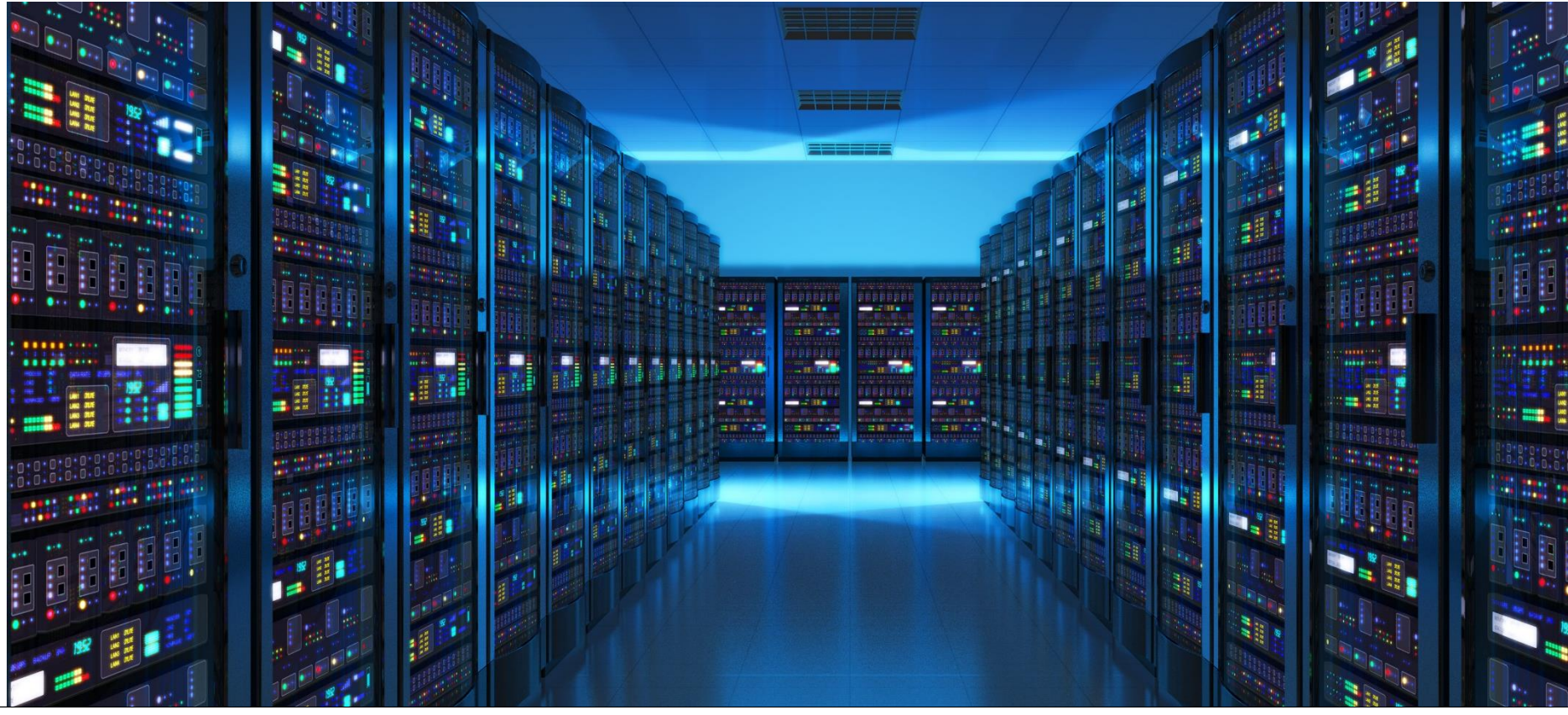
Giesecke+Devrient

Quantum Computing: „it's the end of the world as we know it?“

Giesecke+Devrient
Munich, June 2018

What drives a company's digital strategy in 2020 and beyond?



What drives a company’s digital strategy in 2020 and beyond?

INTERNET OF THINGS?

What drives a company's digital strategy in 2020 and beyond?

CYBER ATTACKS?

What drives a company's digital strategy in 2020 and beyond?

What drives a company's digital strategy in 2020 and beyond?

DIGITAL TRANSFORMATION?

What drives a company's digital strategy in 2020 and beyond?

Regardless of what drives your digital strategy – it will be based on

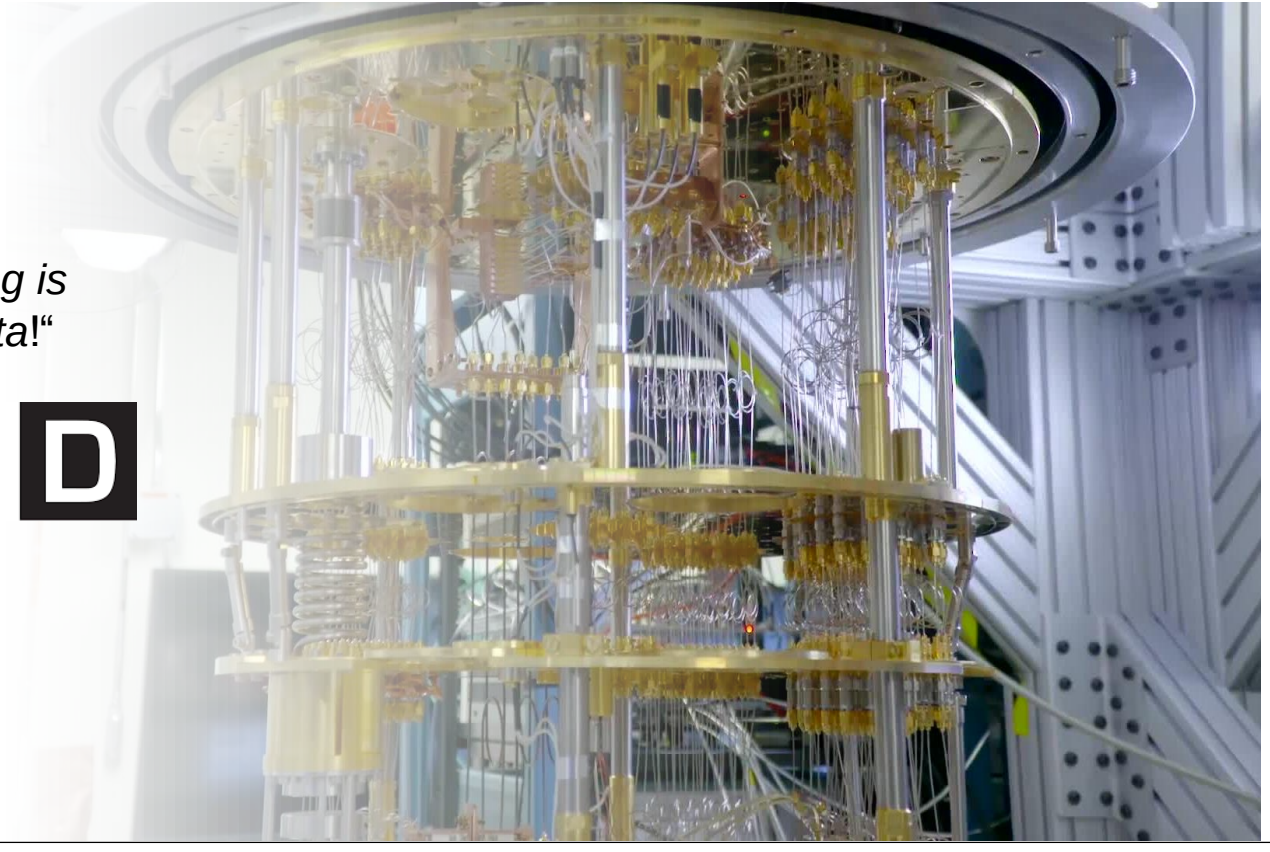
- digital identities
- authentication of these identities
- secret communication

⇨ all driven by digital certificates and encryption!

And then comes Quantum Computing…

„Quantum computing is coming for your data!“

WIRED



Who are we and why do we care?

Giesecke+Devrient – creating confidence since 1852

Giesecke+Devrient
Creating Confidence

G+D provides secure solutions for customers in four major playing fields

Payment

Global leader in physical, electronic and digital payments

Connectivity

Secure connectivity as a gateway to the Internet of Things

Identity

Safeguarding personal identities and authentication

Digital security

Protecting classified data, communication channels & critical infrastructures

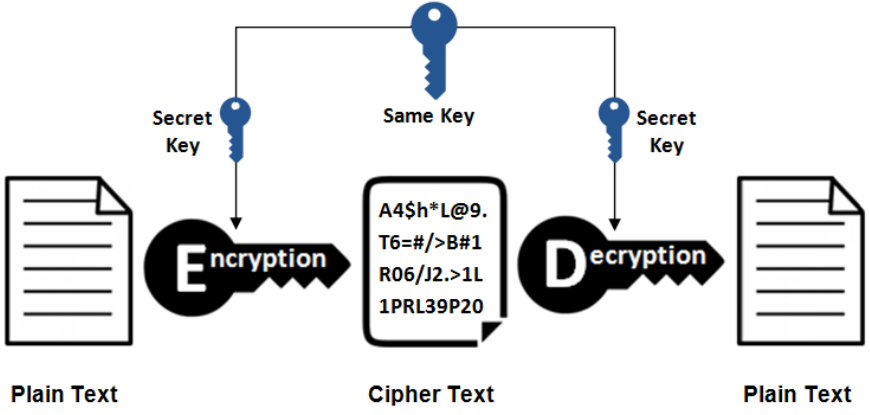
Security

G+D makes the lives of billions of people more secure

The digital world is build on encryption

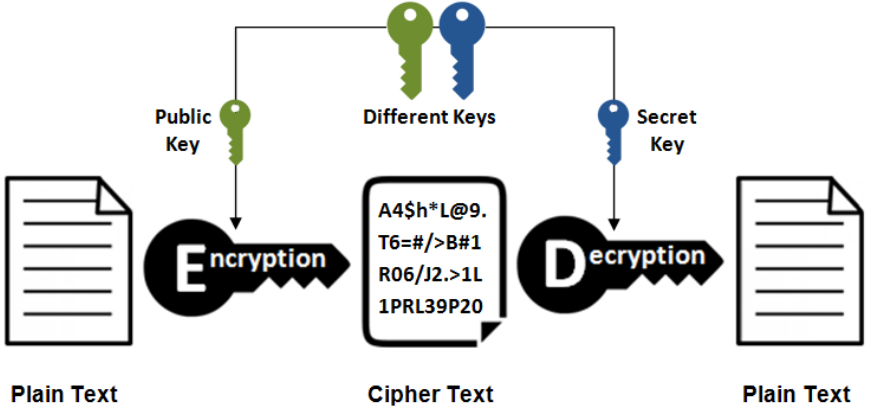
How does classical encryption work?

Symmetric encryption



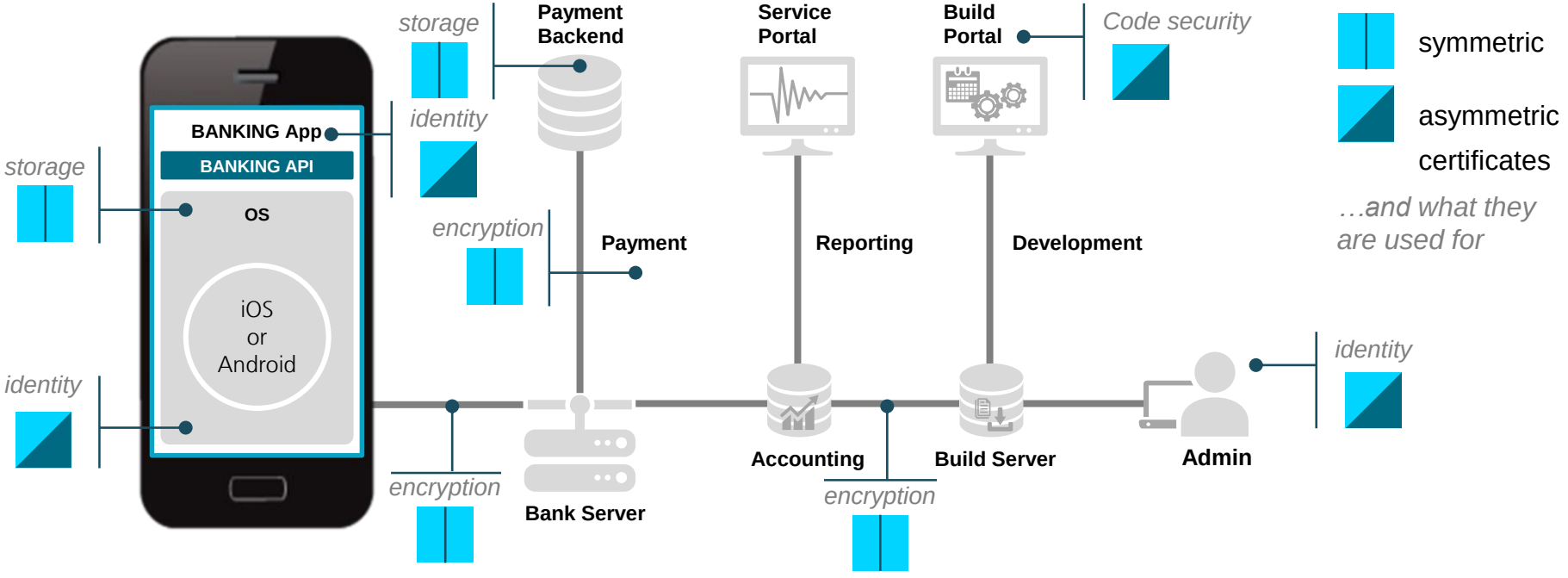
Examples: AES, DES

Asymmetric encryption



Examples: RSA, ECC

Where you would use encryption and certificates in a mobile banking environment?

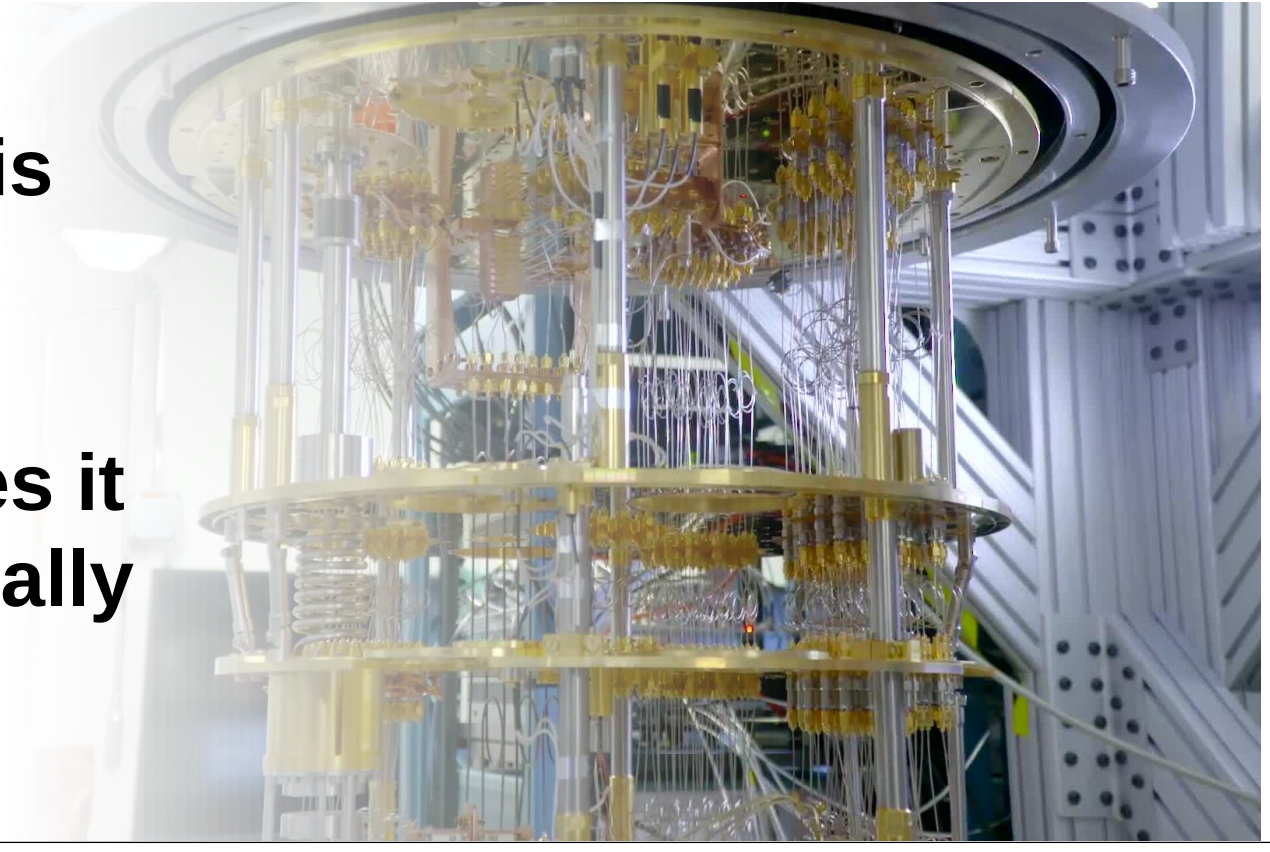


OK, encryption is well understood and widely used – so we are safe, right?

Quantum computing has the potential to shake digital encryption to the core

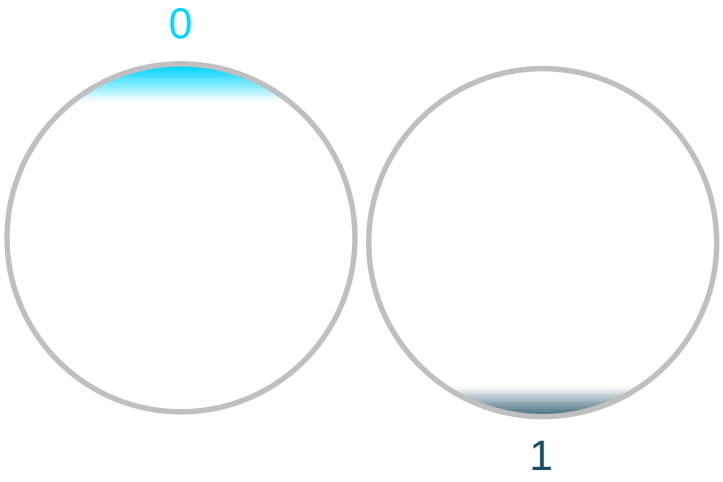
Remember this marvel?

So what makes it so fundamentally different?



The fundamental difference in quantum computing are the Qubits

Classical bits



Clear-cut, either 1 or 0, on or off

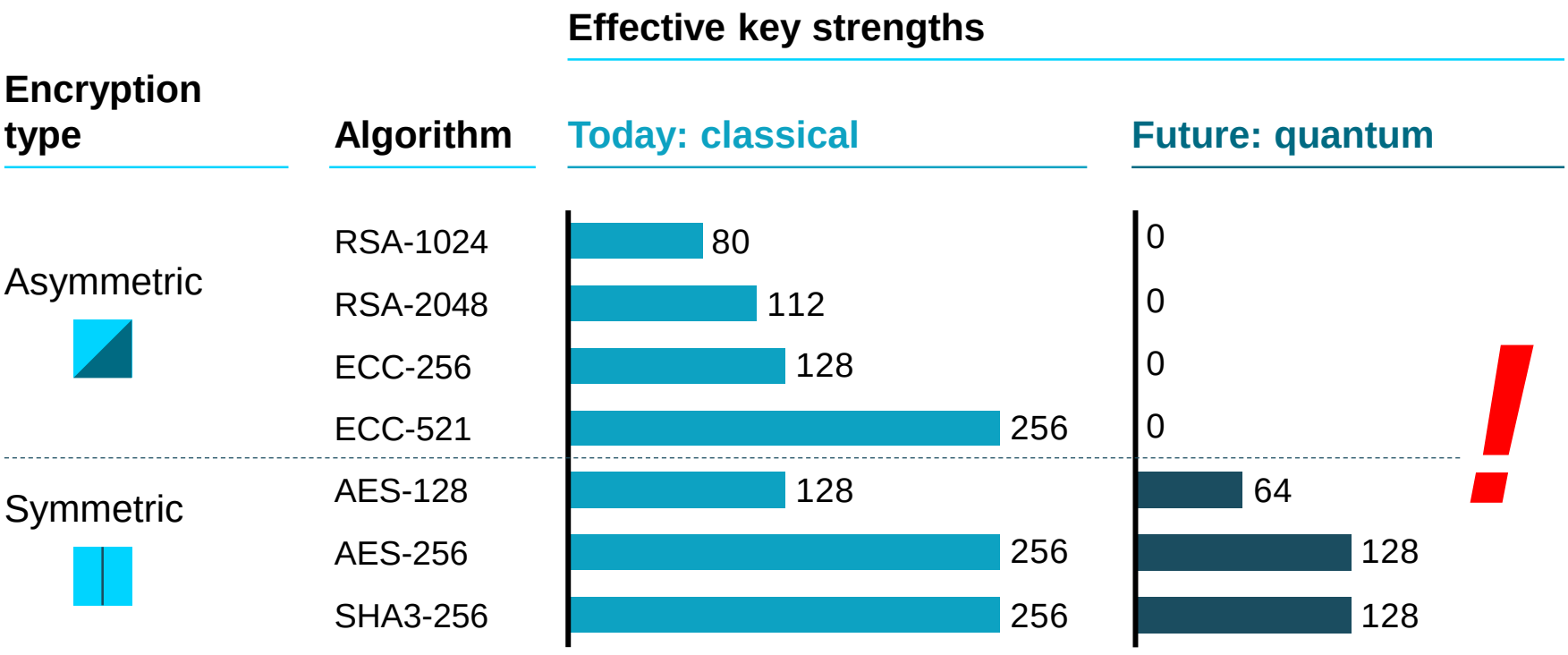
Qubits

Multiple states at the same time („superposition“)

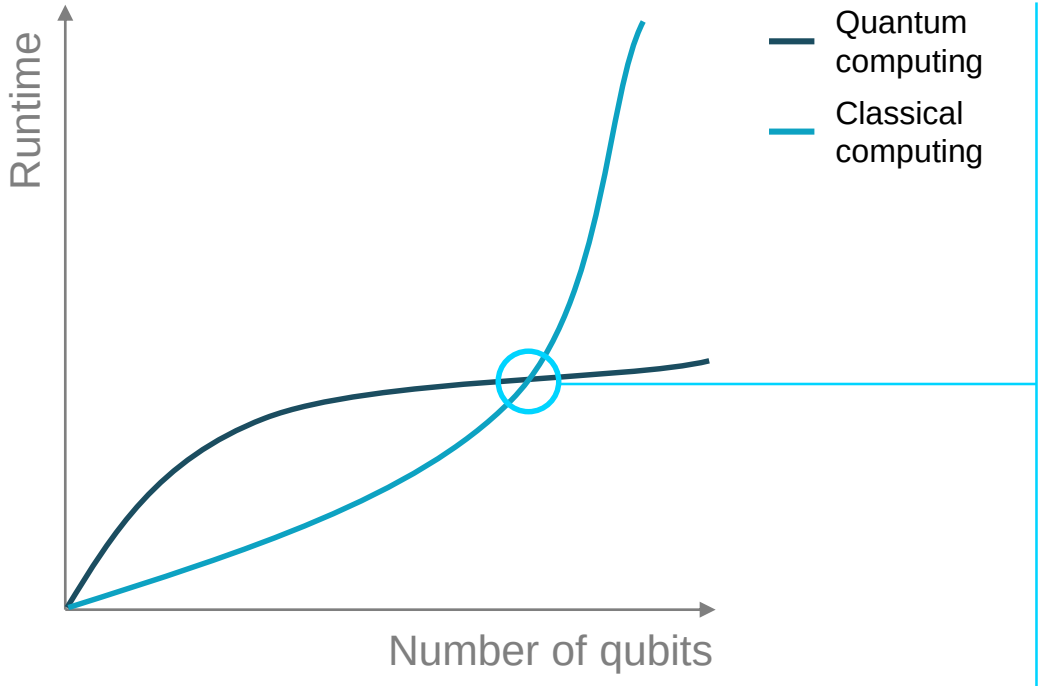
Impact

- When using Qubits, multiple operations can happen **simultaneously**
- Dramatic **speed-up** of certain calculations compared to classical bits

Today‘s encryption will be effectively broken by quantum computers

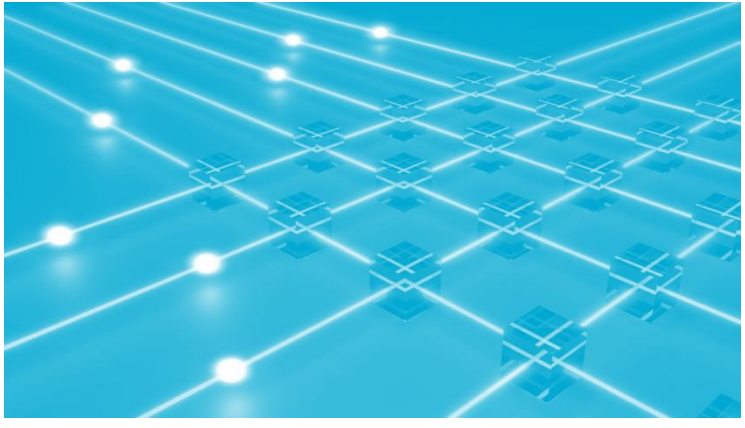


It is expected that one day, quantum computers will outperform classical ones

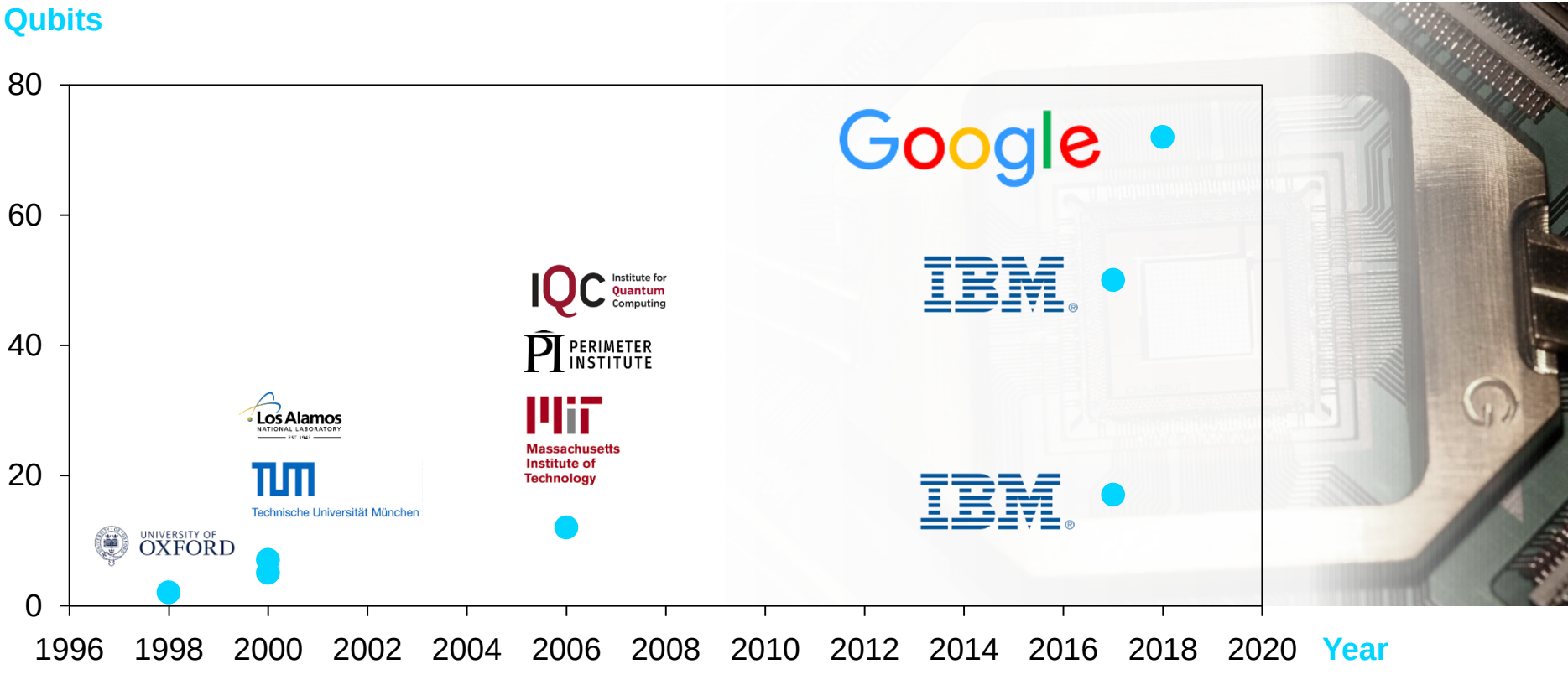


As number of useable qubits will increase, quantum computing will be able to solve problems that classical computers can not:

Quantum Supremacy



Number of qubits have been steadily increasing …

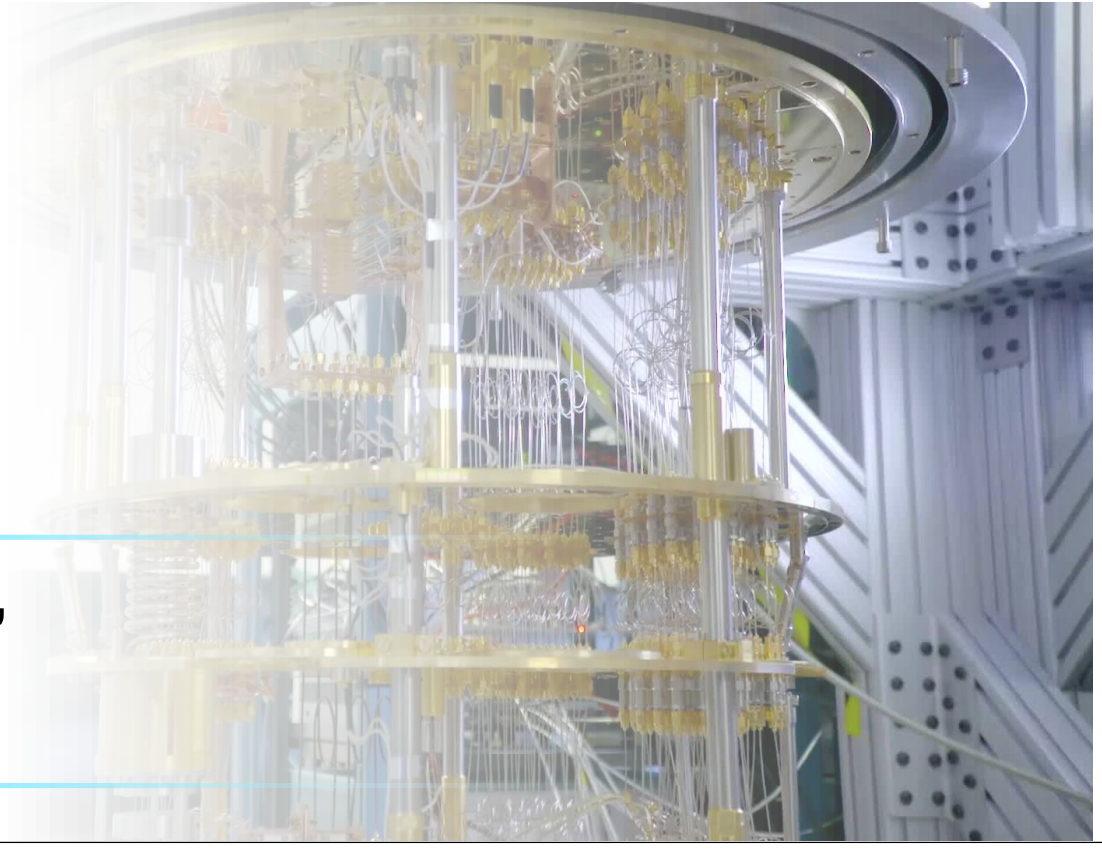


Time to panic?
Not yet!

Currently, qubits are very hard to scale and show high error rates

Obstacles to build and run

- requires intensive **cooling**
- depends on high amount of **magnetic shielding**
- consumes a lot of **energy**



In practice high error rates, reducing the effectiveness of the qubits!

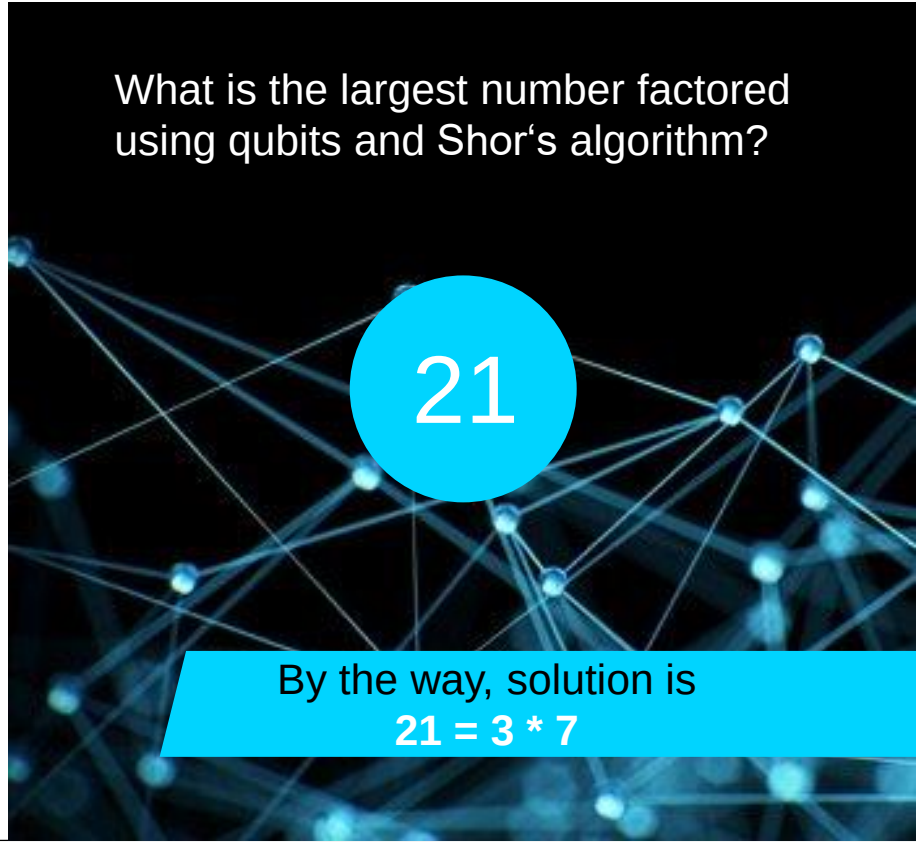
These obstacles still prevent breaking of today‘s encryption

Question How would one break a RSA key?

Approach Take a given very large number **A** and find its two factors **B** and **C**
⇨ **A = B * C**

How large is very large?

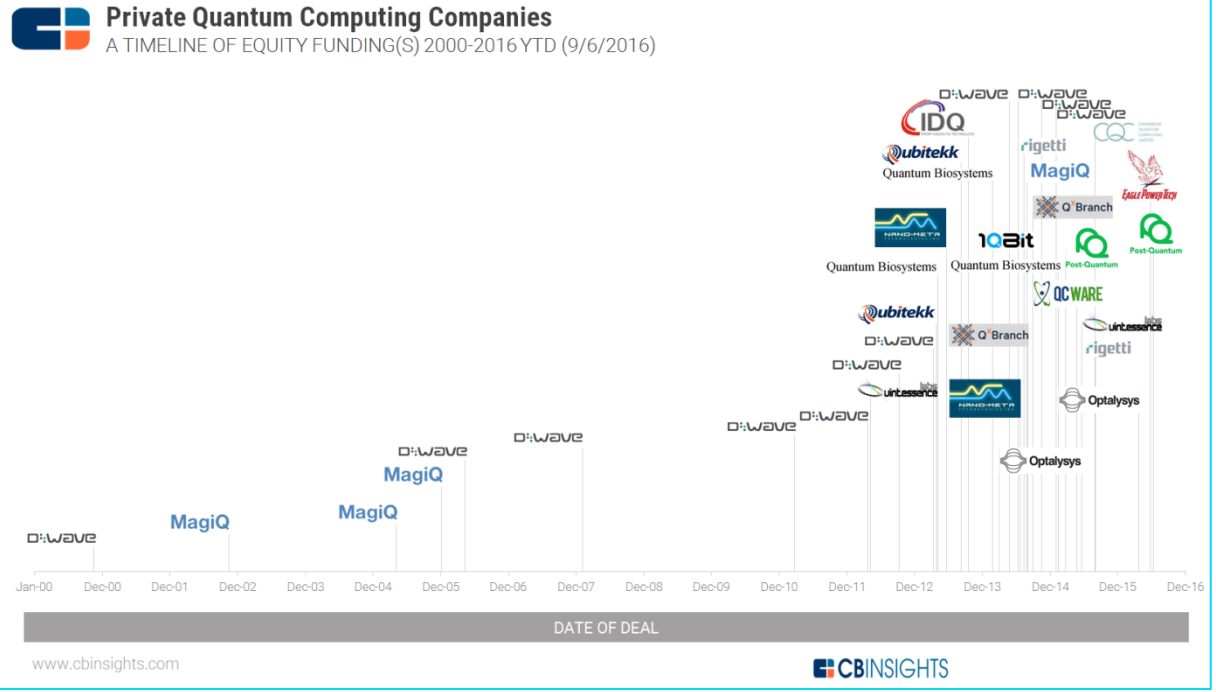
RSA-2048 =
25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357



But we should still take it seriously

> The **National Security Agency** is advising US agencies and businesses to prepare for a time in the **not-too-distant future** when the cryptography protecting virtually all e-mail, medical and financial records, and online transactions is **rendered obsolete** by quantum computing.

ars technica

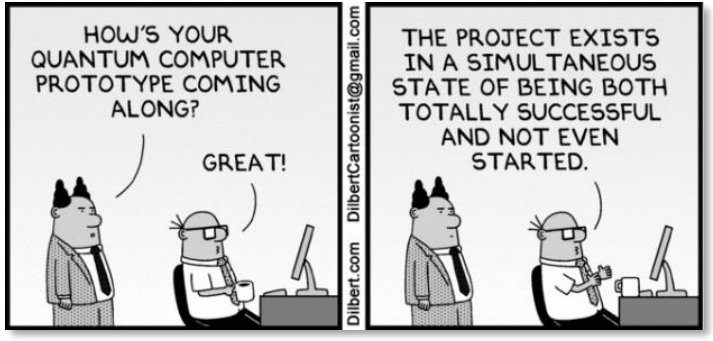


Actions to take to protect your customers and your organization

As new standards for **post-quantum cryptography** are being developed, here is what you can do…

1. Follow **announcements** on recent developments, both from academia and the industry
2. Identify the **critical elements** in your infrastructure depending on encryption
3. Per element, assess **risks** (potential damage) and **effort** to adapt
4. Start drafting a **transition plan** in order to be prepared once new standards are published
5. Be **aware** but don’t panic

Questions & Answers



Dr. Philipp Schulte

Corp. Development & Strategy
G+D Group

philipp.schulte@gi-de.com

Dr. Christian Schläger

Product Management
Cyber Security
G+D Mobile Security

christian.schlaeger@gi-de.com

Giesecke+Devrient

Vielen Dank!