Quantum Cryptography

Christian Schaffner

Research Center for Quantum Software

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

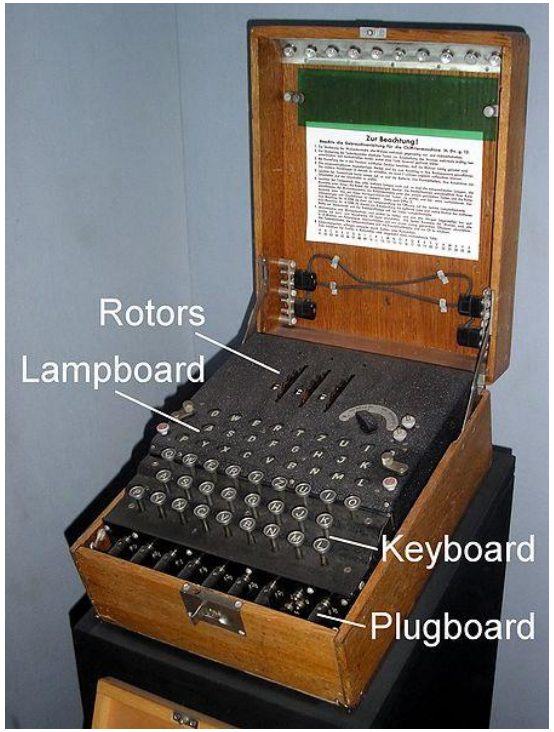
Logic, Language and Computation
Monday, 24 September 2018

Nederlandse Organisatie voor Wetenschappelijk Onderzoek

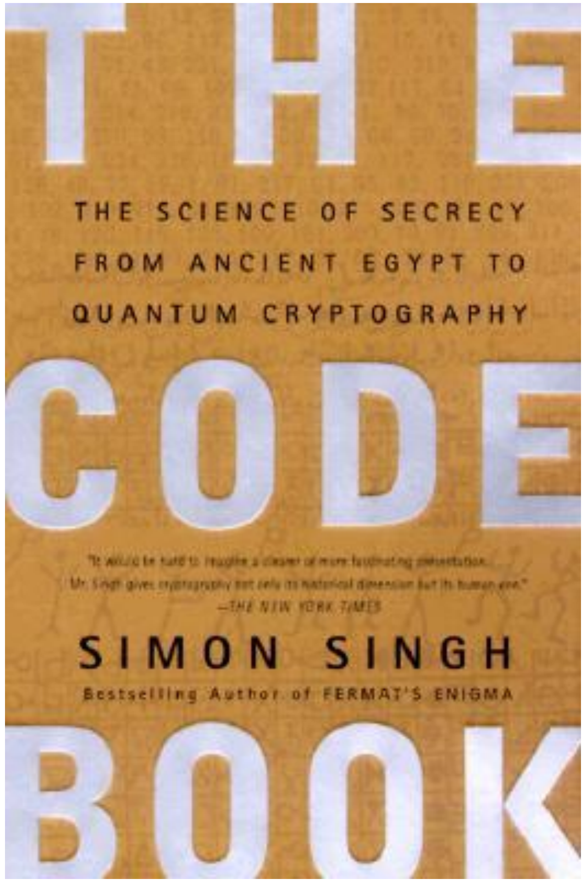
Classical Cryptography

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

[Scytale]



[Enigma]



Modern Cryptography

Edward Snowden

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

What will you Learn from this Talk?

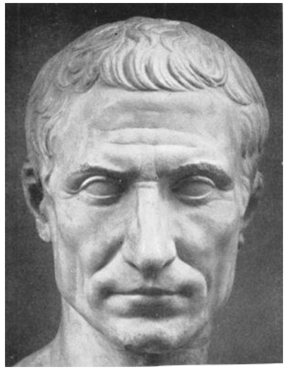
- Classical Cryptography (& Politics)
- Quantum Mechanics
- Crypto Threat of Quantum Computing
- Quantum Cryptography
- Quantum Future

Ancient Cryptography

Scytale

Blaise de Vigenère

500 BC | 50 BC | 500 AD | 1000 AD | 1500 AD | 2015 AD



Caesar Cipher (ROT4)
(variant still in use)

QuSoft

Additional Hints (Decrypt)

baqre jngre / nna xrggvat

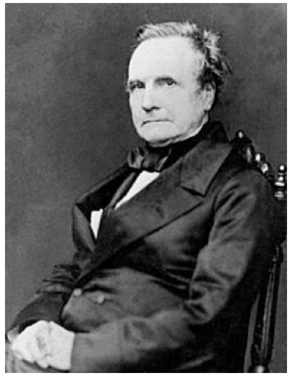
Additional Hints (Encrypt)

onder water / aan ketting

```
Decryption Key
A|B|C|D|E|F|G|H|I|J|K|L|M
-------------------------
N|O|P|Q|R|S|T|U|V|W|X|Y|Z
(letter above equals below, and vice versa)
```

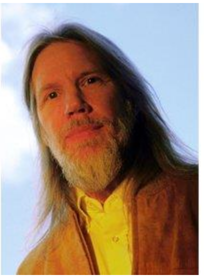
Ancient Cryptography

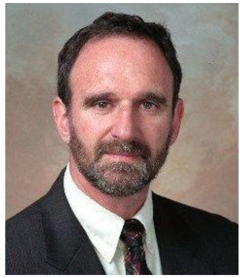
Charles Babbage



Claude Shannon

Diffie / Hellman

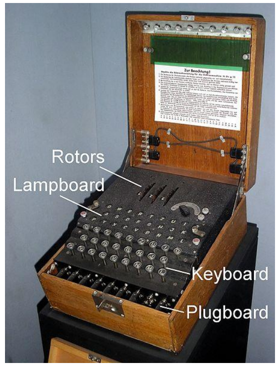




1800 1850 1900 1950 1976 2015

“a cryptographic system should be secure even if everything but the key is known to the adversary”

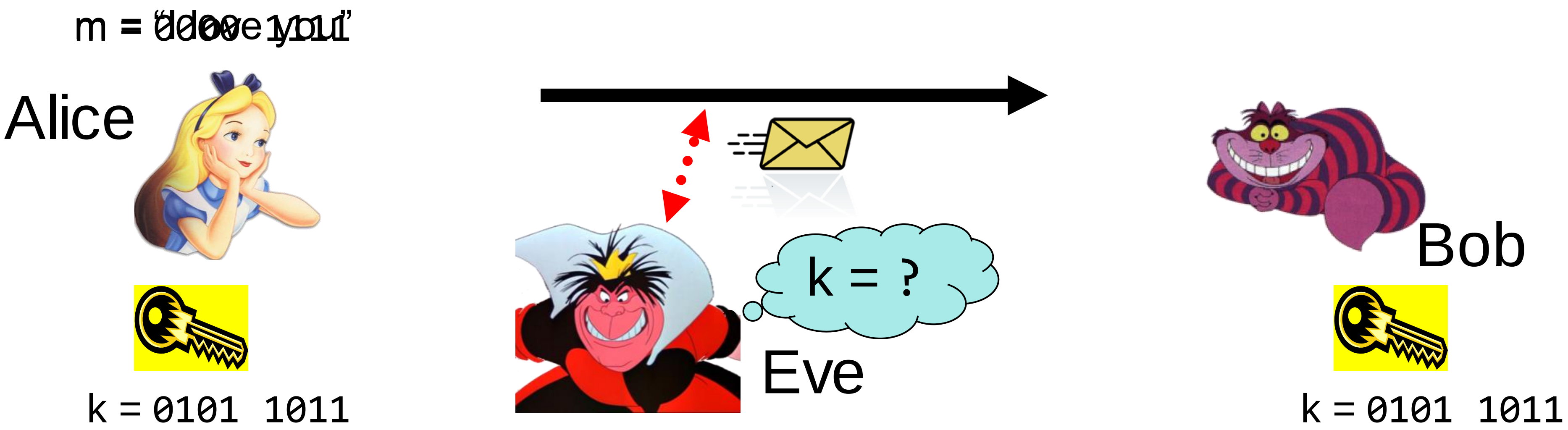
Auguste Kerckhoffs



Enigma

Alan Turing
(The Imitation Game)

Secure Encryption



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

eXclusive OR (XOR) Function (exclusive disjunction)

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

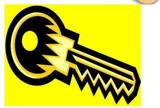
- Some properties:
  - $\forall x : x \oplus 0 = x$
  - $\forall x : x \oplus x = 0$

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

One-Time Pad Encryption

$m = 0000\ 1111$

Alice



$k = 0101\ 1011$

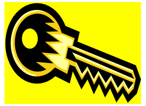
$c = m \oplus k = 0101\ 0100$

k = ?

Eve

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

Bob



$k = 0101\ 1011$

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

$m = 0000\ 1111$

$k = 0101\ 1011$

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

$c = 0101\ 0100$

$k = 0101\ 1011$

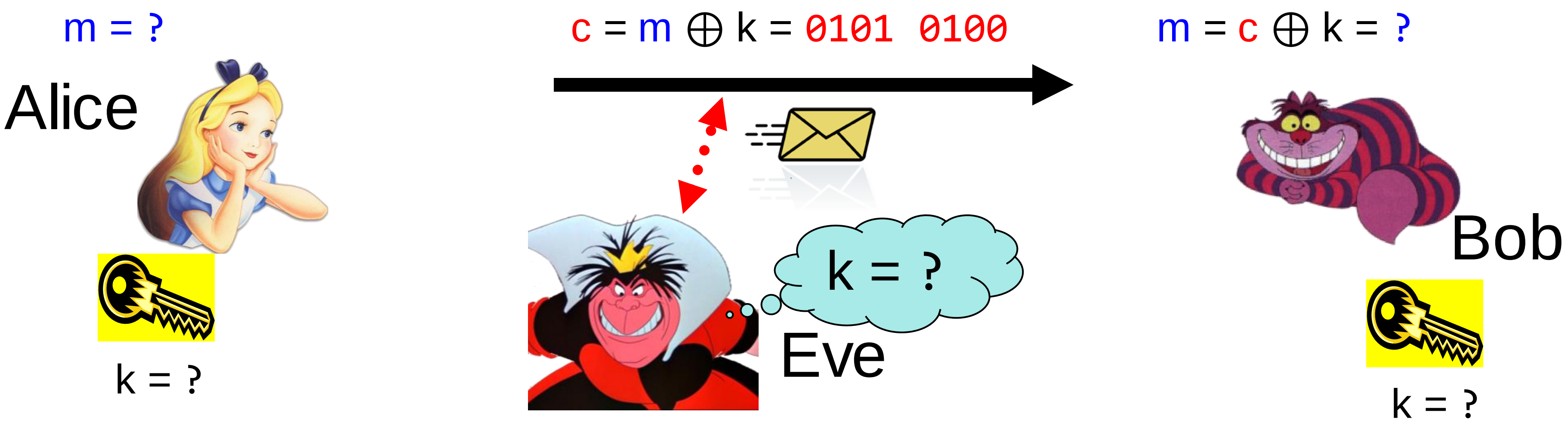
$c \oplus k = 0000\ 1111$

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

- Is it secure?

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

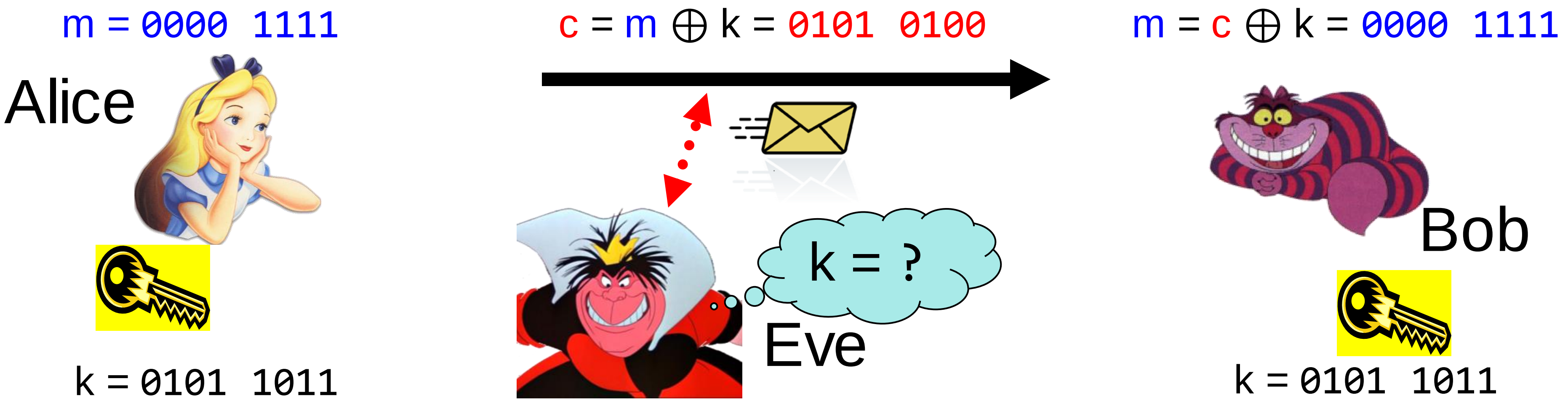
Perfect Security



- 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

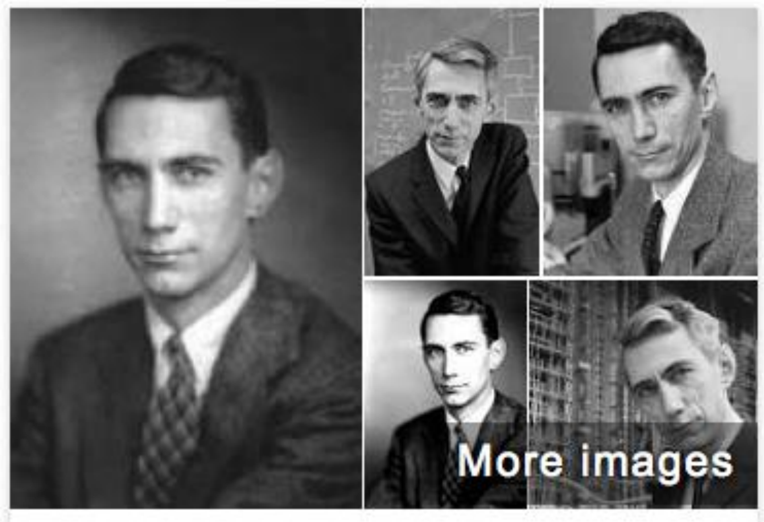
Problems With One-Time Pad



- The key has to be as long as the message.
- The key can only be used once.

Information Theory

- 6 EC MoL course, given in 2nd block: Nov/Dec 2018
- mandatory for Logic & Computation track
- first lecture: Tuesday, 30 October 2017, 9:00
- http://homepages.cwi.nl/~schaffne/courses/inftheory/2018/



Claude Shannon

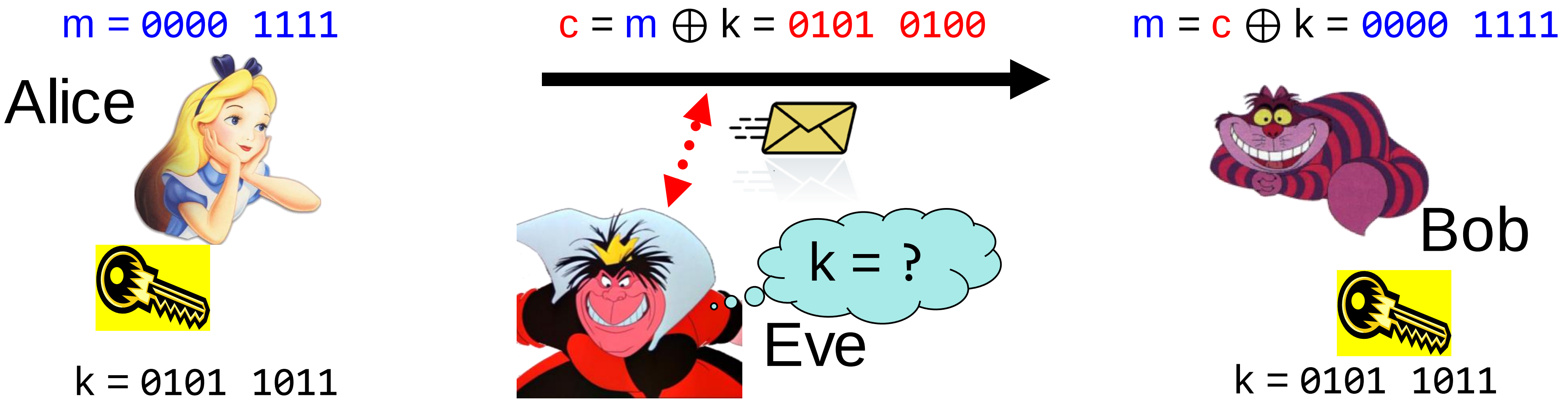
Mathematician

Claude Elwood Shannon was an American mathematician, electronic engineer, and cryptographer known as "the father of information theory". Shannon is famous for having founded information theory with a landmark paper that he published in 1948. Wikipedia

Born: April 30, 1916, Petoskey, Michigan, United States

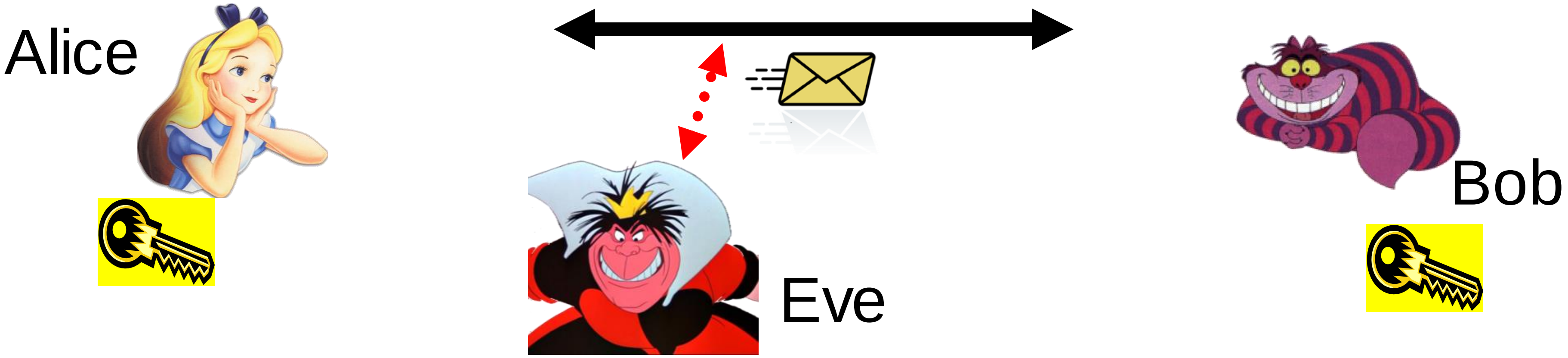
Died: February 24, 2001, Medford, Massachusetts, United States

Problems With One-Time Pad



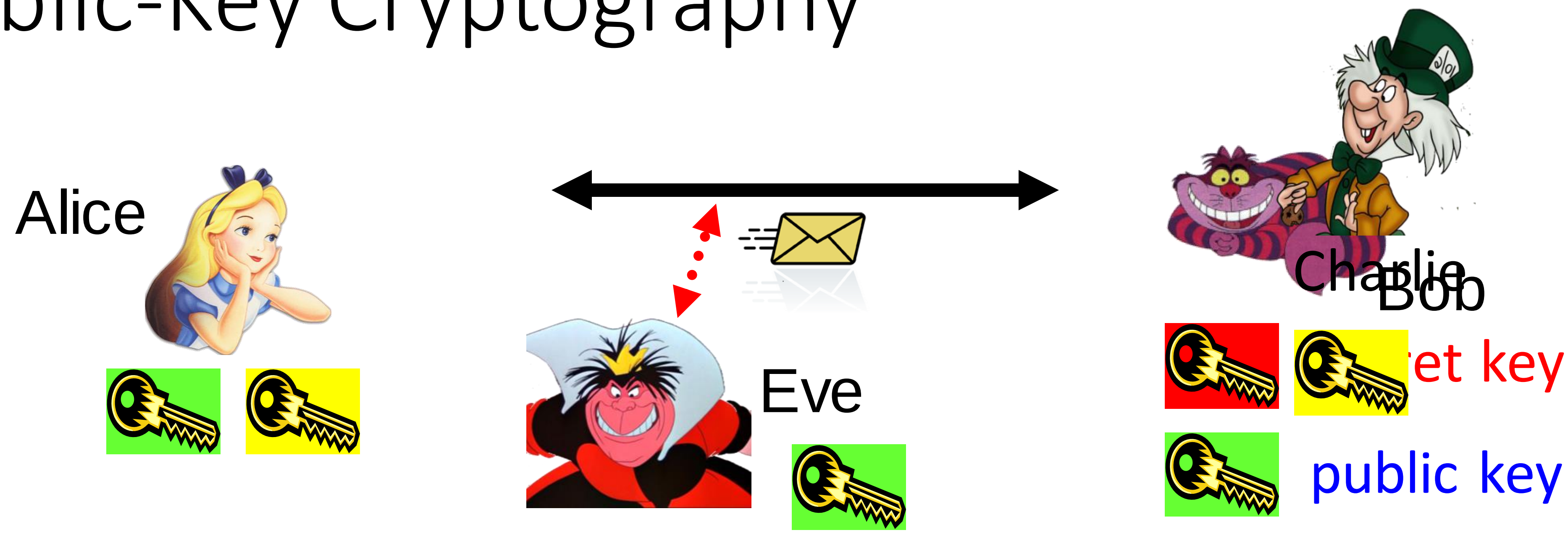
- The key has to be as long as the message.
- The key can only be used once.
- In practice, other encryption schemes (such as AES) are used which allow to encrypt long messages with short keys.
- One-time pad does not provide authentication:
  Eve can easily flip bits in the message

Symmetric-Key Cryptography



- Encryption insures secrecy:
  Eve does not learn the message, e.g. one-time pad
- Authentication insures 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.

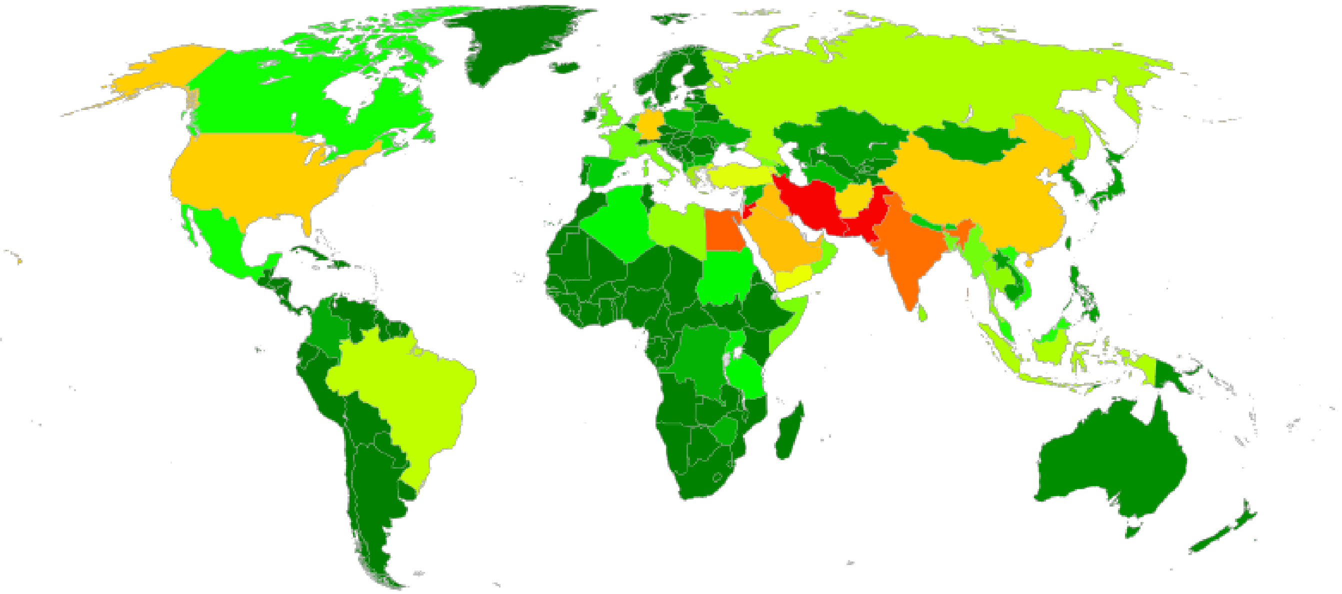
History of Public-Key Crypto

- Early 1970s: invented in the „classified world“ at the British Government Communications Head Quarters (GCHQ) by Ellis, Cocks, Williamson

- Mid/late 1970s: invented in the „academic world“ by Merkle, Hellman, Diffie, and Rivest, Shamir, Adleman (RSA)

Politics of Cyberwar

- Edward Snowden, former CIA and NSA employee, now whistleblower and on (temporary) asylum in Russia
- In 2013, he leaked many thousand top secret documents to various media, documenting
- mass surveillance programs by secret services from all over the world



Politics of Cyberwar

Politics of Cyberwar

- Methods:
  - Break cryptography
  - Influence industrial standards
  - Pressure manufacturers to make insecure devices
  - Infiltrate hardware and software (communication infrastructure, computers, smartphones etc.)

- Why mass surveillance?
  - Other than to combat terrorism, these surveillance programs have been employed to assess the foreign policy and economic stability of other countries, and to gather "commercial secrets“.

Why worry?

- „I have nothing to hide“ is a very naive reaction.
- Think about what your smartphone knows about you.
- Think about what your smartphone does not know about you.

TECHNOLOGY

- 2014: Facebook to Pay $19 Billion for WhatsApp

  price of $42 per user for WhatsApp.

- 2016: MICROSOFT BUYS LINKEDIN FOR $26.2 BILLION

Why worry?

- „I have nothing to hide“ is a very naive reaction.
- Everyone‘s personal privacy is at stake!
- George Orwell‘s surveillance state from his book 1984 is coming true...

- "*They (the NSA) can use the system to go back in time and scrutinize every decision you've ever made, every friend you've ever discussed something with, and attack you on that basis to sort of derive suspicion from an innocent life and paint anyone in the context of a wrongdoer.*" – Edward Snowden

Dutch Example: Dragnet Law

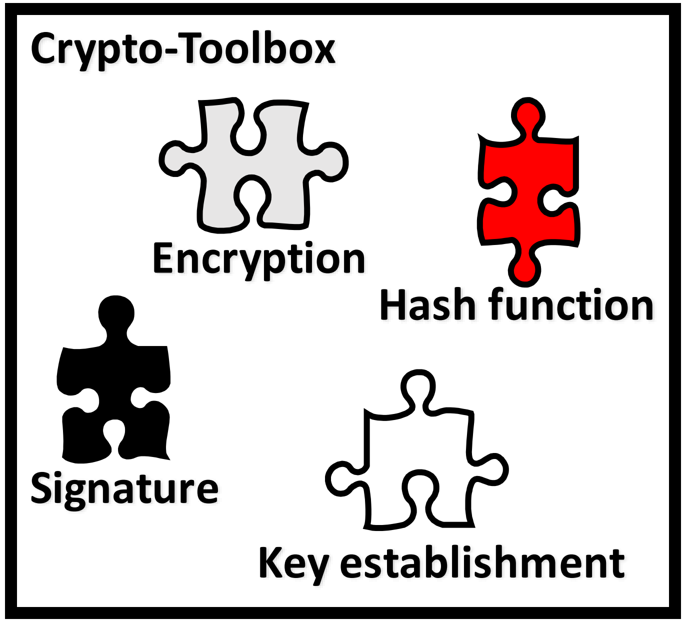
- Law for the intelligence and security services (Wet inlichten en veiligheidsdiensten, Wiv)
- Accepted by parliament in 2017
- Referendum initiated by (former) ILLC students
- 21 March 2018: (6.7 mio votes, participation 51%) 46.5% pro, 49.4% against, 4% empty
- Cosmetic adjustments were done by parliament
- Law is now in effect, allowing Dutch secret services to tap communication infrastructures of “bystanders”, store it for 3 years, share data with foreign services etc.
- https://www.bitsoffreedom.nl/dossiers/sleepnet/
  https://geensleep.net/

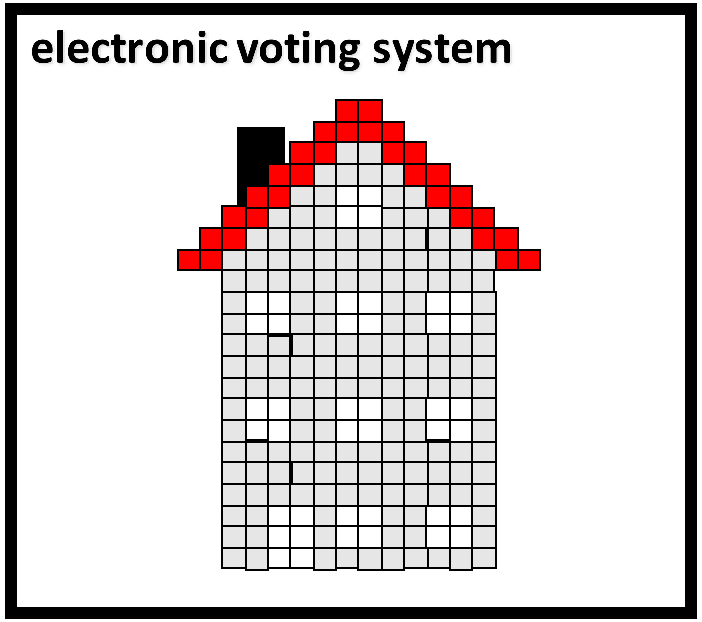
Sleepwet Referendum

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

GCHQ

Cryptography and Logic





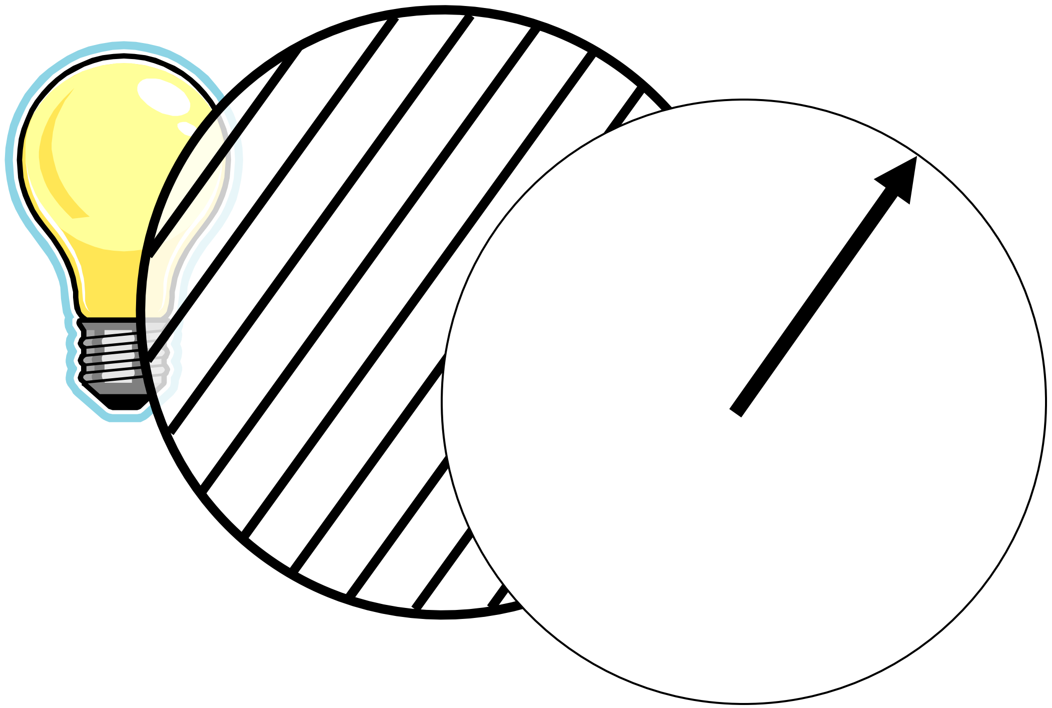
- Cryptographic protocols for advanced tasks are built from basic building blocks
- Problem: security proofs become very hard to verify
- Solution:
  - Logic provides formal methods to specify tools and task
  - Use automatic proof checkers to verify security

What will you Learn from this Talk?

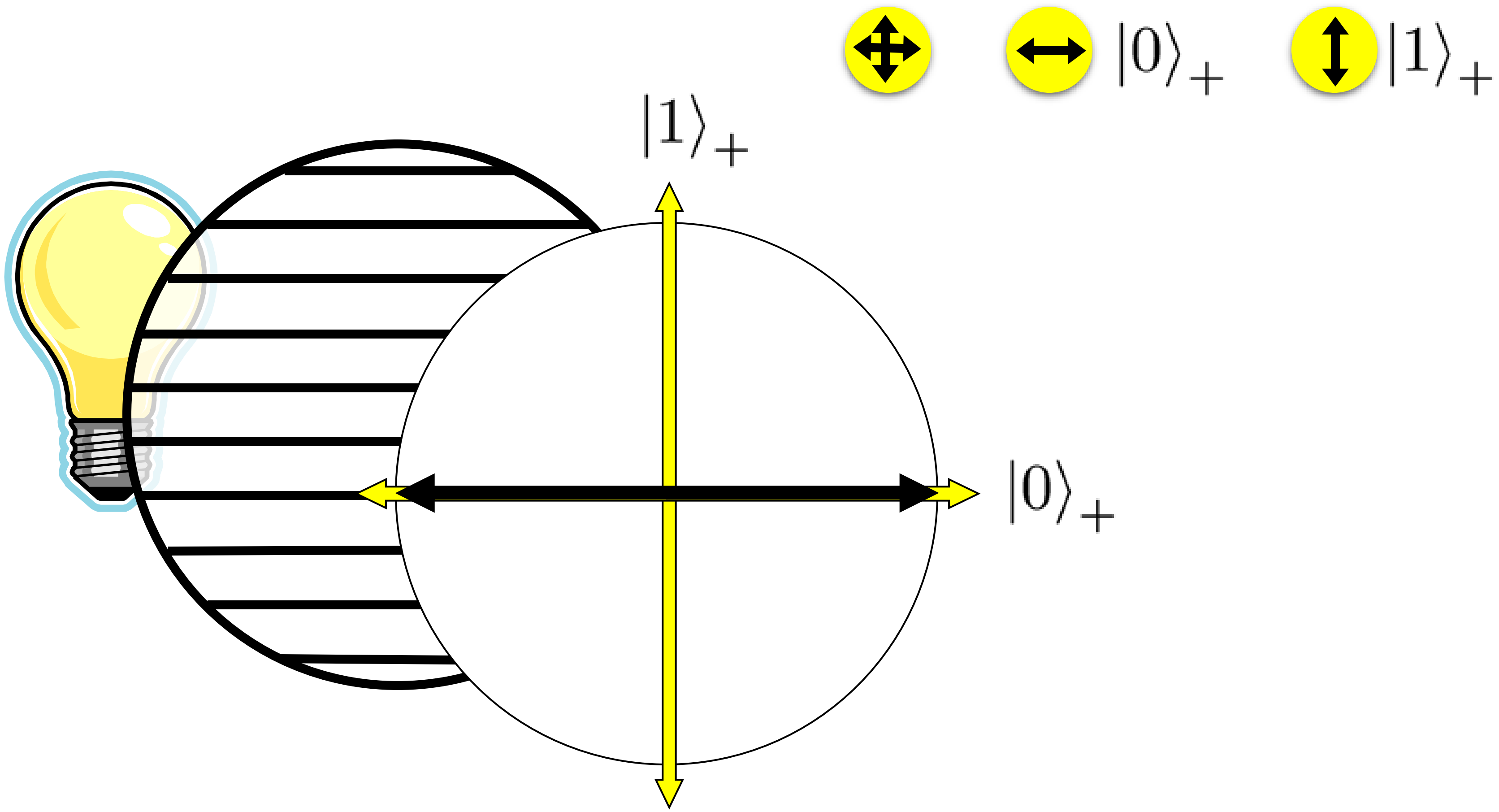
- ✓ Classical Cryptography (& Politics)
- Introduction to Quantum Mechanics
- Crypto Threat of Quantum Computing
- Quantum Cryptography
- Quantum Future

Quantum Bit: Polarization of a Photon

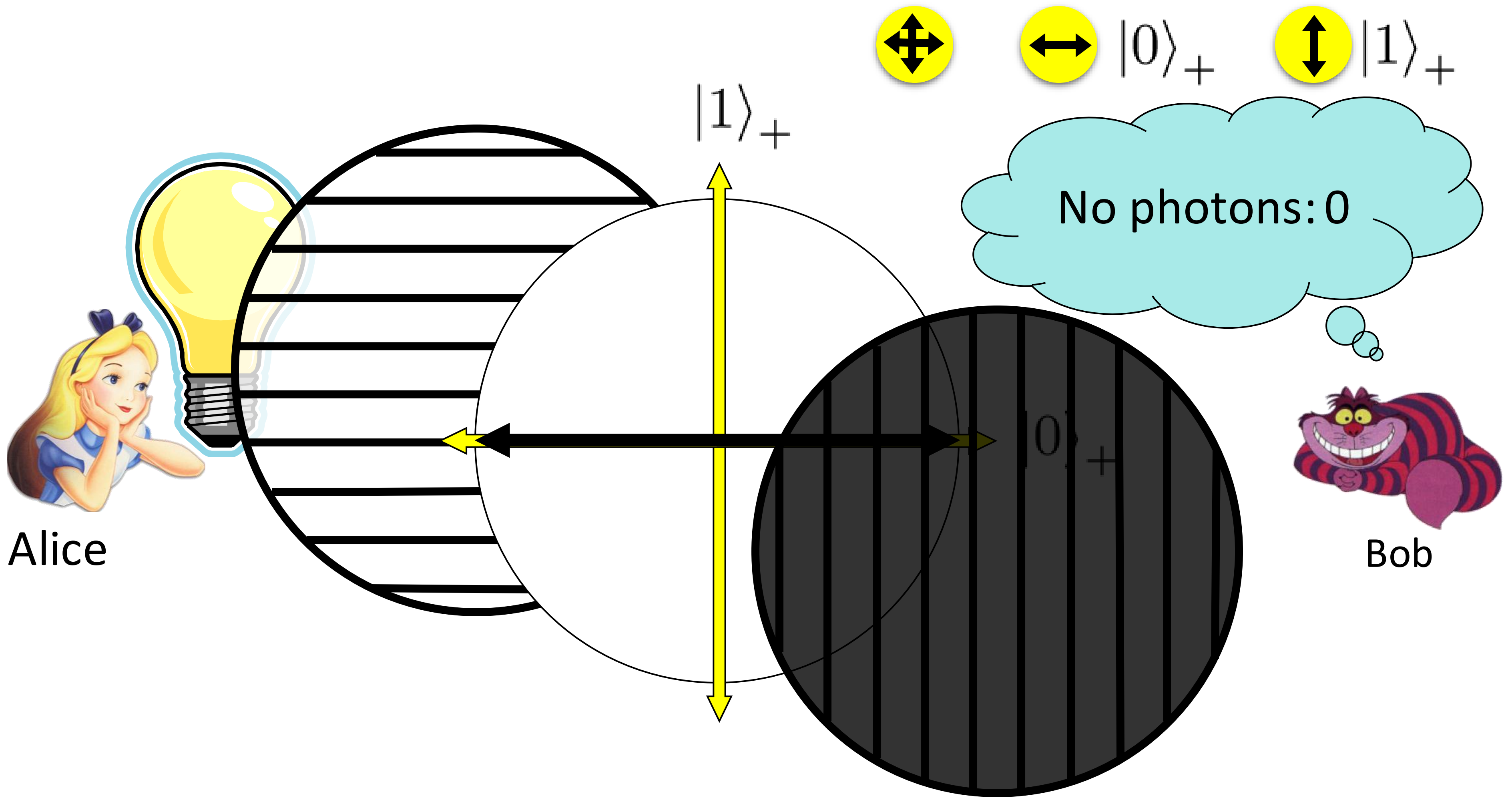
qubit as unit vector in $\mathbb{C}^2$



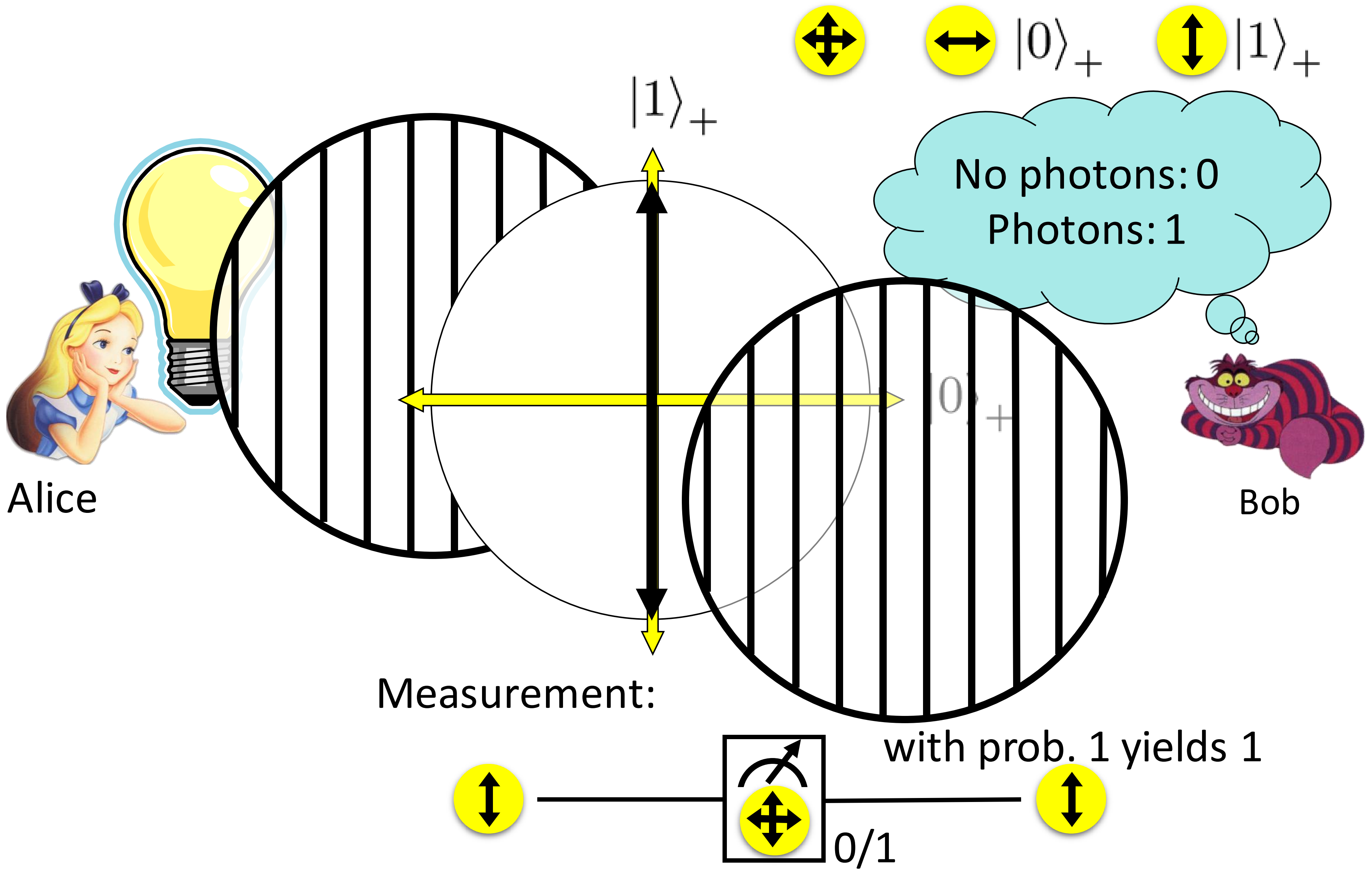
Qubit: Rectilinear/Computational Basis



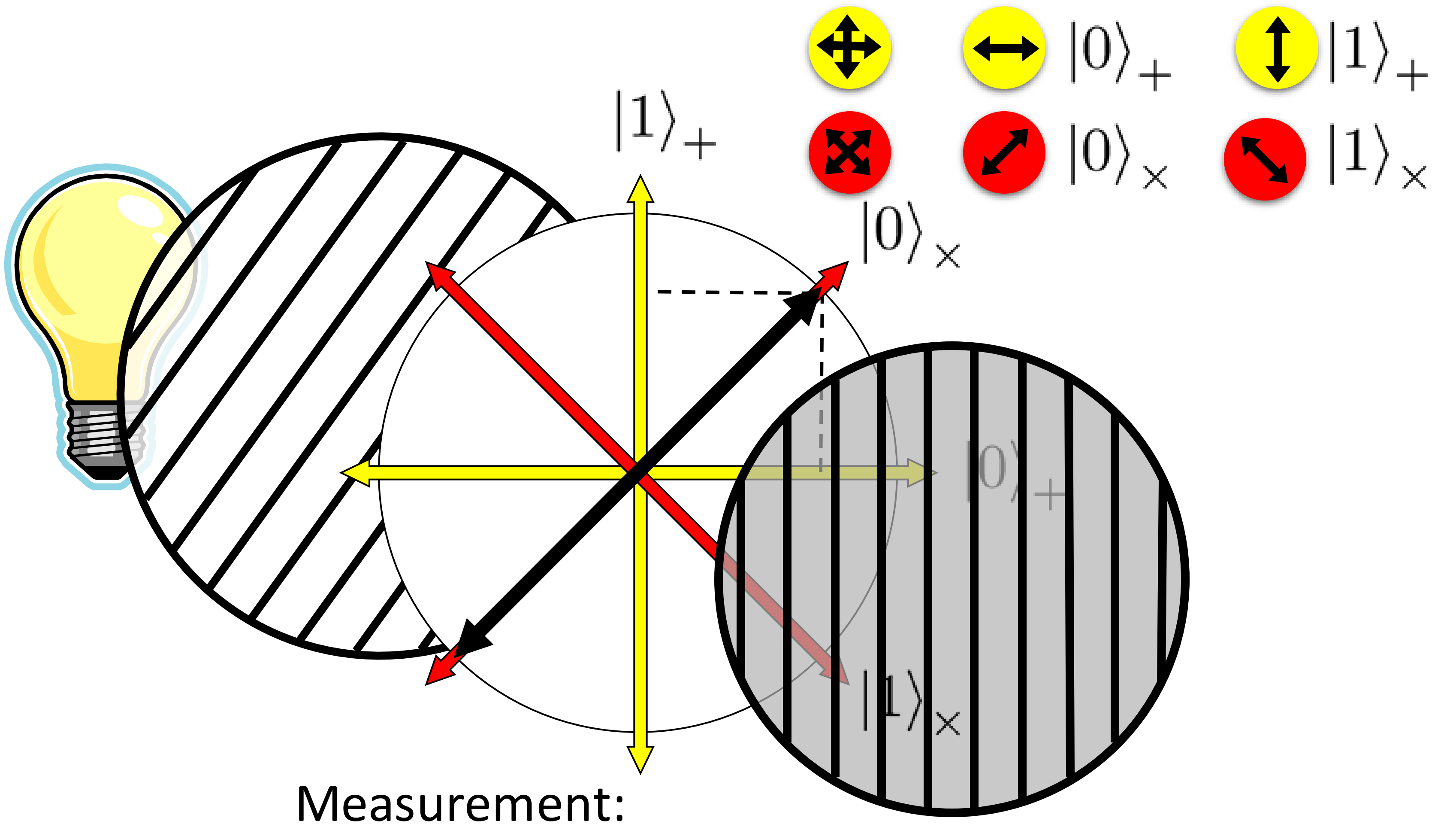
Detecting a Qubit



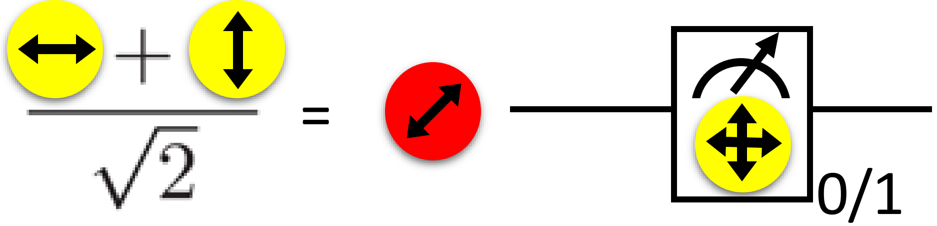
Measuring a Qubit



Diagonal/Hadamard Basis



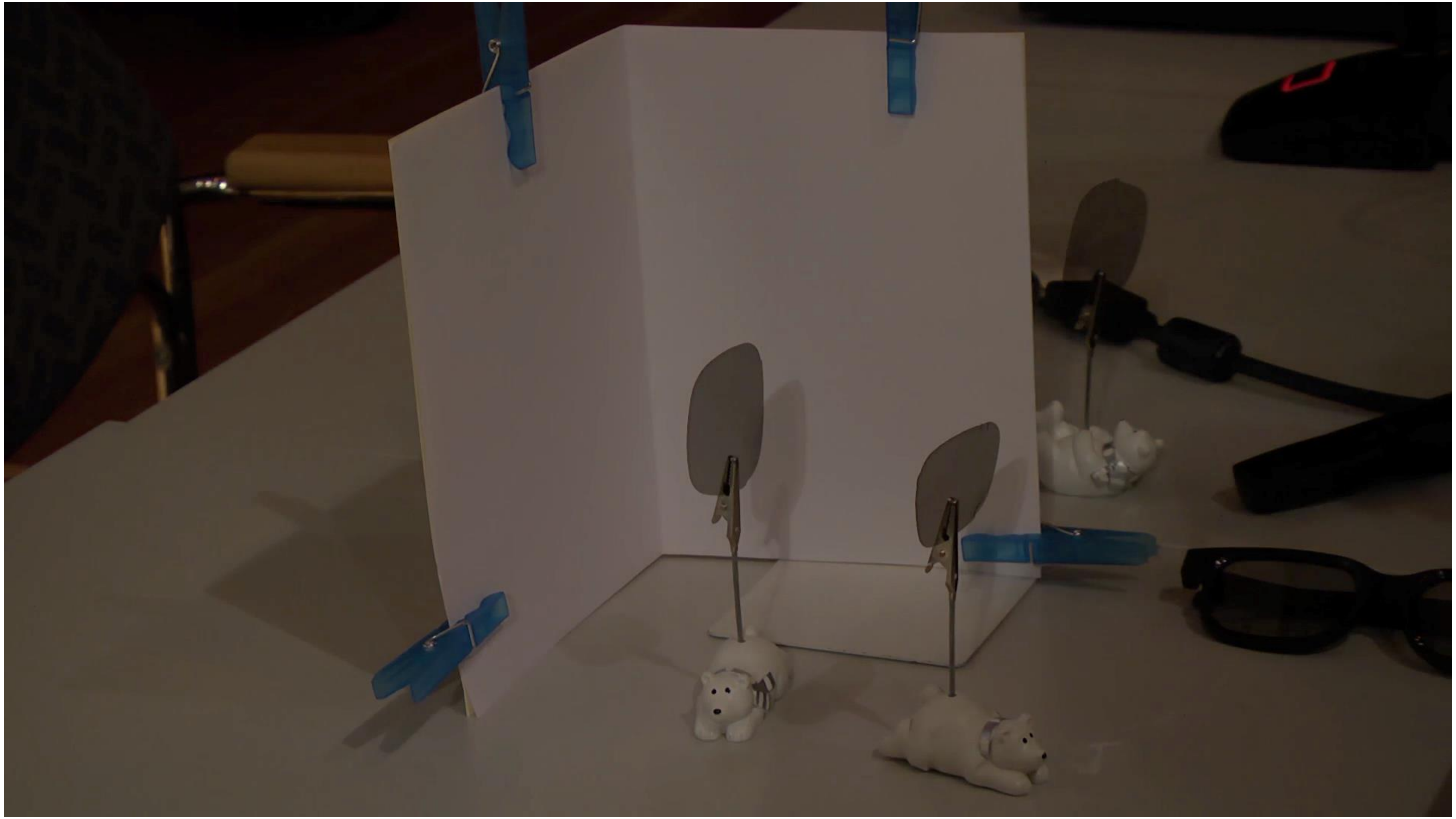
Measurement:



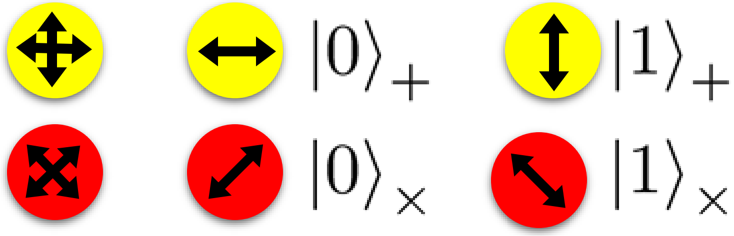
with prob. ½ yields 0

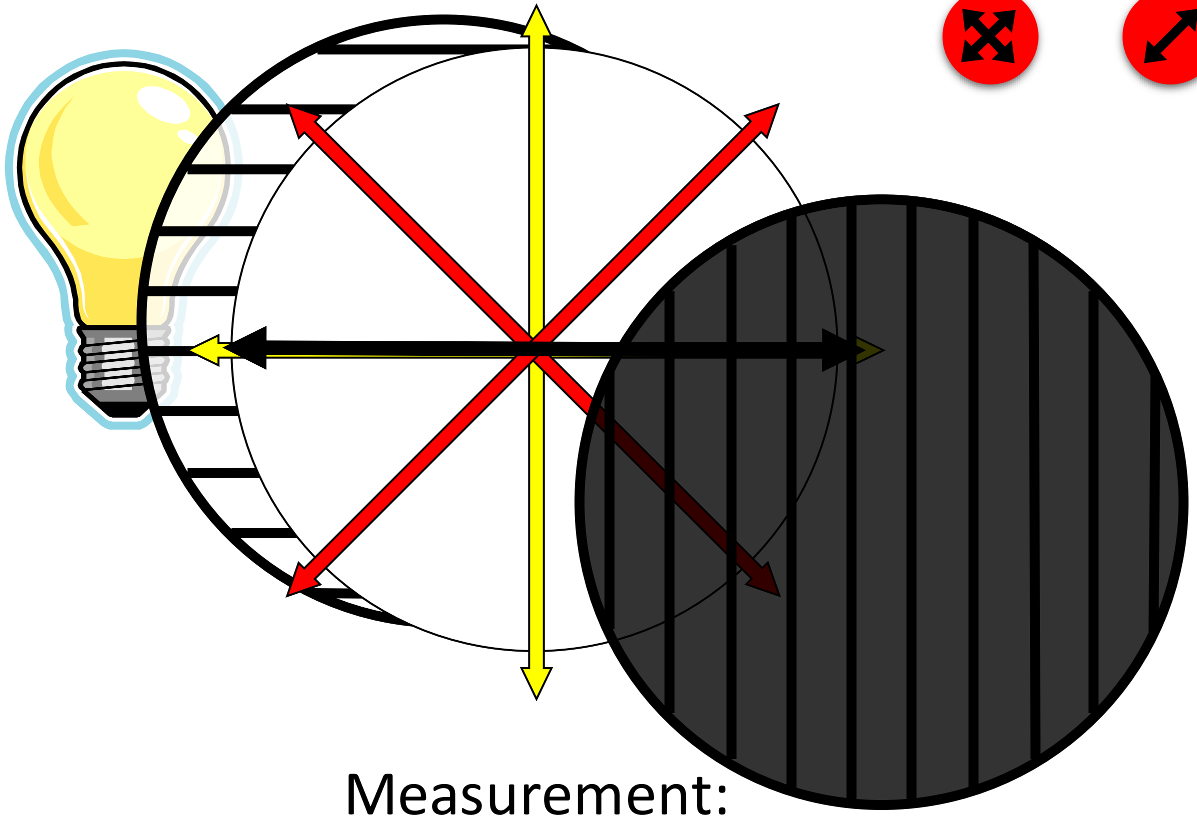
with prob. ½ yields 1

Video

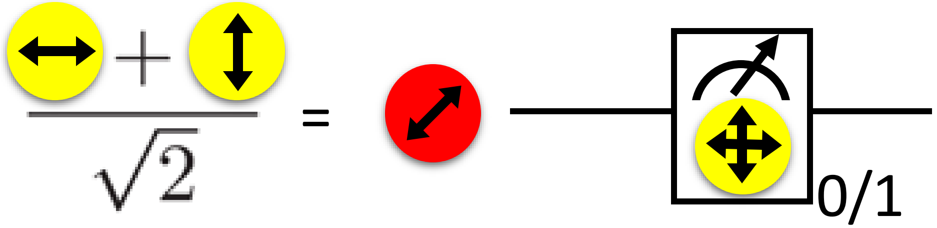


Measuring Collapses the State



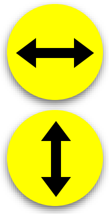


Measurement:

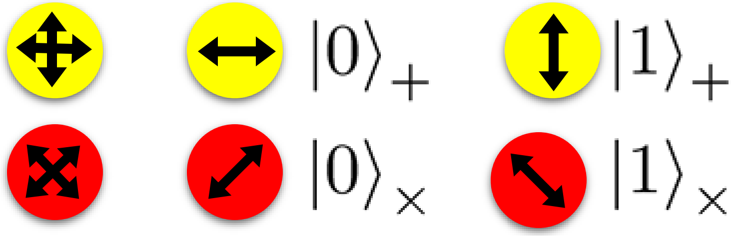


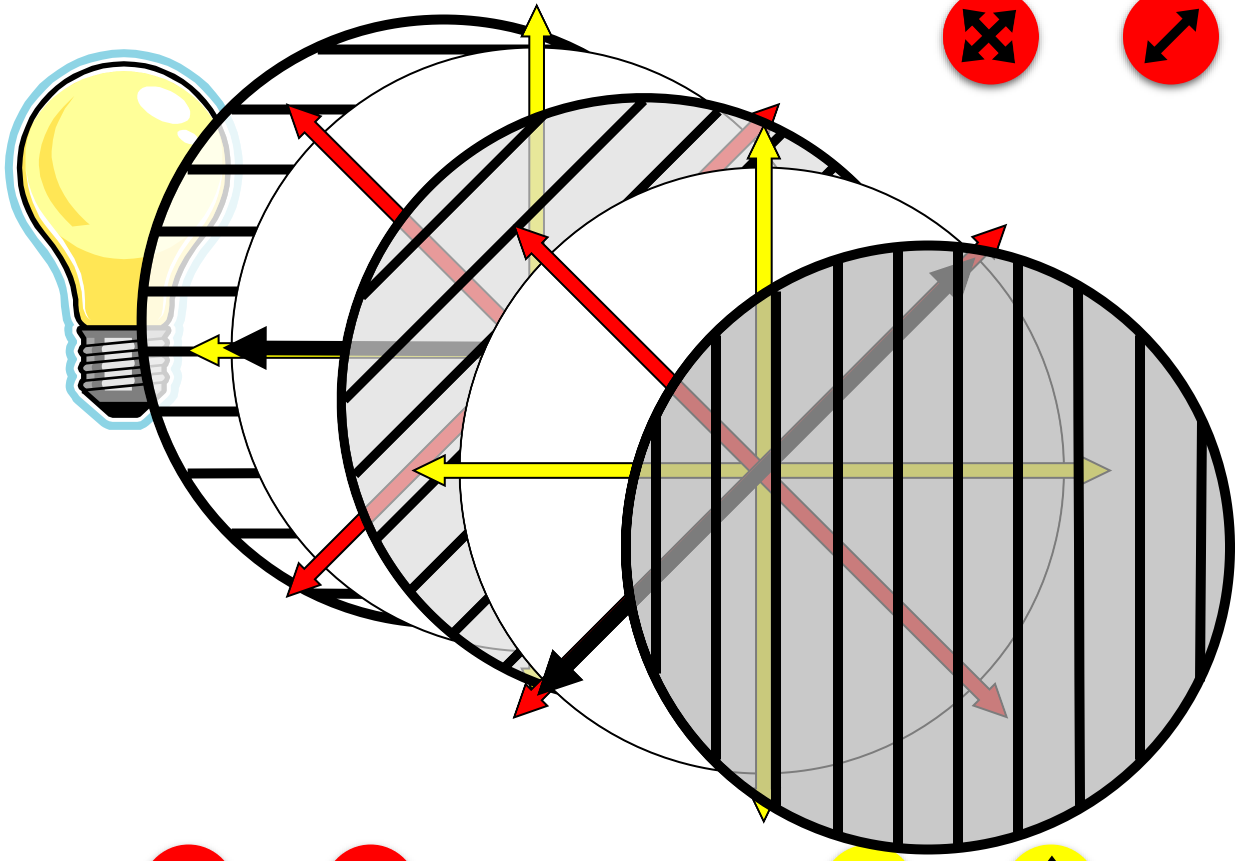
with prob. ½ yields 0

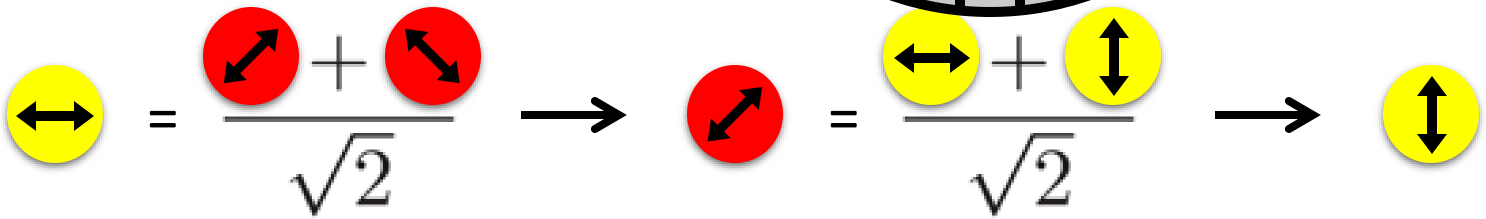
with prob. ½ yields 1



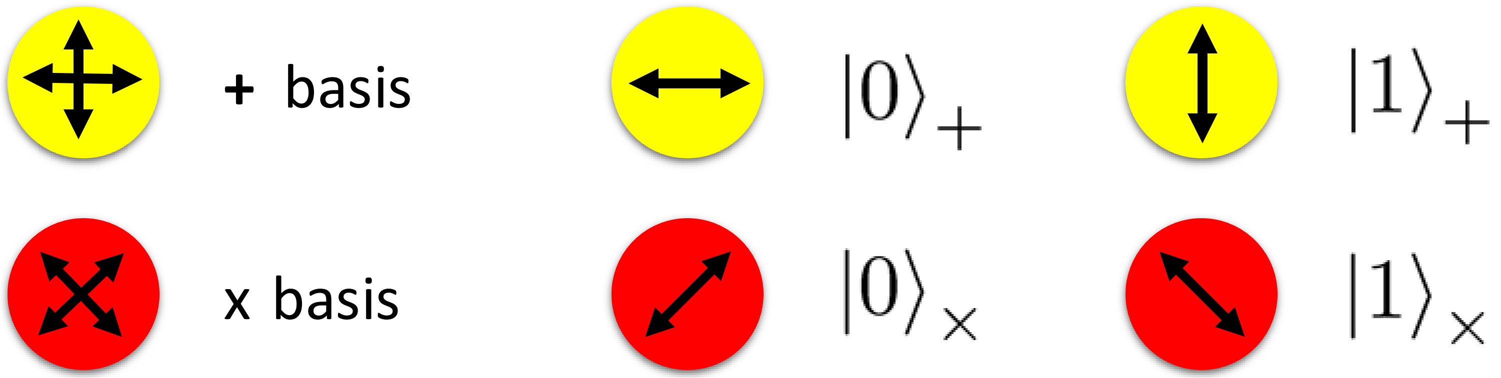
Measuring Collapses the State



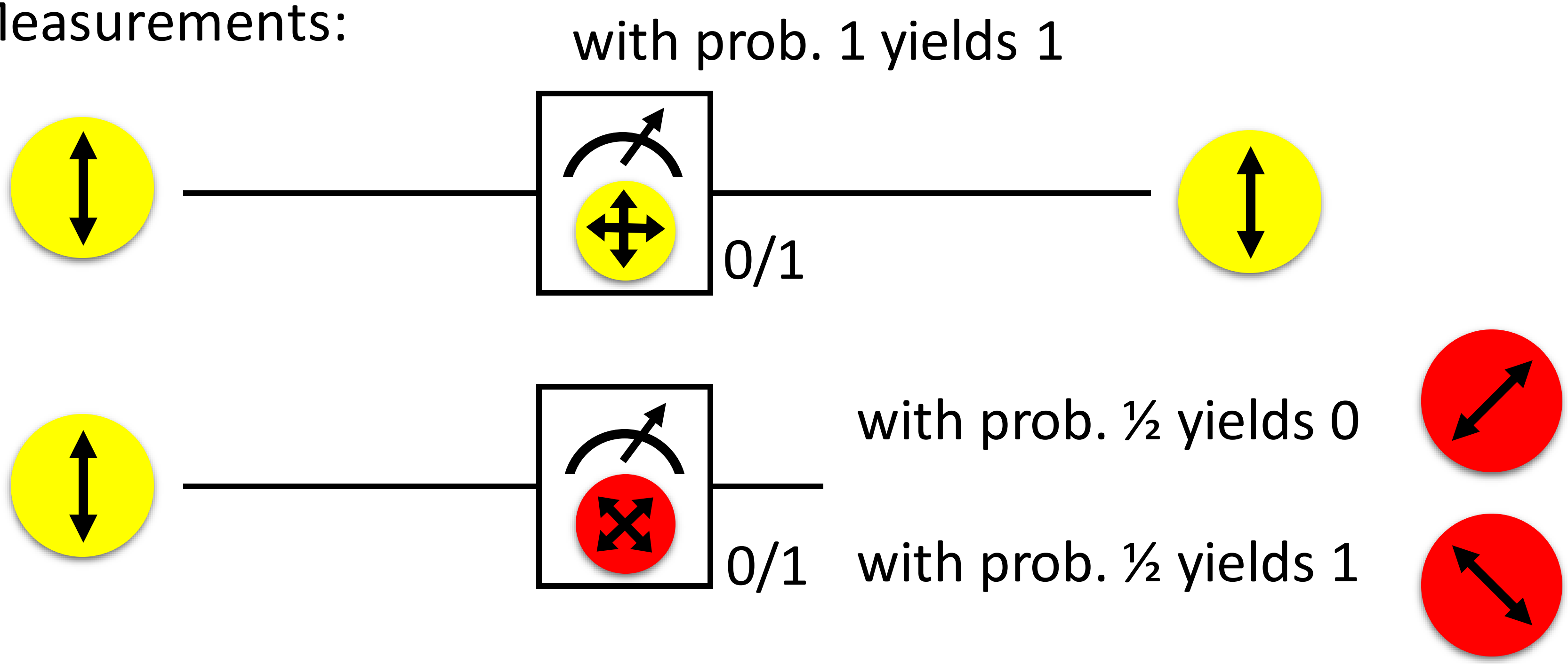




Quantum Mechanics

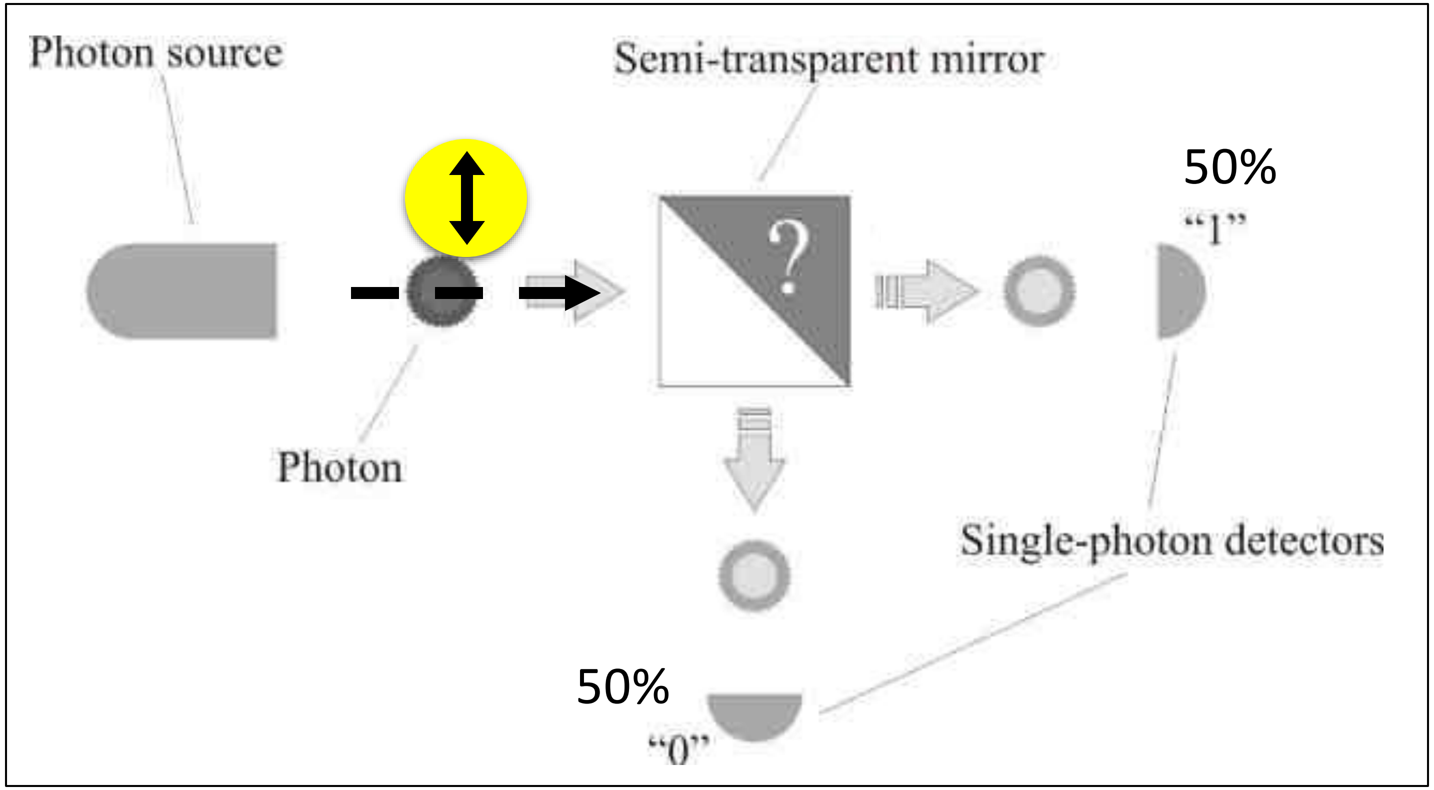


Measurements:



Demonstration of Quantum Technology

- generation of random numbers



(diagram from idQuantique white paper)

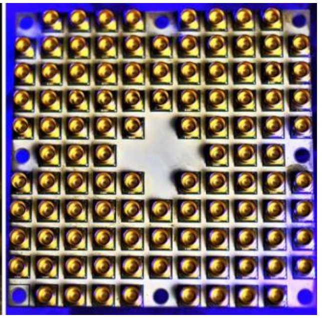
- no quantum computation, only quantum communication required

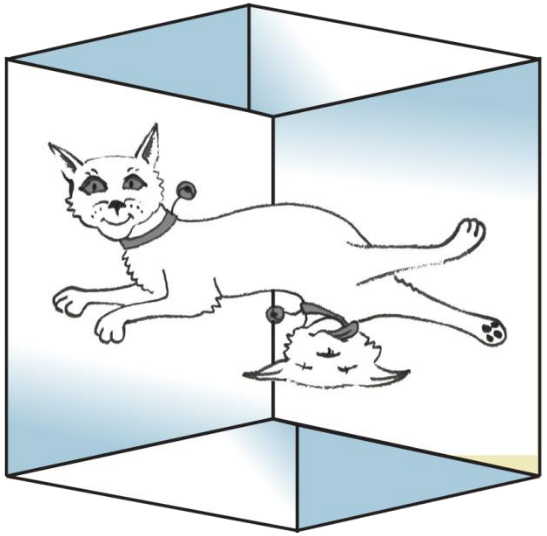
Quantum (Optics) Games

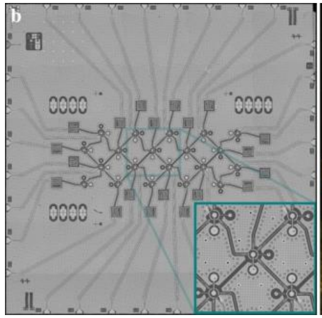
- Single-player puzzle game: Laser Maze, beam bending logic game

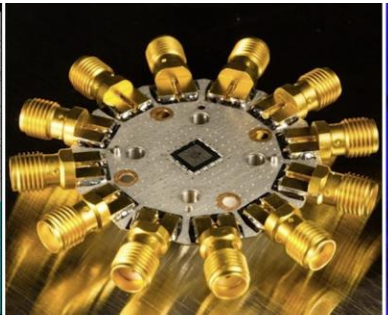
- Virtual game: http://quantumgame.io/

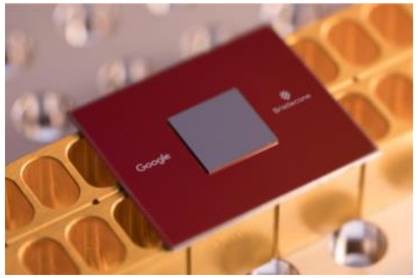
0

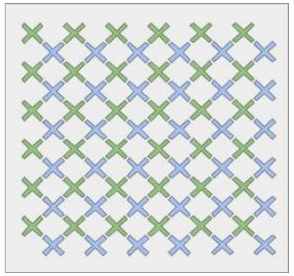




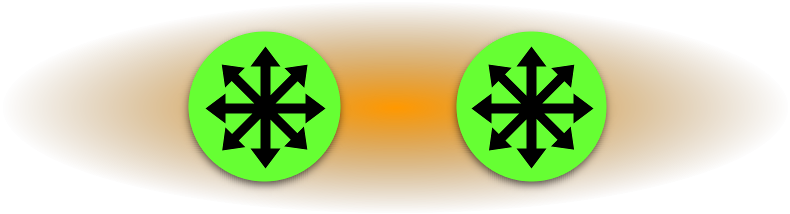


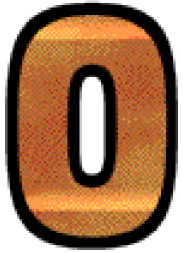






Wonderland of Quantum Mechanics

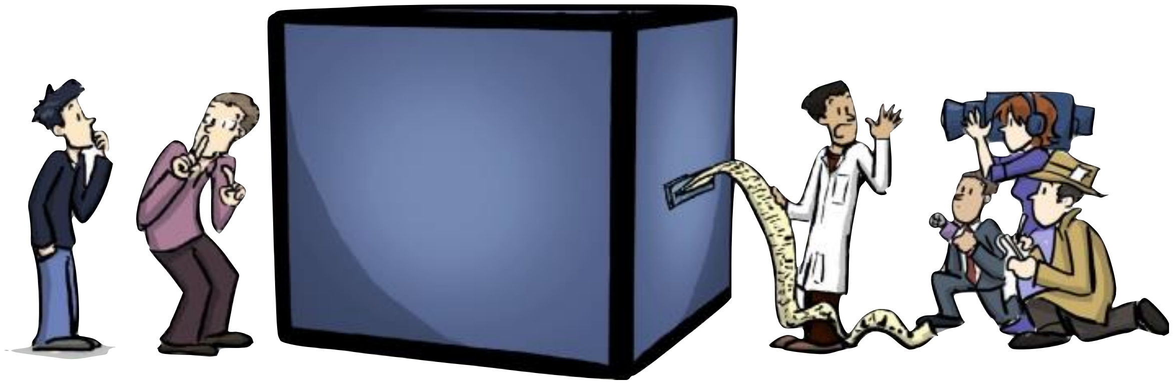


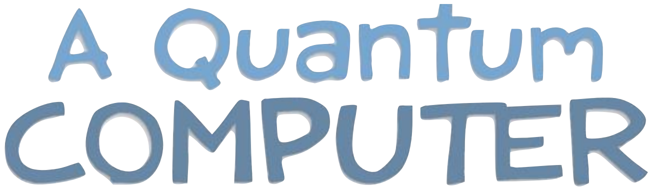


What will you Learn from this Talk?

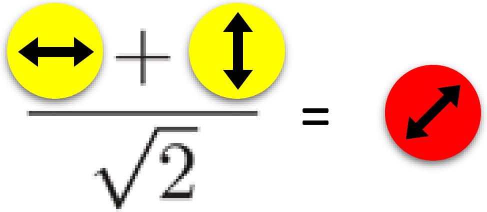
- ✓ Classical Cryptography (& Politics)
- ✓ Introduction to Quantum Mechanics
- Crypto Threat of Quantum Computing
- Quantum Cryptography
- Quantum Future

Quantum Computing





- Classical bit: 0 or 1
- Quantum bit: can be in superposition of 0 and 1

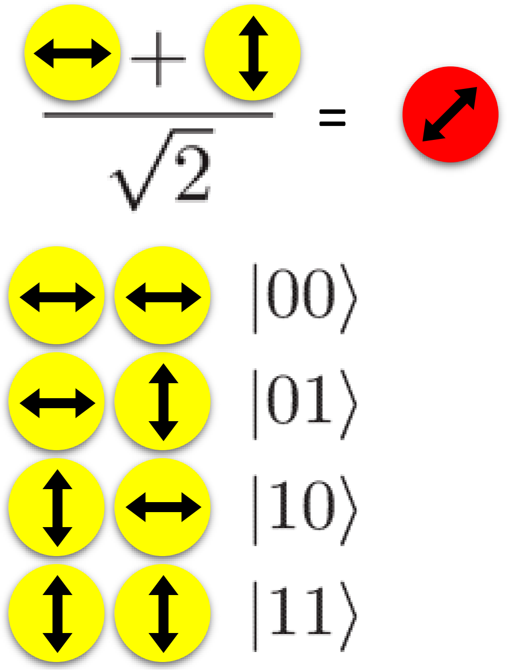


- Yields a (probably) more powerful computational model

Many Qubits

- 1 qubit lives in a 2-dimensional space, can be in a superposition of 2 states
- 2 qubits live in a 4-dimensional space, can be in a superposition of 4 states

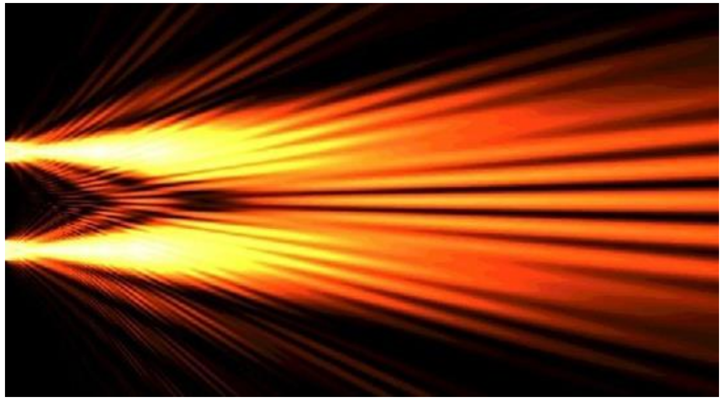
$$\frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

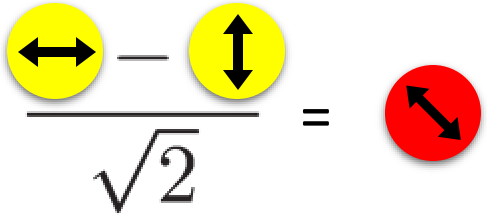


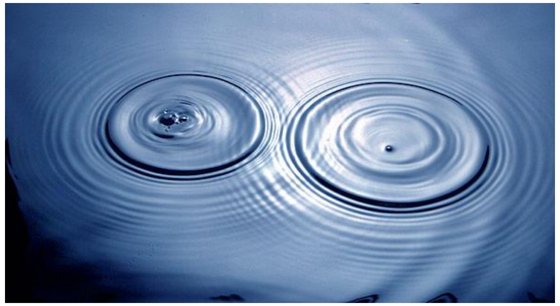
- 3 qubits can be in superposition of 8 states
- n qubits can be in superposition of 2^n states
- So, with 63 qubits, one can do 2^{63} = 9223372036854775808 calculations simultaneously!
- Problem: Measuring this huge superposition collapses everything and yields only one random outcome

Quantum Computing

- With n qubits, one can do 2^n calculations simultaneously
- Problem: Measuring this huge superposition will collapse the state and only give one random outcome
- Solution: Use quantum interference to measure the computation you are interested in!



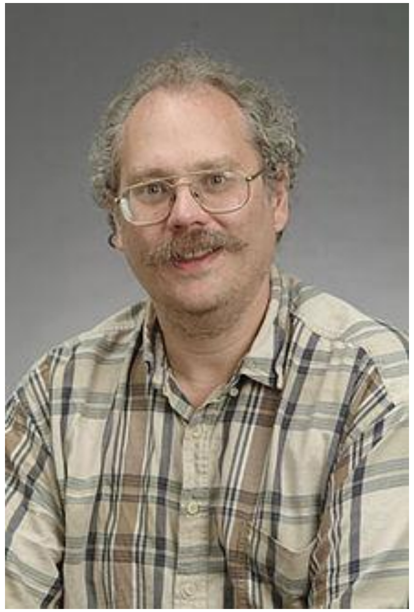




- Seems to work for specific problems only
- Requires clever design of quantum algorithms and quantum software!

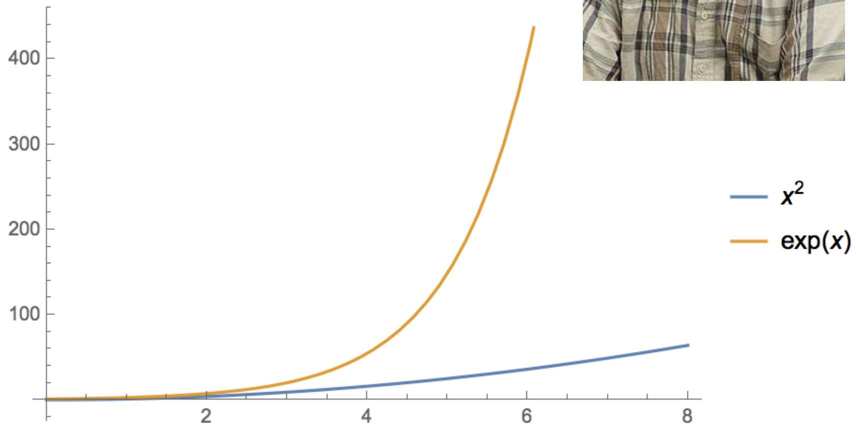
Quantum Algorithms: Factoring

- [Shor ’94] Polynomial-time quantum algorithm for factoring integer numbers
- 15 = 3 * 5
- 27 =
- 31 =
- 57 =
- 91 =
- 173 =
- RSA-100 = 1522605027922533360535618378132637429718068114961380688657908494580122963258952897654000350692006139 =



Quantum Computer breaks Public-Key Crypto

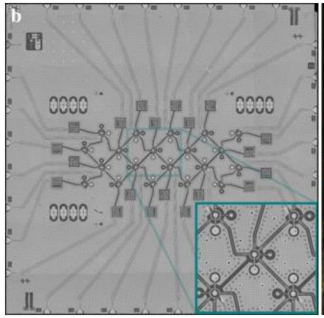
- [Shor '94] Polynomial-time quantum algorithm for factoring integer numbers
- Classical Computer : Exponential time
- Quantum Computer : Poly-time: n^2
- For a 600-digit number (RSA-2048)
  - Classical: age of universe
  - Quantum: few minutes

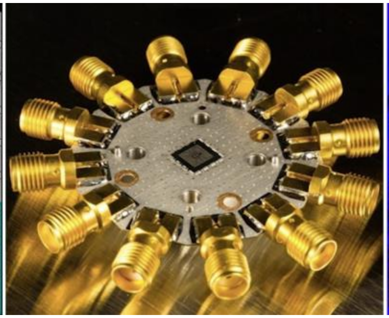


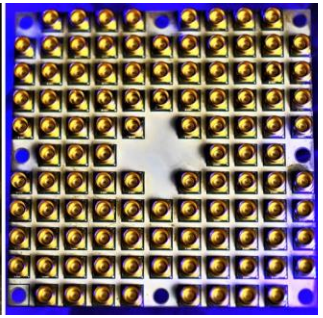
- Consequence: Large enough quantum computers break all currently used public-key cryptosystems!!!

Can We Build Quantum Computers?

- Possible to build in theory, no fundamental theoretical obstacles have been found yet.
- Enormous technical challenge (control vs decoherence)



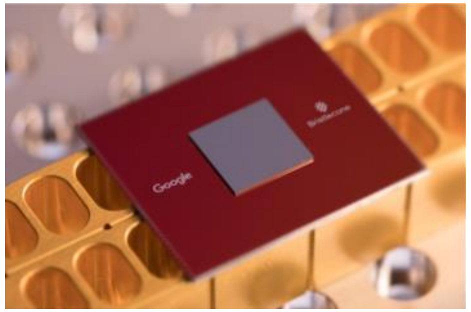


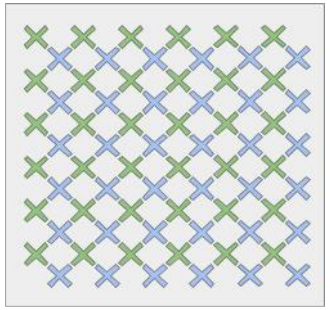


rigetti

Google Research

intel





- 5 March 2018:

Google moves toward quantum supremacy with 72-qubit computer

IBM and Intel recently debuted similarly sized chips

Conventional Quantum-Safe Cryptography

- **Wanted**: new assumptions to replace factoring and discrete logarithms in order to build conventional public-key cryptography

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

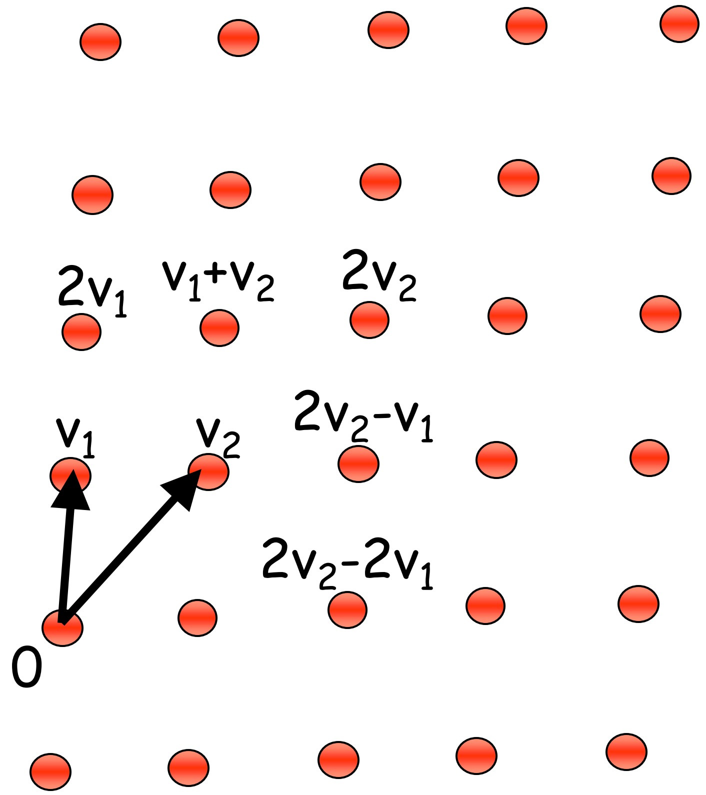
- NIST “competition”: 82 submissions (23 signature, 59 encryption schemes)
- Several submissions have already been broken and withdrawn
- April 2018: First-round workshop in Florida
- Expected: 3-5 years of crypto-analysis
- New standards, world-wide adoption

QuSoft CWI

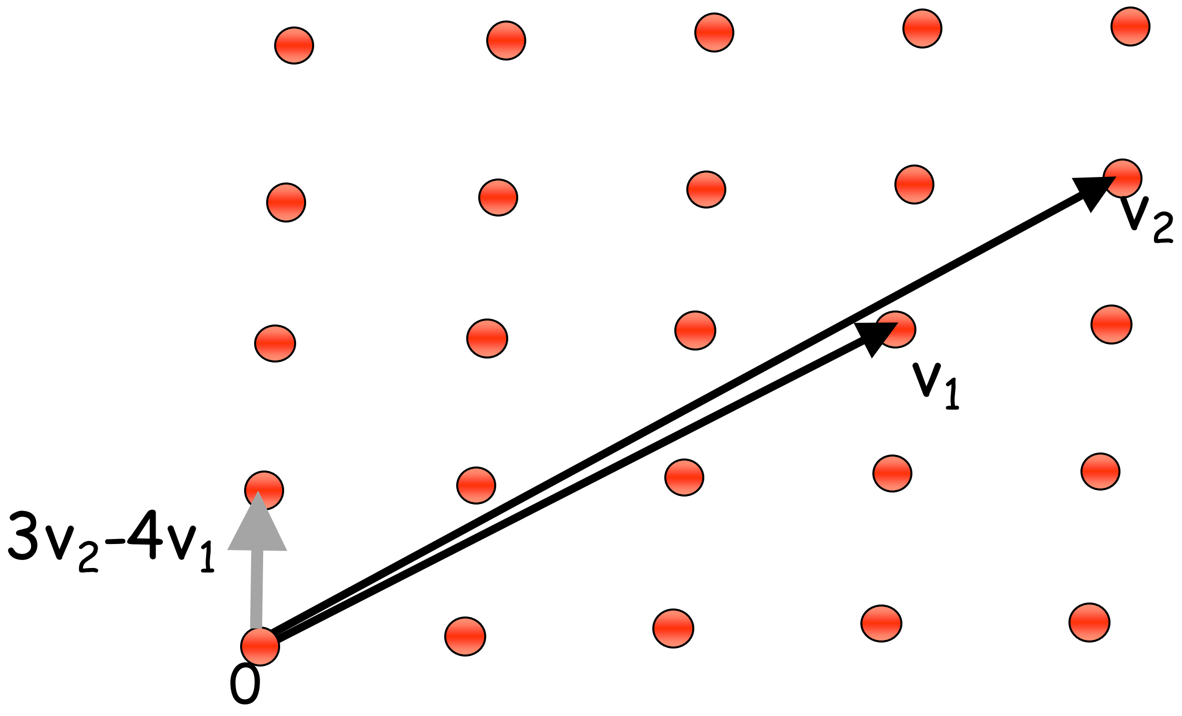
Example: Lattice-Based Cryptography

- For any vectors $v_1, \dots, v_n$ in $\mathbb{R}^n$, the lattice spanned by $v_1, \dots, v_n$ is the set of points $L = \{a_1 v_1 + \cdots + a_n v_n | \; a_i \text{ integers}\}$

- Shortest Vector Problem (SVP): given a lattice L, find a shortest (nonzero) vector



Example: Lattice-Based Cryptography

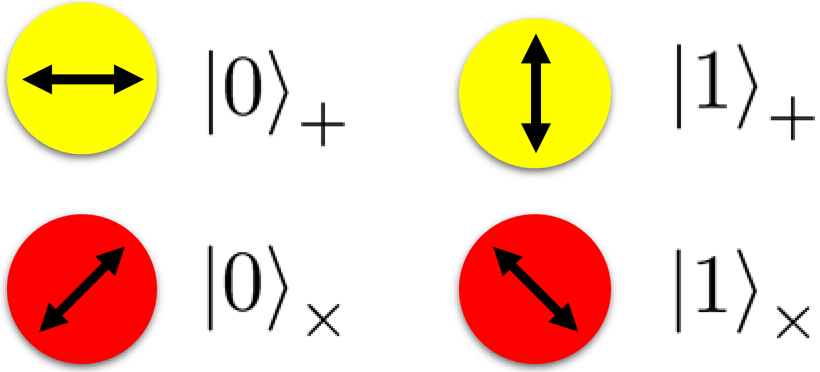


- Shortest Vector Problem (SVP): given a lattice, find a shortest (nonzero) vector
- no efficient (classical or quantum) algorithms known
- public-key encryption schemes can be built on the computational hardness of SVP

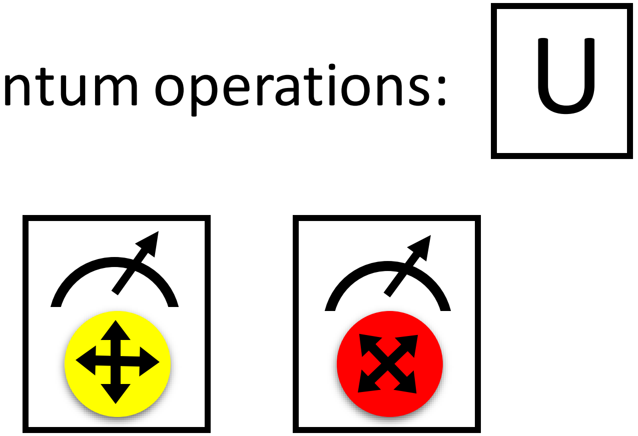
What will you Learn from this Talk?

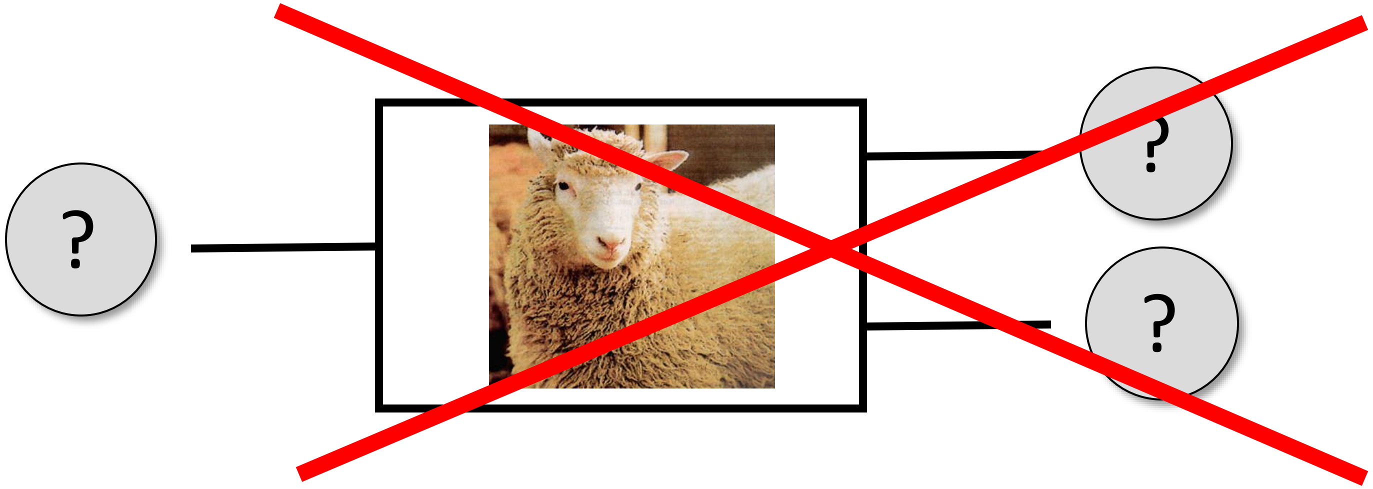
- ✓ Classical Cryptography (& Politics)
- ✓ Introduction to Quantum Mechanics
- ✓ Crypto Threat of Quantum Computing
- Quantum Cryptography
- Quantum Future

No-Cloning Theorem



Quantum operations:

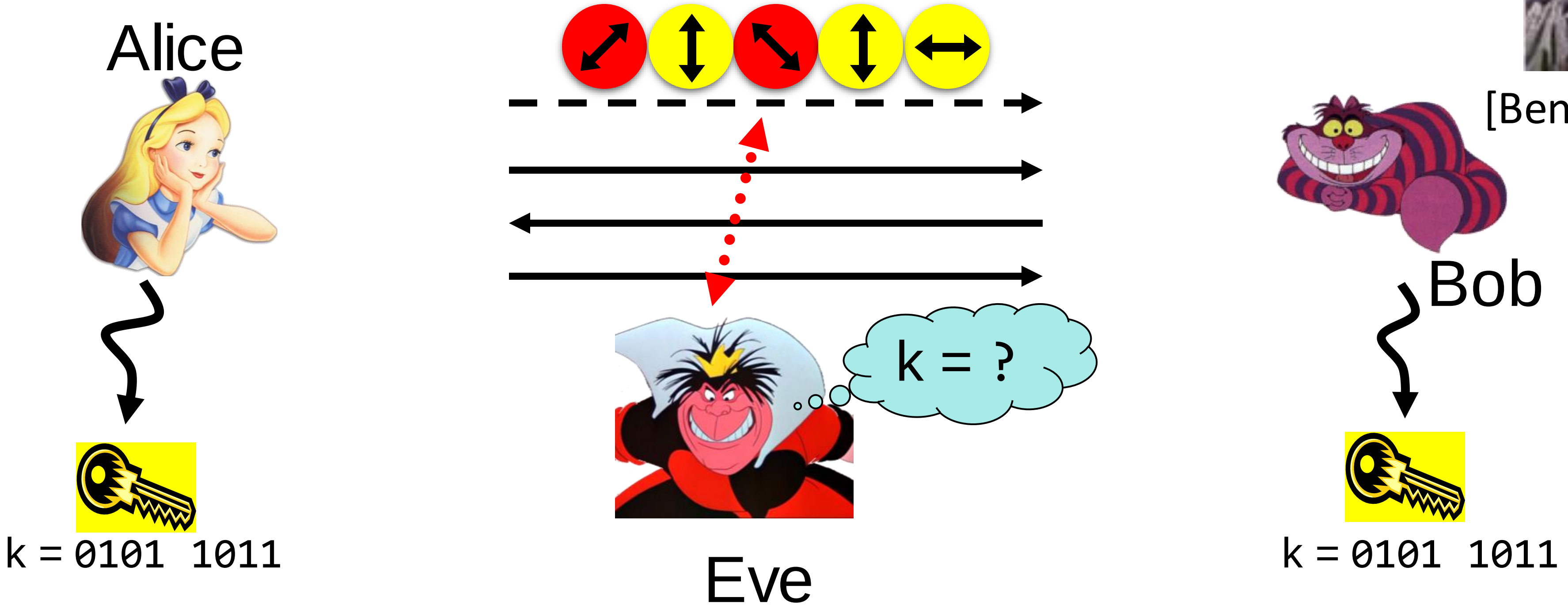




Proof: copying is a non-linear operation

Quantum Key Distribution (QKD)

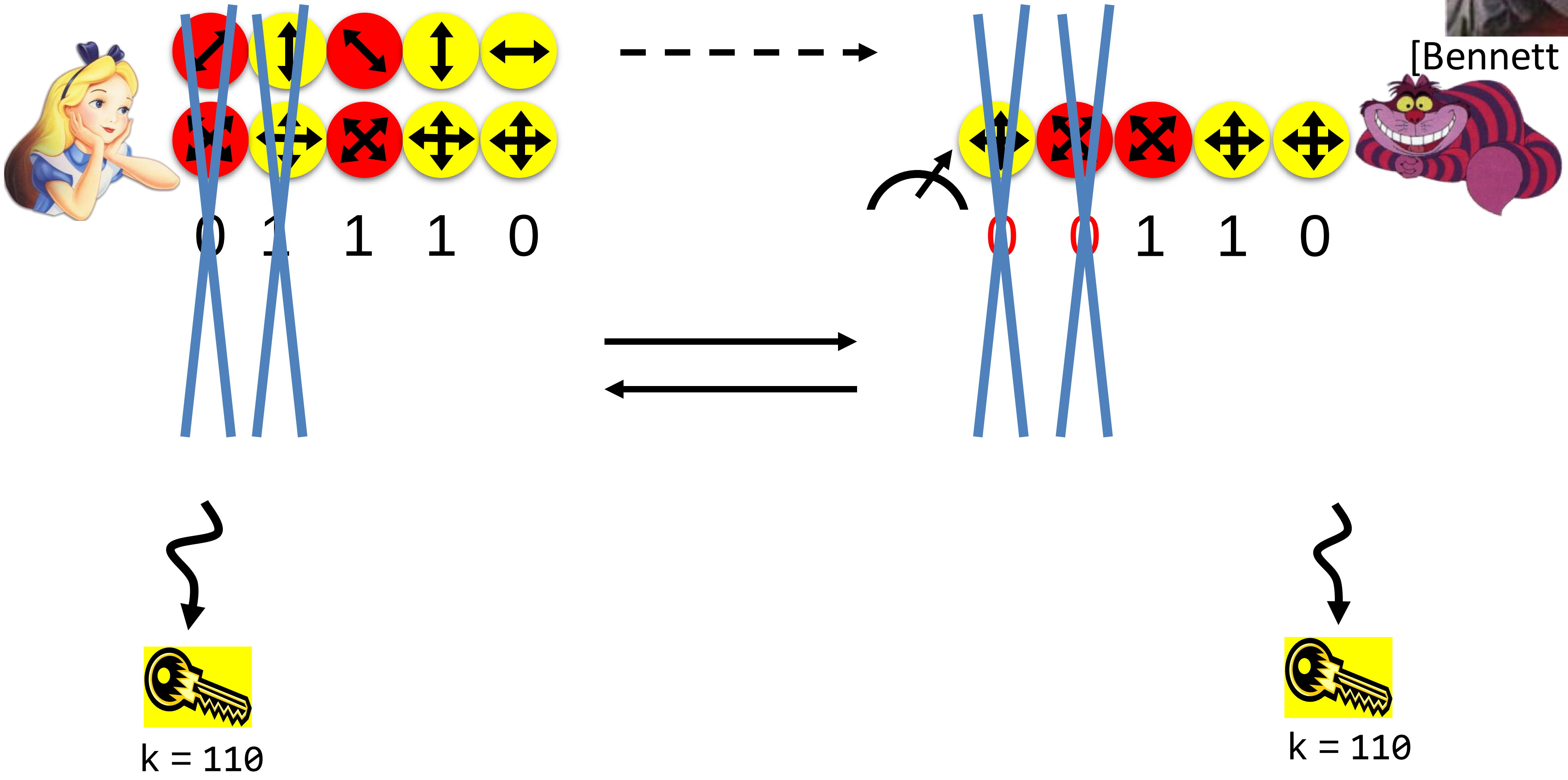
[Bennett Brassard 84]



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

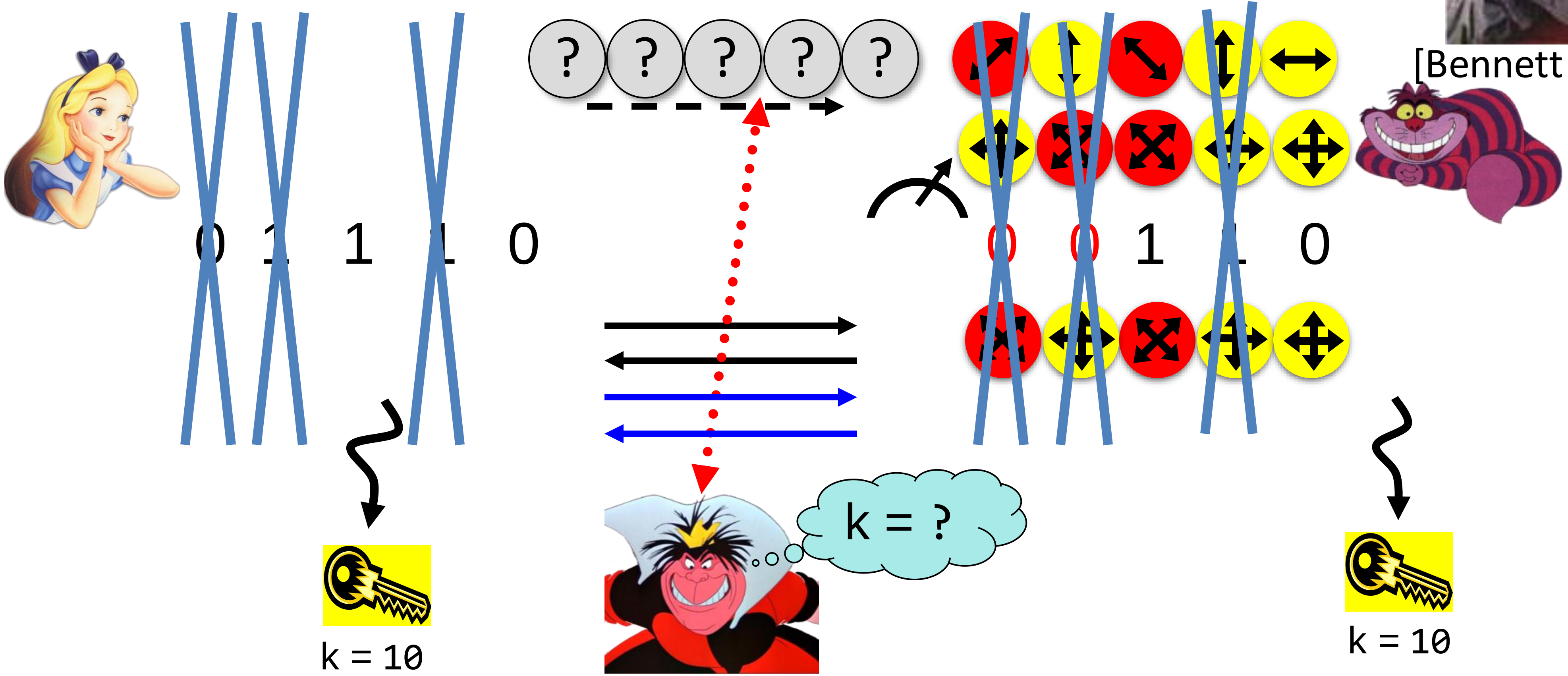
Quantum Key Distribution (QKD)

[Bennett Brassard 84]

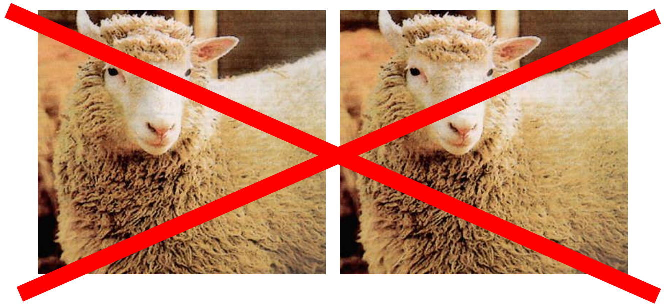


Quantum Key Distribution (QKD)

[Bennett Brassard 84]

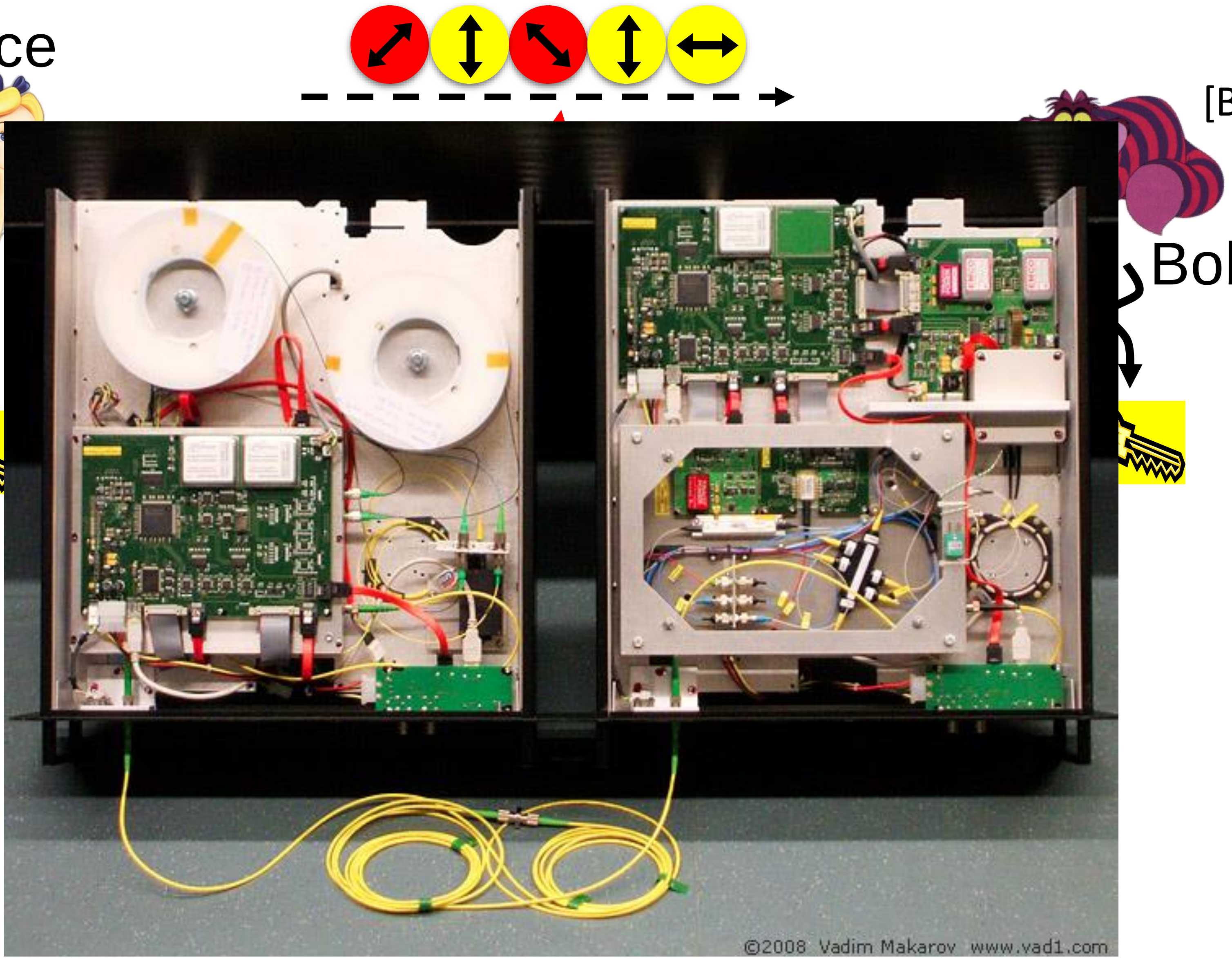


- Quantum states are unknown to Eve, she cannot copy them.
- Honest players can test whether Eve interfered.



Quantum Key Distribution (QKD)

[Bennett Brassard 84]



- tech
  only

What will you Learn from this Talk?

- ✓ Classical Cryptography (& Politics)
- ✓ Introduction to Quantum Mechanics
- ✓ Crypto Threat of Quantum Computing
- ✓ Quantum Cryptography
- Quantum Future

Quantum Research in NL

intel

Microsoft

QUTech

TNO

Universiteit Leiden

Research Center for Quantum Software

TU/e Technische Universiteit **Eindhoven** University of Technology

QuTech: 135 Mio € , 50 Mio $ Intel

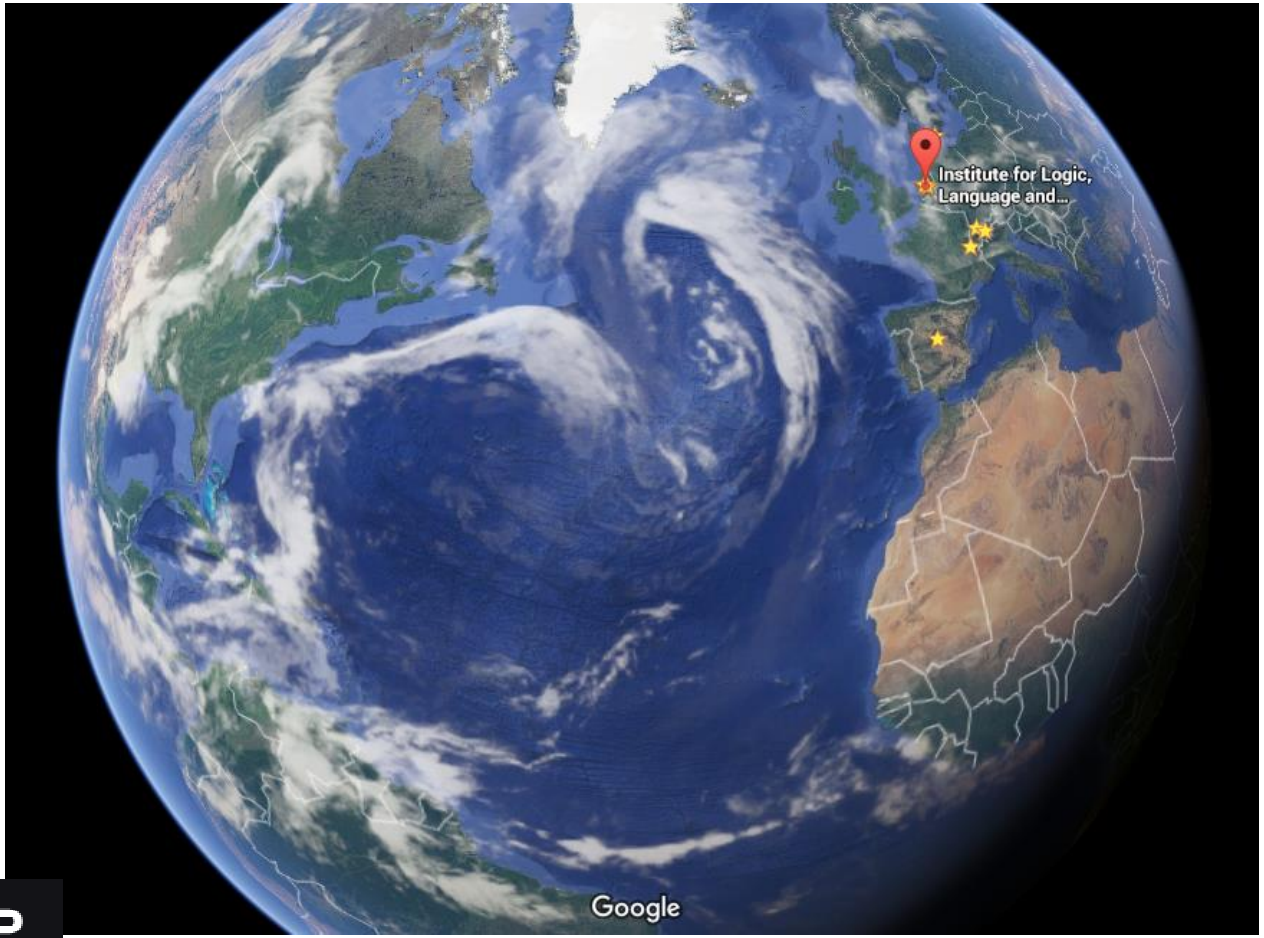
Nov 2017: Quantum Software Consortium, NWO 18.8 Mio € for 10 years

Quantum Research in EU

Starting 2018: 1 (or 2?) Bio. € flagship program on Q technologies

Quantum Research Worldwide

Google
IBM
intel
Microsoft
D:Wave
The Quantum Computing Company™

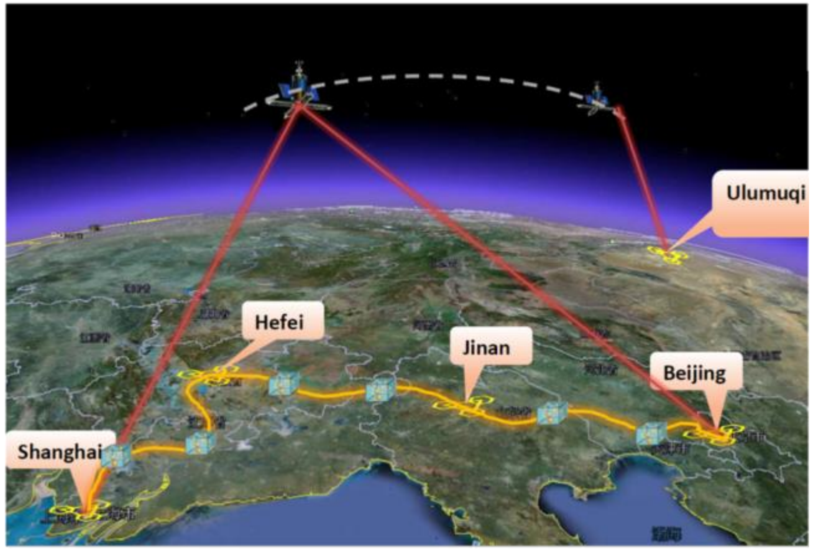


1QBit
Sparrow Quantum
Q^X Branch
rigetti
IONQ
evolutionQ
XANADU
TURING

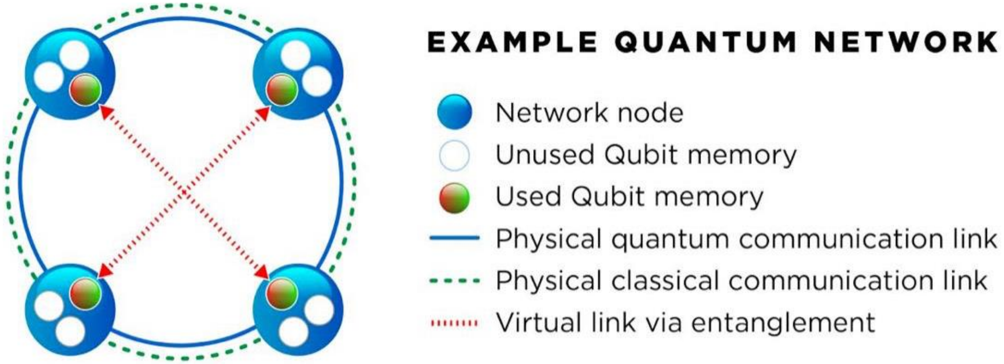
Waterloo, Singapore, Santa Barbara, China, …

Quantum Networks

- 2000km QKD backbone network between Beijing and Shanghai
- first QKD satellite launched in 2016 from China



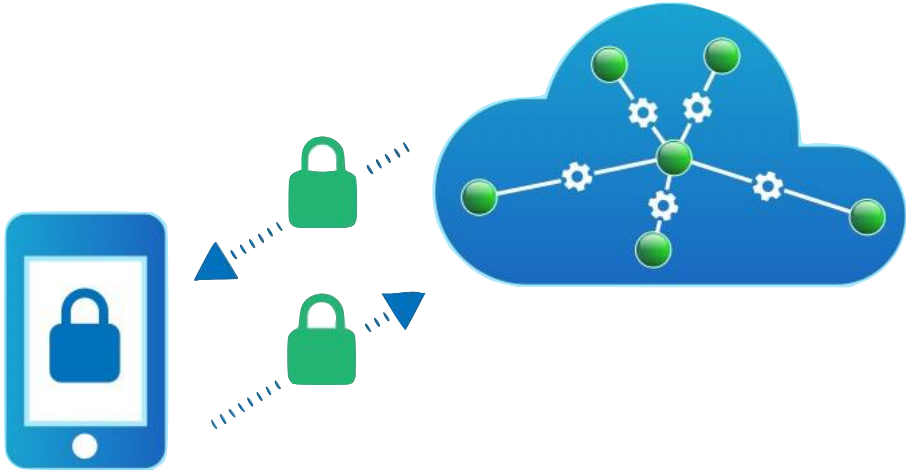
- Quantum entanglement allows to generate secure keys (like QKD)



Secure Computing in Quantum Cloud

- Distributed quantum computing

- Recent result: quantum homomorphic encryption allows for secure delegated quantum computation



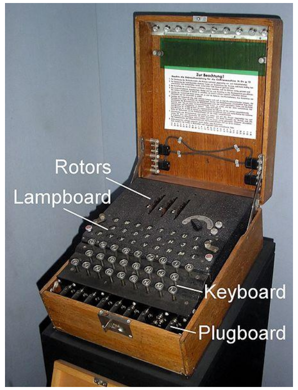
https://quantumexperience.ng.bluemix.net

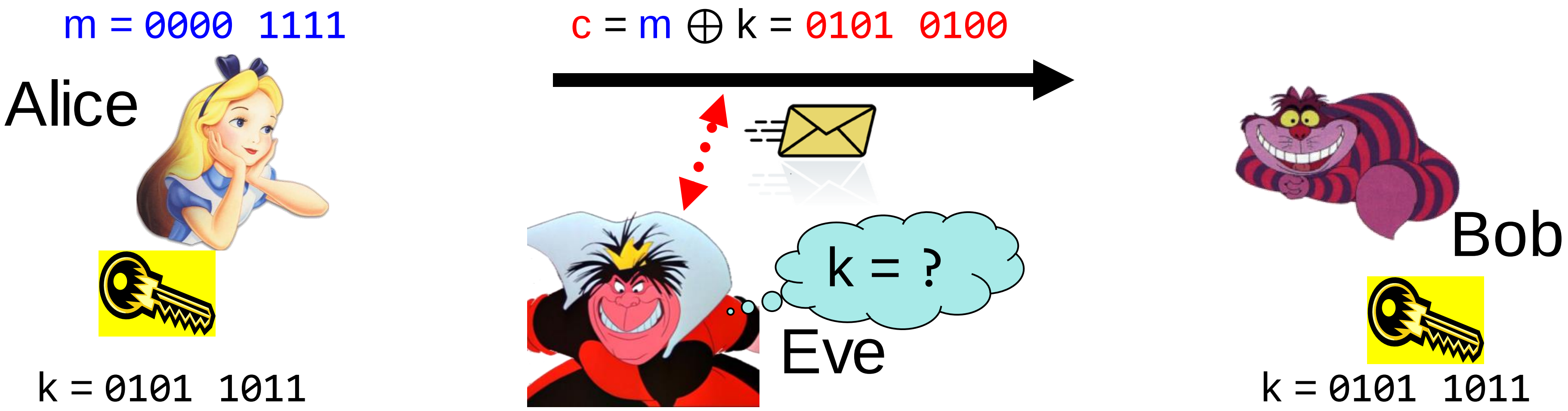
Y. Dulek, C. Schaffner, and F. Speelman, arXiv:1603.09717
Quantum homomorphic encryption for polynomial-sized circuits, in CRYPTO 2016, QIP 2017

What Have You Learned from this Talk?

✓ Classical Cryptography

- Long history
- One-time pad





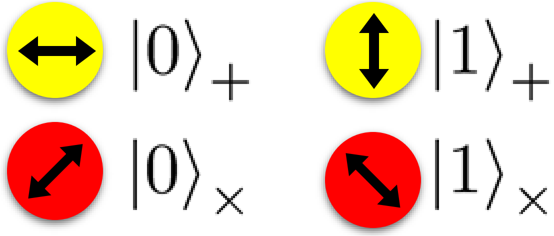
- Public-key cryptography
- Links to Logic and Politics

Sleepwet
Referendum

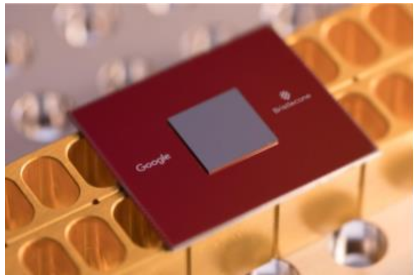
What Have You Learned from this Talk?

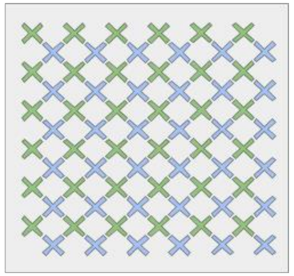
✓ Quantum Mechanics

- Qubits

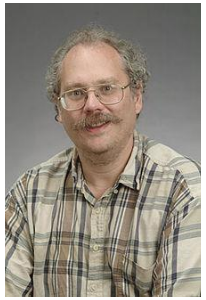


- Quantum Computer

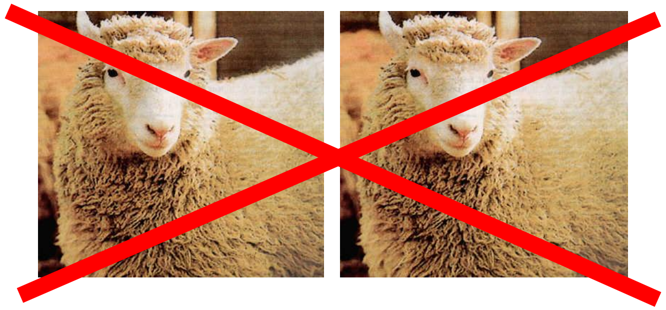




- Shor's Algorithm



- No-cloning



Answers to the Quantum Threat

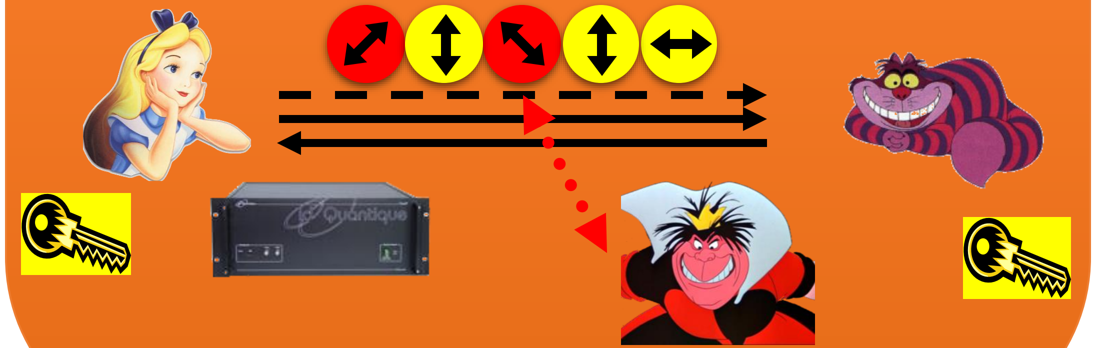
Conventional Post-Quantum Cryptography

- Can be deployed without quantum technologies
- Believed to be secure against quantum attacks of the future

+

Quantum Cryptography

- Requires some quantum technology (but no large-scale quantum computer)
- Typically no computational assumptions



Thank you for your attention!

Questions

http://www.qusoft.org/education/