition of security (informal)

A communication protocol system is ***secure*** if Eve cannot acquire ***any*** information (not even partial information about m)

One-time pad



One-time pad protocol

1. Alice sends $c = m \oplus k$ (the bit-wise $\oplus$ of m and k) to Bob
2. Bob computes $c \oplus k$, which is $(m \oplus k) \oplus k = m$

This is secure because, Eve only sees c, which is uniformly distributed, regardless of m

But how do Alice and Bob set up the secret key to begin with?

Problem of setting up secret keys

Key distribution problem: set up a large number of secret key bits

Note: for the one-time pad, Alice and Bob must never reuse their key bits, because doing so leaks information

Simple, but cumbersome approaches

- Alice and Bob get together and flip coins
- Alice and Bob obtain keys from a trusted third party

An alternative approach …

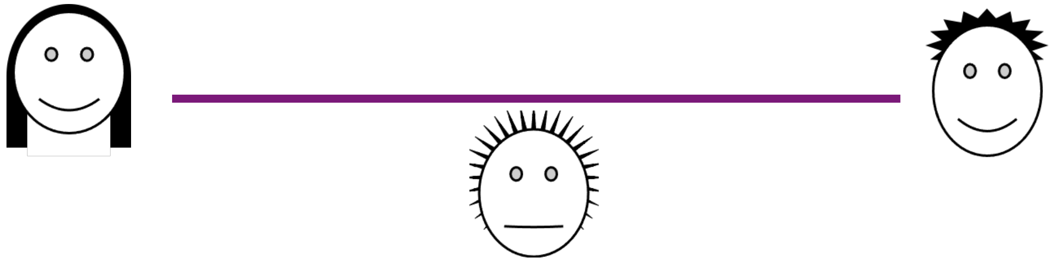
Public key cryptography (based on computational hardness)

Bob produces two keys: a **public key** for efficient **encoding**
a **private key** for efficient **decoding**

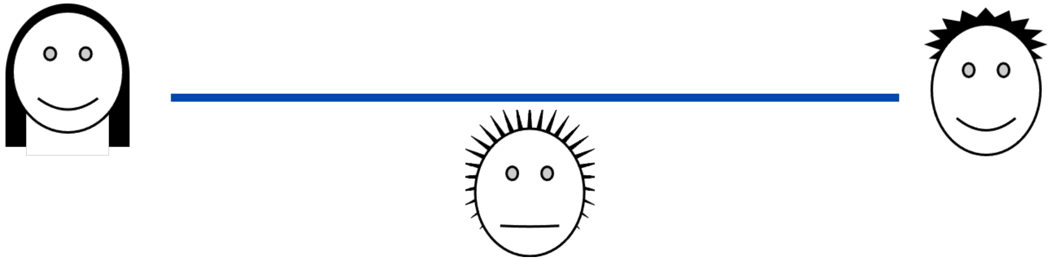
Quantum computers can break many public key cryptosystems

Quantum key distribution scenario

Quantum channel
Eve can measure (and modify) messages



Authenticated classical channel**
Eve can read (but not modify) messages



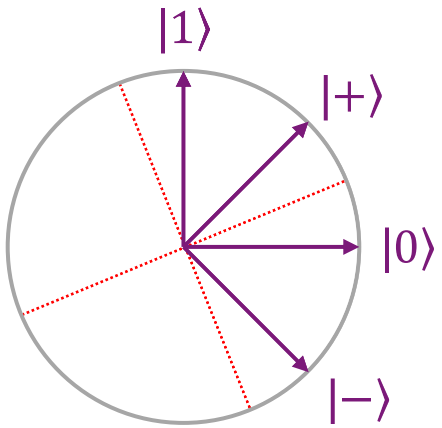
Goal: for Alice and Bob set up a secure key without computational assumptions

BB84 key distribution protocol [Bennett and Brassard, 1984]

** The authenticated classical channel can be simulated by Alice and Bob using a ***very short*** classical secret key

BB84: some preliminary ideas

Imagine Alice sending a bit b to Bob using one of these two encodings, chosen ***randomly***



$+$ encoding

bit	encoding
0	$\|0\rangle$
1	$\|1\rangle$

$\times$ encoding

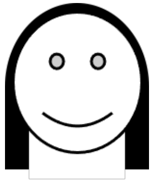
bit	encoding
0	$\|+\rangle$
1	$\|-\rangle$

Some good news
Eve doesn't know which basis to measure in, and cannot determine b

Some bad news
Bob doesn't doesn't know which basis to measure in either

Some mixed news
Eve can obtain ***partial information*** about b but doing this ***disturbs the state***

BB84: protocol



choose n random bits
choose n random bases

$0\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0$

$+ \times + \times \times + + \times + + \times + \times + \times \times$

$|0\rangle|+\rangle|1\rangle|-\rangle|-\rangle|0\rangle|1\rangle|+\rangle|1\rangle|0\rangle|+\rangle|1\rangle|-\rangle|+\rangle|-\rangle|+\rangle$

send encodings →

choose n random bases
measure the qubits

$+ + \times \times + \times + \times \times + \times \times + + \times +$

$|0\rangle|+\rangle|1\rangle|-\rangle|-\rangle|0\rangle|1\rangle|+\rangle|1\rangle|0\rangle|+\rangle|1\rangle|-\rangle|+\rangle|-\rangle|+\rangle$

$0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0$

end of quantum part

$+ + \times \times + \times + \times \times + \times \times + + \times +$

← **reveal bases**

reveal bases →

$+ \times + \times \times + + \times + + \times + \times + \times \times$

discard incompatible bases

0 ✗ ✗ 1 ✗ ✗ 1 0 ✗ 0 0 ✗ ✗ 0 1 ✗

gather remaining bits ($\approx n/2$ bits)

$a = 0\,1\,1\,0\,0\,0\,0\,1$

discard incompatible bases

0 ✗ ✗ 1 ✗ ✗ 1 0 ✗ 0 0 ✗ ✗ 0 1 ✗

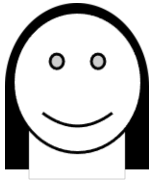
gather remaining bits

$b = 0\,1\,1\,0\,0\,0\,0\,1$

If Eve did not interfere then $a = b$

If Eve interfered then there may be inconsistencies between a and b

BB84: protocol (continued)



$a_1 = 0\,1\,1\,0\,0\,0\,0\,1$
random subset

$a_2 = 1\,0\,0\,1$
remaining bits

$b_1 = 0\,1\,1\,0\,0\,0\,0\,1$
random subset

$b_2 = 1\,0\,0\,1$
remaining bits

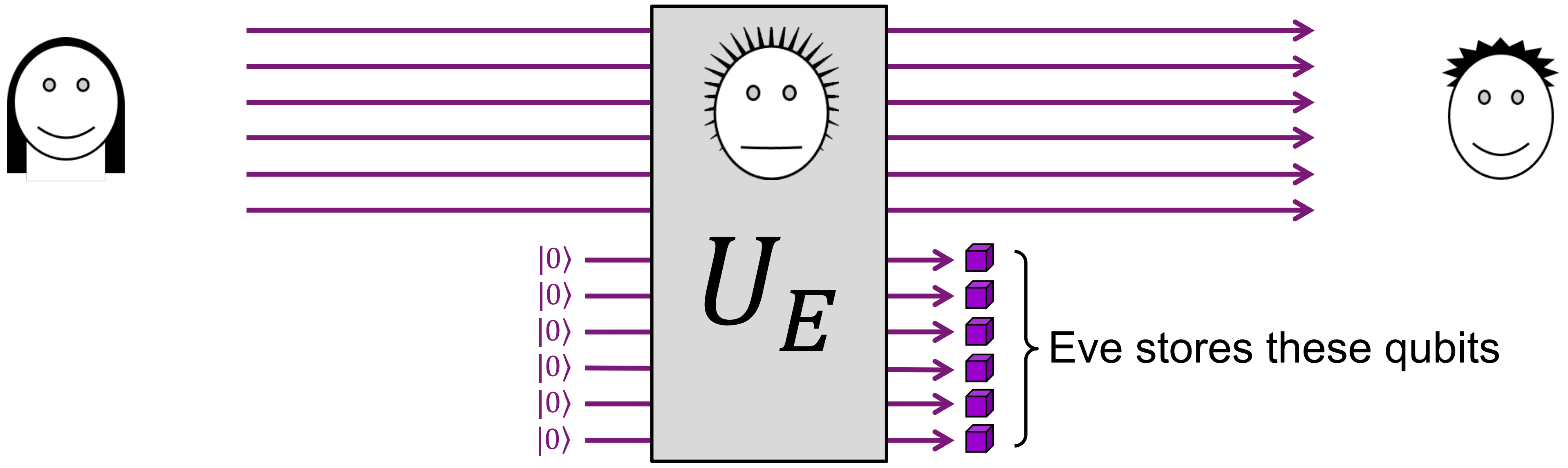
1. Alice and Bob randomly select half of their bits and compare them
2. if there are many inconsistencies then abort; otherwise, continue with remaining bits
3. **information reconciliation:** makes the remaining bits consistent
4. **privacy amplification:** eliminates Eve's partial information

} using ideas from error-correcting codes (details omitted here)

The final result is a secure key

What does it mean to be secure?

BB84: general form of an attack



Then Eve listens in on the entire classical conversation $\mathcal{C}$ between Alice and Bob

Then Eve performs a measurement $\mathcal{M}_{\mathcal{C}}$ on her stored qubits (that depends on $\mathcal{C}$)

[Mayers, 1996]: the first true security proof (very insightful, though complicated)

[Shor & Preskill, 2000]: a relatively simple proof of security