Quantum Cryptography

Christian Schaffner

Institute for Logic, Language and Computation (ILLC)
University of Amsterdam

Centrum Wiskunde & Informatica

BSc IW visit to ILLC

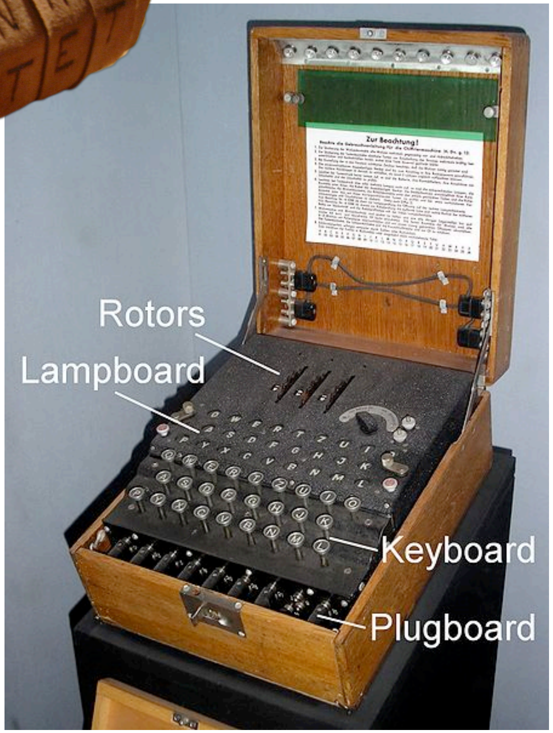
Monday, 2 November 2015

Nederlandse Organisatie voor Wetenschappelijk Onderzoek

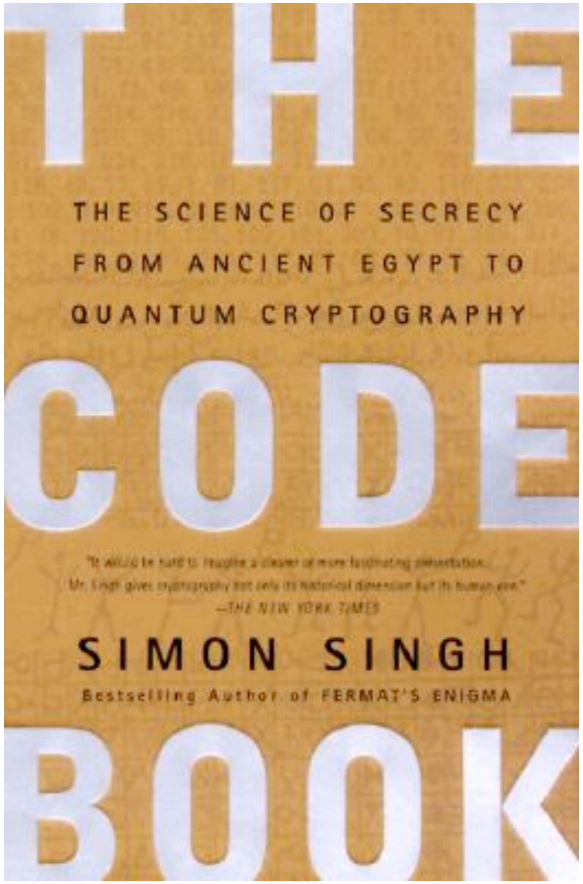
Classical Cryptography

- 3000 years of fascinating history
- Until 1970: private communication was the only goal

Scytale



Enigma



THE

THE SCIENCE OF SECRECY
FROM ANCIENT EGYPT TO
QUANTUM CRYPTOGRAPHY

CODE

"It would be hard to imagine a clearer or more fascinating presentation...
Mr. Singh gives cryptography not only its historical dimension but its human one."
—THE NEW YORK TIMES

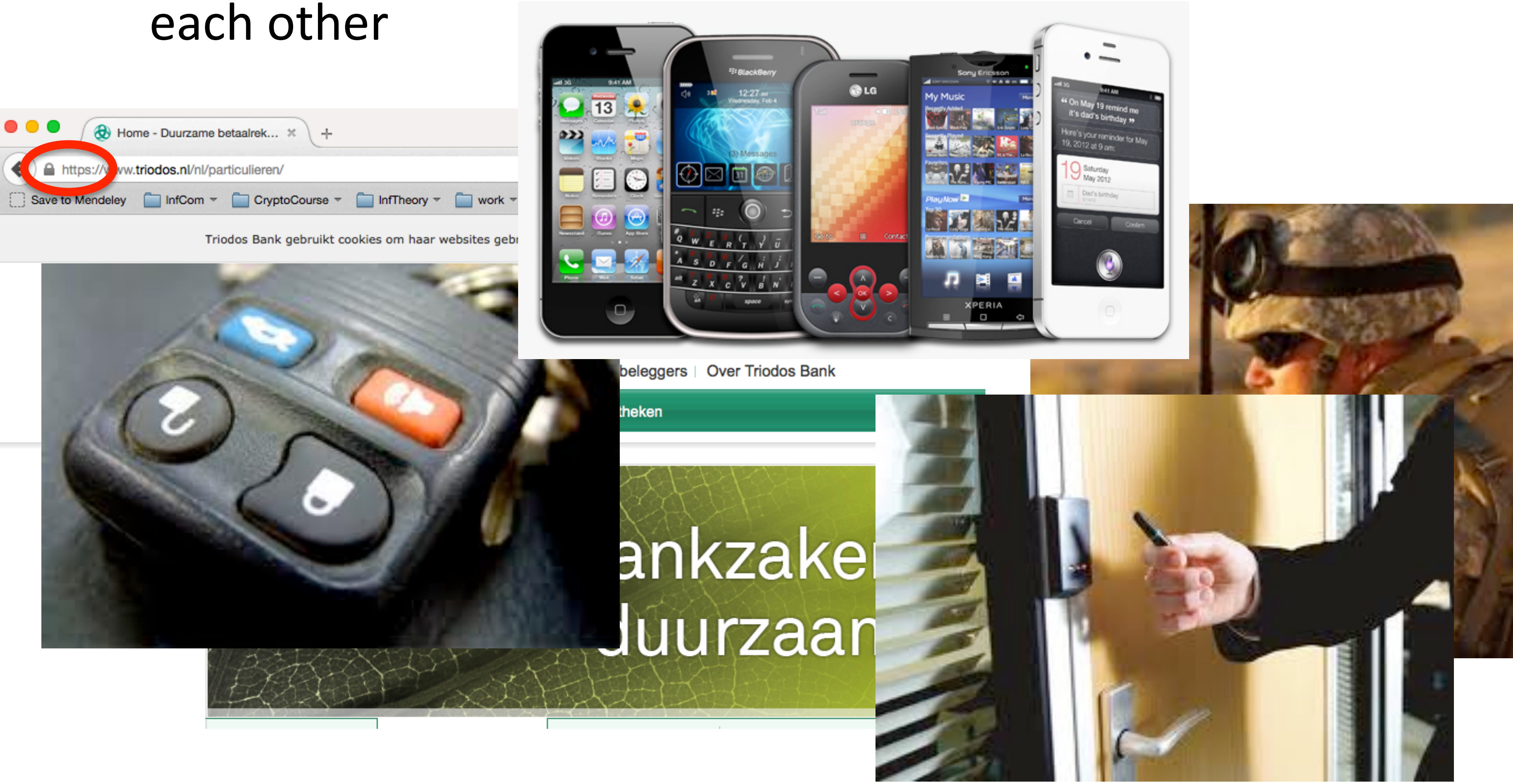
SIMON SINGH

Bestselling Author of FERMAT'S ENIGMA

BOOK

Modern Cryptography

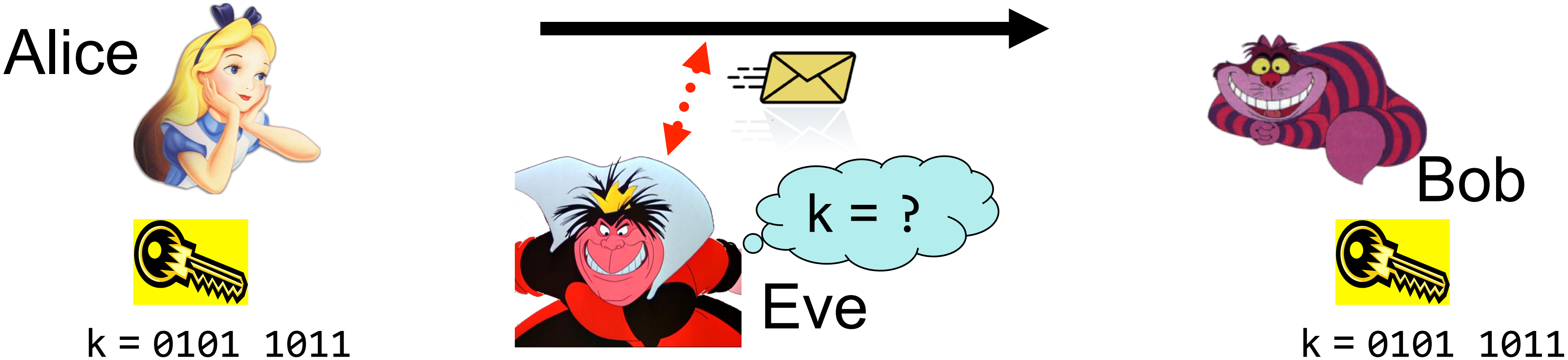
- is everywhere!
- is concerned with all settings where people do not trust each other



Secure Encryption

m = ‘I love you’

0000 1011



Alice

k = ?

Eve

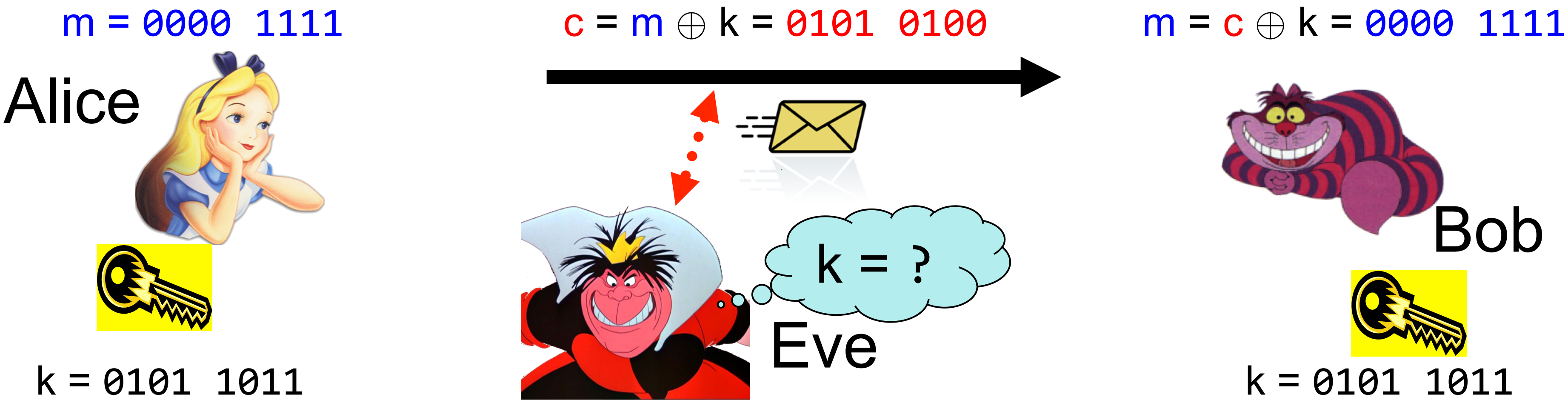
Bob

k = 0101 1011

k = 0101 1011

- Goal: Eve does not learn the message
- Setting: Alice and Bob share a secret key k

Perfectly Secure Encryption: One-Time Pad



$m =$ 0000 1111

$c = m \oplus k =$ 0101 0100

$m = c \oplus k =$ 0000 1111

$k =$ 0101 1011

$k =$ 0101 1011

- Goal: Eve does not learn the message
- Setting: Alice and Bob share a key k
- Recipe:

$m =$ 0000 1111

$k =$ 0101 1011

$c = m \oplus k =$ 0101 0100

$c =$ 0101 0100

$k =$ 0101 1011

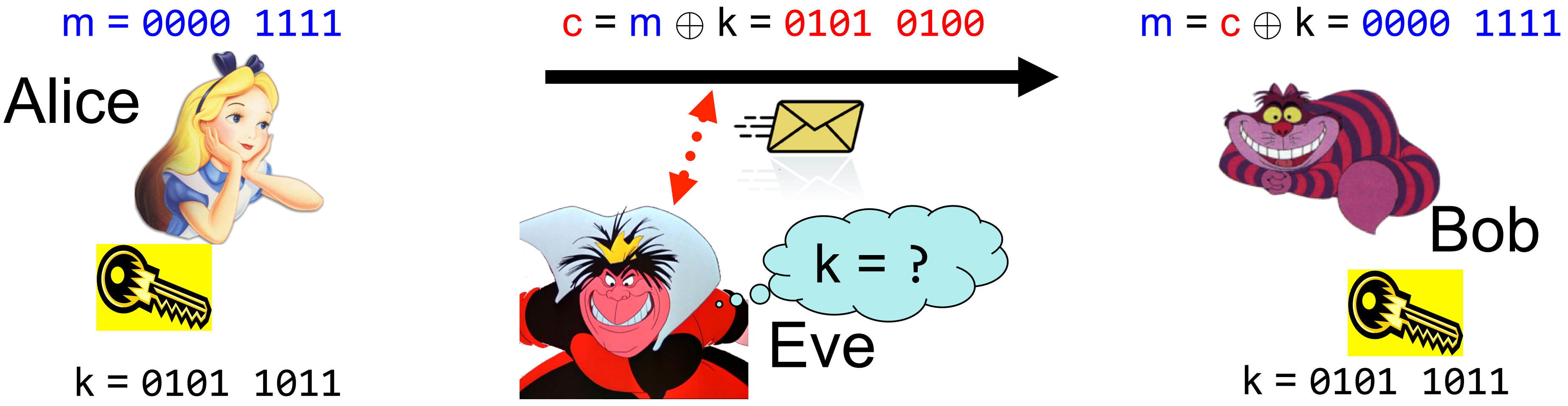
$c \oplus k =$ 0000 1111

$c \oplus k = m \oplus k \oplus k = m \oplus 0 = m$

x	y	x ⊕ y
0	0	0
0	1	1
1	0	1
1	1	0

- It is perfectly secure!

Problems With One-Time Pad



$m = 0000\ 1111$

$c = m \oplus k = 0101\ 0100$

$m = c \oplus k = 0000\ 1111$

$k = 0101\ 1011$

$k = 0101\ 1011$

- The key has to be as long as the message.
- The key can only be used once.
- In practice, other encryption schemes (such as AES) are used which allow to encrypt long messages with short keys.

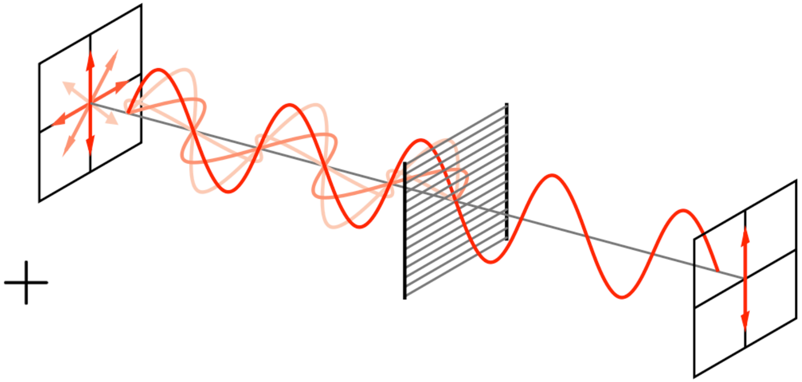
BSc Informatica course: Information & Communication

Master of Logic course: Information Theory

Master of Logic course: Modern Cryptography

Master of Logic course: Computational Complexity

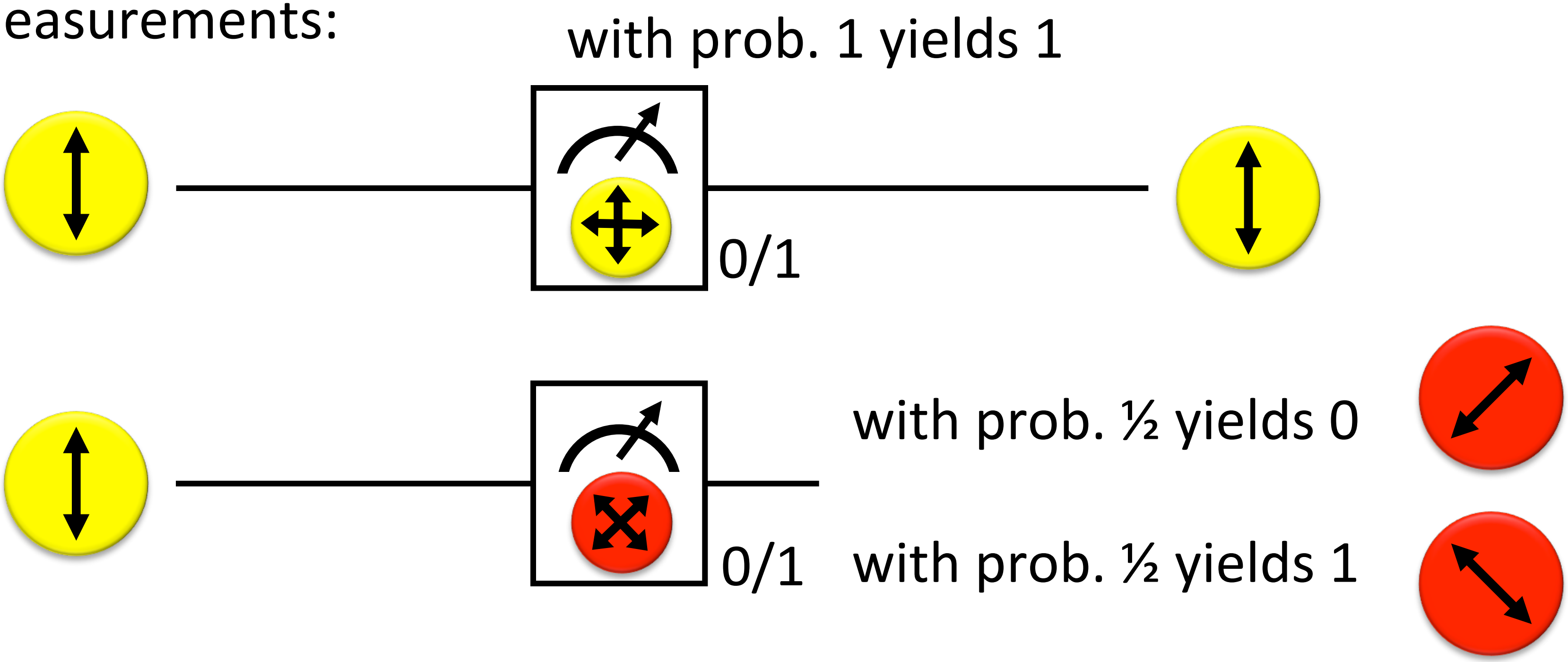
Quantum Mechanics



✛ $+$ basis ↔ $|0\rangle_+$ ↕ $|1\rangle_+$

✕ $\times$ basis ⤢ $|0\rangle_\times$ ⤡ $|1\rangle_\times$

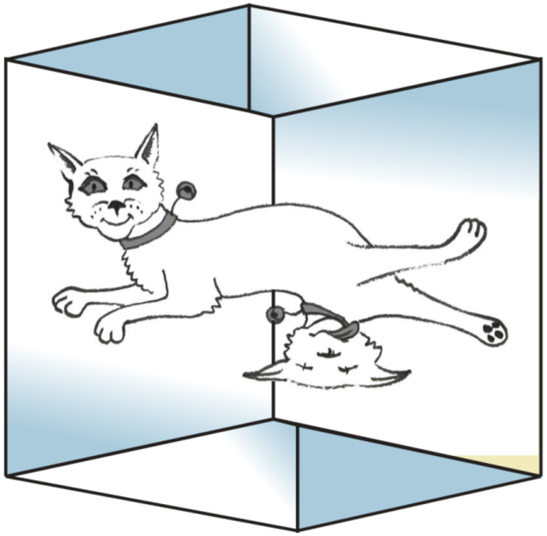
Measurements:

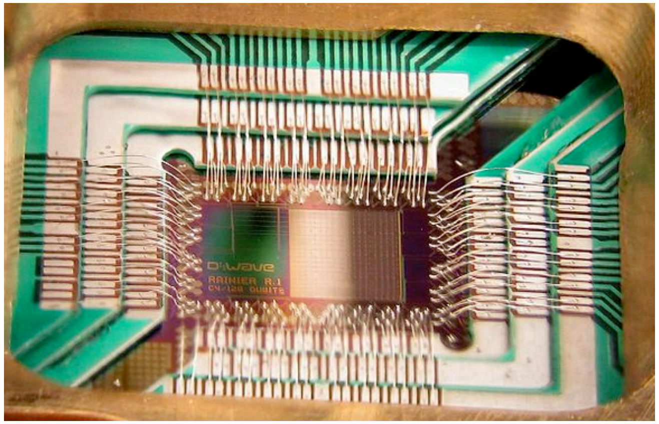


with prob. 1 yields 1

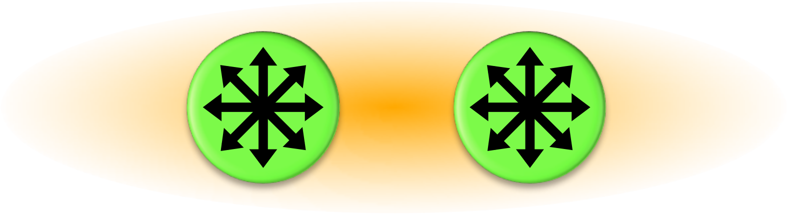
with prob. ½ yields 0

with prob. ½ yields 1



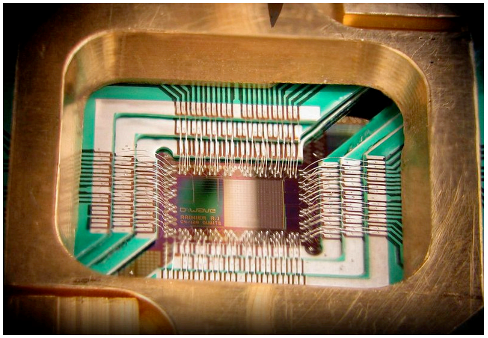


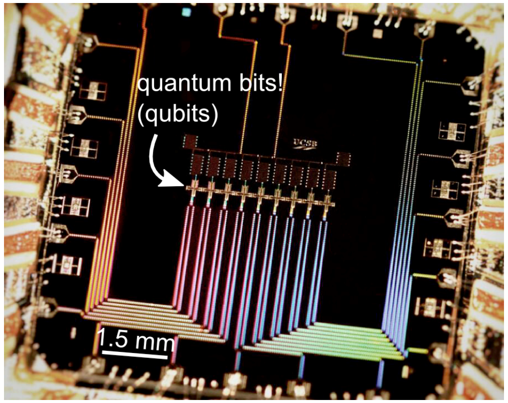
Wonderland of Quantum Mechanics



Can We Build Quantum Computers?

- Possible to build in theory, no fundamental theoretical obstacles have been found yet.





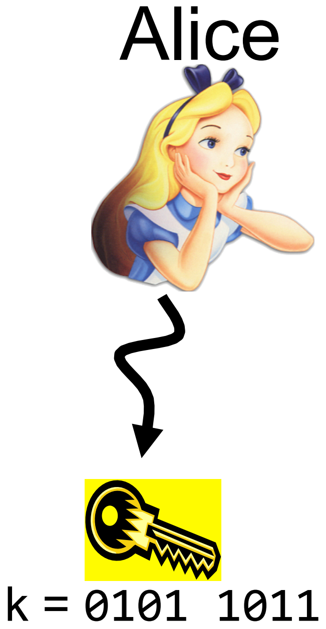
Martinis group (UCSB)
9 qubits

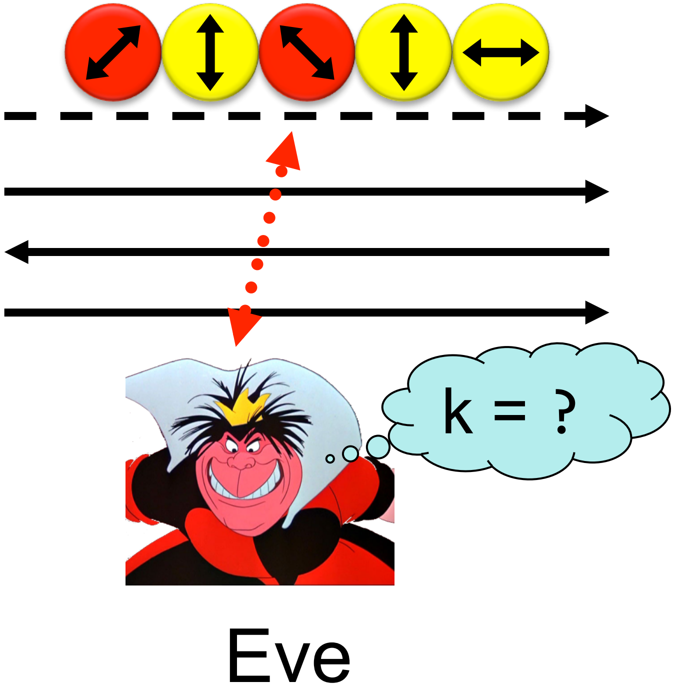
- Canadian company "D-Wave" claims to have build a quantum computer with 1024 qubits. Did they?
- 2014: Martinis group "acquired" by Google
- 2014/15: 135+50 Mio € investment Delft
- 2015: QuSoft center in Amsterdam

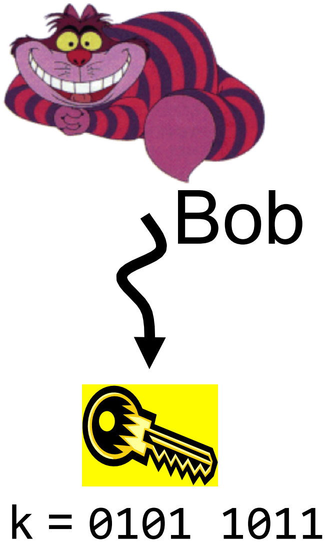
Master of Logic course:
Quantum Computing

Quantum Key Distribution (QKD)

[Bennett Brassard 84]



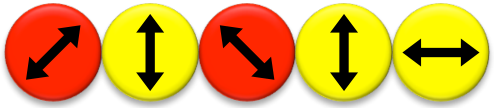


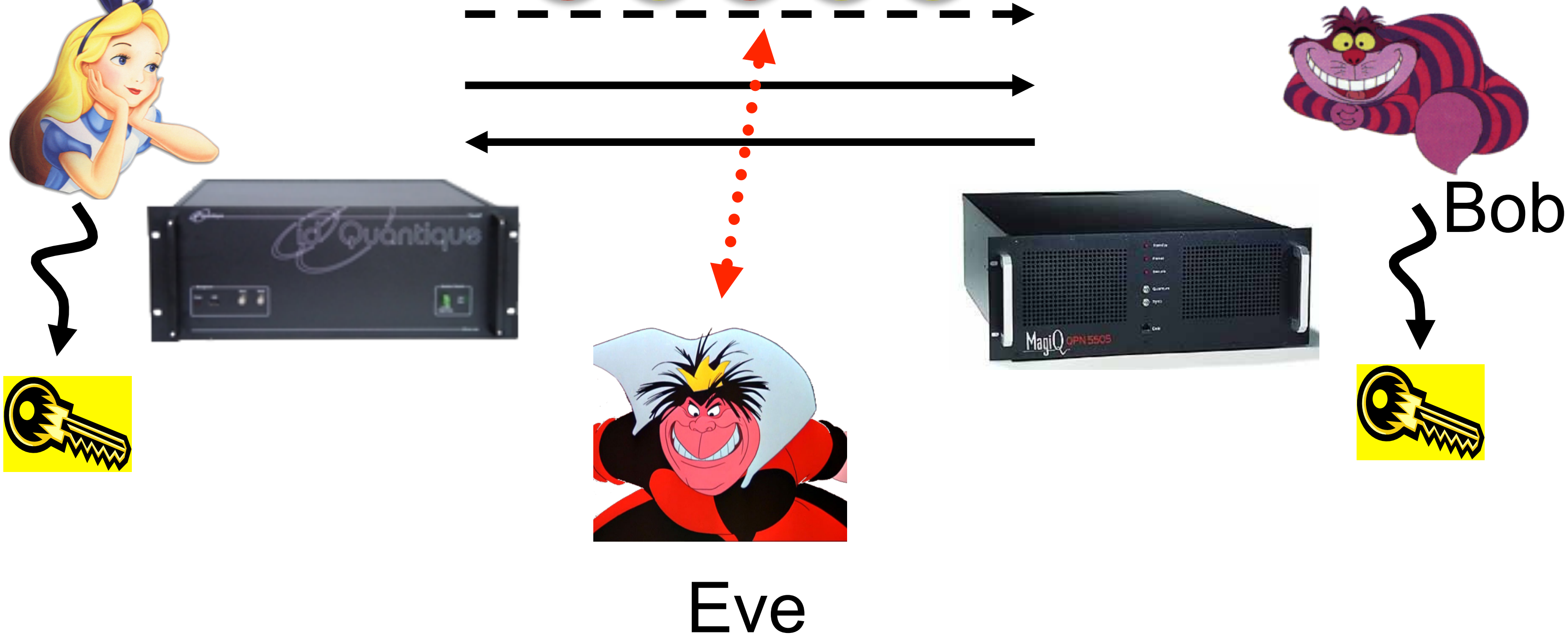


- Offers a quantum solution to the key-exchange problem
- Puts the players into the starting position to use symmetric-key cryptography (such as the one-time pad)

Quantum Key Distribution (QKD)

[Bennett Brassard 84]





Alice

Bob

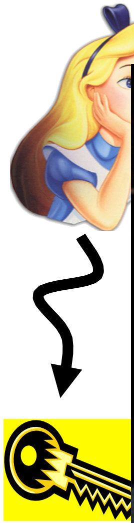
Eve

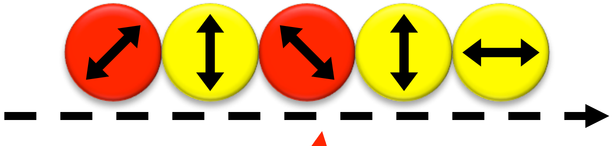
- technically feasible: no quantum computer required, only quantum communication

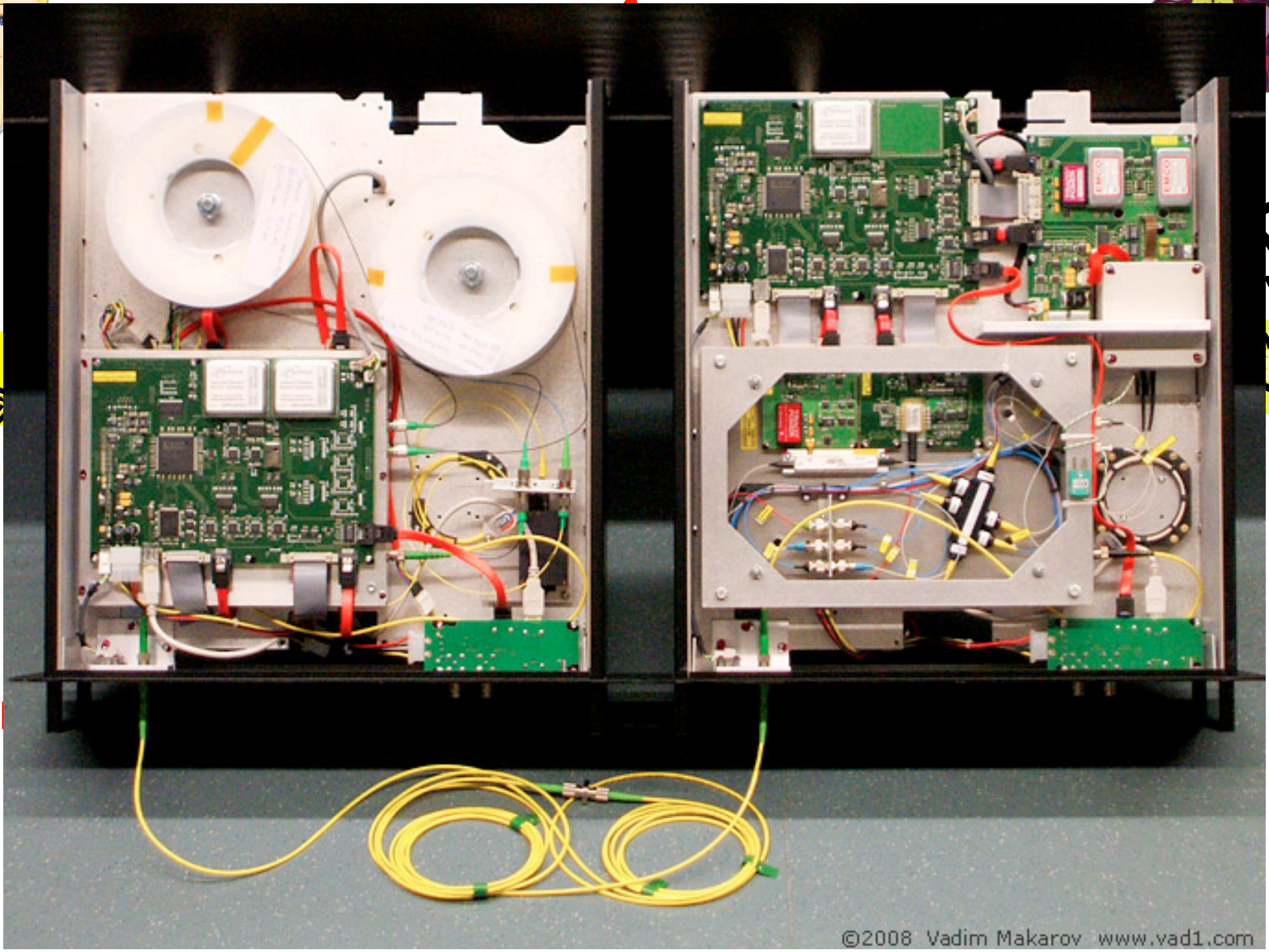
Quantum Key Distribution (QKD)

[Bennett Brassard 84]

Alice

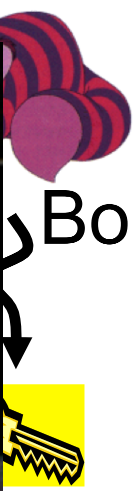






©2008 Vadim Makarov www.vad1.com

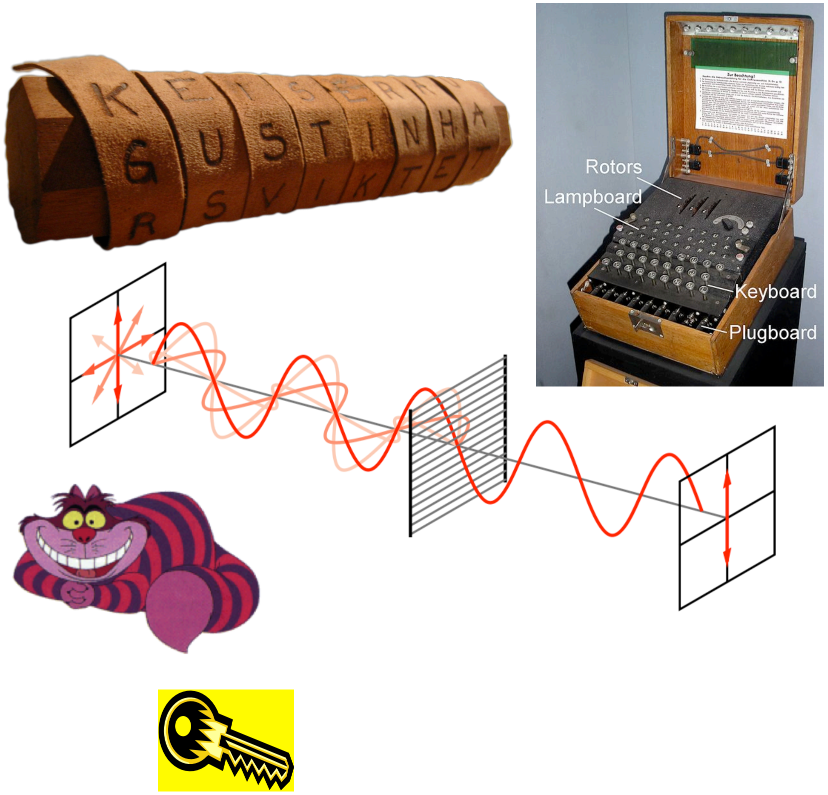
Bob

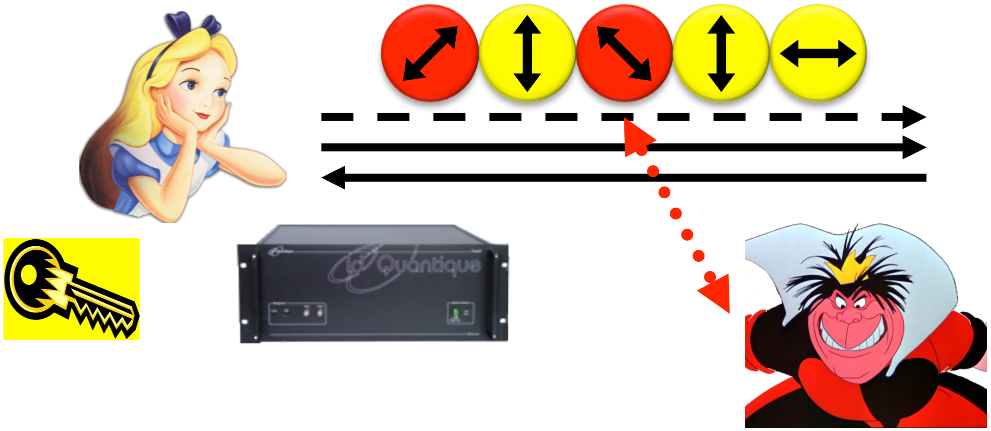


- tech
  only

Summary

- One-Time Pad
- Quantum Key Distribution





Master of Logic course:
Modern Cryptography

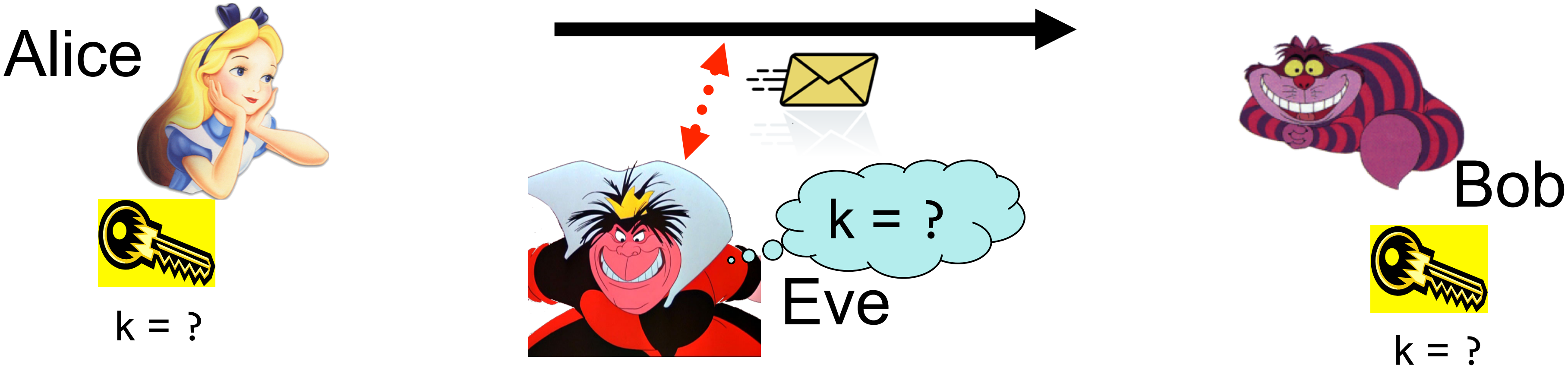
BSc Informatica course:
Information & Communication

Master of Logic course:
Quantum Computing

Master of Logic course:
Information Theory

Master of Logic course:
Computational Complexity

Perfect Security



m = ?

$c = m \oplus k =$ 0101 0100

$m = c \oplus k =$?

Alice

k = ?

Eve

k = ?

Bob

k = ?

- Given that c = 0101 0100,
  - is it possible that m = 0000 0000 ?
    - Yes, if k = 0101 0100.
  - is it possible that m = 1111 1111 ?
    - Yes, if k = 1010 1011.
  - it is possible that m = 0101 0101 ?
    - Yes, if k = 0000 0001
- In fact, every m is possible.
- Hence, the one-time pad is perfectly secure!

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0