iCIS | Digital Security
Radboud University

Post-quantum Cryptography

Simona Samardjiska
Digital Security Group – Radboud University

Outline

What is
Post-quantum Cryptography???

Outline

What is
Post-quantum Cryptography???

1. What is Cryptography?

Outline

What is Post-quantum Cryptography???

1. What is Cryptography?

Important:
Crypto = Cryptography
Crypto ≠ Cryptocurrency

Outline

What is
Post-quantum Cryptography???

1. What is Cryptography?
2. What is quantum cryptography?

Outline

What is
Post-quantum Cryptography???

1. What is Cryptography?
2. ~~What is quantum cryptography?~~

Outline

What is
Post-quantum Cryptography???

1. What is Cryptography?
2. ~~What is quantum cryptography?~~
3. What is a quantum computer?

Outline

What is
Post-quantum Cryptography???

1. What is Cryptography?
2. ~~What is quantum cryptography?~~
3. What is a quantum computer?
4. **1994**: A thought battle

Quantum Computers		Crypto
1	:	0

Outline

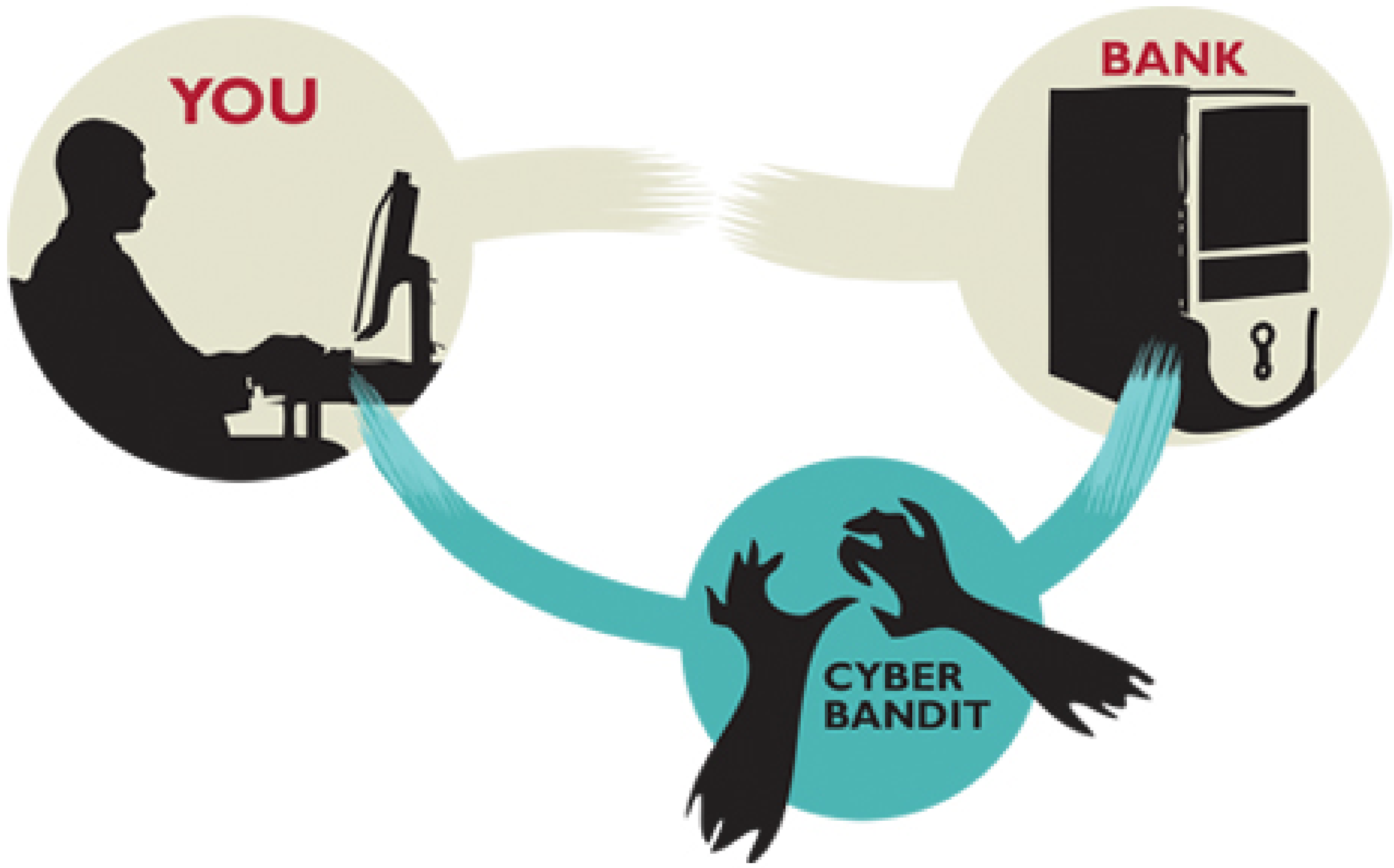
What is
Post-quantum Cryptography???

1. What is Cryptography?
2. ~~What is quantum cryptography?~~
3. What is a quantum computer?
4. **1994**: A thought battle

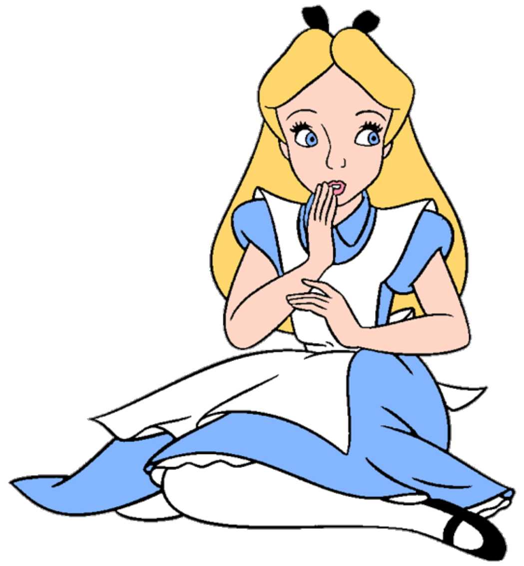
Quantum Computers	:	Crypto
1	:	0

5. **Today**: Are we prepared for the real thing?

Cryptography - Securing our digital world



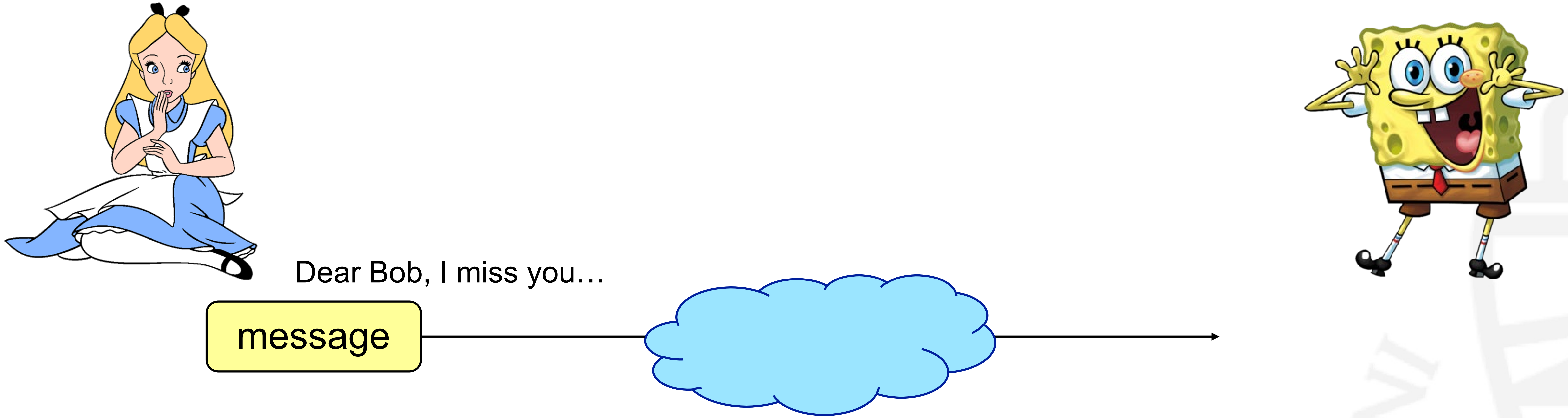
Alice and Bob want to communicate over the Internet…privately



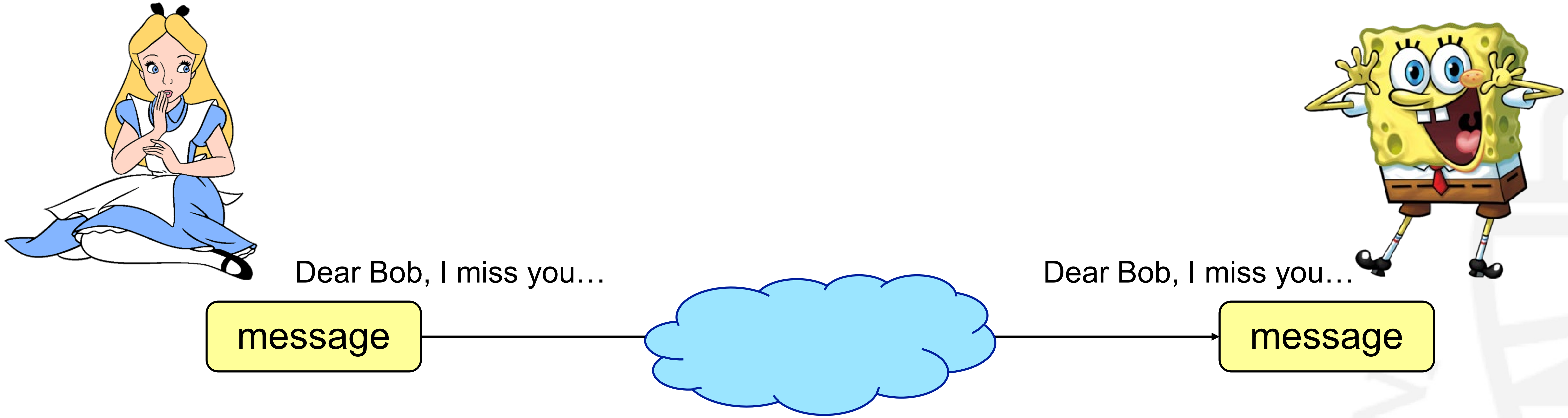
Dear Bob, I miss you…

message

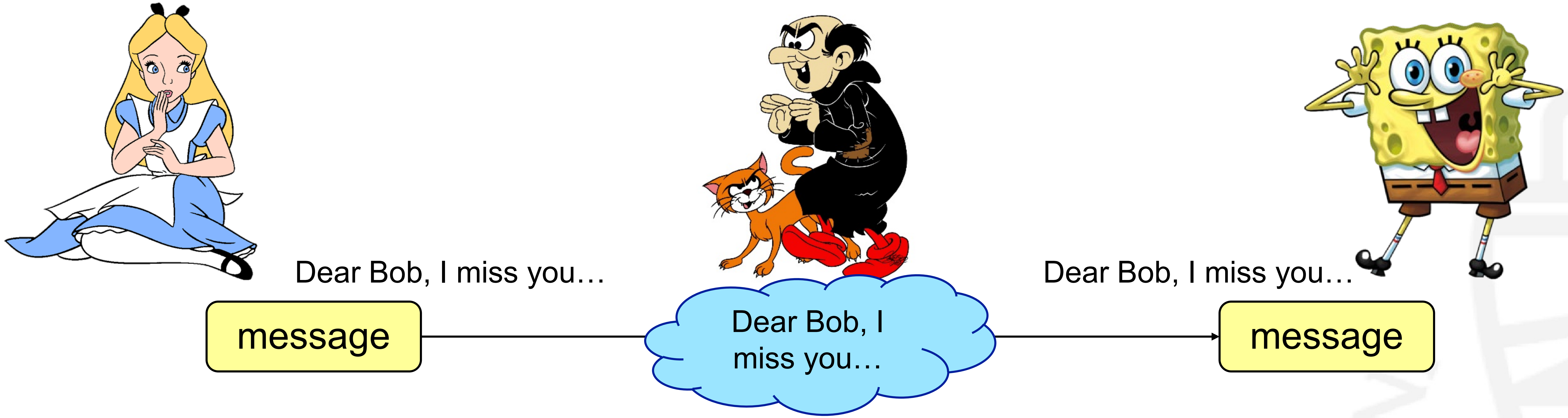
Alice and Bob want to communicate over the Internet…privately



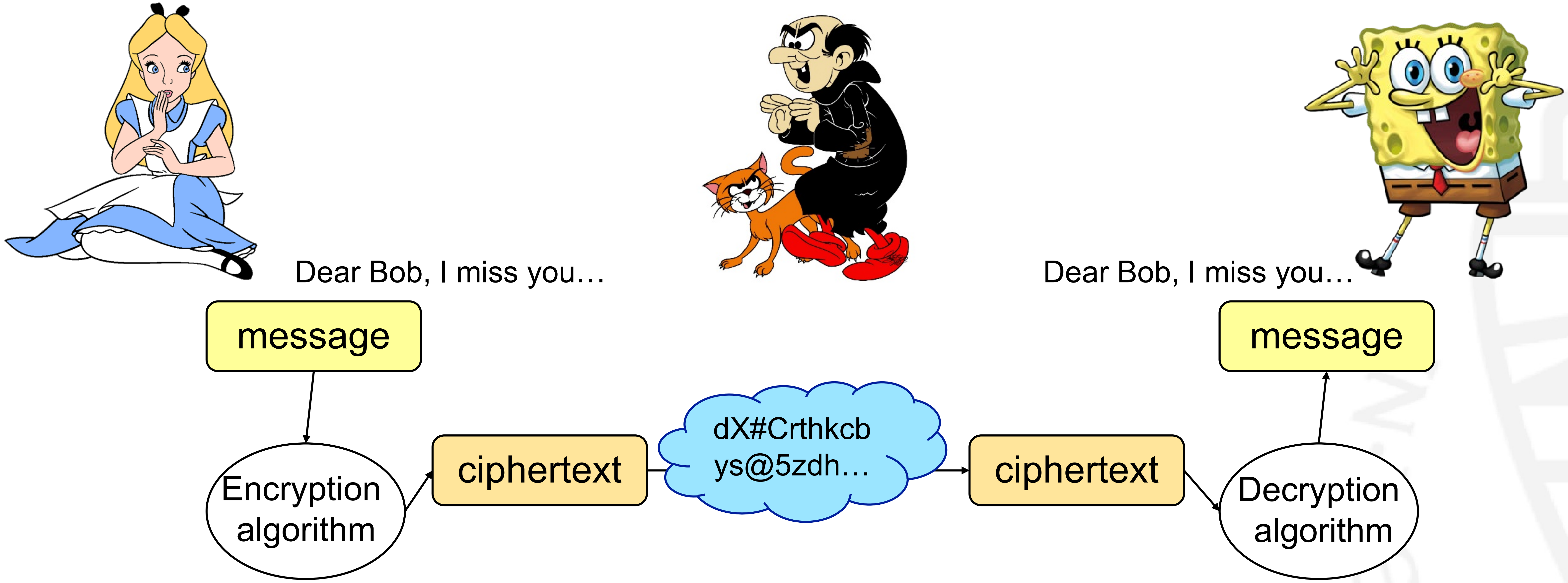
Alice and Bob want to communicate over the Internet…privately



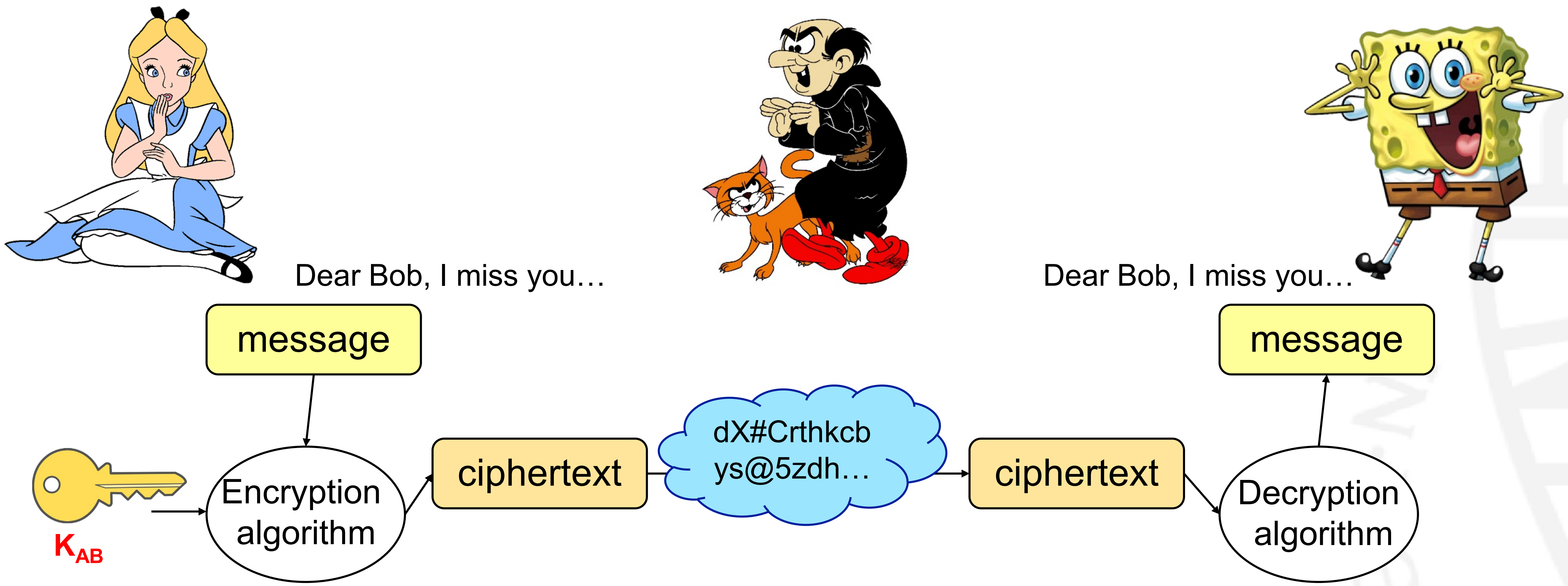
Alice and Bob want to communicate over the Internet…privately



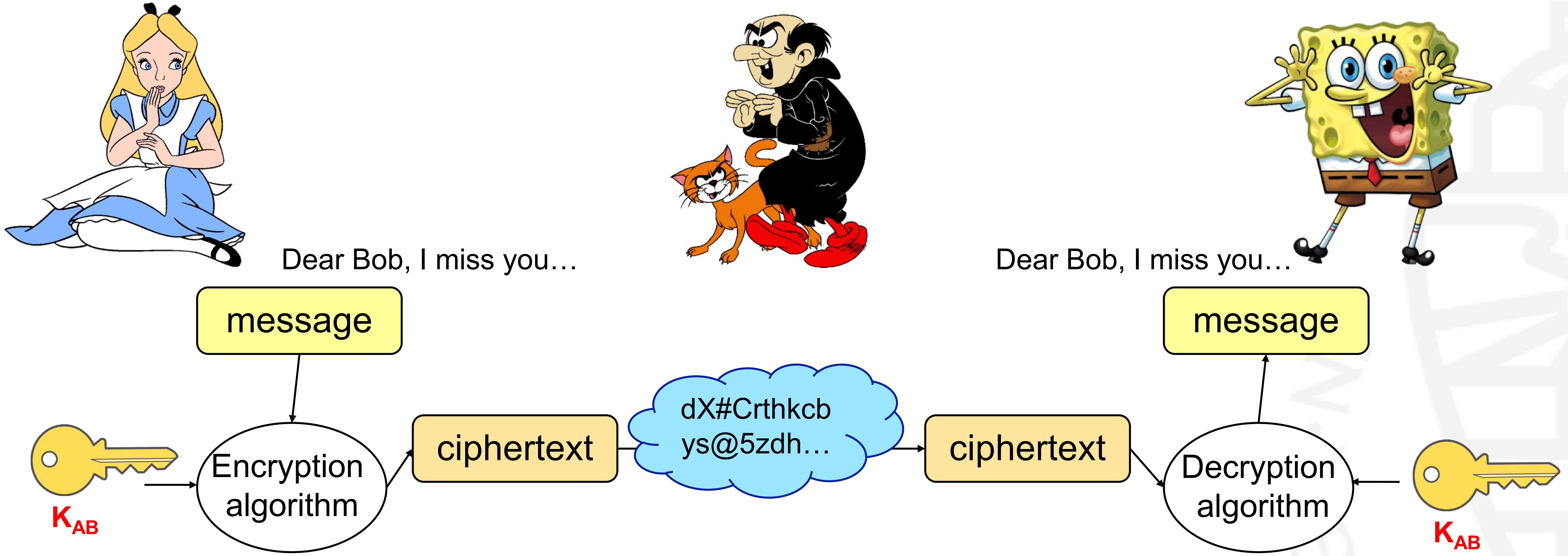
Alice and Bob want to communicate over the Internet…privately



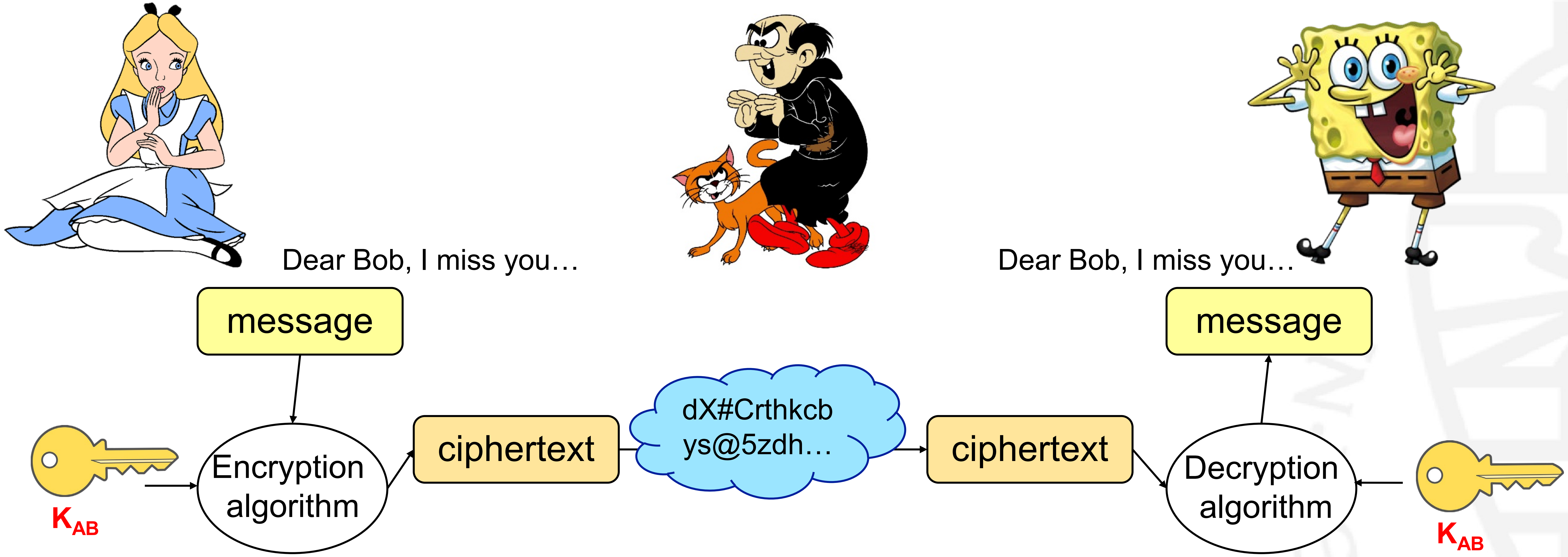
Alice and Bob want to communicate over the Internet…privately



Alice and Bob want to communicate over the Internet…privately

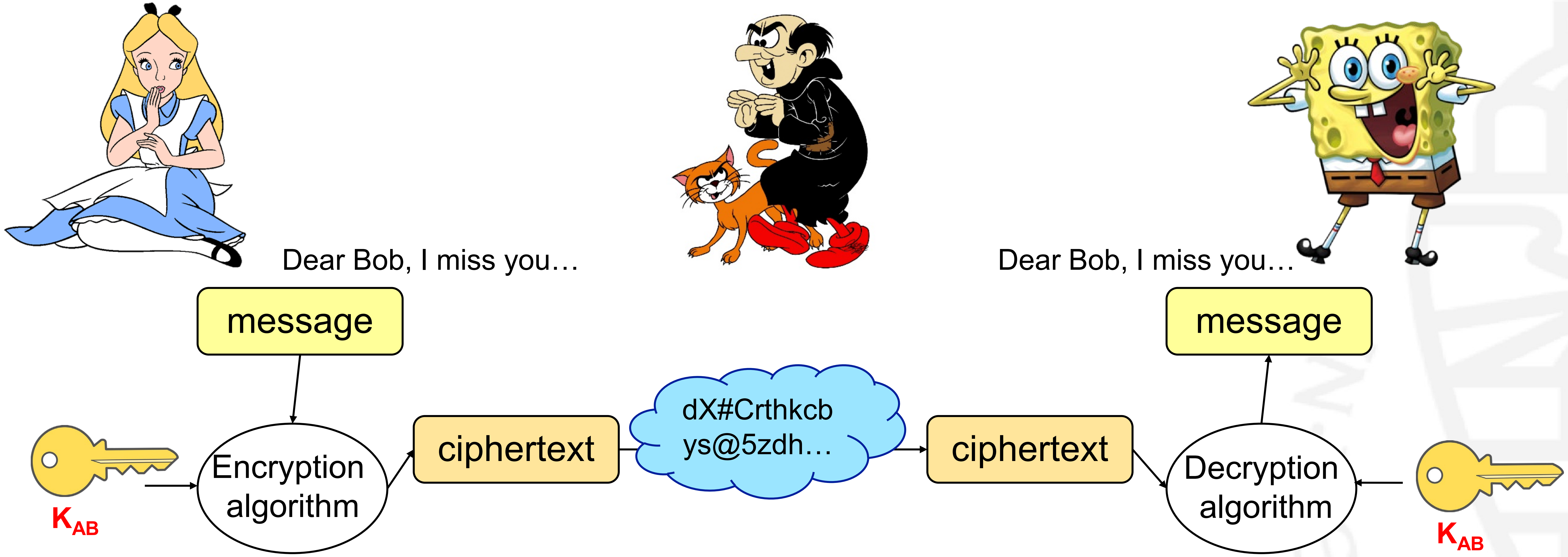


Alice and Bob want to communicate over the Internet…privately



Symmetric cryptography

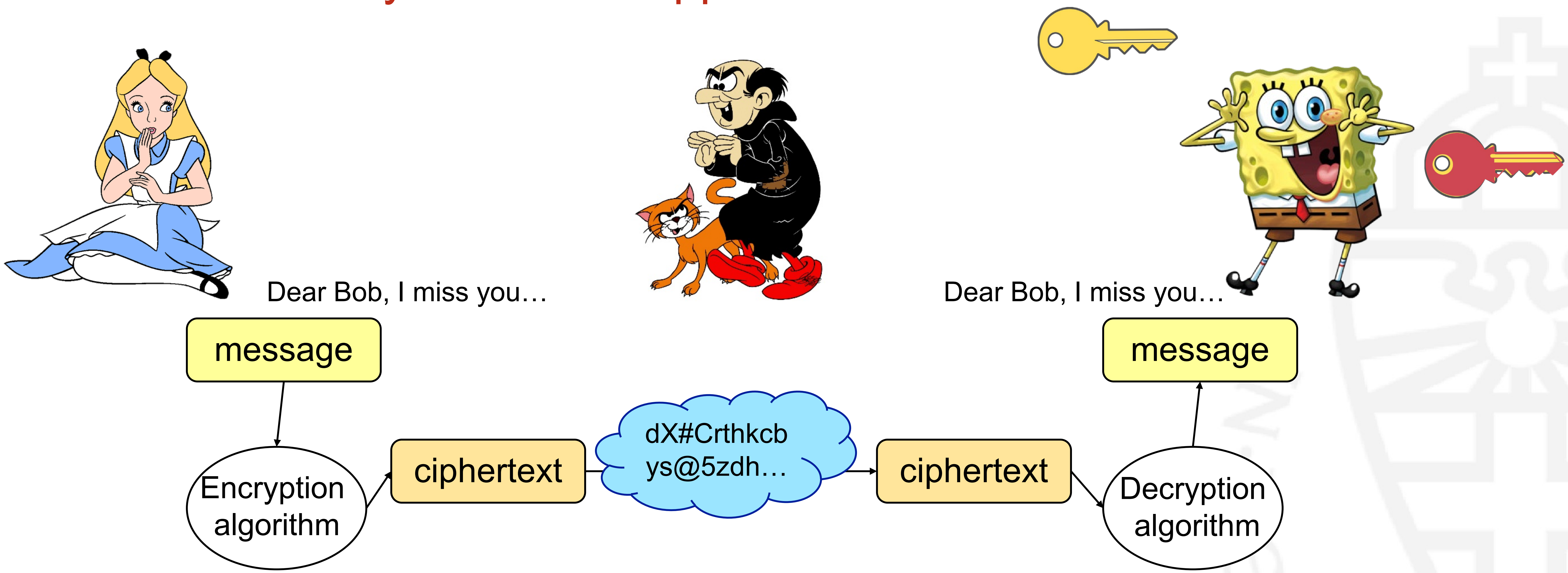
Alice and Bob want to communicate over the Internet…privately



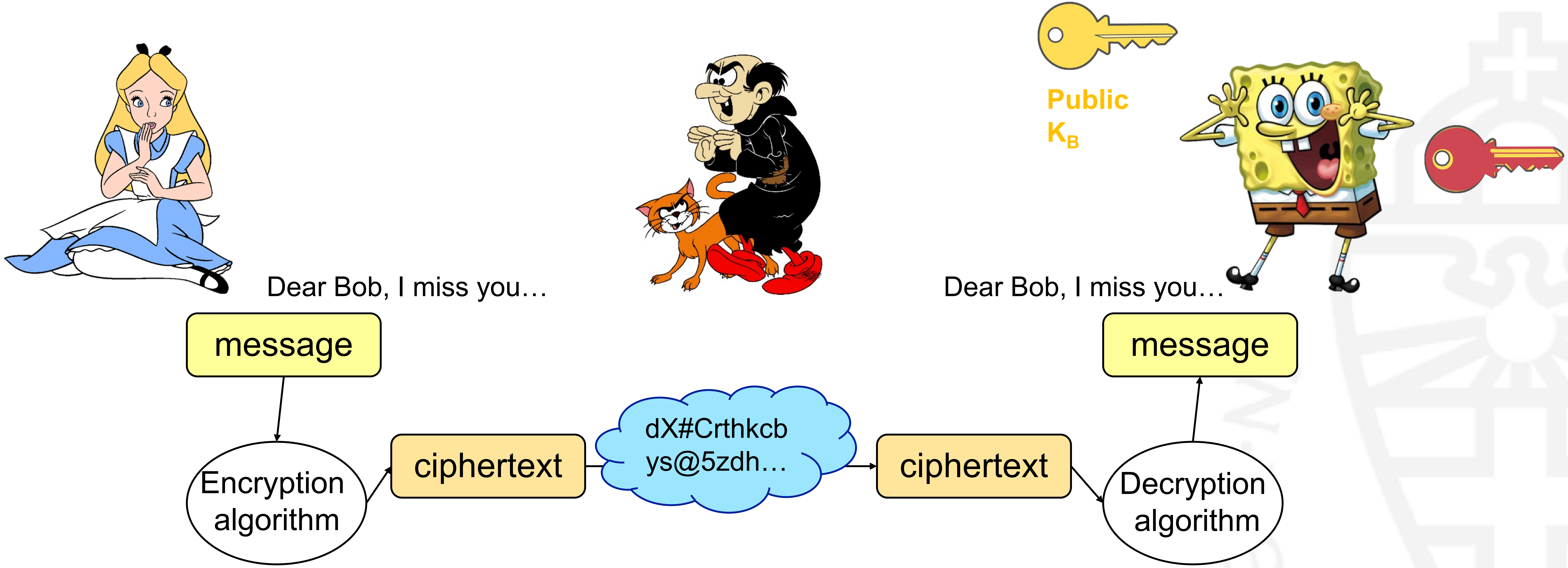
Symmetric cryptography

Problem: Alice and Bob need to agree on the key previously!

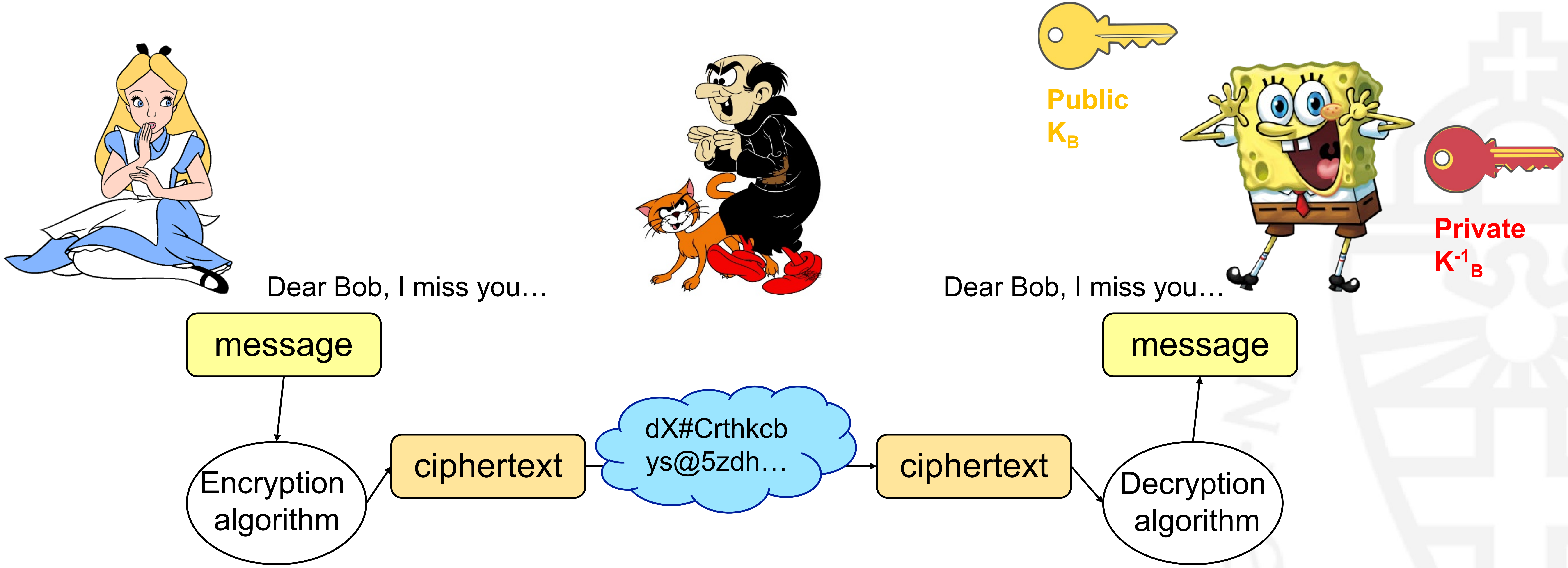
Alice and Bob try a different approach



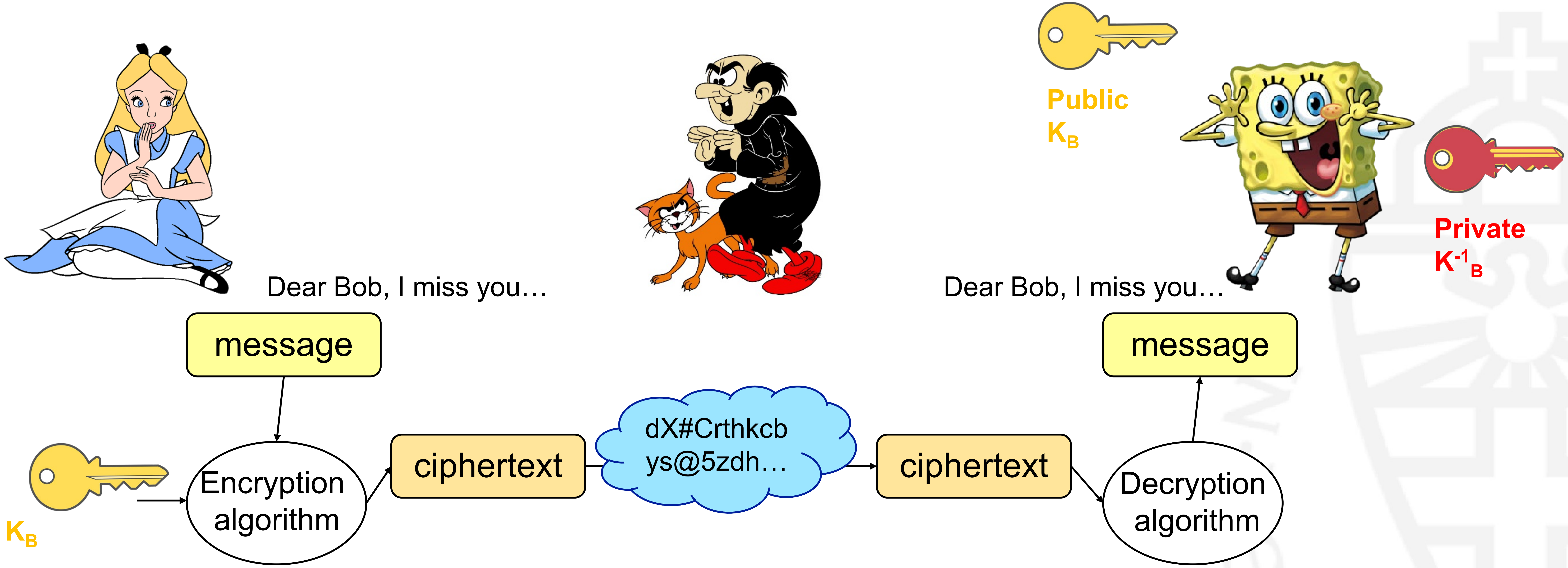
Alice and Bob try a different approach



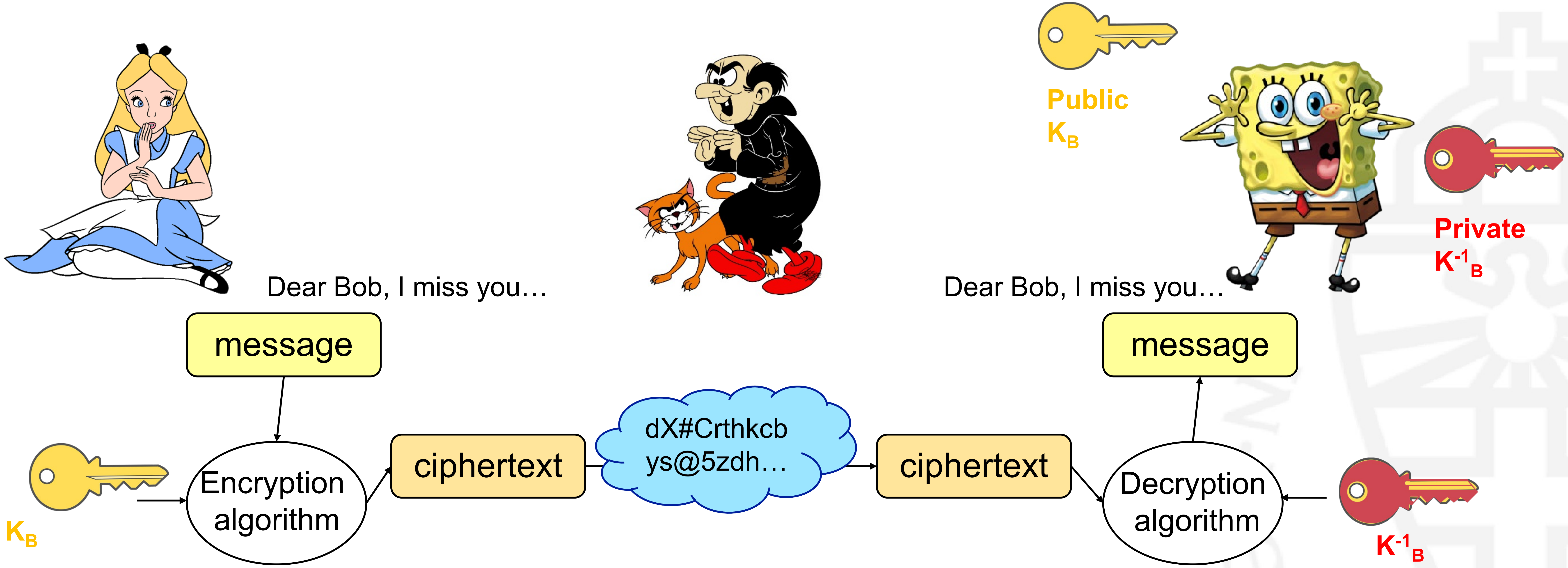
Alice and Bob try a different approach



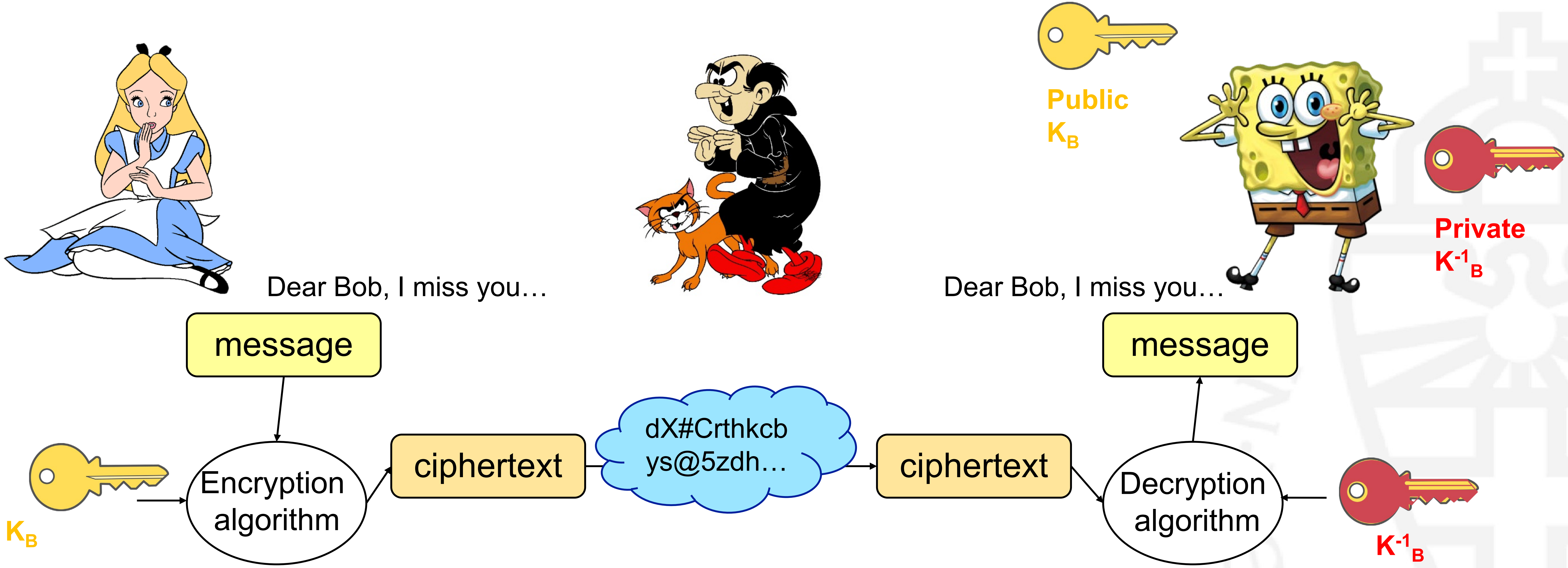
Alice and Bob try a different approach



Alice and Bob try a different approach



Alice and Bob try a different approach



Public key cryptography

Problem: Too costly! But, they can communicate only the key,
and use symmetric crypto afterwards!

Alice and Bob have more problems than just secrecy…

Alice and Bob have more problems than just secrecy…

- How can they make sure nobody changed their messages during transport?

Alice and Bob have more problems than just secrecy…

- How can they make sure nobody changed their messages during transport?
- How can Bob make sure the message comes from Alice?

Alice and Bob have more problems than just secrecy…

- How can they make sure nobody changed their messages during transport?

- How can Bob make sure the message comes from Alice?
- How can Bob make sure he is talking to Alice?

Alice and Bob have more problems than just secrecy…

- How can they make sure nobody changed their messages during transport?

- How can Bob make sure the message comes from Alice?
- How can Bob make sure he is talking to Alice?
- How can Alice make sure she is talking to Bob?

Alice and Bob have more problems than just secrecy…

- How can they make sure nobody changed their messages during transport?

- How can Bob make sure the message comes from Alice?
- How can Bob make sure he is talking to Alice?
- How can Alice make sure she is talking to Bob?

- How can Bob prove that Alice sent some message?

Alice and Bob have more problems than just secrecy…

- How can they make sure nobody changed their messages during transport?

- How can Bob make sure the message comes from Alice?
- How can Bob make sure he is talking to Alice?
- How can Alice make sure she is talking to Bob?

- How can Bob prove that Alice sent some message?

- How can they make sure that even if Malice finds out a private key, their previous communication is secure?

Alice and Bob have more problems than just secrecy…

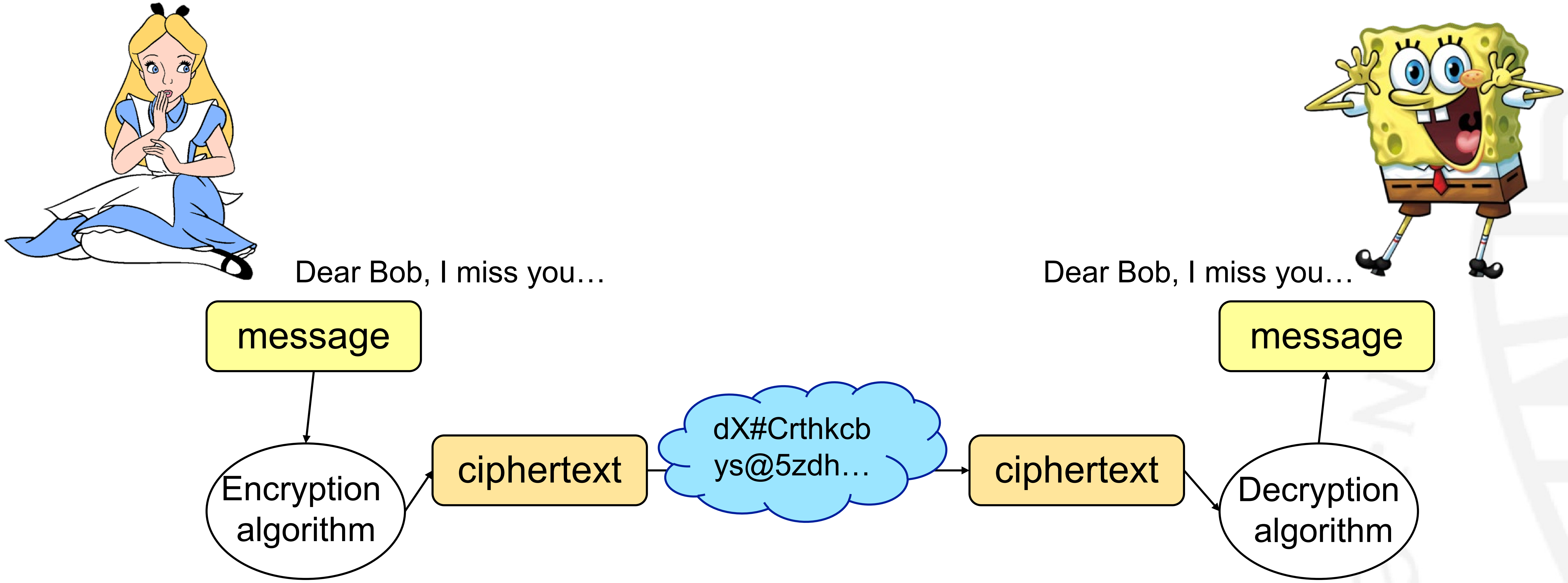
- How can they make sure nobody changed their messages during transport?

- How can Bob make sure the message comes from Alice?
- How can Bob make sure he is talking to Alice?
- How can Alice make sure she is talking to Bob?

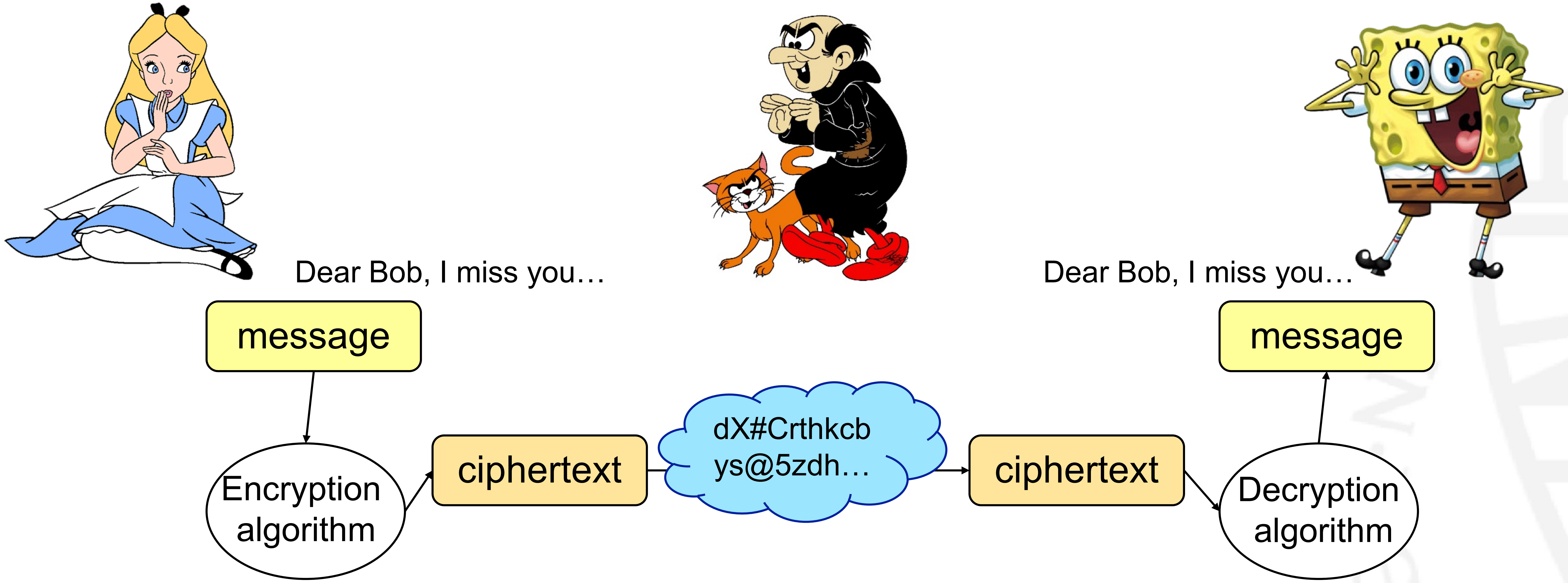
- How can Bob prove that Alice sent some message?

- How can they make sure that even if Malice finds out a private key, their previous communication is secure?
- …
- …
- …

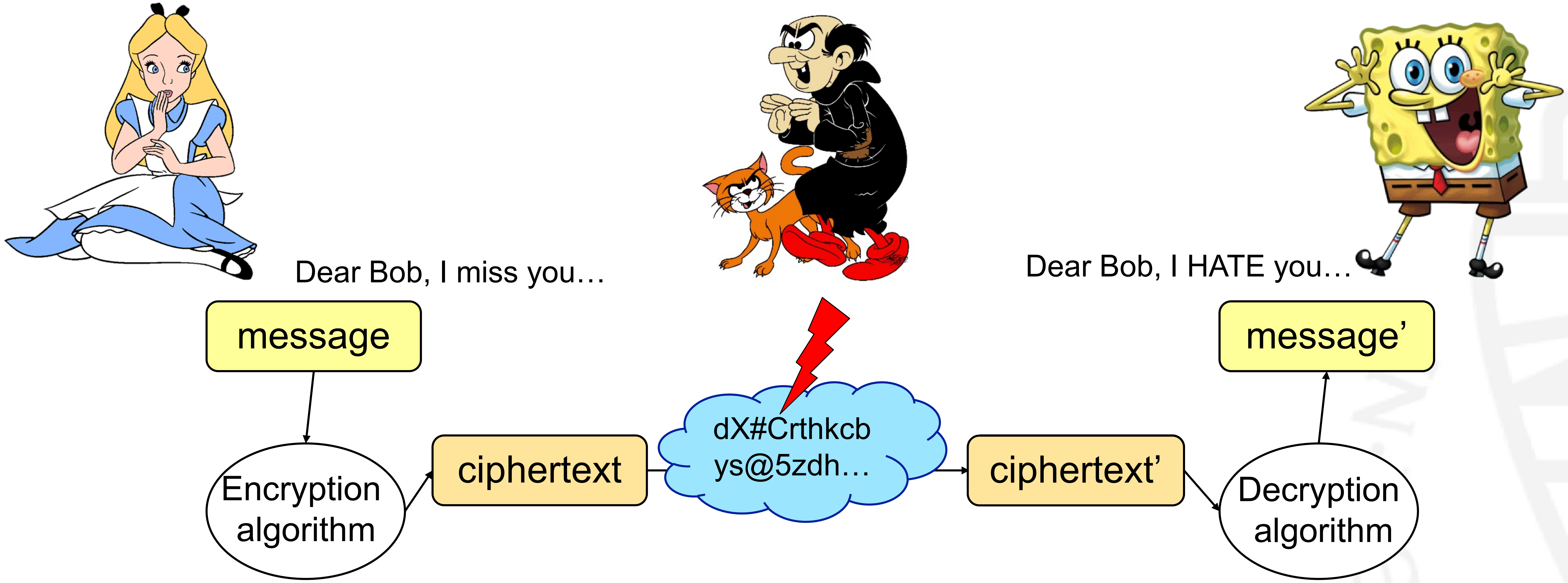
Alice and Bob have more problems than just secrecy…



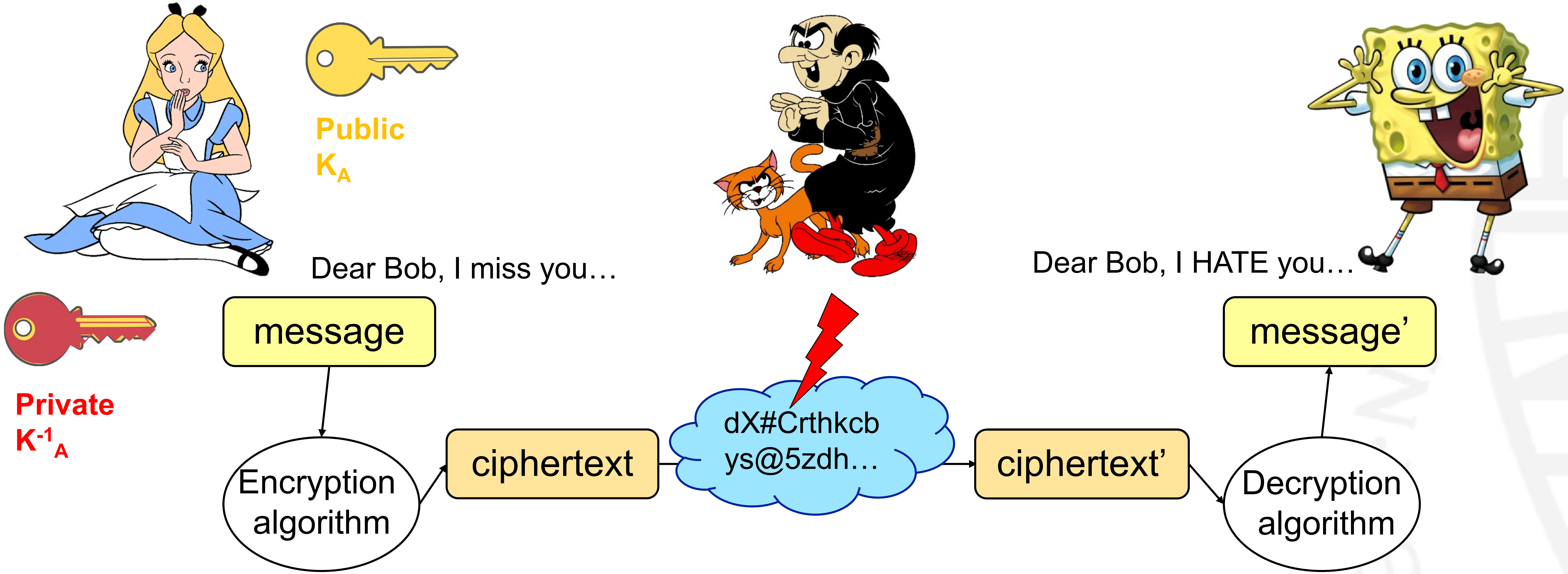
Alice and Bob have more problems than just secrecy…



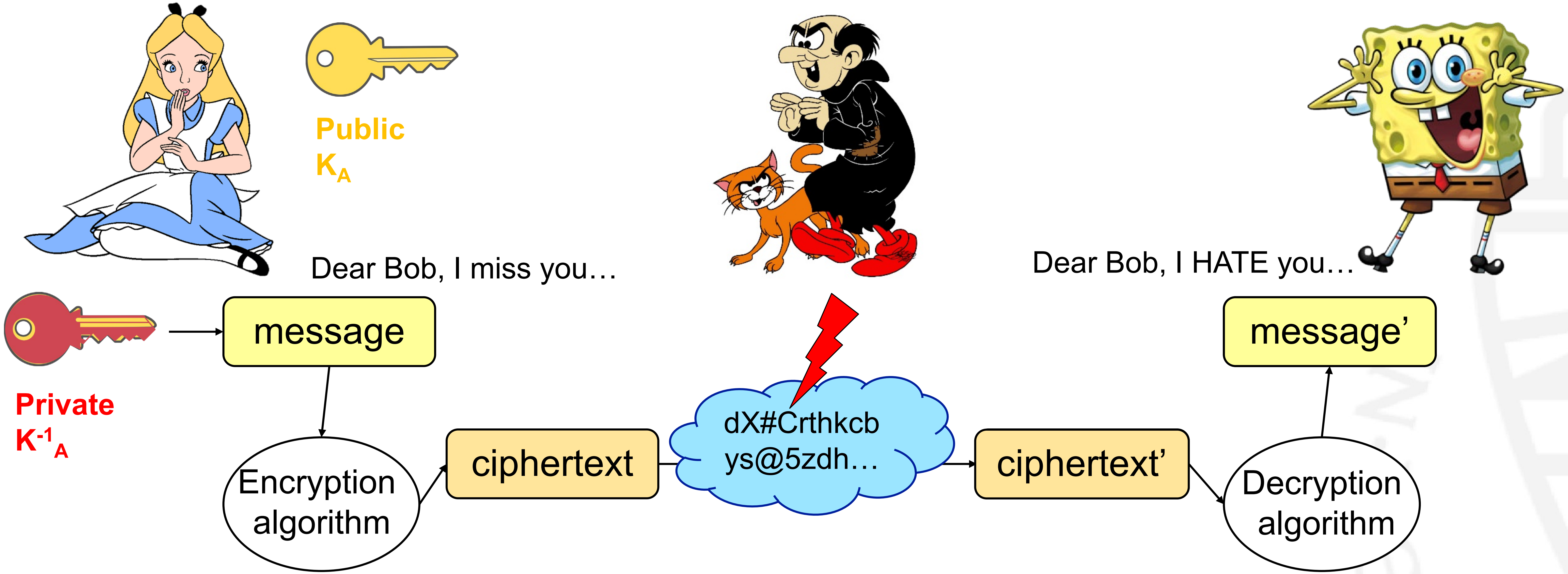
Alice and Bob have more problems than just secrecy…



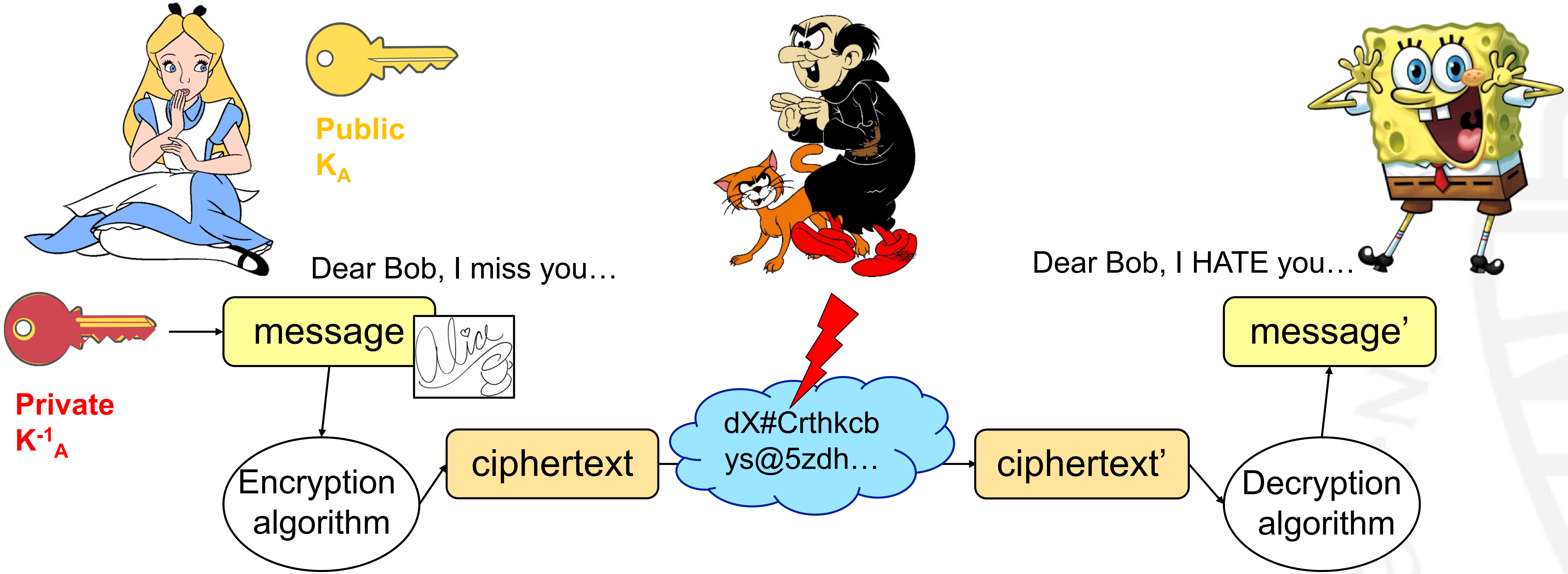
Alice and Bob have more problems than just secrecy…



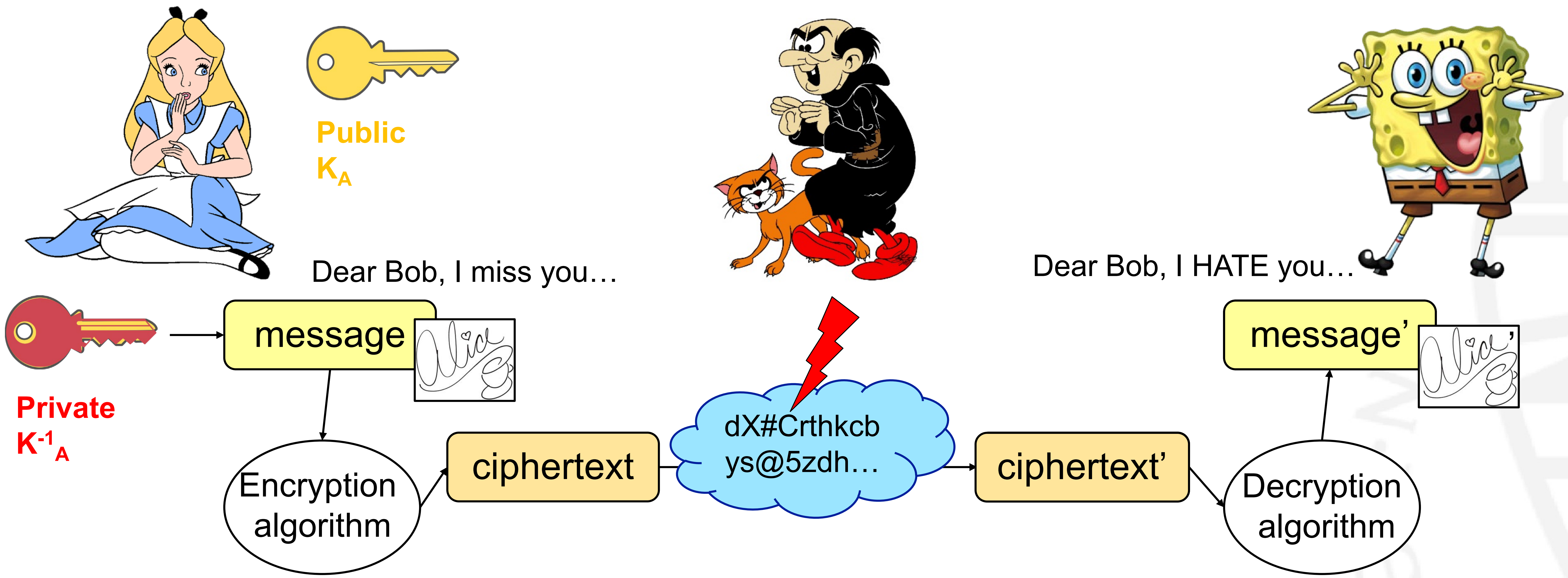
Alice and Bob have more problems than just secrecy…



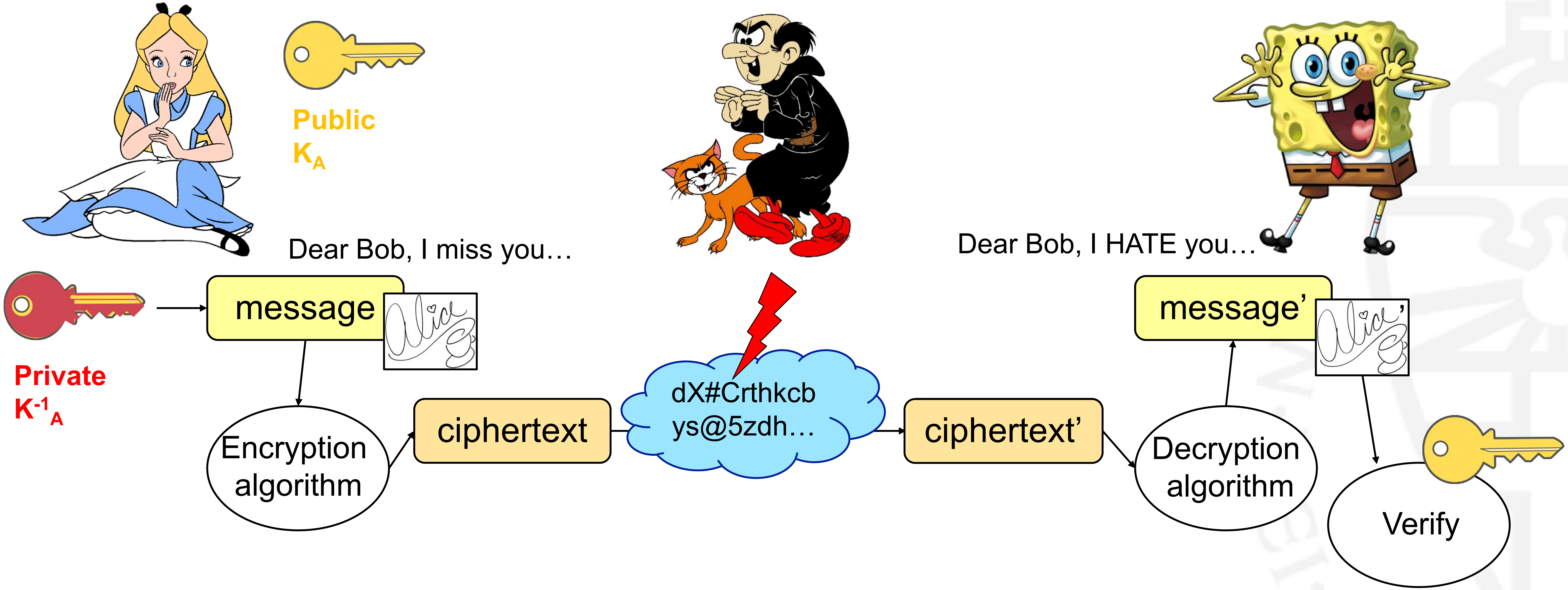
Alice and Bob have more problems than just secrecy…



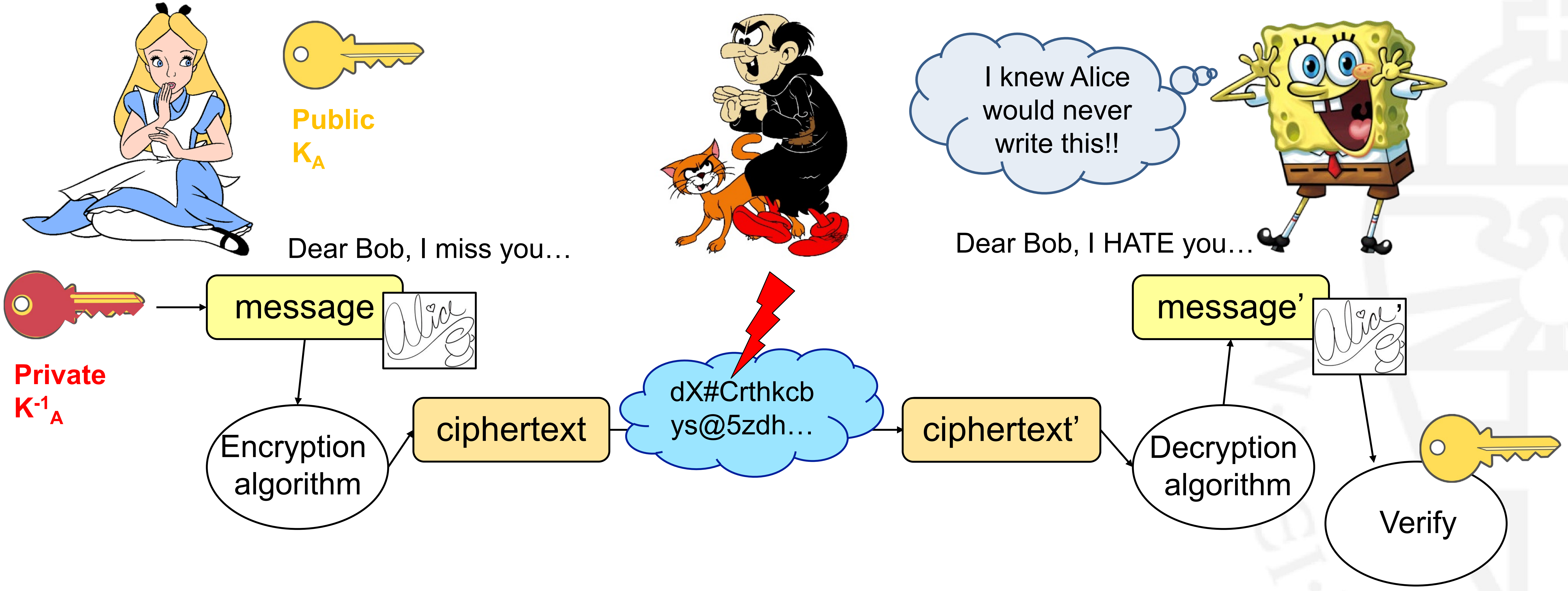
Alice and Bob have more problems than just secrecy…



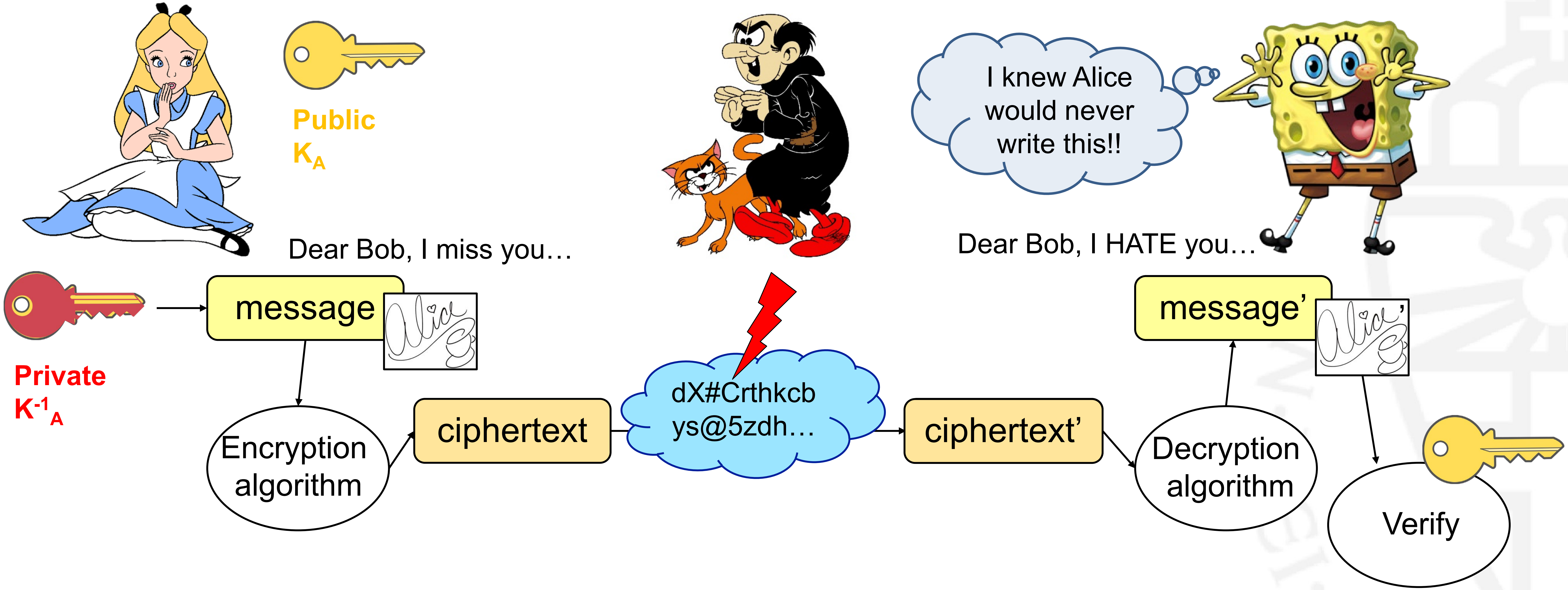
Alice and Bob have more problems than just secrecy…



Alice and Bob have more problems than just secrecy…



Alice and Bob have more problems than just secrecy…



Digital signatures - A Swiss army knife in cryptography

Today's cryptography in use?

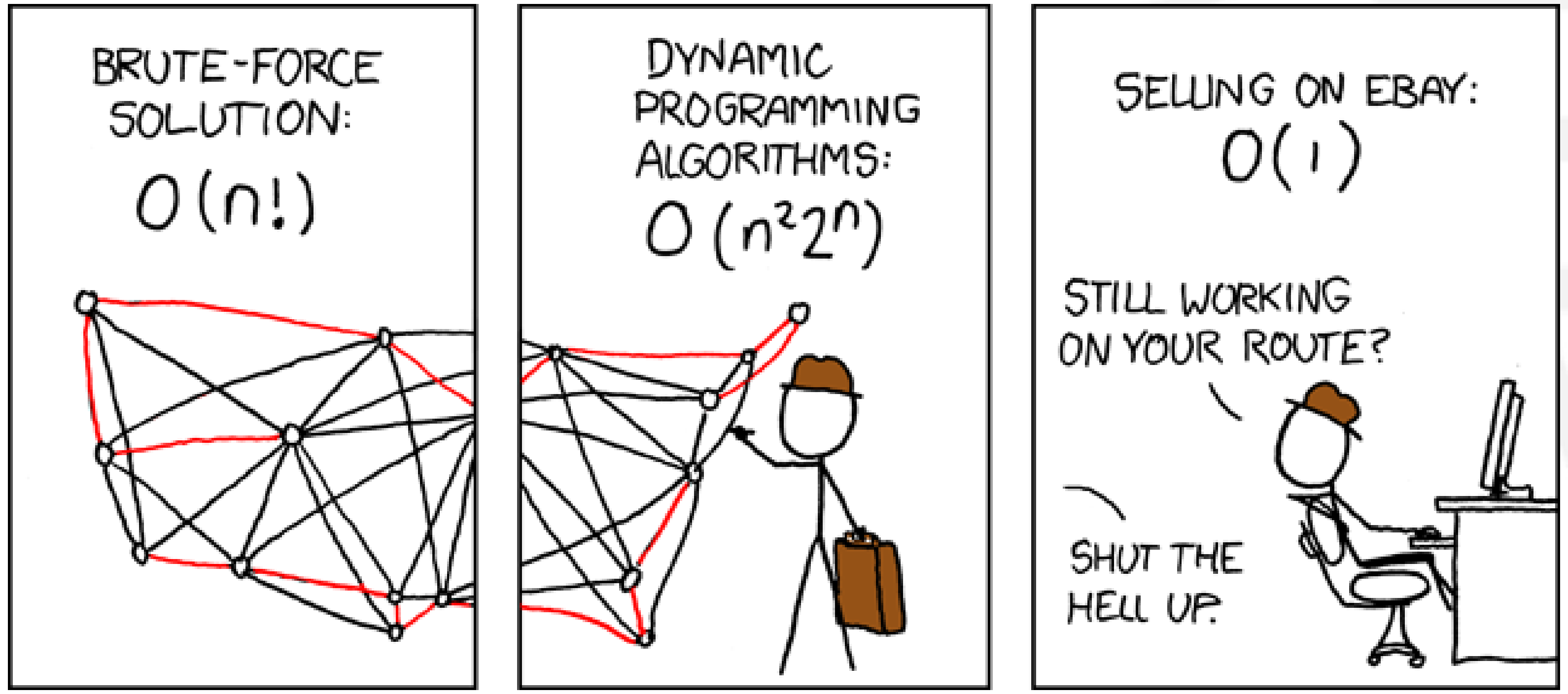
- Based on computationally hard problems

$(x \text{ OR } y \text{ OR } z) \text{ AND } (x \text{ OR } \bar{y} \text{ OR } z) \text{ AND}$

$(x \text{ OR } y \text{ OR } \bar{z}) \text{ AND } (x \text{ OR } \bar{y} \text{ OR } \bar{z}) \text{ AND}$

$(\bar{x} \text{ OR } y \text{ OR } z) \text{ AND } (\bar{x} \text{ OR } \bar{y} \text{ OR } \bar{z})$

$$\underbrace{\begin{bmatrix}1 & 2 & 3\end{bmatrix}}_{1\times 3} \cdot \underbrace{\begin{bmatrix}2 & 1 & 3\\ 3 & 3 & 2\\ 4 & 1 & 2\end{bmatrix}}_{3\times 3} = \begin{bmatrix}1\cdot 2+2\cdot 3+3\cdot 4\\ 1\cdot 1+2\cdot 3+3\cdot 1\\ 1\cdot 3+2\cdot 2+3\cdot 2\end{bmatrix} = \underbrace{\begin{bmatrix}20\\ 10\\ 13\end{bmatrix}}_{1\times 3}$$



Today's cryptography in use?

- Based on computationally hard problems

Easy

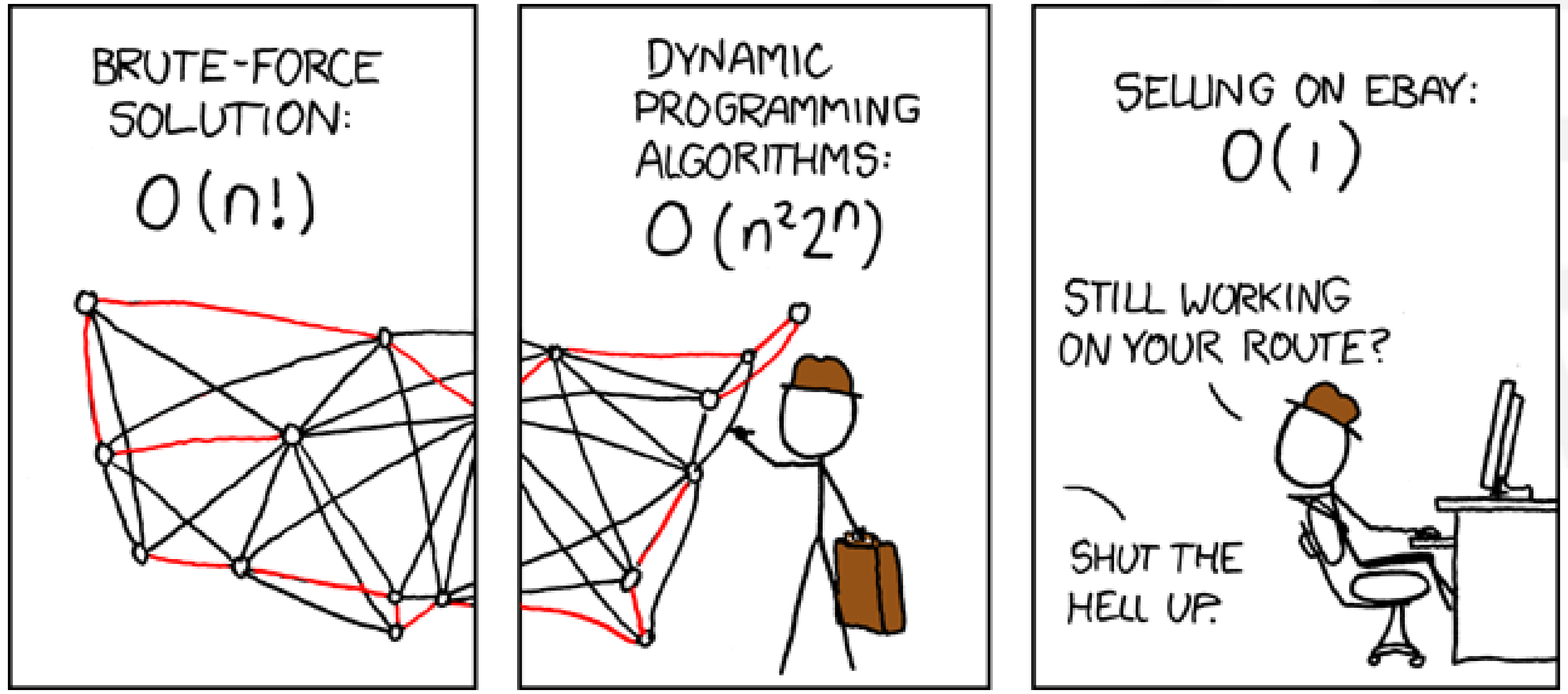
$O(n)$

$(x \text{ OR } y \text{ OR } z) \text{ AND } (x \text{ OR } \bar{y} \text{ OR } z) \text{ AND }$

$(x \text{ OR } y \text{ OR } \bar{z}) \text{ AND } (x \text{ OR } \bar{y} \text{ OR } \bar{z}) \text{ AND }$

$(\bar{x} \text{ OR } y \text{ OR } z) \text{ AND } (\bar{x} \text{ OR } \bar{y} \text{ OR } \bar{z})$

$$\underbrace{\begin{bmatrix} 1 & 2 & 3 \end{bmatrix}}_{1 \times 3} \cdot \underbrace{\begin{bmatrix} 2 & 1 & 3 \\ 3 & 3 & 2 \\ 4 & 1 & 2 \end{bmatrix}}_{3 \times 3} = \begin{bmatrix} 1\cdot 2 + 2\cdot 3 + 3\cdot 4 \\ 1\cdot 1 + 2\cdot 3 + 3\cdot 1 \\ 1\cdot 3 + 2\cdot 2 + 3\cdot 2 \end{bmatrix} = \underbrace{\begin{bmatrix} 20 \\ 10 \\ 13 \end{bmatrix}}_{1 \times 3}$$



Today's cryptography in use?

- Based on computationally hard problems

Easy
$O(n)$

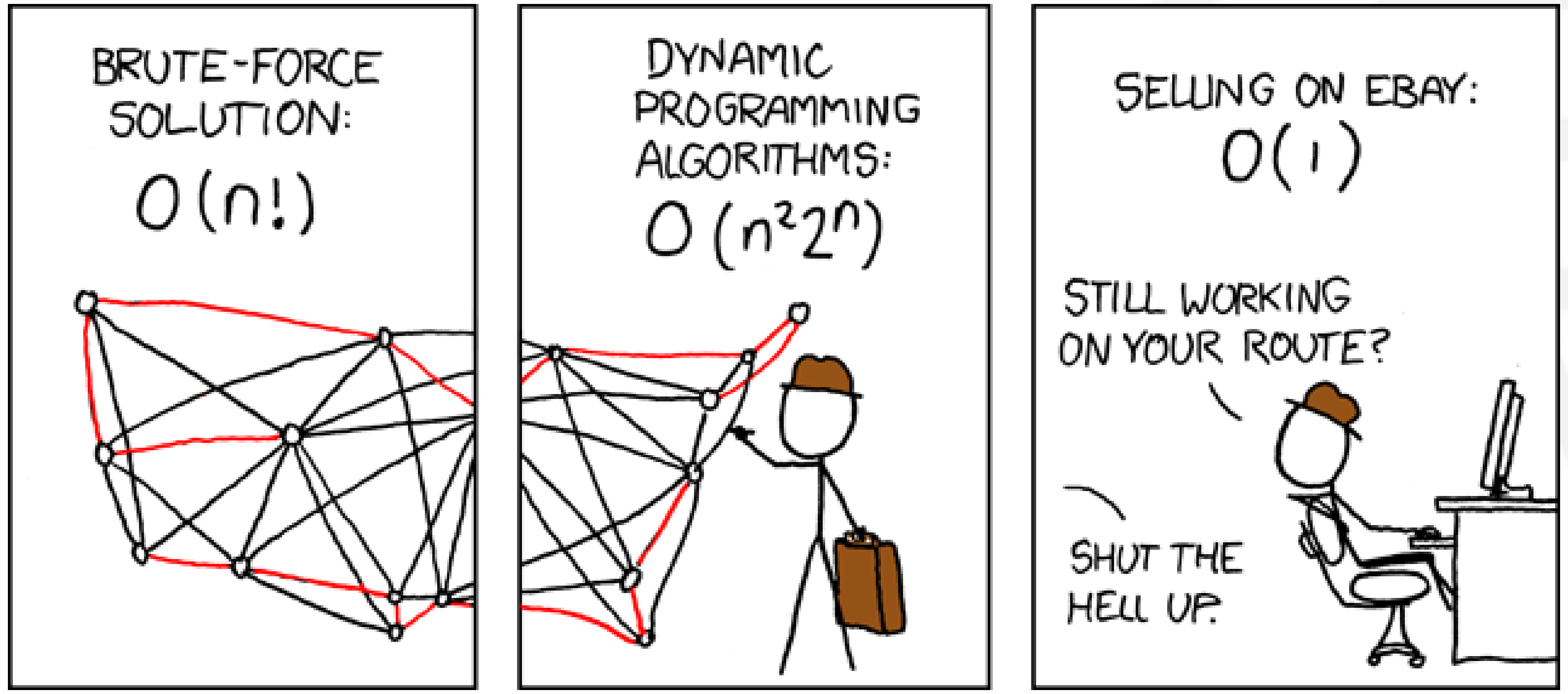
Easy
$O(n^2)$

$$\underbrace{\begin{bmatrix}1 & 2 & 3\end{bmatrix}}_{1\times 3} \cdot \underbrace{\begin{bmatrix}2 & 1 & 3\\ 3 & 3 & 2\\ 4 & 1 & 2\end{bmatrix}}_{3\times 3} = \begin{bmatrix}1\cdot 2+2\cdot 3+3\cdot 4\\ 1\cdot 1+2\cdot 3+3\cdot 1\\ 1\cdot 3+2\cdot 2+3\cdot 2\end{bmatrix} = \underbrace{\begin{bmatrix}20\\ 10\\ 13\end{bmatrix}}_{1\times 3}$$

$(x \text{ OR } y \text{ OR } z) \text{ AND } (x \text{ OR } \bar{y} \text{ OR } z) \text{ AND }$

$(x \text{ OR } y \text{ OR } \bar{z}) \text{ AND } (x \text{ OR } \bar{y} \text{ OR } \bar{z}) \text{ AND }$

$(\bar{x} \text{ OR } y \text{ OR } z) \text{ AND } (\bar{x} \text{ OR } \bar{y} \text{ OR } \bar{z})$



Today's cryptography in use?

- Based on computationally hard problems

Hard
$O(2^n)$

(x OR y OR z) AND (x OR $\bar{y}$ OR z) AND

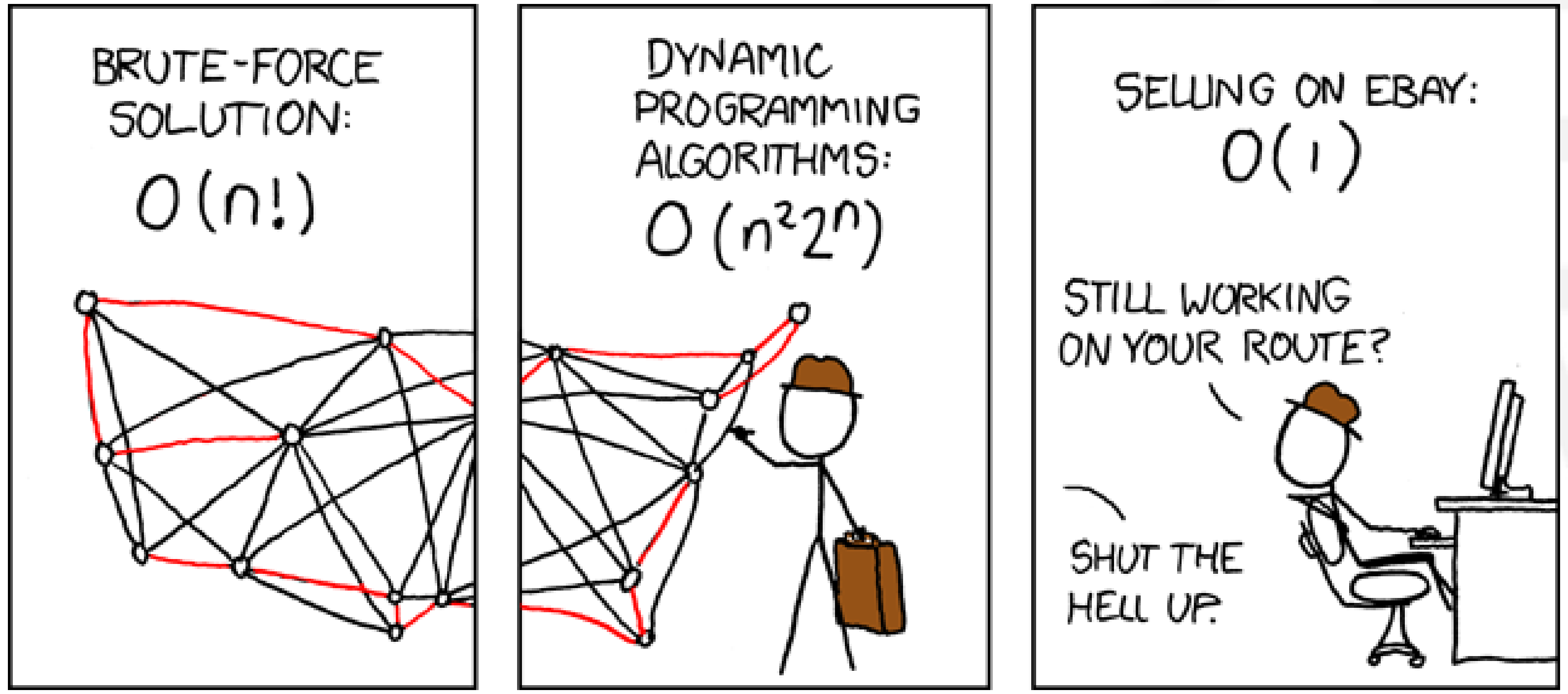
(x OR y OR $\bar{z}$) AND (x OR $\bar{y}$ OR $\bar{z}$) AND

($\bar{x}$ OR y OR z) AND ($\bar{x}$ OR $\bar{y}$ OR $\bar{z}$)

Easy
$O(n)$

Easy
$O(n^2)$

$$\underbrace{\begin{bmatrix}1 & 2 & 3\end{bmatrix}}_{1\times 3} \cdot \underbrace{\begin{bmatrix}2 & 1 & 3\\ 3 & 3 & 2\\ 4 & 1 & 2\end{bmatrix}}_{3\times 3} = \begin{bmatrix}1\cdot 2+2\cdot 3+3\cdot 4\\ 1\cdot 1+2\cdot 3+3\cdot 1\\ 1\cdot 3+2\cdot 2+3\cdot 2\end{bmatrix} = \underbrace{\begin{bmatrix}20\\ 10\\ 13\end{bmatrix}}_{1\times 3}$$



Today's cryptography in use?

- Based on computationally hard problems

Hard
$O(2^n)$

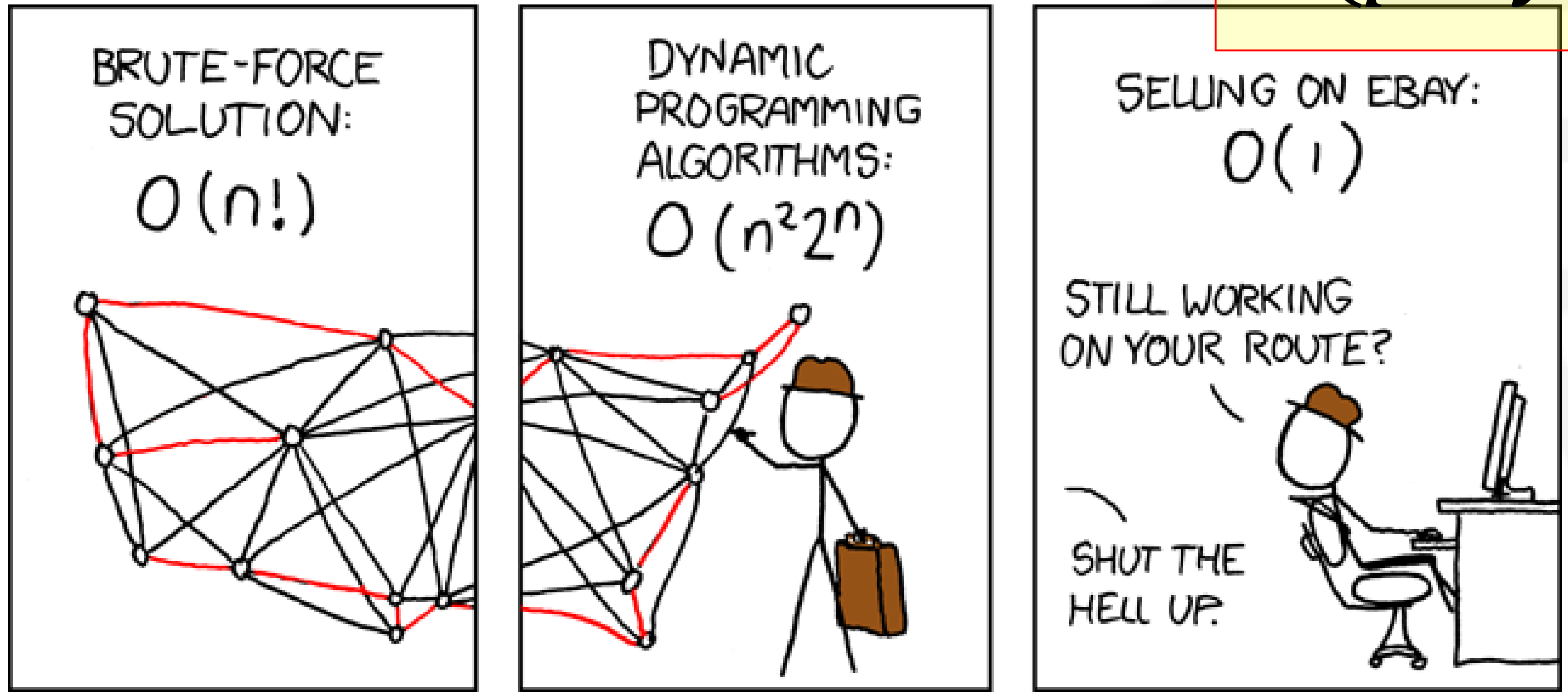
(x OR y OR z) AND (x OR $\bar{y}$ OR z) AND
(x OR y OR $\bar{z}$) AND (x OR $\bar{y}$ OR $\bar{z}$) AND
($\bar{x}$ OR y OR z) AND ($\bar{x}$ OR $\bar{y}$ OR $\bar{z}$)

Easy
$O(n)$

Easy
$O(n^2)$

$$\underbrace{\begin{bmatrix} 1 & 2 & 3 \end{bmatrix}}_{1 \times 3} \cdot \underbrace{\begin{bmatrix} 2 & 1 & 3 \\ 3 & 3 & 2 \\ 4 & 1 & 2 \end{bmatrix}}_{3 \times 3} = \begin{bmatrix} 1\cdot 2 + 2\cdot 3 + 3\cdot 4 \\ 1\cdot 1 + 2\cdot 3 + 3\cdot 1 \\ 1\cdot 3 + 2\cdot 2 + 3\cdot 2 \end{bmatrix} = \underbrace{\begin{bmatrix} 20 \\ 10 \\ 13 \end{bmatrix}}_{1 \times 3}$$

Hard
$O(poly(n)2^n)$

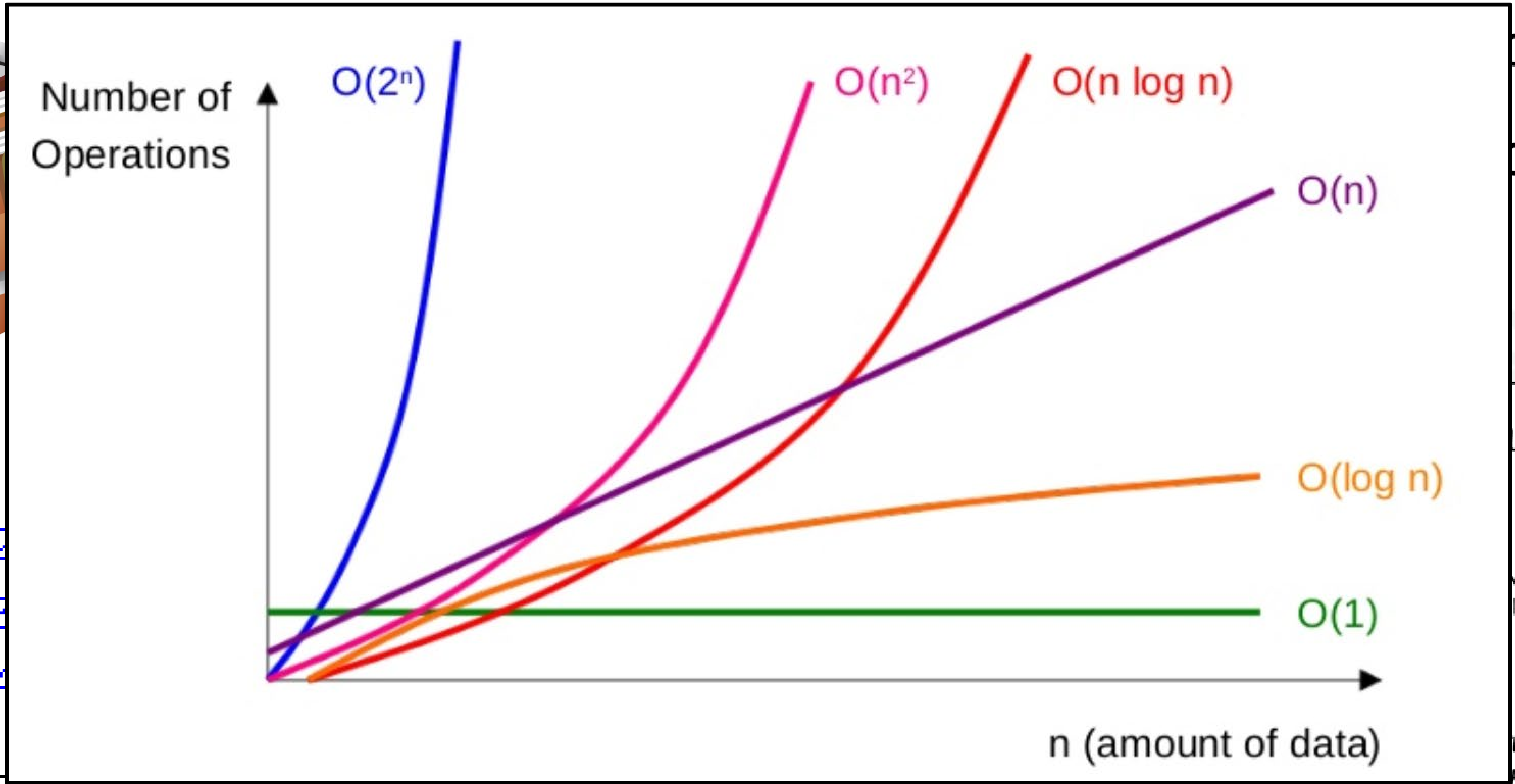


Today's cryptography in use?

- Based on computationally hard problems

Hard
$O(2^n)$

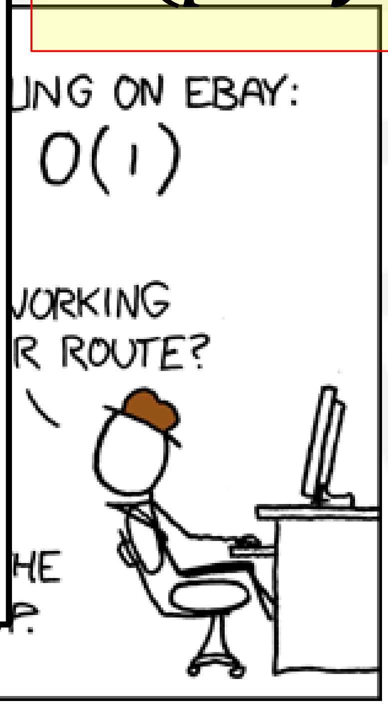
(x OR y OR z) AND (x OR $\bar{y}$ OR z) AND
OR $\bar{z}$) AND
OR $\bar{z}$)



Easy
$O(n^2)$

$\underbrace{[1\ \ 2\ \ 3]}_{1 \times 3} \cdot \underbrace{[\ldots]}_{3 \times 3}$ 1×3

Hard
$O(poly(n)2^n)$



Today's cryptography in use?

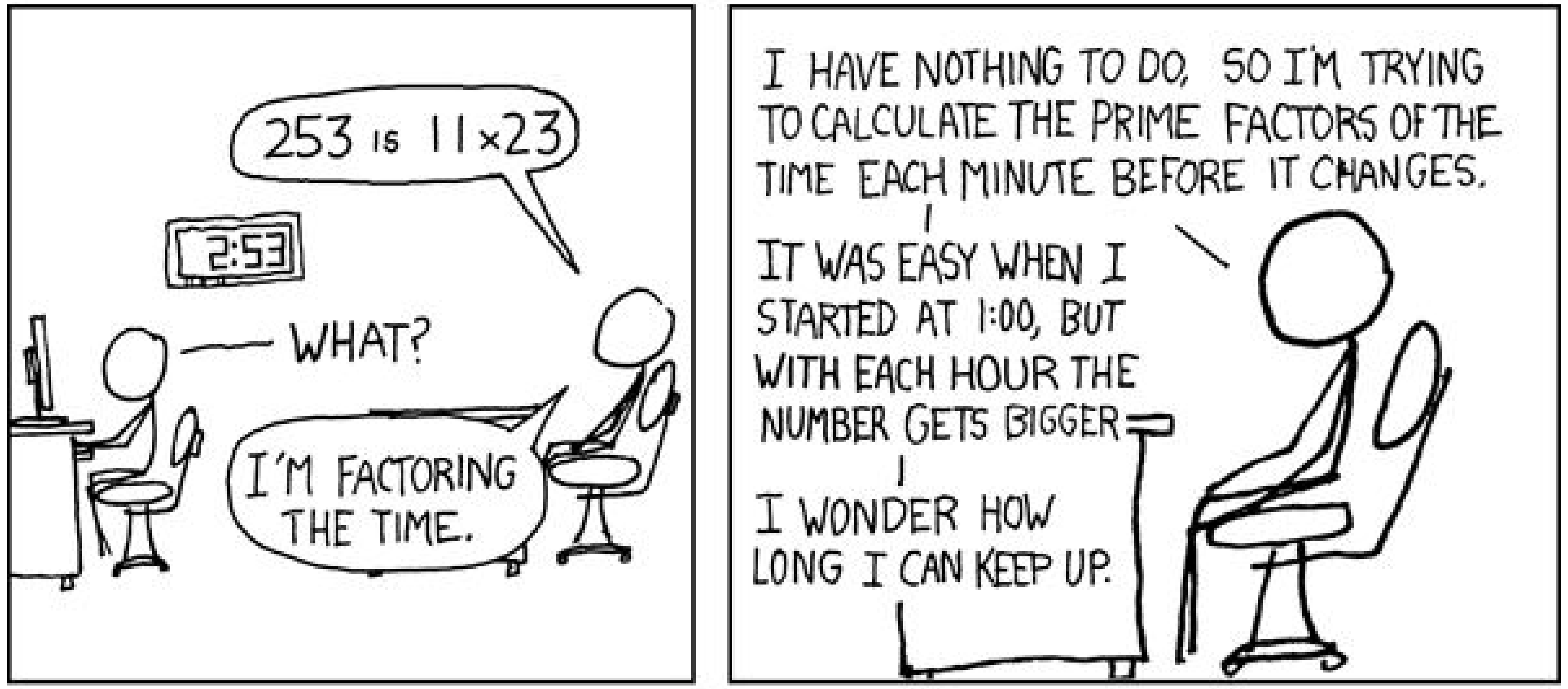
- Algorithms based on

Integer factorization

Given integer N find its prime factors

Discrete logarithm over different groups

Given generator $g \in G$ and any $y \in G$, find x such that $g^x = y$



Today's cryptography in use?

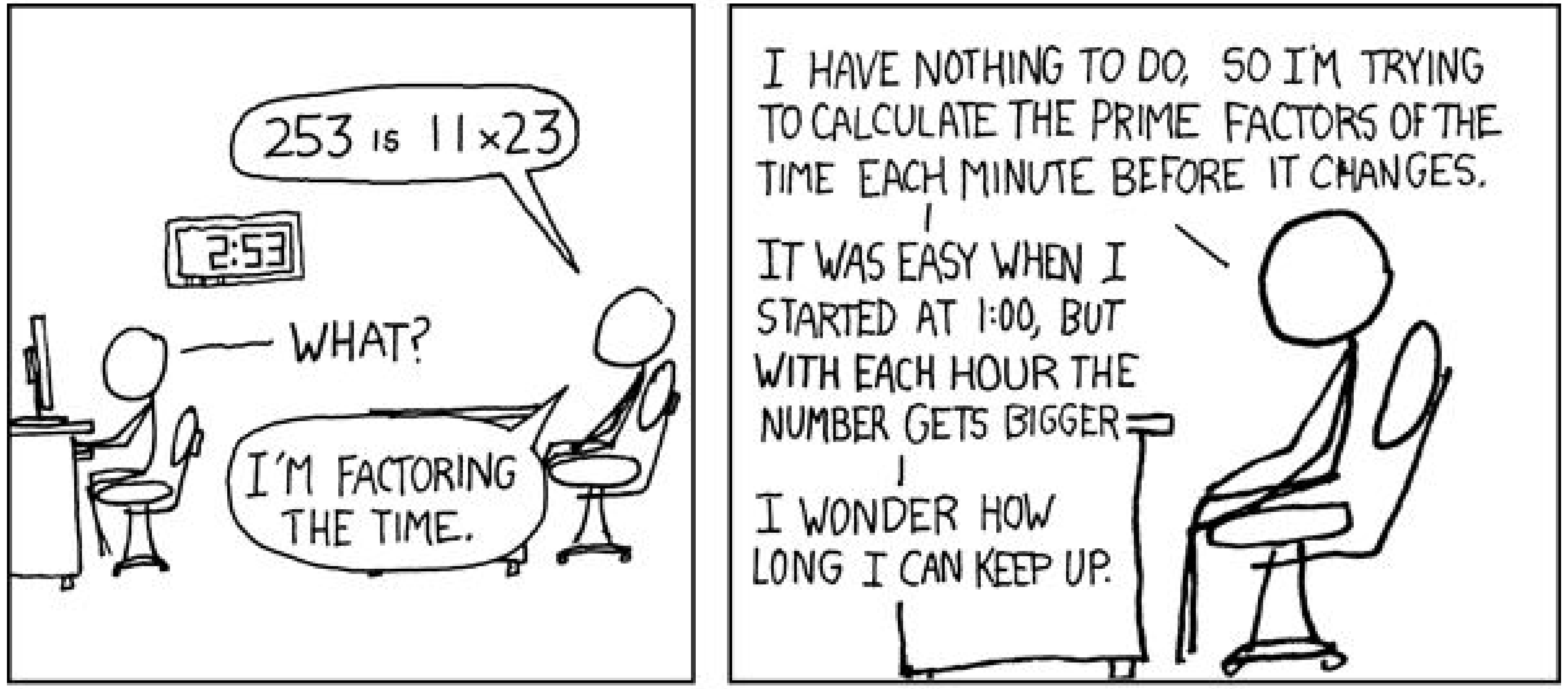
- Algorithms based on

Integer factorization

Given integer N find its prime factors

Discrete logarithm over different groups

Given generator $g \in G$ and any $y \in G$, find x such that $g^x = y$



BOTH:
Subexponential complexity

$$e^{O(n^{1/3} (\log n)^{2/3})}$$

Today's cryptography in use?

- **Integer factorization**
- **Example – RSA:**

Today's cryptography in use?

- **Integer factorization**

- **Example – RSA:**

1. Choose two large prime numbers *p, q.* (e.g., 1024 bits each)
2. Compute $n = pq$, $z = (p-1)(q-1)$
3. Choose e (with $e<n$) coprime with z.
4. Choose d such that $ed \bmod z = 1$

5. *Public* key is $\underbrace{(n,e)}_{K_B^+}$. *Private* key is $\underbrace{(n,d)}_{K_B^-}$.

Today's cryptography in use?

- **Integer factorization**

- **Example – RSA:**

1. Choose two large prime numbers p, q. (e.g., 1024 bits each)
2. Compute $n = pq$, $z = (p-1)(q-1)$
3. Choose e (with $e<n$) coprime with z.
4. Choose d such that $ed \bmod z = 1$

5. *Public* key is $\underbrace{(n,e)}_{K_B^+}$. *Private* key is $\underbrace{(n,d)}_{K_B^-}$.

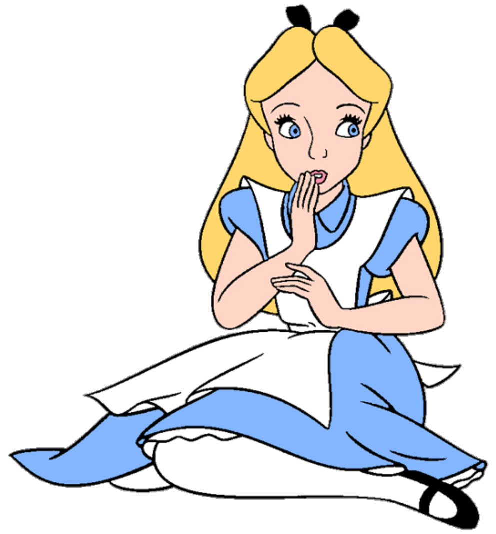
1. To encrypt m, compute $x = m^e \bmod n$
2. To decrypt received x, compute $m = x^d \bmod n$

Magic happens! $m = (\underbrace{m^e \bmod n}_{x})^d \bmod n$

Today's cryptography in use?

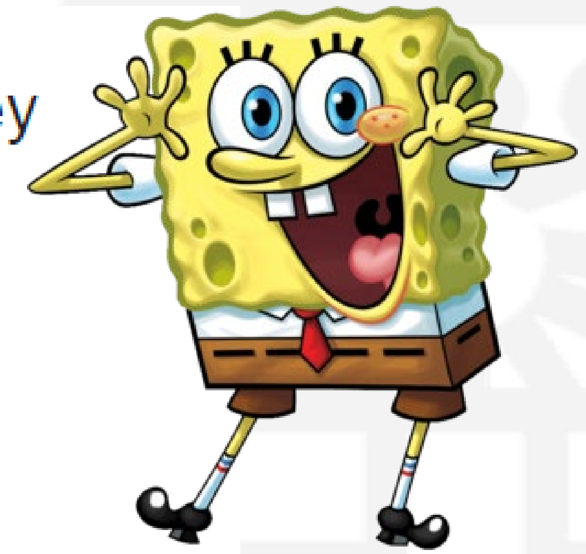
- **Discrete log**

- **Example – Diffie-Hellman Key Exchange:**



Choose random private key
$k_{prA} = a \in \{1,2,\ldots,p-1\}$

Choose random private key
$k_{prB} = b \in \{1,2,\ldots,p-1\}$



Compute corresponding public key
$k_{pubA} = A = \alpha^a \bmod p$

$\xrightarrow{\quad A \quad}$

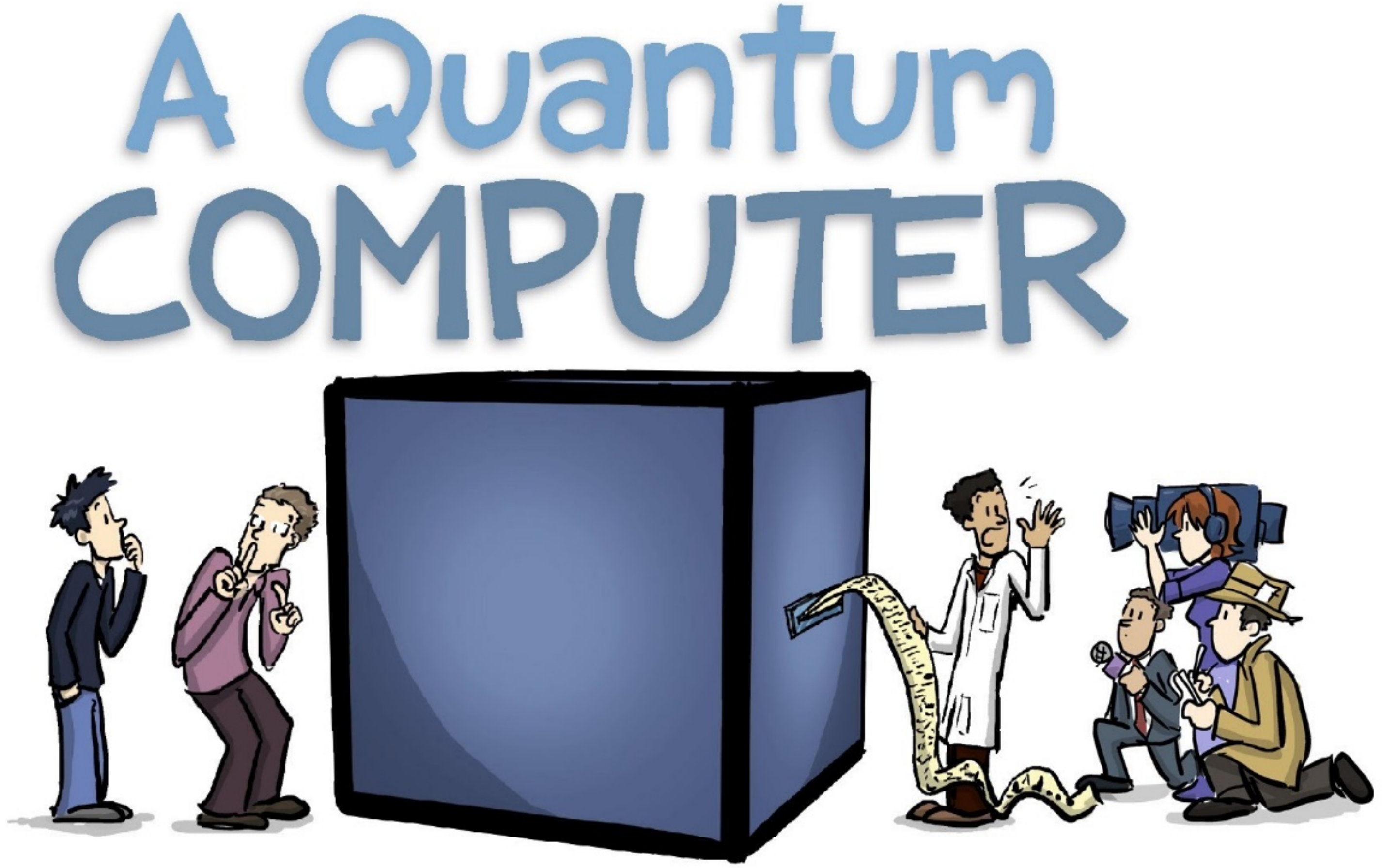
Compute correspondig public key
$k_{pubB} = B = \alpha^b \bmod p$

$\xleftarrow{\quad B \quad}$

Compute common secret
$k_{AB} = B^a = (\alpha^a)^b \bmod p$

Compute common secret
$k_{AB} = A^b = (\alpha^b)^a \bmod p$

What is



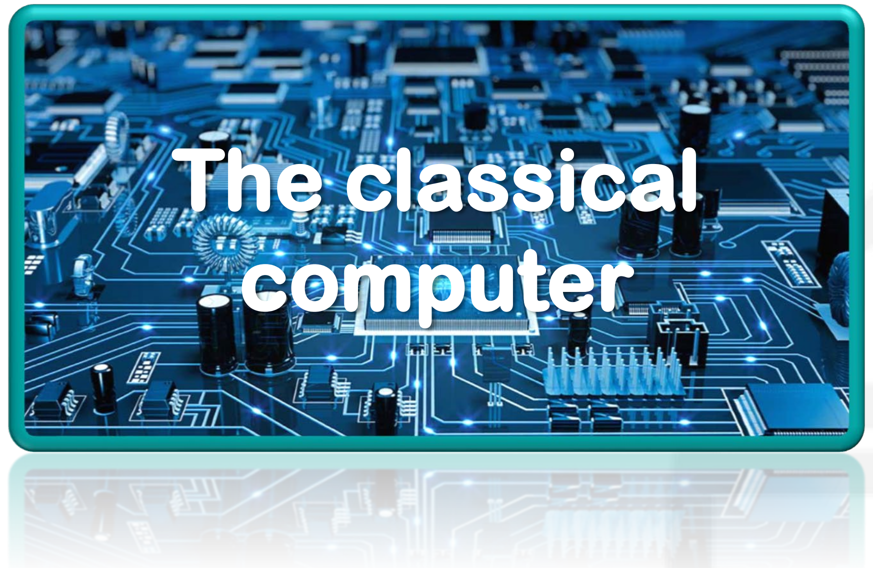
???

The origins …

Probabilistic Turing Machine

Turing ’36

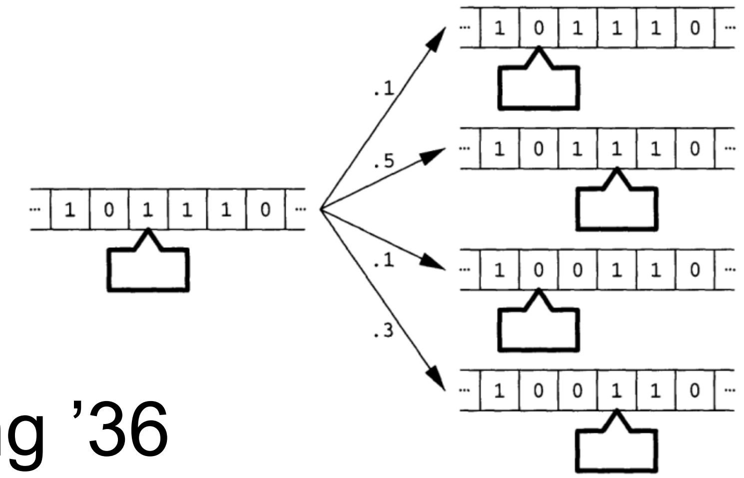
Gill ’77



The origins …

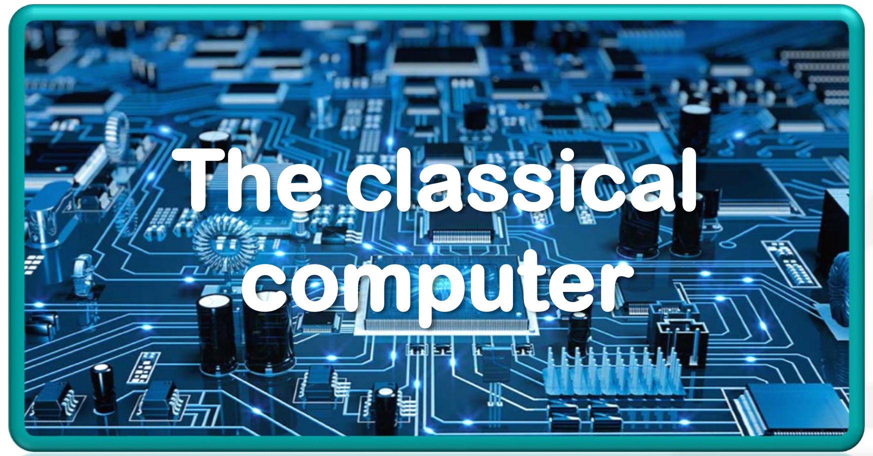
Probabilistic Turing Machine

Any randomized algorithmic process can be simulated efficiently using a Probabilistic Turing machine



Turing '36

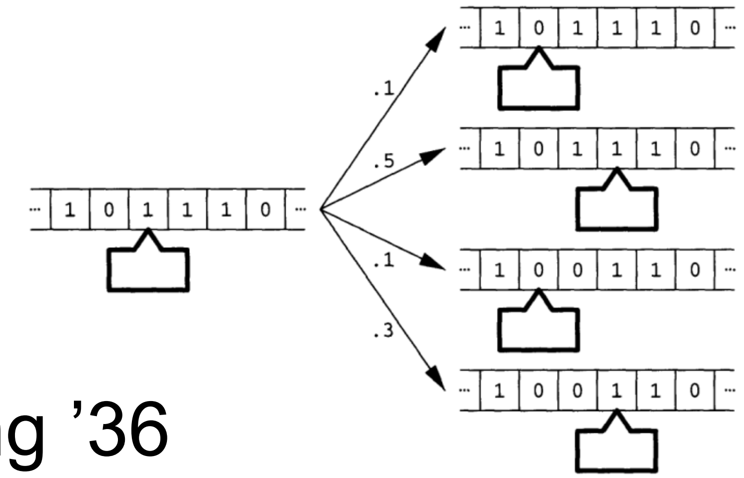
Gill '77



The origins …

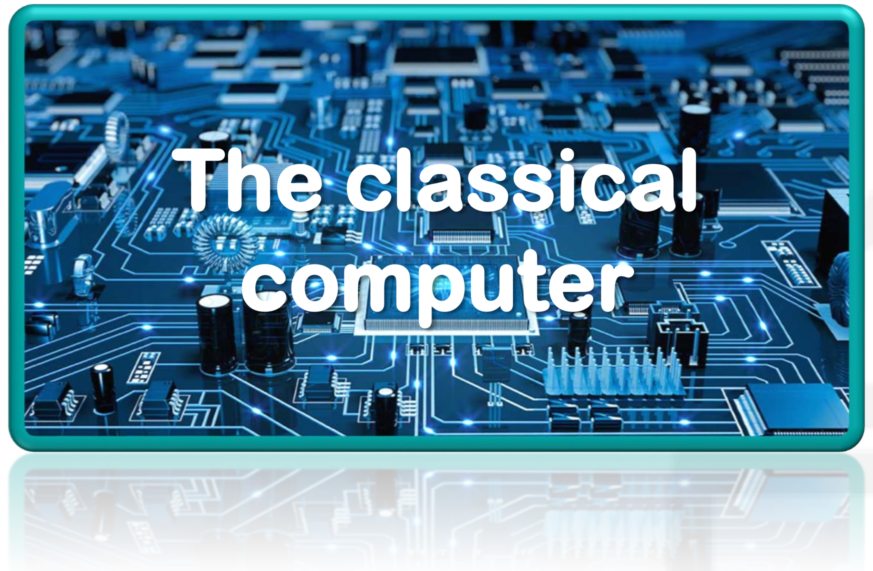
Probabilistic Turing Machine

Any randomized algorithmic process can be simulated efficiently using a Probabilistic Turing machine



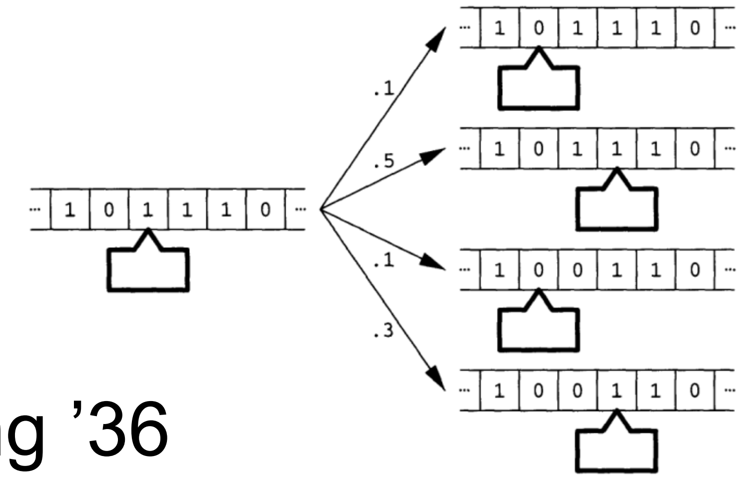
Turing '36

Gill '77



Feynman '82:
*Certain "**quantum**" phenomena*
***can not be efficiently simulated** by a PTM*

The origins …

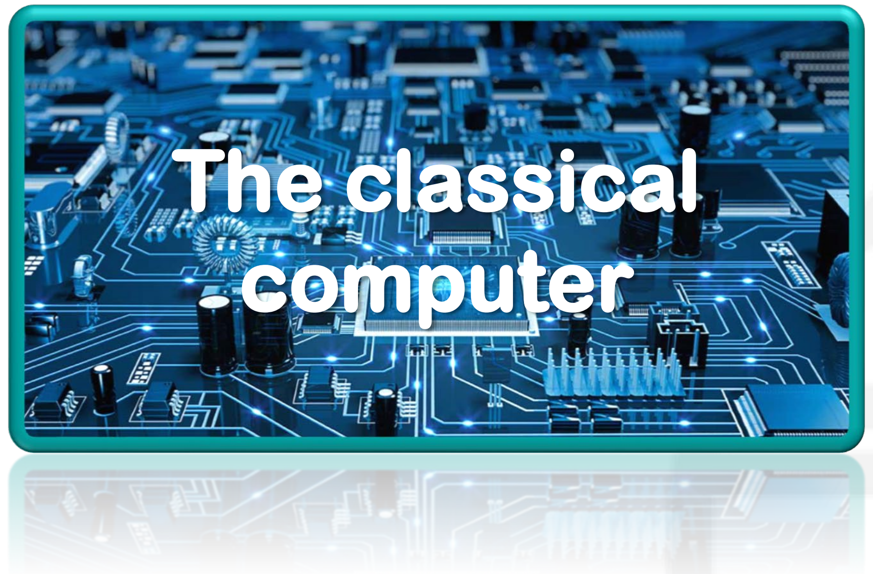


Probabilistic Turing Machine

Any randomized algorithmic process can be simulated efficiently using a Probabilistic Turing machine

Turing ’36

Gill ’77

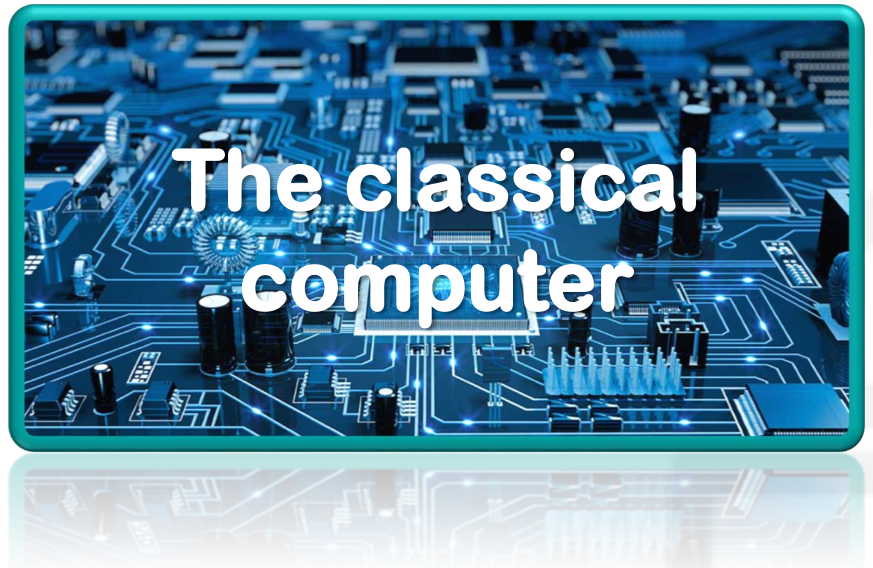


Feynman ’82:
*Certain “**quantum**” phenomena*
***can not be efficiently simulated** by a PTM*

*Can there be a computational device capable of **efficiently simulating** an **arbitrary physical system**?*

The origins …

Probabilistic Turing Machine



Deutsch '85

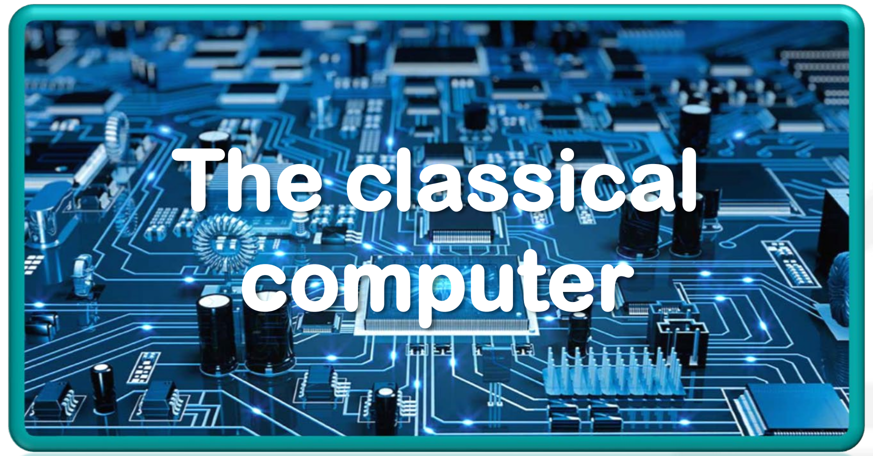
Universal Quantum Computer

Feynman '82:
*Certain "**quantum**" phenomena*
***can not be efficiently simulated** by a PTM*

*Can there be a computational device capable of **efficiently simulating** an **arbitrary physical system**?*

The origins …

Probabilistic Turing Machine



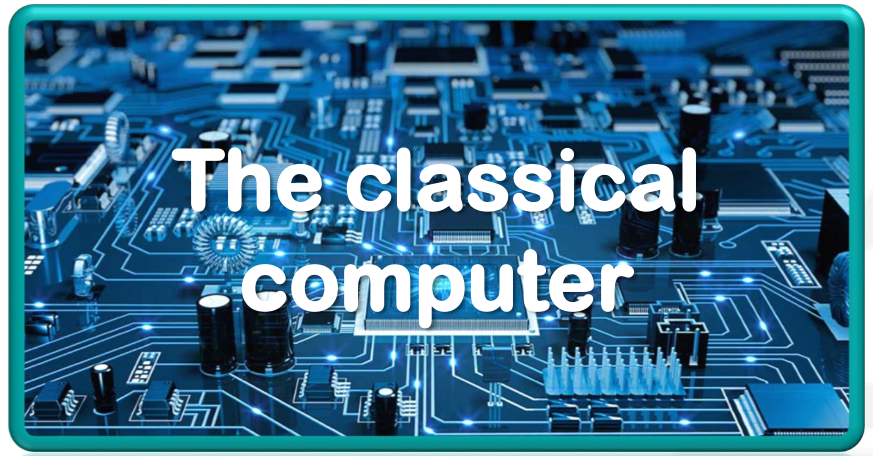
Deutsch '85

Universal Quantum Computer

A computing device based on the principles of Quantum mechanics

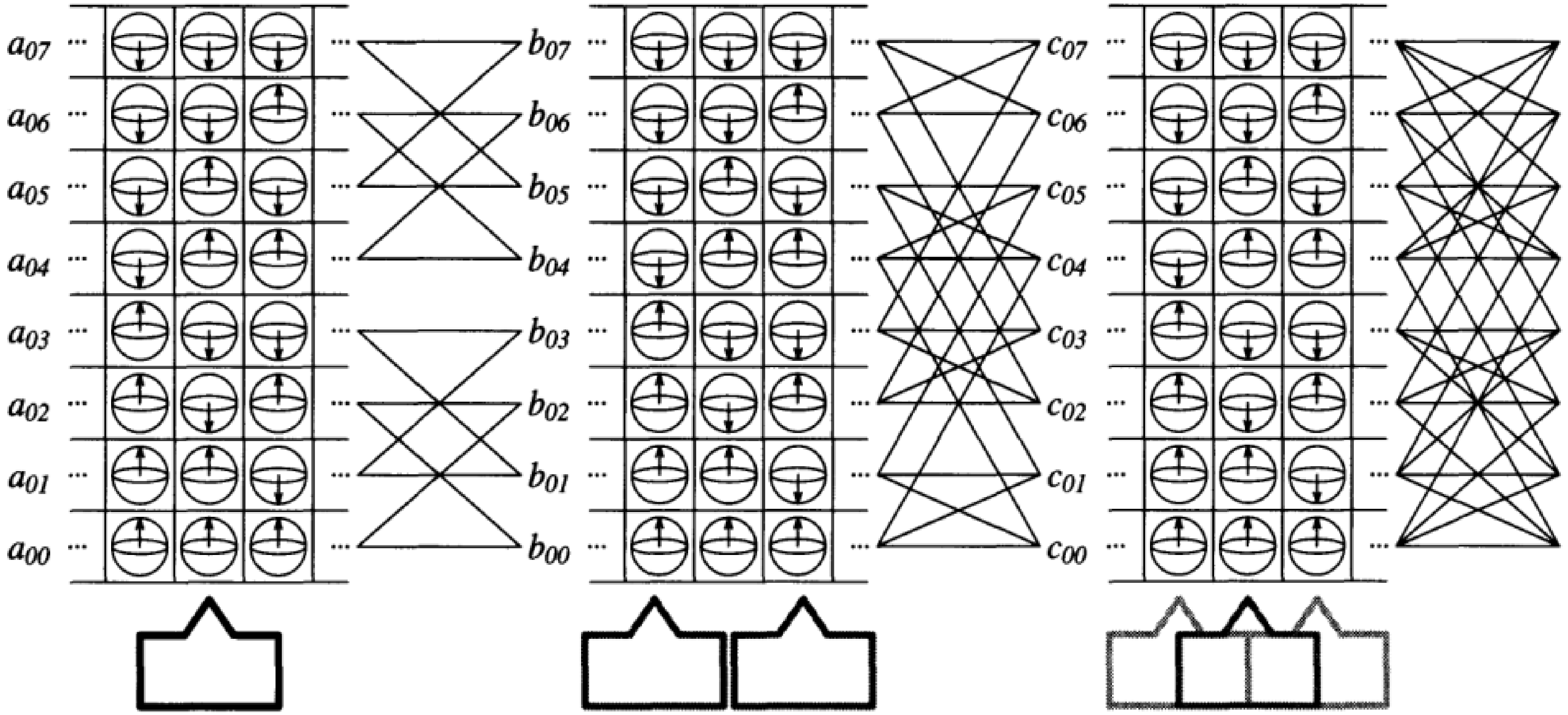
The origins …

Probabilistic Turing Machine



Deutsch ’85

Universal Quantum Computer

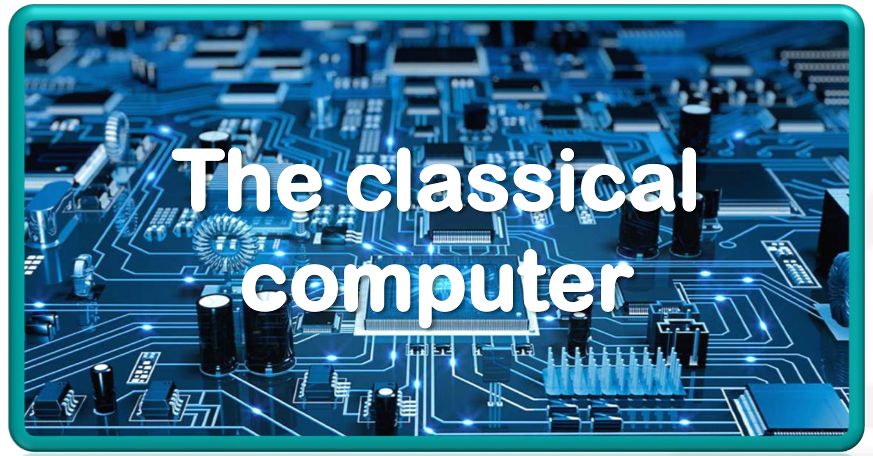


The origins …

Probabilistic Turing Machine

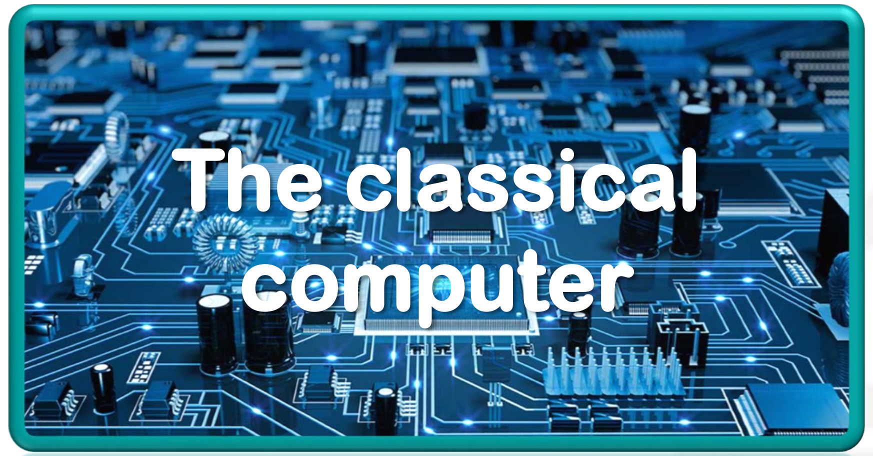
Deutsch ’85

Universal Quantum Computer



The origins …

Probabilistic Turing Machine



Deutsch ’85

Universal Quantum Computer

IMAGE DOES NOT EXIST

FAST COMPANY 29 Apr 2015

THE GOLDEN AGE OF QUANTUM COMPUTING IS UPON US (ONCE WE SOLVE THESE TINY PROBLEMS)

LITERALLY TINY. AS IBM ANNOUNCES A BIG ADVANCE, MANY CHALLENGES REMAIN IN BUILDING A COMPUTER THAT TAKES ADVANTAGE OF QUANTUM WEIRDNESS.

FAST COMPANY 29 Apr 2015

THE GOLDEN AGE OF QUANTUM COMPUTING IS UPON US (ONCE WE SOLVE THESE TINY PROBLEMS)

LITERALLY TINY. AS IBM ANNOUNCES A BIG ADVANCE, MANY CHALLENGES REMAIN IN BUILDING A COMPUTER THAT TAKES ADVANTAGE OF QUANTUM WEIRDNESS.

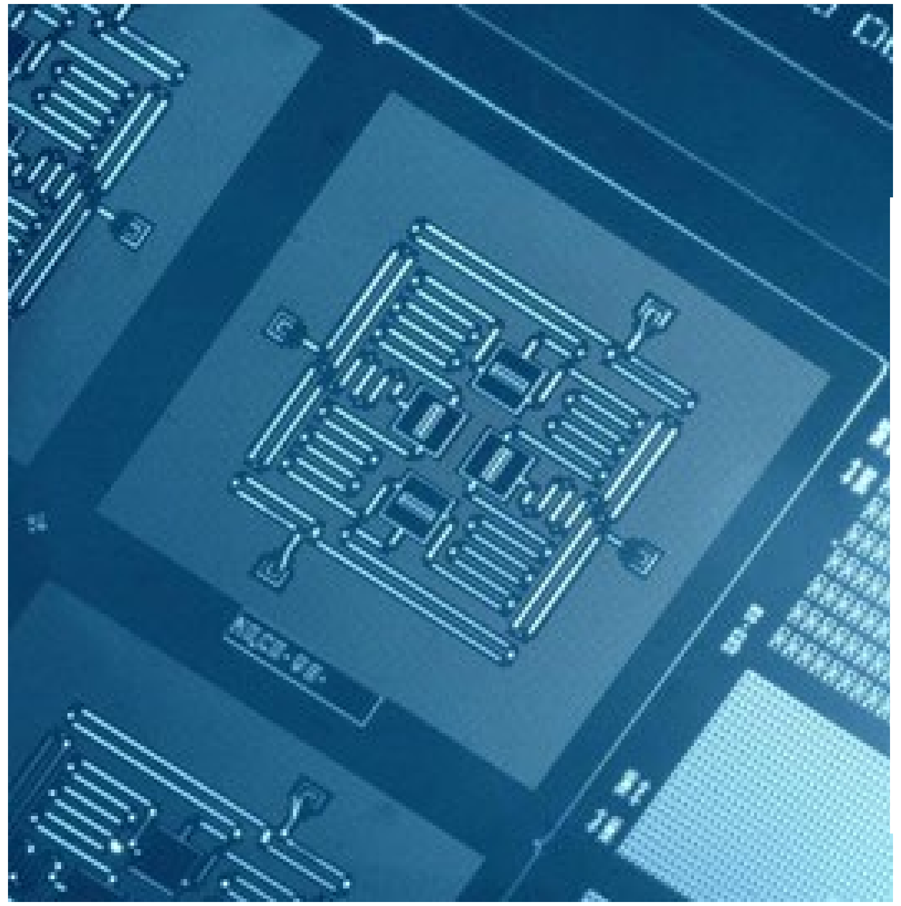


Photo: IBM Research

IEEE SPECTRUM

"With our recent four-qubit network, we built a system that allows us to detect both types of quantum errors," says Jerry Chow, manager of experimental quantum computing at IBM's Thomas J. Watson Research Center, in Yorktown Heights, N.Y. Chow, who, along with his IBM colleagues detailed their experiments in the 29 April issue of the journal Nature Communications, says, "This is the first demonstration of a system that has the ability to detect both bit-flip errors and phase errors" that exist in quantum computing systems.

The IBM system consists of four quantum bits, or qubits, arranged in a 2-by-2 configuration on a chip measuring about 1.6 square centimeters (0.25 square

EXTREMETECH

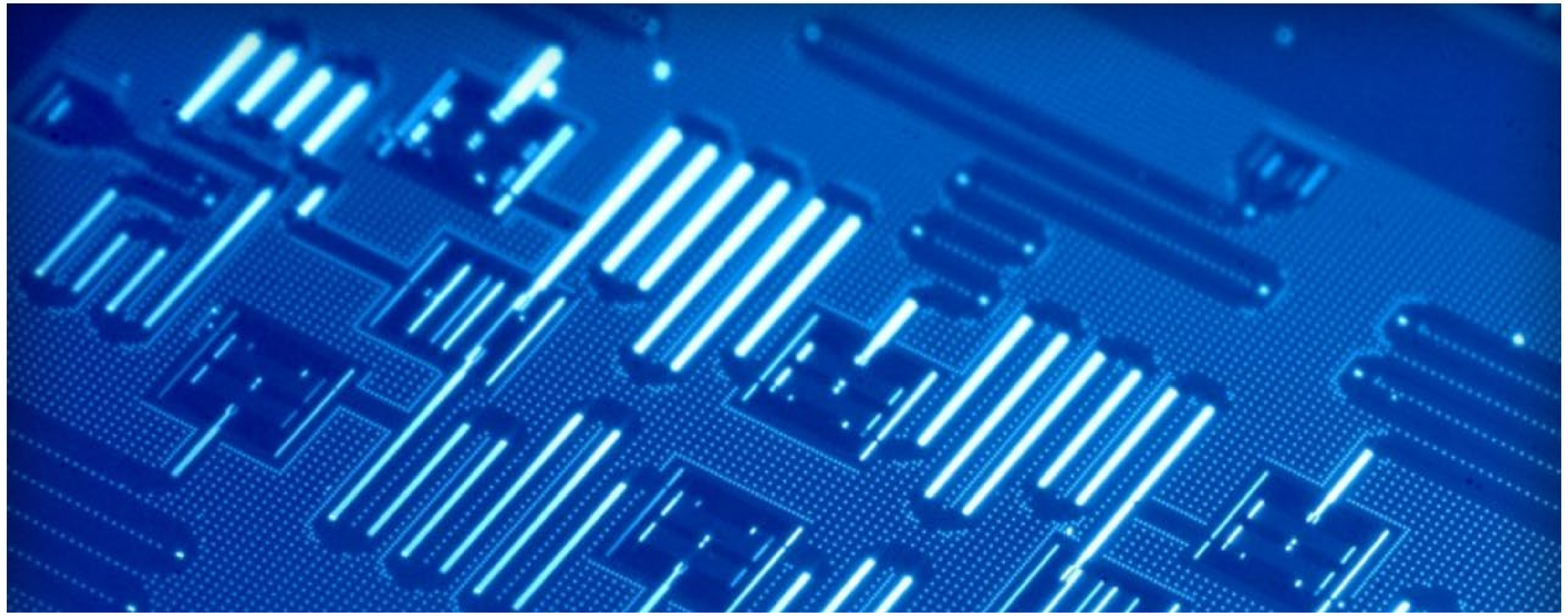
Search Extremetech SEARCH

Computing Phones Cars Gaming Science Extreme Deep Dives Deals

HOME › COMPUTING › IBM IS MAKING ITS QUANTUM COMPUTER API AVAILABLE TO THE PUBLIC

IBM is making its quantum computer API available to the public

By Jessica Hall on March 6, 2017 at 9:22 am | 3 Comments



Futurism

NEWS FEATURES VIDEOS

IBM Just Announced a 50-Qubit Quantum Computer

November 10, 2017

IN BRIEF

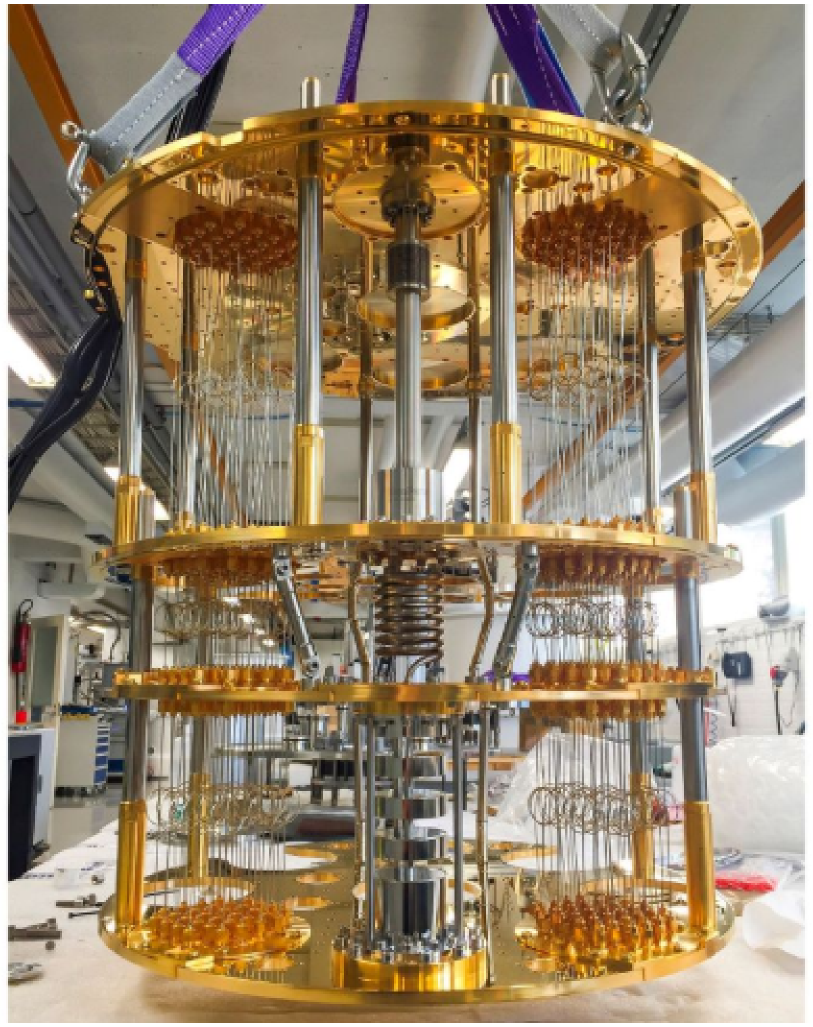
Earlier today, IBM announced a 50-quantum bit (qubit) quantum computer, the largest in the industry so far. As revolutionary as this development is, IBM's 50-qubit machine is still far from a universal quantum computer.

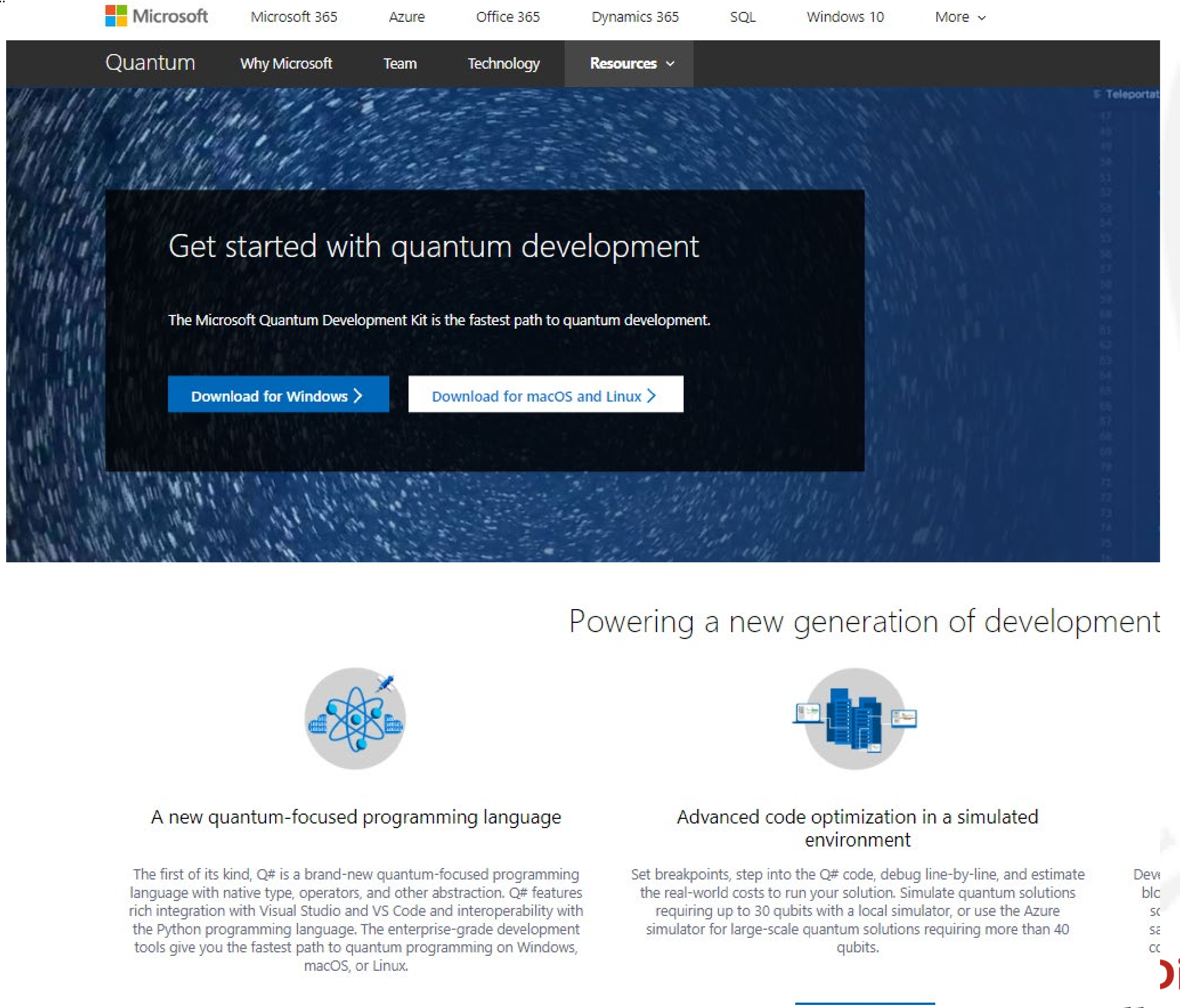
Technology

Microsoft Takes Path Less Traveled to Build a Quantum Computer

Software giant releases a quantum programming language and simulator, but still has no working computer

By Jeremy Kahn and Dina Bass
December 11, 2017, 2:45 PM GMT+1



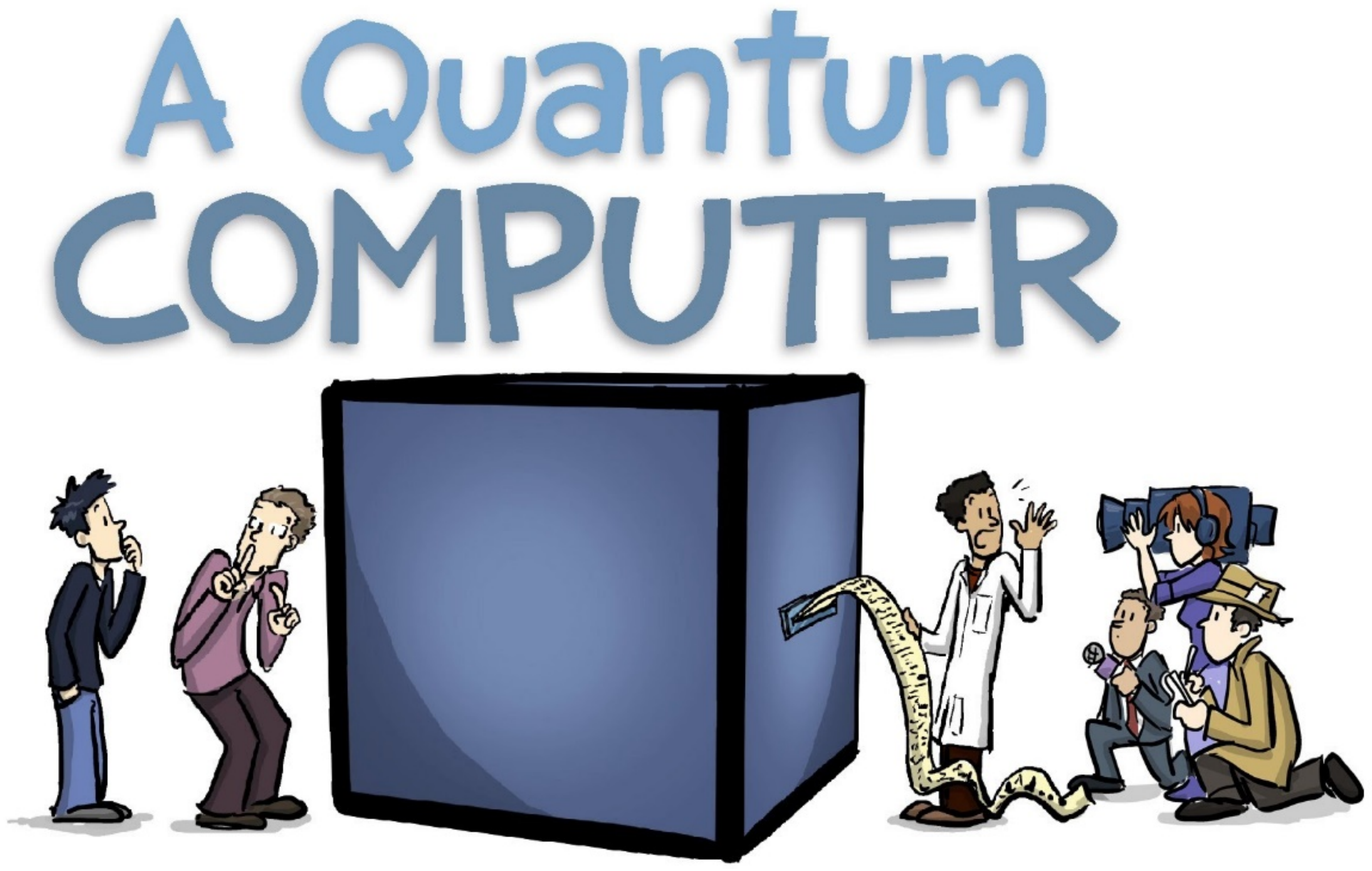


Quantum Projects

COMPANY	TECHNOLOGY	WHY IT COULD FAIL
IBM	Makes qubits from superconducting metal circuits.	The error rate of the qubits is too high to operate them together in a useful computer.
Microsoft	Building a new kind of "topological qubit" that in theory should be more reliable than others.	The existence of the subatomic particle used in this qubit remains unproven. Even if it is real, there isn't yet evidence it can be controlled.
Alcatel-Lucent	Inspired by Microsoft's research, it is pursuing a topological qubit based on a different material.	Same as above.
D-Wave Systems	Sells computers based on superconducting chips with 512 qubits.	It's not clear that its chips harness quantum effects. Even if they do, their design is limited to solving a narrow set of mathematical problems.
Google	After experimenting with D-Wave's computers since 2009, it recently opened a lab to build chips like D-Wave's.	Same as above. Plus, Google is trying to adapt technology first developed for a different kind of qubit to the kind used by D-Wave.

MIT Technology Review

A peak inside



(…a thought experiment…)

Qubit (short of quantum bit)

Bit – the unit of
classical information

0 or 1

Qubit (short of quantum bit)

Bit – the unit of classical information

0 or 1

vs

Qubit – the unit of quantum information

A combination of 0 and 1

Qubit (short of quantum bit)

Bit – the unit of classical information

0 or 1

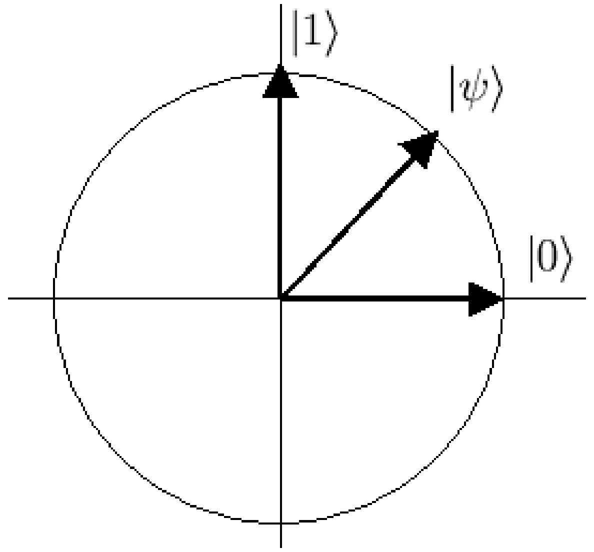
vs

Qubit – the unit of quantum information

A combination of 0 and 1

State of a qubit: $\boxed{|\psi\rangle = \alpha|0\rangle + \beta|1\rangle}$ $\alpha, \beta \in \mathbb{C}$

A vector in two dimensional complex space



Qubit (short of quantum bit)

Bit – the unit of classical information

0 or 1

vs

Qubit – the unit of quantum information

A combination of 0 and 1

State of a qubit: $\boxed{|\psi\rangle = \alpha|0\rangle + \beta|1\rangle}$ $\quad \alpha, \beta \in \mathbb{C}$

Measurement

$|\psi\rangle$ non-deterministic collapse $\rightarrow$ $|0\rangle$, $|1\rangle$

$$P_{|0\rangle} = |\alpha|^2$$

$$|\alpha|^2 + |\beta|^2 = 1$$

$$P_{|1\rangle} = |\beta|^2$$

Qubit (short of quantum bit)

Bit – the unit of classical information

0 or 1

vs

Qubit – the unit of quantum information

A combination of 0 and 1

Caution: a qubit holds only 1 bit of information !!!

State of a qubit: $\boxed{|\psi\rangle = \alpha|0\rangle + \beta|1\rangle}$ $\alpha, \beta \in \mathbb{C}$

Measurement

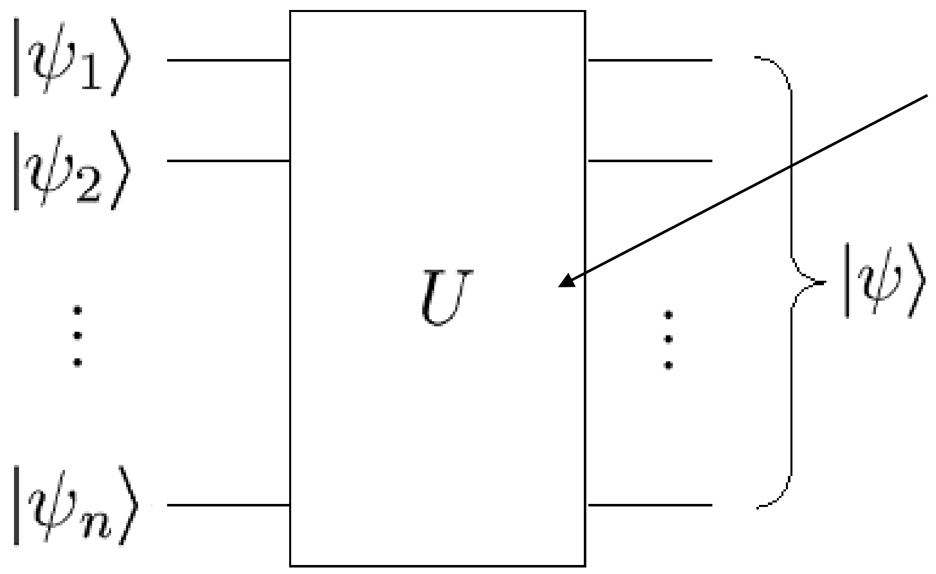
$|\psi\rangle$ non-deterministic collapse

$|0\rangle$ $P_{|0\rangle} = |\alpha|^2$

$|\alpha|^2 + |\beta|^2 = 1$

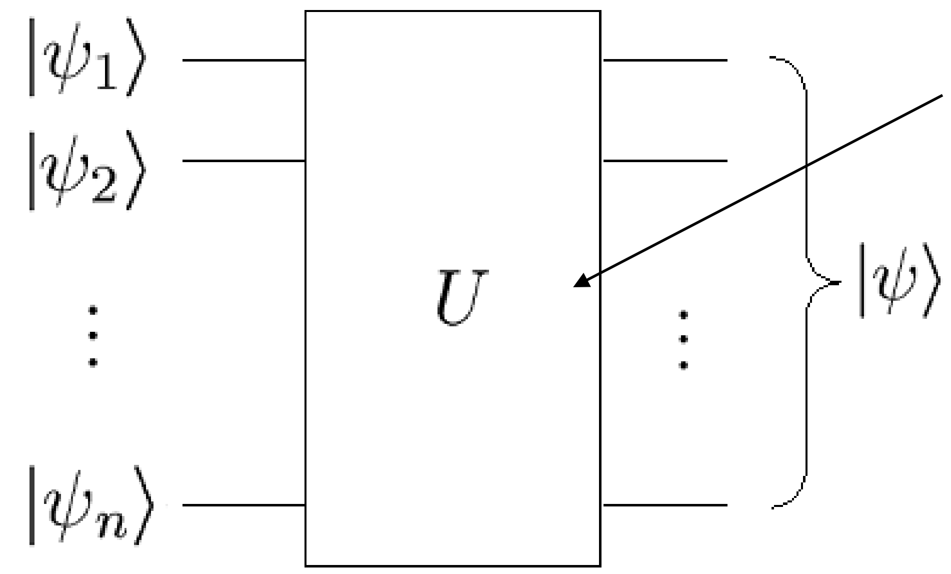
$|1\rangle$ $P_{|1\rangle} = |\beta|^2$

Quantum gates



Unitary operator $UU^\dagger = U^\dagger U = I$

Quantum gates



Unitary operator $UU^\dagger = U^\dagger U = I$

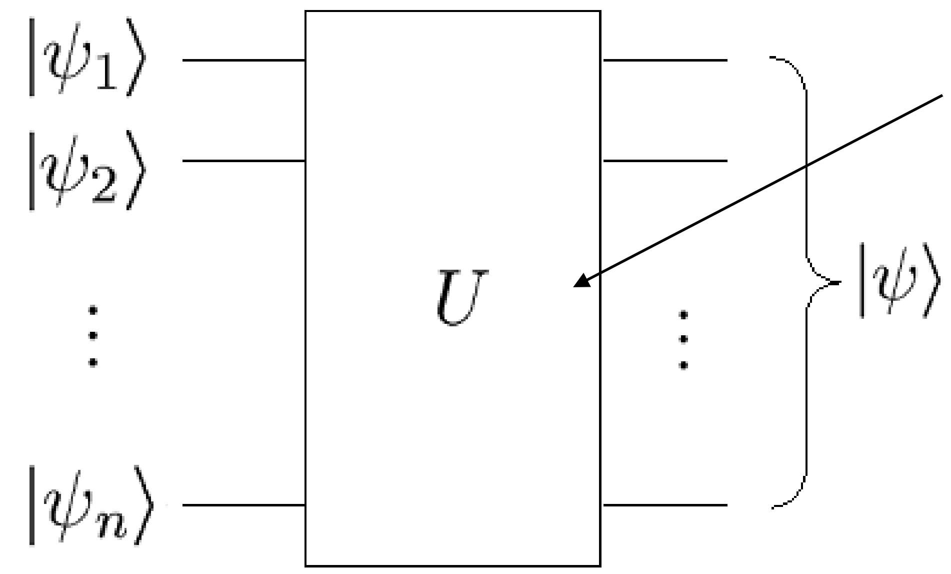
One qubit gates

$$\alpha|0\rangle + \beta|1\rangle \xrightarrow{\boxed{X}} \beta|0\rangle + \alpha|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \xrightarrow{\boxed{Z}} \alpha|0\rangle - \beta|1\rangle$$

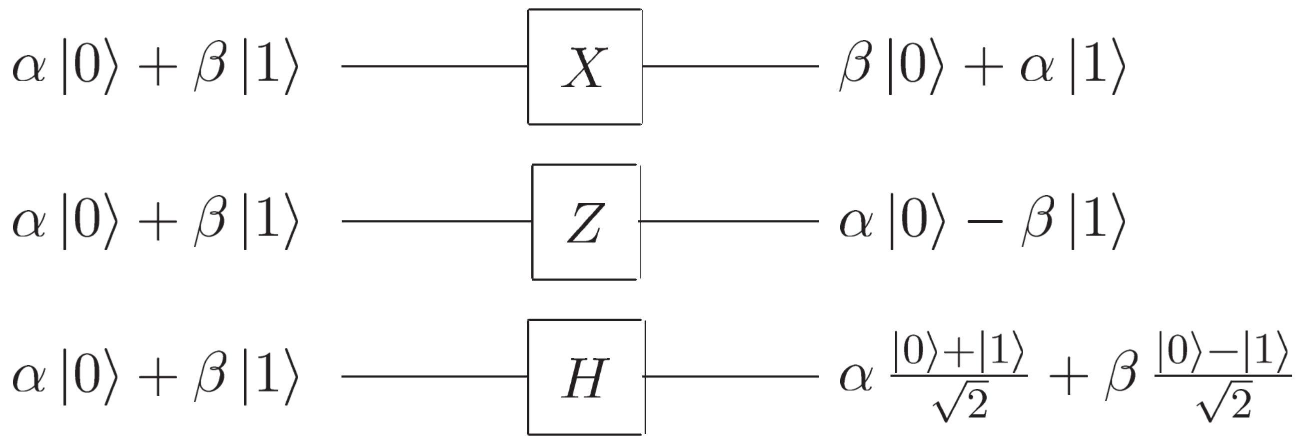
$$\alpha|0\rangle + \beta|1\rangle \xrightarrow{\boxed{H}} \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Quantum gates



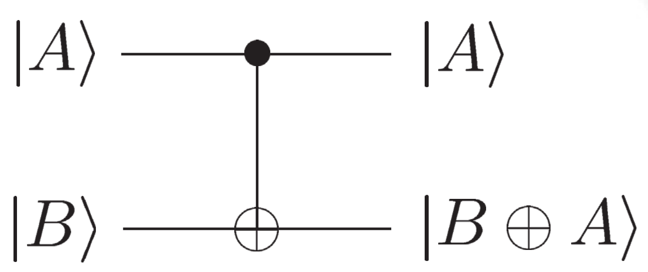
Unitary operator $UU^\dagger = U^\dagger U = I$

One qubit gates

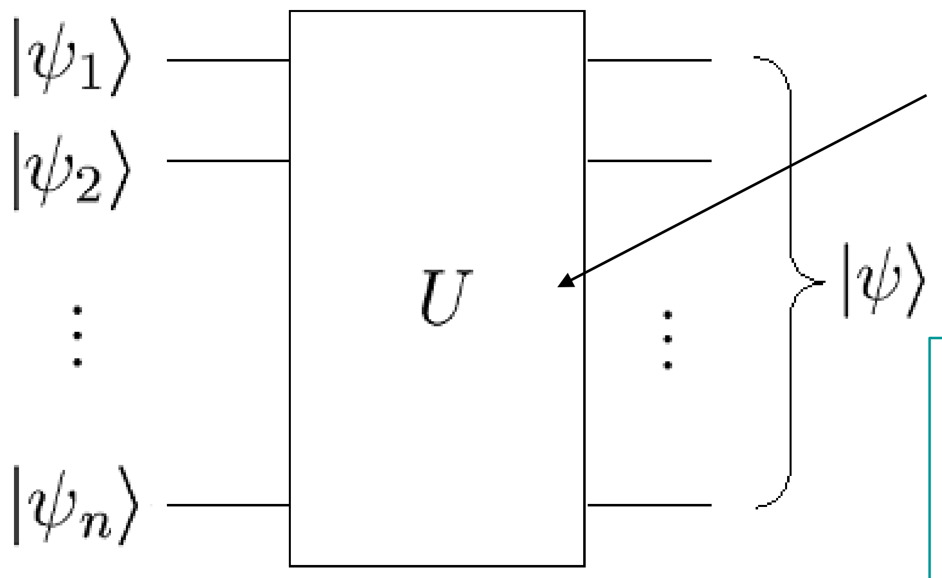


Two qubit gate

controlled-NOT



Quantum gates



Unitary operator $UU^\dagger = U^\dagger U = I$

All quantum transformations
are reversible
(No destruction of information as in classical gates)

One qubit gates

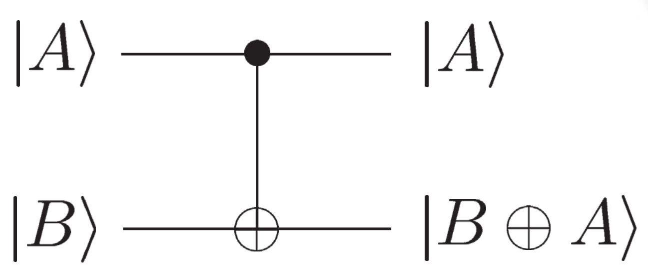
$$\alpha|0\rangle + \beta|1\rangle \;\text{—}\boxed{X}\text{—}\; \beta|0\rangle + \alpha|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \;\text{—}\boxed{Z}\text{—}\; \alpha|0\rangle - \beta|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \;\text{—}\boxed{H}\text{—}\; \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

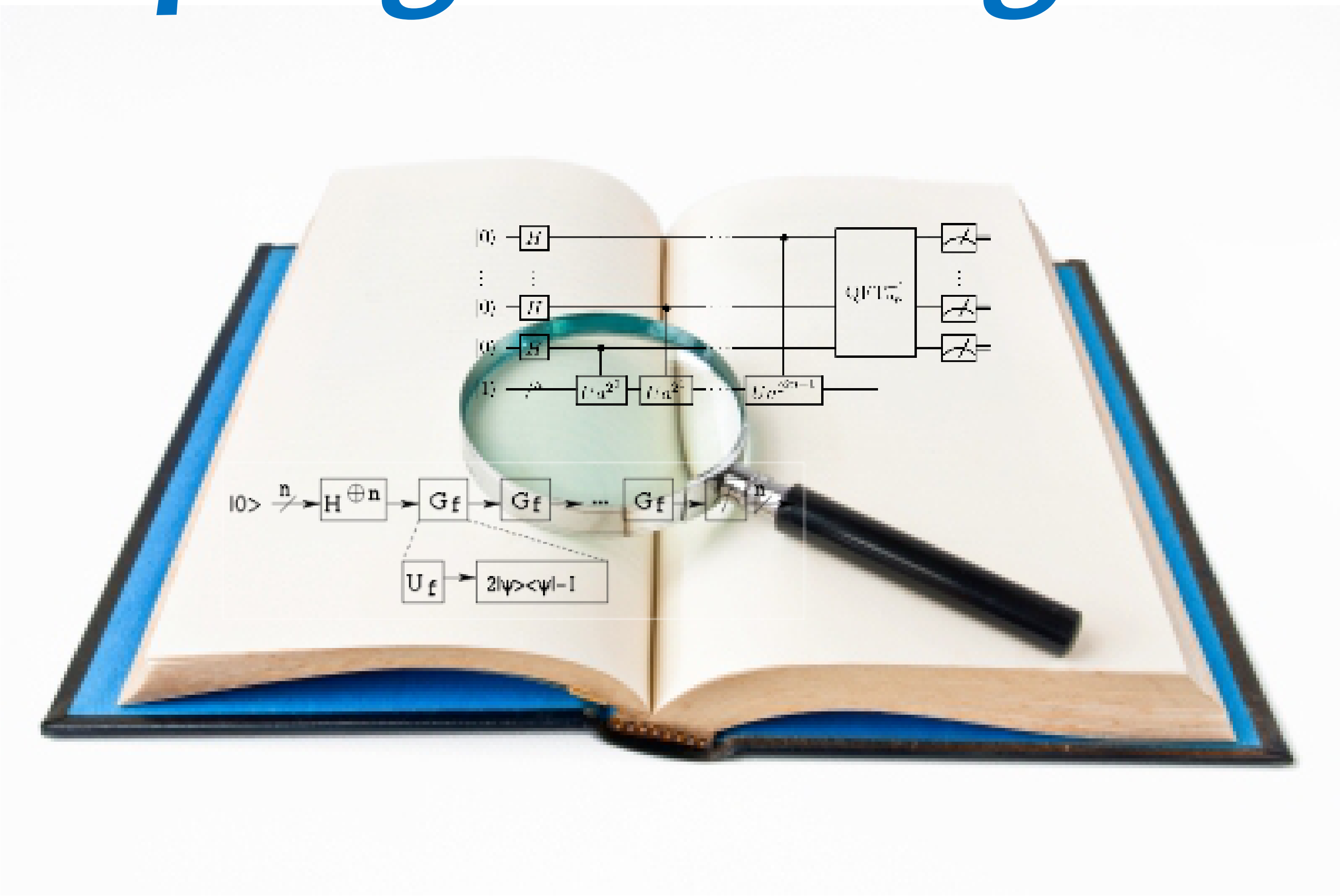
Two qubit gate

controlled-NOT



A peak inside

"The art of quantum programming"



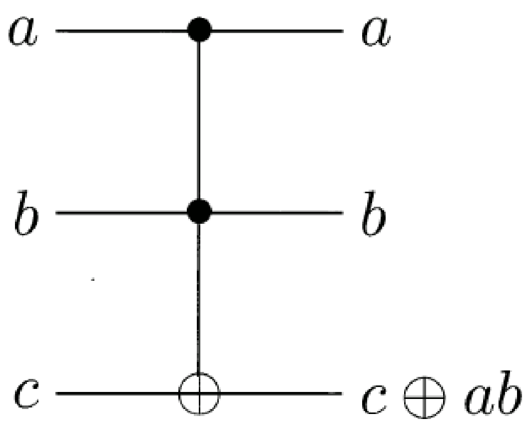
What kind of computations are possible using quantum circuits?

What kind of computations are possible using quantum circuits?

- Classical computations?

What kind of computations are possible using quantum circuits?

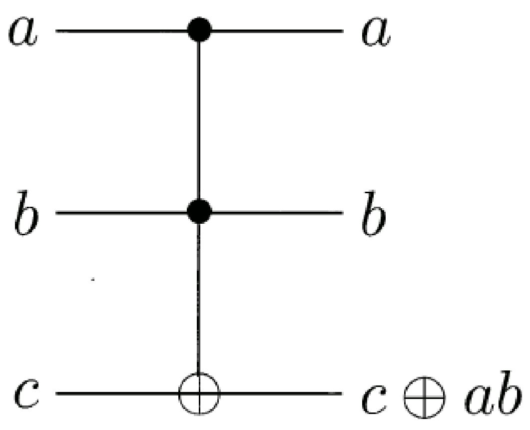
- Classical computations?



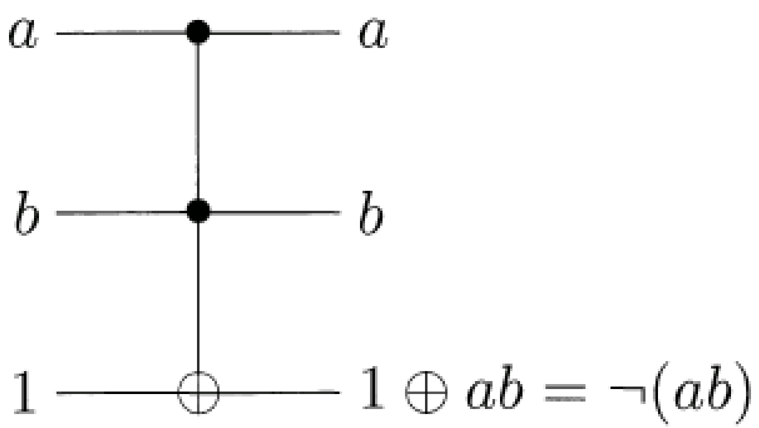
Toffoli gate

What kind of computations are possible using quantum circuits?

- Classical computations?



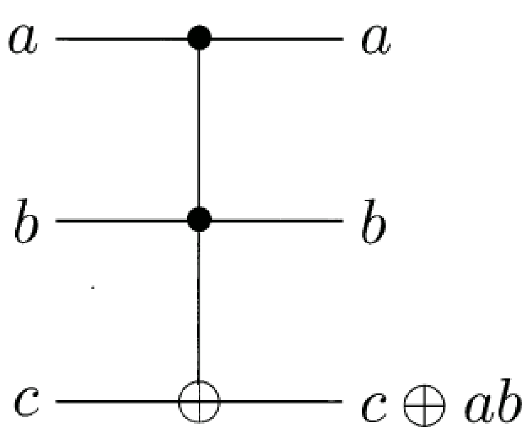
Toffoli gate



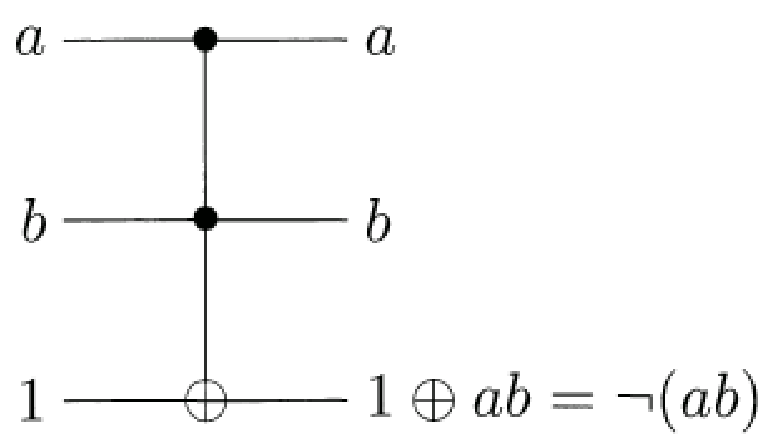
Simulate NAND gate

What kind of computations are possible using quantum circuits?

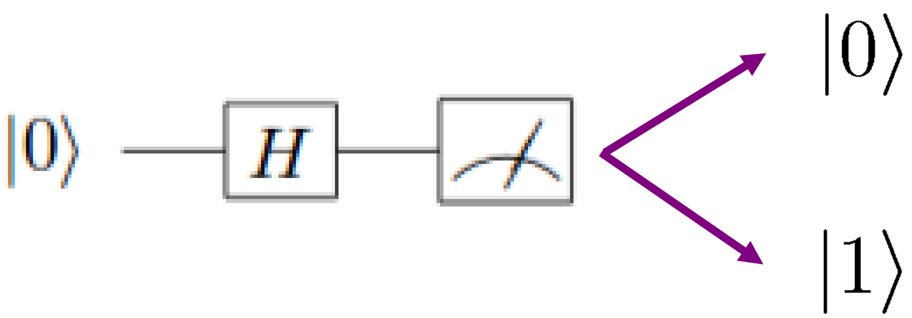
- Classical computations?



Toffoli gate



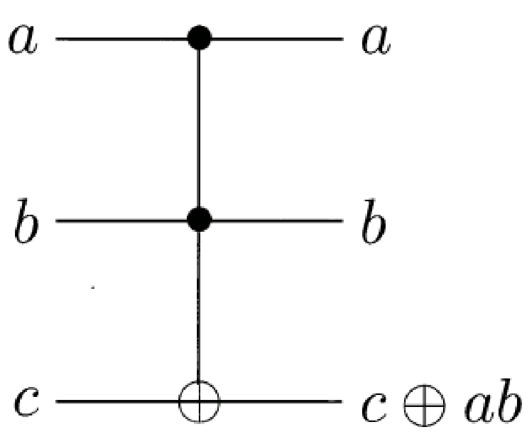
Simulate NAND gate



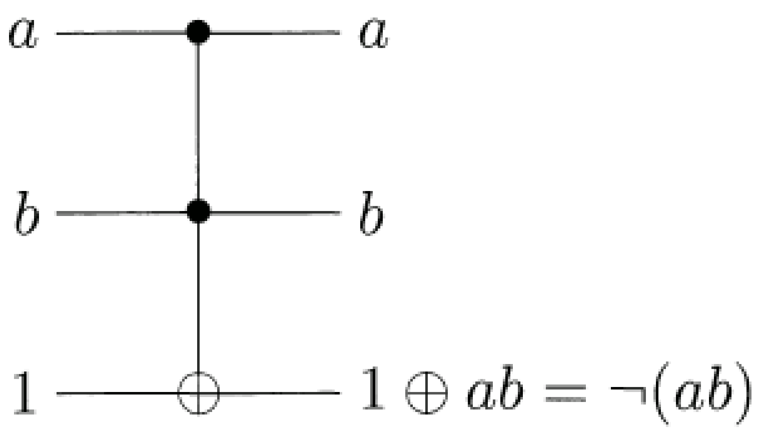
With probability 1/2

What kind of computations are possible using quantum circuits?

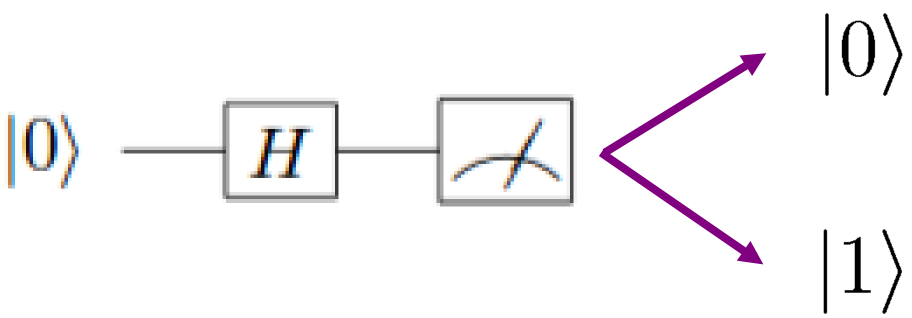
- Classical computations?



Toffoli gate



Simulate NAND gate



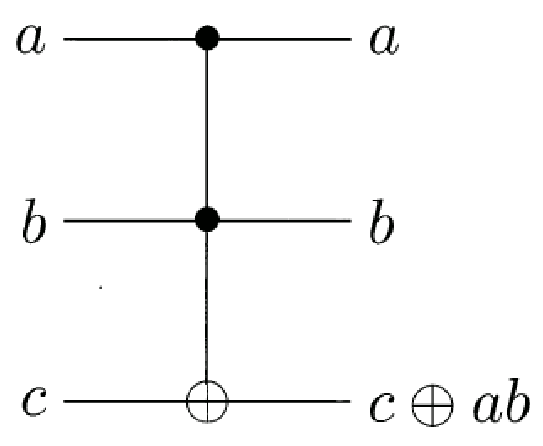
Simulate fair coin toss

With probability 1/2

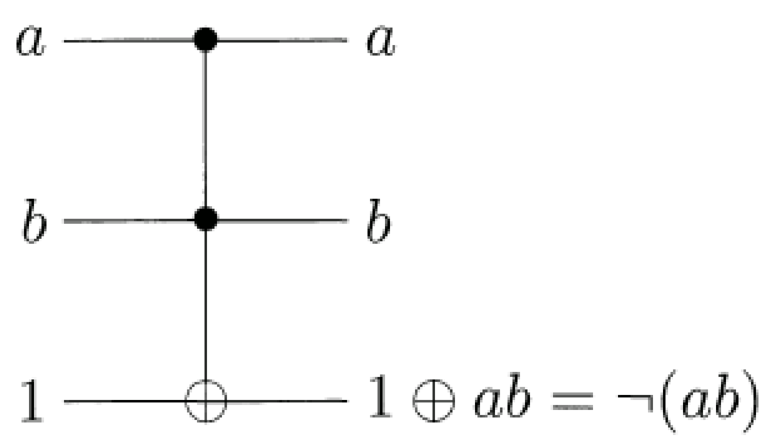
What kind of computations are possible using quantum circuits?

Efficient simulation of a classical non-deterministic computer

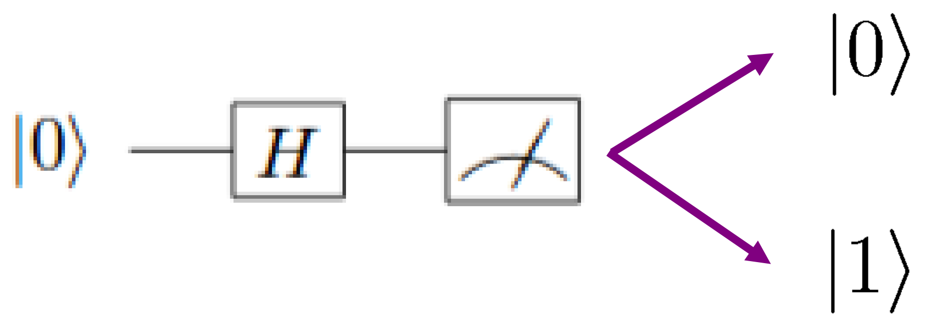
- Classical computations?



Toffoli gate



Simulate NAND gate



With probability 1/2

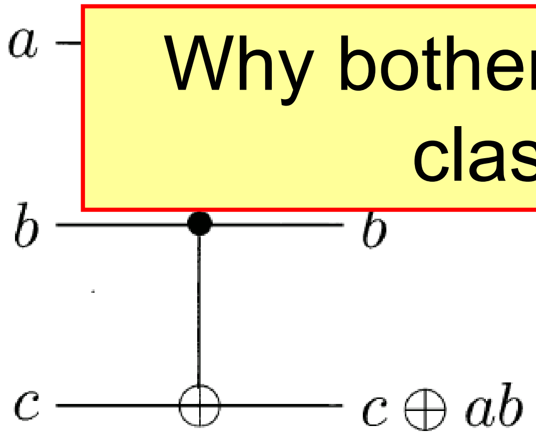
Simulate fair coin toss

What kind of computations are possible using quantum circuits?

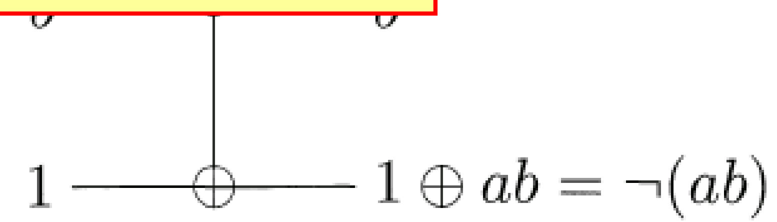
Efficient simulation of a classical non-deterministic computer

- Classical computations?

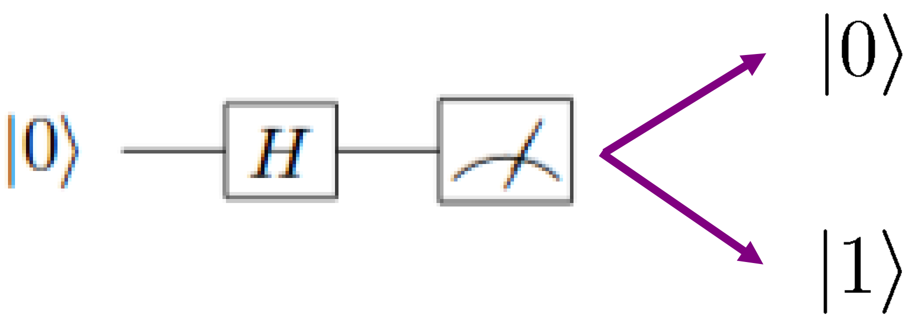
Why bother exploit quantum effects for classical computations?



Toffoli gate



Simulate NAND gate



With probability 1/2

Simulate fair coin toss

What kind of computations are possible using quantum circuits?

Efficient simulation of a
classical non-deterministic computer

- Classical computations?

a

Why bother exploit quantum effects for
classical computations?

b b

c $\oplus\, ab = \neg(ab)$

T

Mass production of silicone chips
almost to perfection

Vs

No stable system of a handful of qubits

ND gate

$|0\rangle$

coin toss

$|1\rangle$

With probability 1/2

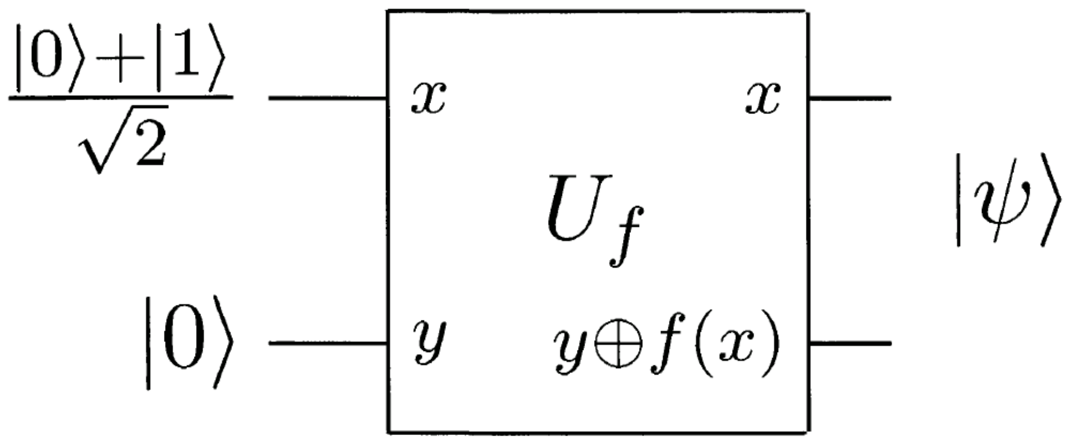
Quantum Parallelism!

Quantum Parallelism!

"Evaluate" $f(x)$ for many ***different*** values of x simultaneously!

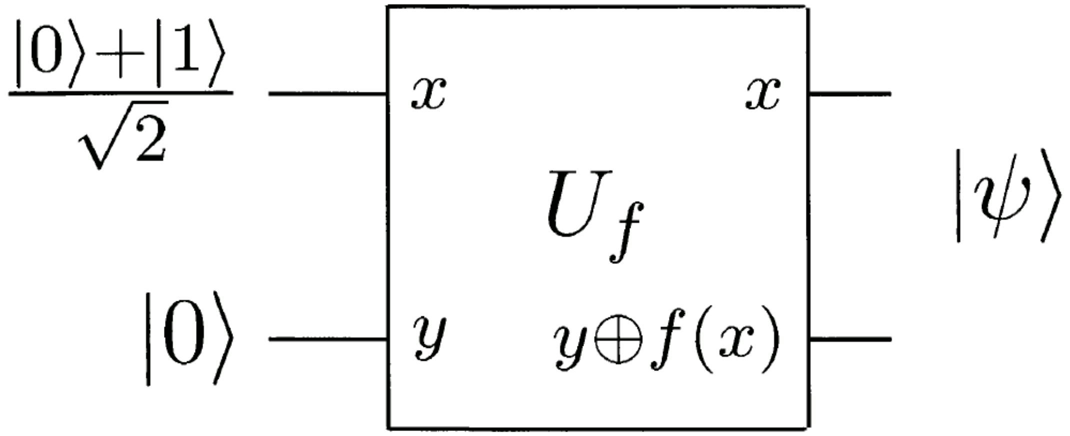
Quantum Parallelism!

"Evaluate" $f(x)$ for many ***different*** values of x simultaneously!



Quantum Parallelism!

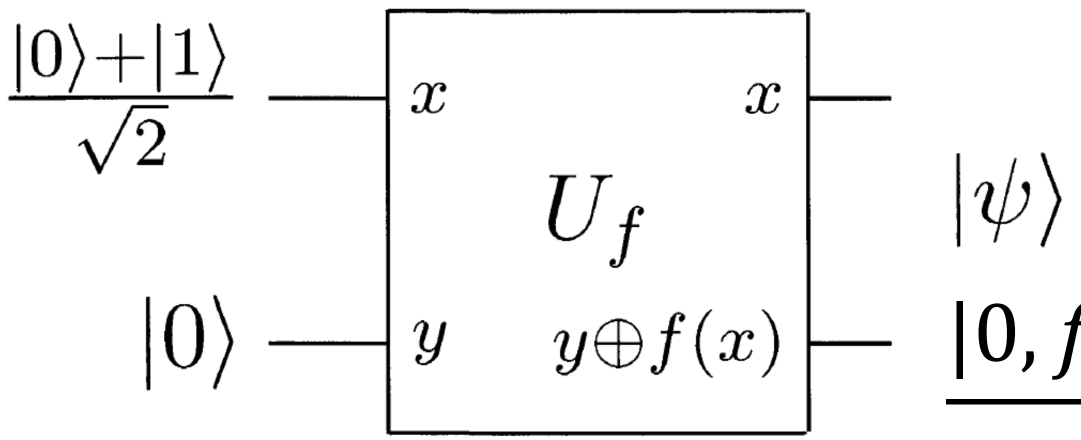
“Evaluate” $f(x)$ for many ***different*** values of x simultaneously!



$$|0{,}0\rangle \longmapsto |0, f(0)\rangle$$
$$|1{,}0\rangle \longmapsto |1, f(1)\rangle$$

Quantum Parallelism!

"Evaluate" $f(x)$ for many ***different*** values of x simultaneously!



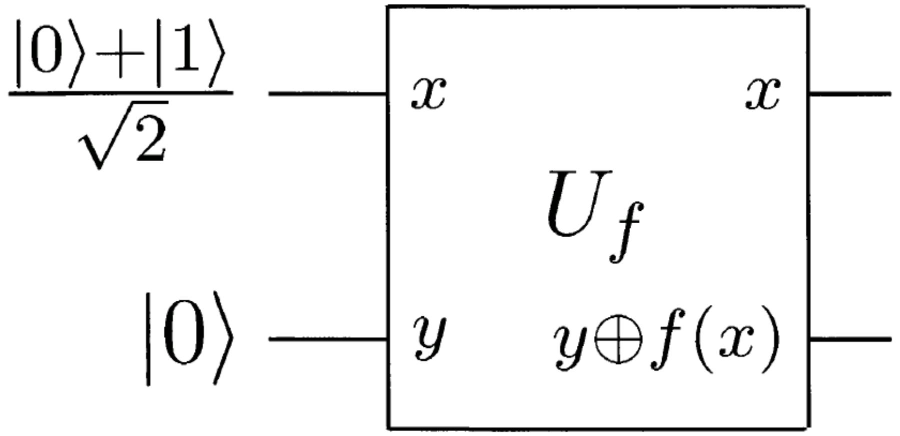
$$\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$$

$$|0,0\rangle \longmapsto |0, f(0)\rangle$$
$$|1,0\rangle \longmapsto |1, f(1)\rangle$$

Single circuit for "simultaneous evaluation" of both $f(0)$ and $f(1)$

Quantum Parallelism!

"Evaluate" $f(x)$ for many ***different*** values of x simultaneously!



$|\psi\rangle$

$$\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$$

$|0{,}0\rangle \longmapsto |0, f(0)\rangle$
$|1{,}0\rangle \longmapsto |1, f(1)\rangle$

Single circuit for "simultaneous evaluation" of both $f(0)$ and $f(1)$

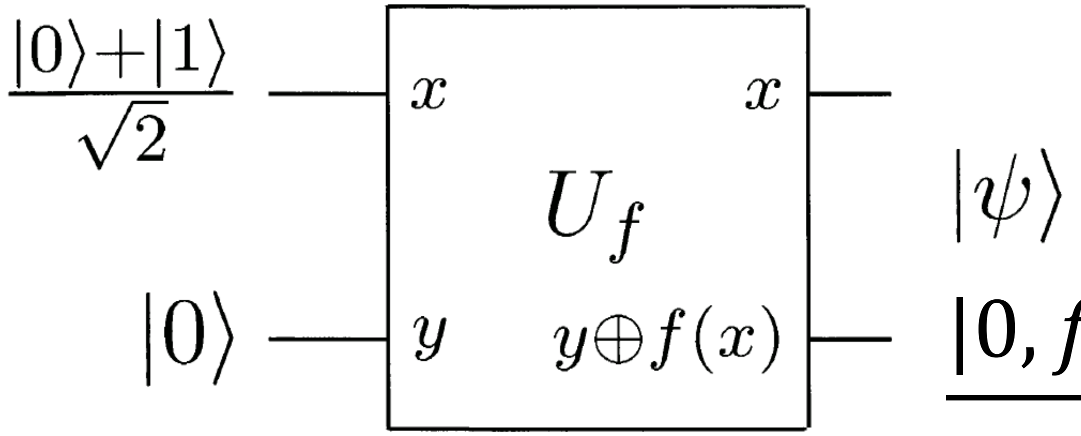
But wait a minute!

Measurement will necessarily destroy the state, yielding ***only one*** of $f(0)$, $f(1)$!!!

Quantum Parallelism!

“Evaluate” $f(x)$ for many ***different*** values of x simultaneously!

How to extract **more useful information** from a superposition state?



$$\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$$

$$|0,0\rangle \longmapsto |0, f(0)\rangle$$
$$|1,0\rangle \longmapsto |1, f(1)\rangle$$

Single circuit for “simultaneous evaluation” of both $f(0)$ and $f(1)$

But wait a minute!

Measurement will necessarily destroy the state, yielding ***only one*** of $f(0)$, $f(1)$!!!

Quantum Parallelism + Quantum Interference!

Quantum Parallelism + Quantum Interference!

Deutsch's problem:
Determine whether $f(x): \{0,1\} \to \{0,1\}$ is constant or balanced

Quantum Parallelism + Quantum Interference!

Deutsch's problem:
Determine whether $f(x): \{0,1\} \rightarrow \{0,1\}$ is constant or balanced

Classically, we need 2 evaluations!
Using quantum parallelism + interference, only one!

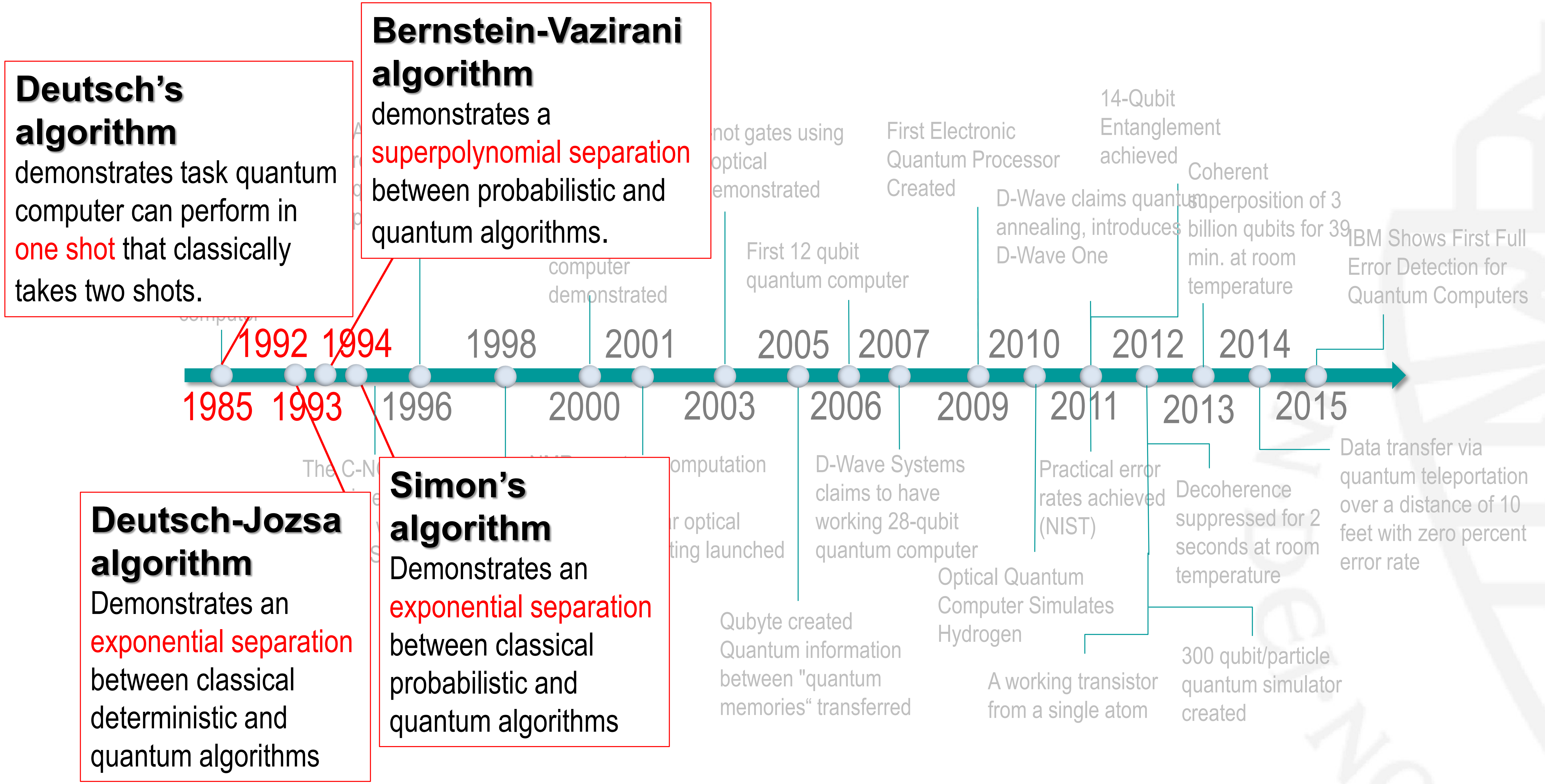
Quantum Parallelism + Quantum Interference!

Deutsch's problem:
Determine whether $f(x): \{0,1\} \to \{0,1\}$ is constant or balanced

Classically, we need 2 evaluations!
Using quantum parallelism + interference, only one!

First algorithm to illustrate the power of Quantum computation!

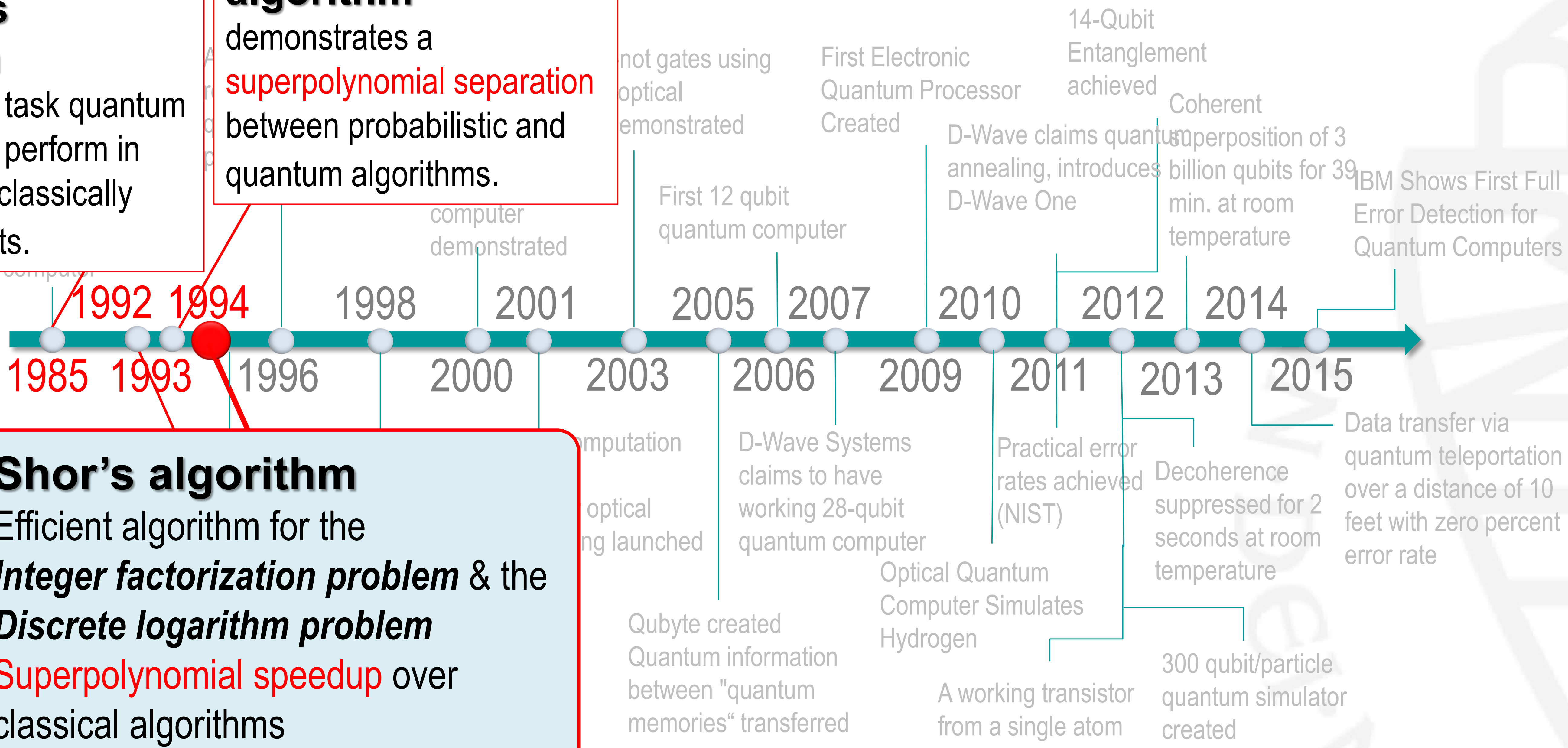
Quantum algorithms breakthroughs



Quantum algorithms breakthroughs

Deutsch's algorithm
demonstrates task quantum computer can perform in one shot that classically takes two shots.

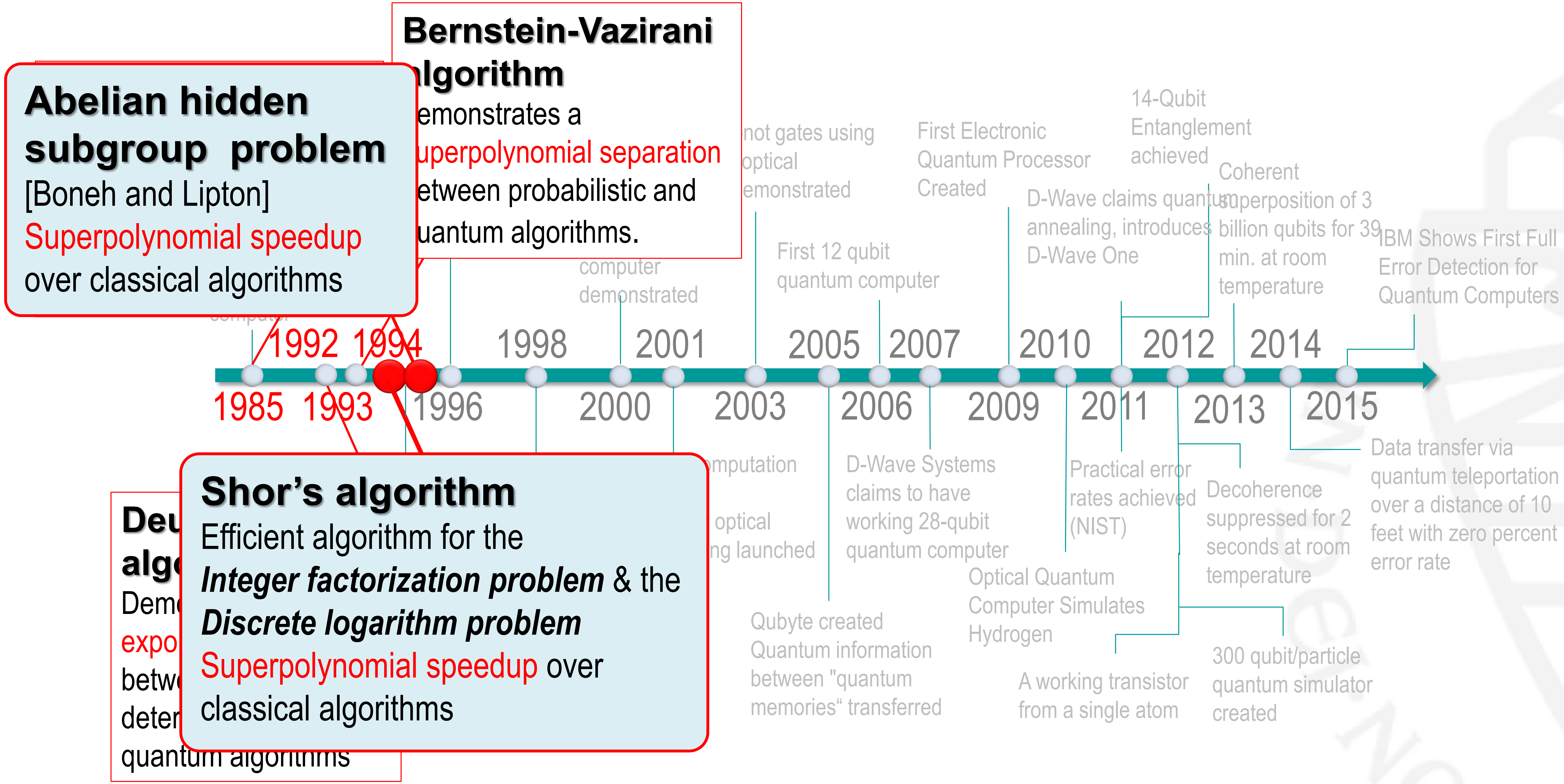
Bernstein-Vazirani algorithm
demonstrates a superpolynomial separation between probabilistic and quantum algorithms.



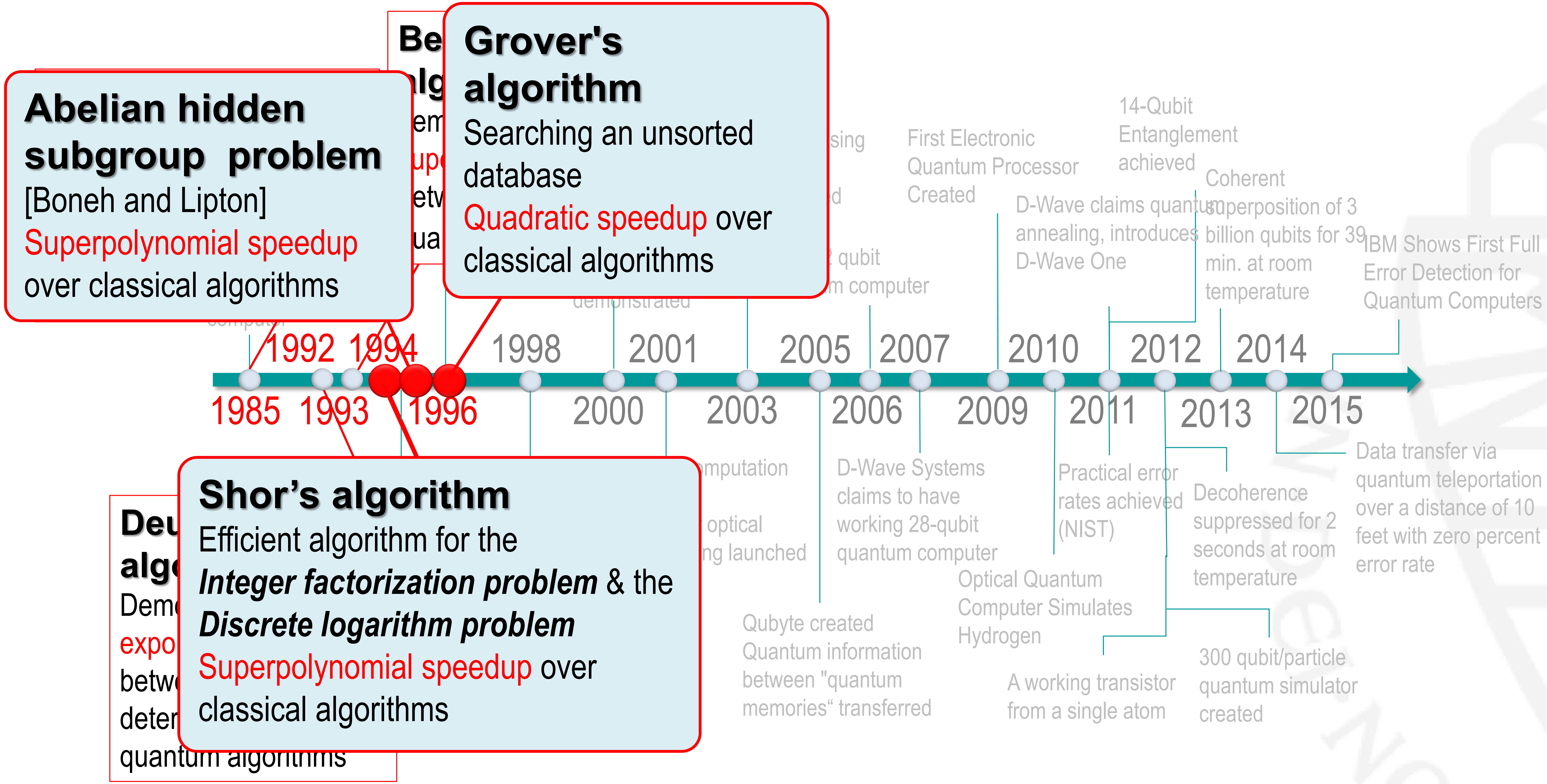
Shor's algorithm
Efficient algorithm for the
Integer factorization problem & the
Discrete logarithm problem
Superpolynomial speedup over classical algorithms

Deu... alg...
Dem...
expo...
betw...
deter...
quantum algorithms

Quantum algorithms breakthroughs



Quantum algorithms breakthroughs



Quantum algorithms breakthroughs

Abelian hidden subgroup problem
[Boneh and Lipton]
Superpolynomial speedup over classical algorithms

Grover's algorithm
Searching an unsorted database
Quadratic speedup over classical algorithms

Shor's algorithm
Efficient algorithm for the ***Integer factorization problem*** & the ***Discrete logarithm problem***
Superpolynomial speedup over classical algorithms

Breakthrough Algorithms

- Not only examples, but
- Of critical practical value
- **Contemporary security relies on these problems**
- Start the era of broader interest in quantum computing and quantum technology

1985 1992 1993 1994 1996 1998 2000 2001 2003 2005

Quantum algorithms breakthroughs

1985 1992 1993 1994 1996 1998 2000 2001 2003 2005

Abelian hidden subgroup problem
[Boneh and Lipton]
Superpolynomial speedup over classical algorithms

Grover's algorithm
Searching an unsorted database
Quadratic speedup over classical algorithms

Shor's algorithm
Efficient algorithm for the ***Integer factorization problem*** & the ***Discrete logarithm problem***
Superpolynomial speedup over classical algorithms

Breakthrough Algorithms
- Not only examples, but
- Of critical practical value
- **Contemporary security relies on these problems**
- Start the era of broader interest in quantum computing and quantum technology

Shor’s algorithm [Shor ’94]

- Integer factorization algorithm
- Discrete logarithm problem

Number theory + Parallelism + Interference

Shor's algorithm [Shor '94]

- Integer factorization algorithm
- Discrete logarithm problem

Number theory + Parallelism + Interference

Best classical algorithm

General number field sieve

$$e^{O(n^{1/3}(\log n)^{2/3})}$$

(Subexponential complexity)

Shor's algorithm [Shor '94]

- Integer factorization algorithm
- Discrete logarithm problem

Number theory + Parallelism + Interference

Best classical algorithm

General number field sieve

$$e^{O(n^{1/3}\,(\log n)^{\,2/3})}$$

(Subexponential complexity)

Shor's algorithm

$$O(n^3)$$

(Polynomial complexity)

Shor's algorithm [Shor '94]

- Integer factorization algorithm
- Discrete logarithm problem

Number theory + Parallelism + Interference

Best classical algorithm

General number field sieve

$$e^{O(n^{1/3}(\log n)^{2/3})}$$

(Subexponential complexity)

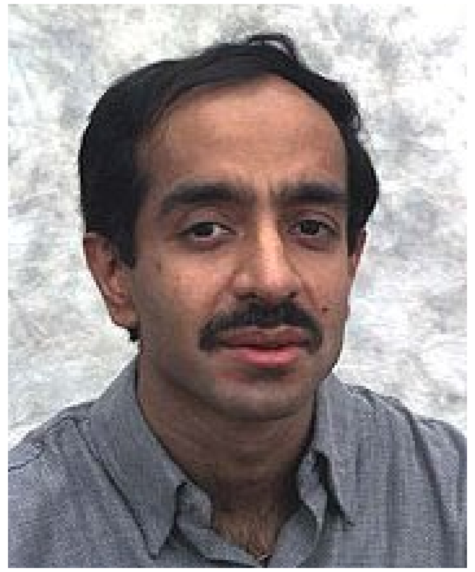
Shor's algorithm

$$O(n^3)$$

(Polynomial complexity)

To factor a 2048 bit number:

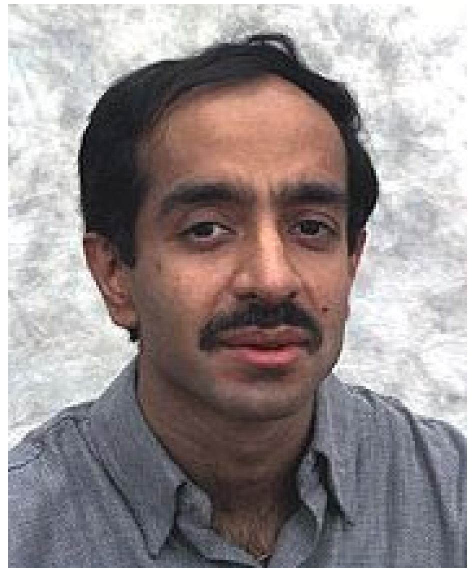
Best classical algorithm	Shor's algorithm
~ 150,000 years	< 1 second



Grover's algorithm [Grover '96]

Search problem

Input: A search space of N elements.
Problem: Find an element of the space that satisfies a property

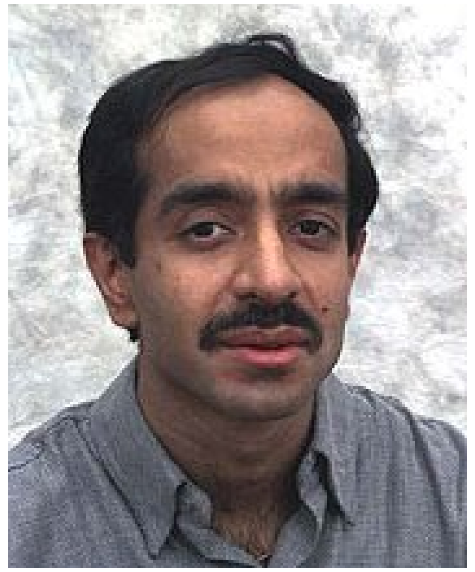


Grover's algorithm [Grover '96]

Search problem

Input: A search space of N elements.
Problem: Find an element of the space that satisfies a property

- A quantum algorithm based on **amplitude amplification**



Grover's algorithm [Grover '96]

Search problem

Input: A search space of N elements.
Problem: Find an element of the space that satisfies a property

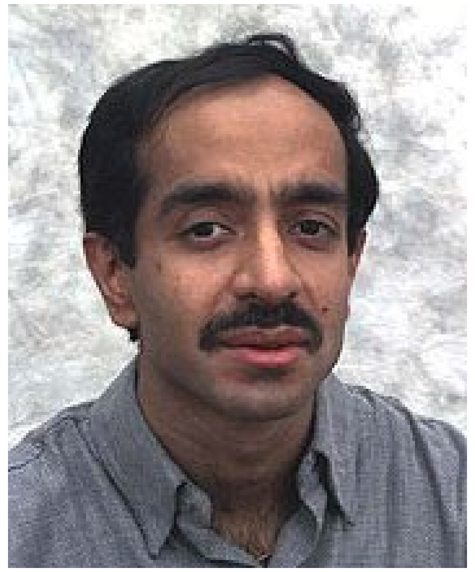
- A quantum algorithm based on **amplitude amplification**
- Offers **quadratic speedup** over classical algorithms

Classical algorithms

$\Omega(N)$ operations

Grover's algorithm

$O(\sqrt{N})$ operations



Grover's algorithm [Grover '96]

Search problem

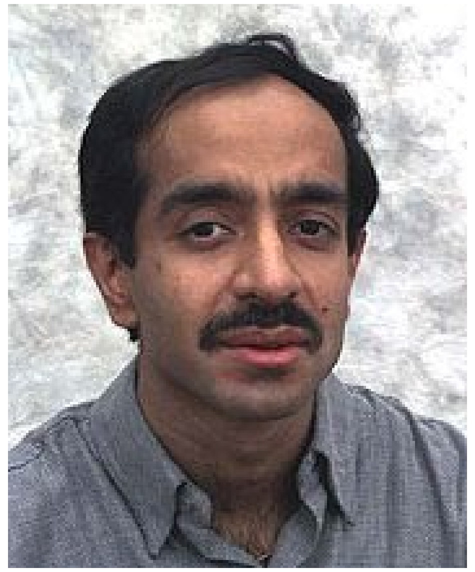
Input: A search space of N elements.
Problem: Find an element of the space that satisfies a property

- A quantum algorithm based on **amplitude amplification**
- Offers **quadratic speedup** over classical algorithms

Classical algorithms	Grover's algorithm
$\Omega(N)$ operations	$O(\sqrt{N})$ operations

Break a 8 character password of only lowercase letters:

$\sim$ 4.13 years	$<$ 5 days



Grover's algorithm [Grover '96]

Search problem

Input: A search space of N elements.
Problem: Find an element of the space that satisfies a property

- A quantum algorithm based on **amplitude amplification**
- Offers **quadratic speedup** over classical algorithms

Classical algorithms	Grover's algorithm
$\Omega(N)$ operations	$O(\sqrt{N})$ operations

Provably optimal runtime!

Break a 8 character password of only lowercase letters:

Classical algorithms	Grover's algorithm
$\sim$ 4.13 years	$<$ 5 days

Quantum computer – The Crypto eating monster

Today’s cryptography in use?

Algorithms we use:

- *RSA encryption scheme*
- *DSA – digital signature*
- *Diffie-Hellman (DH) key exchange*
- *ECDSA (Elliptic curve cryptography)*
- *Pairing based cryptography*

Practically implemented in:

- *PKI / PGP*
- *SSL/TLS (HTTPS, FTPS)*
- *SSH (SFTP, SCP)*
- *IPsec (IKE)*
- *IEEE 802.11*
- ……
- *Commitments*
- *Electronic voting*
- *Digital cash/credentials*
- *Multiparty computation*
- *……*

Today's cryptography in use?

Algorithms we use:

- *RSA encryption scheme*
- *DSA – di*
- *Diffie-He*
- *ECDSA (*
- *Pairing b*

Broken by Shor-like Quantum Algorithms

Algorithm	Key Length	Security Level	
		Conventional Computing	Quantum Computing
RSA-1024	1024 bits	80 bits	0 bits
RSA-2048	2048 bits	112 bits	0 bits
ECC-256	256 bits	128 bits	0 bits
ECC-384	384 bits	256 bits	0 bits

Effective key strength for conventional computing derived from NIST SP 800-57 "Recommendation for Key Management"

Today's cryptography in use?

Influenced by Grover – like Algorithms

Doubling of key size

- *Block ciphers*
  - *AES*
- *Stream ciphers*
- *Hash functions*
  - *SHA-1, SHA-2, SHA-3*
- *(All symmetric key primitives)*
  - *MACs, HMACs, PRNGs, AE ciphers…*
- *Primitives based on NP-hard problems*
  - *Code-based, Lattice-based, Multivariate systems*

Today's cryptography in use?

Influenced by Grover – like Algorithms

Not trivial, but manageable!

Doubling of key

- *Block ciphers*
  - *AES*
- *Stream ciphers*
- *Hash functions*
  - *SHA-1, SHA-2, SHA-3*
- *(All symmetric key*
  - *MACs, HMACs, PRNG*
- *Primitives based o*
  - *Code-based, Lattice-b*

Algorithm	Key Length	Security Level	
		Conventional	Quantum
AES-128	128 bits	128 bits	64 bits
AES-256	256 bits	256 bits	128 bits

Algorithm	Security Level	
	Conventional (Preimage/Collisions)	Quantum (Preimage/Collisions)
SHA-256	256/128 bits	128/85 bits
SHA-512	512/256 bits	256/170 bits

Effective key strength for conventional computing derived from NIST SP 800-57 “Recommendation for Key Management”

Some emerging questions!

Some emerging questions!

- Is it possible that in the future we come up with algorithms that **totally break symmetric crypto** just as Shor's algorithm breaks Integer Factorization and Discrete Log?

Some emerging questions!

- Is it possible that in the future we come up with algorithms that **totally break symmetric crypto** just as Shor's algorithm breaks Integer Factorization and Discrete Log?
- … and algorithms that **break NP-compete problems?**

Some emerging questions!

- Is it possible that in the future we come up with algorithms that **totally break symmetric crypto** just as Shor's algorithm breaks Integer Factorization and Discrete Log?
- … and algorithms that **break NP-compete problems?**

… **OR** …

Some emerging questions!

- Is it possible that in the future we come up with algorithms that **totally break symmetric crypto** just as Shor's algorithm breaks Integer Factorization and Discrete Log?
- … and algorithms that **break NP-compete problems?**

… **OR** …

- Is it just a **mere coincidence** that we came up with efficient Quantum Integer Factorization algorithm before classical….

Some emerging questions!

- Is it possible that in the future we come up with algorithms that **totally break symmetric crypto** just as Shor's algorithm breaks Integer Factorization and Discrete Log?
- … and algorithms that **break NP-compete problems?**

… **OR** …

- Is it just a **mere coincidence** that we came up with efficient Quantum Integer Factorization algorithm before classical….

NOBODY KNOWS!!!

Some emerging questions!

- Is it possible that in the future we come up with algorithms that **totally break symmetric crypto** just as Shor's algorithm breaks Integer Factorization and Discrete Log?
- … and algorithms that **break NP-compete problems?**

… **OR** …

- Is it just a **mere coincidence** that we came up with efficient Quantum Integer Factorization algorithm before classical….

Actually nobody knows…

Where exactly

the algorithms solvable by quantum computers in polynomial time

fit in our established complexity hierarchy!

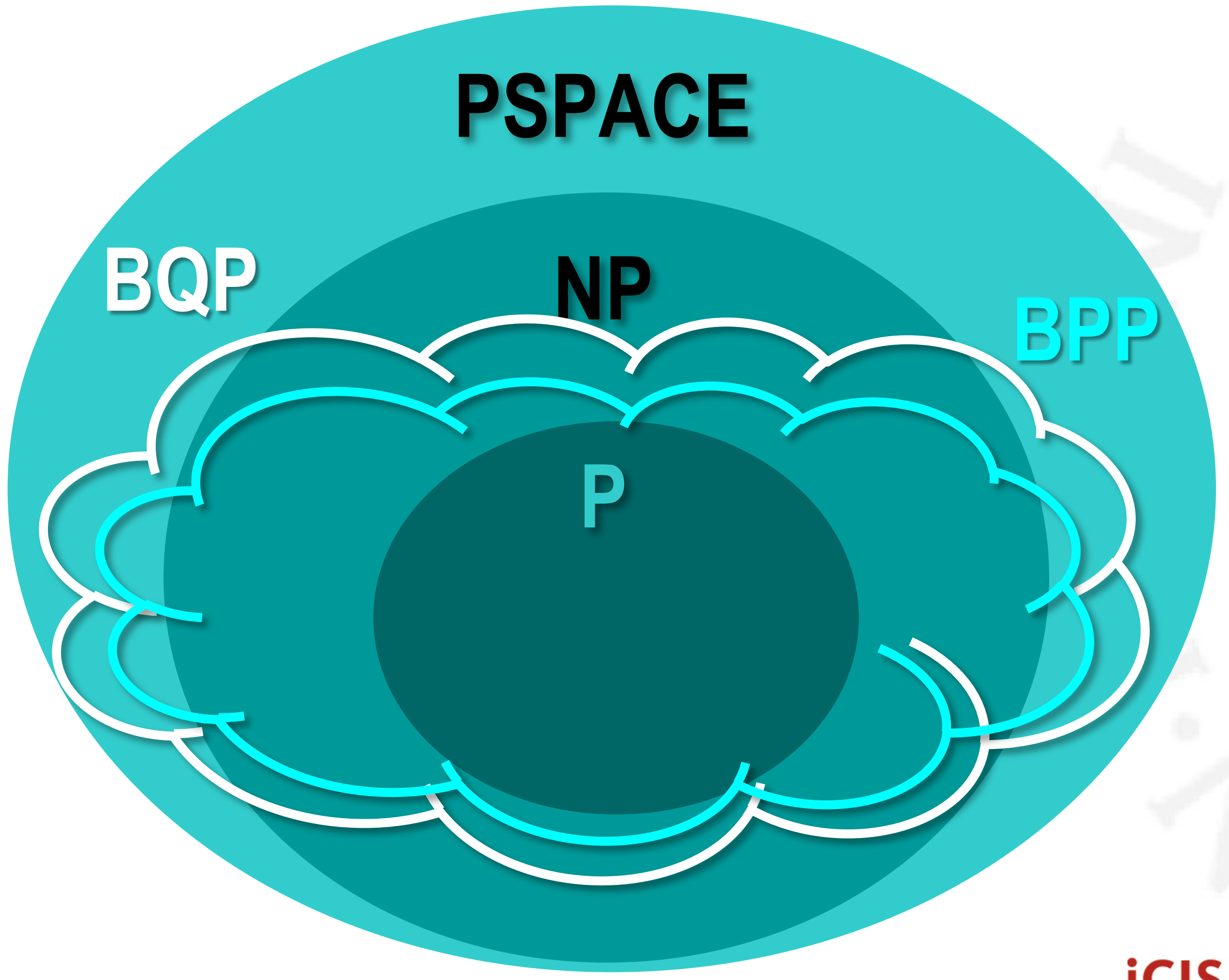
Alphabet soup of Computational problems

- **P**: solvable in deterministic polynomial time
- **NP**: solvable in non-deterministic polynomial time
- **PSPACE**: solvable in polynomial space
- **BPP**: solvable in polynomial time with bounded probability error
- **BQP**: solvable in polynomial time by a quantum computer with bounded probability error

We know that:

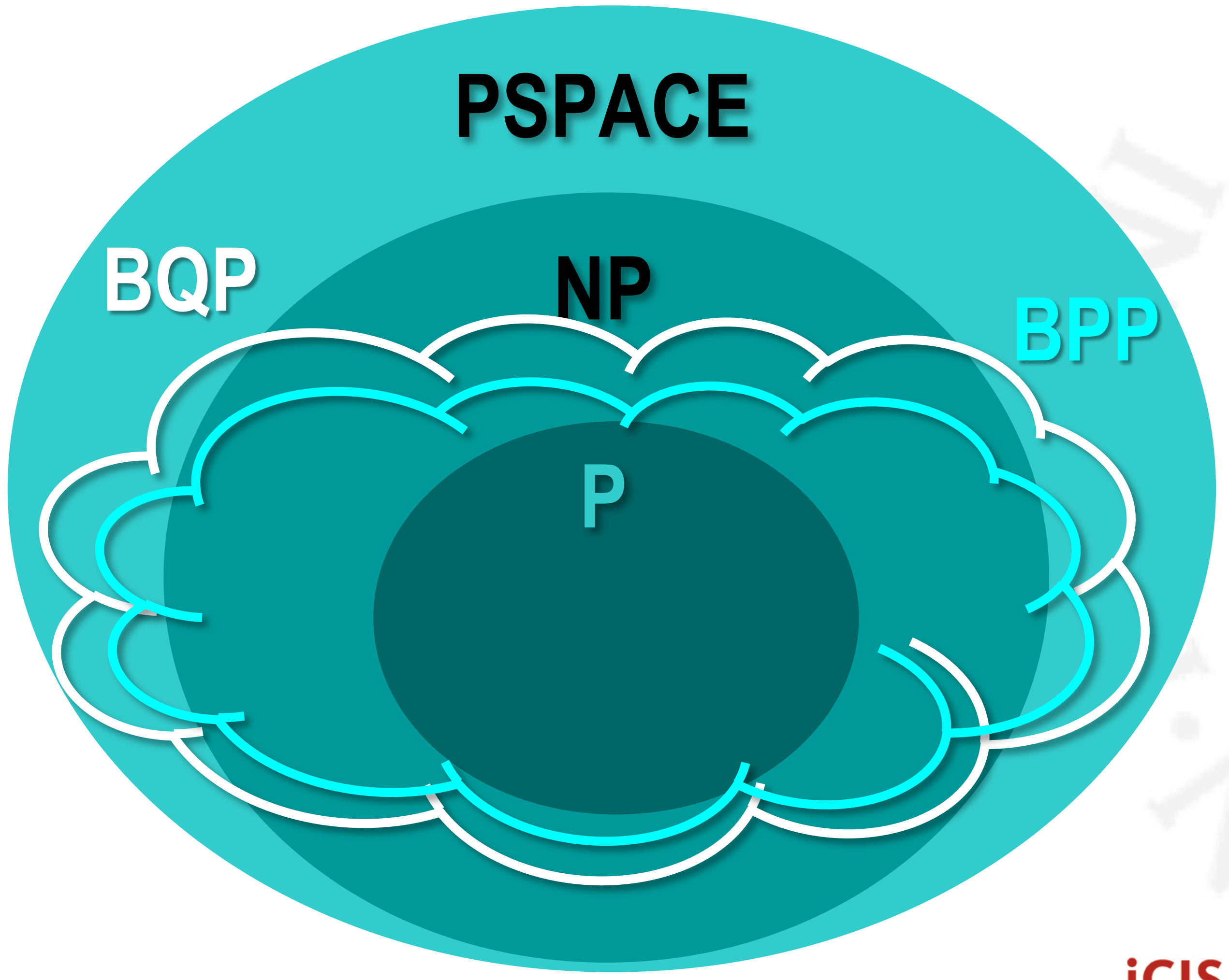
$P \subseteq NP \subseteq PSPACE$

$P \subseteq BPP \subseteq BQP \subseteq PSPACE$



What we don't know (and has implications to crypto):

BPP ? BQP   BQP ? NP



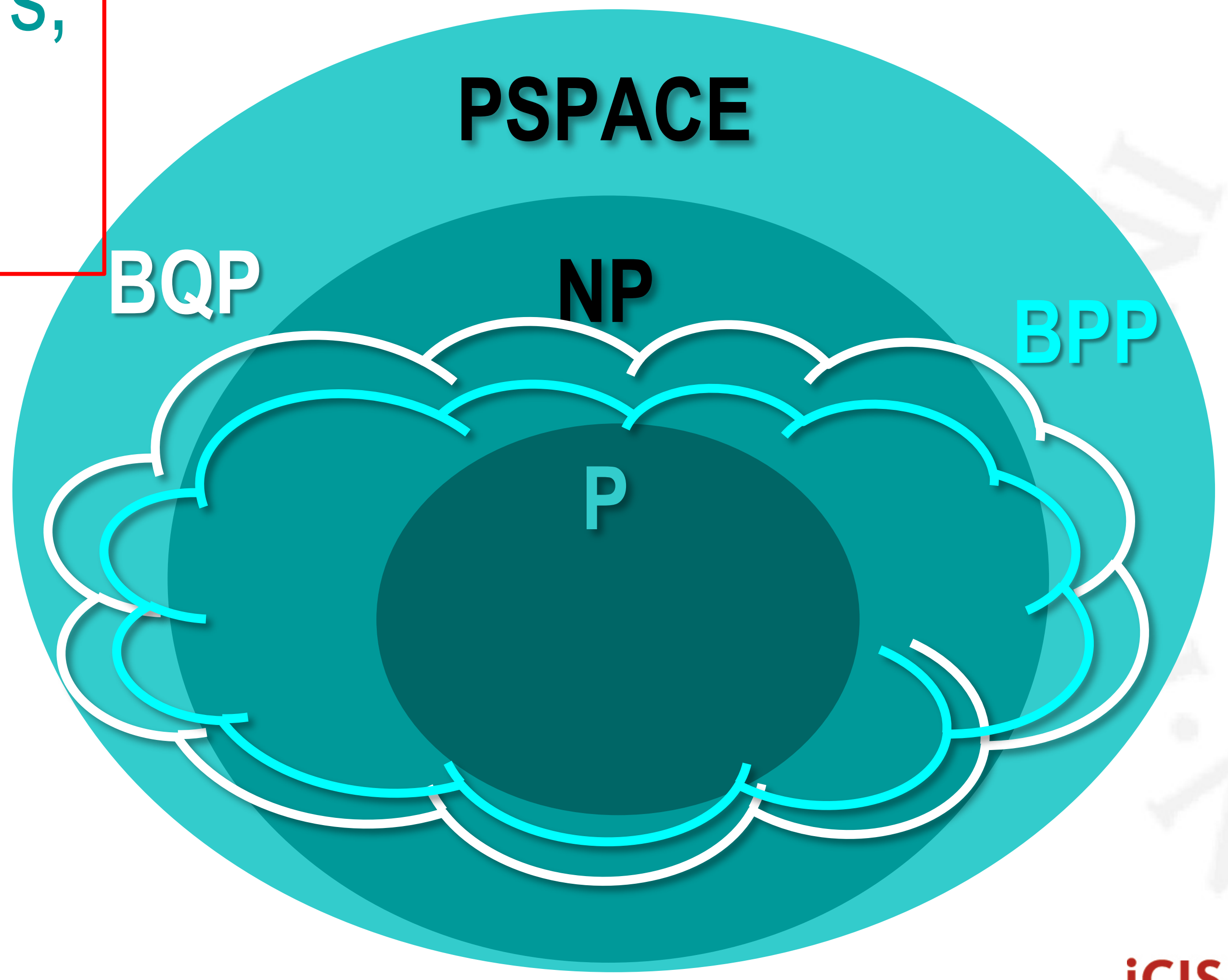
What we don’t know (and has implications to crypto):

BPP ? BQP   BQP ? NP

Extreme cases:

BPP = BQP

We don’t need quantum computers, we just need to discover the classical algorithms!!!



What we don't know (and has implications to crypto):

BPP ? BQP   BQP ? NP

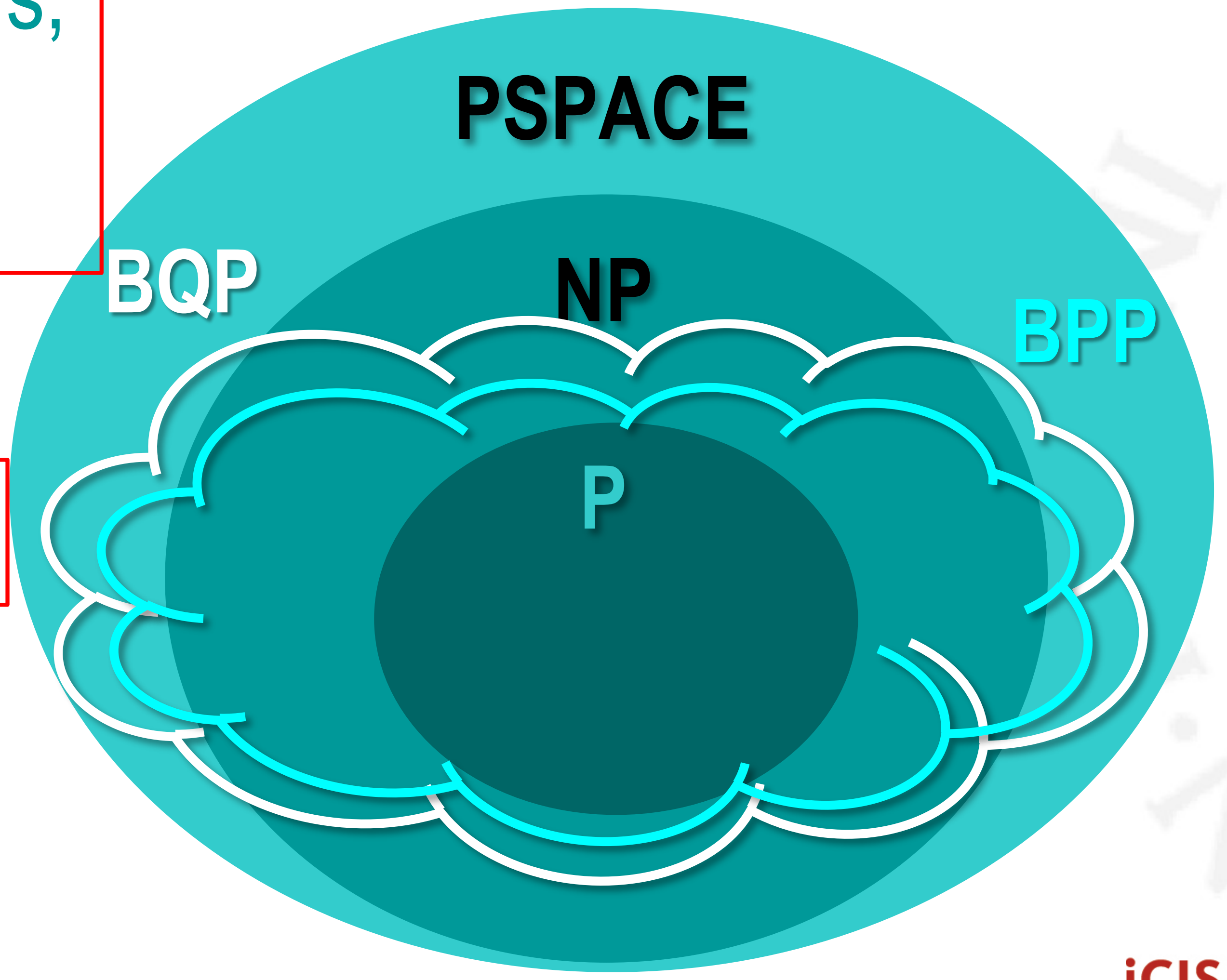
Extreme cases:

BPP = BQP

We don't need quantum computers, we just need to discover the classical algorithms!!!

NP $\subseteq$ BQP

Classical cryptography is dead!!!



What we don't know (and has implications to crypto):

BPP ? BQP BQP ? NP

Extreme cases:

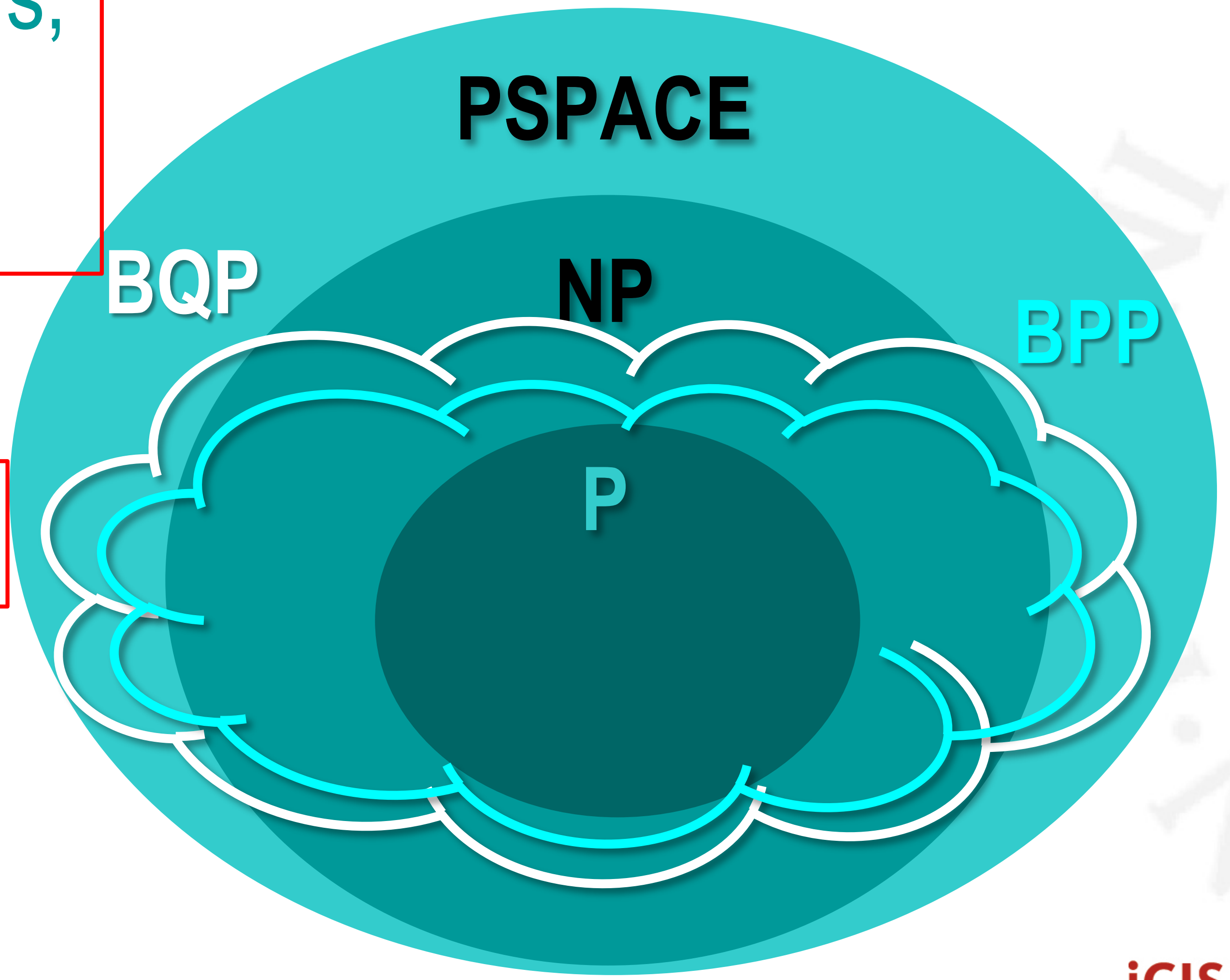
BPP = BQP

We don't need quantum computers, we just need to discover the classical algorithms!!!

NP ⊆ BQP

Classical cryptography is dead!!!

Both rather unlikely!



What we don't know (and has implications to crypto):

BPP ? BQP BQP ? NP

Both rather unlikely!

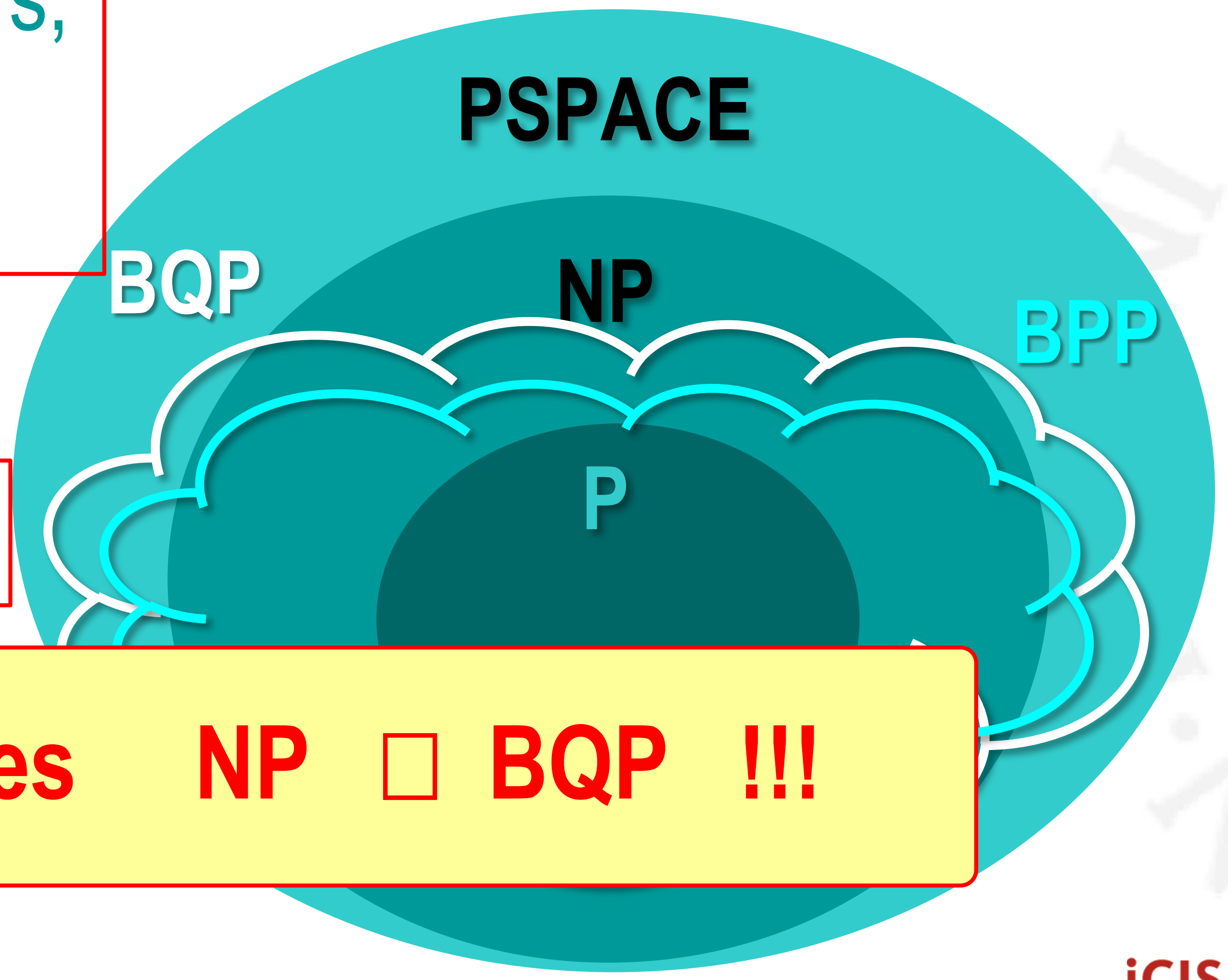
Extreme cases:

BPP = BQP

We don't need quantum computers, we just need to discover the classical algorithms!!!

NP $\subseteq$ BQP

Classical cryptography is dead!!!



Optimality of Grover's algorithm indicates NP □ BQP !!!

It's **rather unlikely** that (under the assumption that they are ever built) **quantum computers will kill ALL classical cryptography**…

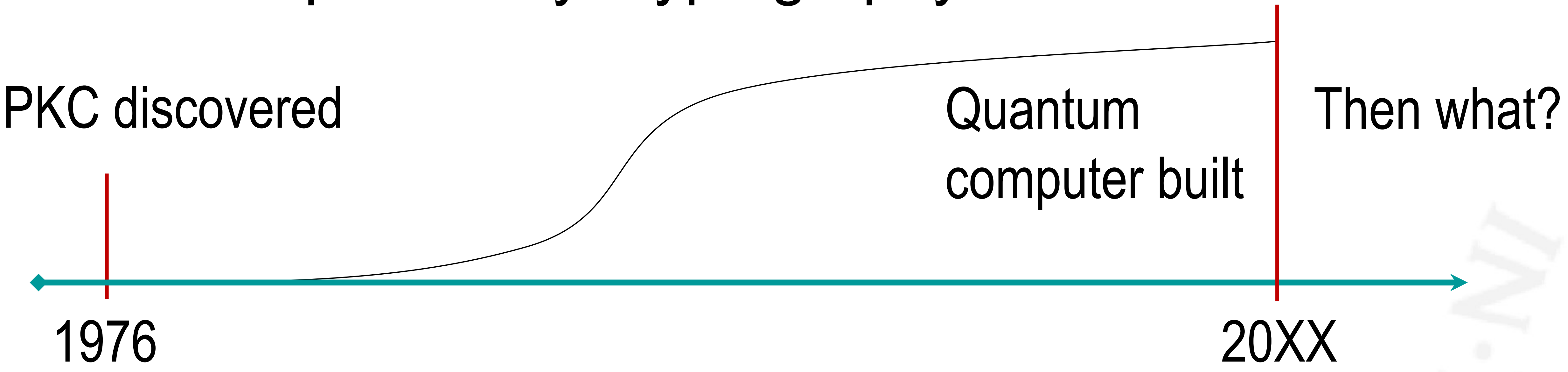
…At least not symmetric cryptography!

It’s **rather unlikely** that (under the assumption that they are ever built) **quantum computers will kill ALL classical cryptography**…
…At least not symmetric cryptography!

What about public key cryptography?

It's **rather unlikely** that (under the assumption that they are ever built) **quantum computers will kill ALL classical cryptography**…
…At least not symmetric cryptography!

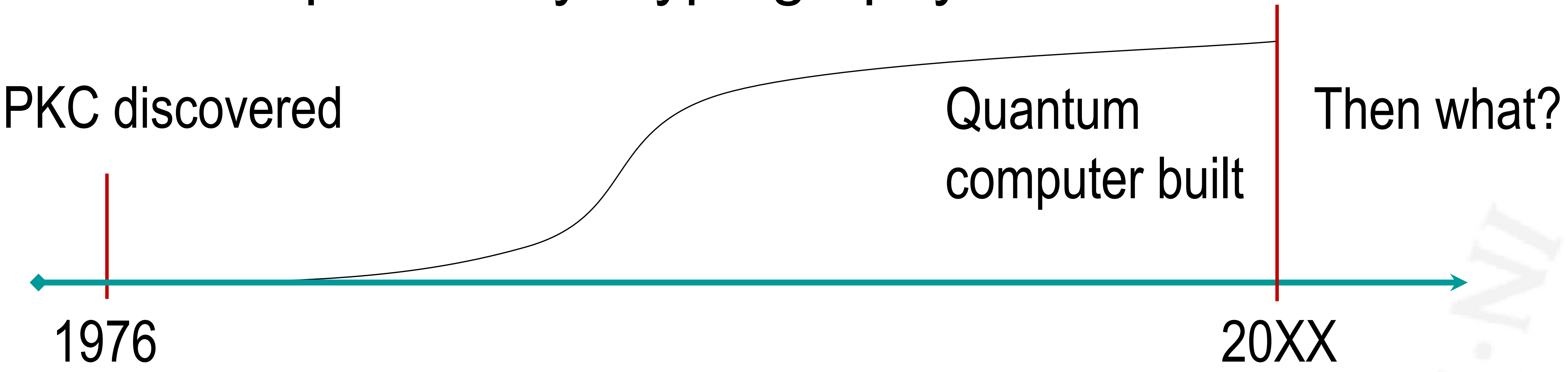
What about public key cryptography?



It's **rather unlikely** that (under the assumption that they are ever built) **quantum computers will kill ALL classical cryptography**…

…At least not symmetric cryptography!

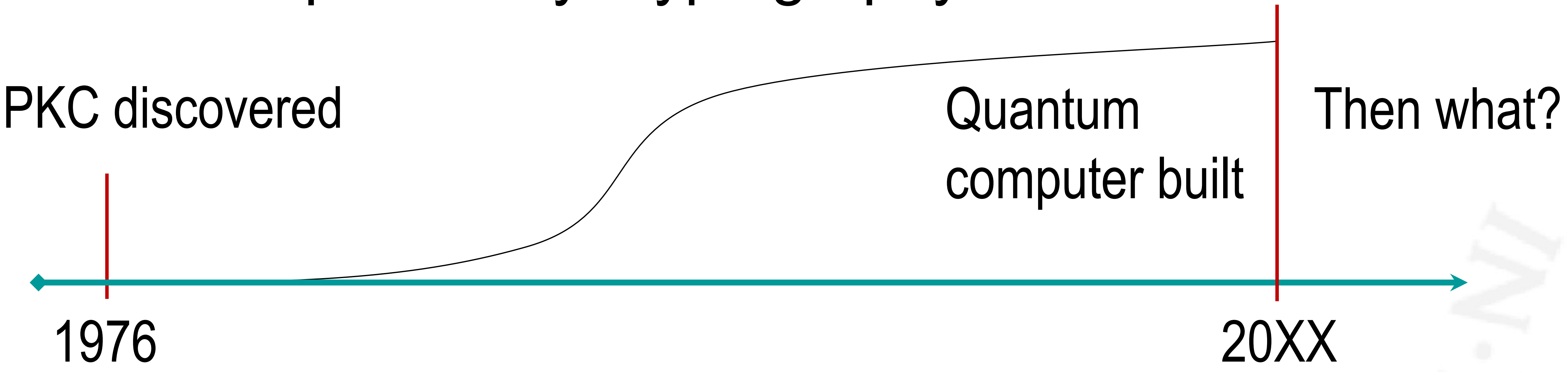
What about public key cryptography?



Will we need **quantum cryptography?**

It’s **rather unlikely** that (under the assumption that they are ever built) **quantum computers will kill ALL classical cryptography**…
…At least not symmetric cryptography!

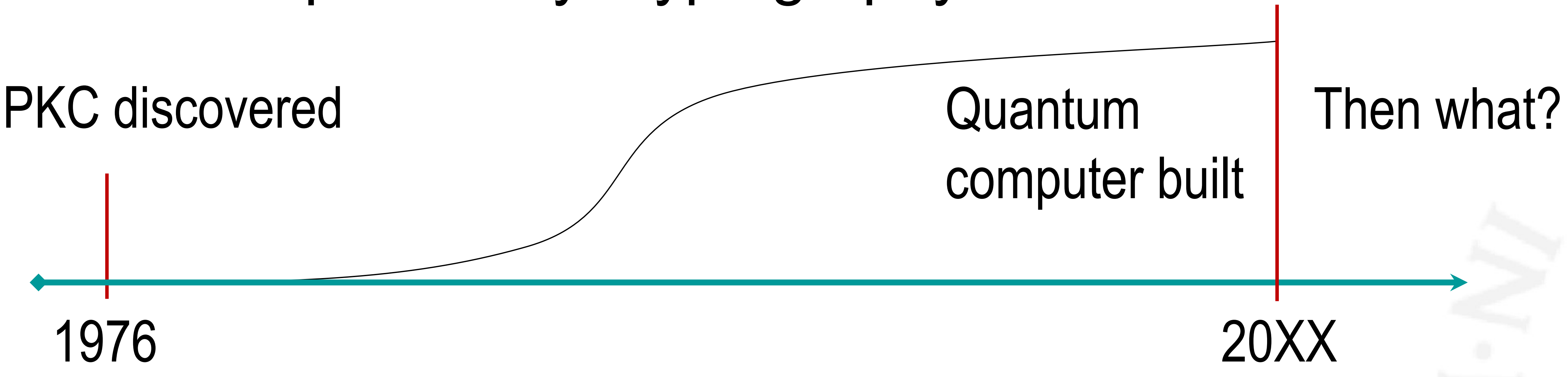
What about public key cryptography?



Will we need **quantum cryptography?**
Or

It's **rather unlikely** that (under the assumption that they are ever built) **quantum computers will kill ALL classical cryptography**…
…At least not symmetric cryptography!

What about public key cryptography?



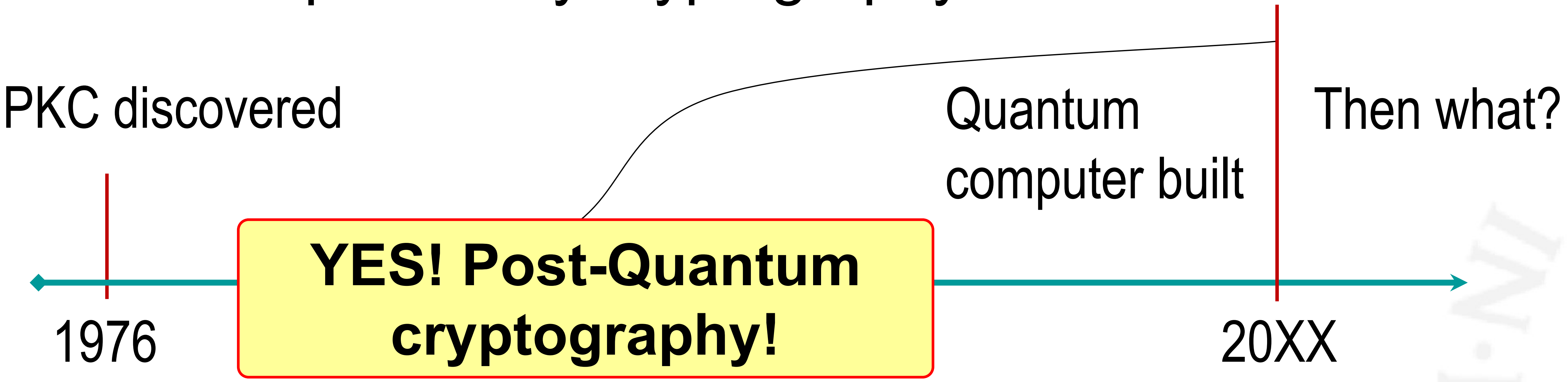
Will we need **quantum cryptography?**

Or

Is it possible to have **strong classical cryptography** in the quantum world?

It's **rather unlikely** that (under the assumption that they are ever built) **quantum computers will kill ALL classical cryptography**…
…At least not symmetric cryptography!

What about public key cryptography?



Will we need **quantum cryptography?**

Or

Is it possible to have **strong classical cryptography** in the quantum world?

Quantum Cryptography

Use quantum mechanical properties to perform cryptographic tasks

Not based on computational assumptions

Quantum Cryptography

Use quantum mechanical properties to perform cryptographic tasks

Not based on computational assumptions

- Quantum key distribution

Quantum Cryptography

Use quantum mechanical properties to perform cryptographic tasks

Not based on computational assumptions

- Quantum key distribution
- Quantum random number generator

Quantum Cryptography

Use quantum mechanical properties to perform cryptographic tasks

Not based on computational assumptions

- Quantum key distribution
- Quantum random number generator
- Quantum commitment

Quantum Cryptography

Use quantum mechanical properties to perform cryptographic tasks

Not based on computational assumptions

- Quantum key distribution
- Quantum random number generator
- Quantum commitment
- Quantum money

Quantum Cryptography

Use quantum mechanical properties to perform cryptographic tasks

Not based on computational assumptions

- Quantum key distribution
- Quantum random number generator
- Quantum commitment
- Quantum money
- Quantum e-voting

Quantum Cryptography

Use quantum mechanical properties to perform cryptographic tasks

Not based on computational assumptions

- Quantum key distribution
- Quantum random number generator
- Quantum commitment
- Quantum money
- Quantum e-voting
- …

Quantum Cryptography

Use quantum mechanical properties to perform cryptographic tasks

Not based on computational assumptions

- Quantum key distribution
- Quantum random number generator
- Quantum commitment
- Quantum money
- Quantum e-voting
- …

Even if quantum computers are built it may take years (if ever) until quantum cryptography is used in everyday life!!!

Quantum Cryptography

Use quantum mechanical properties to perform cryptographic tasks

Not based on computational assumptions

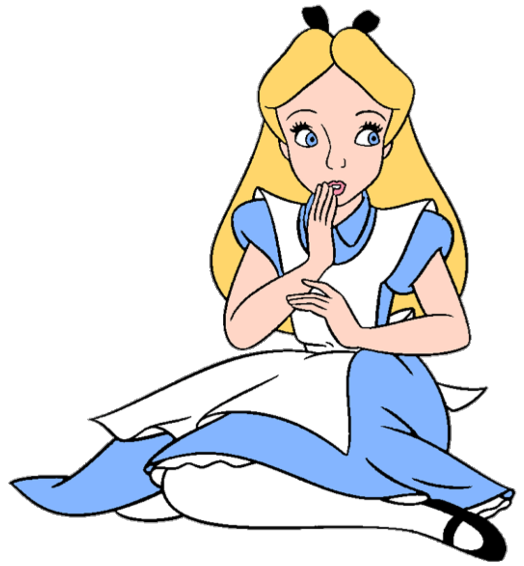
- Quantum key distribution
- Quantum random number generator
- Quantum commitment
- Quantum money
- Quantum e-voting
- …

Benefit only to governments, corporations, not to protect the people!

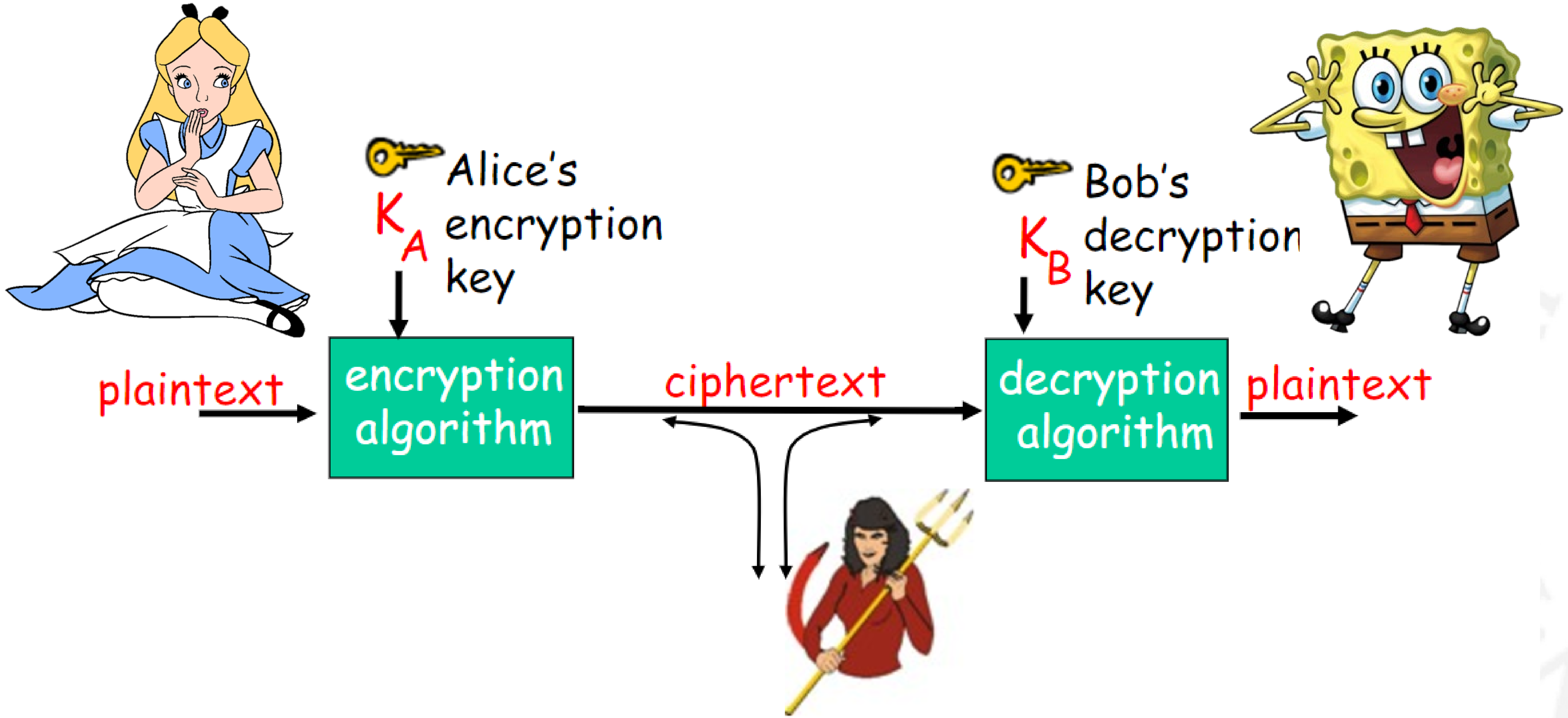
Even if quantum computers are built it may take years (if ever) until quantum cryptography is used in everyday life!!!

A better alternative - **Post Quantum Cryptography**

Post Quantum Cryptography

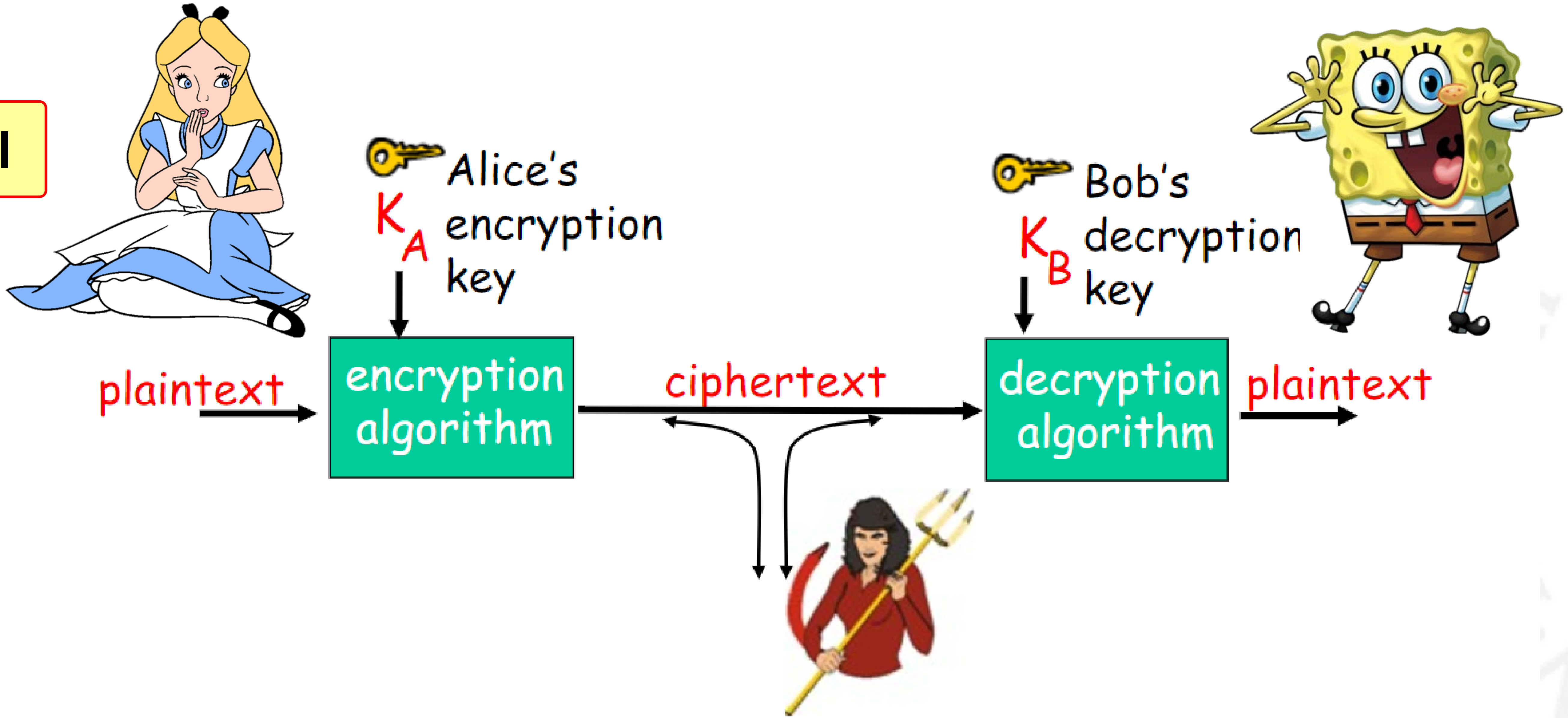


Post Quantum Cryptography



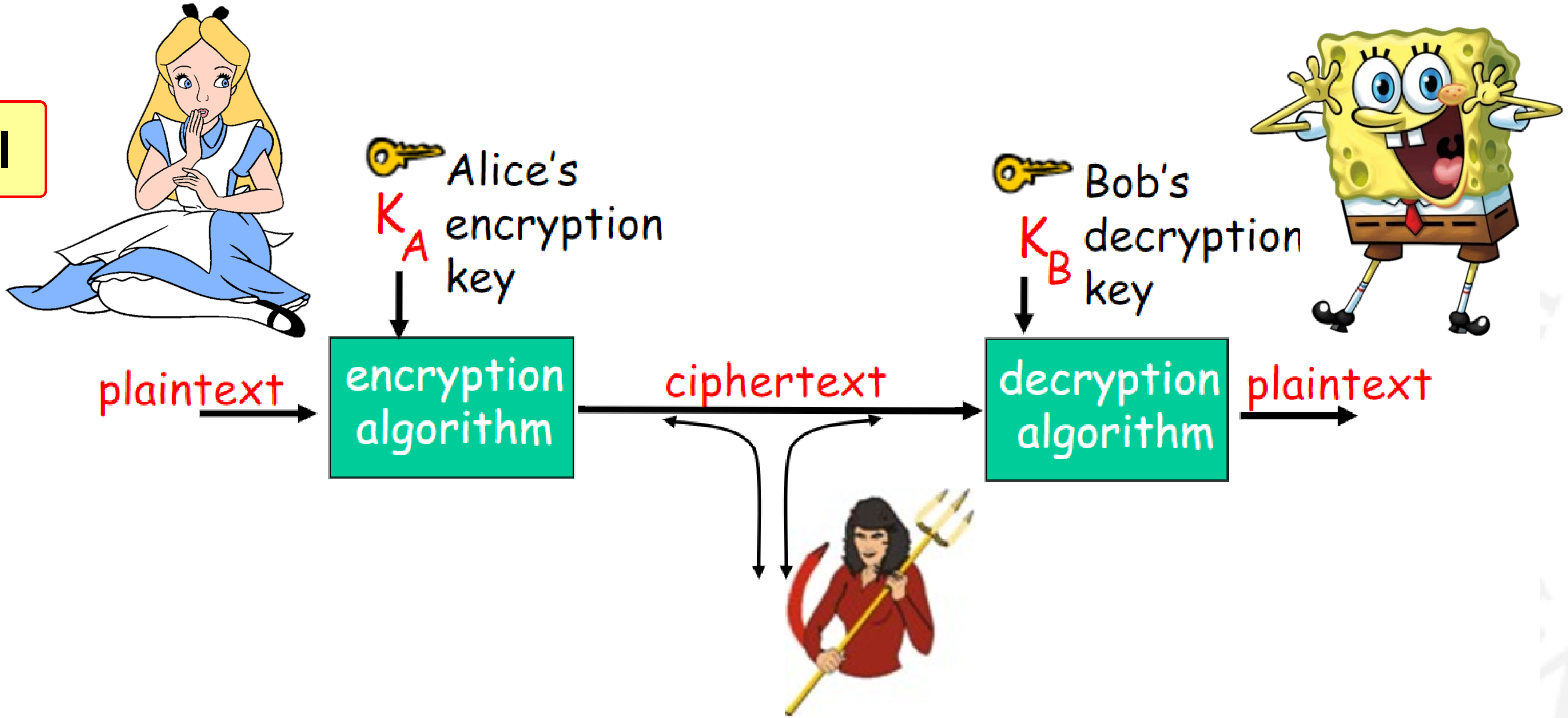
Post Quantum Cryptography

Classical



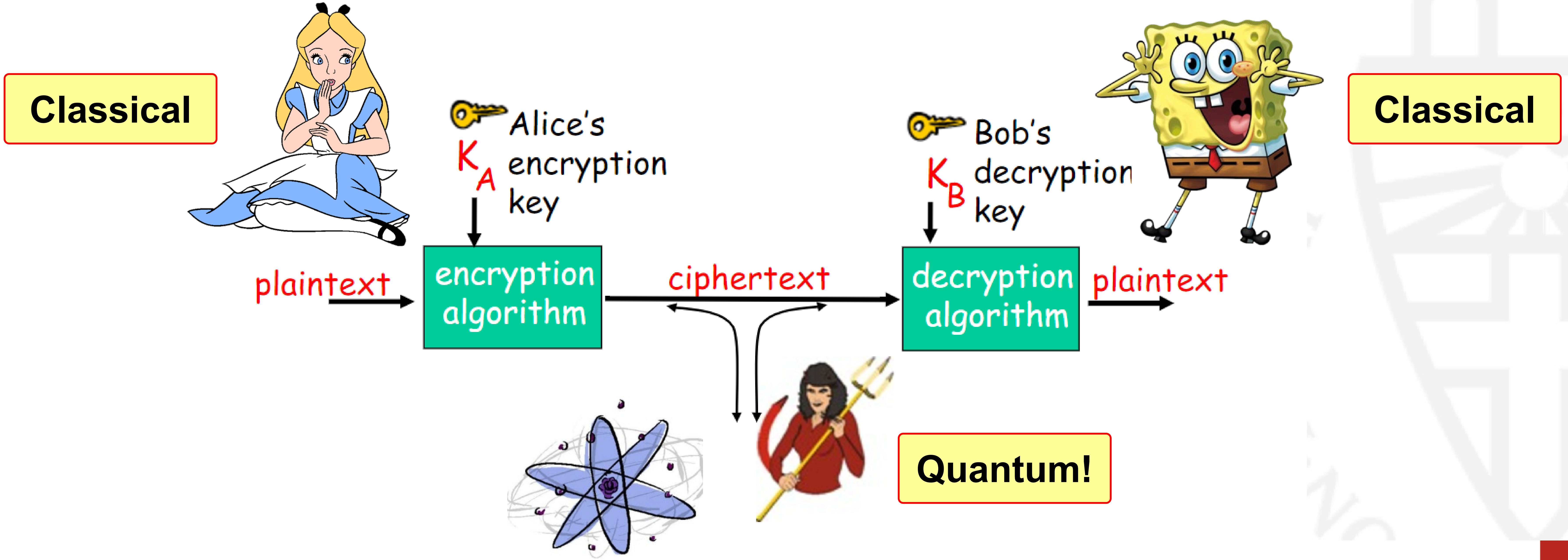
Post Quantum Cryptography

Classical



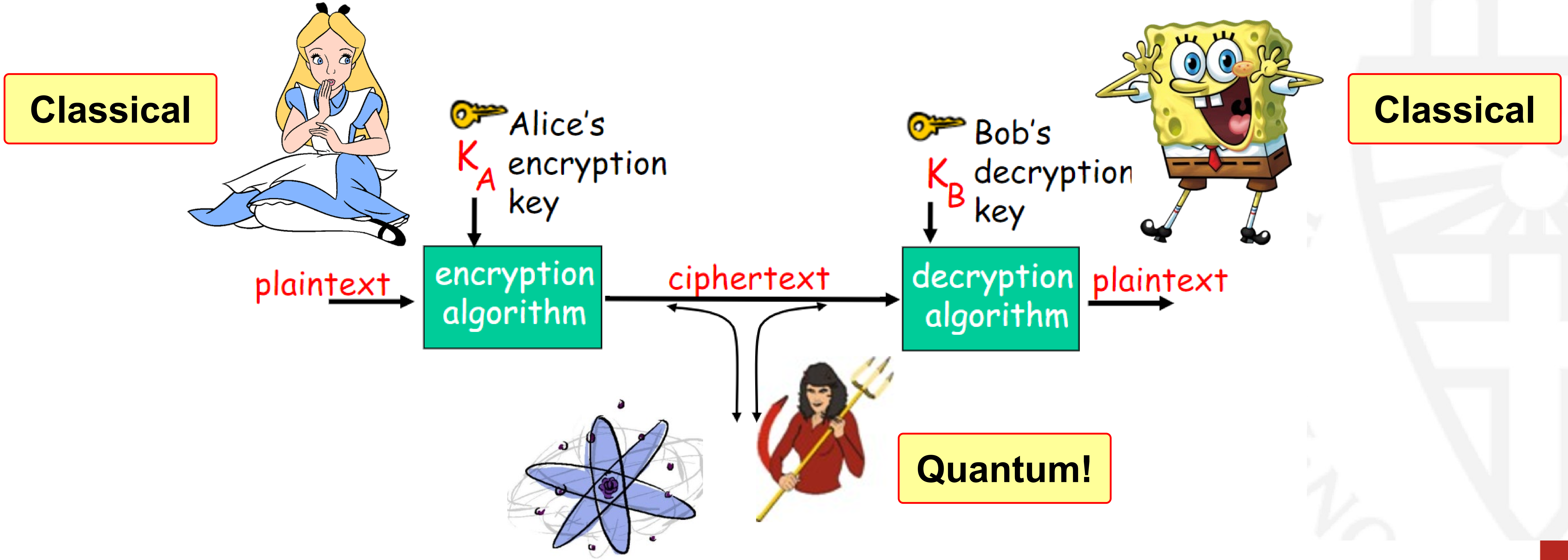
Classical

Post Quantum Cryptography



Post Quantum Cryptography

Classical Cryptosystems believed to be secure against quantum computer attacks



Post Quantum Cryptography

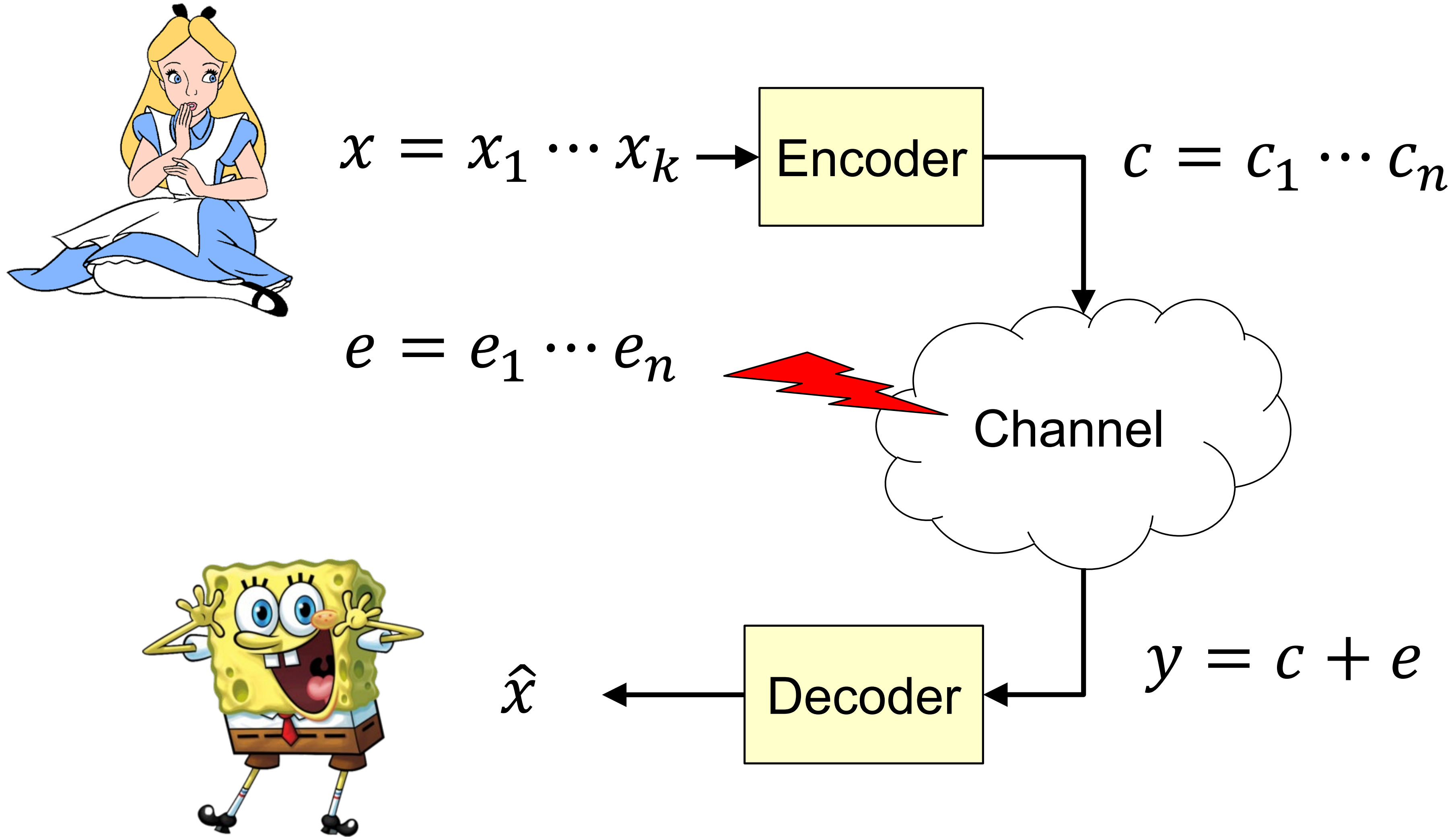
Cryptosystems believed to be secure against quantum computer attacks

- ***Code-based systems***
- ***Multivariate Quadratic systems***
- ***Lattice-based systems***
- ***Hash-based systems***
- ***Isogeny based systems***

Code-based Cryptosystems

McEliece '78! **As old as RSA!**

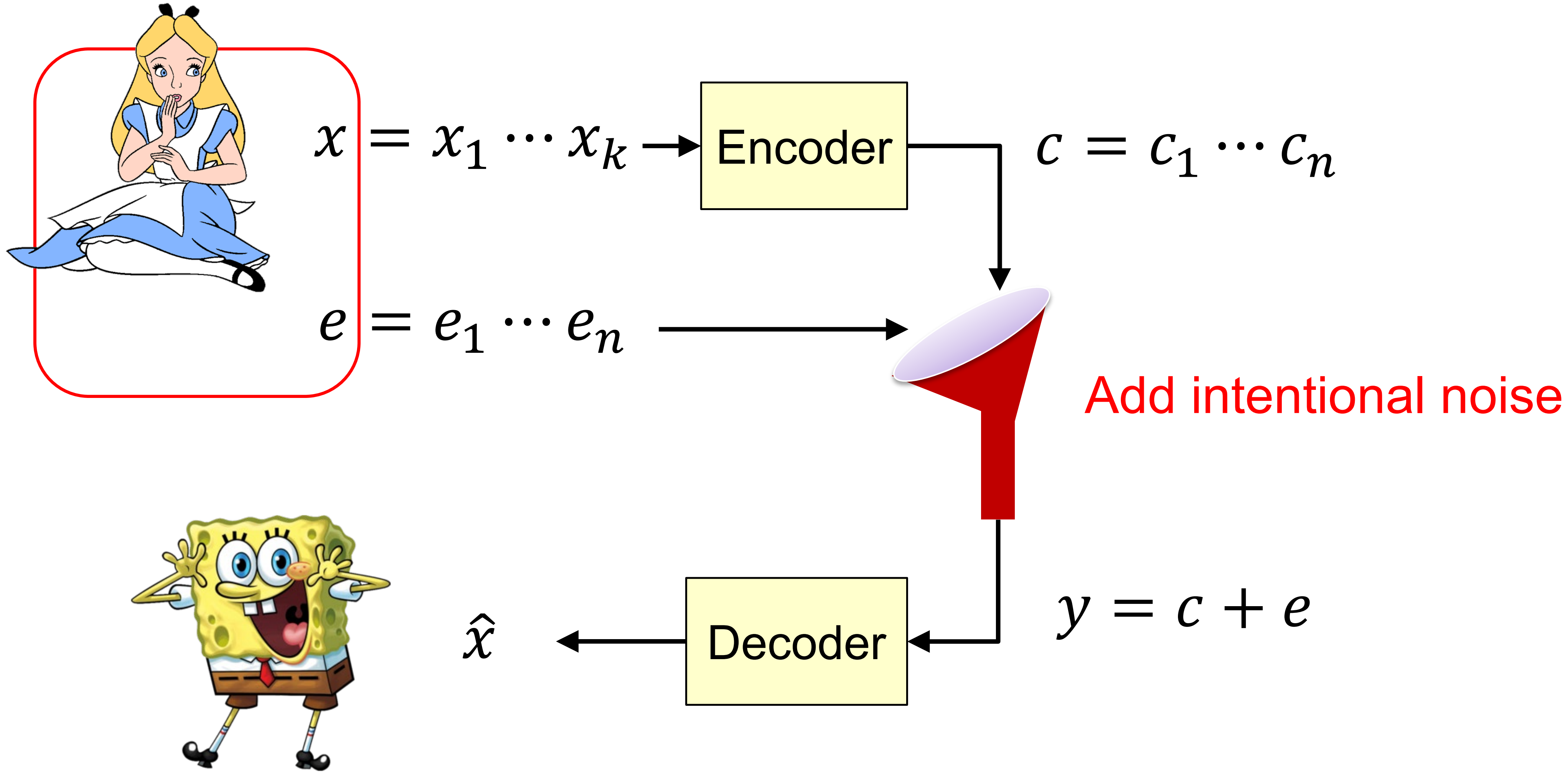
- Noisy channel communication:



Code-based Cryptosystems

McEliece ’78! **As old as RSA!**

- In cryptography:

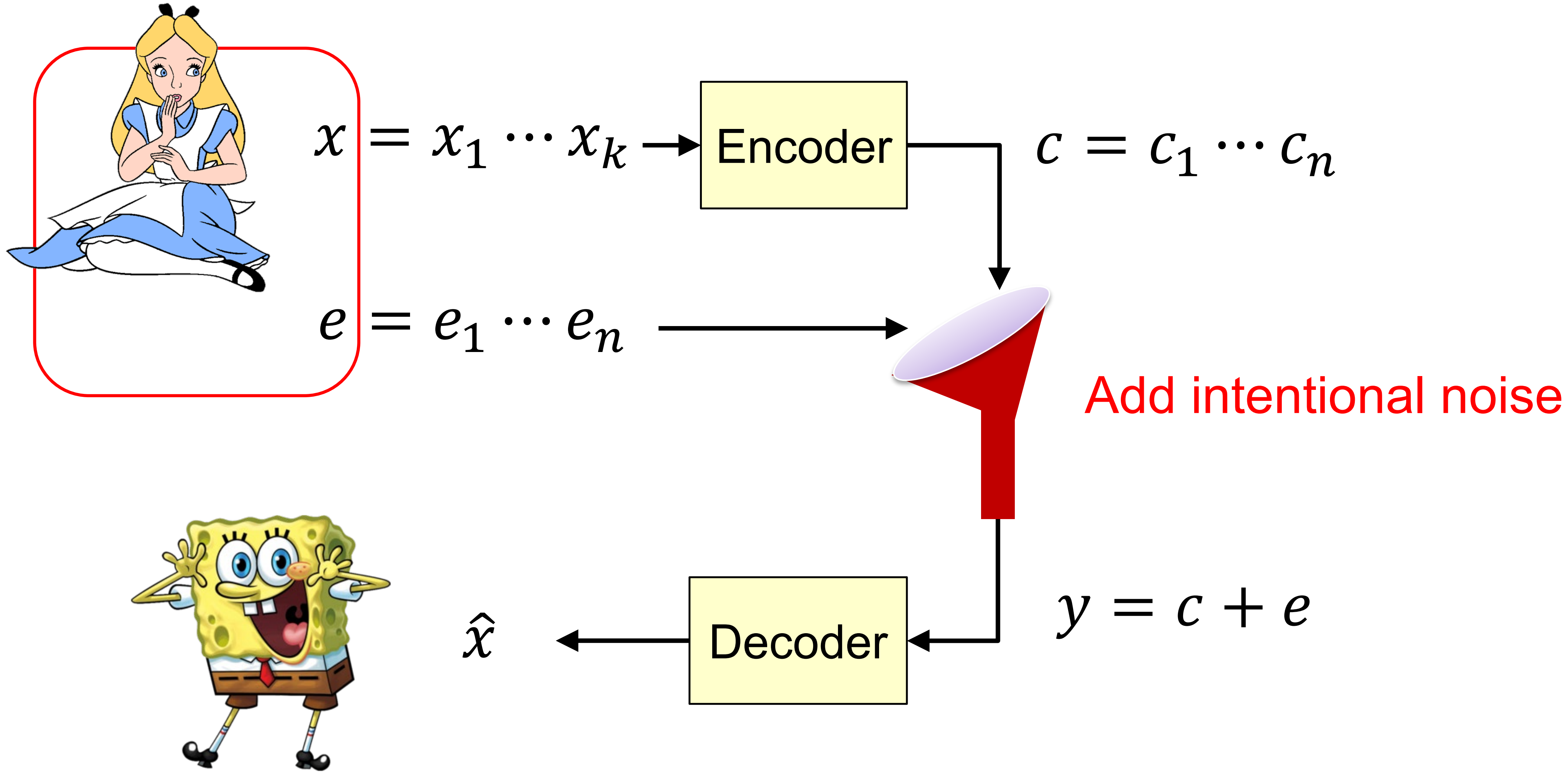


Code-based Cryptosystems

- Hard underlying problem (NP hard): Decoding random linear codes

  Given $mG + e$ find m

- Confidence in encryption schemes

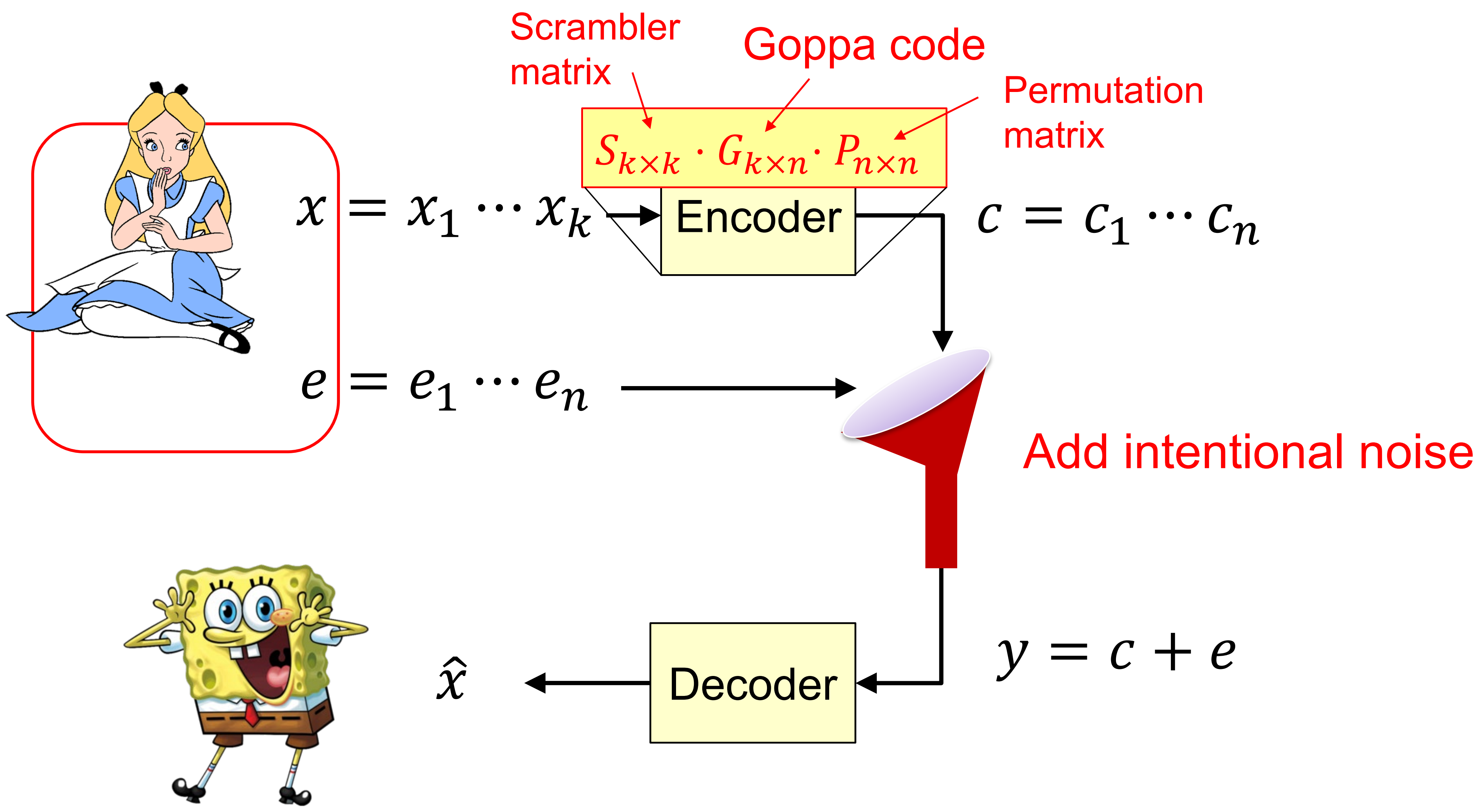


Code-based Cryptosystems

- Hard underlying problem (NP hard): Decoding random linear codes

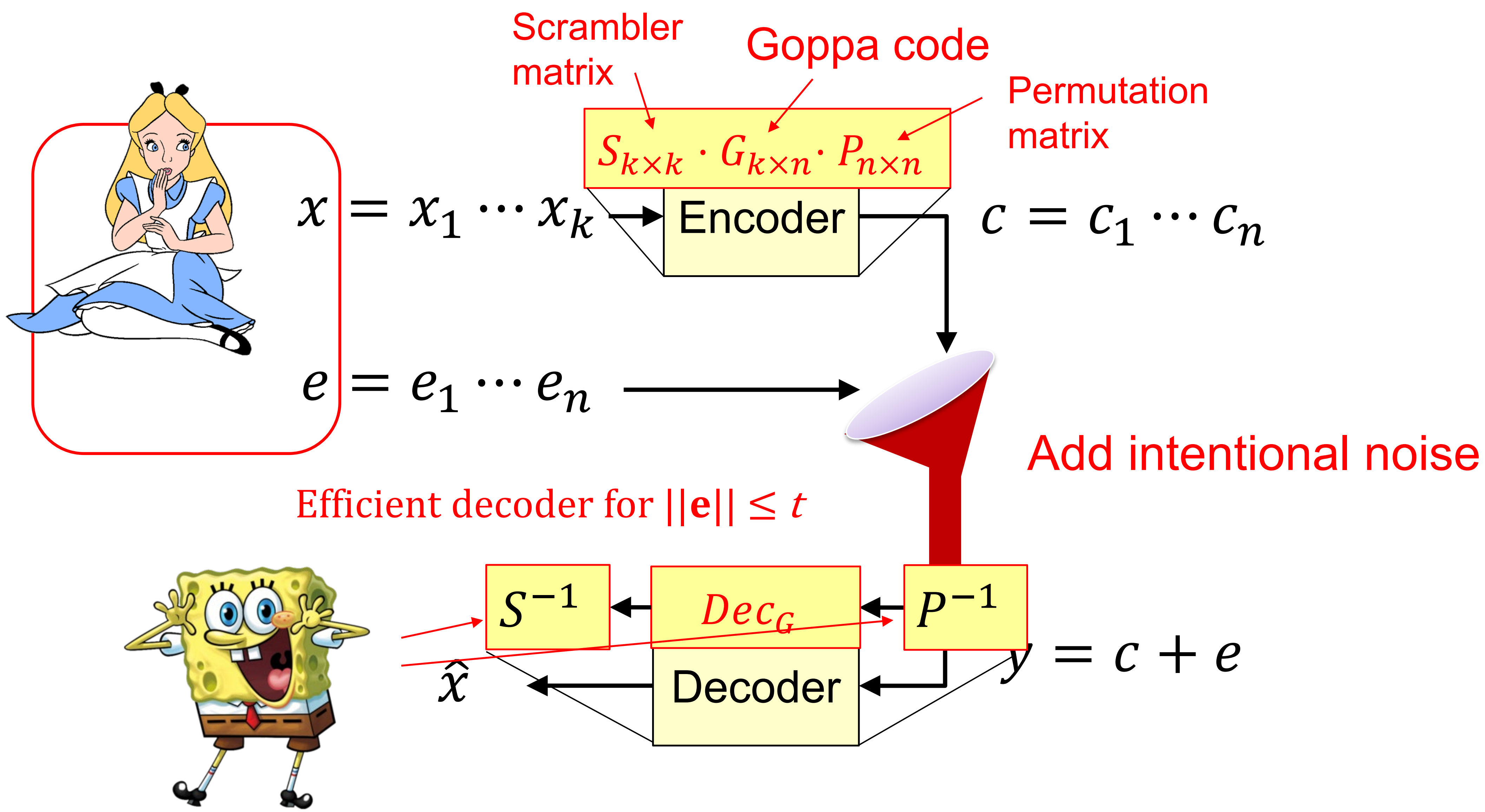
  Given $mG + e$ find m

- Confidence in encryption schemes



Code-based Cryptosystems

- Hard underlying problem (NP hard): Decoding random linear codes
  Given $mG + e$ find m
- Confidence in encryption schemes



Multivariate Quadratic systems

- Hard underlying problem (NP hard): Solving systems of quadratics (MQ problem)
- Signatures

Multivariate Quadratic systems

- Hard underlying problem (NP hard): Solving systems of quadratics (MQ problem)
- Signatures

Lattice-based systems

- Many different hard problems (SVP, Learning with errors (LWE, Ring-LWE, LPN))
- Encryption, signatures, key agreement

Multivariate Quadratic systems

- Hard underlying problem (NP hard): Solving systems of quadratics (MQ problem)
- Signatures

Lattice-based systems

- Many different hard problems (SVP, Learning with errors (LWE, Ring-LWE, LPN))
- Encryption, signatures, key agreement

Hash-based systems

- Merkle, 89
- **Only secure hash function needed** (security well understood)
- Most trusted post quantum signatures

Multivariate Quadratic systems

- Hard underlying problem (NP hard): Solving systems of quadratics (MQ problem)
- Signatures

Lattice-based systems

- Many different hard problems (SVP, Learning with errors (LWE, Ring-LWE, LPN))
- Encryption, signatures, key agreement

Hash-based systems

- Merkle, 89
- **Only secure hash function needed** (security well understood)
- Most trusted post quantum signatures

Isogeny based systems

- Hard underlying problem: Finding isogenies on supersingular elliptic curves
- Very new area
- Key agreement

Multivariate Quadratic systems

- Hard underlying problem (NP hard): Solving systems of quadratics (MQ problem)
- Signatures

Lattice-based systems

- Many different hard problems (SVP, Learning with errors (LWE, Ring-LWE, LPN))
- Encryption, signatures, key agreement

Hash-based systems

- Merkle, 89
- **Only secure hash function needed** (security well understood)
- Most trusted post quantum signatures

Isogeny based systems

- Hard underlying problem: Finding isogenies on supersingular elliptic curves
- Very new area
- Key agreement

Challenges in Post Quantum Cryptography

- **Security models**
  - What are the exact capabilities of quantum adversaries?
- **Security proofs**
  - Many classical techniques don't work in the quantum world
- **Security of hard problems**
  - Quantum algorithms for the hard problems?
  - Ex. Smart use of Grover, dedicated algorithms
  - Number of qubits for the algorithms?

Challenges in Post Quantum Cryptography

- **Key sizes, signature sizes and speed**
  - Huge public keys, or signatures …. Or slow
  - ex. ECC 256b key vs McElliece 500KB key
  - ex. ECC 80B signature vs MQDSS 40KB signature

- **Software and hardware implementation**
  - Optimizations, physical security

- **Standardization**
  - What is the right choice of algorithm?

- **Deployment**
  - In TLS, smart cards, storage…
  - Will take a long time…

POST-QUANTUM CRYPTO STANDARDIZATION

Call For Proposals Announcement

The National Institute of Standards and Technology (NIST) has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Currently, public-key cryptographic algorithms are specified in FIPS 186-4, Digital Signature Standard, as well as special publications SP 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography and SP 800-56B Revision 1, Recommendation for Pair-Wises Key-Establishment Schemes Using Integer Factorization Cryptography. However, these algorithms are vulnerable to attacks from large-scale quantum computers (see NISTIR 8105 Report on Post Quantum Cryptography). It is intended that the new public-key cryptography standards will specify one or more additional unclassified, publicly disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide, and are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.

NIST National Institute of Standards and Technology
Information Technology Laboratory

SEARCH: Search

CONTACT SITE MAP

Computer Security Division
Computer Security Resource Center

CSRC Home | About | Projects / Research | Publications | News & Events

CSRC HOME > GROUPS > CT > POST-QUANTUM CRYPTOGRAPHY PROJECT

POST-QUANTUM CRYPTO STANDARDIZATION

Call For Proposals Announcement

The National Institute of Standards and Technology (NIST) has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Currently, public-key cryptographic algorithms are specified in FIPS 186-4, Digital Signature Standard, as well as special publications SP 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography and SP 800-56B Revision 1, Recommendation for Pair-Wises Key-Establishment Schemes Using Integer Factorization Cryptography. However, these algorithms are vulnerable to attacks from large-scale quantum computers (see NISTIR 8105 Report on Post Quantum Cryptography). It is intended that the new public-key cryptography standards will specify one or more additional unclassified, publicly disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide, and are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.

- Call for Proposals
- Submission Requirements
- Minimum Acceptability Requirements

Timeline

- Fall 2016 – formal Call For Proposals
- Nov 2017 – Deadline for submissions
- 3–5 years – Analysis phase
  - NIST will report its findings
- 2 years later – Draft standards ready

NIST National Institute of Standards and Technology
Information Technology Laboratory

SEARCH: Search

CONTACT SITE MAP

Computer Security Division
Computer Security Resource Center

CSRC Home | About | Projects / Research | Publications | News & Events

CSRC HOME > GROUPS > CT > POST-QUANTUM CRYPTOGRAPHY PROJECT

Timeline

- Fall 2016 – formal Call For Proposals
- Nov 2017 – Deadline for submissions
- 3-5 years – Analysis phase
  - NIST will report its findings
- 2 years later – Draft standards ready

- NOT a competition
- 82 submissions, 69 "complete and proper"
- 20 signatures
- 49 Key encapsulation mechanisms
- Around 10 broken
- **Radboud involved in 8 !**

Call for Proposals
Submission Requirements
Minimum Acceptability Requirements

government information well into the foreseeable future, including after the advent of quantum computers.

Digital Security Group – Radboud University involved in 8 Post Quantum Crypto candidates

KEMs

- Classic McEliece
  - Code-based

Lattice based
- CRYSTALS-KYBER
- NTRU-HRSS-KEM
- New Hope
  - Implemented and tested by Google

- SIKE
  - Isogeny-based

Signatures

- CRYSTALS-DILITHIUM
  - Lattice based

- SPHINCS+
  - Hash based
  - Provably secure from minimal assumptions

- MQDSS
  - First provably secure MQ signature

MQDSS

- [Chen, Hülsing, Rijneveld, S, Schwabe, 16]
- NIST candidate
- **First provably secure signature scheme**
- Hard problem: Solving systems of quadratic equations (MQ problem)

Input: Quadratic polynomials

$p_1, p_2, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$

Question:

Solve the system of equations

$$\begin{cases} p_1(u_1, \ldots, u_n) = & 0 \\ p_2(u_1, \ldots, u_n) = & 0 \\ \quad \cdots & \\ p_m(u_1, \ldots, u_n) = & 0 \end{cases}$$

Some final words

If computers that you build are quantum,
Then spies everywhere will all want 'em.
Our codes will all fail,
And they'll read our email,
Till we get crypto that's quantum,
and daunt 'em.
Jennifer and Peter Shor

To read our E-mail, how mean
of the spies and their quantum machine;
be comforted though,
they do not yet know
how to factorize twelve or fifteen.
Volker Strassen

Thank you for listening!

?

MQDSS

IDS

$\mathcal{P}$		$\mathcal{V}$
$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}_1}$	$\mathsf{ch}_1 \leftarrow_R \mathsf{ChS}_1(1^k)$
$\mathsf{resp}_1 \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1)$	$\xrightarrow{\mathsf{resp}_1}$	
	$\xleftarrow{\mathsf{ch}_2}$	$\mathsf{ch}_2 \leftarrow_R \mathsf{ChS}_2(1^k)$
$\mathsf{resp}_2 \leftarrow \mathcal{P}_2(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2)$	$\xrightarrow{\mathsf{resp}_2}$	
		$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$

$\downarrow \quad \downarrow \quad \downarrow$

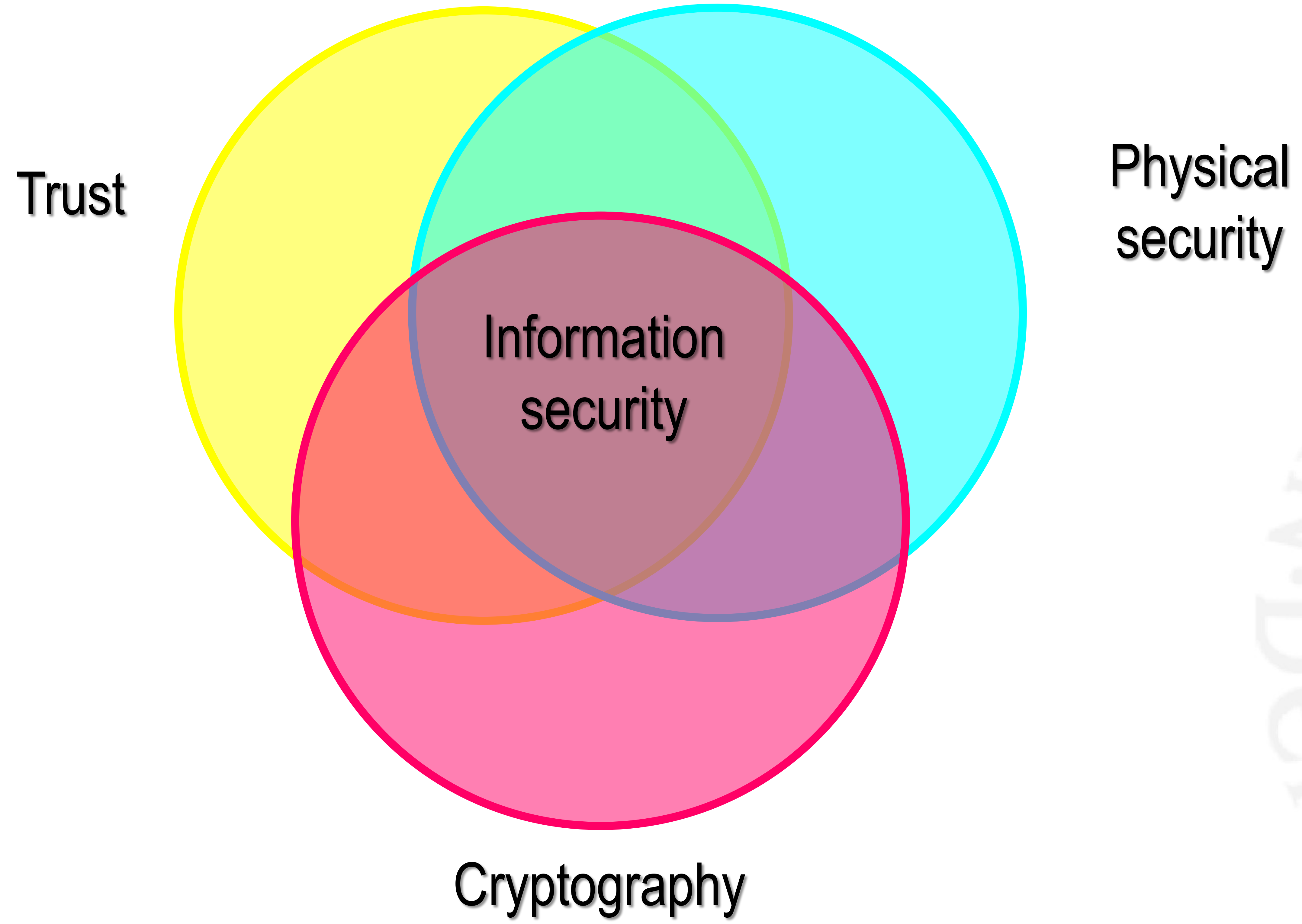
FS signature

Signer	**Verifier**
$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$	
$\mathsf{ch}_1 \leftarrow H_1(m, \mathsf{com})$	$\mathsf{ch}_1 \leftarrow H_1(m, \mathsf{com})$
$\mathsf{resp}_1 \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1)$	$\mathsf{ch}_2 \leftarrow H_2(m, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1)$
$\mathsf{ch}_2 \leftarrow H_2(m, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1)$	$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$
$\mathsf{resp}_2 \leftarrow \mathcal{P}_2(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2)$	
output : $\sigma = (\mathsf{com}, \mathsf{resp}_1, \mathsf{resp}_2)$	**output** : b

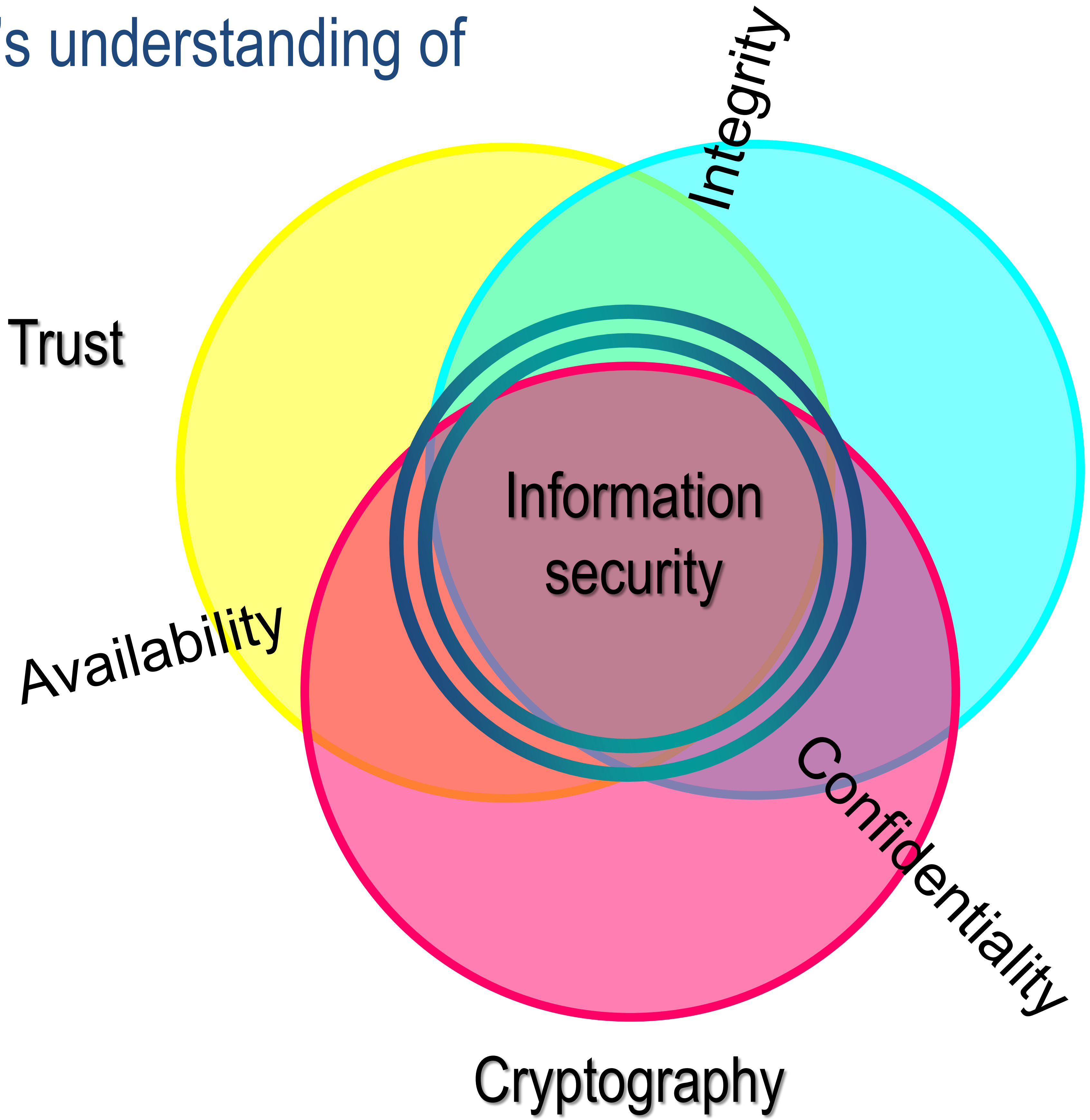
Today’s understanding of

Information
security

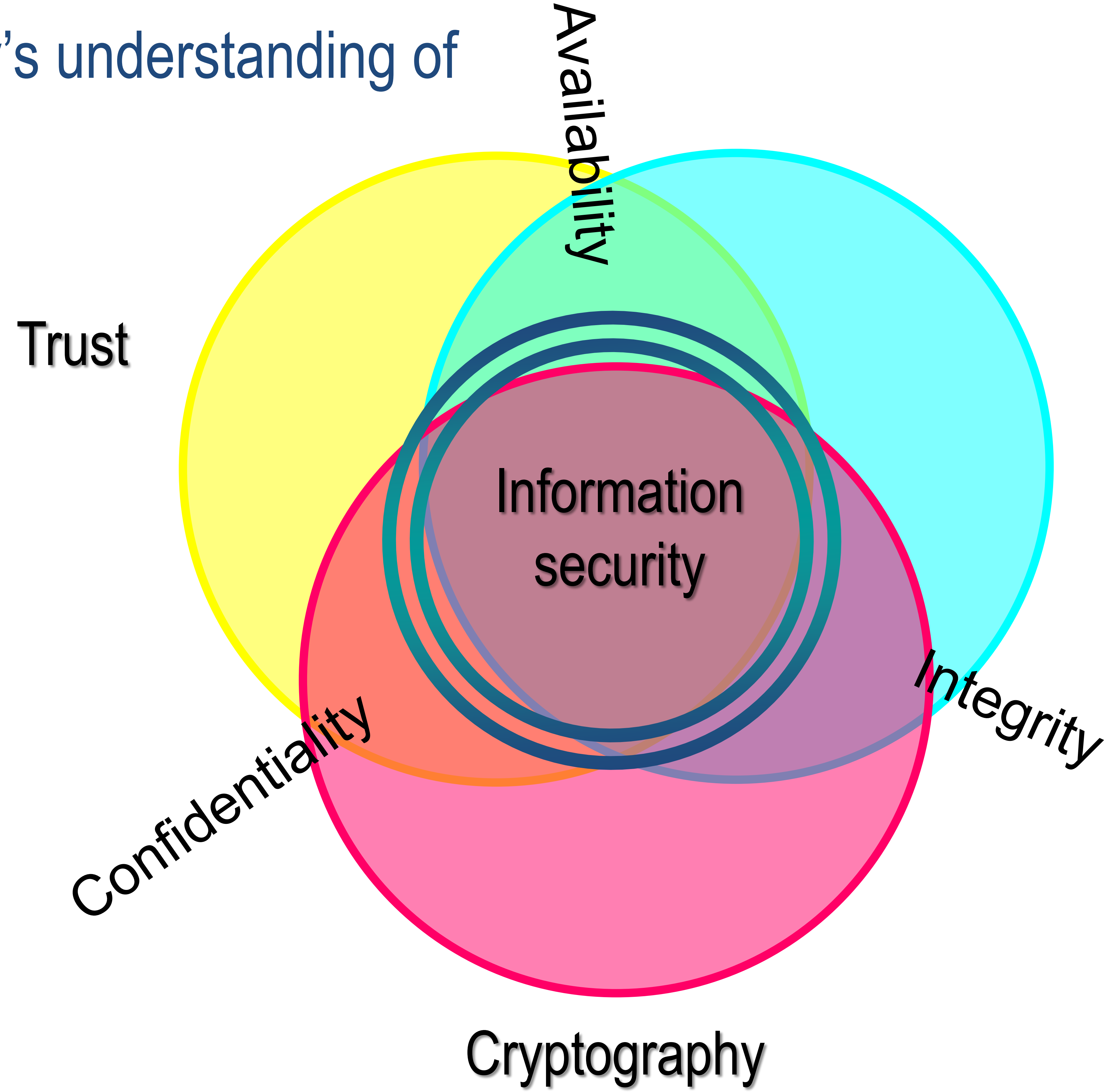
Today's understanding of



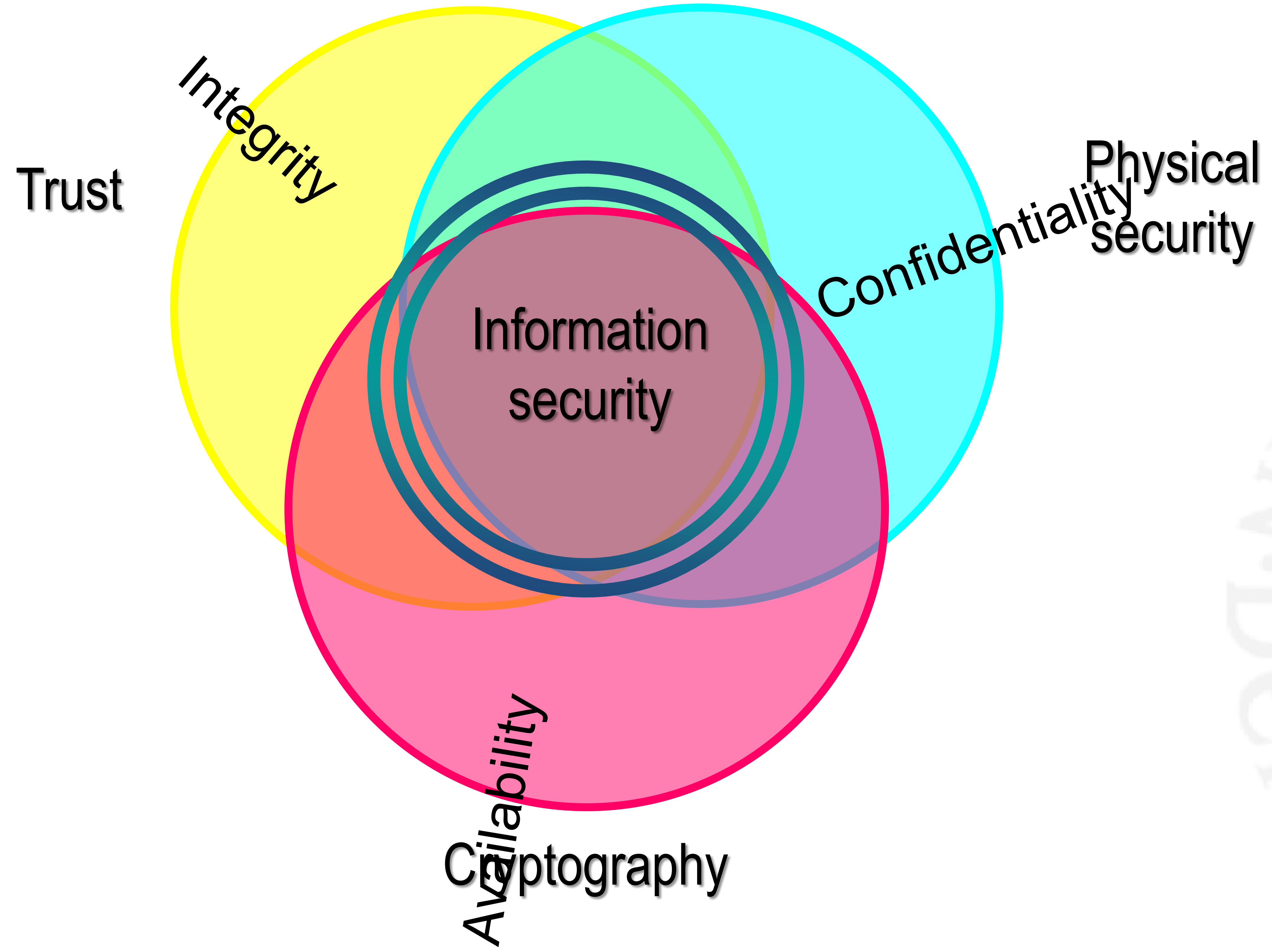
Today's understanding of



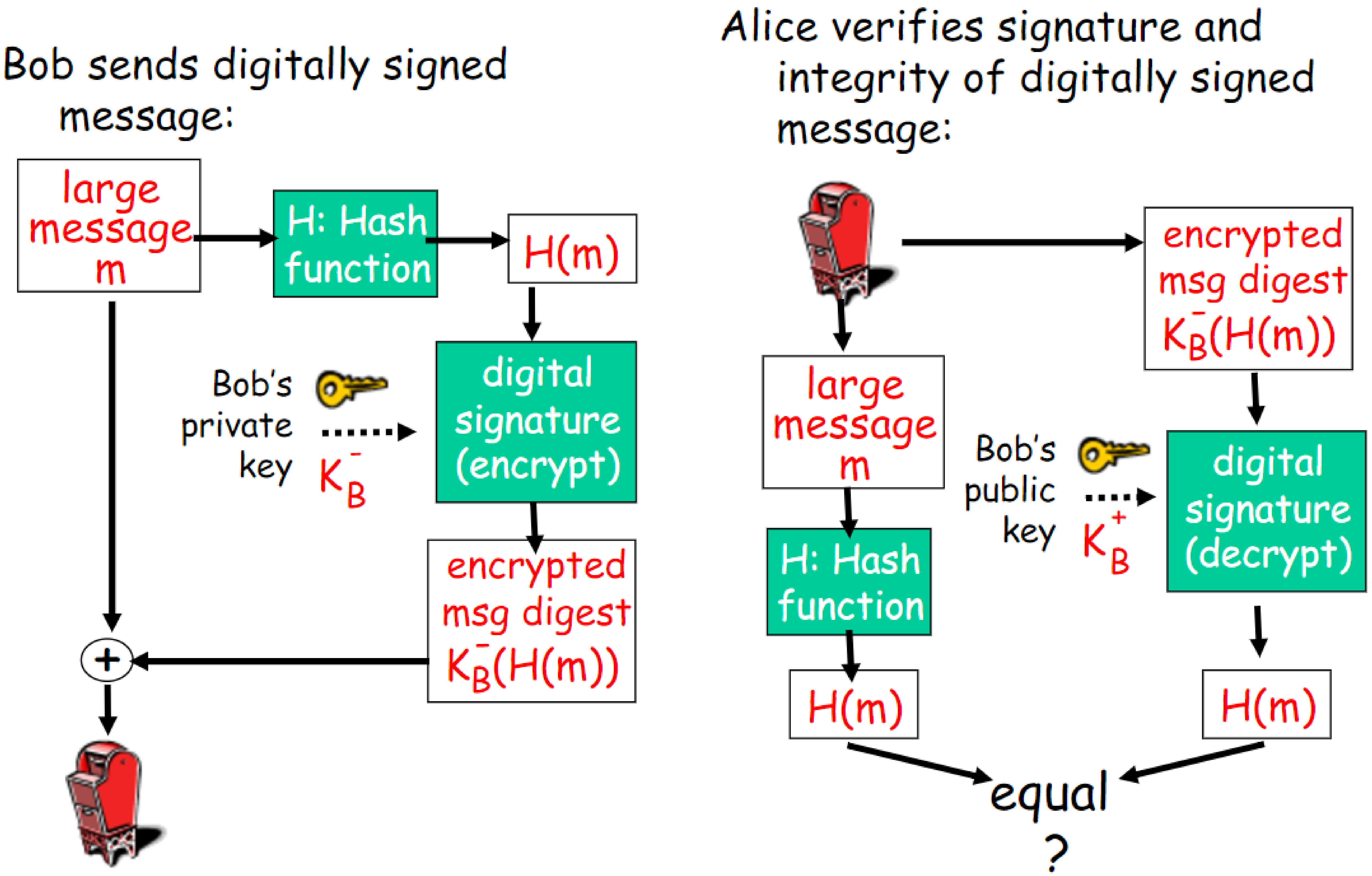
Today's understanding of



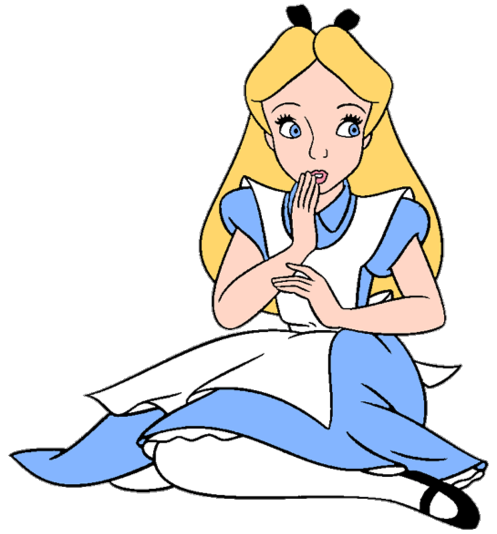
Today's understanding of



A Swiss army knife in cryptography – Digital signatures



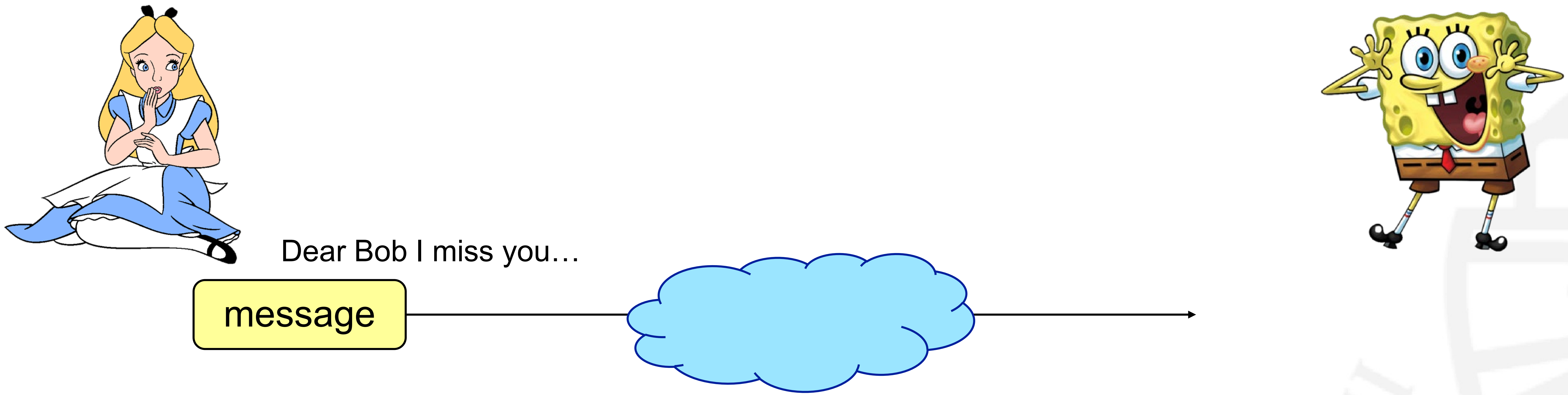
What is Authenticated Encryption (AE)?



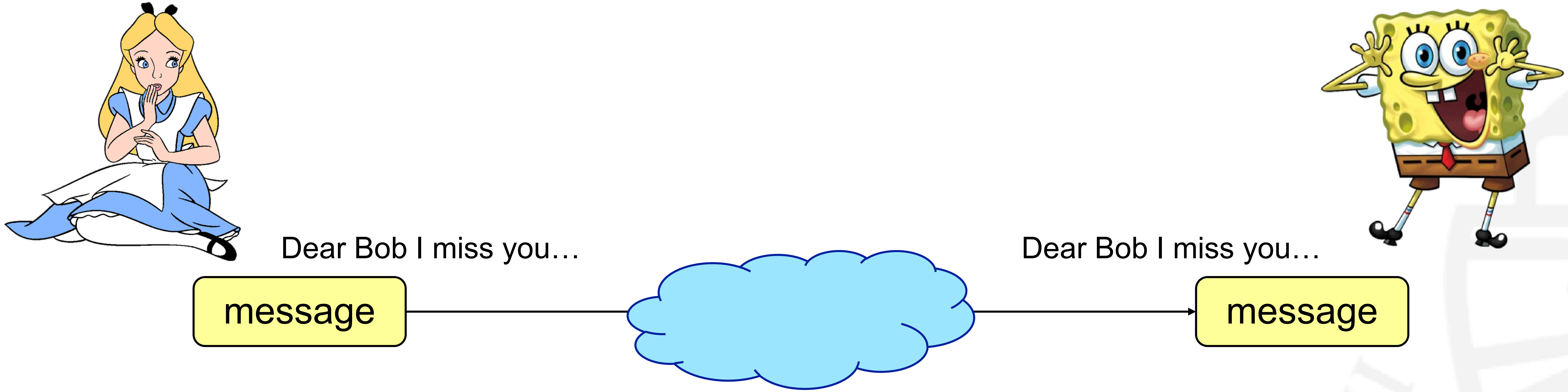
Dear Bob I miss you…

message

What is Authenticated Encryption (AE)?

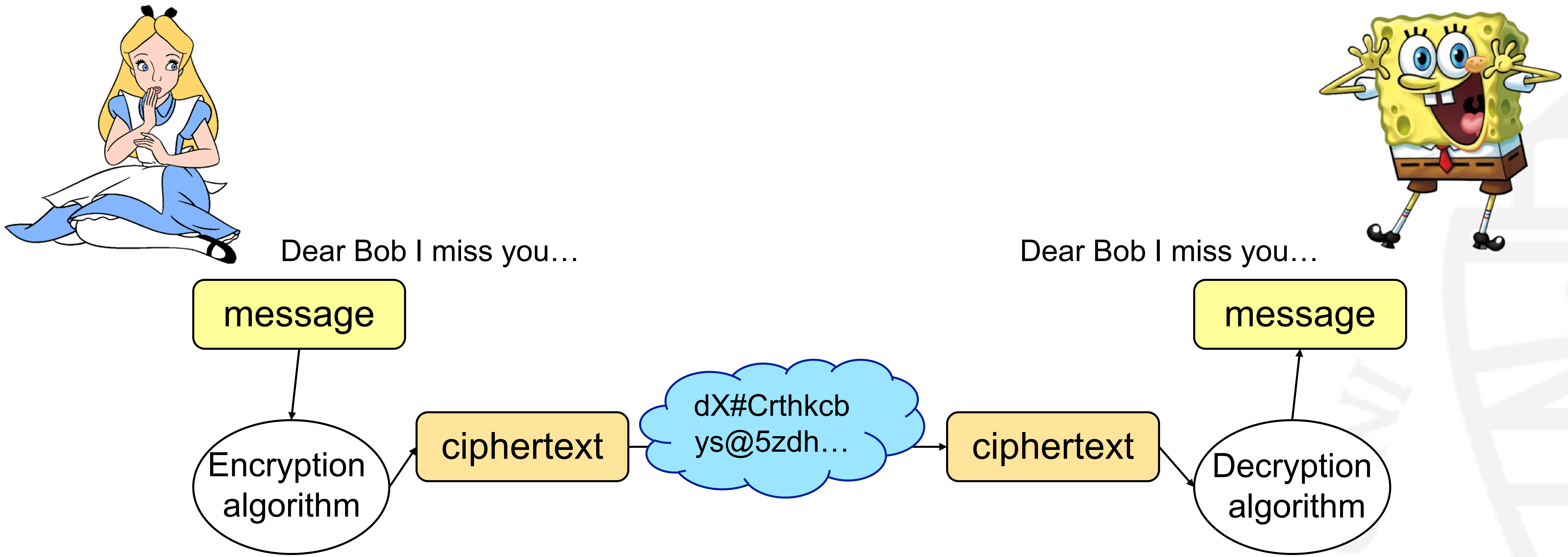


What is Authenticated Encryption (AE)?

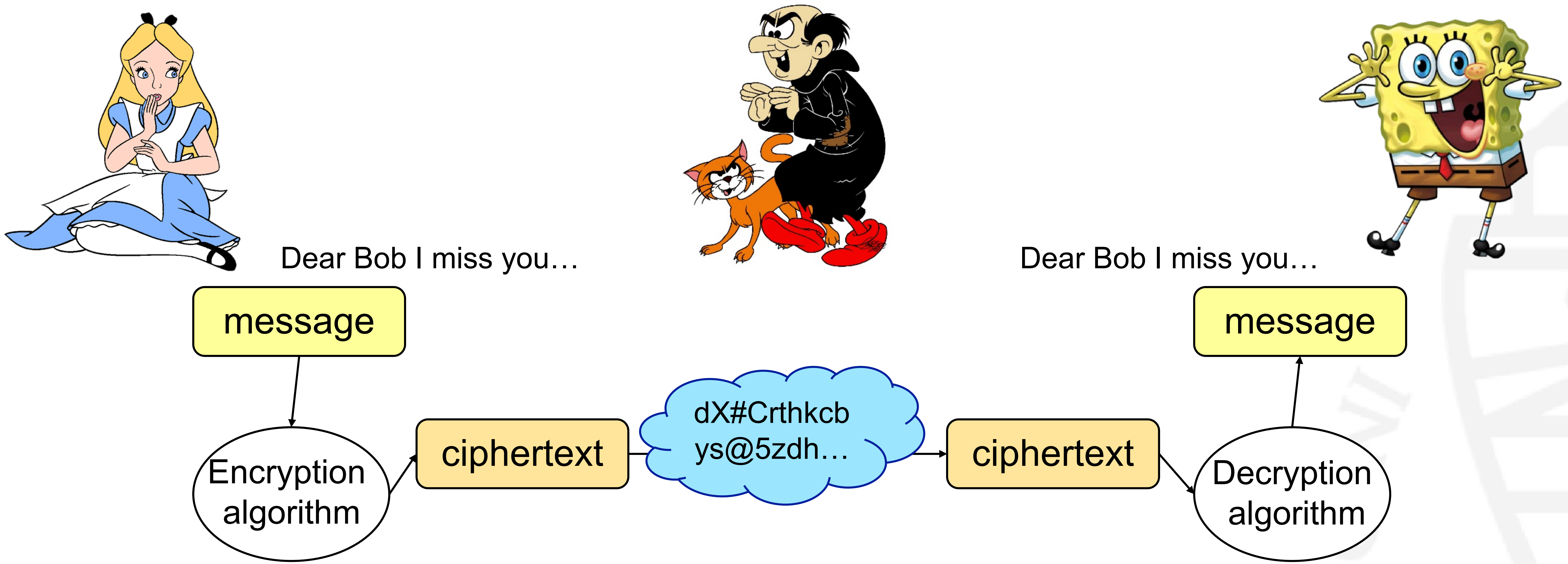


What is Authenticated Encryption (AE)?

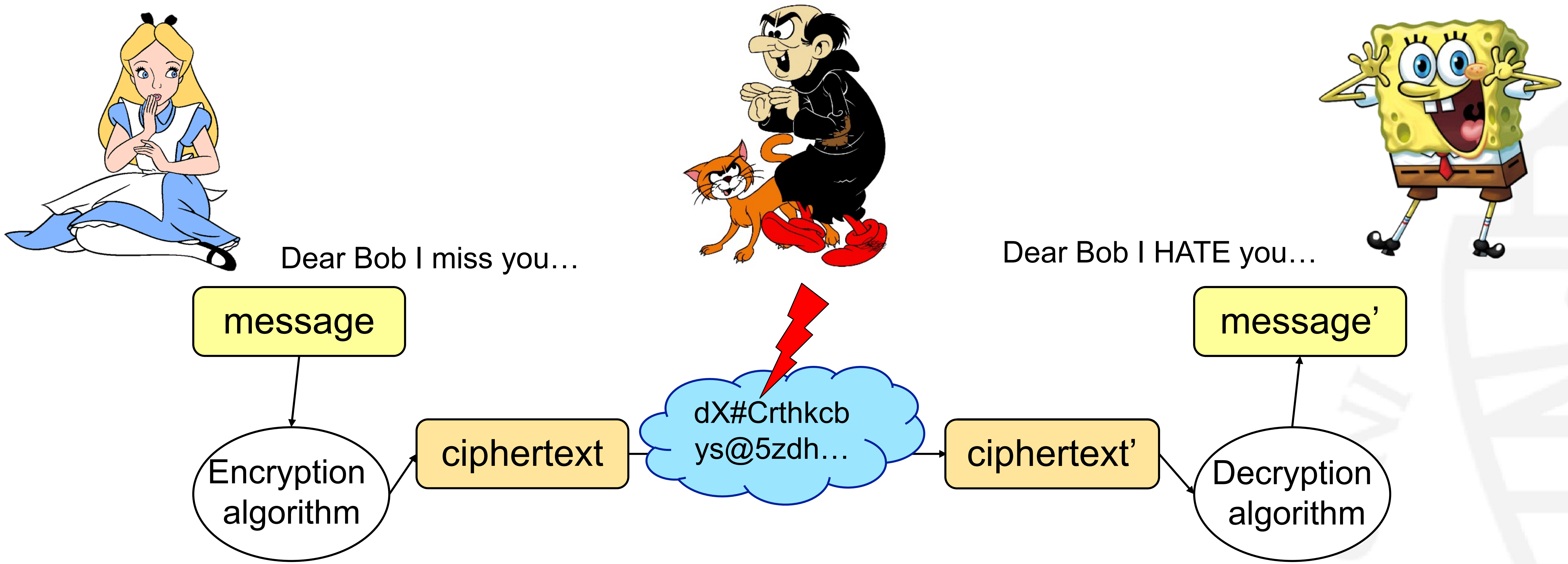
What is Authenticated Encryption (AE)?



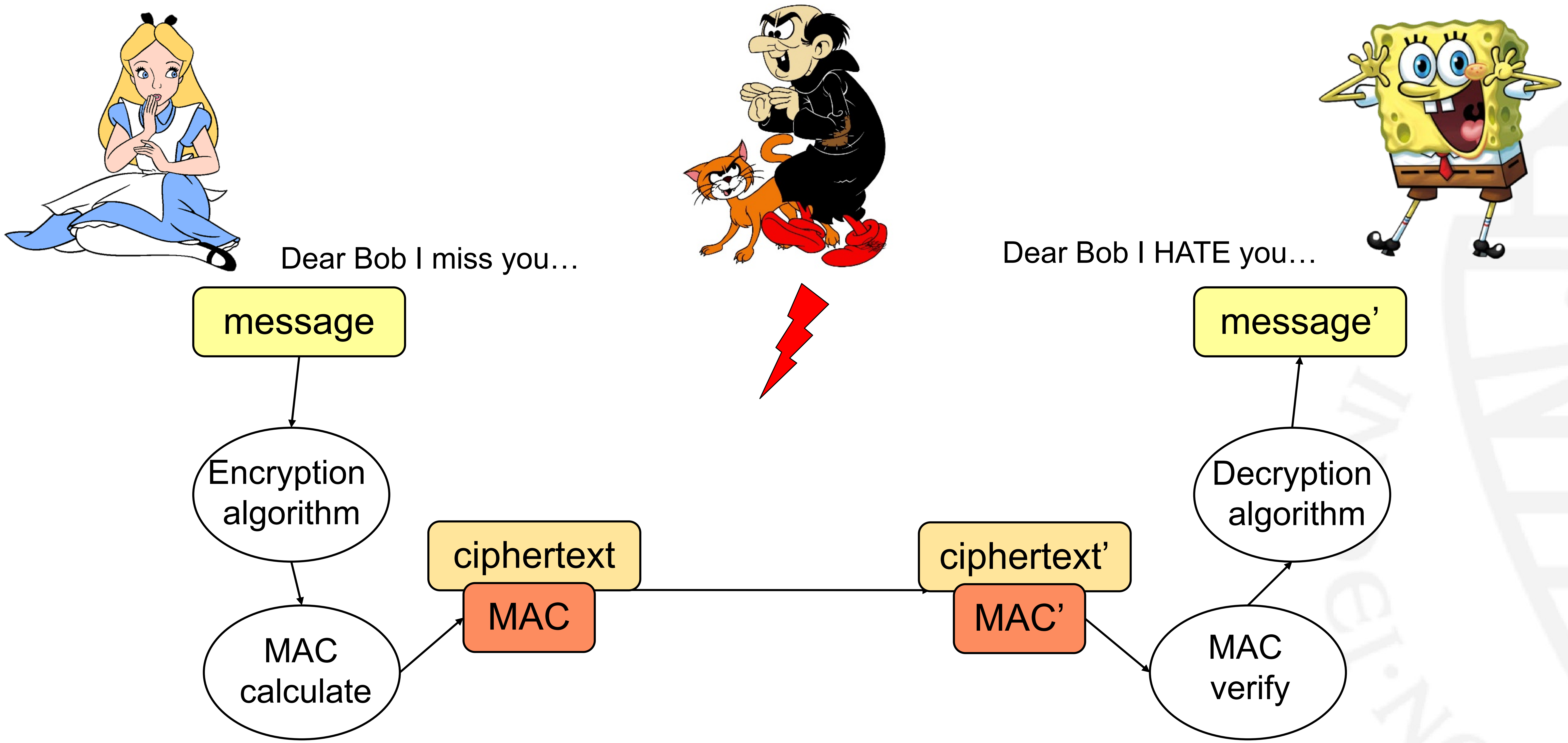
What is Authenticated Encryption (AE)?



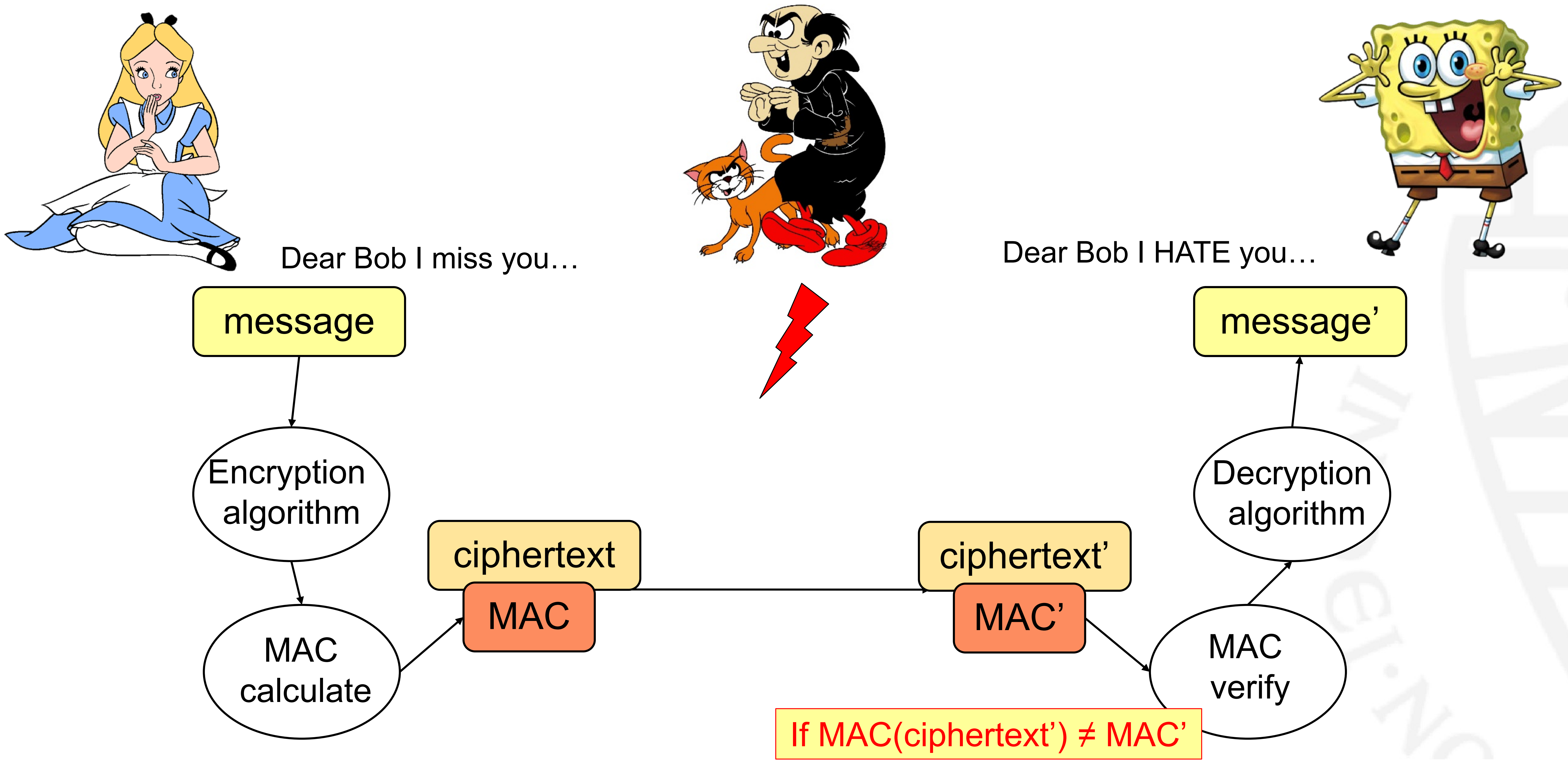
What is Authenticated Encryption (AE)?



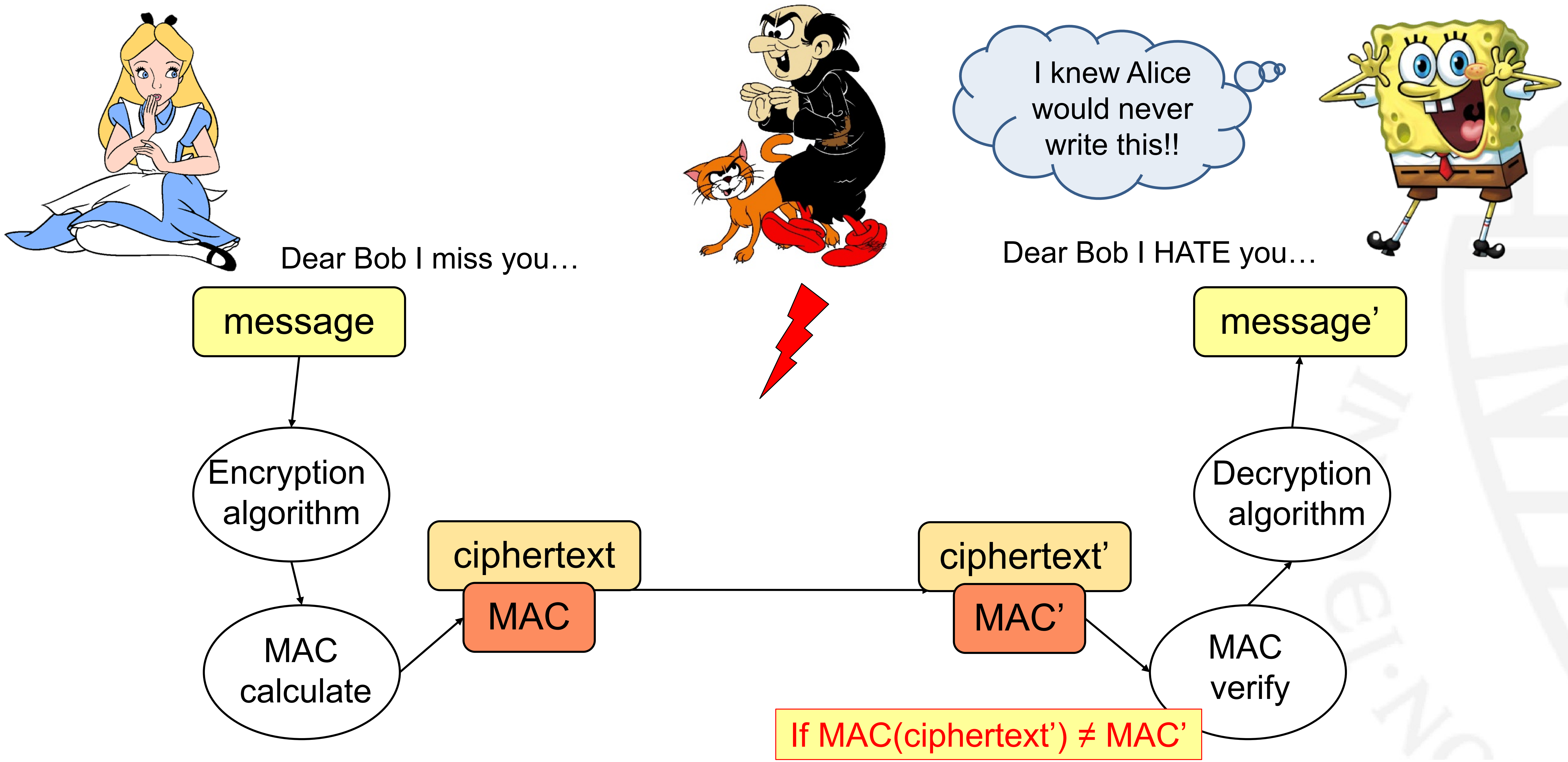
What is Authenticated Encryption (AE)?



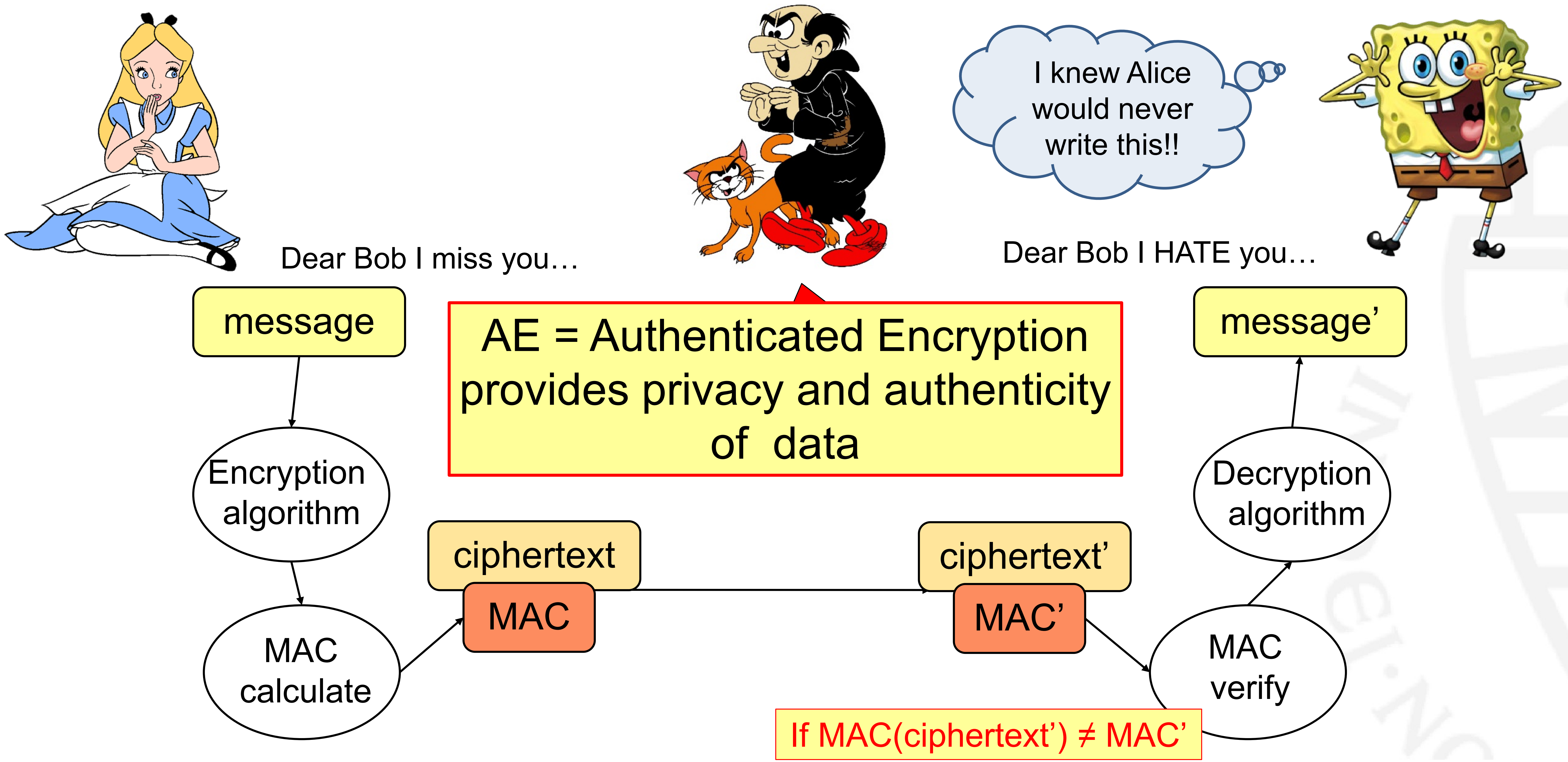
What is Authenticated Encryption (AE)?



What is Authenticated Encryption (AE)?



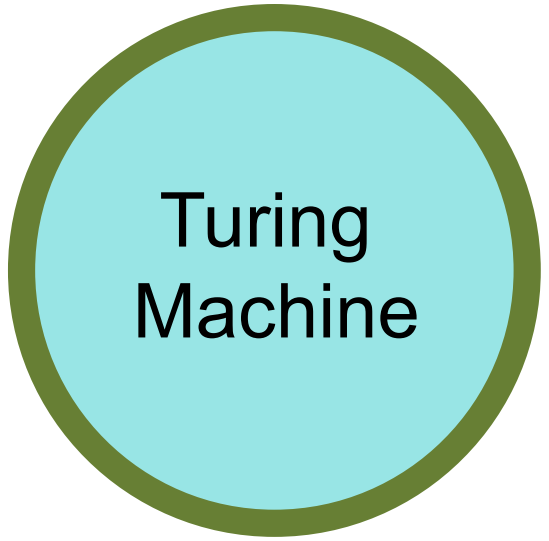
What is Authenticated Encryption (AE)?



The origins …

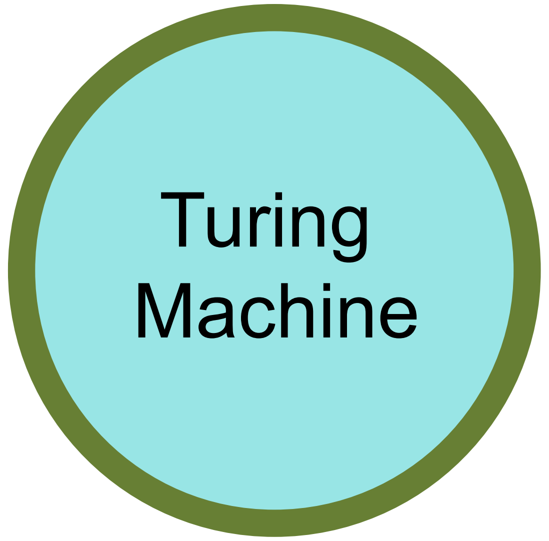
The origins …

Turing ’36



The origins …

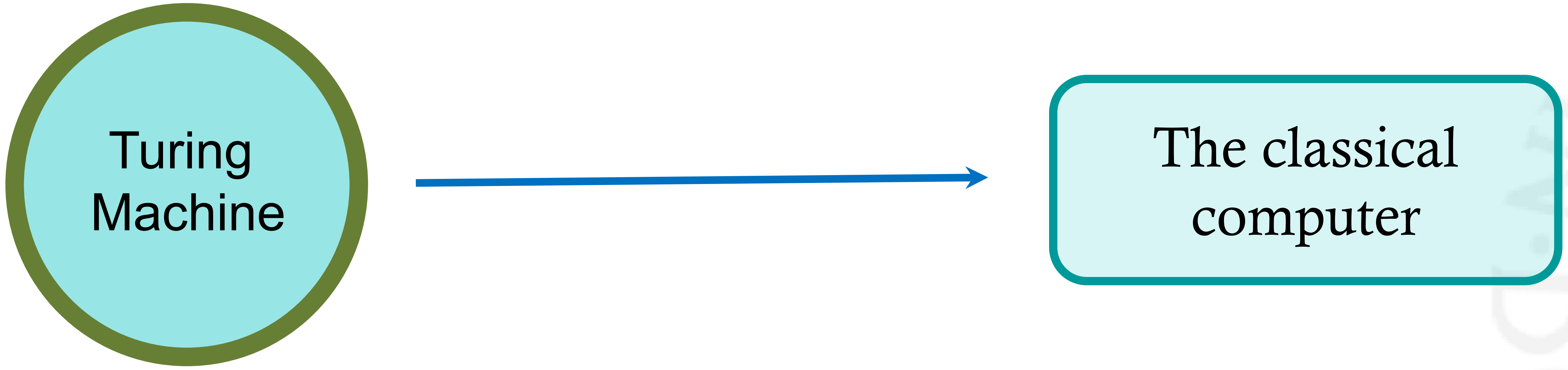
Turing ’36



Any algorithmic process can be simulated efficiently using a Turing machine

The origins …

Turing ’36

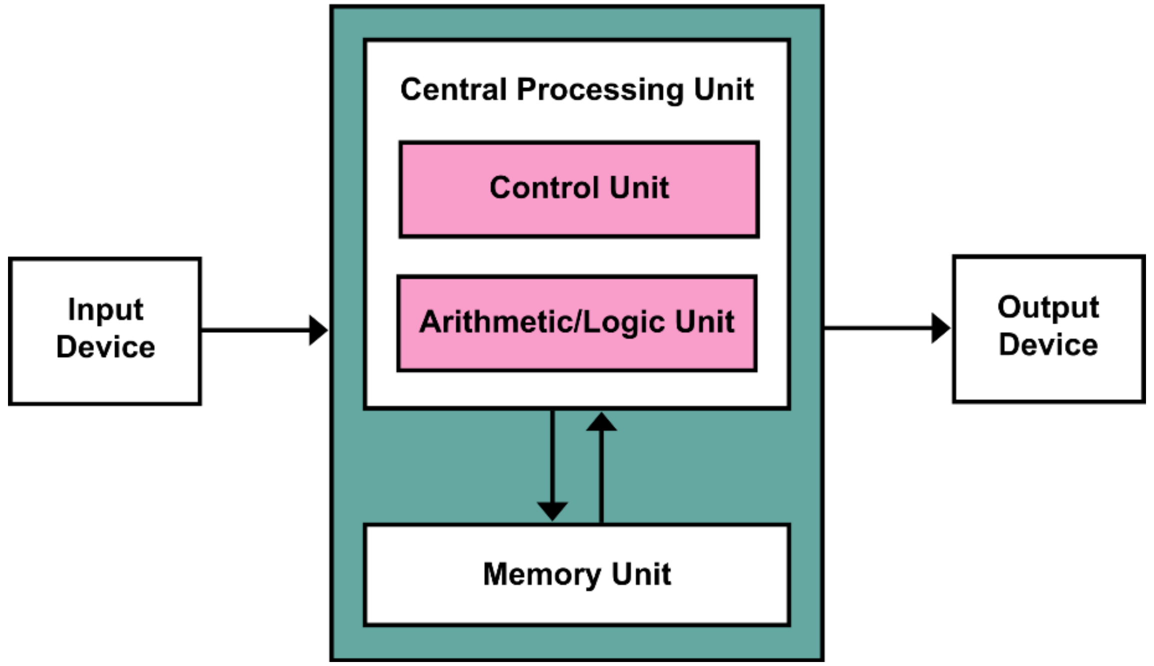


Any algorithmic process
can be simulated efficiently
using a Turing machine

The origins …

Theoretical model

von Neumann architecture



Turing '36

Turing Machine

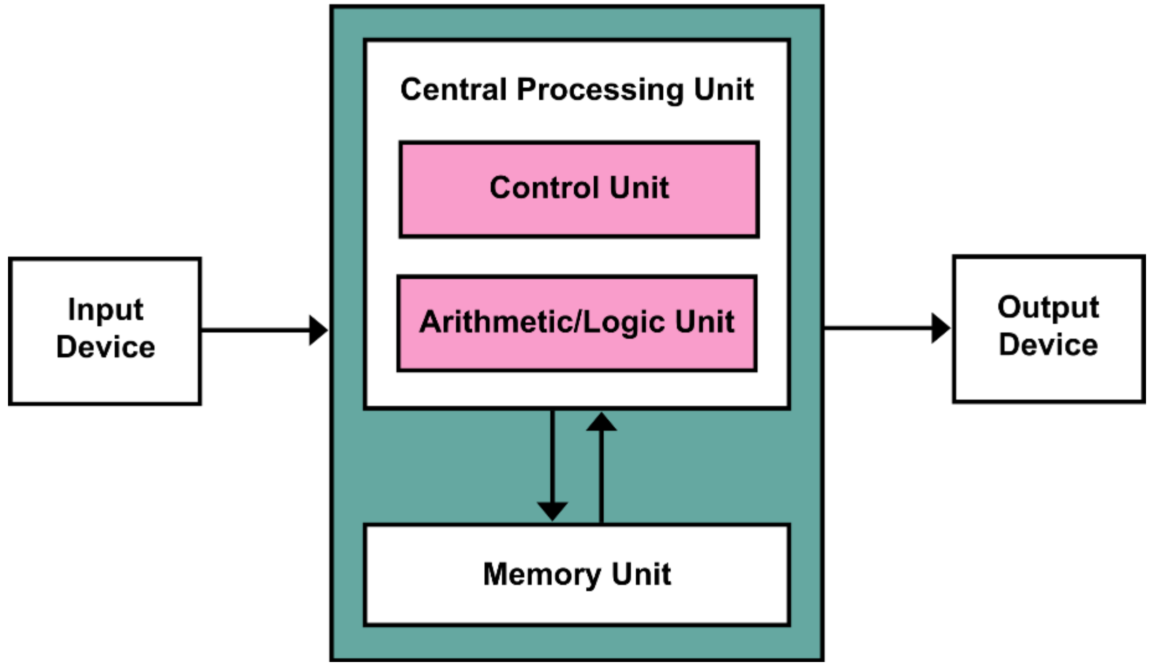
The classical computer

Any algorithmic process can be simulated efficiently using a Turing machine

The origins …

Theoretical model

von Neumann architecture



Turing '36

Turing Machine

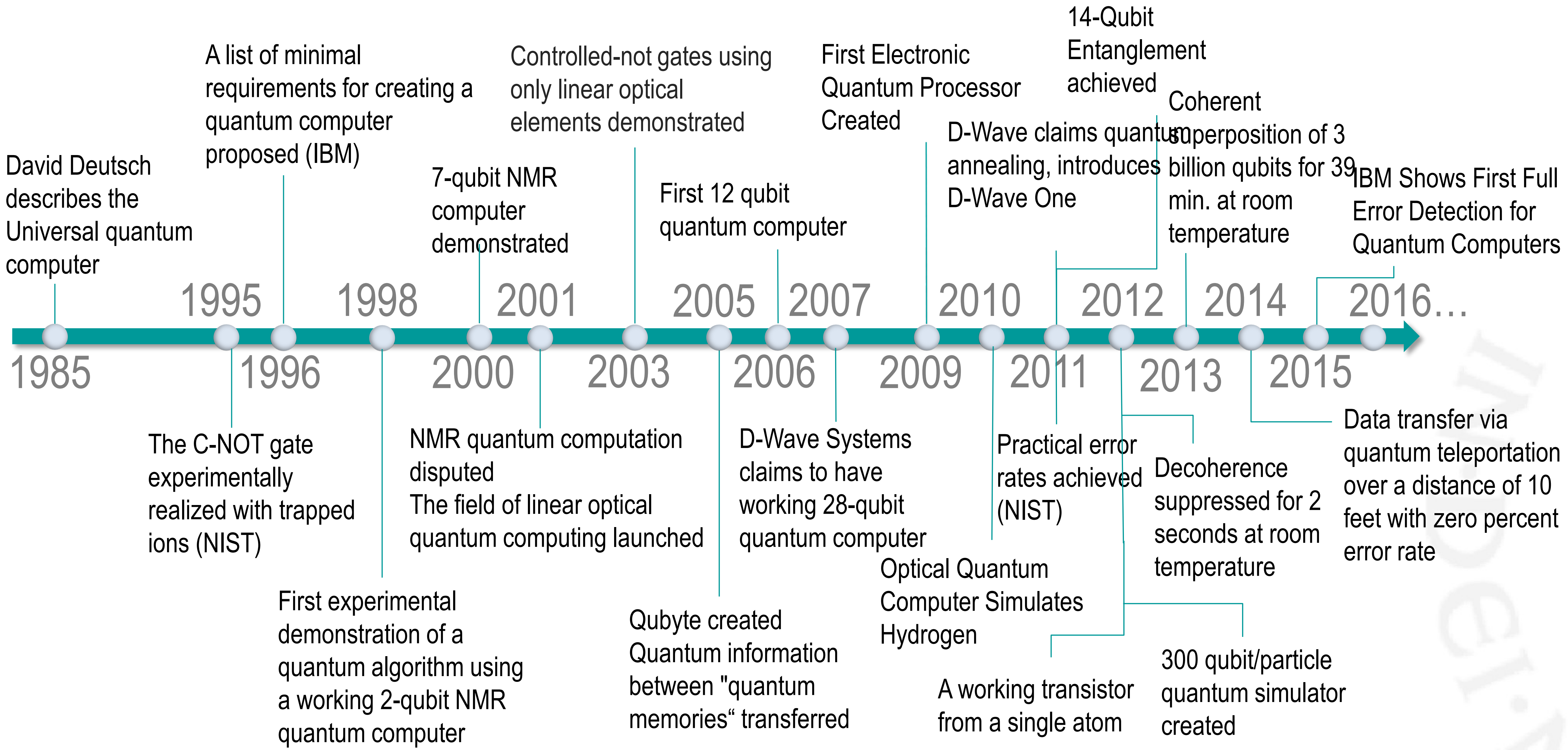
Any algorithmic process can be simulated efficiently using a Turing machine

The classical computer

Transistors

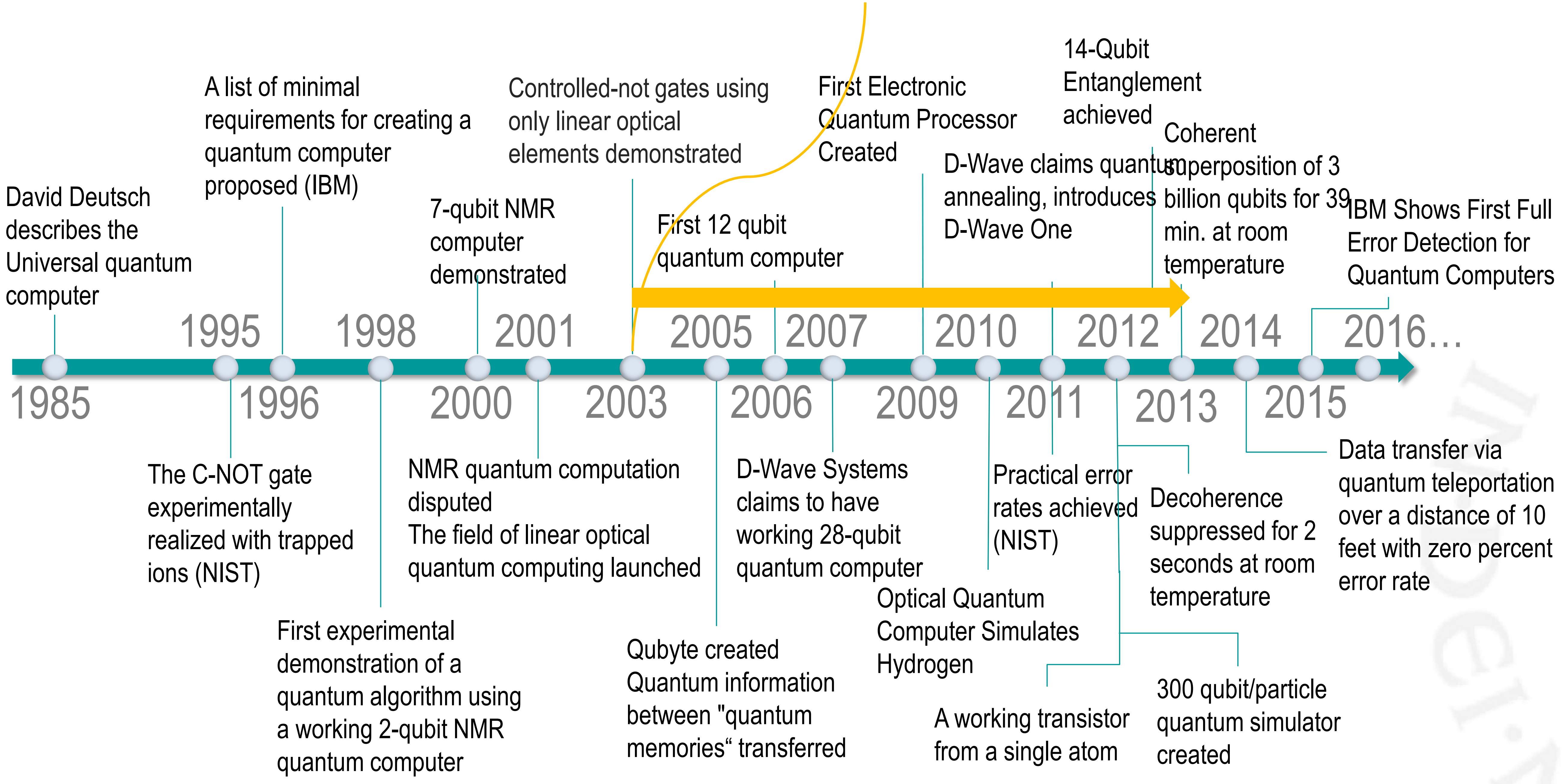
Hardware

Implementation milestones

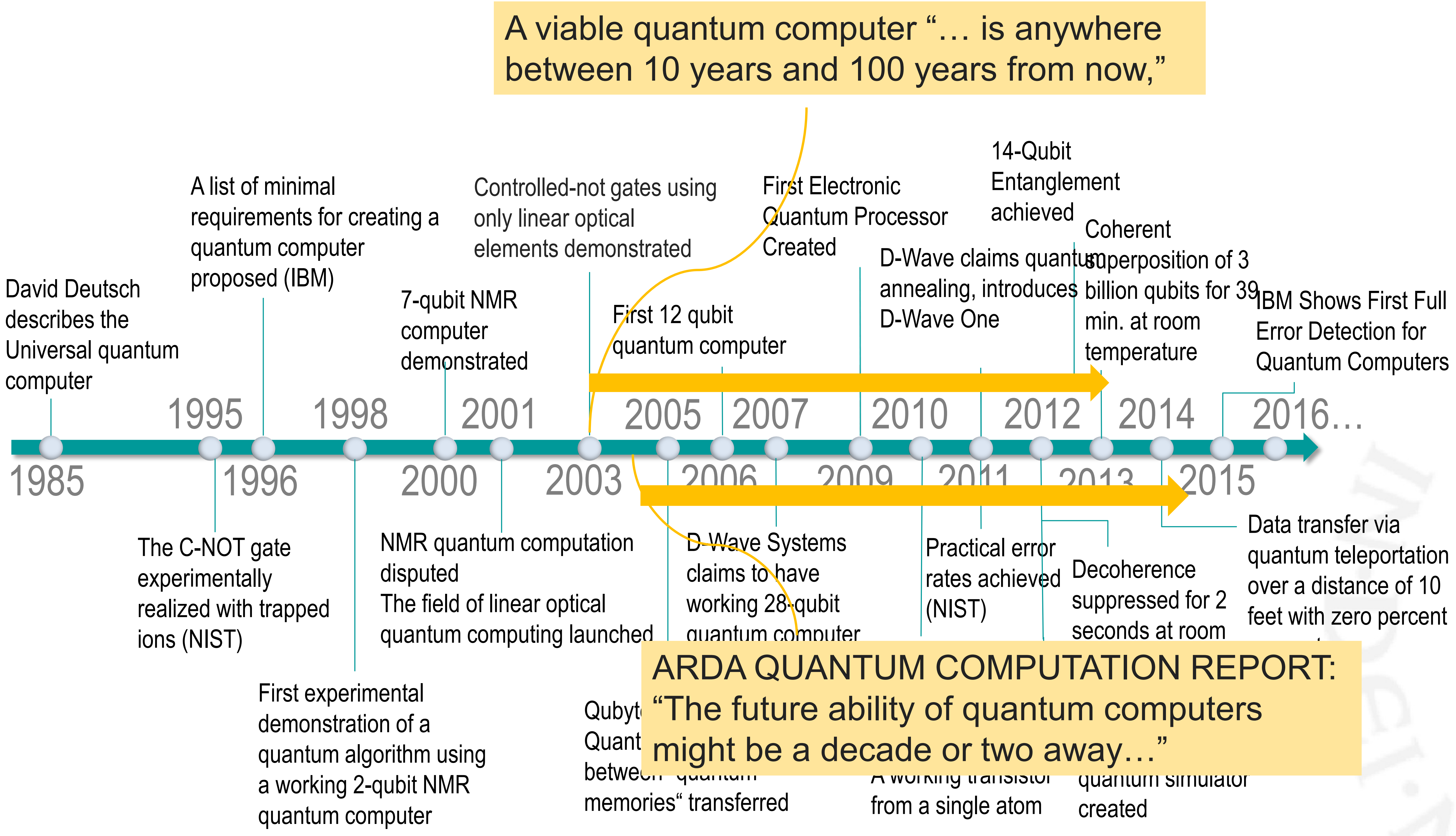


Implementation milestones

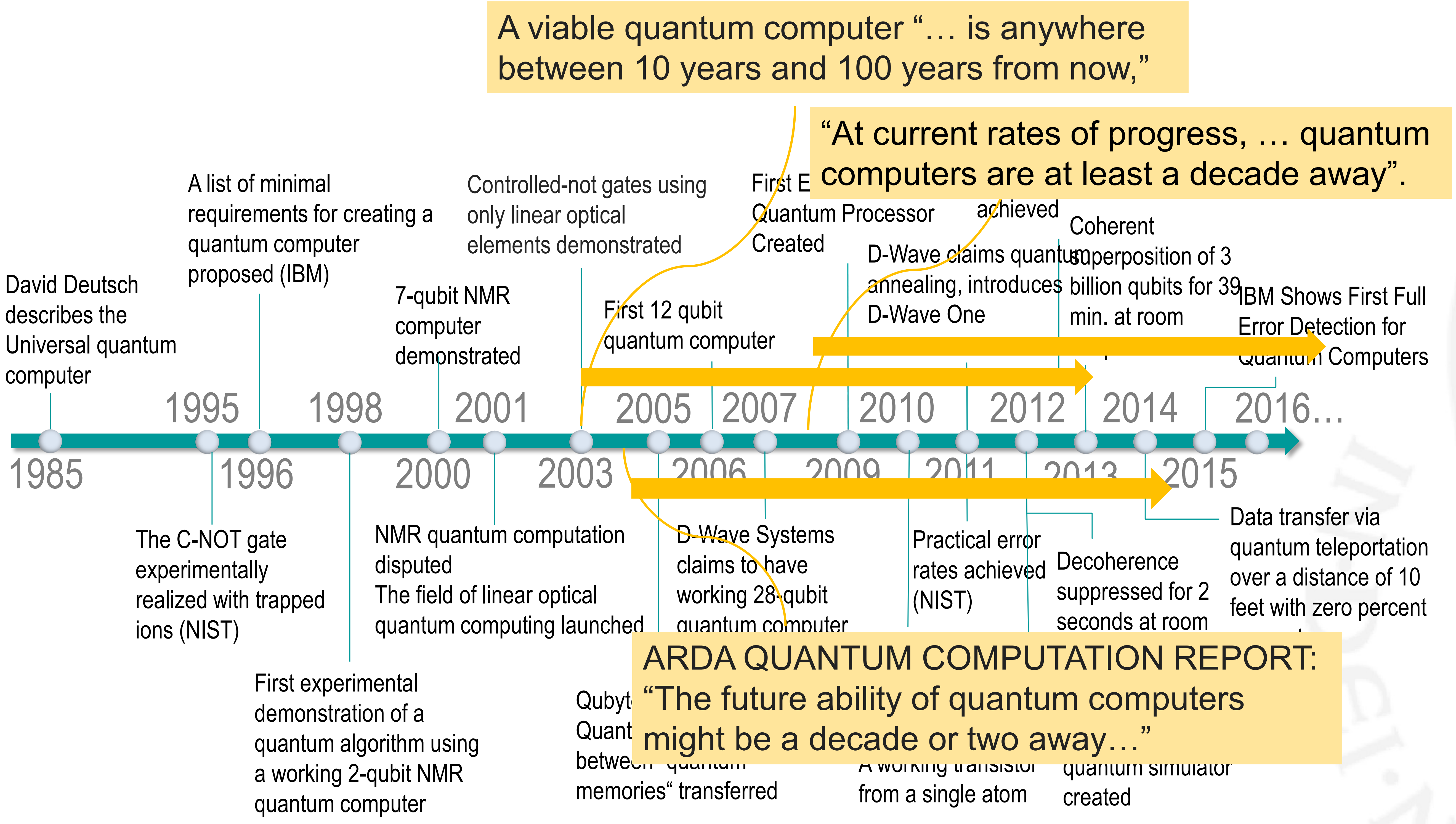
A viable quantum computer "… is anywhere between 10 years and 100 years from now,"



Implementation milestones



Implementation milestones



Implementation milestones

A viable quantum computer "… is anywhere between 10 years and 100 years from now,"

"At current rates of progress, … quantum computers are at least a decade away".

David Deutsch describes the Universal quantum computer

1985

A list of minimal requirements for creating a quantum computer proposed (IBM)

1995

1996

The C-NOT gate experimentally realized with trapped ions (NIST)

199

First experimental demonstration of a quantum algorithm using a working 2-qubit NMR quantum computer

Controlled-not gates using only linear optical

First E Quantum Processor

achieved

"Some physicist predicted that within the next 10 to 20 years quantum computers will be built that are sufficiently powerful to implement Shor's ideas and to break all existing public key schemes"

- Post Quantum Crypto 2008

First Full tion for omputers

via portation over a distance of 10 feet with zero percent

disputed

The field of linear optical quantum computing launched

claims to have working 28-qubit quantum computer

rates achieved (NIST)

Decoherence suppressed for 2 seconds at room

ARDA QUANTUM COMPUTATION REPORT: "The future ability of quantum computers might be a decade or two away…"

Qubyt Quant between "quantum memories" transferred

A working transistor from a single atom

quantum simulator created

Quantum Projects

COMPANY	TECHNOLOGY	WHY IT COULD FAIL
IBM	Makes qubits from superconducting metal circuits.	The error rate of the qubits is too high to operate them together in a useful computer.
Microsoft	Building a new kind of "topological qubit" that in theory should be more reliable than others.	The existence of the subatomic particle used in this qubit remains unproven. Even if it is real, there isn't yet evidence it can be controlled.
Alcatel-Lucent	Inspired by Microsoft's research, it is pursuing a topological qubit based on a different material.	Same as above.
D-Wave Systems	Sells computers based on superconducting chips with 512 qubits.	It's not clear that its chips harness quantum effects. Even if they do, their design is limited to solving a narrow set of mathematical problems.
Google	After experimenting with D-Wave's computers since 2009, it recently opened a lab to build chips like D-Wave's.	Same as above. Plus, Google is trying to adapt technology first developed for a different kind of qubit to the kind used by D-Wave.

MIT Technology Review

Quantum Projects

COMPANY	TECHNOLOGY	WHY IT COULD FAIL
IBM		bits is too high to operate them nputer.
Microsoft	Building a new kind of "topological qubit" that in theory should be more reliable than others.	The existence of the subatomic particle used in this qubit remains unproven. Even if it is real, there isn't yet evidence it can be controlled.
Alcatel-Lucent	Inspired by Microsoft's research, it is pursuing a topological qubit based on a different material.	Same as above.
D-Wave Systems	Sells computers based on superconducting chips with 512 qubits.	It's not clear that its chips harness quantum effects. Even if they do, their design is limited to solving a narrow set of mathematical problems.
Google	After experimenting with D-Wave's computers since 2009, it recently opened a lab to build chips like D-Wave's.	Same as above. Plus, Google is trying to adapt technology first developed for a different kind of qubit to the kind used by D-Wave.

IBM'S $3 BILLION INVESTMENT IN SYNTHETIC BRAINS AND QUANTUM COMPUTING

IBM THINKS THE FUTURE BELONGS TO COMPUTERS THAT MIMIC THE HUMAN BRAIN AND USE QUANTUM PHYSICS...AND THEY'RE BETTING $3 BILLION ON IT.

MIT Technology Review

Quantum Projects

COMPANY	TECHNOLOGY	WHY IT COULD FAIL
IBM	**IBM'S $3 BILLION INVESTMENT IN SYNTHETIC BRAINS AND QUANTUM COMPUTING** IBM THINKS THE FUTURE BELONGS TO COMPUTERS THAT MIMIC THE HUMAN BRAIN AND USE QUANTUM PHYSICS...AND THEY'RE BETTING $3 BILLION ON IT.	bits is too high to operate them nputer.
Microsoft	Building a new kind of "topological qubit" that in theory should be more reliable than others.	The existence of the subatomic particle used in this qubit remains unproven. Even if it is real, there isn't yet evidence it can be controlled.
Alcatel-Lucent	Inspired by Microsoft's research, it is pursuing a topological qubit based on a different material.	Same as above.
D-Wave Systems	D:Wave The Quantum Computing Company™ JAN 29, 2015 D-Wave Systems Raises an Additional $29M, Closing 2014 Financing at $62M	antum effects. Even ving a narrow set of
Google	After experimenting with D-Wave's computers since 2009, it recently opened a lab to build chips like D-Wave's.	Same as above. Plus, Google is trying to adapt technology first developed for a different kind of qubit to the kind used by D-Wave.

MIT Technology Review

Quantum Projects

COMPANY	TECHNOLOGY	WHY IT COULD FAIL
IBM	**IBM'S $3 BILLION INVESTMENT IN SYNTHETIC BRAINS AND QUANTUM COMPUTING** IBM THINKS THE FUTURE BELONGS TO COMPUTERS THAT MIMIC THE HUMAN BRAIN AND USE QUANTUM PHYSICS...AND THEY'RE BETTING $3 BILLION ON IT.	bits is too high to operate them nputer.
Microsoft	Building a new kind of "topological qubit" that in theory should be more reliable than others.	The existence of the subatomic particle used in this qubit remains unproven. Even if it is real, there isn't yet evidence it can be controlled.
Alcatel-Lucent	Inspired by Microsoft's research, it is pursuing a topological qubit based on a different material.	Same as above.
D-Wave Systems	D:Wave The Quantum Computing Company™ JAN 29, 2015 D-Wave Systems Raises an Additional $29M, Closing 2014 Financing at $62M	antum effects. Even ving a narrow set of
Google	After experimenting with D-Wave's computers since 2009, it recently opened a lab to build chips like D-Wave's.	

MOTHERBOARD

September 7, 2014 // 03:42 PM EST

Recent experiments have suggested that nothing particularly quantum is going on in the D-Wave machines, despite heavy interest and investment in the technology by both Google and NASA. A crucial paper in *Science* from July, "found no evidence of quantum speedup." Now, Google is going in a different, more back-to-the-basics quantum direction. For one thing, the author of the *Science* paper, John Martinis, is now in Google's employ, tasked with advancing beyond tentative D-Wave technology

MIT Technology Review

Quantum Projects

COMPANY	TECHNOLOGY	WHY IT COULD FAIL
IBM	IBM'S $3 BILLION INVESTMENT IN SYNTHETIC BRAINS AND QUANTUM COMPUTING IBM THINKS THE FUTURE BELONGS TO COMPUTERS THAT MIMIC THE HUMAN BRAIN AND USE QUANTUM PHYSICS...AND THEY'RE BETTING $3 BILLION ON IT.	bits is too high to operate them nputer.
Microsoft	Building a new kind of "topological qubit" that in theory should be more reliable than others.	The existence of the subatomic particle used in this qubit remains unproven. Even if it is real, there isn't yet evidence it can be controlled.
Alcatel-Lucent	Inspired by Microsoft's research, it is pursuing a topological qubit based on a different material.	Same as above.
D-Wave Systems	D:WAVE The Quantum Computing Company™ JAN 29, 2015 D-Wave Systems Raises an Additional $29M, Closing 2014 Financing at $62M	antum effects. Even ving a narrow set of
Google	future tense THE CITIZEN'S GUIDE TO THE FUTURE SEPT. 3 2014 7:56 PM **Google Is Investing More in Quantum Computing Research to Create Better AI**	MOTHERBOARD September 7, 2014 // 03:42 PM EST Recent experiments have suggested that nothing particularly quantum is going on in the D-Wave machines, despite heavy interest and investment in the technology by both Google and NASA. A crucial paper in *Science* from July, "found no evidence of quantum speedup." Now, Google is going in a different, more back-to-the-basics quantum direction. For one thing, the author of the *Science* paper, John Martinis, is now in Google's employ, tasked with advancing beyond tentative D-Wave technology

MIT Technology Review

Quantum Projects

COMPANY	TECHNOLOGY	WHY IT COULD FAIL
IBM	**IBM'S $3 BILLION INVESTMENT IN SYNTHETIC BRAINS AND QUANTUM COMPUTING** IBM THINKS THE FUTURE BELONGS TO COMPUTERS THAT MIMIC THE HUMAN BRAIN AND USE QUANTUM PHYSICS...AND THEY'RE BETTING $3 BILLION ON IT.	bits is too high to operate them nputer.
Microsoft	Neowin NEWS FEATURES FORUMS DEALS MORE Microsoft's making big investments into quantum computing	subatomic particle used in this qubit ven if it is real, there isn't yet evidence it
Alcatel-Lucent	Inspired by Microsoft's research, it is pursuing a topological qubit based on a different material.	Same as above.
D-Wave Systems	D:WAVE The Quantum Computing Company™ JAN 29, 2015 D-Wave Systems Raises an Additional $29M, Closing 2014 Financing at $62M	antum effects. Even ving a narrow set of
Google	future tense THE CITIZEN'S GUIDE TO THE FUTURE SEPT. 3 2014 7:56 PM **Google Is Investing More in Quantum Computing Research to Create Better AI**	

MOTHERBOARD

September 7, 2014 // 03:42 PM EST

Recent experiments have suggested that nothing particularly quantum is going on in the D-Wave machines, despite heavy interest and investment in the technology by both Google and NASA. A crucial paper in *Science* from July, "found no evidence of quantum speedup." Now, Google is going in a different, more back-to-the-basics quantum direction. For one thing, the author of the *Science* paper, John Martinis, is now in Google's employ, tasked with advancing beyond tentative D-Wave technology

MIT Technology Review

Quantum Projects

COMPANY	TECHNOLOGY	WHY IT COULD FAIL
IBM		bits is too high to operate them nputer.
Microsoft		subatomic particle used in this qubit ven if it is real, there isn't yet evidence it
D-Wave Systems		antum effects. Even ving a narrow set of
Google		

IBM'S $3 BILLION INVESTMENT IN SYNTHETIC BRAINS AND QUANTUM COMPUTING

IBM THINKS THE FUTURE BELONGS TO COMPUTERS THAT MIMIC THE HUMAN BRAIN AND USE QUANTUM PHYSICS...AND THEY'RE BETTING $3 BILLION ON IT.

Neowin NEWS FEATURES FORUMS DEALS MORE

Microsoft's making big investments into quantum computing

NIST Home > Public Affairs Office > News Releases > Joint Quantum Institute Created by University of Maryland, NIST and NSA

Joint Quantum Institute Created by University of Maryland, NIST and NSA

For Immediate Release: September 11, 2006

D-Wave The Quantum Computing Company™

JAN 29, 2015

D-Wave Systems Raises an Additional $29M, Closing 2014 Financing at $62M

MOTHERBOARD

September 7, 2014 // 03:42 PM EST

Recent experiments have suggested that nothing particularly quantum is going on in the D-Wave machines, despite heavy interest and investment in the technology by both Google and NASA. A crucial paper in *Science* from July, "found no evidence of quantum speedup." Now, Google is going in a different, more back-to-the-basics quantum direction. For one thing, the author of the *Science* paper, John Martinis, is now in Google's employ, tasked with advancing beyond tentative D-Wave technology

future tense THE CITIZEN'S GUIDE TO THE FUTURE SEPT. 3 2014 7:56 PM

Google Is Investing More in Quantum Computing Research to Create Better AI

MIT Technology Review

Quantum Projects

COMPANY	TECHNOLOGY	WHY IT COULD FAIL
IBM	IBM'S $3 BILLION INVESTMENT IN SYNTHETIC BRAINS AND QUANTUM COMPUTING IBM THINKS THE FUTURE BELONGS TO COMPUTERS THAT MIMIC THE HUMAN BRAIN AND USE QUANTUM PHYSICS...AND THEY'RE BETTING $3 BILLION ON IT.	bits is too high to operate them mputer.
Microsoft	Neowin NEWS FEATURES FORUMS DEALS MORE Microsoft's making big investments into quantum computing	subatomic particle used in this qubit ven if it is real, there isn't yet evidence it

NIST Home > Public Affairs Office > News Releases > Joint Quantum Institute Created by University of Maryland, NIST and NSA

Joint Quantum Institute Created by University of Maryland, NIST and NSA

For Immediate Release: September 11, 2006

The Washington Post PostTV Politics Opinions Local Sports National World Business Tech

National Security

A description of the Penetrating Hard Targets project

The effort to build "a cryptologically useful quantum computer" -- a machine exponentially faster than classical computers-- is part of a $79.7 million research program called "Penetrating Hard Targets." Read about the NSA's efforts

MIT Technology Review

Quantum Projects

COMPANY	TECHNOLOGY	WHY IT COULD FAIL
IBM		...bits is too high to operate them ...puter.

IBM'S $3 BILLION INVESTMENT IN SYNTHETIC BRAINS AND QUANTUM COMPUTING

IBM THINKS THE FUTURE BELONGS TO COMPUTERS THAT MIMIC THE HUMAN BRAIN

TechWeek europe

Search ...

Follow us NEWSLETTER LOGIN

Menu Mobility Networks Cloud Security Workspace Projects Events Tech Club IT Life Jobs Mobility Focus Whitepapers

UK Government Announces £270m Investment In Quantum Computing

NIST Home > Public Affairs Office > News Releases > Joint Quantum Institute Created by University of Maryland, NIST and NSA

Joint Quantum Institute Created by University of Maryland, NIST and NSA

For Immediate Release: September 11, 2006

The Washington Post PostTV Politics Opinions Local Sports National World Business Tech

National Security

A description of the Penetrating Hard Targets project

The effort to build "a cryptologically useful quantum computer" -- a machine exponentially faster than classical computers-- is part of a $79.7 million research program called "Penetrating Hard Targets." Read about the NSA's efforts

MIT Technology Review

Quantum Projects

COMPANY	TECHNOLOGY	WHY IT COULD FAIL
IBM		bits is too ... nputer.

IBM'S $3 BILLION INVESTMENT IN SYNTHETIC BRAINS AND QUANTUM COMPUTING

IBM THINKS THE FUTURE BELONGS TO COMPUTERS THAT MIMIC THE HUMAN BRAIN

DutchNews.nl

23° Sky is Clear

Thursday 11 June 2015

Home | Politics | Business | Society | Sport | Education

Dutch invest €135m in developing a quantum computer

TechWeek europe

Search ...

Follow us | NEWSLETTER | LOGIN

Menu | Mobility | Networks | Cloud | Security | Workspace | Projects | Events | Tech Club | IT Life | Jobs | Mobility Focus | Whitepapers

UK Government Announces £270m Investment In Quantum Computing

NIST Home > Public Affairs Office > News Releases > Joint Quantum Institute Created by University of Maryland, NIST and NSA

Joint Quantum Institute Created by University of Maryland, NIST and NSA

For Immediate Release: September 11, 2006

The Washington Post | PostTV | Politics | Opinions | Local | Sports | National | World | Business | Tech

National Security

A description of the Penetrating Hard Targets project

The effort to build "a cryptologically useful quantum computer" -- a machine exponentially faster than classical computers-- is part of a $79.7 million research program called "Penetrating Hard Targets." Read about the NSA's efforts

MIT Technology Review

Multi Qubit systems

2-qubit system:

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle\,, \quad |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle \mapsto |0\rangle, |1\rangle, |2\rangle, |3\rangle$$

Multi Qubit systems

2-qubit system:

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle\,, \quad |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle \mapsto |0\rangle, |1\rangle, |2\rangle, |3\rangle$$

N-qubit system:

$\rightarrow$ 2^n states $|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle$

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle\,, \quad \sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$$

Entanglement – Quantum weirdness example

Bell states: $$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Measurement of first qubit

$$\begin{tikzcd} & |00\rangle \\ |\psi\rangle \arrow[ur] \arrow[dr] & \\ & |11\rangle \end{tikzcd}$$

$P_{|00\rangle} = \frac{1}{2} \Rightarrow$ The first qubit is $|0\rangle$

$P_{|11\rangle} = \frac{1}{2} \Rightarrow$ The first qubit is $|1\rangle$

Entanglement – Quantum weirdness example

Bell states: $$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Measurement of first qubit

$$|\psi\rangle \to |00\rangle \qquad P_{|00\rangle} = \frac{1}{2} \quad \Rightarrow \quad \text{The first qubit is } |0\rangle$$

$$|\psi\rangle \to |11\rangle \qquad P_{|11\rangle} = \frac{1}{2} \quad \Rightarrow \quad \text{The first qubit is } |1\rangle$$

The only two possible outcomes!

Entanglement – Quantum weirdness example

Bell states: $$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Measurement of first qubit

$|\psi\rangle$

$|00\rangle$ $$P_{|00\rangle} = \frac{1}{2} \Rightarrow$$ The first qubit is $|0\rangle$

The second qubit is $|0\rangle$ with probability 1

$|11\rangle$ $$P_{|11\rangle} = \frac{1}{2} \Rightarrow$$ The first qubit is $|1\rangle$

The second qubit is $|1\rangle$ with probability 1

The only two possible outcomes!

Entanglement – Quantum weirdness example

Bell states: $$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Measurement of first qubit

$|\psi\rangle$ → $|00\rangle$: $P_{|00\rangle} = \frac{1}{2} \Rightarrow$ The first qubit is $|0\rangle$

The second qubit is $|0\rangle$ with probability 1

$|\psi\rangle$ → $|11\rangle$: $P_{|11\rangle} = \frac{1}{2} \Rightarrow$ The first qubit is $|1\rangle$

The second qubit is $|1\rangle$ with probability 1

The measurement of the second qubit **always gives the same result** as the measurement of the first qubit!

Entanglement – Quantum weirdness example

Bell states: $|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

Possible since $|\psi\rangle \neq |\varphi_1\rangle \otimes |\varphi_2\rangle$!!!

Measurement of first qubit

$|\psi\rangle \to |00\rangle$: $P_{|00\rangle} = \frac{1}{2} \Rightarrow$ The first qubit is $|0\rangle$

The second qubit is $|0\rangle$ with probability 1

$|\psi\rangle \to |11\rangle$: $P_{|11\rangle} = \frac{1}{2} \Rightarrow$ The first qubit is $|1\rangle$

The second qubit is $|1\rangle$ with probability 1

The measurement of the second qubit **always gives the same result** as the measurement of the first qubit!

Quantum Interference!

Quantum Interference!

Deutsch's problem:
Determine whether $f(x): \{0,1\} \rightarrow \{0,1\}$ is constant or balanced

Quantum Interference!

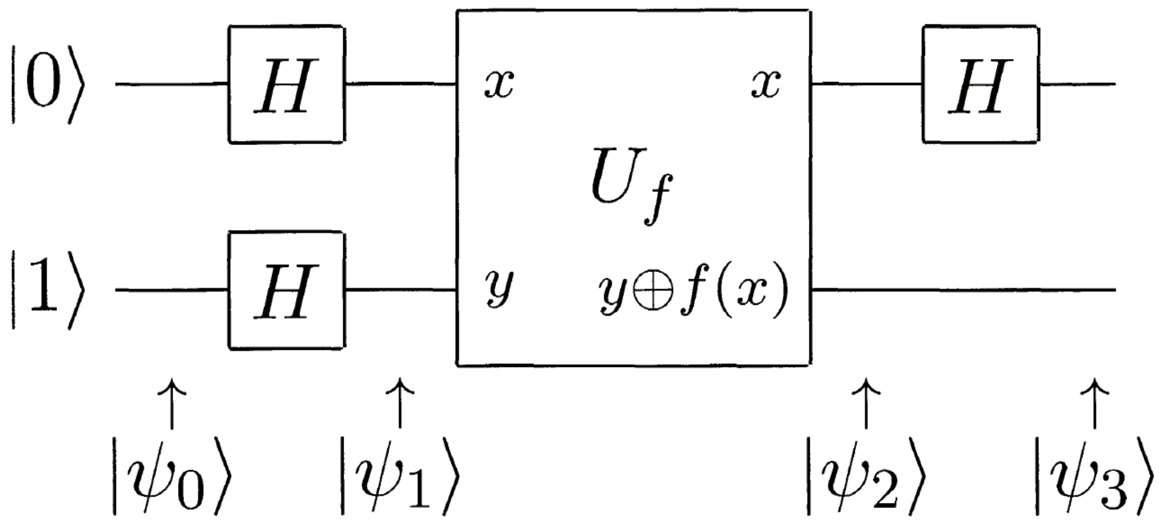
Deutsch's problem:
Determine whether $f(x): \{0,1\} \to \{0,1\}$ is constant or balanced

Classically, we need 2 evaluations!
Using quantum parallelism + interference, only one!

Quantum Interference!

Deutsch's problem:
Determine whether $f(x): \{0,1\} \rightarrow \{0,1\}$ is constant or balanced

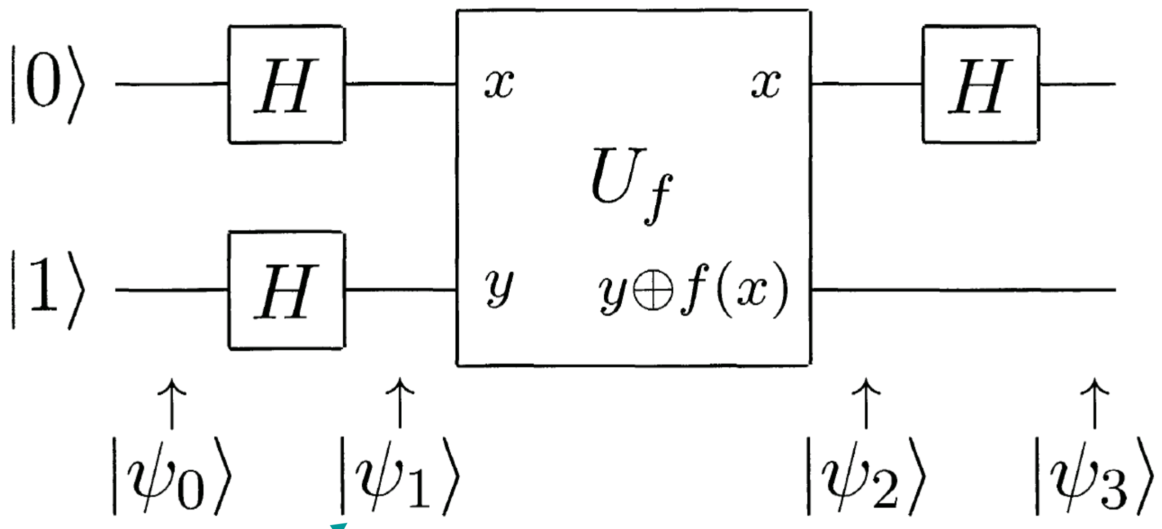
Classically, we need 2 evaluations!
Using quantum parallelism + interference, only one!



Quantum Interference!

Deutsch's problem:
Determine whether $f(x): \{0,1\} \rightarrow \{0,1\}$ is constant or balanced

Classically, we need 2 evaluations!
Using quantum parallelism + interference, only one!

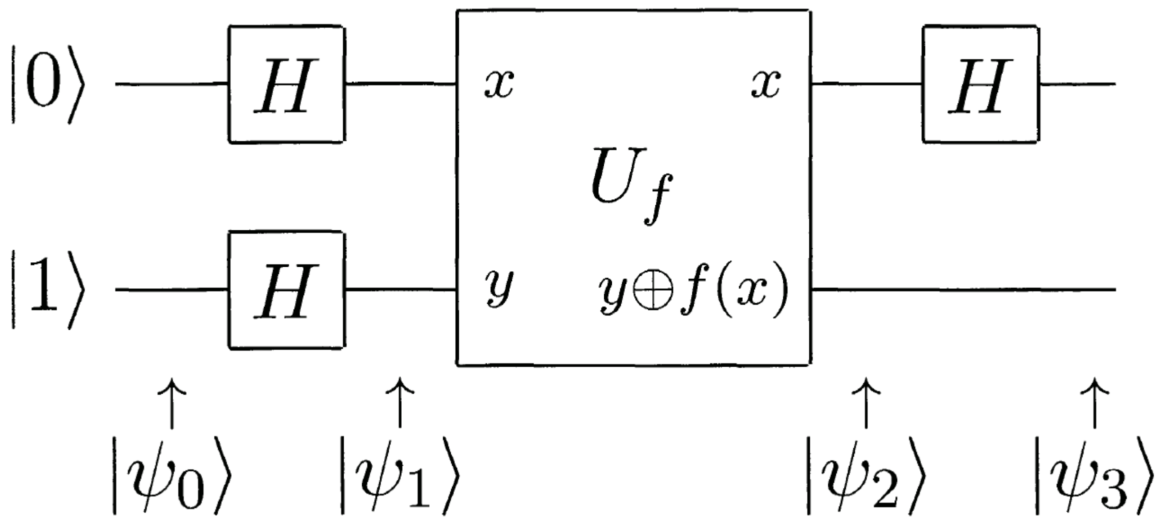


$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

Quantum Interference!

Deutsch's problem:
Determine whether $f(x)\colon \{0,1\} \to \{0,1\}$ is constant or balanced

Classically, we need 2 evaluations!
Using quantum parallelism + interference, only one!



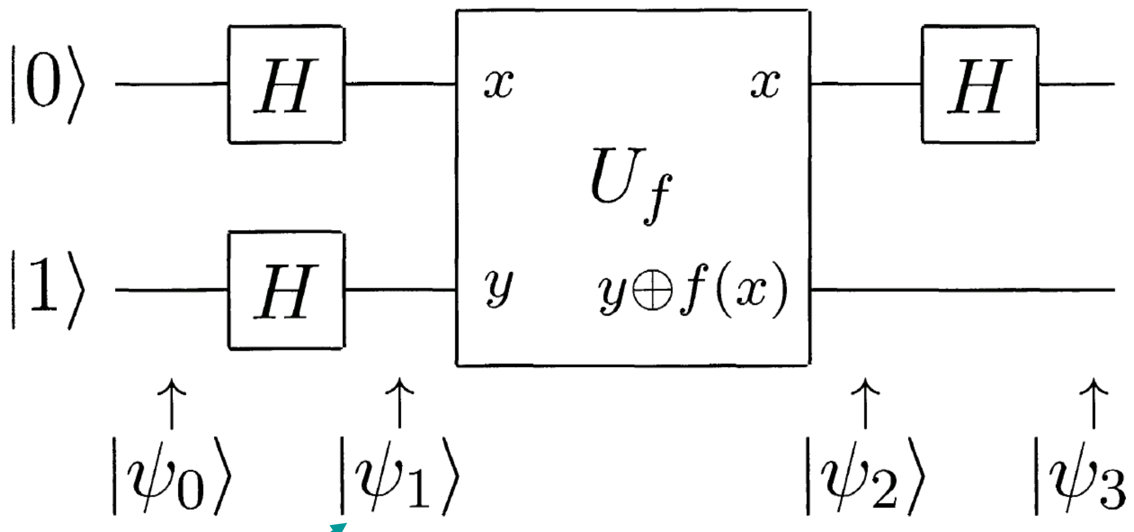
$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$$

Quantum Interference!

Deutsch's problem:
Determine whether $f(x): \{0,1\} \rightarrow \{0,1\}$ is constant or balanced

Classically, we need 2 evaluations!
Using quantum parallelism + interference, only one!



$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

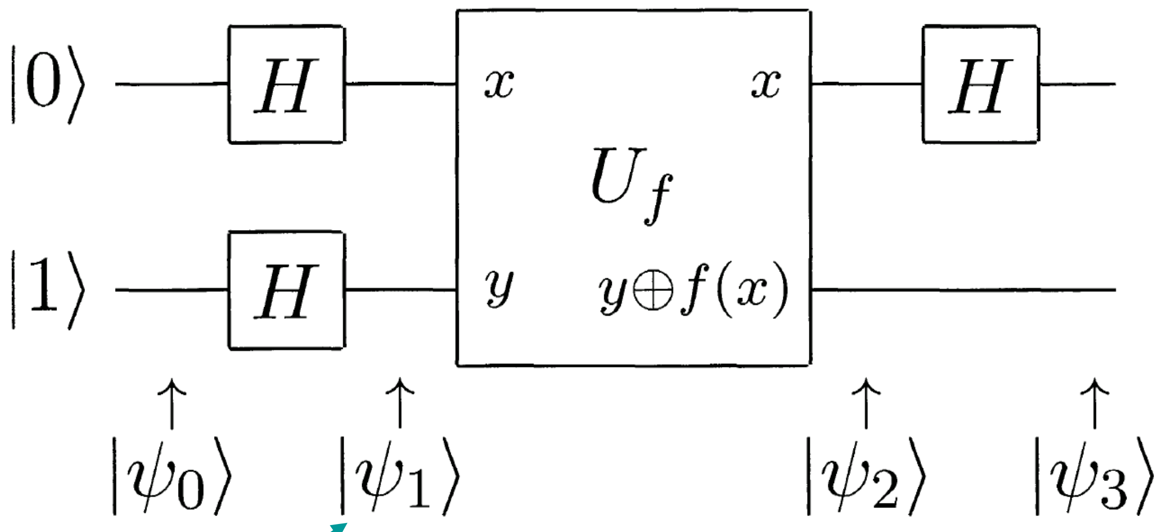
$$(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$$

$$|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

Quantum Interference!

Deutsch's problem:
Determine whether $f(x): \{0,1\} \rightarrow \{0,1\}$ is constant or balanced

Classically, we need 2 evaluations!
Using quantum parallelism + interference, only one!



Measuring the first qubit yields:

$$f(0) \oplus f(1)$$

$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

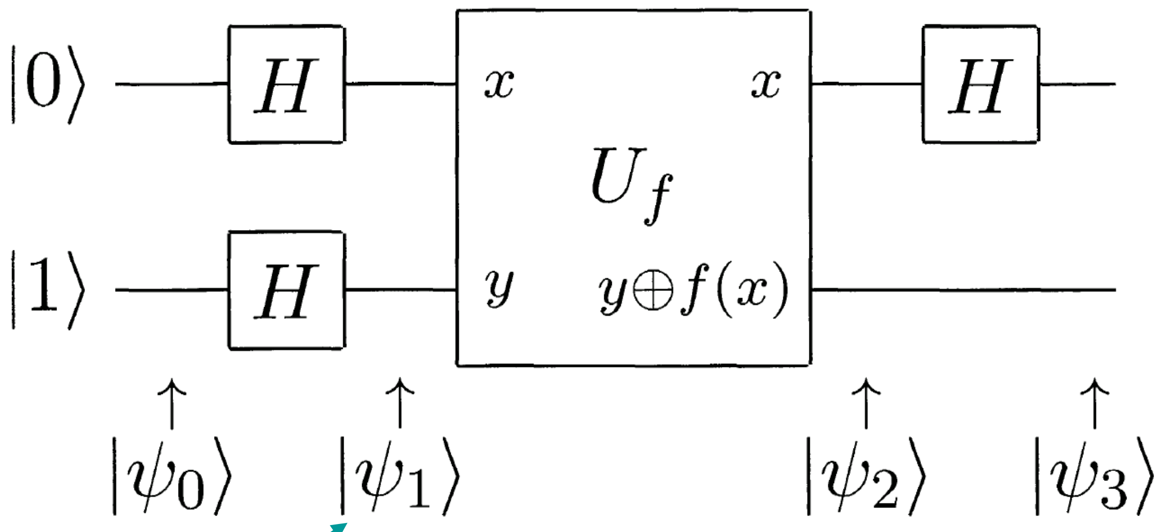
$$|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$$

Quantum Interference!

Deutsch's problem:
Determine whether $f(x)\colon \{0,1\} \to \{0,1\}$ is constant or balanced

Classically, we need 2 evaluations!
Using quantum parallelism + interference, only one!



Measuring the first qubit yields:

$f(0) \oplus f(1)$

0 constant

1 balanced

$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

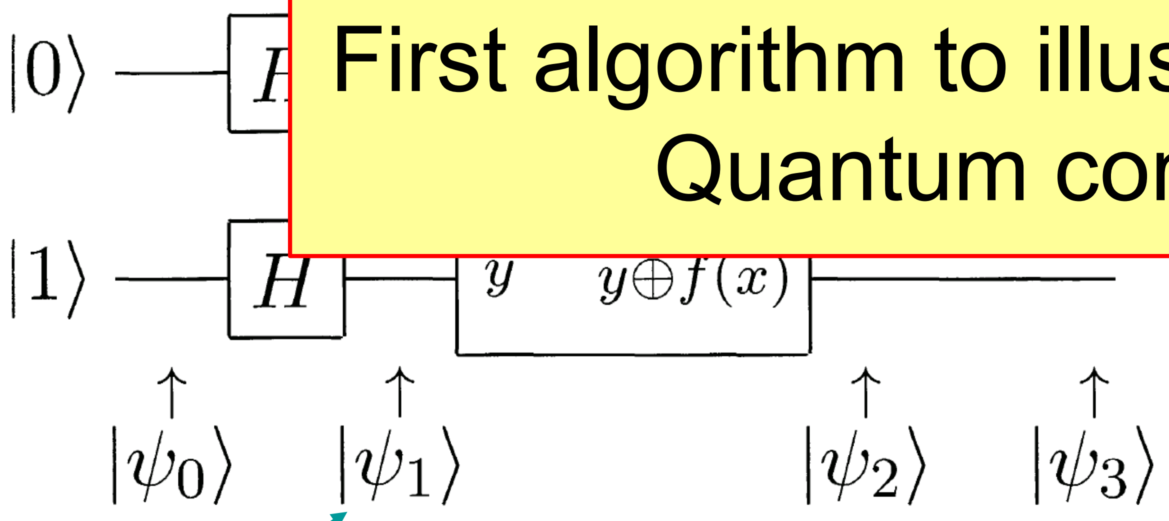
$$|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$$

Quantum Interference!

Deutsch's problem:
Determine whether $f(x): \{0,1\} \rightarrow \{0,1\}$ is constant or balanced

Classically, we need 2 evaluations!
Using quantum parallelism + interference, only one!



First algorithm to illustrate the power of Quantum computation!

qubit yields:

1)

0
constant

1
balanced

$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$$

$$|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$|\psi_2\rangle = \begin{cases} \pm \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1). \end{cases} \tag{1.43}$$

The final Hadamard gate on the first qubit thus gives us

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm|1\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1). \end{cases} \tag{1.44}$$

Realizing that $f(0) \oplus f(1)$ is 0 if $f(0) = f(1)$ and 1 otherwise, we can rewrite this result concisely as

$$|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right], \tag{1.45}$$

Shor’s algorithm [Shor ’94]

- Integer factorization algorithm
- Discrete logarithm problem

Number theory + Parallelism + Interference

Shor's algorithm [Shor '94]

- Integer factorization algorithm
- Discrete logarithm problem

Number theory + Parallelism + Interference

Convert the problem
to the problem of
period finding
(can be implemented
efficiently classically)

Shor's algorithm [Shor '94]

- Integer factorization algorithm
- Discrete logarithm problem

Number theory + Parallelism + Interference

Convert the problem
to the problem of period finding
(can be implemented **efficiently classically**)

Simon's algorithm:
Finds the unknown period of a periodic function

Shor's algorithm [Shor '94]

- Integer factorization algorithm
- Discrete logarithm problem

Number theory + Parallelism + Interference

Convert the problem **to the problem of period finding** (can be implemented **efficiently classically**)

Find the period using **Simultaneous evaluation** and **Quantum Fourier Transform** (**quantum speedup**)

Simon's algorithm:
Finds the unknown period of a periodic function

Shor's algorithm [Shor '94]

Number theory + Parallelism + Interference

Shor's algorithm [Shor '94]

Number theory + Parallelism + Interference

od NN (xx≠±1 mod NN) then gcd(xx+1, NN) is a nontrivial factor of NN.

$\boldsymbol{x\ a\ xx\ x\ a\ aa\ x\ a}$ $\mathrm{mod}\ NN$ is a periodic function, gcd x, N $\mathrm{gcd}\ \mathrm{gcd}$ x, N

$x, N\ xx, NN\ x, N$ gcd x, N $=1$

Important **facts**:

- If x is a nontrivial square root of 1 $\mathrm{mod}\ N$ $(x \neq \pm 1 \mathrm{\ mod\ } N)$ then $\mathrm{gcd}(x+1, N)$ is a nontrivial factor of N.

Shor’s algorithm [Shor ’94]

Number theory + Parallelism + Interference

cd(y r/2 yy y r/2 rr/2 y r/2 +1, NN) is a nontrivial factor of NN.

2 y r/2 is a nontrivial square root of 1 mod NN. Thus

cd gcd y, N y, N yy, NN y, N gcd y, N =1, then with probability at least ½,

od **NN (xx≠±1 mod NN) then gcd(xx+1, NN) is a nontrivial factor of NN.**

x a xx x a aa x a mod NN is a periodic function, gcd x, N gcd gcd x, N x, N xx, NN x, N gcd x, N =1

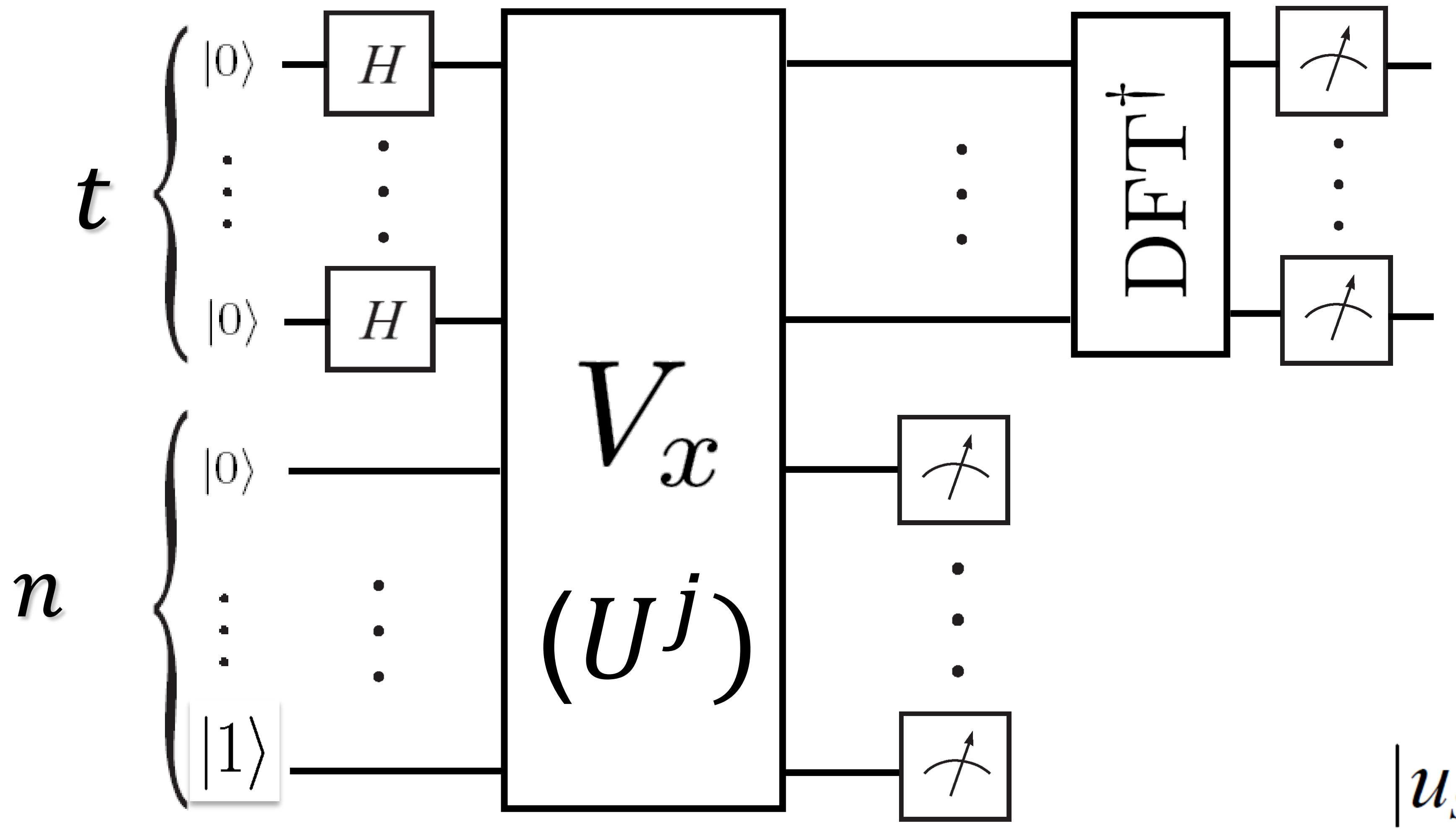
Important **facts**:

- If x is a nontrivial square root of 1 $\bmod N$ $(x \neq \pm 1 \bmod N)$ then $\gcd(x+1, N)$ is a nontrivial factor of N.

Thm: If N is an odd composite number, r is a period of F,
$\gcd(y^{r/2}+1, N)$ is a nontrivial factor of N.

Shor's algorithm [Shor '94] - **Step by step**

1. Choose $1 \leq x \leq N-1$, such that $\gcd(x, N) = 1$
2. Prepare a quantum circuit:



$$\boxed{V_x(|j\rangle\,|k\rangle) = |j\rangle\,|k\,x^j\rangle}$$

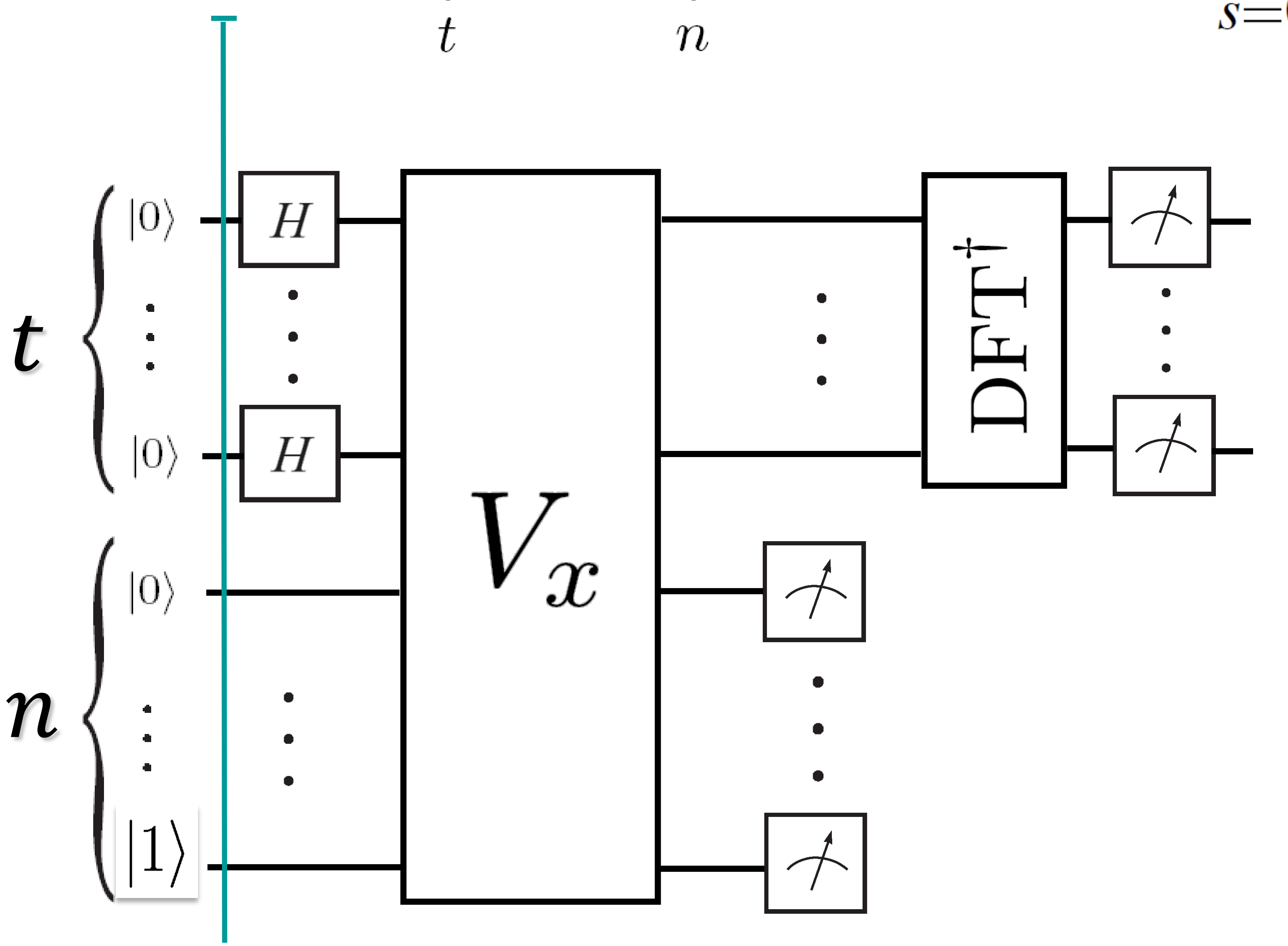
$$U|y\rangle \equiv |xy(modN)\rangle$$

$$U|u_s\rangle = e^{2\pi i \frac{s}{r}}|u_s\rangle$$

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2\pi i \frac{s}{r}k}|x^k modN\rangle$$

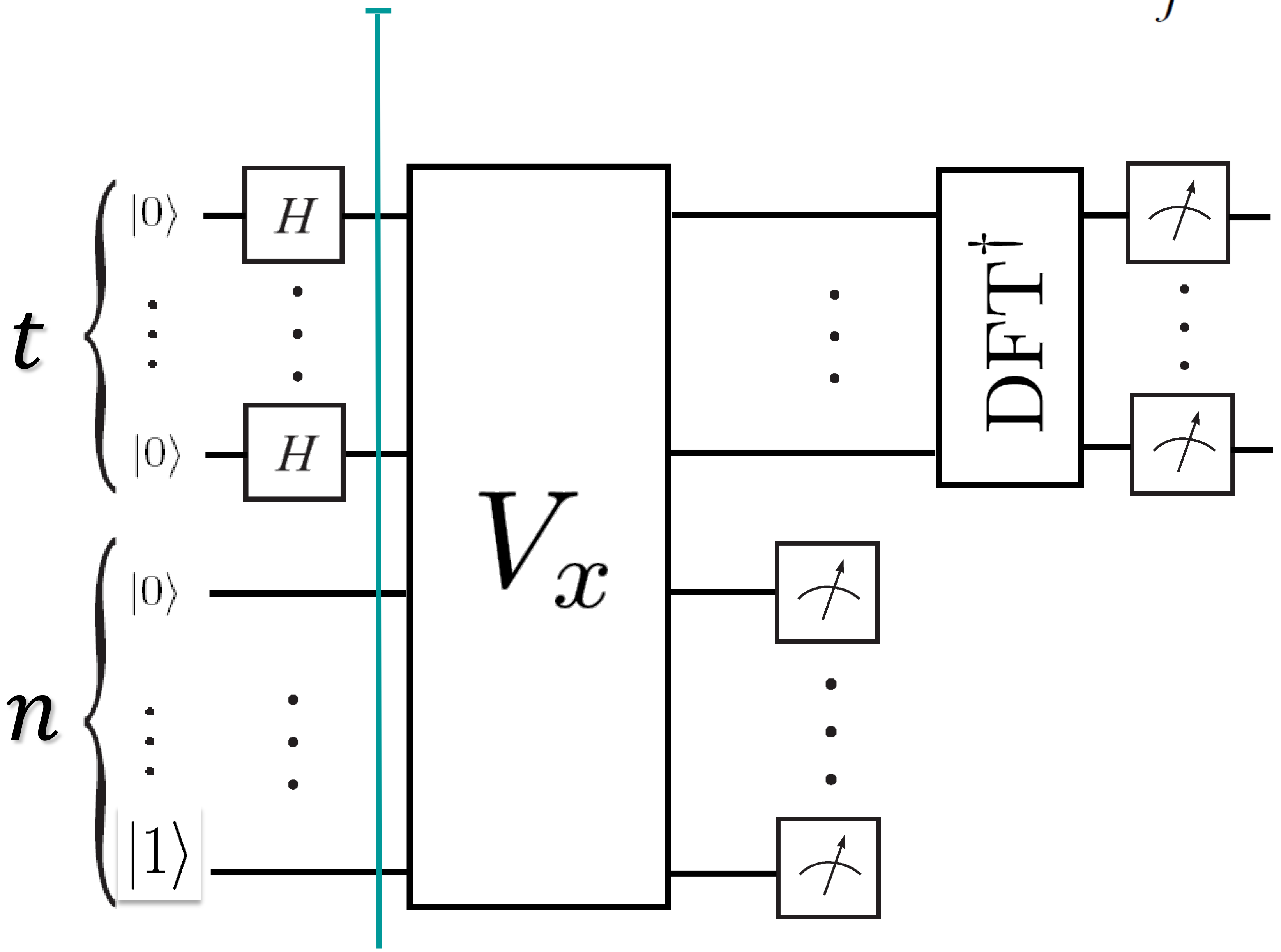
Shor's algorithm [Shor '94] - **Step by step**

3. $|\psi_0\rangle = \underbrace{|0\ldots0\rangle}_{t}\underbrace{|0\ldots1\rangle}_{n} = |0\rangle^{\otimes t}\frac{1}{\sqrt{r}}\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\sum_{k=0}^{r-1} e^{-2\pi i\frac{s}{r}k}|x^k modN\rangle$



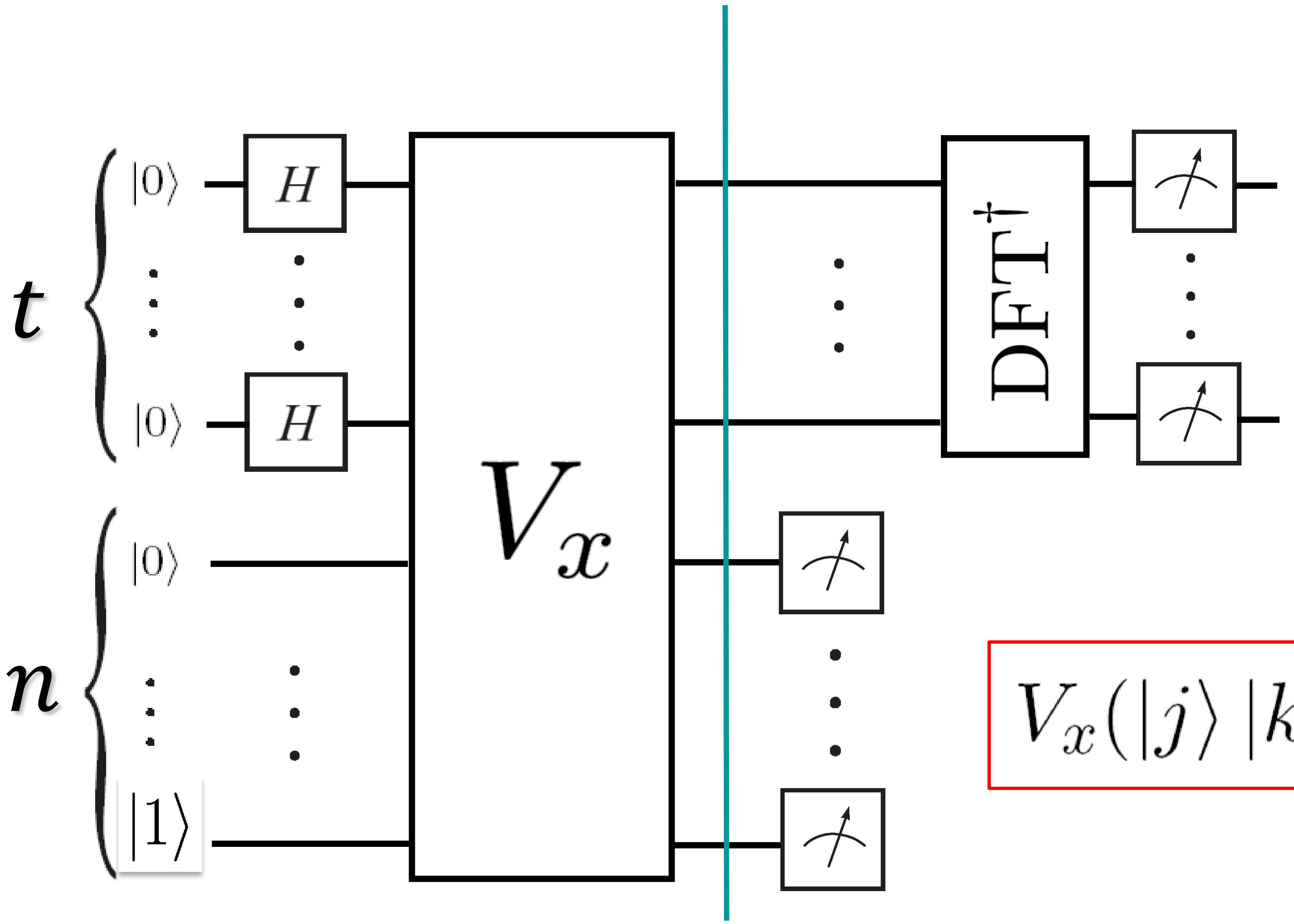
Shor's algorithm [Shor '94] - **Step by step**

4. $|\varphi_1\rangle = \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|0\rangle\ |1\rangle = \frac{1}{\sqrt{2^t}} \sum_{j} |j\rangle \frac{1}{\sqrt{r}} \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \sum_{k=0}^{r-1} e^{-2\pi i \frac{s}{r} k} |x^k mod N\rangle$



Shor's algorithm [Shor '94] - Step by step

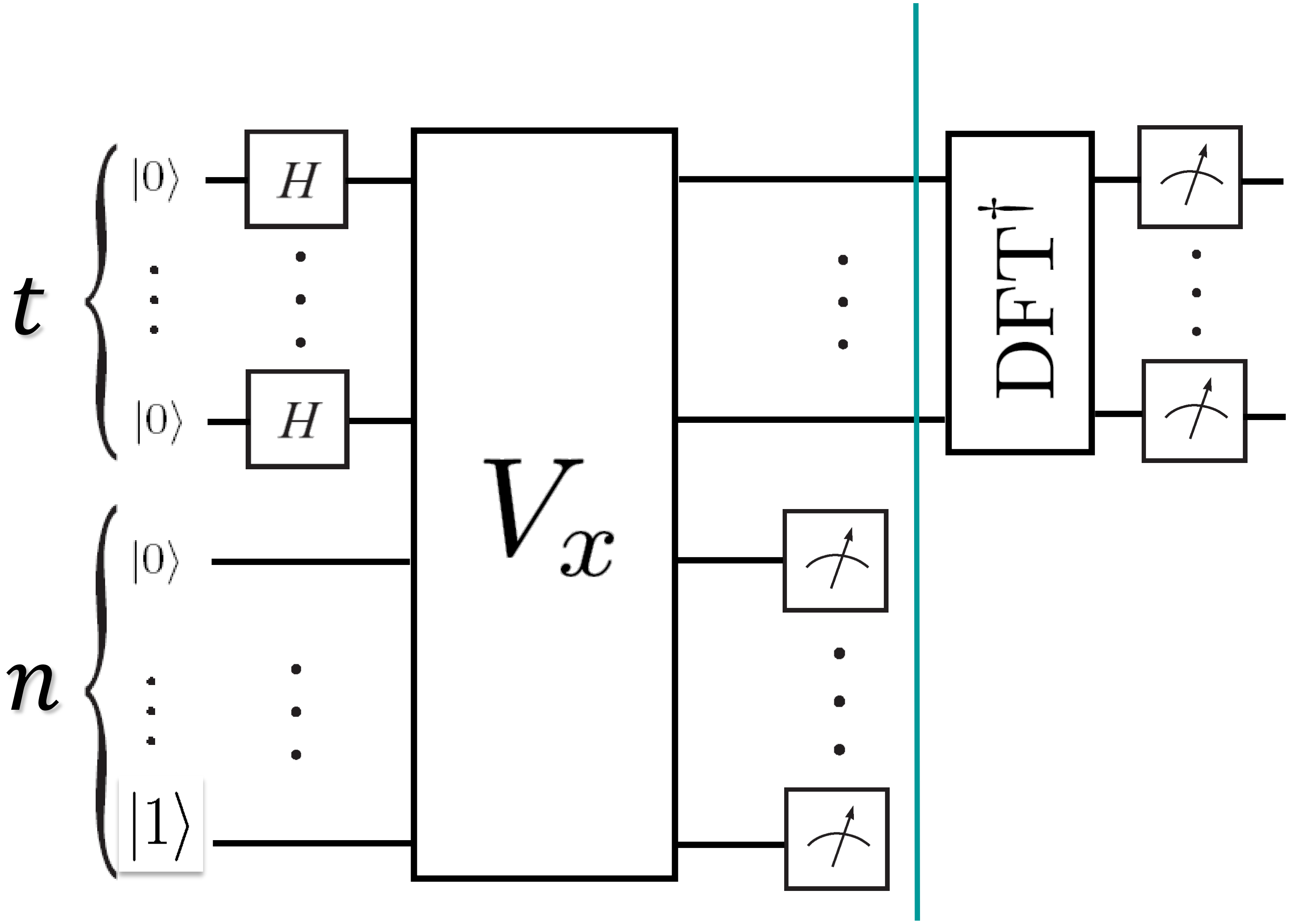
5. $$|\varphi_2\rangle = \frac{1}{\sqrt{2^t}} \sum_j |j\rangle \frac{1}{\sqrt{r}} \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \sum_{k=0}^{r-1} e^{-2\pi i \frac{s}{r} j + (-2\pi i \frac{s}{r} k)} |x^k mod N\rangle$$



$$V_x(|j\rangle |k\rangle) = |j\rangle |k\, x^j\rangle$$

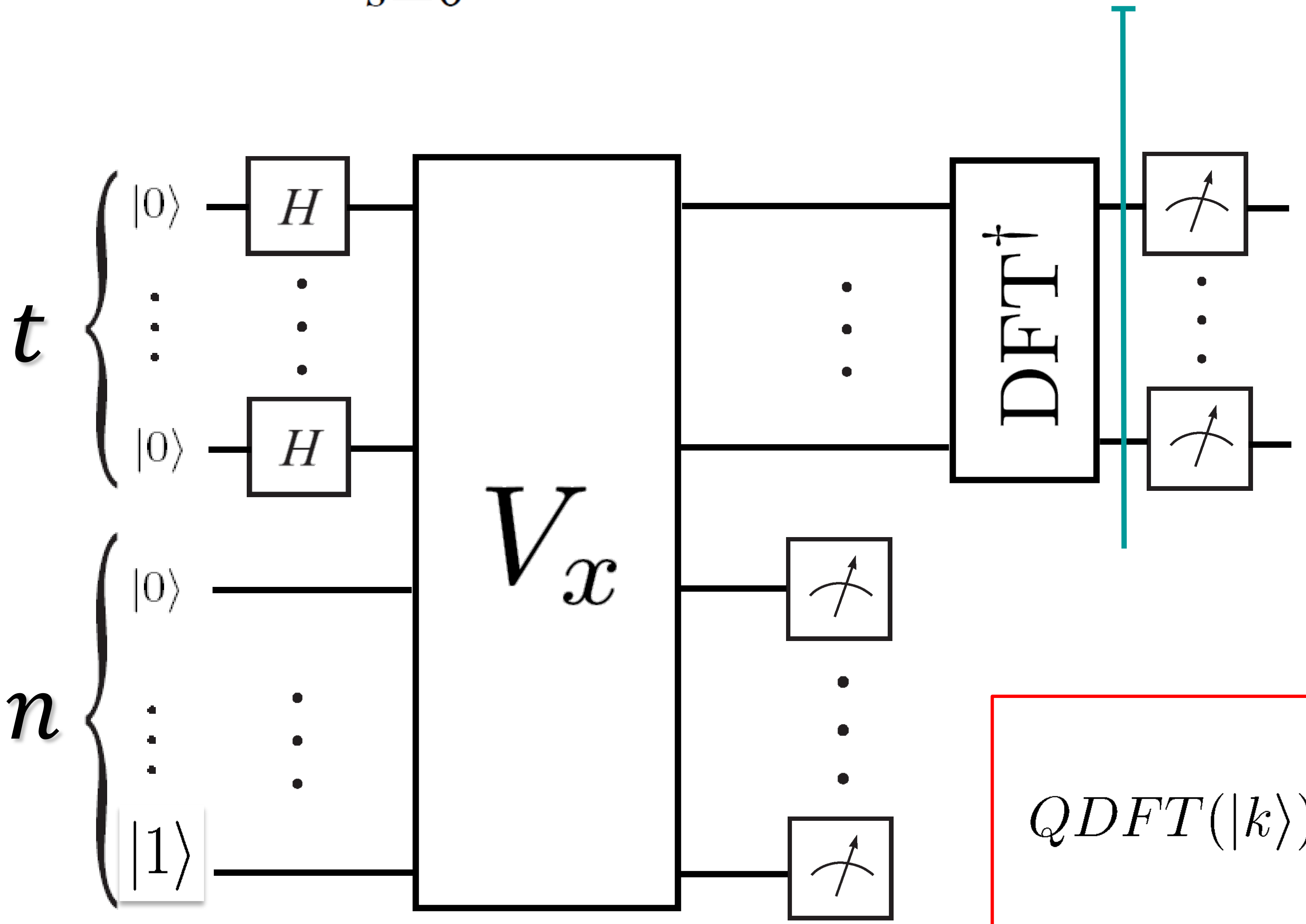
Shor's algorithm [Shor '94] - **Step by step**

6. $$|\varphi_3\rangle = \frac{1}{\sqrt{2^t}}\sum_j \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1} e^{-2\pi i \frac{s}{r}(j+k)}|j\rangle|x^k modN\rangle$$



Shor's algorithm [Shor '94] - **Step by step**

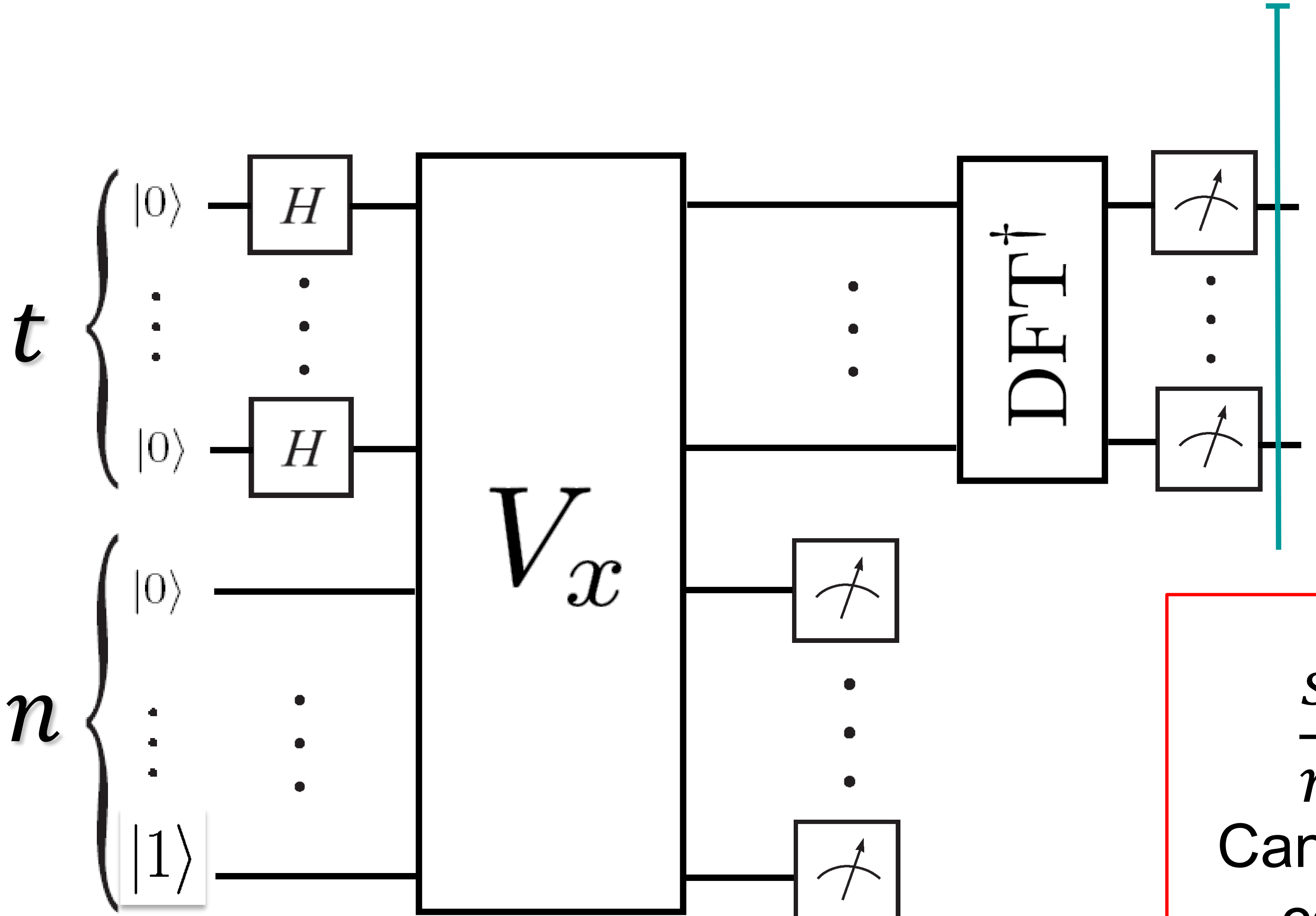
7. $|\varphi_4\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\widetilde{s/r}\rangle |x^k mod N\rangle$ (inverse *QDFT*)



$$QDFT(|k\rangle) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} |j\rangle$$

Shor's algorithm [Shor '94] - **Step by step**

4. Measure to obtain $\frac{s}{r}$

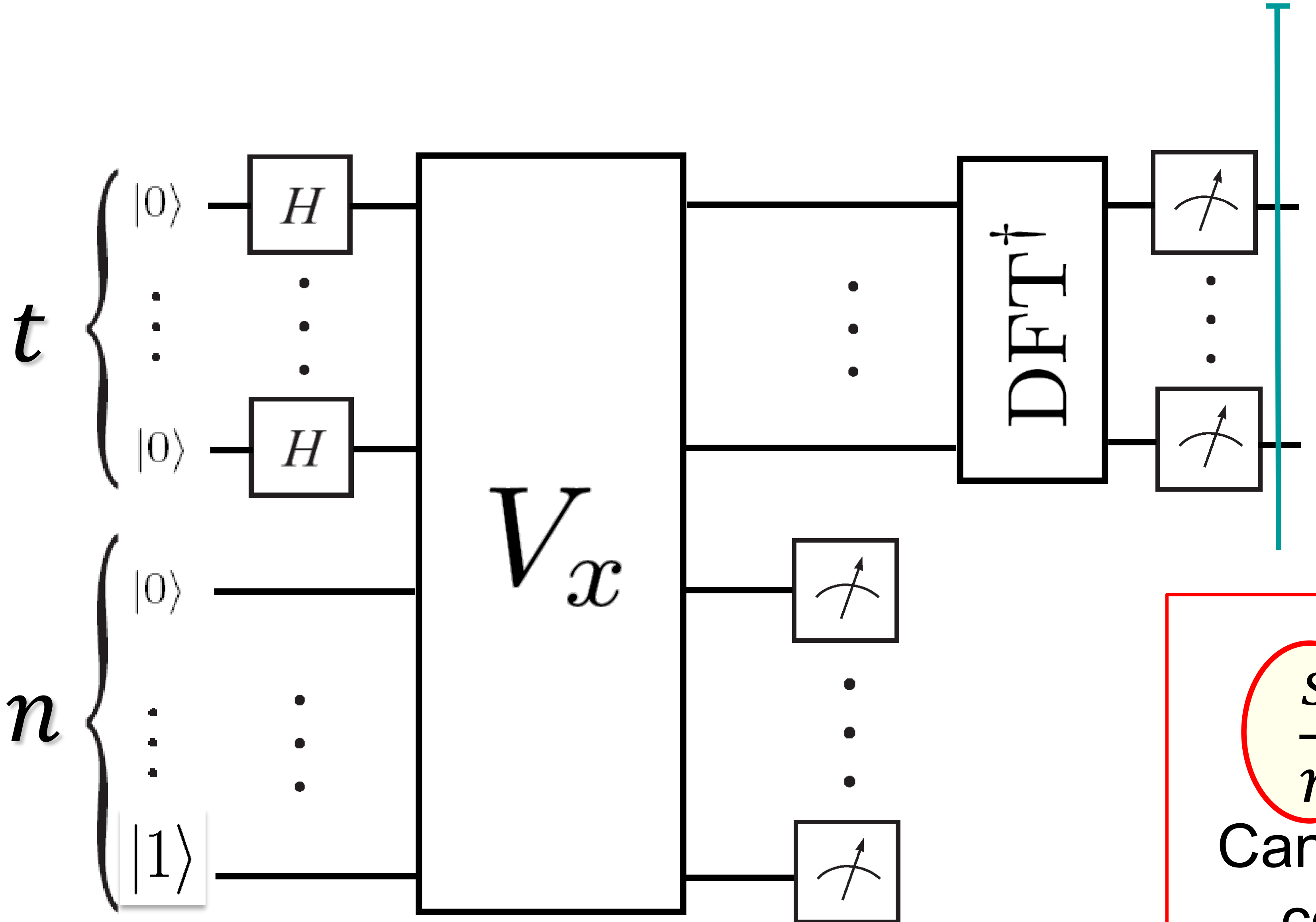


$\frac{s}{r}$ is rational

Can be estimated using continued fractions

Shor's algorithm [Shor '94] - **Step by step**

4. Measure to obtain $\frac{s}{r}$



A candidate for the period!

$\frac{s}{r}$ is rational

Can be estimated using continued fractions

Shor's algorithm [Shor '94]

- Shor also proposed how to solve the

Discrete logarithm problem

Input: $g, b = g^s \in \mathbb{Z}_p^*$ where $g^p = 1,\ s \in \{0,1,\dots,p-1\}$.
Problem: Find s.

Shor's algorithm [Shor '94]

- Shor also proposed how to solve the

Discrete logarithm problem

Input: $g, b = g^s \in \mathbb{Z}_p^*$ where $g^p = 1,\ s \in \{0,1,\dots,p-1\}$.
Problem: Find s.

Main Idea

$ss,1)$
$f\colon \mathbb{Z}\ p \times \mathbb{Z}\ p\ \to \mathbb{Z}\ p * ff\colon \mathbb{Z}\ p\ \mathbb{Z}\ \mathbb{Z}\ p\ pp\ \mathbb{Z}\ p \times \mathbb{Z}\ p\ \mathbb{Z}\ \mathbb{Z}\ p$
$pp\ \mathbb{Z}\ p\ \to \mathbb{Z}\ f\colon \mathbb{Z}\ p \times \mathbb{Z}\ p\ \to \mathbb{Z}\ p * pp\ f\colon \mathbb{Z}\ p \times \mathbb{Z}\ p\ \to \mathbb{Z}$
$p * * f\colon \mathbb{Z}\ p \times \mathbb{Z}\ p\ \to \mathbb{Z}\ p * ,\ ff\ x,y\ xx,yy\ x,y = g\ x\ gg$
$g\ x\ xx\ g\ x\ \ b\ {-y}\ bb\ b\ {-y}\ {-yy}\ b\ {-y}$

, $f(x,y) = g^x b^{-y}$
f is periodic with period $(s,1)$

Shor’s algorithm [Shor ’94]

- Shor also proposed how to solve the

Discrete logarithm problem

Input: $g, b = g^s \in \mathbb{Z}_p^*$ where $g^p = 1,\ s \in \{0,1,\dots,p-1\}$.
Problem: Find s.

Main Idea

$ss,1)$
$f: \mathbb{Z}\ p \times \mathbb{Z}\ p\ \ \to \mathbb{Z}\ p *\ ff: \mathbb{Z}\ p\ \mathbb{Z}\ \mathbb{Z}\ p\ pp\ \mathbb{Z}\ p \times \mathbb{Z}\ p\ \mathbb{Z}\ \mathbb{Z}\ p$
$pp\ \mathbb{Z}\ p\ \ \to \mathbb{Z}\ f: \mathbb{Z}\ p \times \mathbb{Z}\ p\ \ \to \mathbb{Z}\ p * pp\ f: \mathbb{Z}\ p \times \mathbb{Z}\ p\ \ \to \mathbb{Z}$
$p * * f: \mathbb{Z}\ p \times \mathbb{Z}\ p\ \ \to \mathbb{Z}\ p *,\ \ ff\ x,y\ xx,yy\ x,y = g\ x\ gg$
$g\ x\ xx\ g\ x\ \ b - y\ bb\ b - y - yy\ b - y$

$, \ f(x,y) = g^x b^{-y}$
f is periodic with period $(s, 1)$
Again reduce the problem to period finding!!!

Shor's algorithm [Shor '94]

- Shor also proposed how to solve the

Discrete logarithm problem

Input: $g, b = g^s \in \mathbb{Z}_p^*$ where $g^p = 1,\ s \in \{0,1,\ldots,p-1\}$.

Problem: Find s.

Classical algorithms

Various number/function field sieve algorithms

$$e^{O(n^{1/3}\,(\log n)^{2/3})}$$

(Subexponential complexity where $n \approx \log p$)

$\mathbb{Z}\ \mathbb{Z}\ p\ pp\ \mathbb{Z}\ p \times \mathbb{Z}\ p\ \mathbb{Z}\ \mathbb{Z}\ p$

$p * pp\ f: \mathbb{Z}\ p \times \mathbb{Z}\ p \ \to \mathbb{Z}$

$f\ x,y\ xx,yy\ x,y = g\ x\ gg$

$b\ -y$

$, \ f(x,y) = g^x b^{-y}$

f is periodic with period $(s, 1)$

Again reduce the problem to period finding!!!

Shor's algorithm [Shor '94]

- Shor also proposed how to solve the

Discrete logarithm problem

Input: $g, b = g^s \in \mathbb{Z}_p^*$ where $g^p = 1,\ s \in \{0,1,\ldots,p-1\}$.
Problem: Find s.

Classical algorithms

Various number/function field sieve algorithms

$$e^{O(n^{1/3}\,(\log n)^{\,2/3})}$$

(Subexponential complexity where $n \approx \log p$)

Shor's algorithm

$$O(n^2 \log n \log\log n)$$

(Polynomial complexity where $n \approx \log p$)

, $f(x,y) = g^x b^{-y}$

f is periodic with period $(s, 1)$

Again reduce the problem to period finding!!!

Shor's algorithm for discrete log [Shor '94]

Setup

An implementation of the unitary
$U\colon |x\rangle|y\rangle|z\rangle \longmapsto |x\rangle|y\rangle|z + f(x,y)\rangle$, where $f(x,y) = g^x b^{-y}$

1. $0\rangle|0\rangle|0\rangle$ - initial state
2. $\longrightarrow \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}|x\rangle|y\rangle|0\rangle$ - superposition
3. $\longrightarrow \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}|x\rangle|y\rangle|f(x,y)\rangle$ - apply U
4. $\longrightarrow \frac{1}{\sqrt{p}}\sum_{l=0}^{p-1}|sl/p\rangle|l/p\rangle|\hat{f}\,(sl,l)\rangle$ - apply inverse Fourier transform
5. $\longrightarrow sl/p, l/p$ – measure first two registers
6. If p is known, easy to find s, otherwise use continuous fraction algorithm

Shor's algorithm for discrete log [Shor '94]

Setup

$sl l/p p, l l/p p$ – measure first two registers

1 p 1 1 p p p pp p 1 p l=0 p−1 | sl/p | l/p | f (sl,l) ll=0 l=0 p−1 | sl/p | l/p | f (sl,l) pp−1 l=0 p−1 | sl/p | l/p | f (sl,l) | l/p | l/p ll/pp l/p | f (sl,l) f ff f ($ssll$,ll) f (sl,l) l=0 p −1 | sl/p | l/p | f (sl,l) - apply inverse Fourier transform

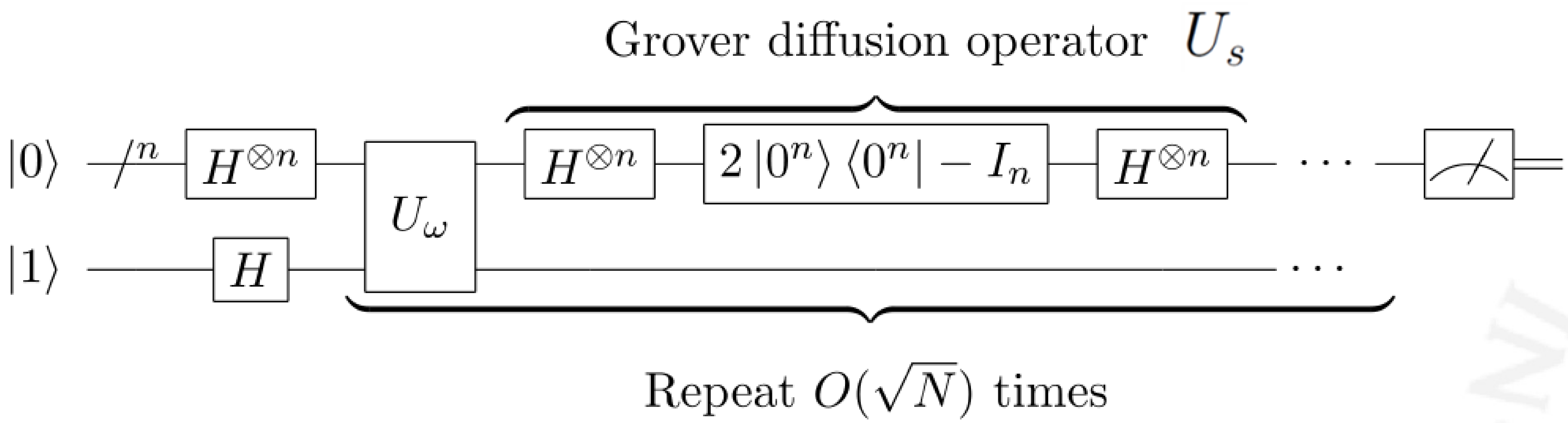
Procedure

1 2 n 1 1 2 n 2 n 2 2 n nn 2 n 1 2 n x=0 2 n −1 y=0 2 n −1 | x | y | f(x,y) xx=0 x=0 2 n −1 y=0 2 n −1 | x | y | f(x,y) 2 n 2 2 n nn 2 n −1 x=0 2 n −1 y=0 2 n −1 | x | y | f(x,y) y=0 2 n −1 | x | y | f(x,y) yy=0 y=0 2 n −1 | x | y | f(x,y) 2 n 2 2 n nn 2 n −1 y=0 2 n −1 | x | y | f(x,y) | x xx x | y yy y | f(x,y) f f(xx,yy) f(x,y) y=0 2 n −1 | x | y | f(x,y) x=0 2 n −1 y=0 2 n −1 | x | y | f(x,y) - apply UU

1 2 n 1 1 2 n 2 n 2 2 n nn 2 n 1 2 n x=0 2 n −1 y=0 2 n −1 | x | y | 0 xx=0 x=0 2 n −1 y=0 2 n −1 | x | y | 0 2 n 2 2 n nn 2 n −1 x=0 2 n −1 y=0 2 n −1 | x | y | 0 y=0 2 n −1 | x | y | 0 yy=0 y=0 2 n −1 | x | y | 0 2 n 2 2 n nn 2 n −1 y=0 2 n −1 | x | y | 0 | x xx x | y yy y | 0 0 0 y=0 2 n −1 | x | y | 0 x=0 2 n −1 y=0 2 n −1 | x | y | 0 superposition

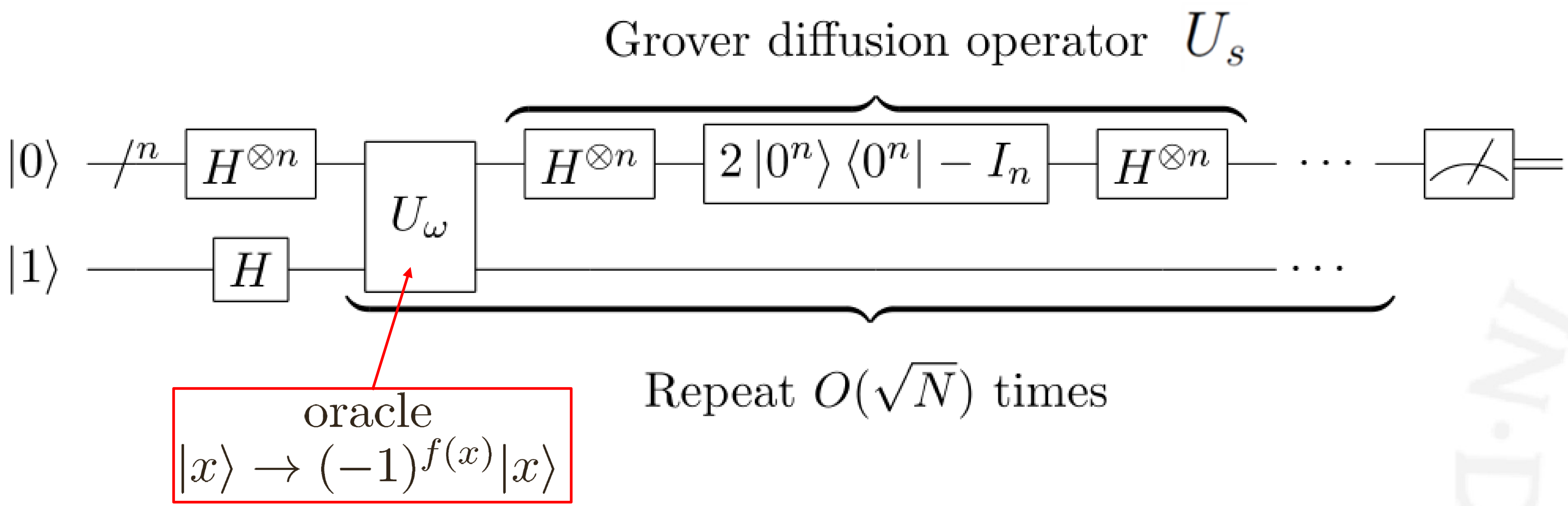
Grover's algorithm [Grover '96]

$$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|s\rangle\langle s| - I$$



Grover’s algorithm [Grover ’96]

$$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|s\rangle\langle s| - I$$

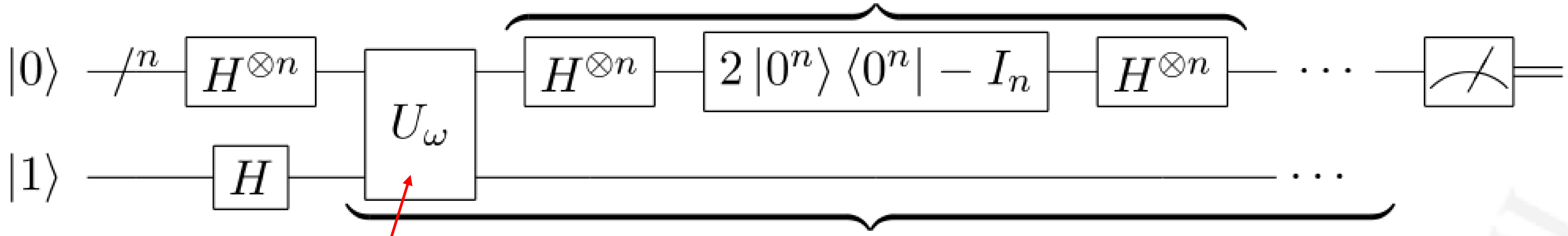


Recognizes a solution
of the search problem

Grover's algorithm [Grover '96]

$$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|s\rangle\langle s| - I$$

Grover diffusion operator U_s



Repeat $O(\sqrt{N})$ times

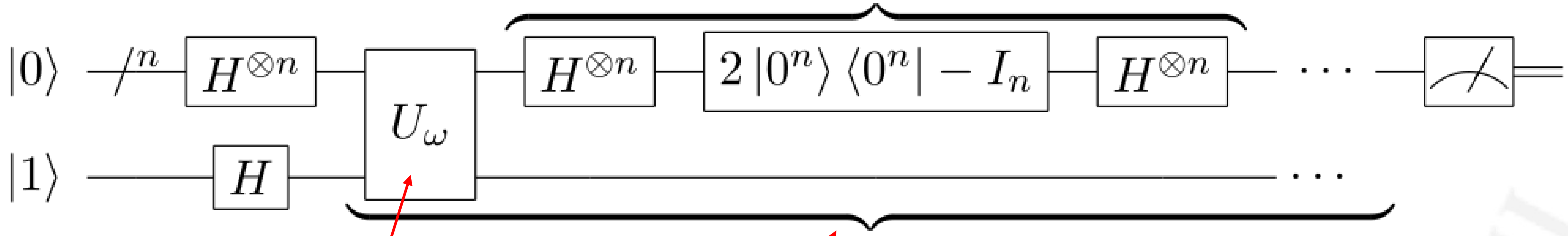
oracle
$|x\rangle \rightarrow (-1)^{f(x)}|x\rangle$

Recognizes a solution
of the search problem

Grover’s algorithm [Grover ’96]

$$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|s\rangle\langle s| - I$$

Grover diffusion operator U_s



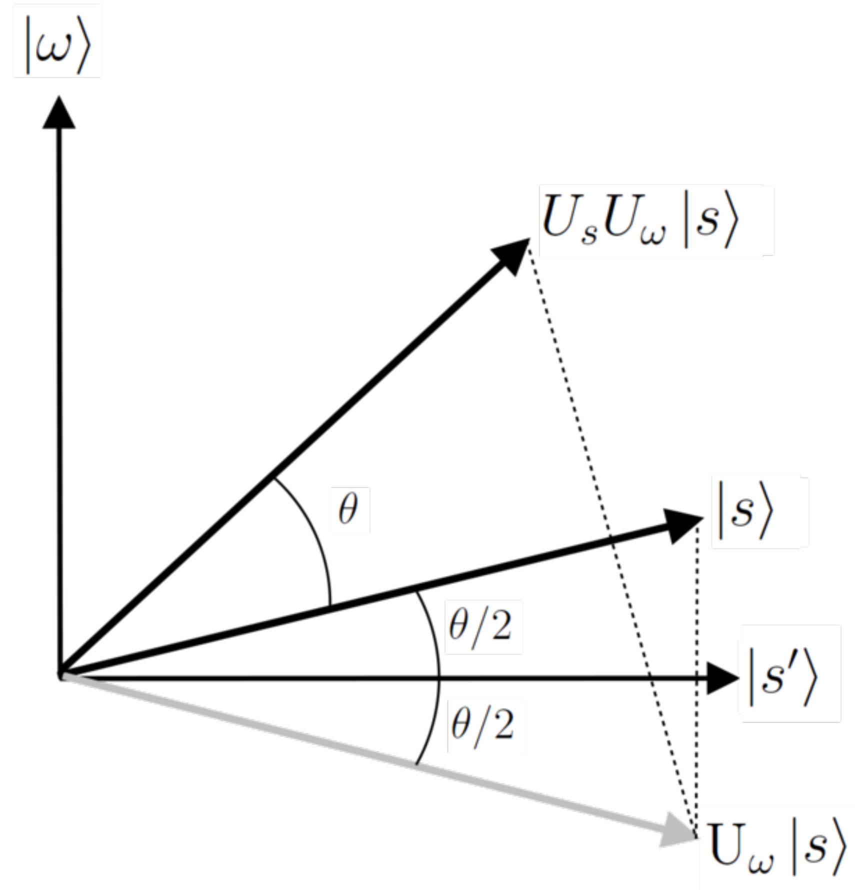
oracle
$|x\rangle \rightarrow (-1)^{f(x)}|x\rangle$

Repeat $O(\sqrt{N})$ times

Recognizes a solution of the search problem

Moves the state vector closer to the solution space

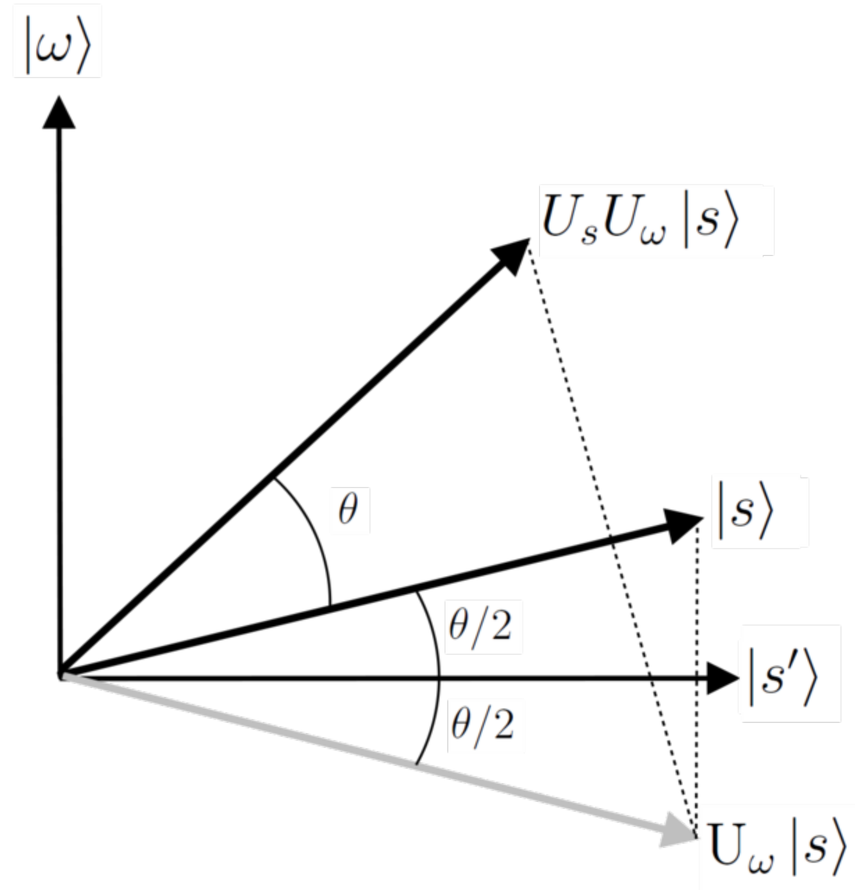
Grover's algorithm [Grover '96]



(For simplicity: One solution)

- $|\omega\rangle$ - solution, $|s'\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq \omega} |x\rangle$ - not solutions
- $|s\rangle = \sqrt{\frac{N-1}{N}} |s'\rangle + \sqrt{\frac{1}{N}} |\omega\rangle$
- $U_\omega |s\rangle = \sqrt{\frac{N-1}{N}} |s'\rangle - \sqrt{\frac{1}{N}} |\omega\rangle$ - action of the oracle
- $U_s U_\omega |s\rangle = \frac{N-4}{N} \sqrt{\frac{N-1}{N}} |s'\rangle - \frac{3N-4}{N} \sqrt{\frac{1}{N}} |\omega\rangle$

Grover's algorithm [Grover '96]

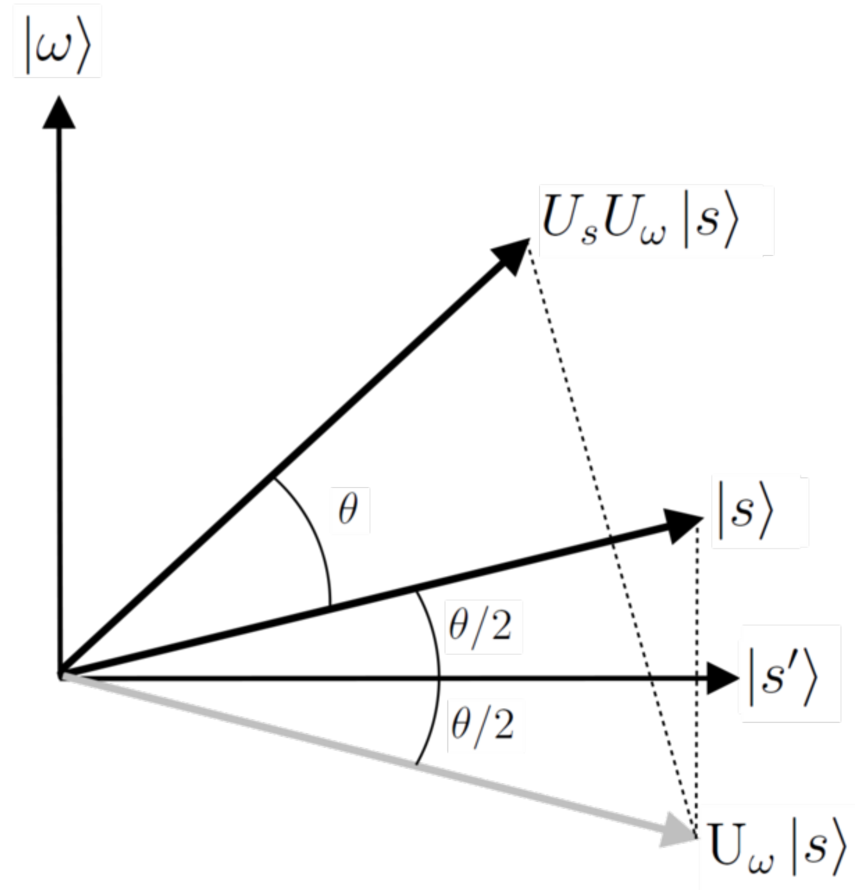


(For simplicity: One solution)

- $|\omega\rangle$ - solution, $|s'\rangle = \frac{1}{\sqrt{N-1}}\sum_{x\neq\omega}|x\rangle$ - not solutions
- $|s\rangle = \sqrt{\frac{N-1}{N}}|s'\rangle + \sqrt{\frac{1}{N}}|\omega\rangle$
- $U_\omega|s\rangle = \sqrt{\frac{N-1}{N}}|s'\rangle - \sqrt{\frac{1}{N}}|\omega\rangle$ - action of the oracle
- $U_s U_\omega|s\rangle = \frac{N-4}{N}\sqrt{\frac{N-1}{N}}|s'\rangle - \frac{3N-4}{N}\sqrt{\frac{1}{N}}|\omega\rangle$

Increase of amplitude of solution space

Grover's algorithm [Grover '96]



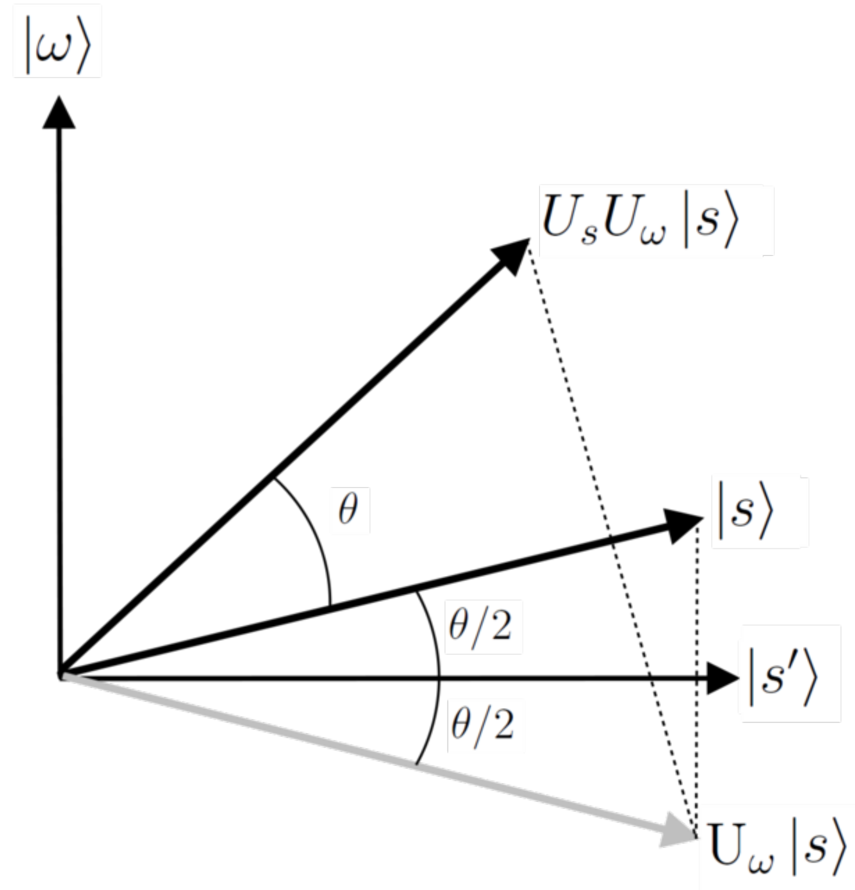
(For simplicity: One solution)

- $|\omega\rangle$ - solution, $|s'\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq \omega} |x\rangle$ - not solutions
- $|s\rangle = \sqrt{\frac{N-1}{N}} |s'\rangle + \sqrt{\frac{1}{N}} |\omega\rangle$
- $U_\omega |s\rangle = \sqrt{\frac{N-1}{N}} |s'\rangle - \sqrt{\frac{1}{N}} |\omega\rangle$ - action of the oracle
- $U_s U_\omega |s\rangle = \frac{N-4}{N} \sqrt{\frac{N-1}{N}} |s'\rangle - \frac{3N-4}{N} \sqrt{\frac{1}{N}} |\omega\rangle$

Increase of amplitude of solution space

$$\boxed{|s\rangle = \cos\frac{\theta}{2}|s'\rangle + \sin\frac{\theta}{2}|\omega\rangle \mapsto \cos\frac{3\theta}{2}|s'\rangle + \sin\frac{3\theta}{2}|\omega\rangle \mapsto \cdots \mapsto \cos\frac{(2r+1)\theta}{2}|s'\rangle + \sin\frac{(2r+1)\theta}{2}|\omega\rangle}$$

Grover’s algorithm [Grover ’96]



(For simplicity: One solution)

- $|\omega\rangle$ - solution, $|s'\rangle = \frac{1}{\sqrt{N-1}}\sum_{x\neq\omega}|x\rangle$ - not solutions
- $|s\rangle = \sqrt{\frac{N-1}{N}}|s'\rangle + \sqrt{\frac{1}{N}}|\omega\rangle$
- $U_\omega|s\rangle = \sqrt{\frac{N-1}{N}}|s'\rangle - \sqrt{\frac{1}{N}}|\omega\rangle$ - action of the oracle
- $U_s U_\omega|s\rangle = \frac{N-4}{N}\sqrt{\frac{N-1}{N}}|s'\rangle - \frac{3N-4}{N}\sqrt{\frac{1}{N}}|\omega\rangle$

Increase of amplitude of solution space

$$\boxed{|s\rangle = \cos\frac{\theta}{2}|s'\rangle + \sin\frac{\theta}{2}|\omega\rangle \mapsto \cos\frac{3\theta}{2}|s'\rangle + \sin\frac{3\theta}{2}|\omega\rangle \mapsto \cdots \mapsto \cos\frac{(2r+1)\theta}{2}|s'\rangle + \sin\frac{(2r+1)\theta}{2}|\omega\rangle}$$

After $r \approx \pi\sqrt{N}/4$ rounds the solution is obtained with great probability!

Summary of quantum algorithms

Based on **Quantum Fourier Transform**	**Based on** **Amplitude amplification**

Summary of quantum algorithms

Based on **Quantum Fourier Transform**	**Based on** **Amplitude amplification**

- *Shor's algorithm ('94)*
  - ***Integer factorization problem***
  - ***Discrete logarithm problem***
  - Superpolynomial speedup over classical algorithms

Summary of quantum algorithms

Based on
Quantum Fourier Transform

- *Shor's algorithm ('94)*
  - ***Integer factorization problem***
  - ***Discrete logarithm problem***
  - Superpolynomial speedup over classical algorithms

Based on
Amplitude amplification

- *Grover's algorithm ('96)*
  - Searching an unsorted database
  - Quadratic speedup over classical algorithms

Summary of quantum algorithms

Based on
Quantum Fourier Transform

- *Shor's algorithm ('94)*
  - ***Integer factorization problem***
  - ***Discrete logarithm problem***
  - Superpolynomial speedup over classical algorithms
- *Abelian hidden subgroup problem*
  - Superpolynomial speedup over classical algorithms

Based on
Amplitude amplification

- *Grover's algorithm ('96)*
  - Searching an unsorted database
  - Quadratic speedup over classical algorithms

Summary of quantum algorithms

Based on
Quantum Fourier Transform

- ***Shor's algorithm ('94)***
  - ***Integer factorization problem***
  - ***Discrete logarithm problem***
  - Superpolynomial speedup over classical algorithms
- ***Abelian hidden subgroup problem***
  - Superpolynomial speedup over classical algorithms

Based on
Amplitude amplification

- ***Grover's algorithm ('96)***
  - Searching an unsorted database
  - Quadratic speedup over classical algorithms
- ***Collision finding problem (Brassard et al. '97)***
  - Polynomial (3/2) speedup over classical algorithms

Summary of quantum algorithms

Based on
Quantum Fourier Transform

- *Shor's algorithm ('94)*
  - ***Integer factorization problem***
  - ***Discrete logarithm problem***
  - Superpolynomial speedup over classical algorithms
- *Abelian hidden subgroup problem*
  - Superpolynomial speedup over classical algorithms
-
-
-

Based on
Amplitude amplification

- *Grover's algorithm ('96)*
  - Searching an unsorted database
  - Quadratic speedup over classical algorithms
- *Collision finding problem (Brassard et al. '97)*
  - Polynomial (3/2) speedup over classical algorithms
-
-
-

Why do we care so much about these algorithms?

Based on
Quantum Fourier Transform

- *Shor's algorithm ('94)*
  - ***Integer factorization problem***
  - ***Discrete logarithm problem***
  - Superpolynomial speedup over classical algorithms
- *Abelian hidden subgroup problem*
  - Superpolynomial speedup over classical algorithms
-
-
-

Based on
Amplitude amplification

- *Grover's algorithm ('96)*
  - Searching an unsorted database
  - Quadratic speedup over classical algorithms
- *Collision finding problem (Brassard et al. '97)*
  - Polynomial (3/2) speedup over classical algorithms
-
-
-

Why do we care so much about these algorithms?

Based on
Quantum Fourier Transform

- *Shor's algorithm ('94)*
  - ***Integer factorization problem***
  - ***Discrete logarithm problem***
  - Superpolynomial speedup over classical algorithms
- *Abelian hidden subgroup problem*
  - Superpolynomial speedup over classical algorithms

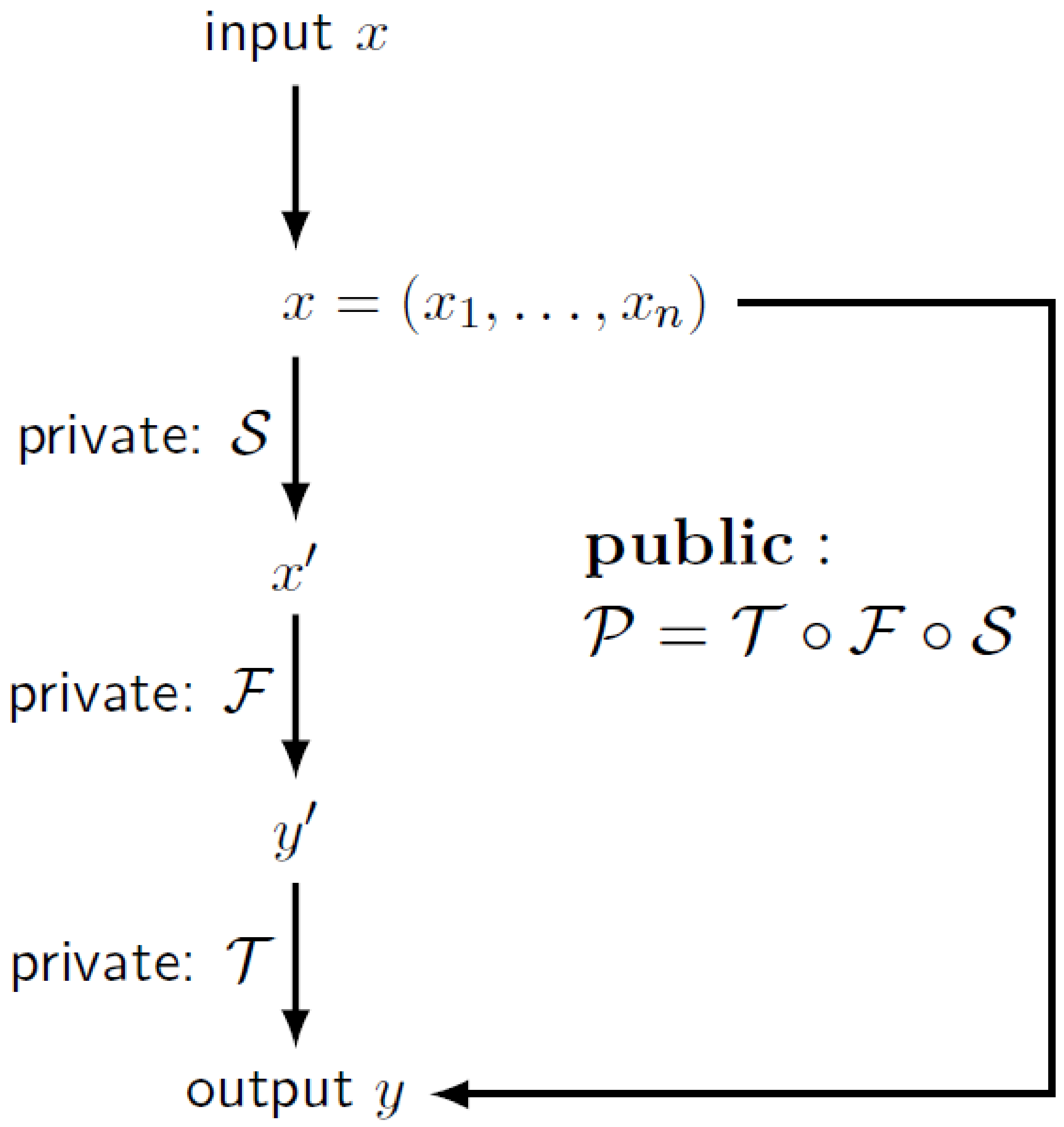
Based on
Amplitude amplification

- *Grover's algorithm ('96)*
  - Searching an unsorted database
  - Quadratic speedup over classical algorithms
- *Collision finding problem (Brassard et al. '97)*
  - Polynomial (3/2) speedup over classical algorithms

If they are ever practically implemented → *Today's security infrastructure for any kind of data communication/ storage will be rendered worthless!?!*

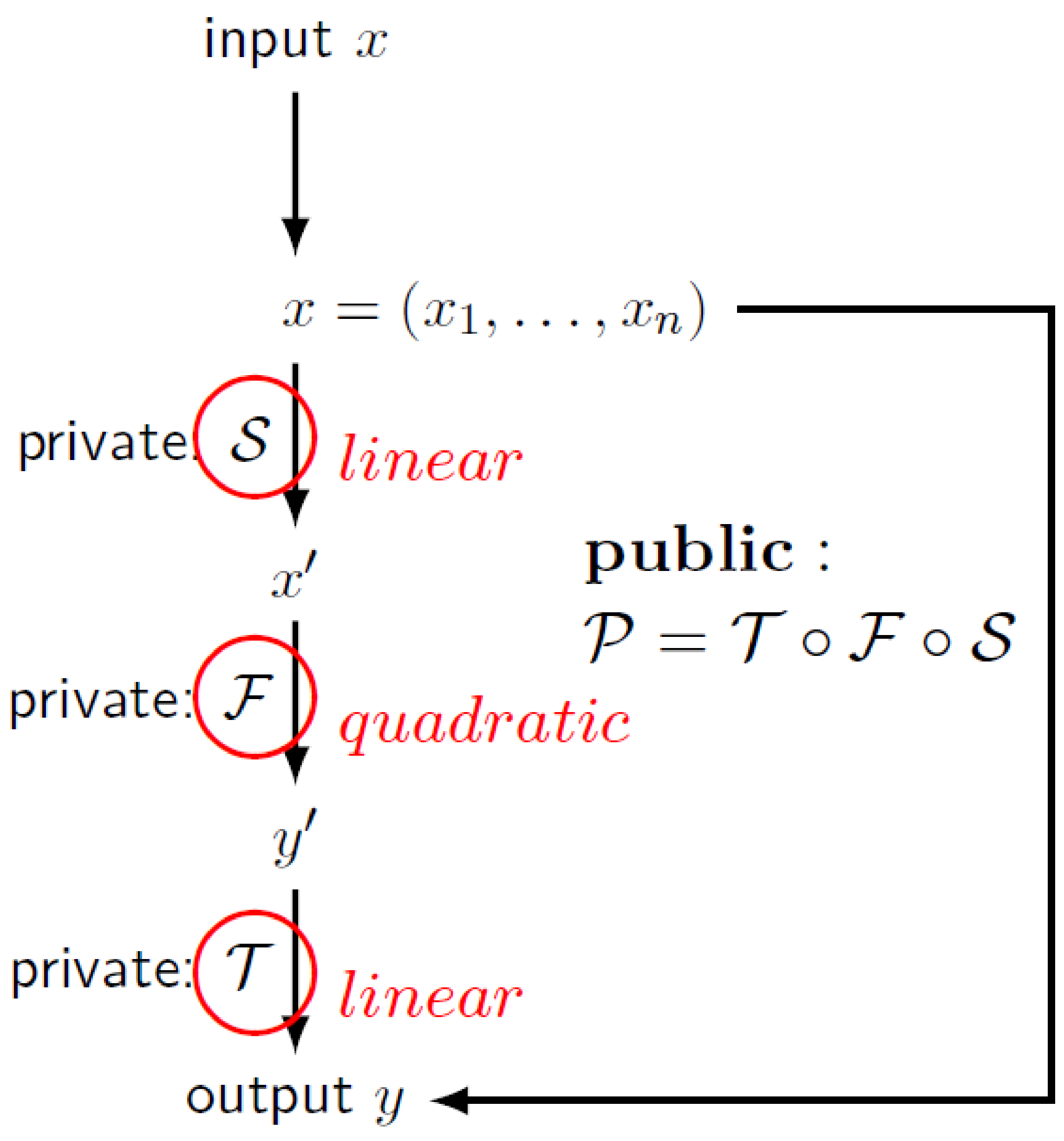
MQ (multivariate quadratic) Cryptosystems

- Hard underlying problem (NP hard): Polynomial system solving (PoSSo)
- (**Mainstream**) No reduction to the hard problem – related problems believed to be hard
- Confidence in signatures



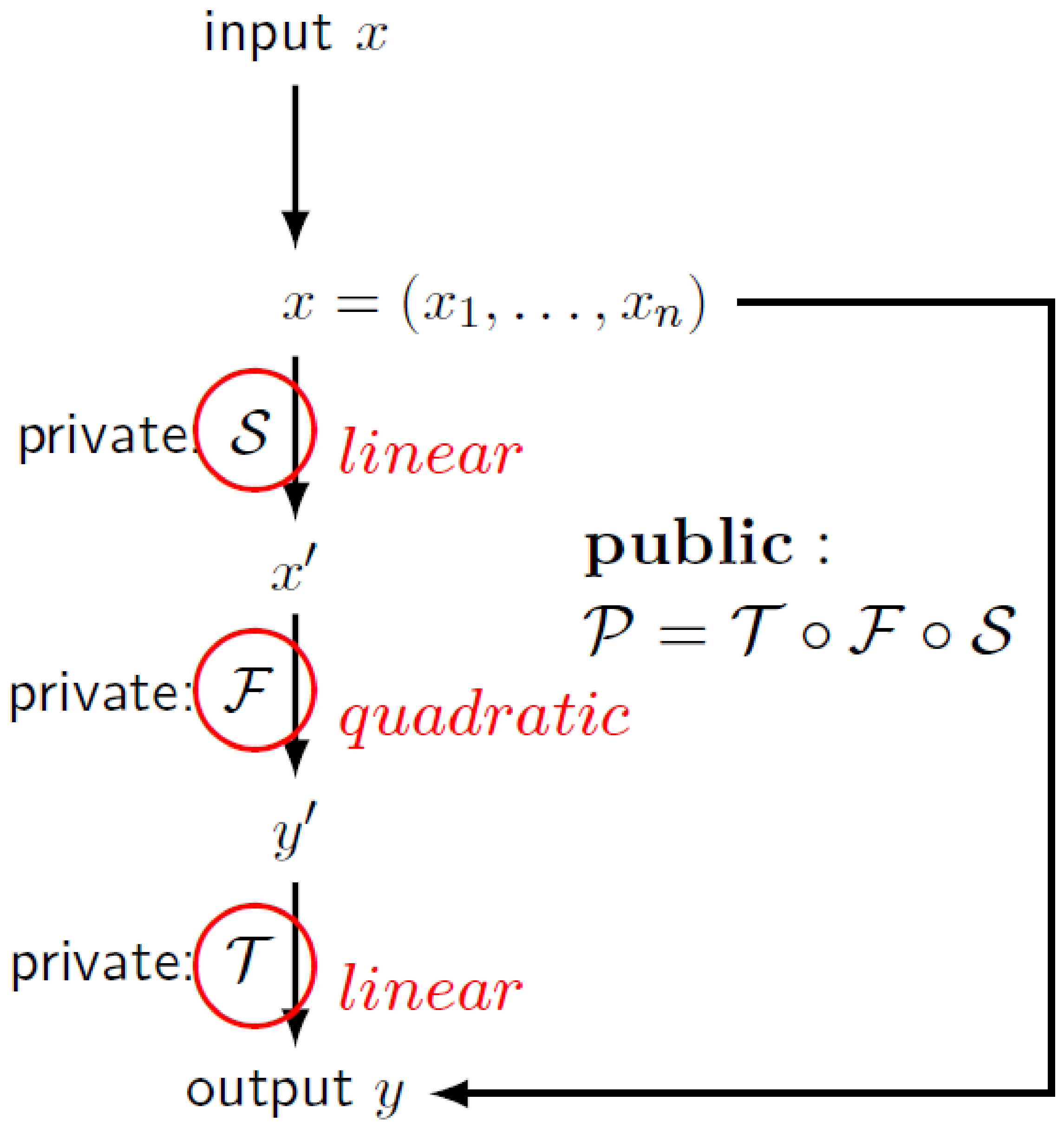
MQ (multivariate quadratic) Cryptosystems

- Hard underlying problem (NP hard): Polynomial system solving (PoSSo)
- (**Mainstream**) No reduction to the hard problem – related problems believed to be hard
- Confidence in signatures



MQ (multivariate quadratic) Cryptosystems

- Hard underlying problem (NP hard): Polynomial system solving (PoSSo)
- (**Mainstream**) No reduction to the hard problem – related problems believed to be hard
- Confidence in signatures

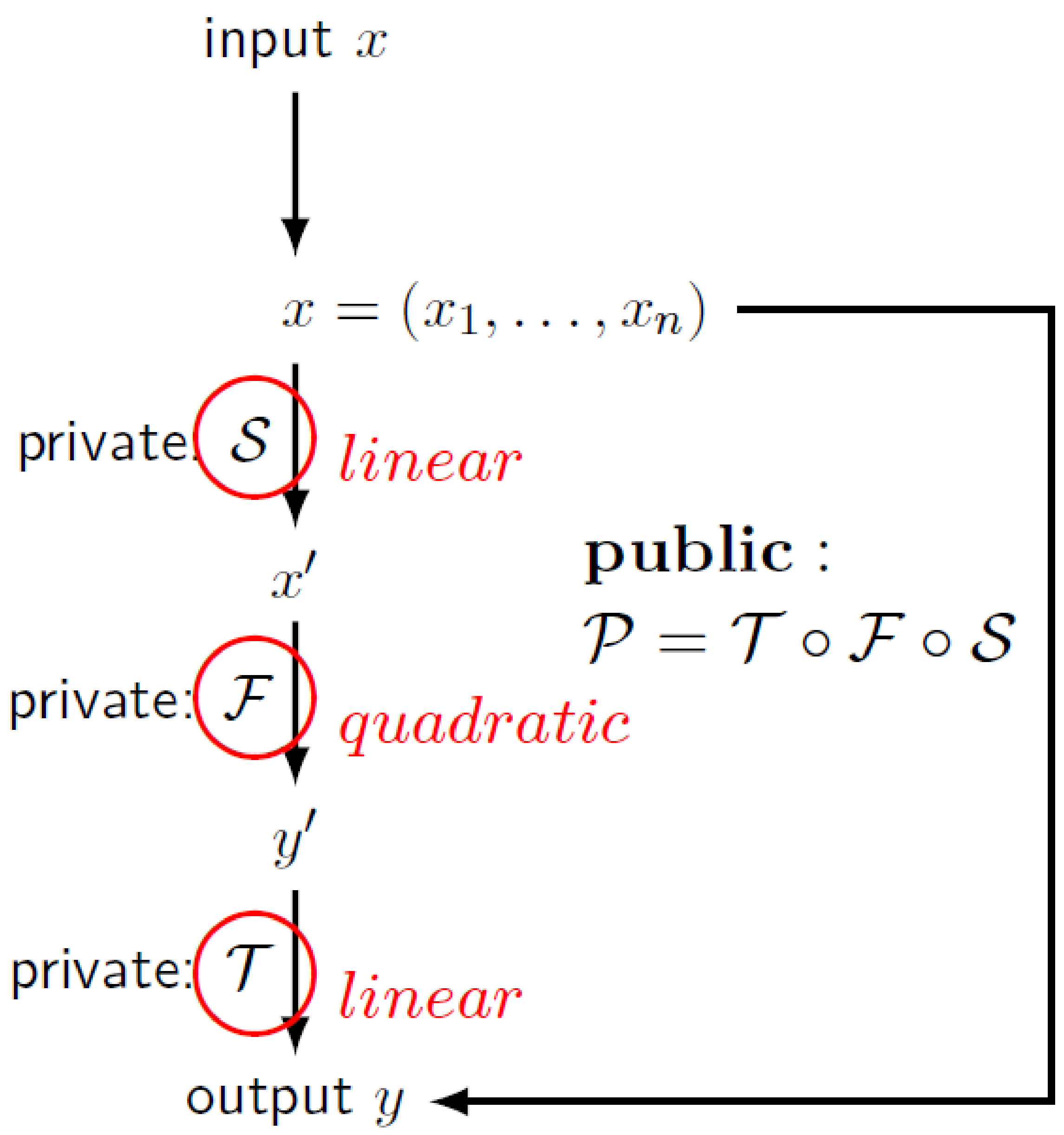


Public $\mathcal{P}$

$$p_1(x_1, \ldots, x_n)$$
$$p_2(x_1, \ldots, x_n)$$
$$\ldots$$
$$p_m(x_1, \ldots, x_n)$$

MQ (multivariate quadratic) Cryptosystems

- Hard underlying problem (NP hard): Polynomial system solving (PoSSo)
- (**Mainstream**) No reduction to the hard problem – related problems believed to be hard
- Confidence in signatures



$\mathcal{PoSSo}$:

Input:

$p_1, p_2, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$

Question:

Find - if any - $(u_1, \ldots, u_n) \in \mathbb{F}_q^n$ st.

$$\begin{cases} p_1(u_1, \ldots, u_n) = & 0 \\ p_2(u_1, \ldots, u_n) = & 0 \\ \quad \ldots & \\ p_m(u_1, \ldots, u_n) = & 0 \end{cases}$$

MQ (multivariate quadratic) Cryptosystems

- Fast, simple operations, short signatures 👍
- Large keys, no security proofs 👎
- Parameters for Gui [Petzoldt, Chen, Yang, Tao, Ding, 15], Rainbow [Ding, Schmidt, 04]
- Implementation [Chen, Li, Peng, Yang, Cheng, 17]

Security (post quantum)	Signature scheme	Public key (kB)	Private key (kB)	Signature size (bit)	Sign() k cycles	Verify() k cycles
80	Gui(GF(2),120,9,3,3,2)	110.7	3.8	129		
100	Gui(GF(2),161,9,6,7,2)	271.8	7.5	181		
128	GUI(4,120,17,8,8,2)	225.8	9.6	288	7,992.8	342.5
80	Rainbow(GF(256),19,12,13)	25.3	19.3	352		
100	Rainbow(GF(16),25,25,25)	65.9	43.2	288		
128	Rainbow(GF(31),28,28,28)	123.2	74.5	420	77.4	70.8

MQ (multivariate quadratic) Cryptosystems

- Hard underlying problem (NP hard): Polynomial system solving (PoSSo)

Two new provably secure signatures

- **MQDSS** [Chen, Hülsing, Rijneveld, S, Schwabe, 16] – security proof in the ROM
- **Sofia** [Chen, Hülsing, Rijneveld, S, Schwabe, 17] – security proof in the Quantum ROM

Security (post quantum)	Signature scheme	Public key (B)	Private key (B)	Signature size (KB)	Sign() k cycles	Verify() k cycles
128 (ROM)	MQDSS-31-64	72	64	40	8,510.6	5,752.6
128 (QROM)	Sofia-4-128	64	32	123	21,305.5	15,492.6

- Transform from provably secure Identification schemes

MQDSS

IDS

$\mathcal{P}$		$\mathcal{V}$
$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}_1}$	$\mathsf{ch}_1 \leftarrow_R \mathsf{ChS}_1(1^k)$
$\mathsf{resp}_1 \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1)$	$\xrightarrow{\mathsf{resp}_1}$	
	$\xleftarrow{\mathsf{ch}_2}$	$\mathsf{ch}_2 \leftarrow_R \mathsf{ChS}_2(1^k)$
$\mathsf{resp}_2 \leftarrow \mathcal{P}_2(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2)$	$\xrightarrow{\mathsf{resp}_2}$	
		$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$

$\downarrow \quad \downarrow \quad \downarrow$

FS signature

Signer	**Verifier**
$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$	
$\mathsf{ch}_1 \leftarrow H_1(m, \mathsf{com})$	$\mathsf{ch}_1 \leftarrow H_1(m, \mathsf{com})$
$\mathsf{resp}_1 \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1)$	$\mathsf{ch}_2 \leftarrow H_2(m, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1)$
$\mathsf{ch}_2 \leftarrow H_2(m, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1)$	$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$
$\mathsf{resp}_2 \leftarrow \mathcal{P}_2(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2)$	
	output : b
output : $\sigma = (\mathsf{com}, \mathsf{resp}_1, \mathsf{resp}_2)$	

Lattice-based Cryptosystems

- Encryption, signatures, key exchange
- Many different hard problems

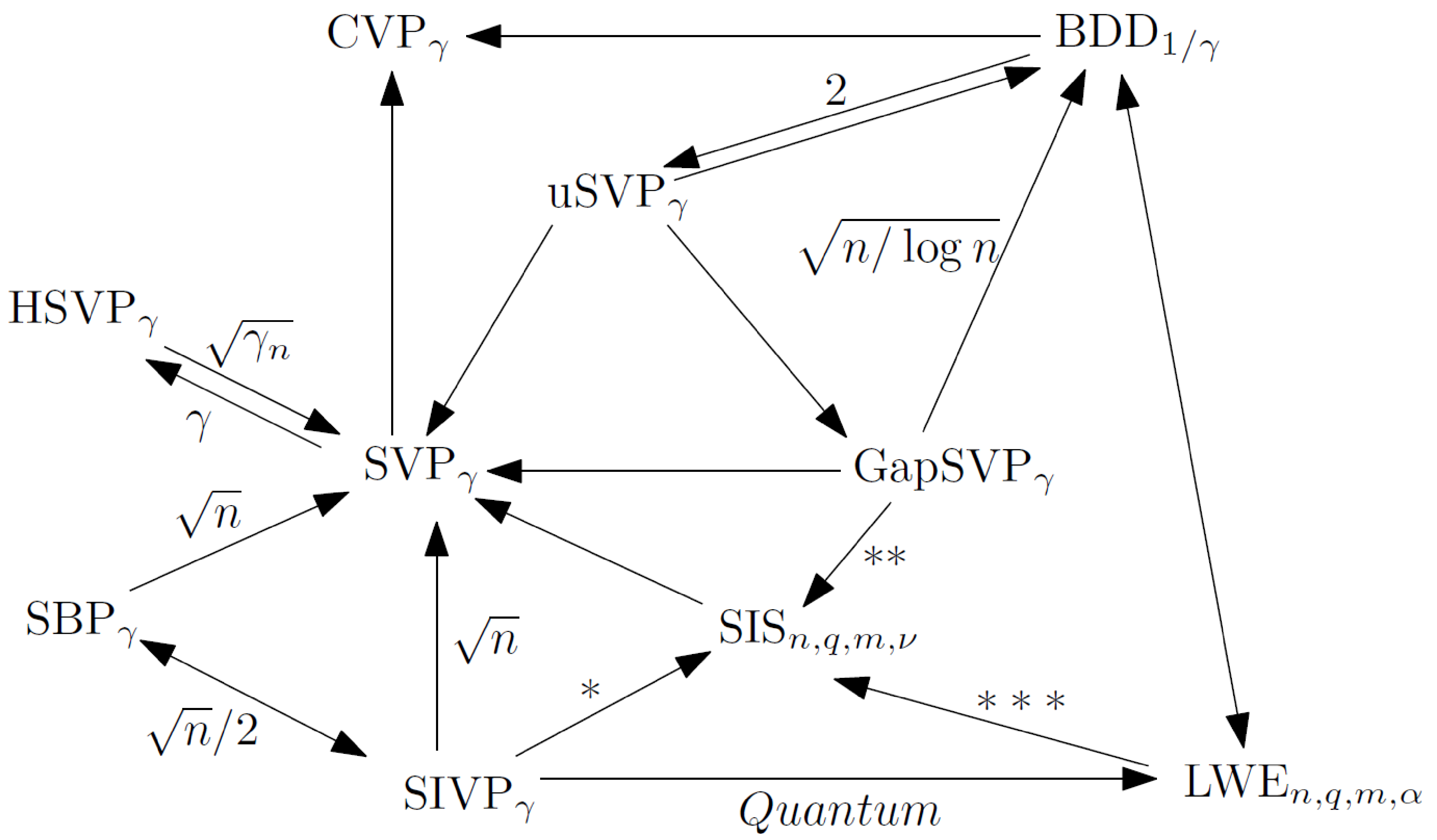


Fig. from Joop van de Pol's MSc-thesis

Lattice-based Cryptosystems

- Learning with errors (LWE)
- Variants R-LWE, Module-LWE, LPN, …
  - Additional structure undermines security claims

- Let $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^n + 1)$
- Let χ be an *error distribution* on $\mathcal{R}_q$
- Let $\mathbf{s} \in \mathcal{R}_q$ be secret
- Attacker is given pairs $(\mathbf{a}, \mathbf{as} + \mathbf{e})$ with
  - $\mathbf{a}$ uniformly random from $\mathcal{R}_q$
  - $\mathbf{e}$ sampled from χ
- Task for the attacker: find $\mathbf{s}$
- Common choice for χ: discrete Gaussian

Lattice-based Cryptosystems

- Learning with errors (LWE)
- Variants R-LWE, Module-LWE, LPN, …
  - Additional structure undermines security claims

- Let $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^n+1)$
- Let χ be an *error distribution* on $\mathcal{R}_q$
- Let $\mathbf{s} \in \mathcal{R}_q$ be secret
- Attacker is given pairs $(\mathbf{a}, \mathbf{as}+\mathbf{e})$ with
  - $\mathbf{a}$ uniformly random from $\mathcal{R}_q$
  - $\mathbf{e}$ sampled from χ
- Task for the attacker: find $\mathbf{s}$
- Common choice for χ: discrete Gaussian

Alice (server)		Bob (client)
$\mathbf{s}, \mathbf{e} \xleftarrow{\$} \chi$		$\mathbf{s}', \mathbf{e}' \xleftarrow{\$} \chi$
$\mathbf{b} \leftarrow \mathbf{as}+\mathbf{e}$	$\xrightarrow{\mathbf{b}}$	$\mathbf{u} \leftarrow \mathbf{as}'+\mathbf{e}'$
	$\xleftarrow{\mathbf{u}}$	

$$\begin{array}{llll} \text{Alice has} & \mathbf{v} & = \mathbf{us} & = \mathbf{ass}' + \mathbf{e}'\mathbf{s} \\ \text{Bob has} & \mathbf{v}' & = \mathbf{bs}' & = \mathbf{ass}' + \mathbf{es}' \end{array}$$

Lattice-based Cryptosystems

- Learning with errors (LWE)
- Variants R-LWE, Module-LWE, LPN, …
  - Additional structure undermines security claims

- Let $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^n + 1)$
- Let χ be an *error distribution* on $\mathcal{R}_q$
- Let $\mathbf{s} \in \mathcal{R}_q$ be secret
- Attacker is given pairs $(\mathbf{a}, \mathbf{as} + \mathbf{e})$ with
  - $\mathbf{a}$ uniformly random from $\mathcal{R}_q$
  - $\mathbf{e}$ sampled from χ
- Task for the attacker: find $\mathbf{s}$
- Common choice for χ: discrete Gaussian

Alice (server)		Bob (client)
$\mathbf{s}, \mathbf{e} \xleftarrow{\$} \chi$		$\mathbf{s}', \mathbf{e}' \xleftarrow{\$} \chi$
$\mathbf{b} \leftarrow \mathbf{as} + \mathbf{e}$	$\xrightarrow{\mathbf{b}}$	$\mathbf{u} \leftarrow \mathbf{as}' + \mathbf{e}'$
	$\xleftarrow{\mathbf{u}}$	

$$\begin{aligned} &\text{Alice has} \quad \mathbf{v} &&= \mathbf{us} &&= \mathbf{ass}' + \mathbf{e}'\mathbf{s} \\ &\text{Bob has} \quad \mathbf{v}' &&= \mathbf{bs}' &&= \mathbf{ass}' + \mathbf{es}' \end{aligned}$$

approximately same

small

Lattice-based Cryptosystems

- FRODO [Bos, Costello, Ducas, Mironov, Naehrig, Nikolaenko, Raghunathan, Stebila, 16]
- NewHope [Alkim, Ducas, Pöppelmann, Schwabe, 16]
  - Google Experiment for Chrome 2016: New hope + X25519 used in Chrome Canary for access to some Google services
- NTRU Prime [Bernstein, Chuengsatiansup, Lange, van Vredendaal, 16]
- Kyber [Bos, Ducas, Kiltz, Lepoint, Lyubashevsky, Schanck, Schwabe, Stehlé, 17]

Scheme	Security bits/(type)	Hard problem	KeyGen (cycles)	Enc (cycles)	Dec (cycles)	Public key (bytes)	Private key (bytes)	Ciphertext (bytes)
FRODO	130 (pass.)	LWE	2 938 K	3 484 K	338 K	11 296	11280	11288
NewHope	255 (pass.)	Ring-LWE	88 920	110 986	19 422	1824	1792	2048
NTRU Prime	129 (CCA)	NTRU like		> 51488		1232	1417	1141
Kyber	161 (CCA)	Module-LWE	77 892	119 652	125 736	1088	2400	1184

Hash-based Signatures

- **Only secure hash function needed** (security well understood, standard model proof)
- Merkle, 89

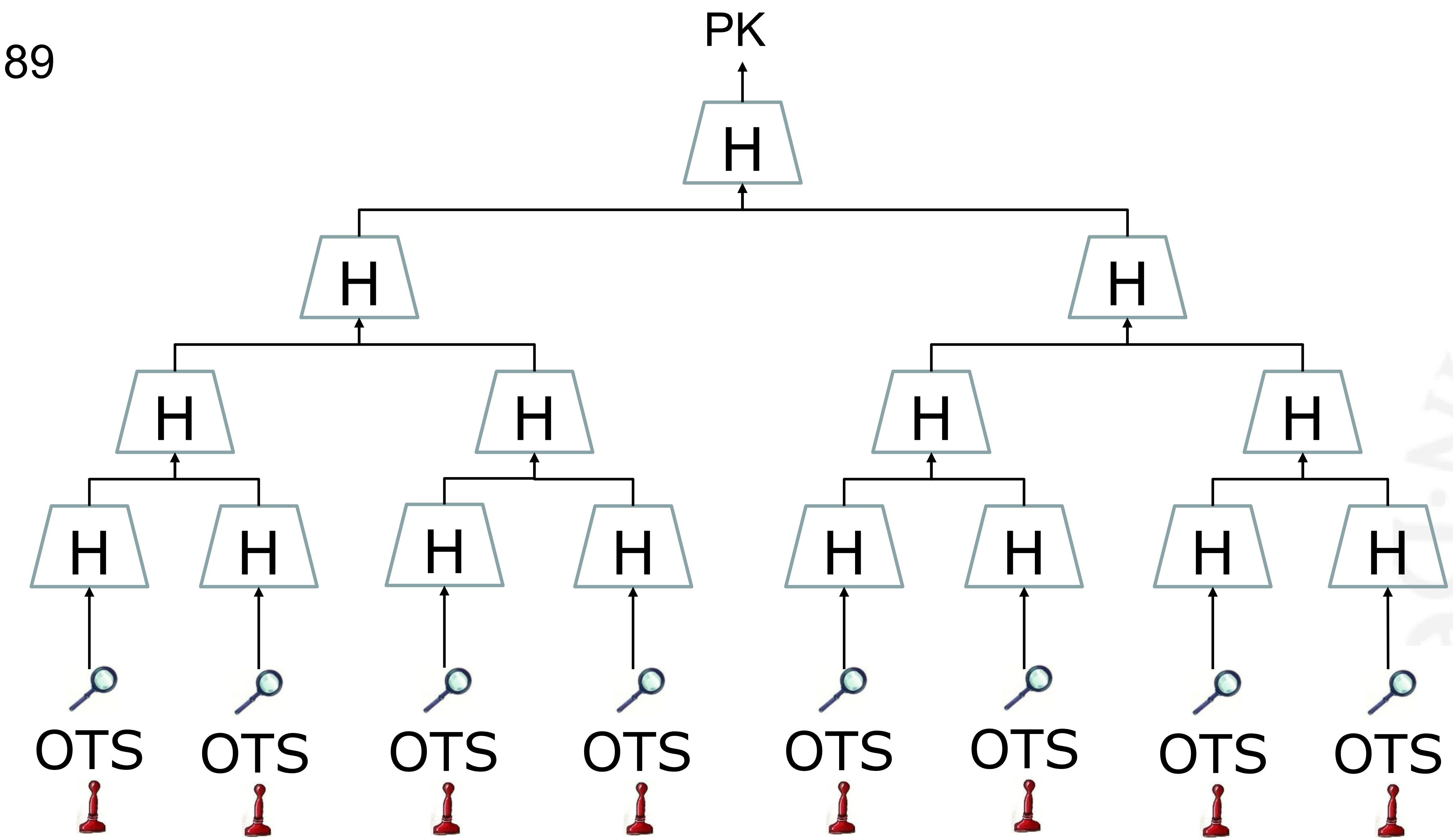


Figure: Andreas Hülsing

Hash-based Signatures

- **Only secure hash function needed** (security well understood, standard model proof)
- Merkle, 89

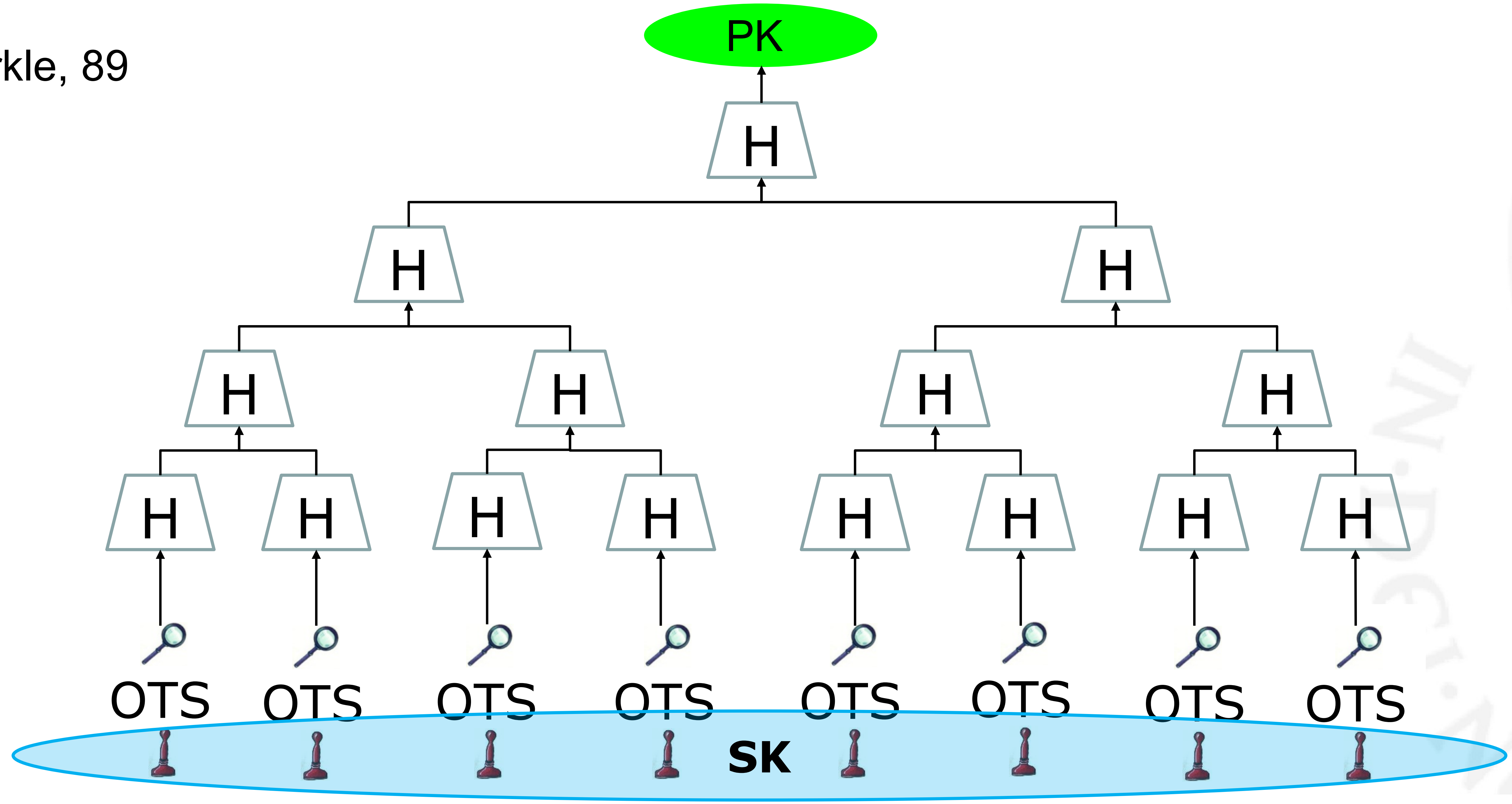


Figure: Andreas Hülsing

Hash-based Signatures

- **Only secure hash function needed** (security well understood, standard model proof)
- Merkle, 89

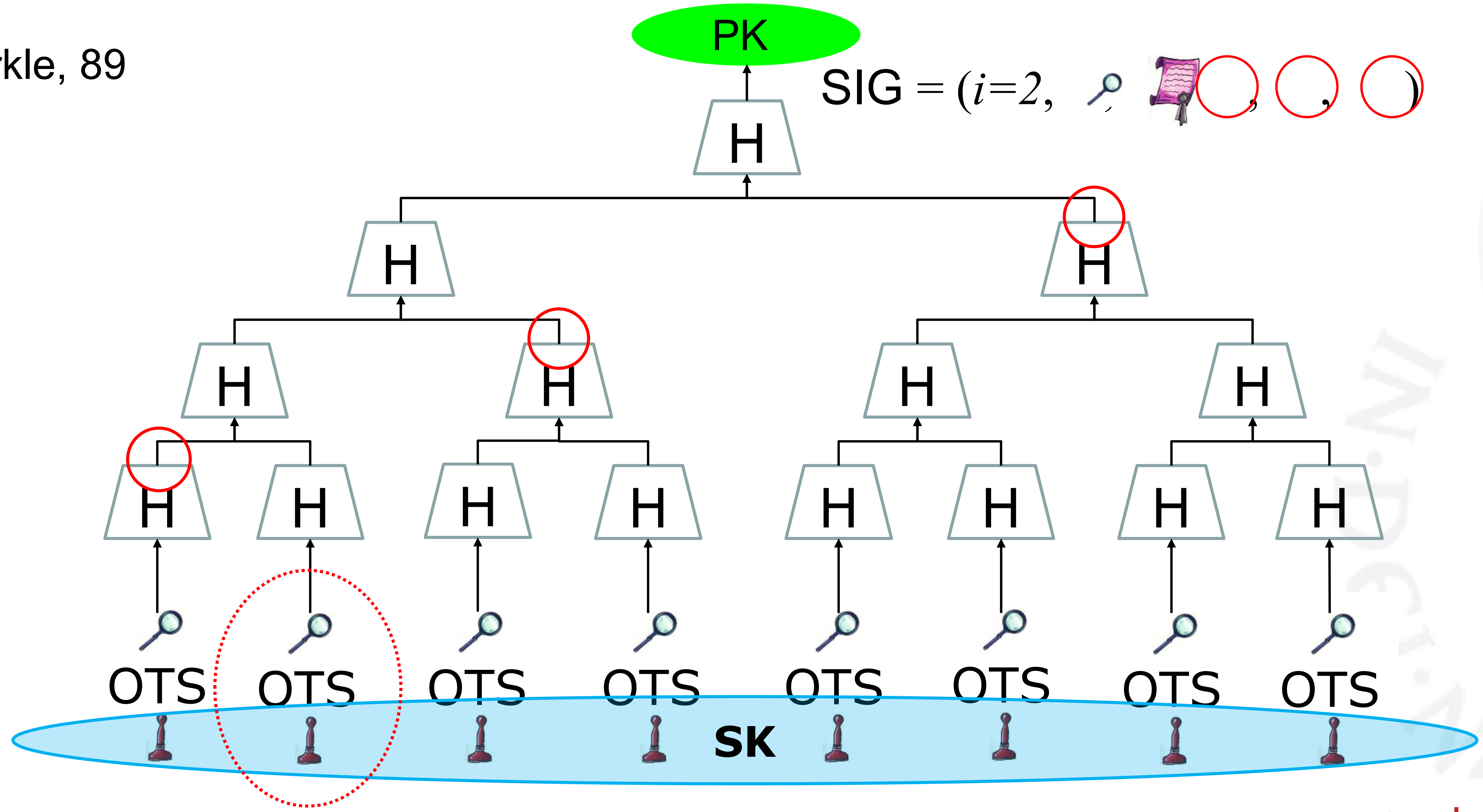


Figure: Andreas Hülsing

Hash-based Signatures

- Most trusted post quantum signatures
- Two Internet drafts (drafts for RFCs), one in „waiting for ISRG review“

- XMSS – stateful, but forward secrecy [Buchmann, Dahmen, Hülsing, 11]
- SPHINCS – stateless [Bernstein, Hopwood, Hülsing, Lange, Niederhagen, Papachristodoulou, Schneider, Schwabe, O’Hearn, 15]

	Sign (ms)	Verify (ms)	Signature (byte)	Public Key (byte)	Secret Key (byte)	Bit Security
XMSS-SHA-2	35.60	1.98	2084	1700	3,364	157
XMSS-AES-NI	0.52	0.07	2452	916	1,684	84
SPHINCS-256	13.56	0.39	41000	1056	1088	128

Challenges in Post Quantum Cryptography

- **Key sizes, signature sizes and speed**
  - Huge public keys, or signatures …. Or slow
  - ex. ECC 256b key vs McElliece 500KB key
  - ex. ECC 80B signature vs MQDSS 40KB signature
- **Software and hardware implementation**
  - Optimizations, physical security
- **Standardization**
  - What is the right choice of algorithm?
- **Deployment**
  - In TLS, DTLS, constrained devices, storage…
  - Will take a long time…

PQCRYPTO
ICT-645622

Thank you again for listening!