Post-Quantum Cryptography

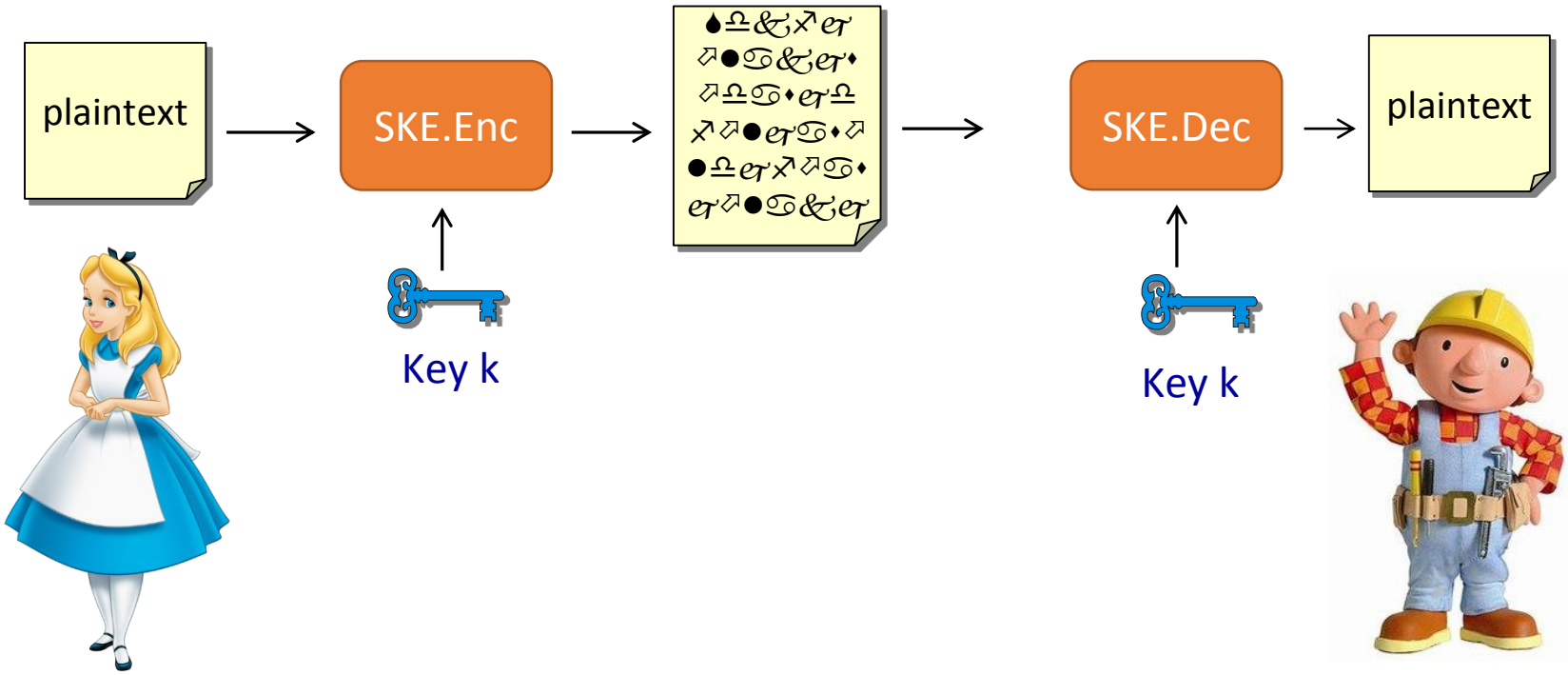
Andreas Hülsing

TU Eindhoven

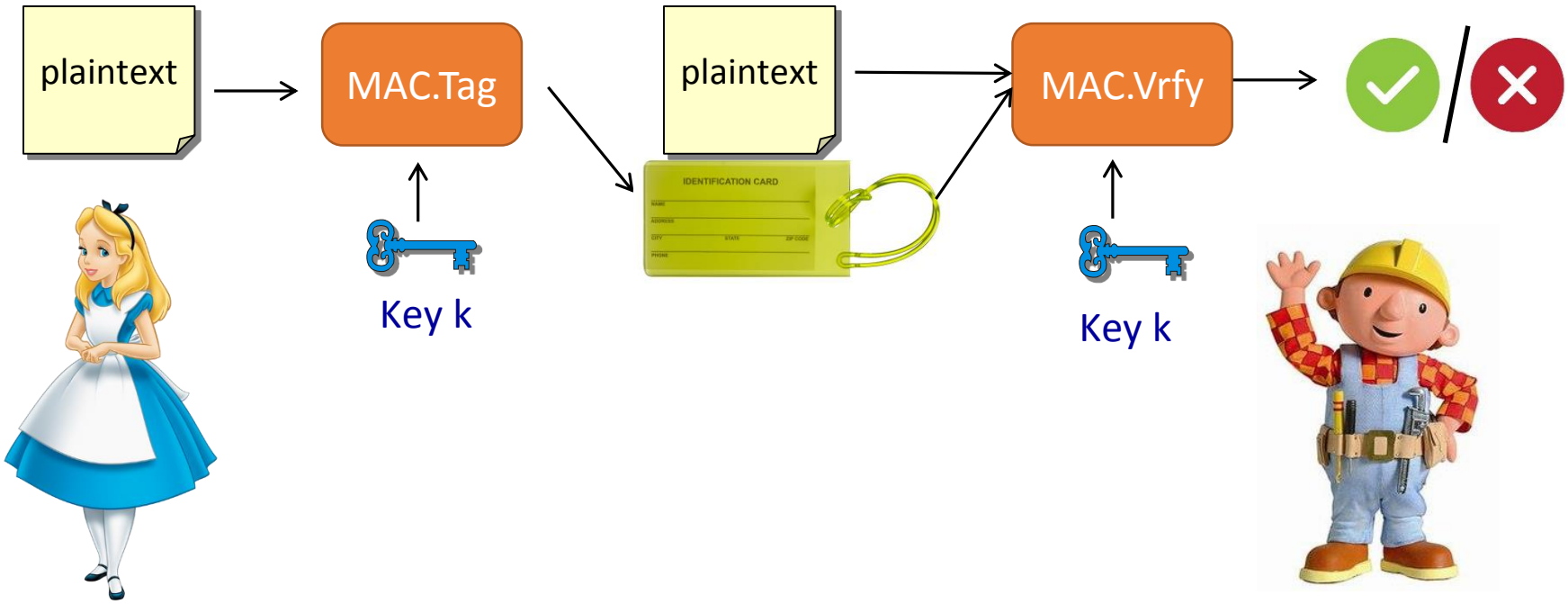
Quantum kills the Internet

Background: Cryptography

Secret key encryption (SKE)



Message authentication (MAC)



How to build secret key crypto?

- Random function sufficient (we need one-wayness)
- Attacks ≈ unstructured search
- How

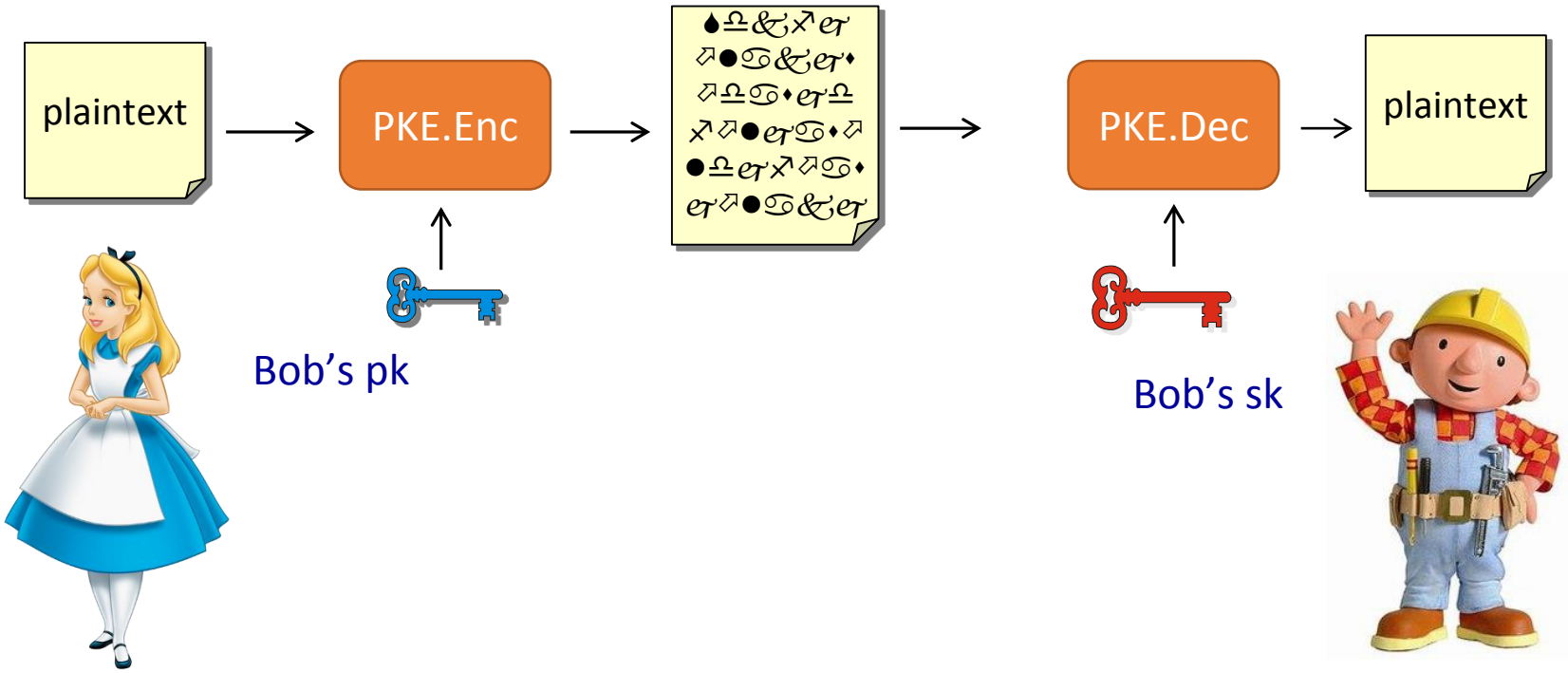
Spoiler:
Killed by quantum? Not that we know.
(but weakened)*

Engineering*

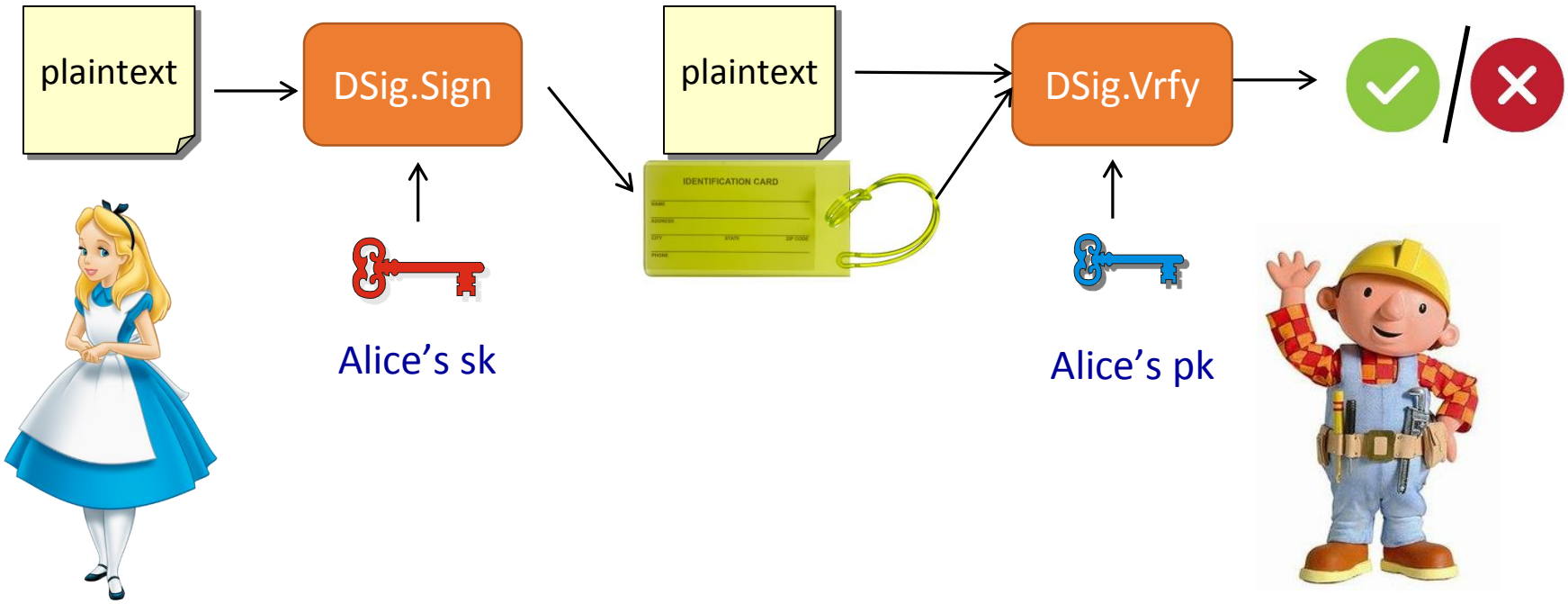
* Disclaimer: Massive simplification

How does Bob learn shared key k?

Public key encryption (PKE)



Digital Signature (DSig)



Applications

- Code signing (DSIG)
  - Software updates
  - Software distribution
  - Mobile code

- Communication security (DSIG, PKE / KEX /KEM)
  - TLS, SSH, IPSec, ...
  - eCommerce, online banking, eGovernment, ...
  - Private online communication

Communication security (simplified)

Hi

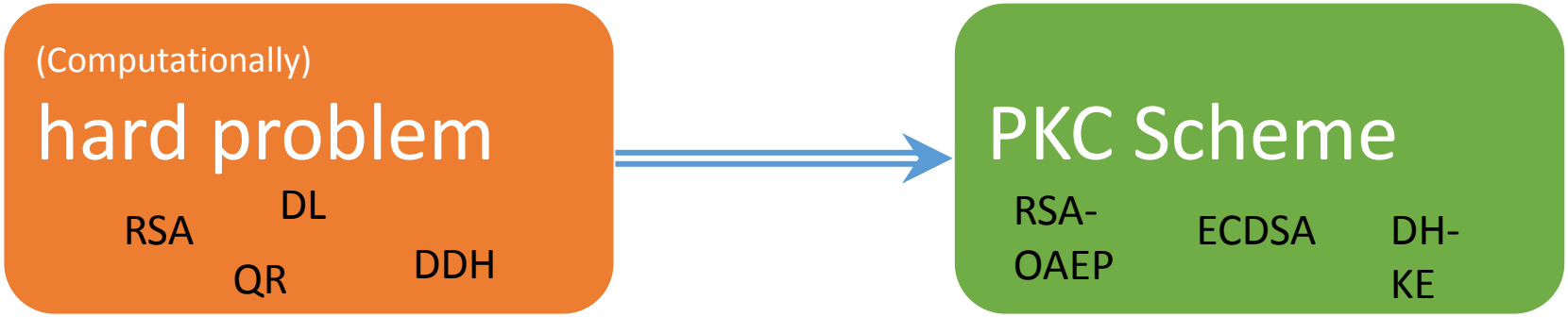
pk, Cert(pk belongs to shop)

PKC to establish shared secret sk

SKC secured communication using sk

The TEA SHOP
FINE TEAS & TISANES
PURE & BLENDED

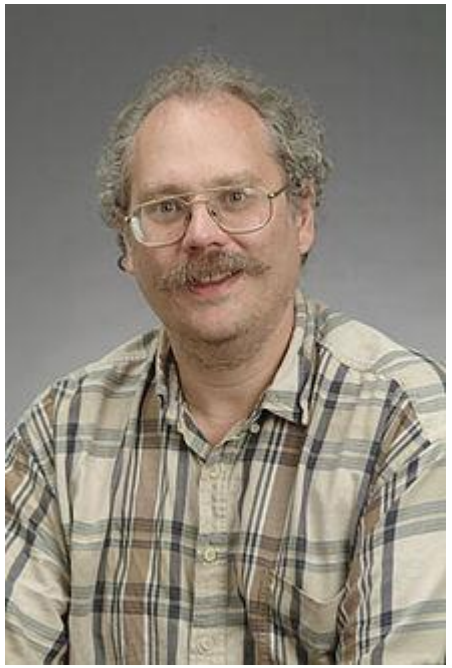
How to build PKC



The Quantum Threat

Shor‘s algorithm (1994)

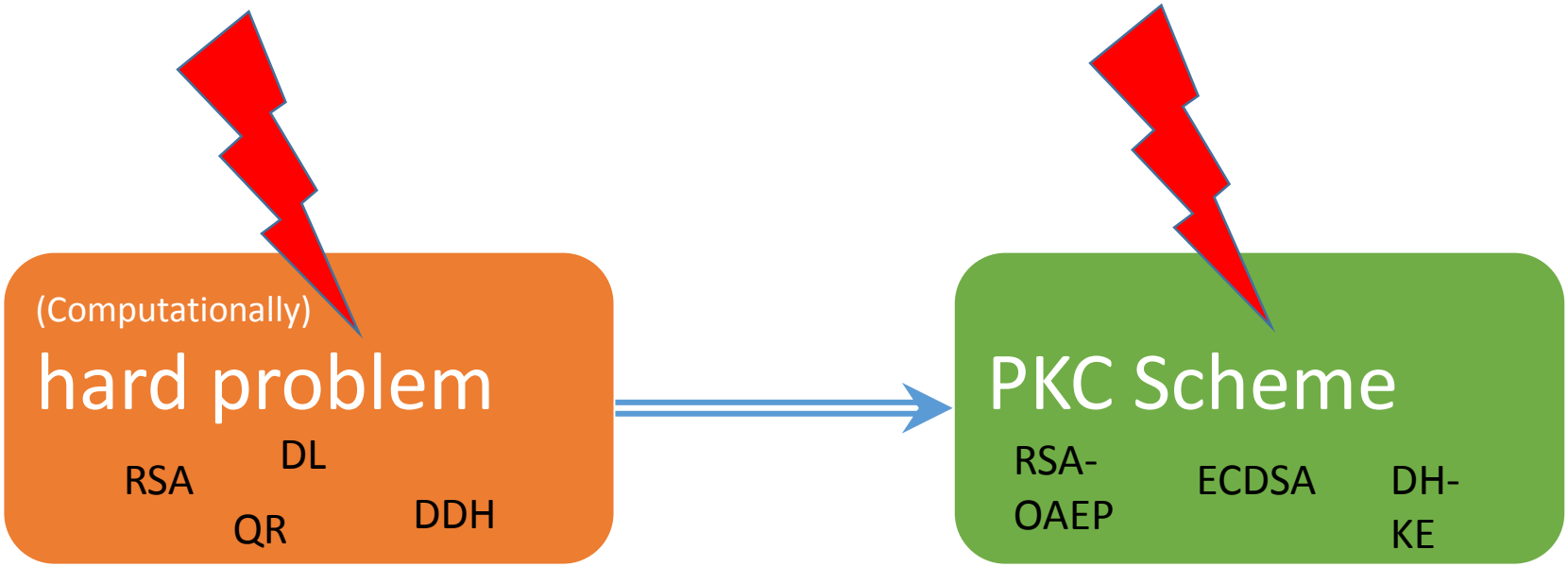
- Quantum computers can do FFT very efficiently
- Can be used to find period of a function
- This can be exploited to factor efficiently (RSA)
- Shor also shows how to solve discrete log efficiently (DSA, DH, ECDSA, ECDH)



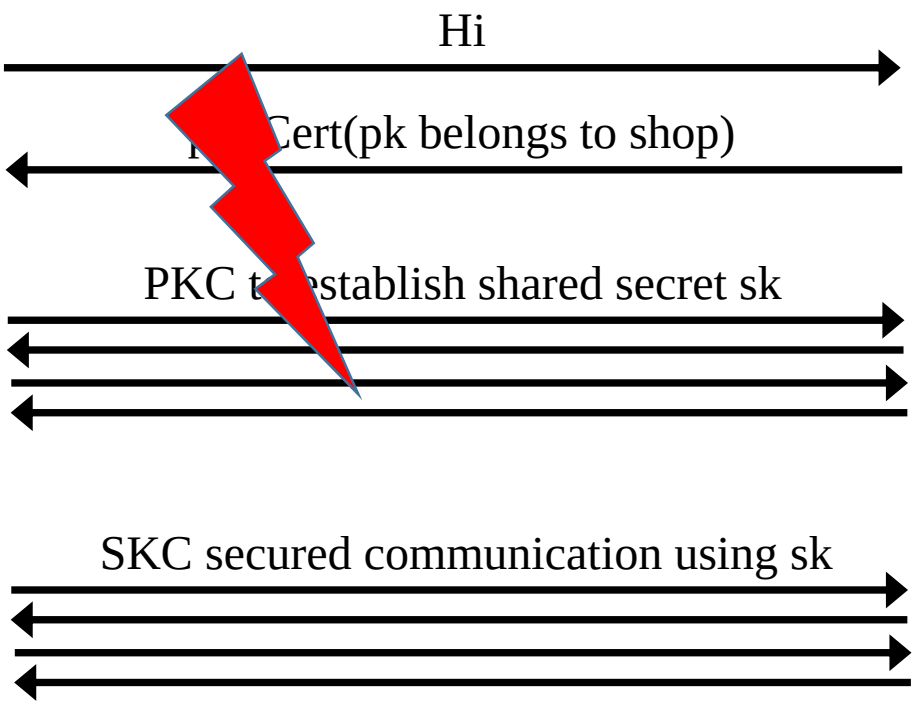
Grover‘s algorithm (1996)

- Quantum computers can search N entry DB in $\Theta(\sqrt{N})$
- Application to symmetric crypto
- Nice: Grover is provably optimal (For random function)
- Double security parameter.

How to build PKC

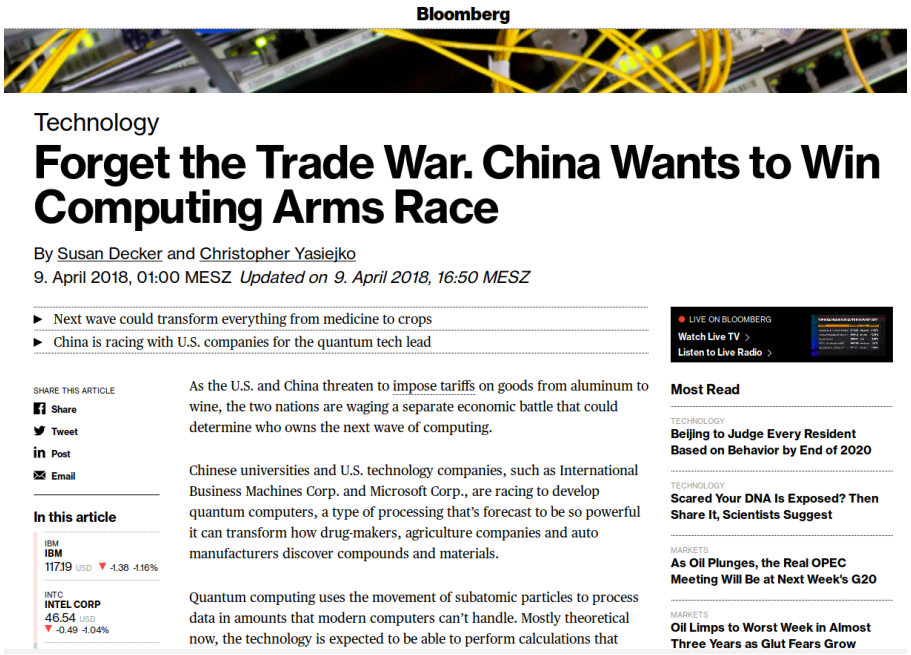


Communication security (simplified)



Why care today

- **EU** launched a one billion Euro project on quantum technologies
- Similar range is spent in **China**
- **US** administration passed a bill on spending $1.275 billion US dollar on quantum computing research
- **Google**, **IBM**, **Microsoft**, **Alibaba**, and others run their own research programs.



Bloomberg

Technology

Forget the Trade War. China Wants to Win Computing Arms Race

By Susan Decker and Christopher Yasiejko

9. April 2018, 01:00 MESZ *Updated on 9. April 2018, 16:50 MESZ*

- Next wave could transform everything from medicine to crops
- China is racing with U.S. companies for the quantum tech lead

SHARE THIS ARTICLE
Share
Tweet
Post
Email

In this article

IBM
IBM
117.19 USD ▼ -1.38 -1.16%

INTC
INTEL CORP
46.54 USD
▼ -0.49 -1.04%

As the U.S. and China threaten to impose tariffs on goods from aluminum to wine, the two nations are waging a separate economic battle that could determine who owns the next wave of computing.

Chinese universities and U.S. technology companies, such as International Business Machines Corp. and Microsoft Corp., are racing to develop quantum computers, a type of processing that's forecast to be so powerful it can transform how drug-makers, agriculture companies and auto manufacturers discover compounds and materials.

Quantum computing uses the movement of subatomic particles to process data in amounts that modern computers can't handle. Mostly theoretical now, the technology is expected to be able to perform calculations that

LIVE ON BLOOMBERG
Watch Live TV
Listen to Live Radio

Most Read

TECHNOLOGY
Beijing to Judge Every Resident Based on Behavior by End of 2020

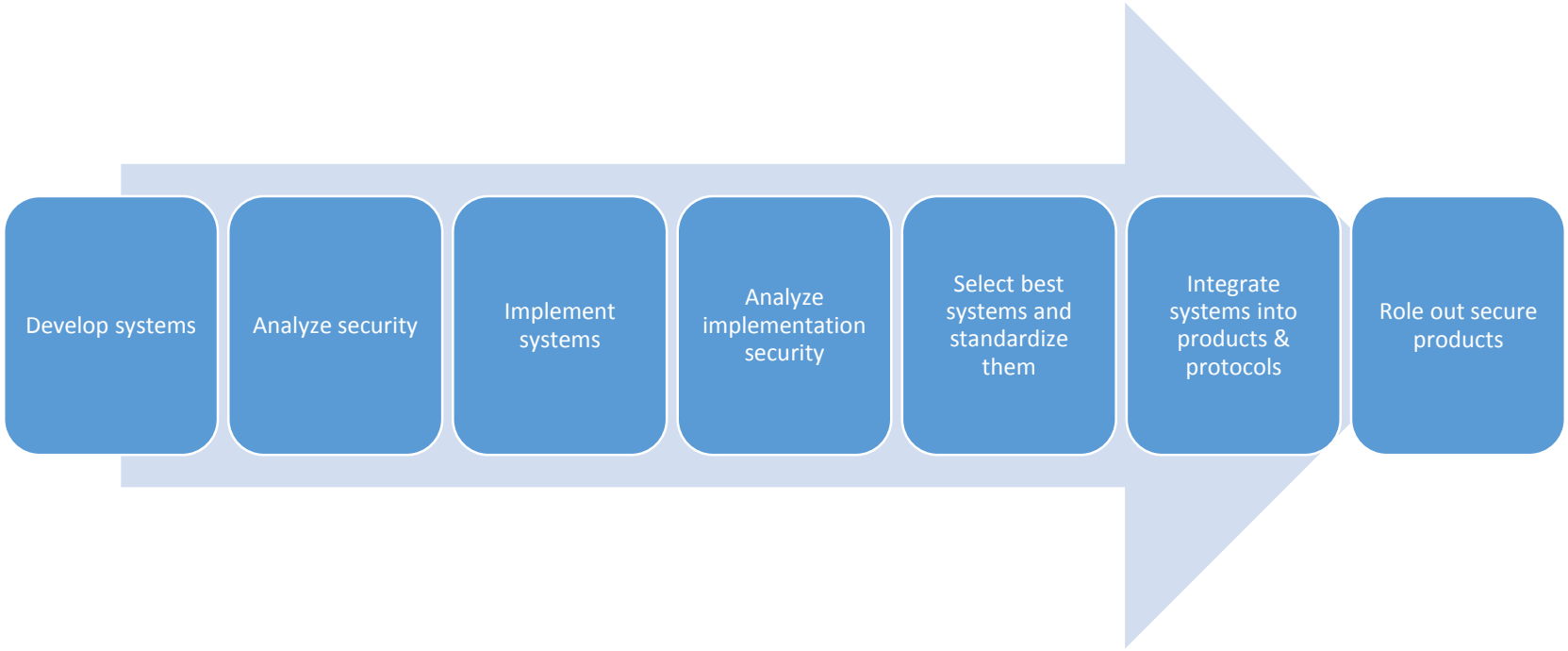
TECHNOLOGY
Scared Your DNA Is Exposed? Then Share It, Scientists Suggest

MARKETS
As Oil Plunges, the Real OPEC Meeting Will Be at Next Week's G20

MARKETS
Oil Limps to Worst Week in Almost Three Years as Glut Fears Grow

It‘s a question of risk assessment

Real world cryptography development



Who would store all encrypted data traffic? That must be expensive!

Long-lived systems

- Development time easily 10+ years
- Lifetime easily 10+ years

- At least make sure you got a secure update channel!

What about QKD?

Recall: Communication security (simplified)

Hi

pk, Cert(pk belongs to shop)

PKC to establish shared secret sk

SKC secured communication using sk

The TEA SHOP
FINE TEAS & TISANES
PURE & BLENDED

The problem solved by QKD

Given

- a shared classical secret.
- a phys… …ports QKD
- compa… … chann…

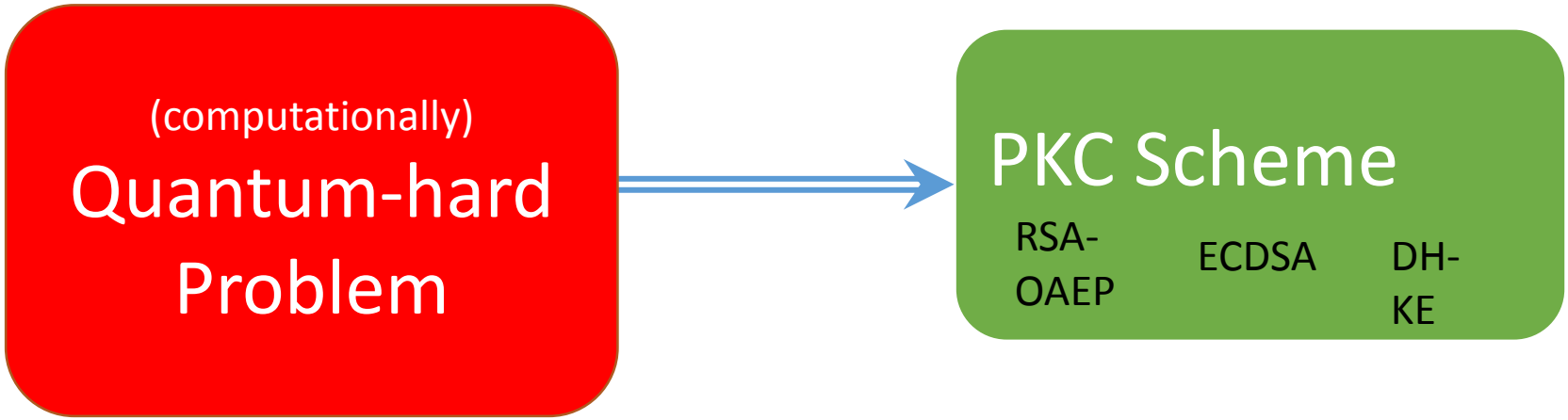
It is poss…

- generate a longer shared classical secret.

"Key growing"
(≠ "Key establishment")

Solution to the problem caused by Shor? Post-quantum cryptography

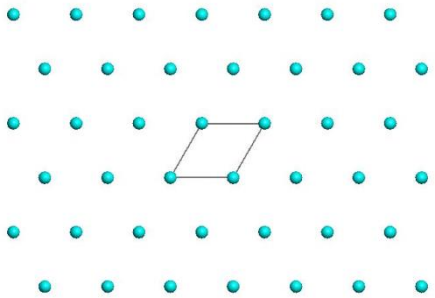
How to build PKC



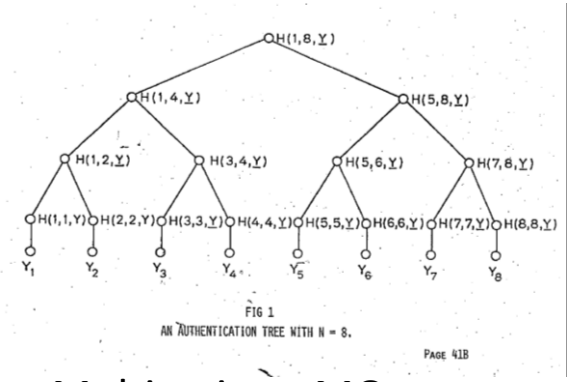
Early post-quantum crypto

„Cryptography based on problems that are conjectured to be hard even for quantum computers.“

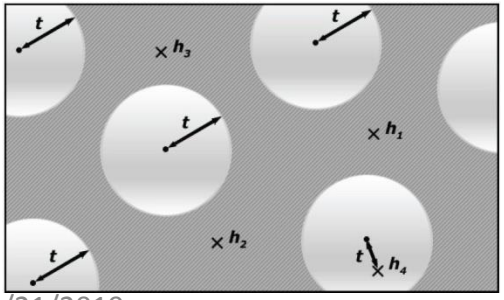
Lattice-based: SVP / CVP



Hash-based: CR / SPR / ...



Code-based: SD



Multivariate: MQ

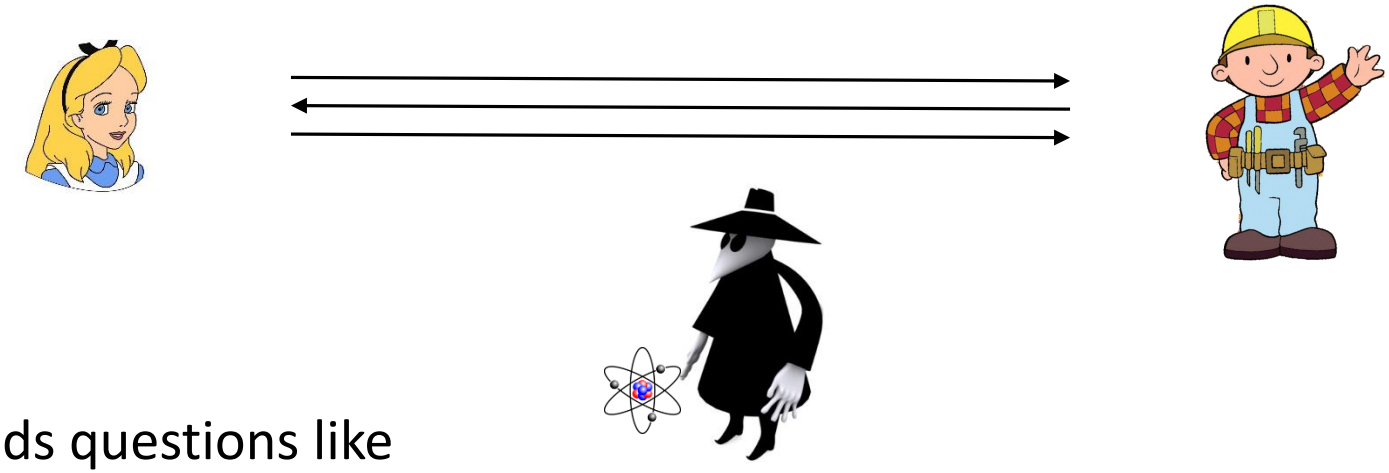
$$y_1 = x_1^2 + x_1x_2 + x_1x_4 + x_3$$

$$y_2 = x_3^2 + x_2x_3 + x_2x_4 + x_1 + 1$$

$$y_3 = \ldots$$

Modern post-quantum crypto

„Users using cryptography on conventional computers facing quantum adversaries“



Adds questions like

- How to argue security?
- Are our security models sound?
- What is the complexity of actual quantum attacks?

NIST Competition

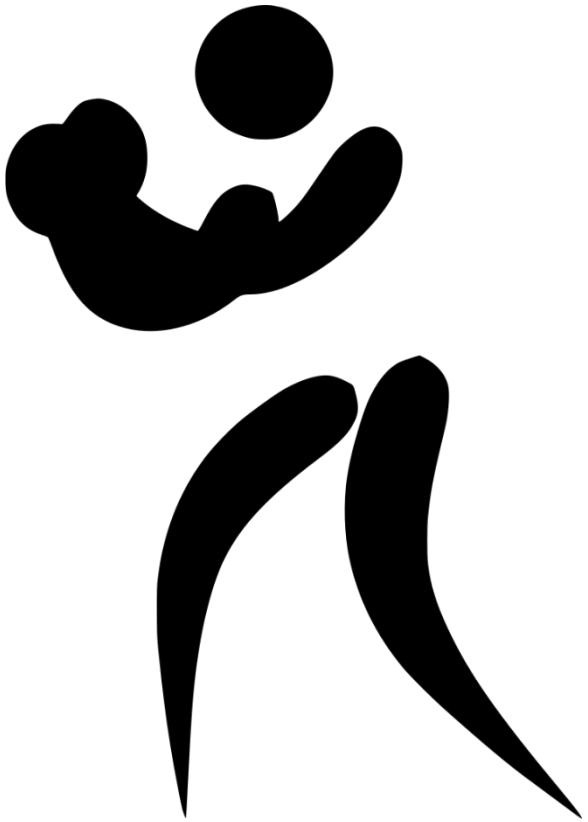
"We see our role as managing a process of achieving community consensus in a transparent and timely manner" NIST's Dustin Moody 2018

Status of the competition

- Nov 2017: 82 submissions collected
- Dec 2017: 69 “complete & proper” proposals published
  - -> Starts round 1 (of 2 or 3 rounds)
- Jan 2019: 26 proposals selected for 2nd round.
  - 17 KEM, 9 Signature
- 2022 – 2024 Draft standards exist

General conflict

Security



Performance

Open questions

Proofs are complicated

Possible issues with “proofs“

“Security proof“ = proof that breaking scheme is as hard as solving hard math problem

- Some proofs are in the wrong models
- Some proofs are massively loose
- Some proofs are just wrong

In PQC we have to deal with new math, new models of computation & security!

Way out?

- Reviewing is hard, time-consuming, and not rewarding
- Possible solution: Computer-verified proofs

Protocol integration

Plug‘n‘play?

- Today‘s protocols are built around DH
- NIST selects KEM and DSig
- Performance gap between SKC and PKC widens
- Efficient schemes are less mature than today‘s crypto

- Requires new protocol design

Conclusion

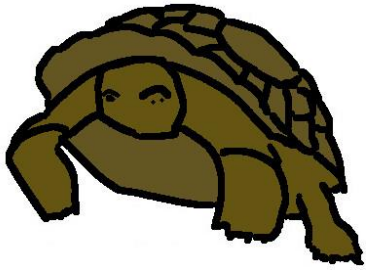
- When large-scale QC are built, we need new PKC
- It remains a question of risk assessment
- We are making progress to standardize PQC but we still need time
  - (For applications with long-term secrecy requirements you can move now at the price of higher costs)

Resources

- PQ Summer School: http://www.pqcschool.org/
- NIST PQC Standardization Project: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

PQCrypto

PQCRYPTO
ICT-645622



Thank you!
Questions?