Quantum Cryptography

Christian Schaffner

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

Centrum Wiskunde & Informatica

DESDA symposium, Nijmegen
Friday, 5 June 2015

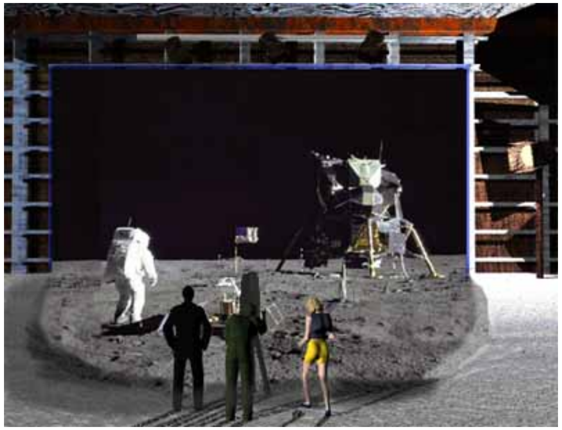
1969: Man on the Moon

http://www.unmuseum.org/moonhoax.htm

- How can you prove that you are at a specific location?

What will you learn from this Talk?

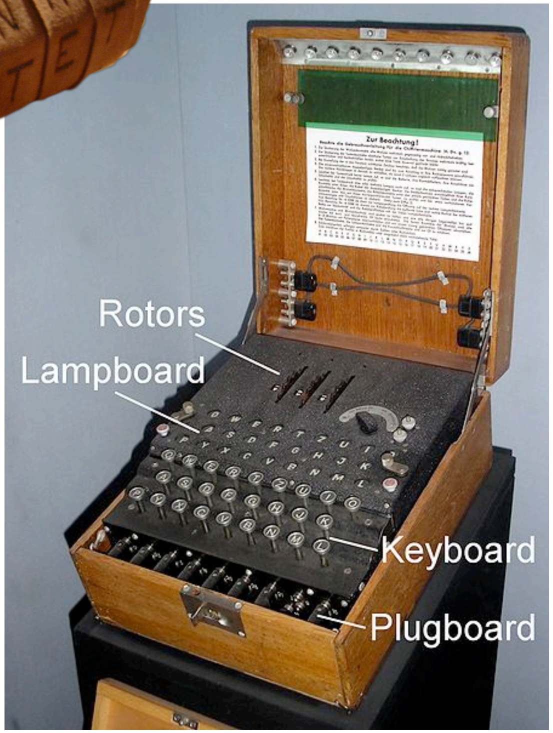
- Classical Cryptography
- Quantum Mechanics
- Quantum Key Distribution
- Position-Based Cryptography



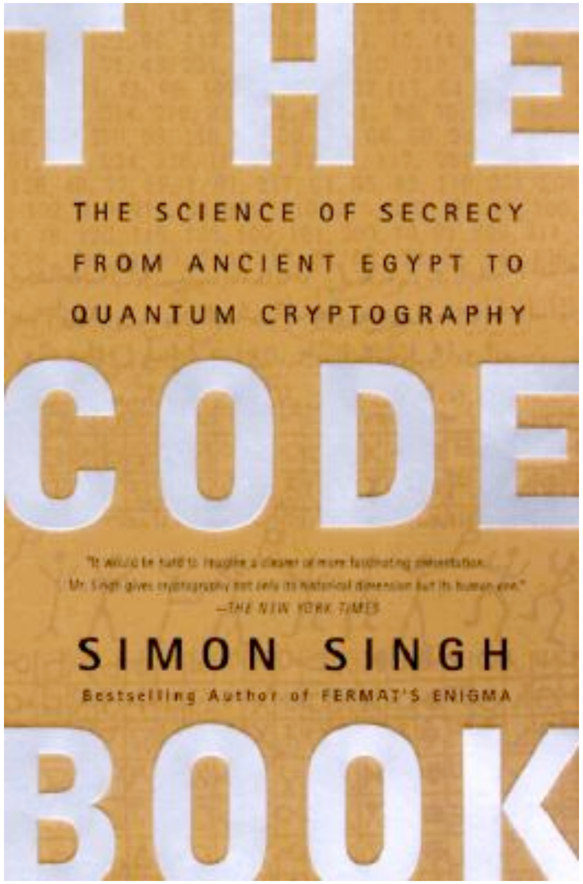
Classical Cryptography

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

Scytale

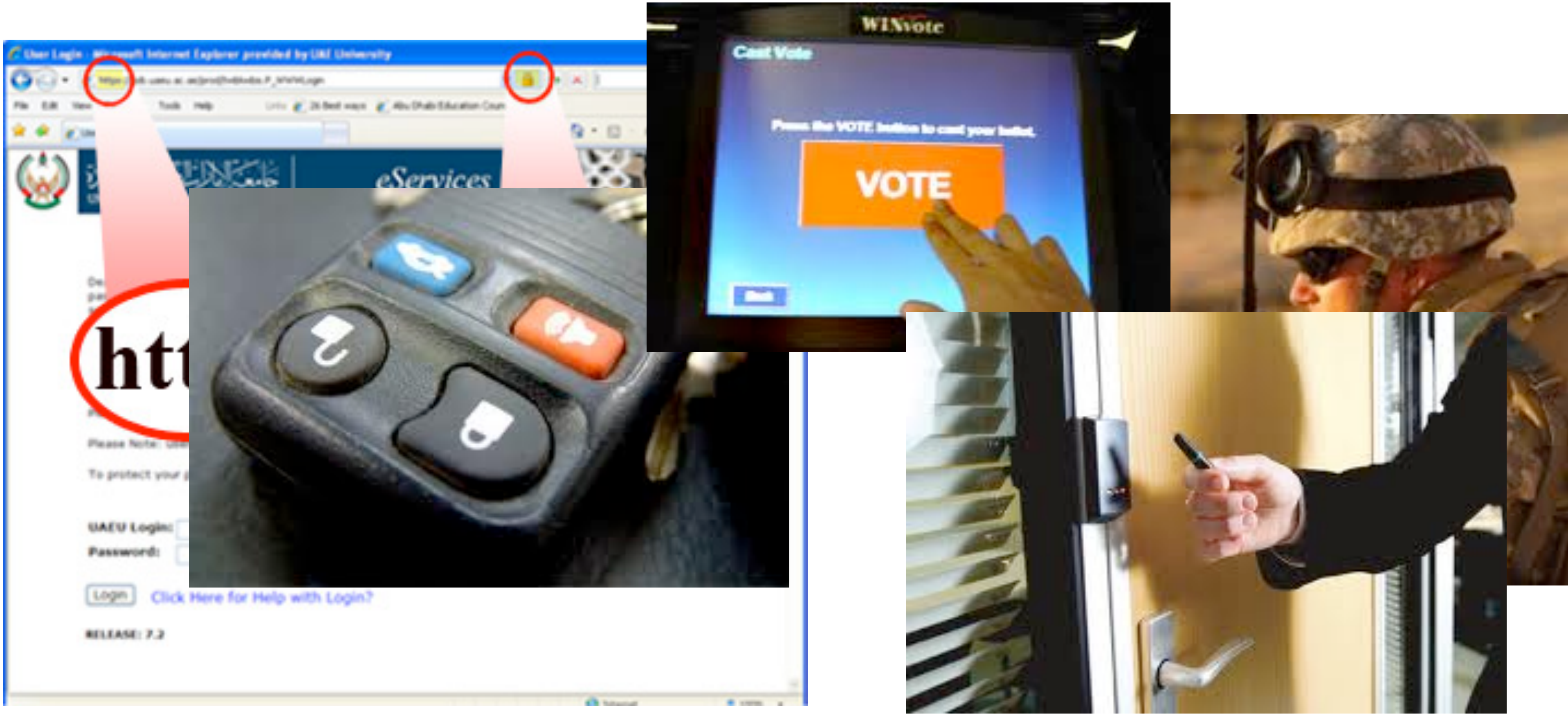


Enigma


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

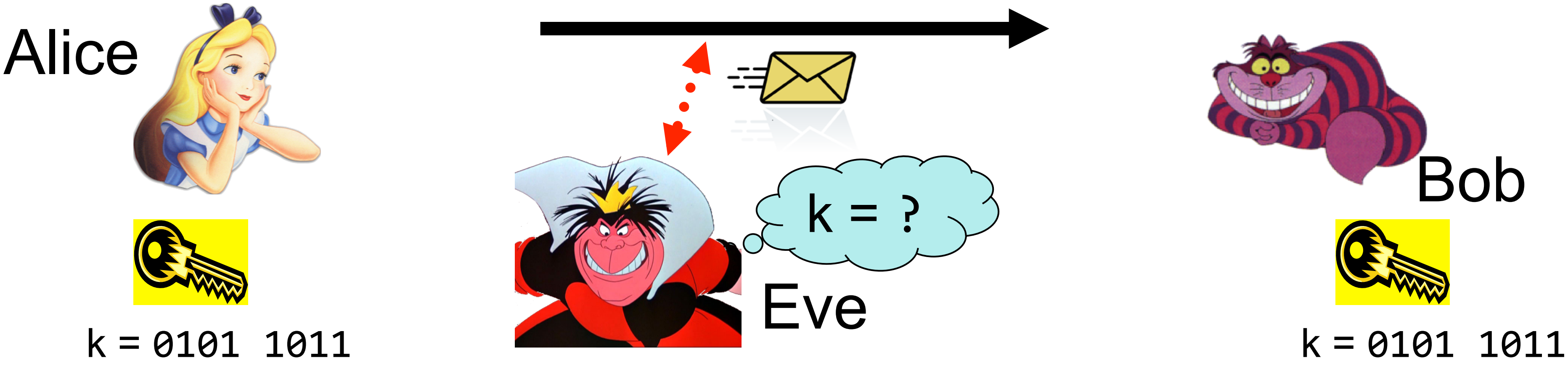
- is everywhere!
- is concerned with all settings where people do not trust each other


User Login - Microsoft Internet Explorer provided by UAE University
eServices
htt
UAEU Login:
Password:
Login
Click Here for Help with Login?
RELEASE: 7.2
WINvote
Cast Vote
Press the VOTE button to cast your ballot.
VOTE
Back

Secure Encryption

m = ‘I love you’

0000 1011



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

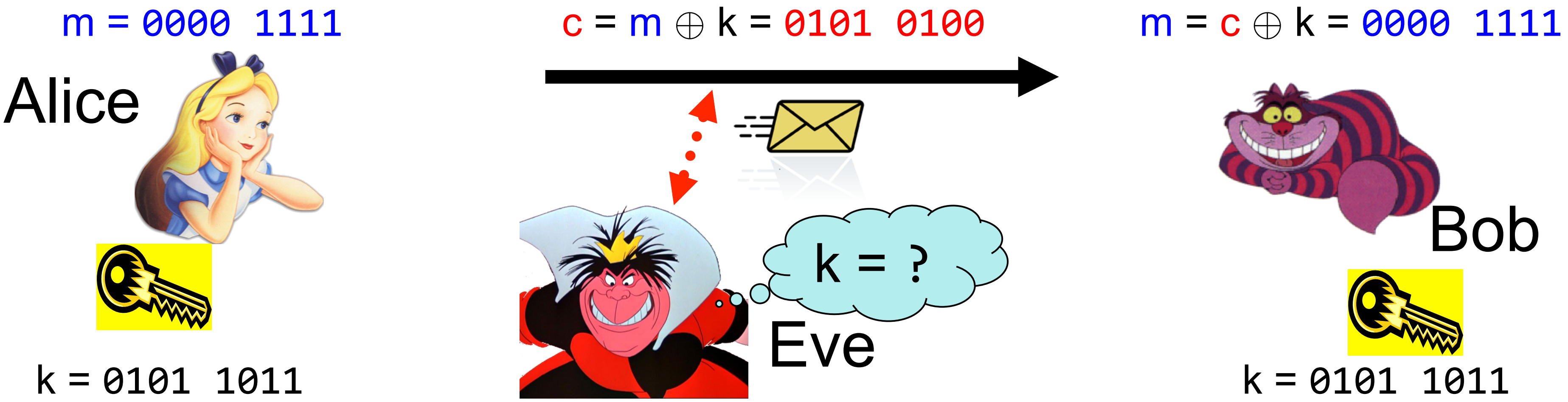
eXclusive OR (XOR) Function

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

- Some properties:
  - $\forall x : x \oplus 0 = x$
  - $\forall x : x \oplus x = 0$

$\Rightarrow \forall x,y : x \oplus y \oplus y = x$

One-Time Pad Encryption



$m = 0000\ 1111$

Alice

$k = 0101\ 1011$

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

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

Bob

$k = 0101\ 1011$

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

$m = 0000\ 1111$

$k = 0101\ 1011$

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

$c = 0101\ 0100$

$k = 0101\ 1011$

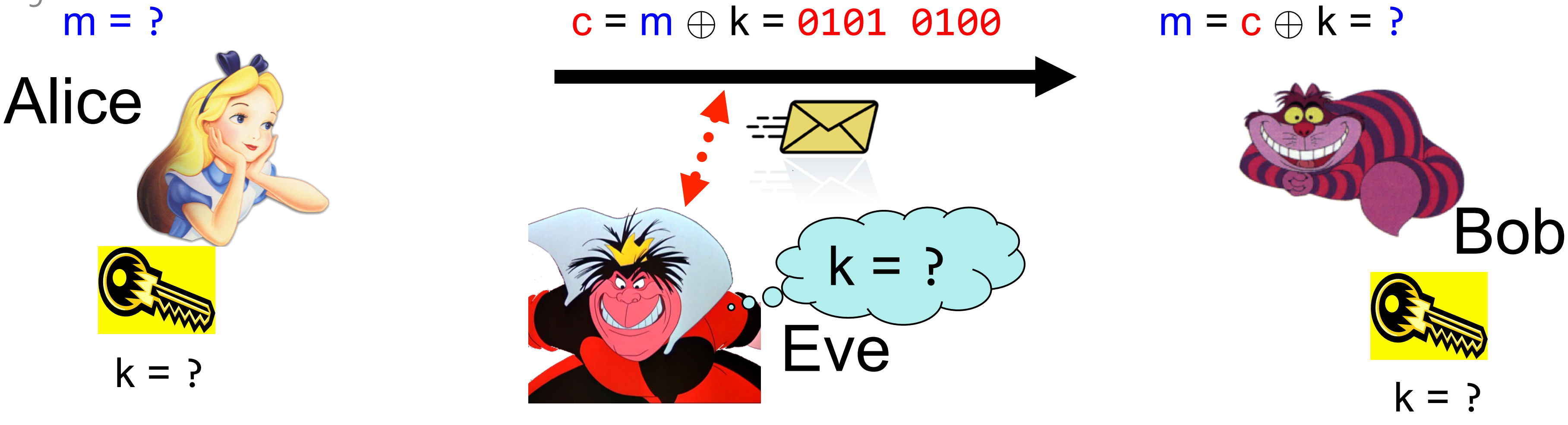
$c \oplus k = 0000\ 1111$

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

x	y	x ⊕ y
0	0	0
0	1	1
1	0	1
1	1	0

- Is it secure?

Perfect Security



$m = ?$

Alice

$k = ?$

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

Eve

$k = ?$

$m = c \oplus k = ?$

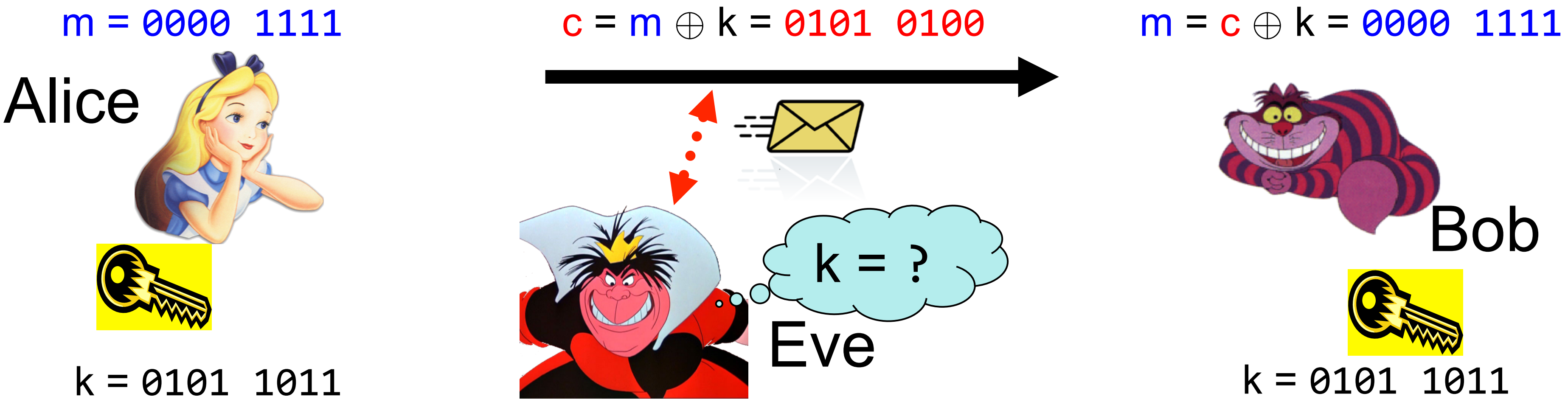
Bob

$k = ?$

- 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

Problems With One-Time Pad



m = 0000 1111

$c = m \oplus k =$ 0101 0100

$m = c \oplus k =$ 0000 1111

Alice

Eve

k = ?

Bob

k = 0101 1011

k = 0101 1011

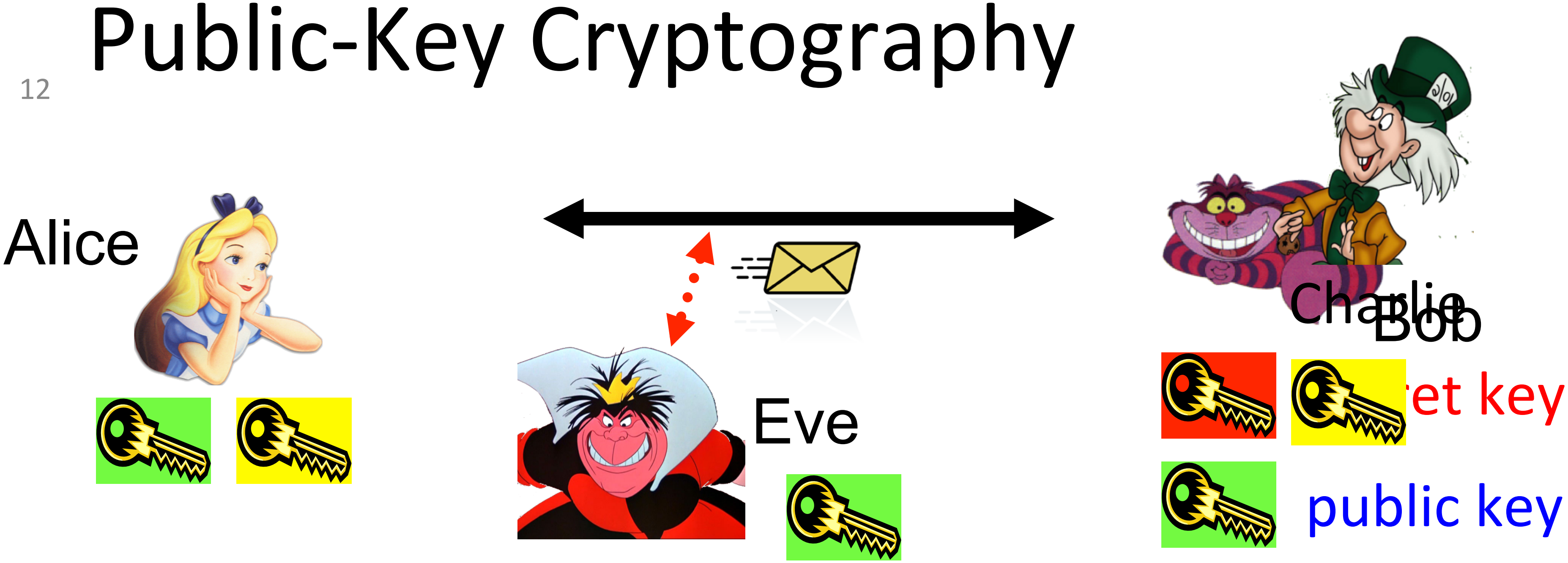
- The key has to be as long as the message.
- The key can only be used once.
- In practice, other encryption schemes (such as AES) are used which allow to encrypt long messages with short keys.
- One-time pad does not provide authentication:
  Eve can easily flip bits in the message

Symmetric-Key Cryptography

Alice
Eve
Bob

- Encryption ensures secrecy:
  Eve does not learn the message, e.g. one-time pad
- Authentication ensures integrity:
  Eve cannot alter the message
- General problem: players have to exchange a key to start with

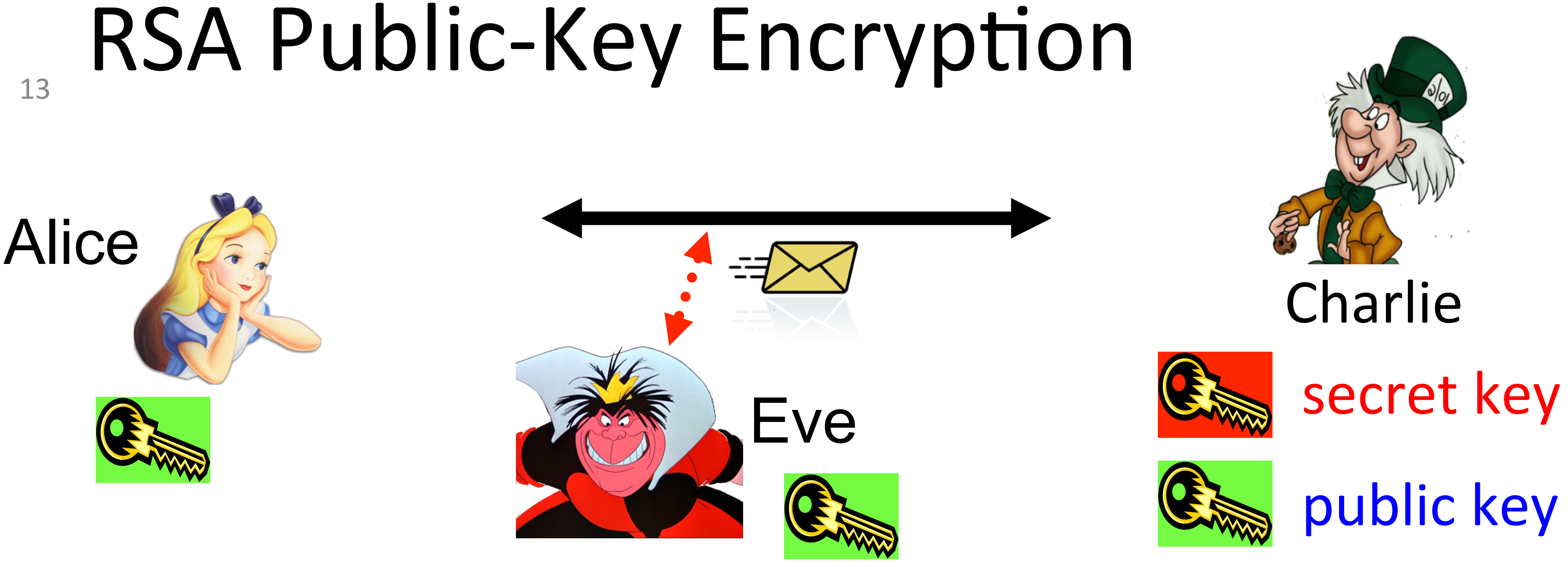
Public-Key Cryptography



- Solves the key-exchange problem.
- Everyone can encrypt using the public key.
- Only the holder of the secret key can decrypt.

- Digital signatures: Only secret-key holder can sign, but everyone can verify signatures using the public-key.

RSA Public-Key Encryption



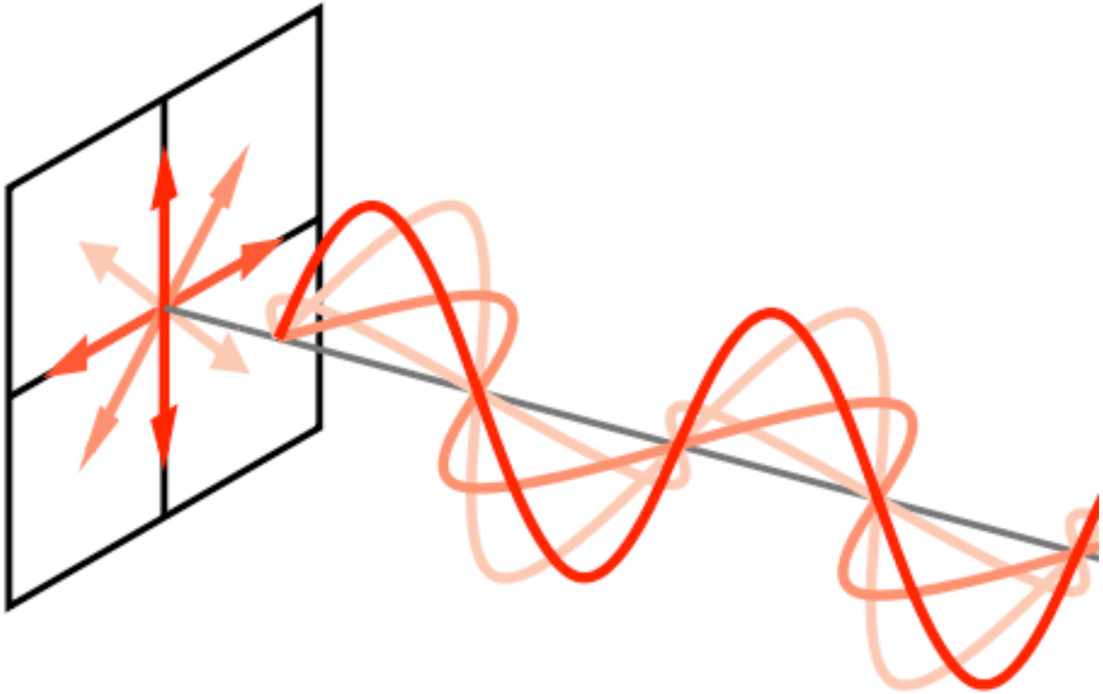
- Key generation: pick two large primes p and q, set $N=p*q$
- public key: $N, e \in Z_N^*$, secret key: $d = e^{-1} \bmod \phi(N)$
- $Enc_{pk}(m) = m^e \bmod N$
- $Dec_{sk}(c) = c^d \bmod N$
- security relies on the difficulty of factoring N, because $\phi(N)=(p-1)(q-1)$

What will you Learn from this Talk?

- ✓ Classical Cryptography
- Quantum Mechanics
- Quantum Key Distribution
- Position-Based Cryptography

Quantum Mechanics (of Photons)

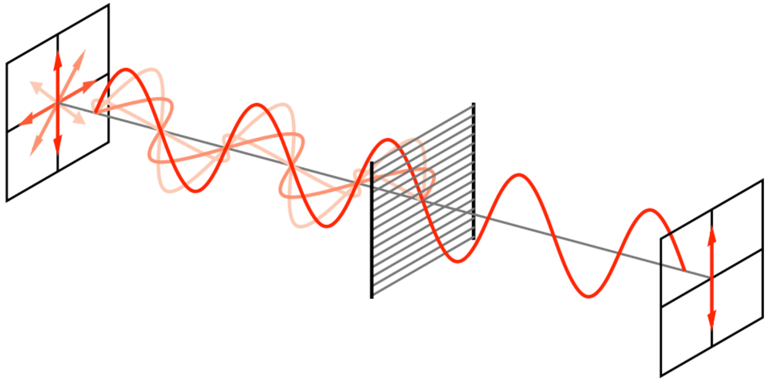
✥	$+$ basis	↔	$|0\rangle_+$	↕	$|1\rangle_+$
✕	$\times$ basis	⤢	$|0\rangle_\times$	⤡	$|1\rangle_\times$



Quantum Mechanics

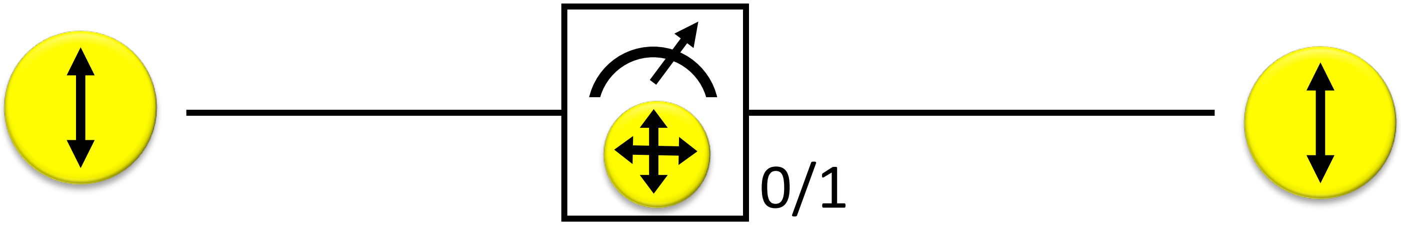
✥ + basis ↔ $|0\rangle_+$ ↕ $|1\rangle_+$

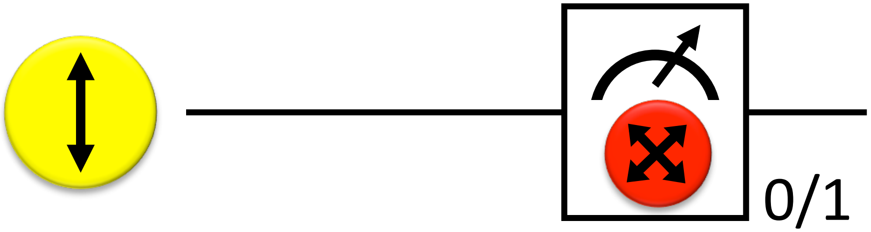
⤧ × basis ⤢ $|0\rangle_\times$ ⤡ $|1\rangle_\times$



Measurements:

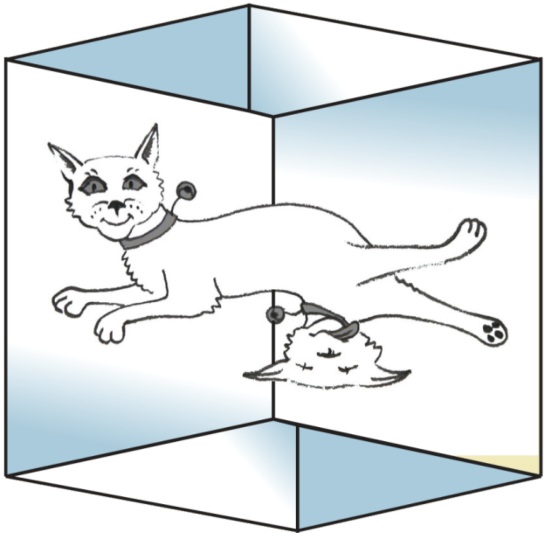
with prob. 1 yields 1

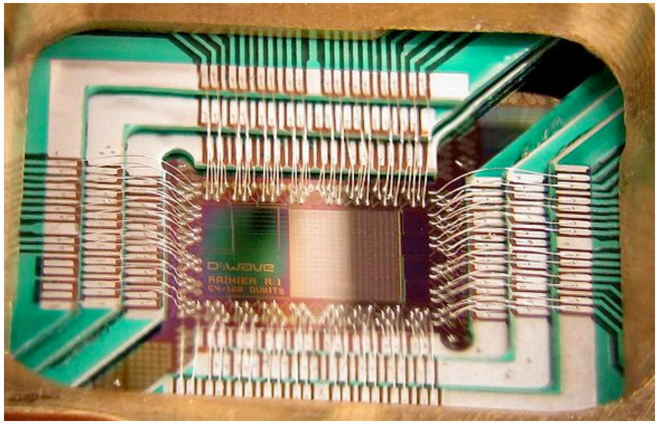




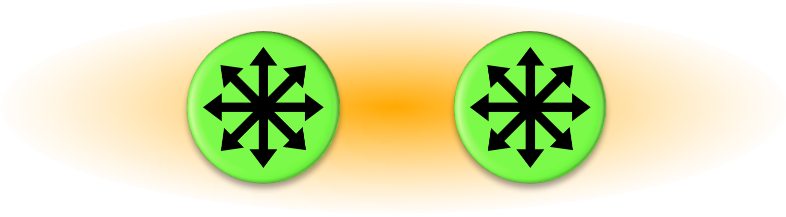
with prob. ½ yields 0 ⤢

with prob. ½ yields 1 ⤡



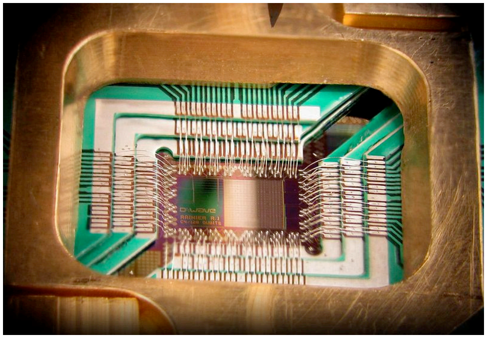


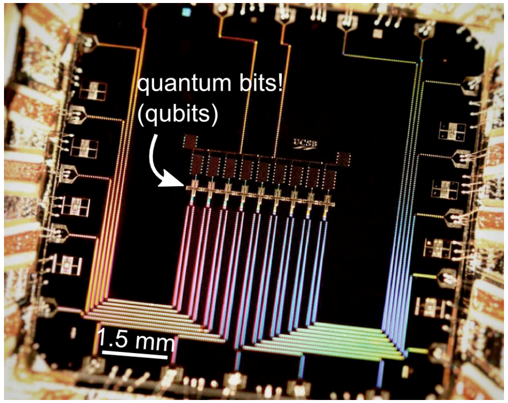
Wonderland of Quantum Mechanics



Can We Build Quantum Computers?

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



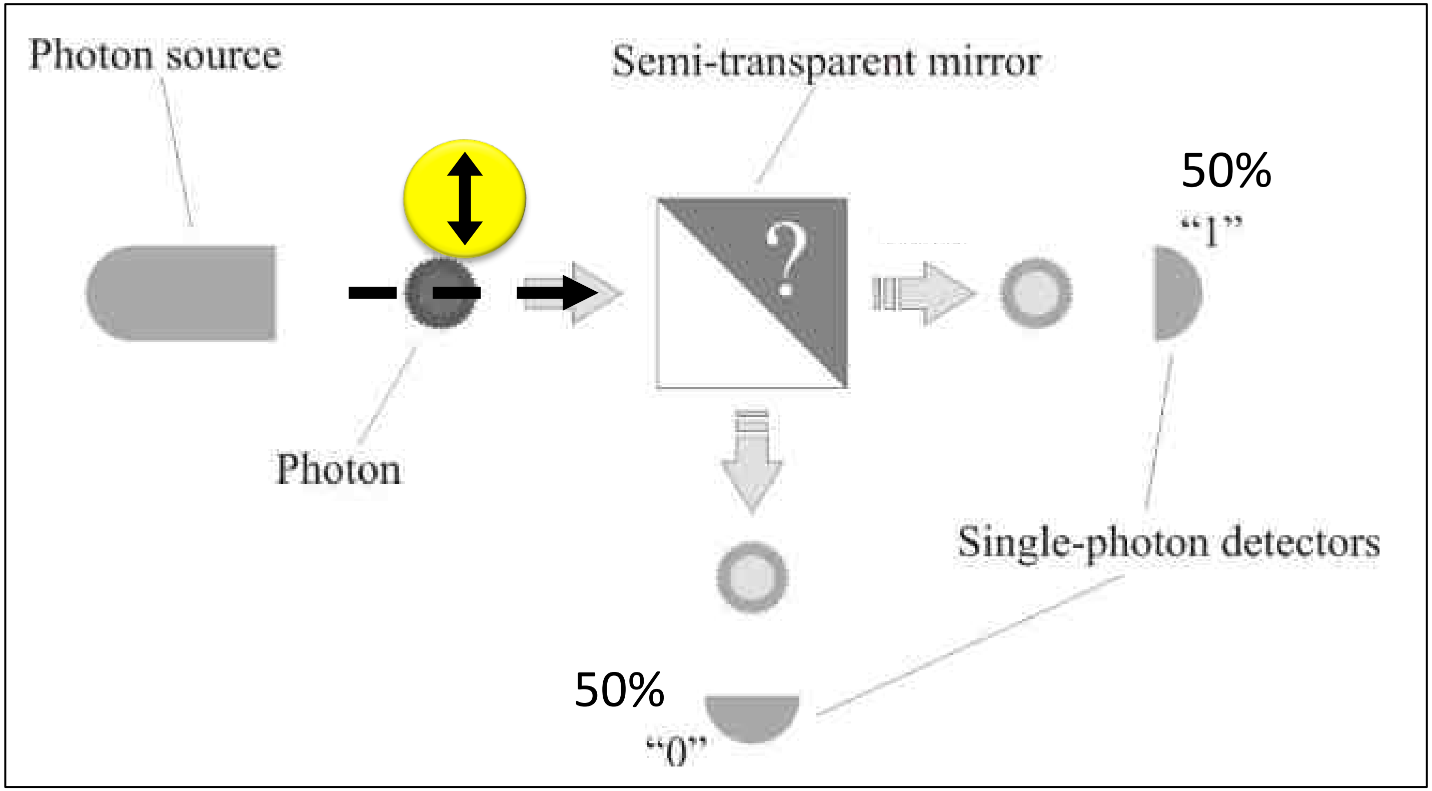


Martinis group (UCSB)
9 qubits

- Canadian company “D-Wave” claims to have build one. Did they?
- 2014: Martinis group “acquired” by Google
- 2014: 1.35 Mio € investment in QuTech centre in Delft

Demonstration of Quantum Technology

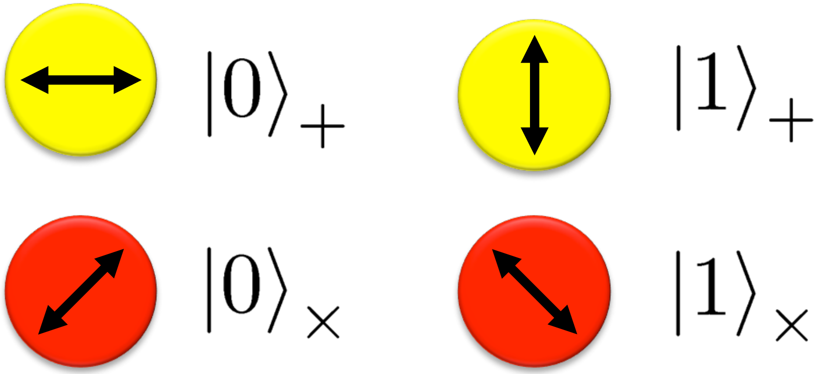
- generation of random numbers



(diagram from idQuantique white paper)

- no quantum computation, only quantum communication required

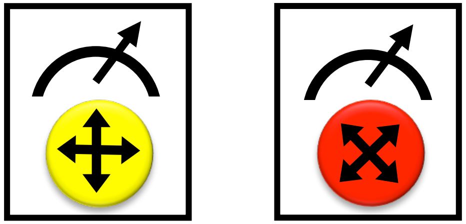
No-Cloning Theorem

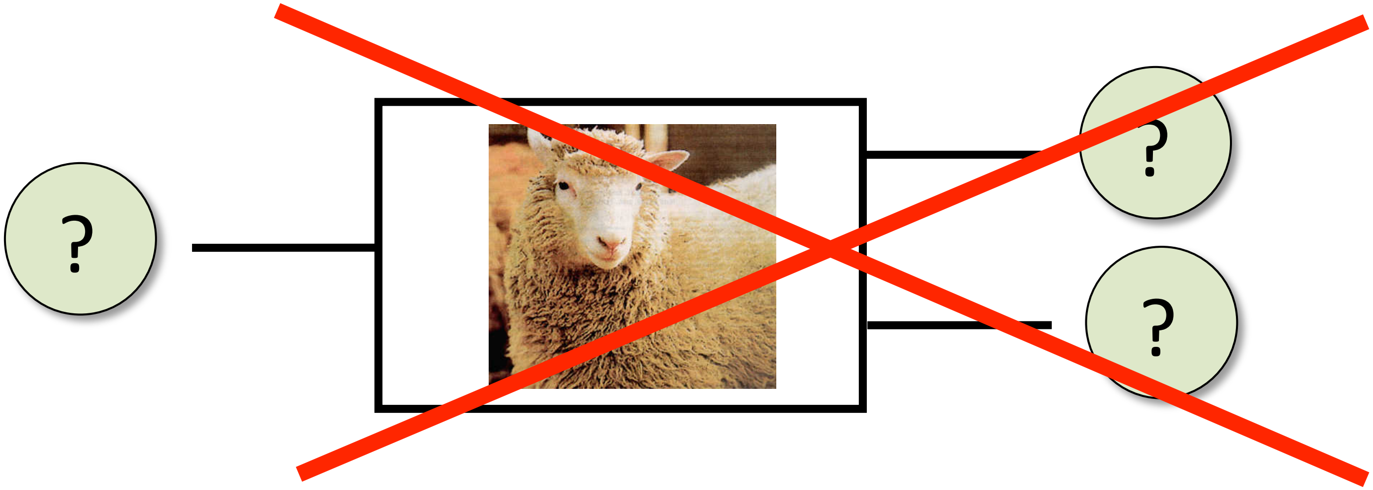


$|0\rangle_+$ $|1\rangle_+$

$|0\rangle_\times$ $|1\rangle_\times$

Quantum operations: $\boxed{U}$

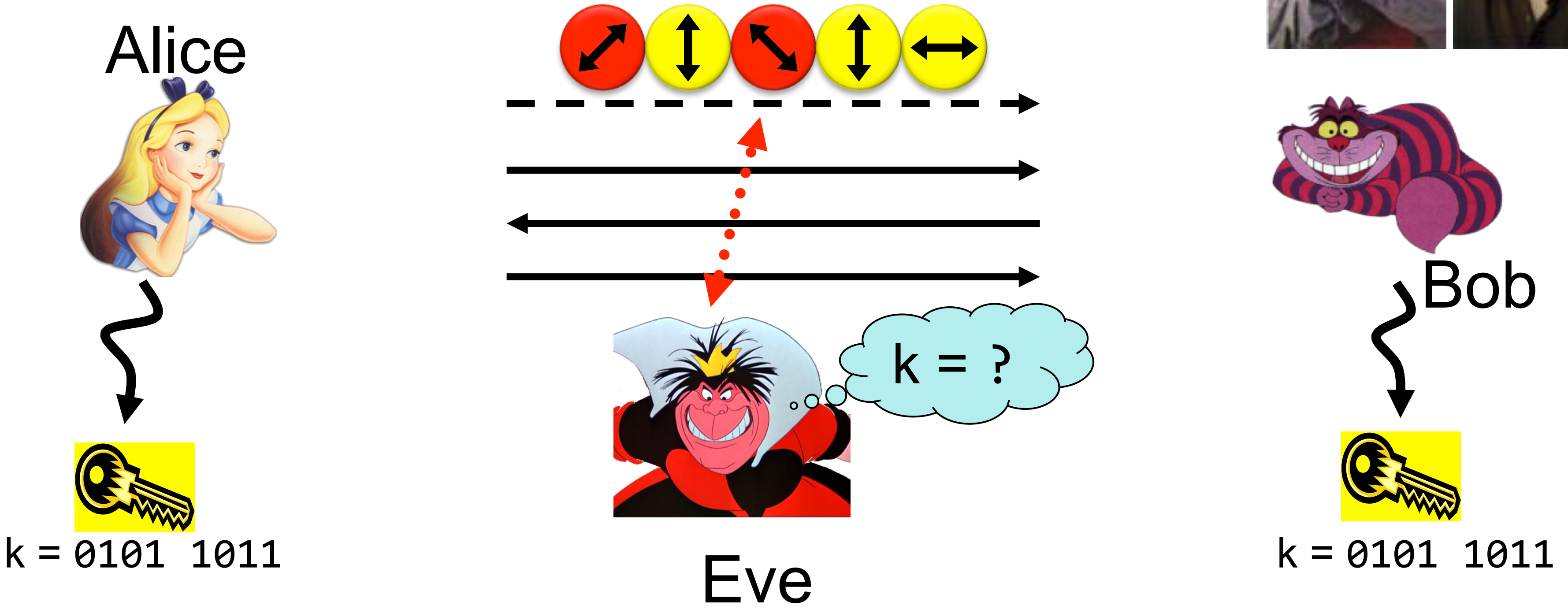




Proof: copying is a non-linear operation

Quantum Key Distribution (QKD)

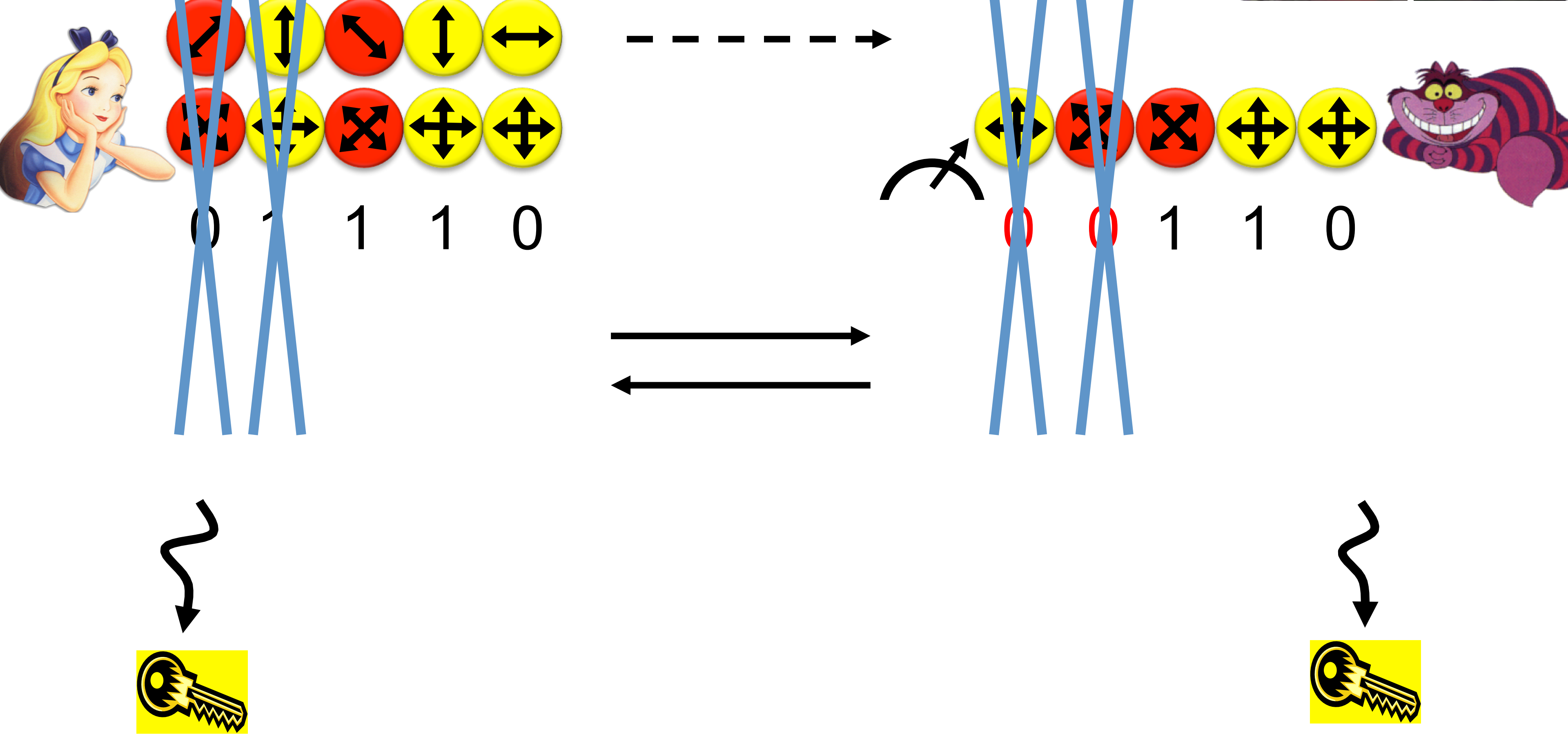
[Bennett Brassard 84]



- Offers a quantum solution to the key-exchange problem
- Puts the players into the starting position to use symmetric-key cryptography (encryption, authentication etc.).

Quantum Key Distribution (QKD)

[Bennett Brassard 84]

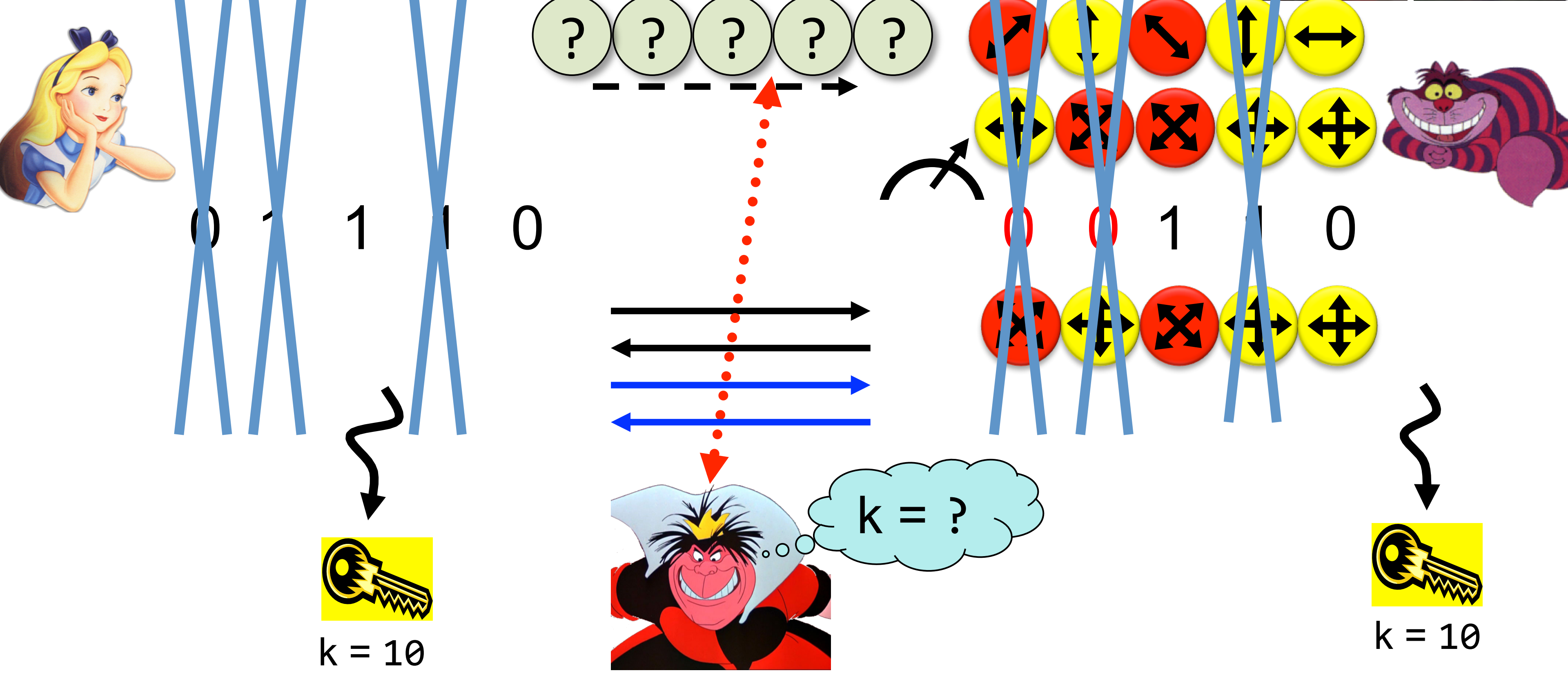


k = 110

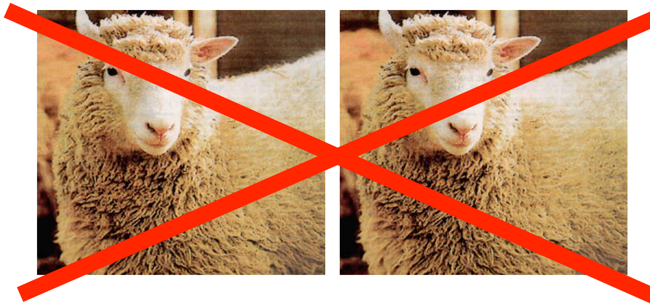
k = 110

Quantum Key Distribution (QKD)

[Bennett Brassard 84]

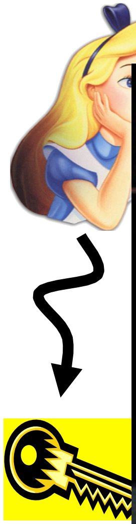


- Quantum states are unknown to Eve, she cannot copy them.
- Honest players can test whether Eve interfered.

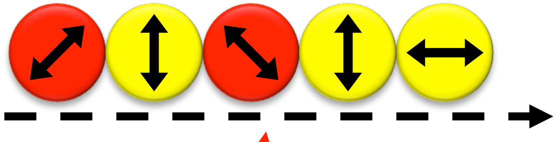


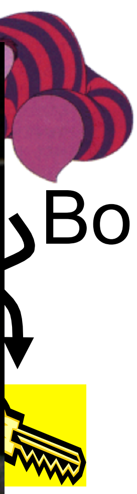
Quantum Key Distribution (QKD)

[Bennett Brassard 84]

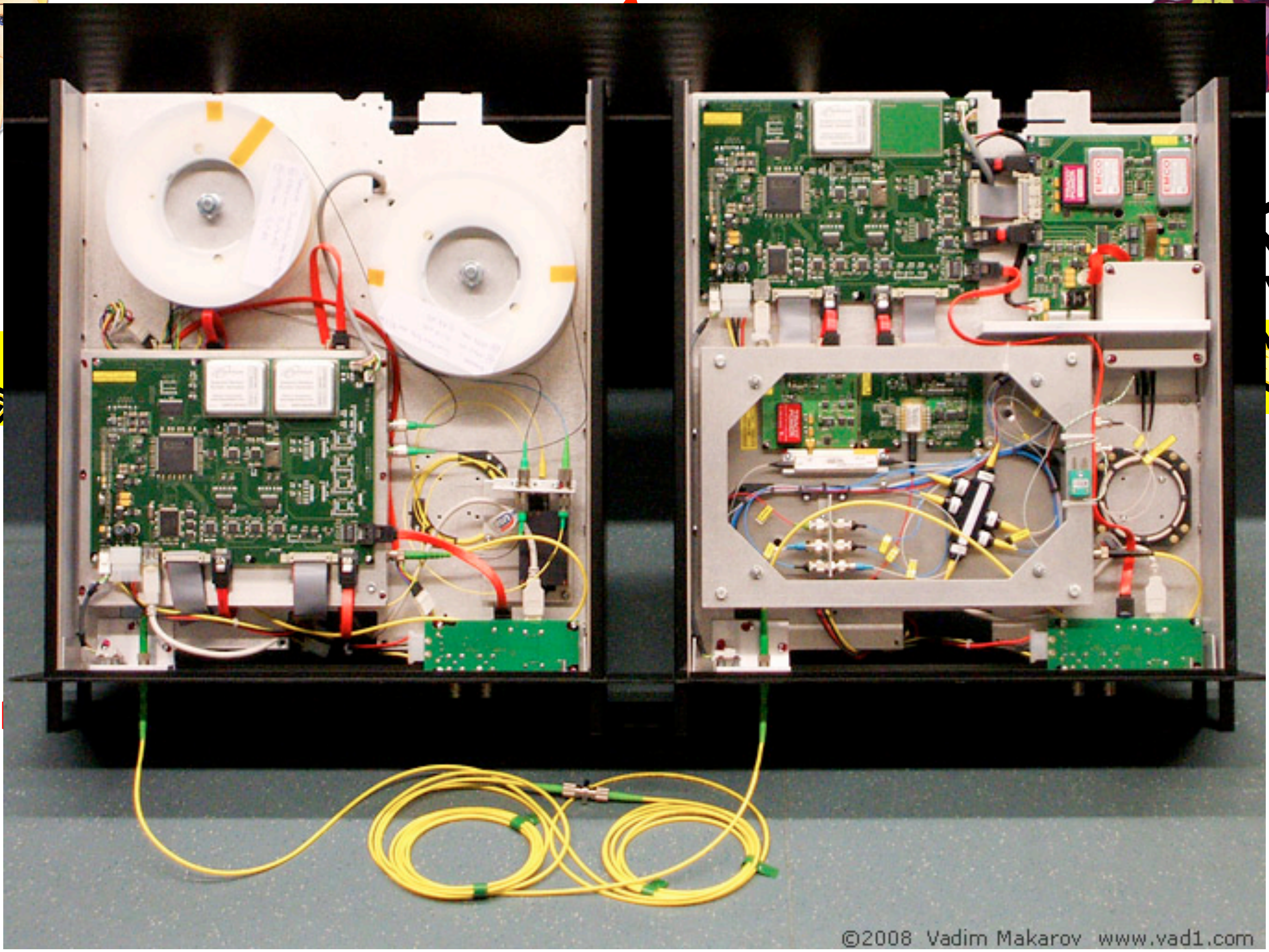


Alice





Bob



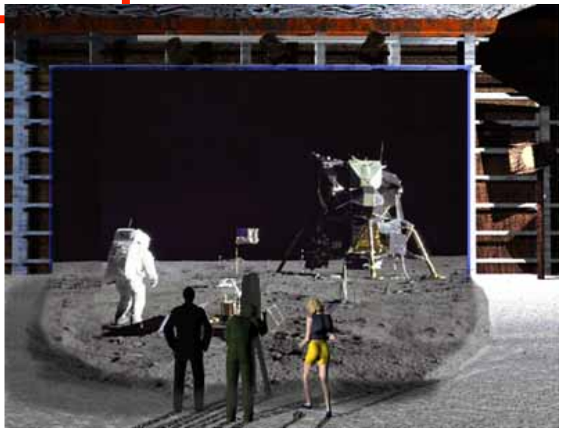
©2008 Vadim Makarov www.vad1.com

- techn

  only

What will you Learn from this Talk?

- ✓ Classical Cryptography
- ✓ Quantum Mechanics
- ✓ Quantum Key Distribution
- Position-Based Cryptography



Position-Based Cryptography

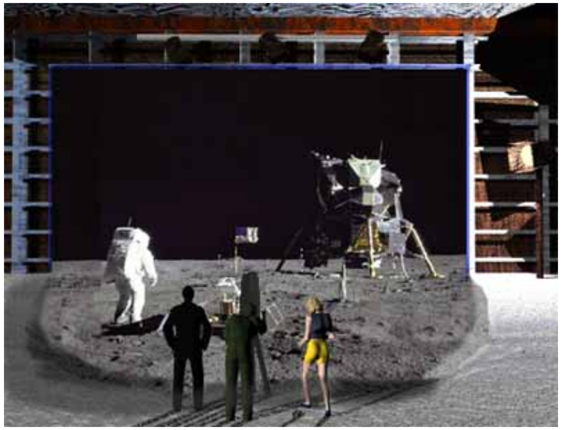
- Typically, cryptographic players use credentials such as
  - secret information (e.g. password or secret key)
  - authenticated information
  - biometric features

Can the geographical location of a player be used as cryptographic credential ?

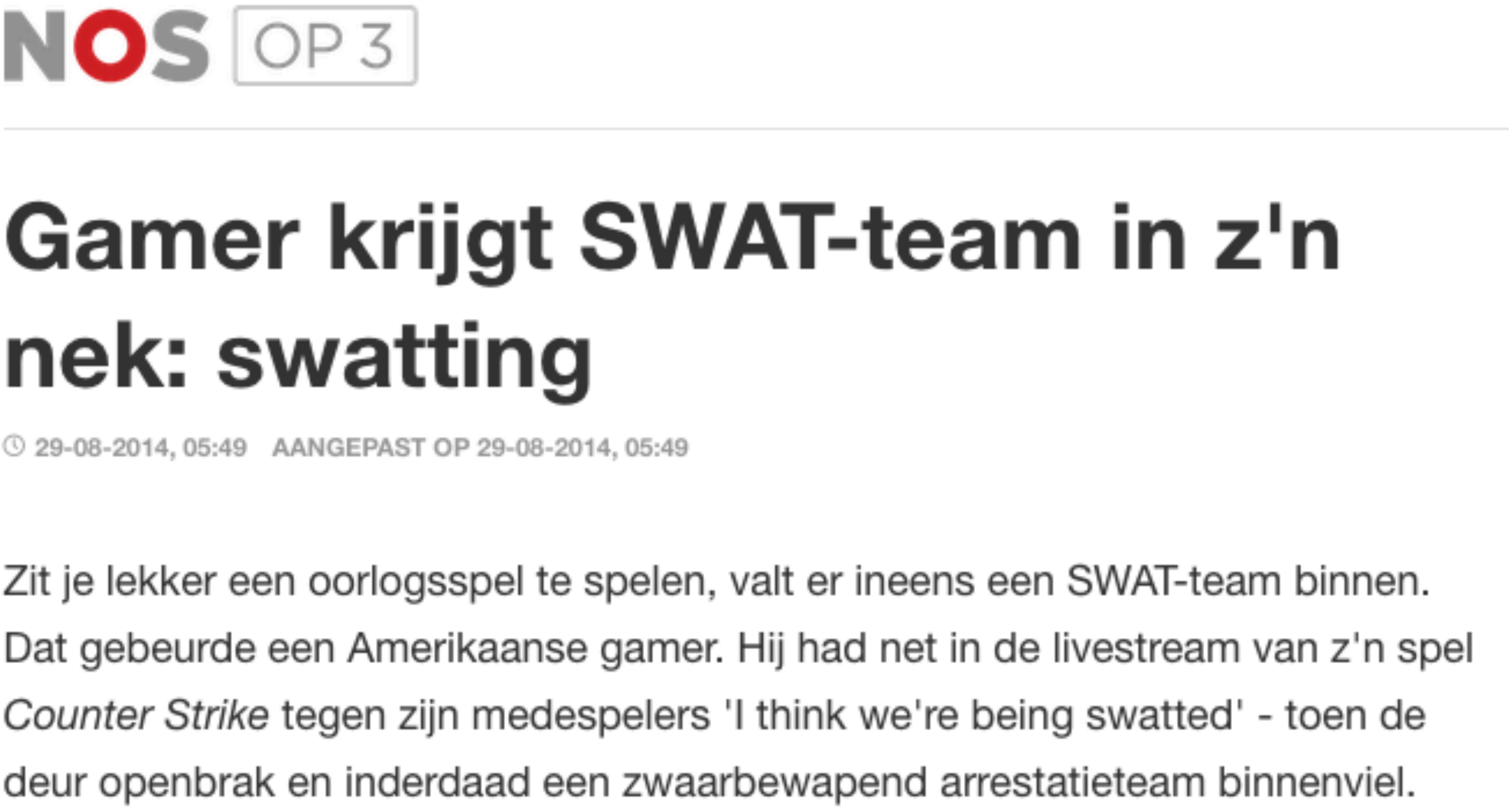
Position-Based Cryptography

Can the geographical location of a player be used as sole cryptographic credential ?

- Possible Applications:
  - Launching-missile command comes from within the military headquarters
  - Talking to the correct country
  - Pizza-delivery problem / avoid fake calls to emergency services
  - …



Position-Based Cryptography



NOS OP 3

Gamer krijgt SWAT-team in z'n nek: swatting

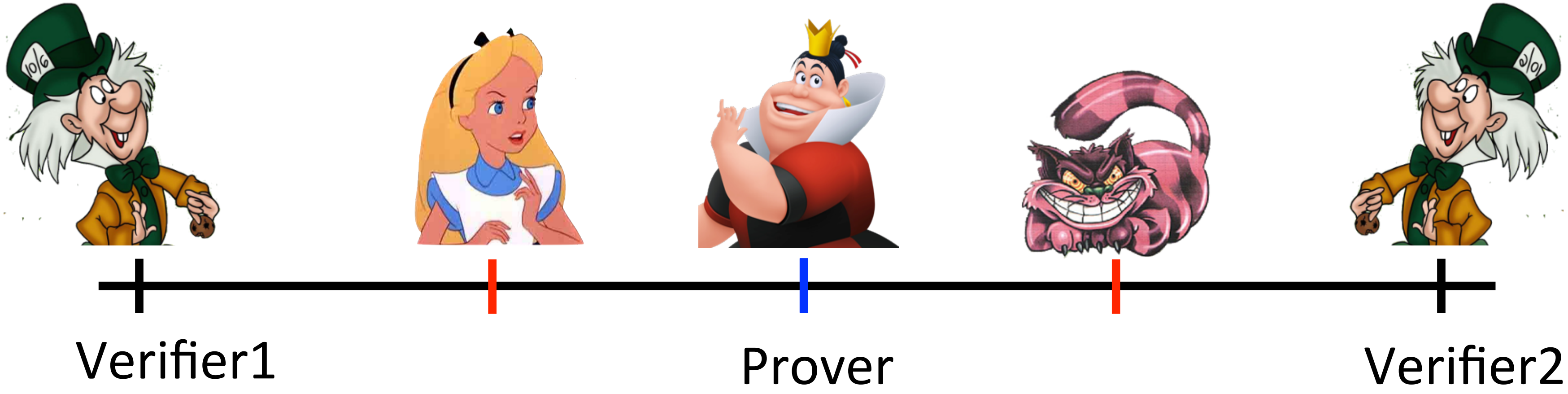
29-08-2014, 05:49 AANGEPAST OP 29-08-2014, 05:49

Zit je lekker een oorlogsspel te spelen, valt er ineens een SWAT-team binnen. Dat gebeurde een Amerikaanse gamer. Hij had net in de livestream van z'n spel *Counter Strike* tegen zijn medespelers 'I think we're being swatted' - toen de deur openbrak en inderdaad een zwaarbewapend arrestatieteam binnenviel.

Dat was allemaal live te zien op de webcam:

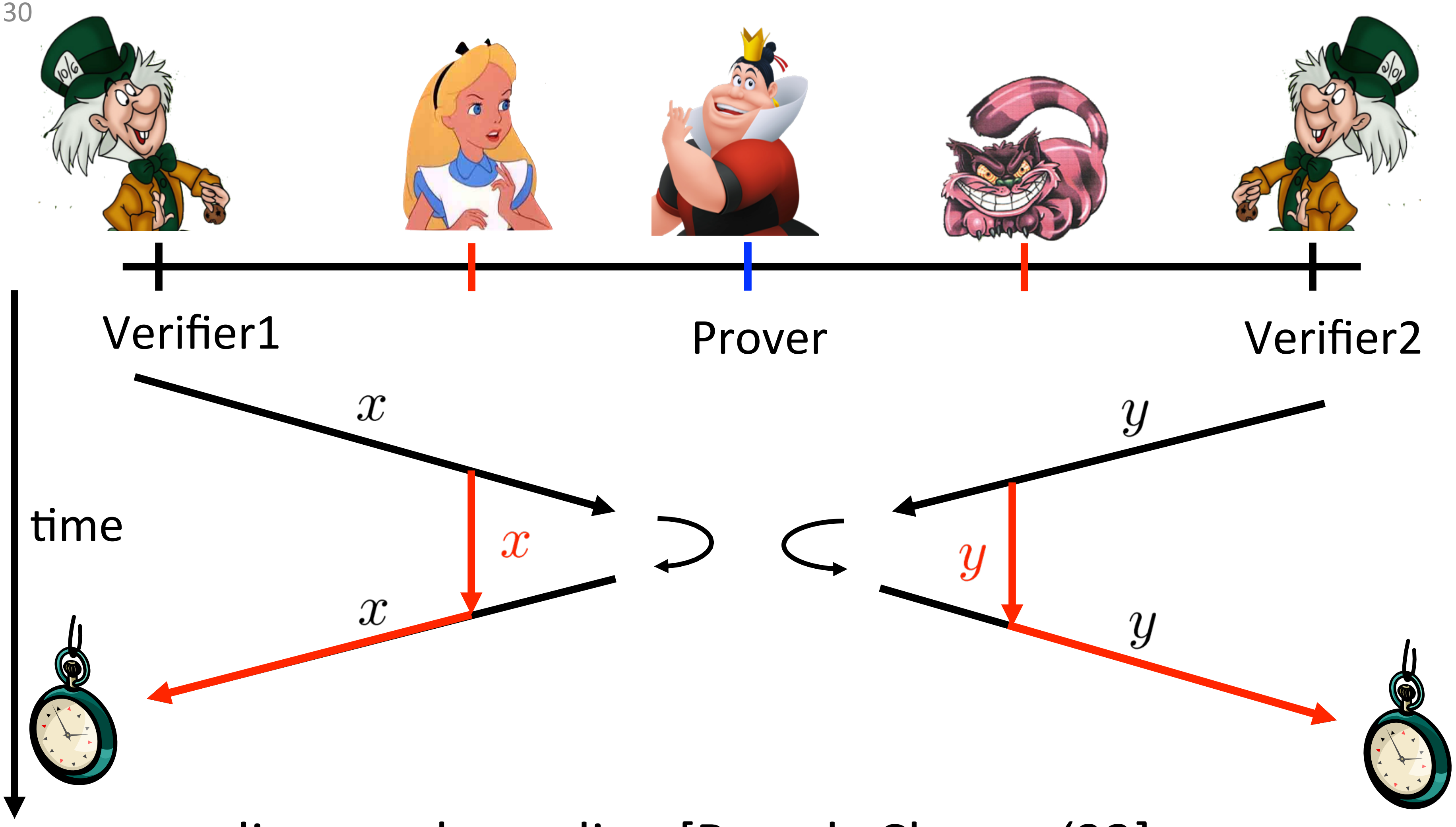
https://youtu.be/TiW-BVPCbZk?t=117

Basic task: Position Verification



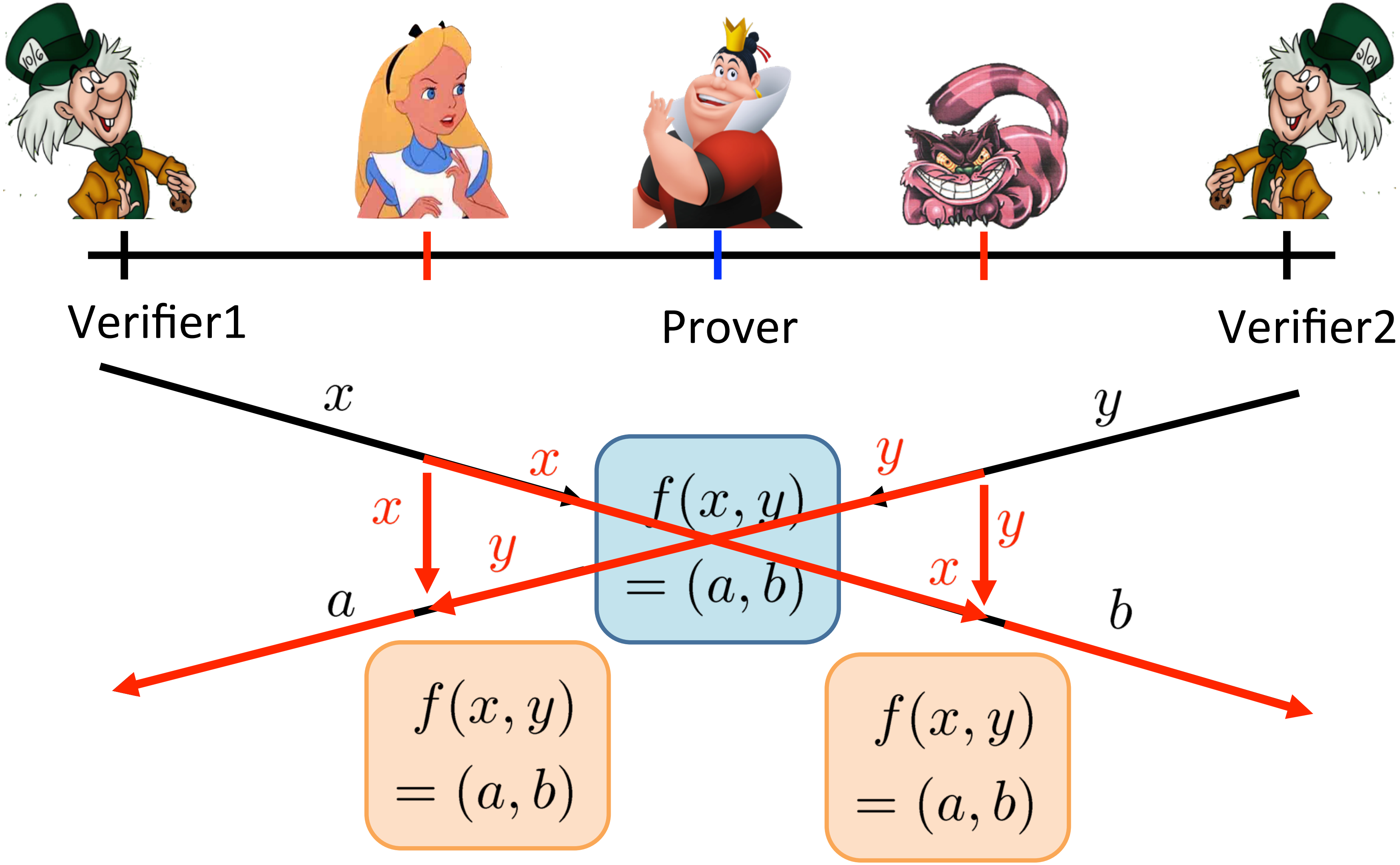
- Prover wants to convince verifiers that she is at a particular position
- no coalition of (fake) provers, i.e. not at the claimed position, can convince verifiers
- assumptions:
  - communication at speed of light
  - instantaneous computation
  - verifiers can coordinate

Position Verification: First Try



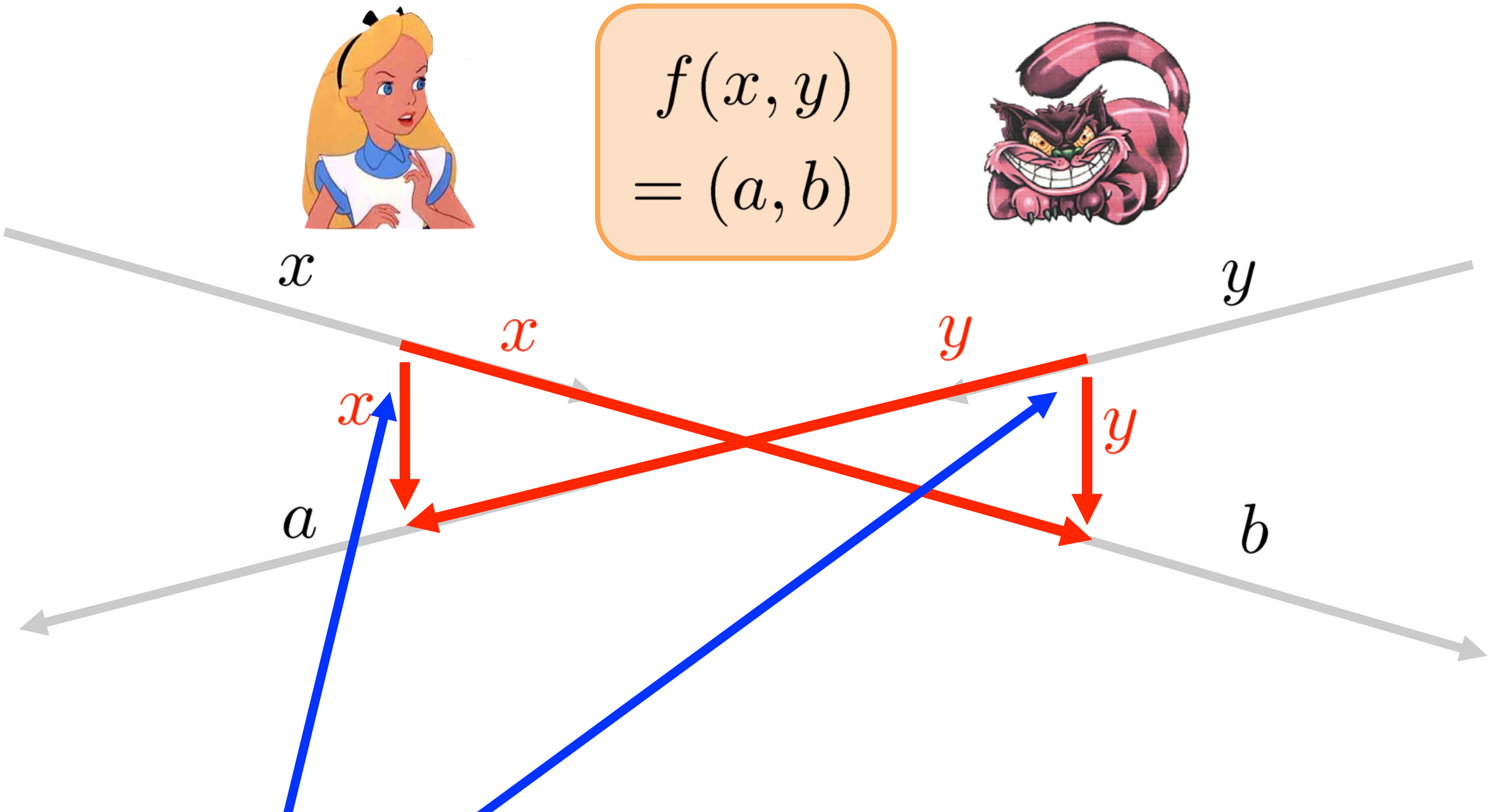
- distance bounding [Brands Chaum '93]

Position Verification: Second Try



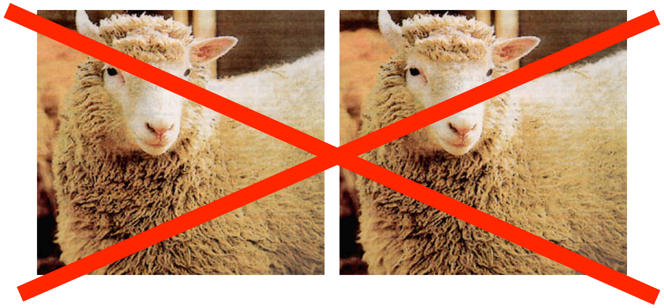
position verification is classically impossible !

The Attack



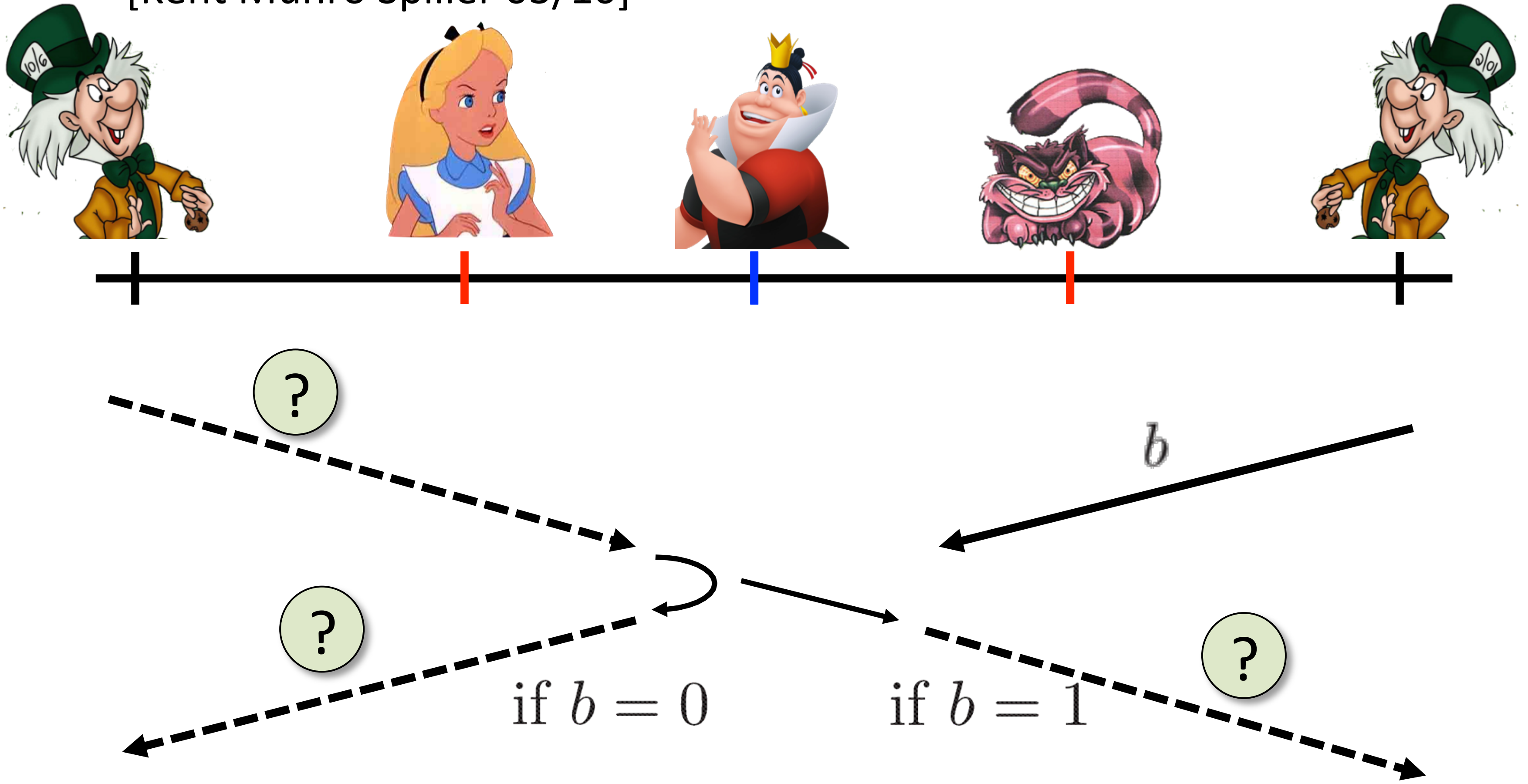
$f(x,y)$
$= (a,b)$

- copying classical information
- this is impossible quantumly



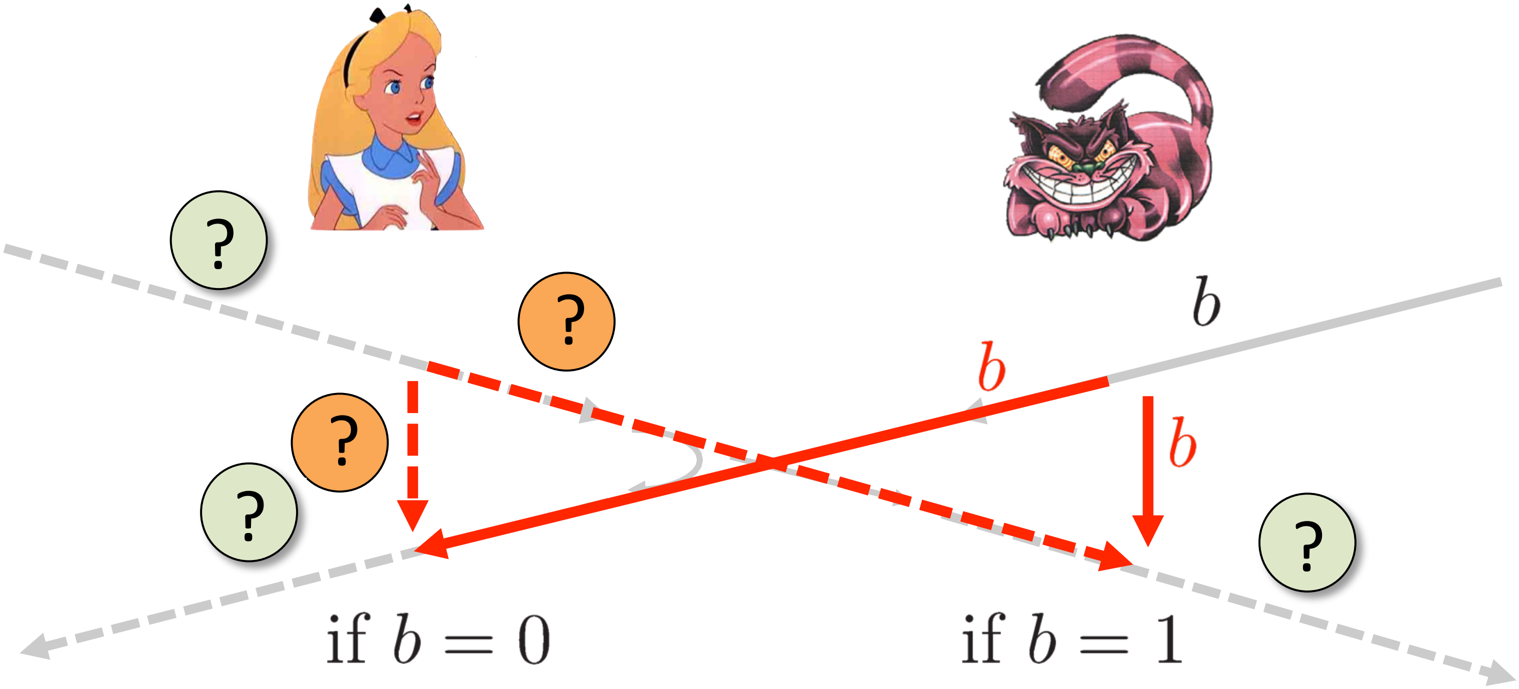
Position Verification: Quantum Try

[Kent Munro Spiller 03/10]

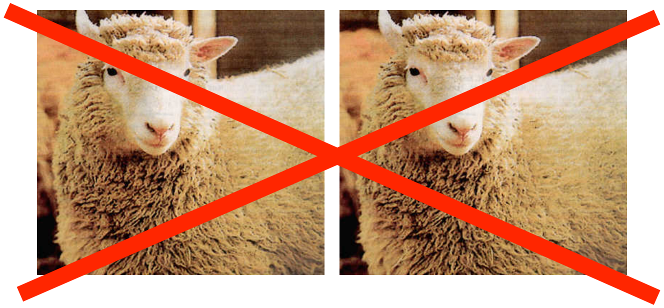


- Can we brake the scheme now?

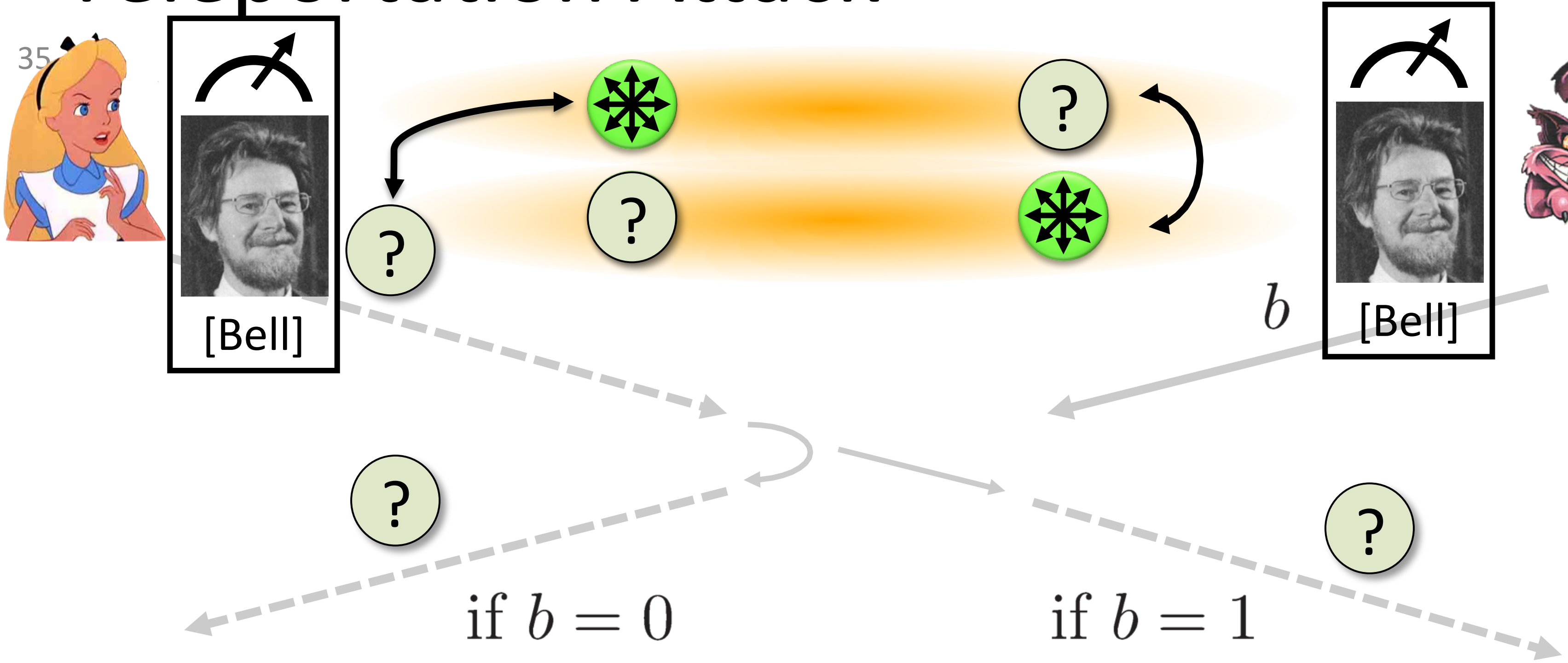
Attacking Game



- Impossible to cheat due to non-cloning theorem
- Or not?



Teleportation Attack



- It is possible to cheat with entanglement !!
- Quantum teleportation allows to break the protocol perfectly.

No-Go Theorem

[Buhrman, Chandran, Fehr, Gelles, Goyal, Ostrovsky, Schaffner 2010]

- Any position-verification protocol can be broken using an exponential number of entangled qubits.

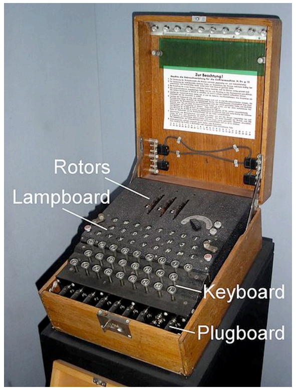
- Question: Are so many quantum resources really necessary?

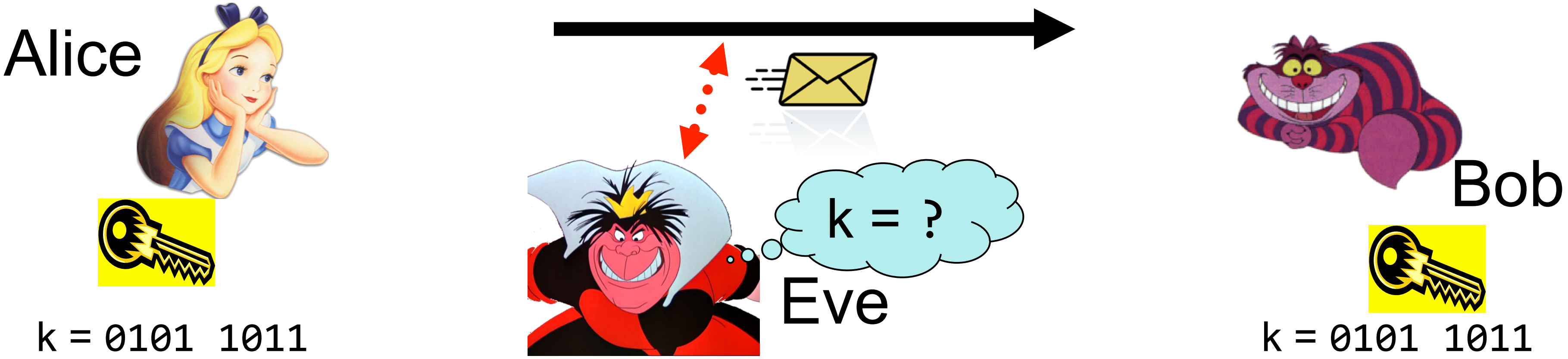
- Does there exist a protocol such that:
  - honest prover and verifiers are efficient, but
  - any attack requires lots of entanglement

What Have You Learned from this Talk?

✓ Classical Cryptography

- Long history
- One-time pad





m = 0000 1111

c = m ⊕ k = 0101 0100

Alice

k = 0101 1011

Eve

k = ?

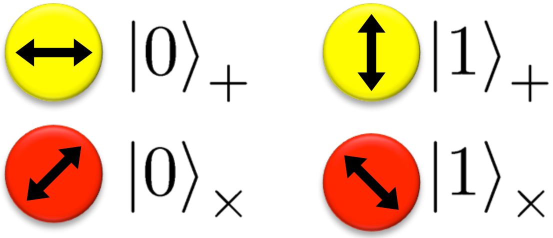
Bob

k = 0101 1011

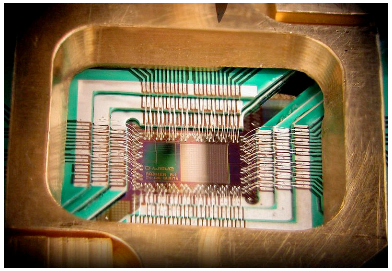
- Public-key cryptography

What Have You Learned from this Talk?

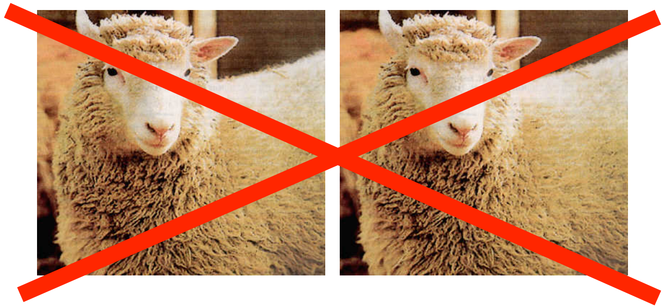
✓ Quantum Mechanics



- Qubits
- Quantum Computer



- No-cloning

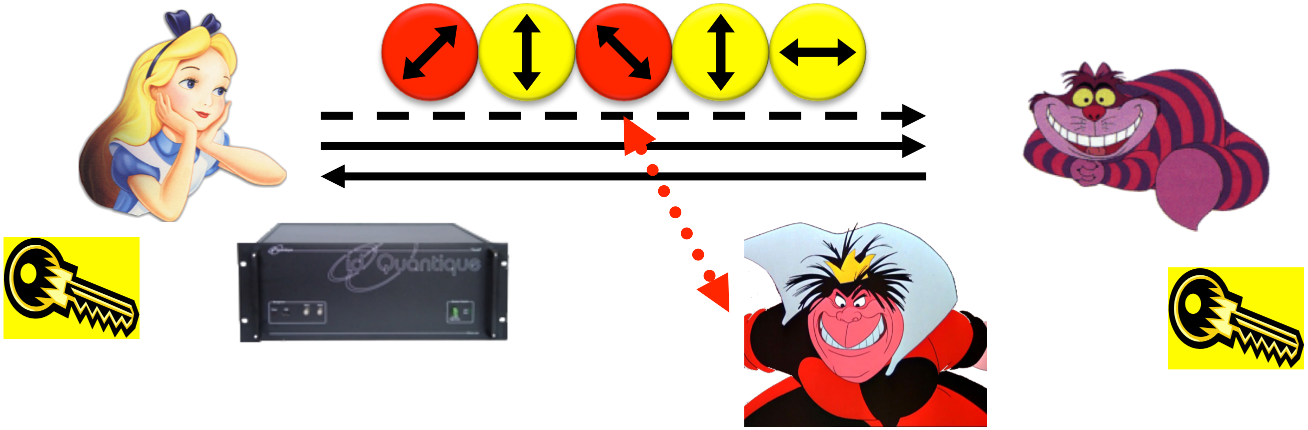


- Entanglement

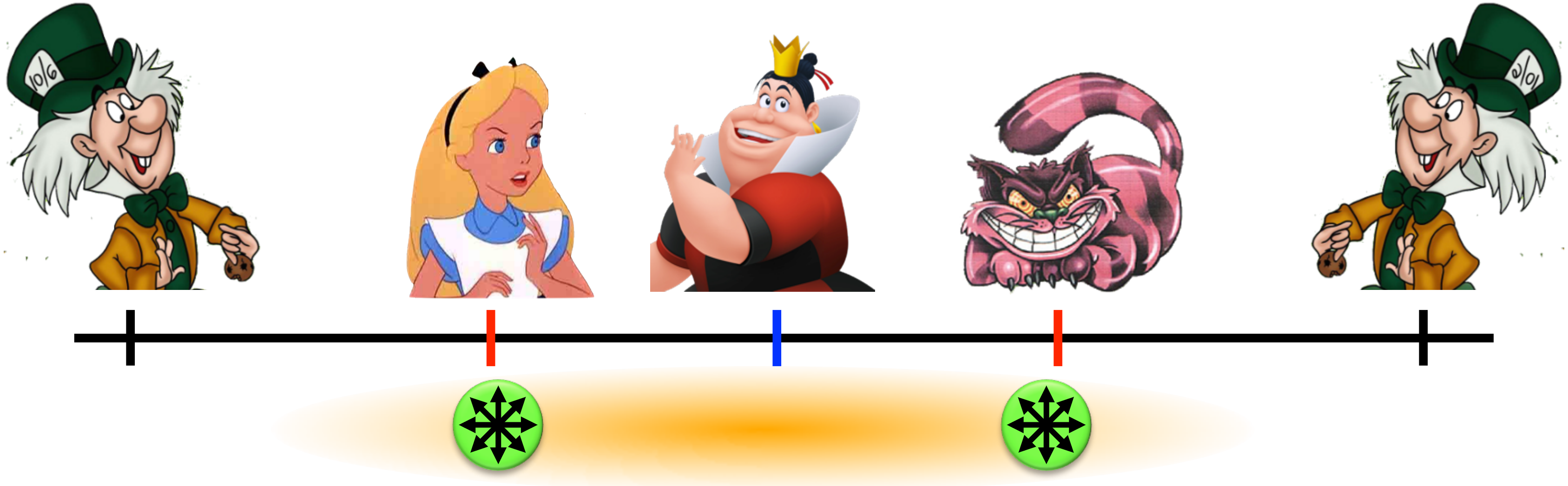
- Quantum Teleportation

What Have You Learned from this Talk?

✓ Quantum Key Distribution (QKD)



✓ Position-Based Cryptography



Thank you for your attention!

Questions