Security Risks in Space and Time

Dipl. Math. X. Bogomolec
Quant-X Security & Coding GmbH
xb@quant-x-sec.com

24/10/19

About Me

Education

Mathematics

Work Fields

Algorithms | IT-Security

Latest Projects

Cryptographic certificate management | eAES Quantum Analysis

My GPIF Bank Summit Mission

Drawing you maps of facts, potentials and their interrelations

contact: xb@quant-x-sec.com
website: https://quant-x-sec.com

My Perspective

From Europe (Regulations, Regulations, and Regulations)

Information Security

What is it and what do we want to be secure?

CIA, the heart of information security

- Confidentiality
- Integrity
- Accessibilty

To identify, measure and mitigate risks for data relating to

- Financial assets
- Knowledge
- Privacy
- Health
- Safety
- …

Information Security

Technological Context

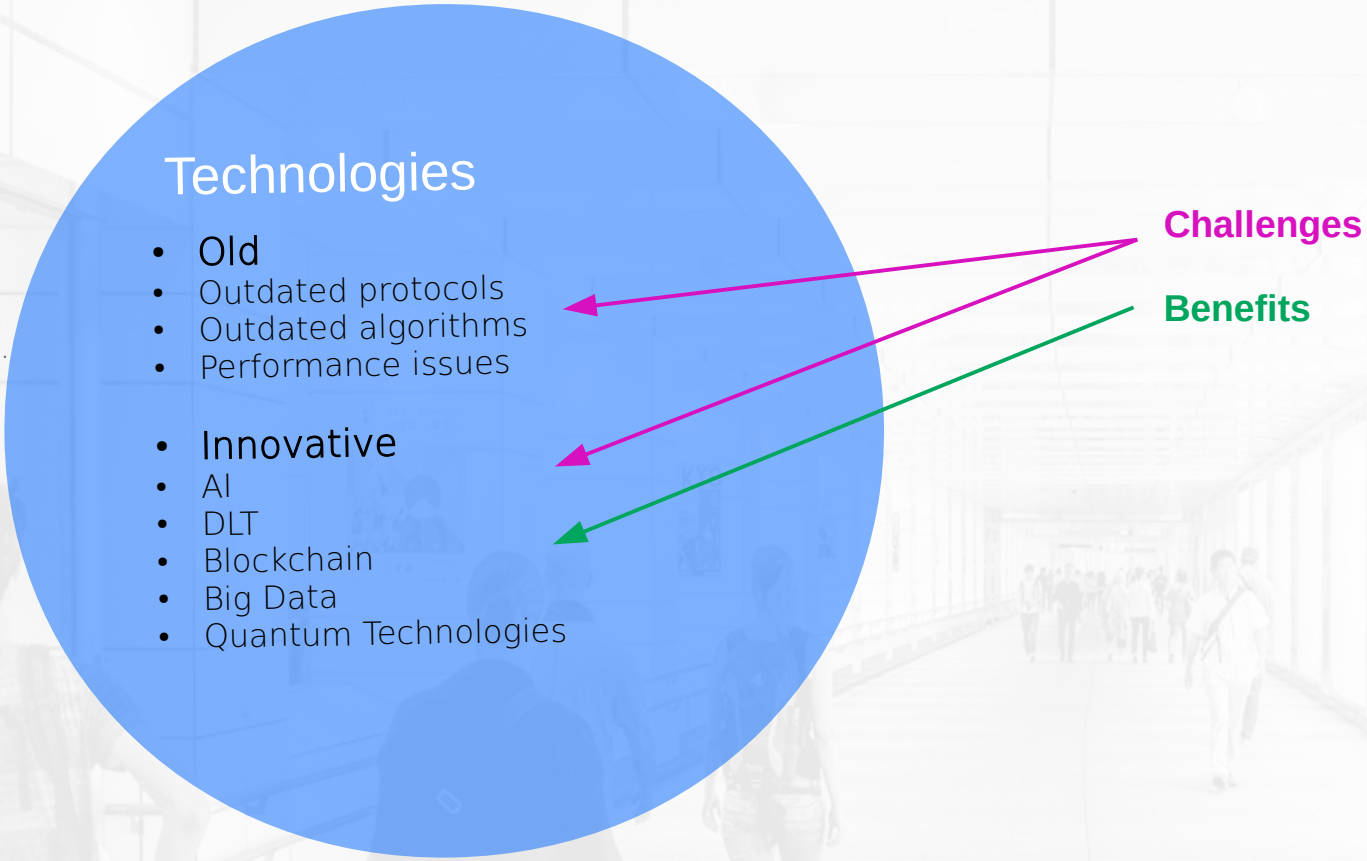
Technologies

- Old
- Outdated protocols
- Outdated algorithms
- Performance issues

- Innovative
- AI
- DLT
- Blockchain
- Big Data
- Quantum Technologies

Information Security

Technological Context



Technologies and Science

AI from a scientific perspective

Is it possible for computers to own a conscience and rule the world?

"Computers will stay stupid and they rule the world since a long time already."

Prof. Raul Rojas, computer science professor with special field neuroinformatics, Freie Universität Berlin

"I believe that the complexity gap between AI and the human brain is massively underestimated."

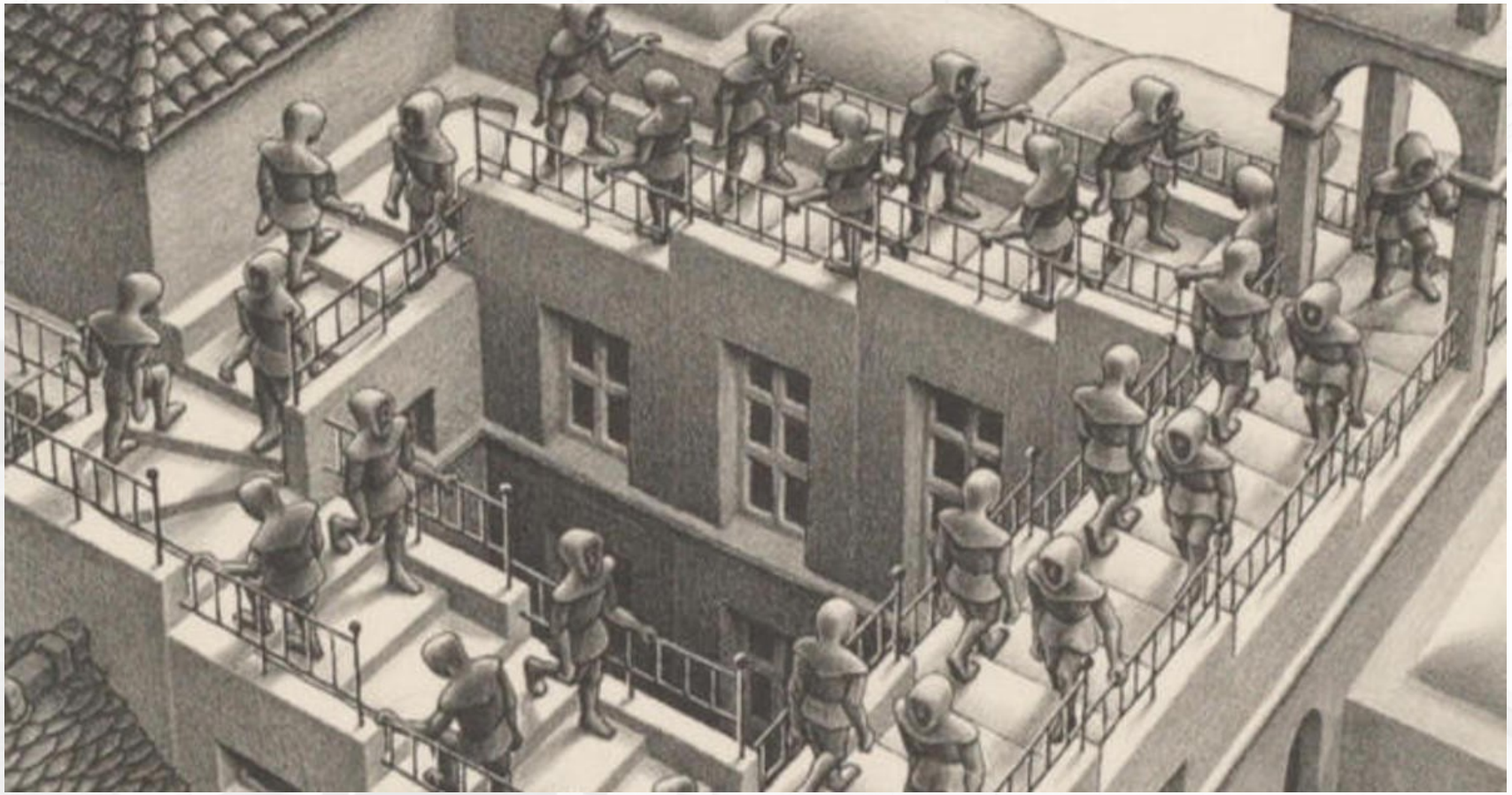
Dr. Peter Nonnenmann, computer science expert with special field neuroinformatics, cryptography and quantum computing, Frankfurt Institute for advanced studies

https://fias.academia.edu/PeterDrNonnenmann

Technologies and Science

AI from a scientific perspective

The previous views are based on questions such as:
When can a drawn figure be realized in 3-D?



Technologies and Science

AI from a scientific perspective

The previous views are based on questions such as:

When can a drawn figure be realized in 3-D?

Answer: Conventional machine learning, such as deep-learning networks in autonomous driving cars only process images locally, not globally. Global 3-D image recognition can therefore not be realized like this.

Related articles:

https://www.mobile.ifi.lmu.de/team/claudia-linnhoff-popien/

https://digitaleweltmagazin.de/2019/07/15/topologische-komplexe-informationsverarbeitung-in-neuroalen-netzen/

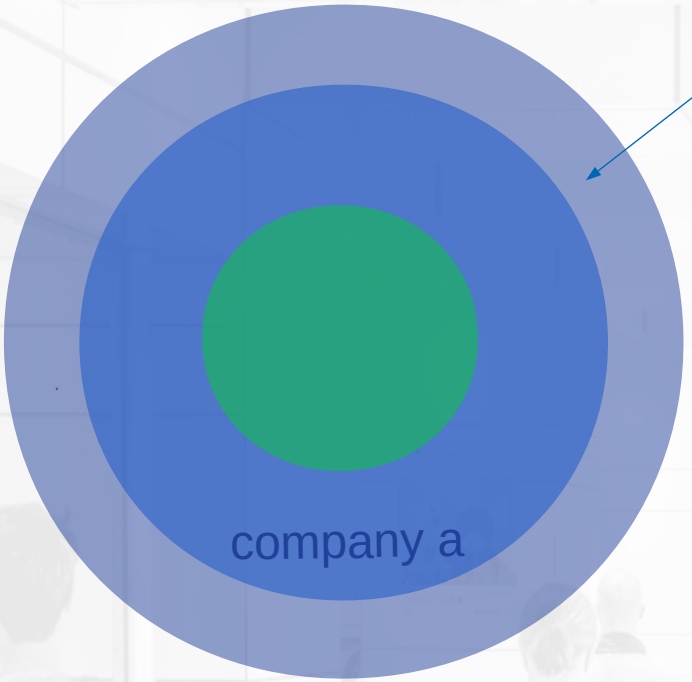
https://link.springer.com/article/10.1007/s42354-019-0215-6

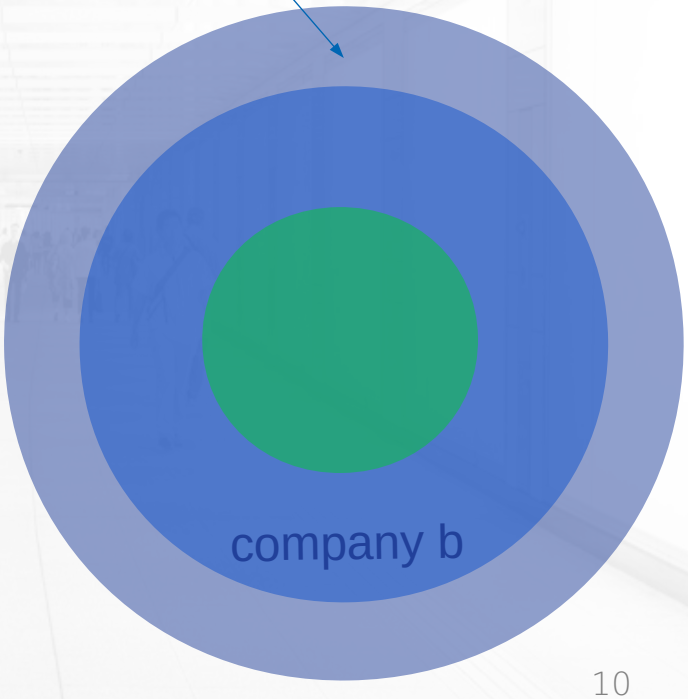
Information Security

Protective Measurements

Infrastructure & Computing

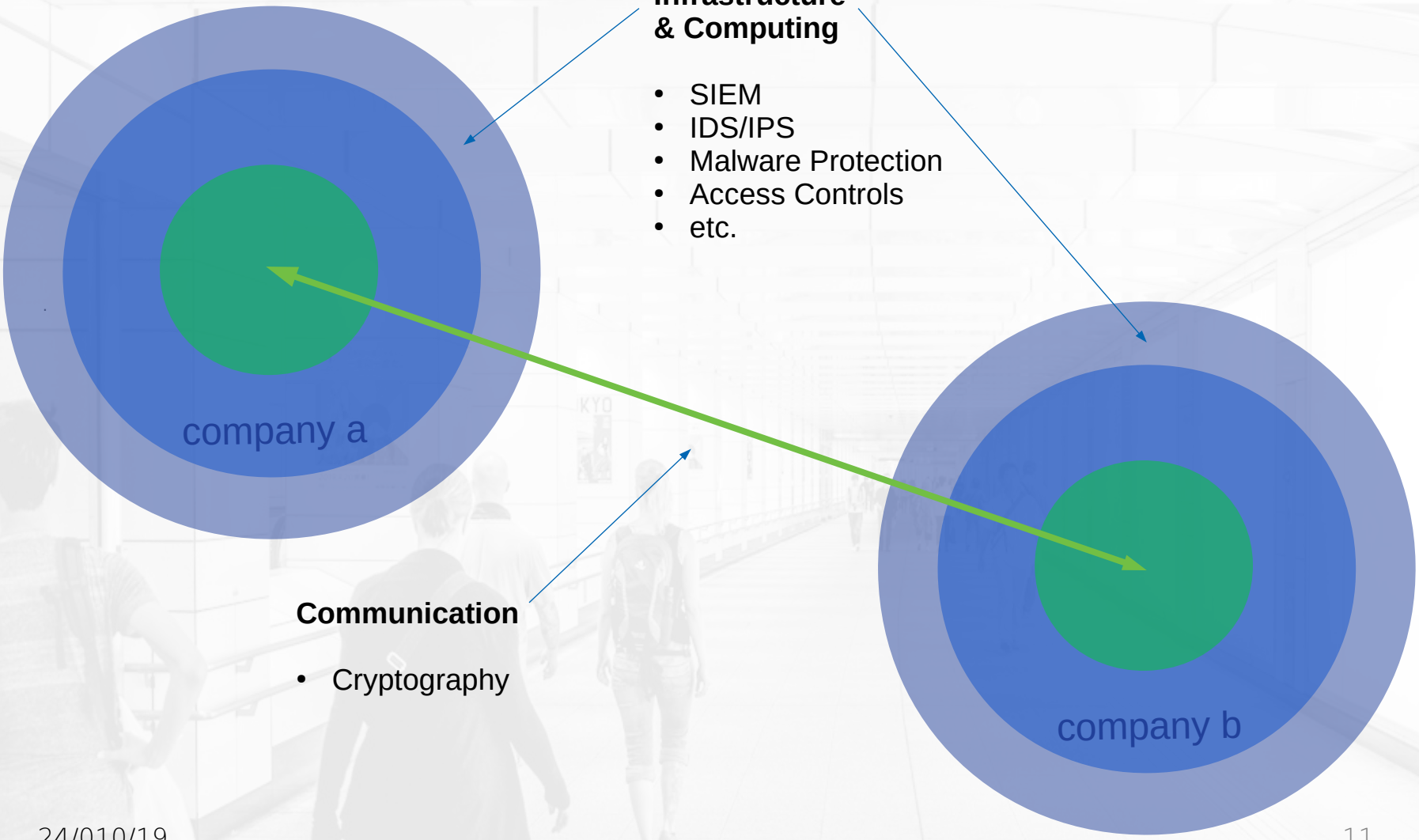
- SIEM
- IDS/IPS
- Malware Protection
- etc.





Information Security

Protective Measurements



Cryptography

Confidentiality, Integrity and Authentication

The stack:

- Users
- Management
- Administration
- Network
- Application Integration
- System Integration
- Implementation
- Computer Science
- Mathematics

Cryptography

Confidentiality, Integrity and Authentication

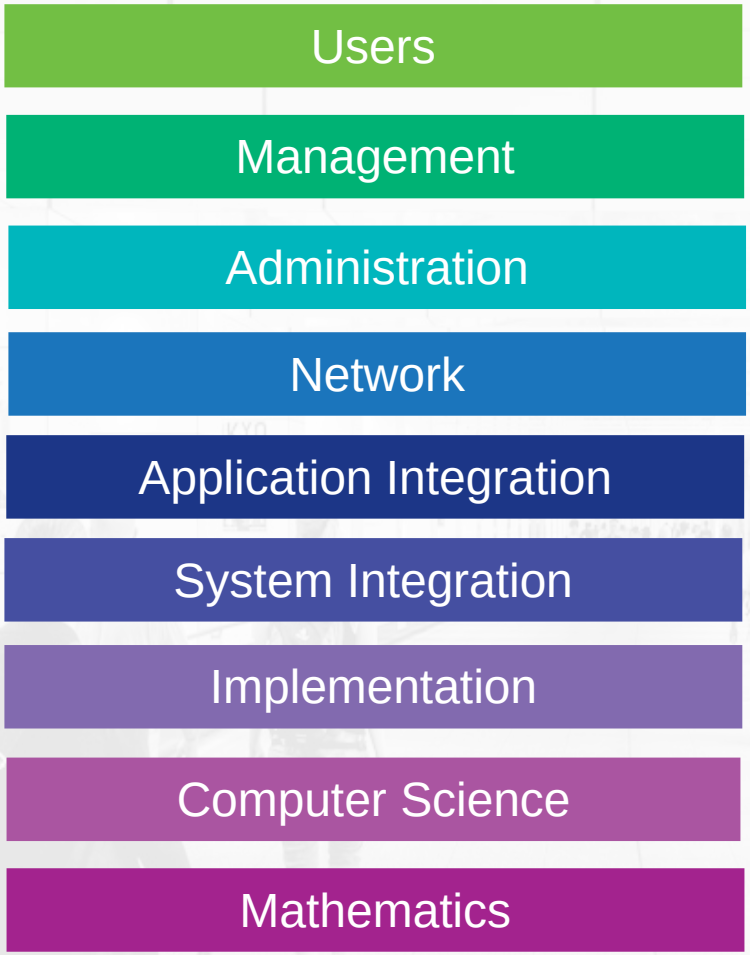
THREATS

New Mathematical Solutions

Increasing Performance of Binary Technologies

Quantum Computing

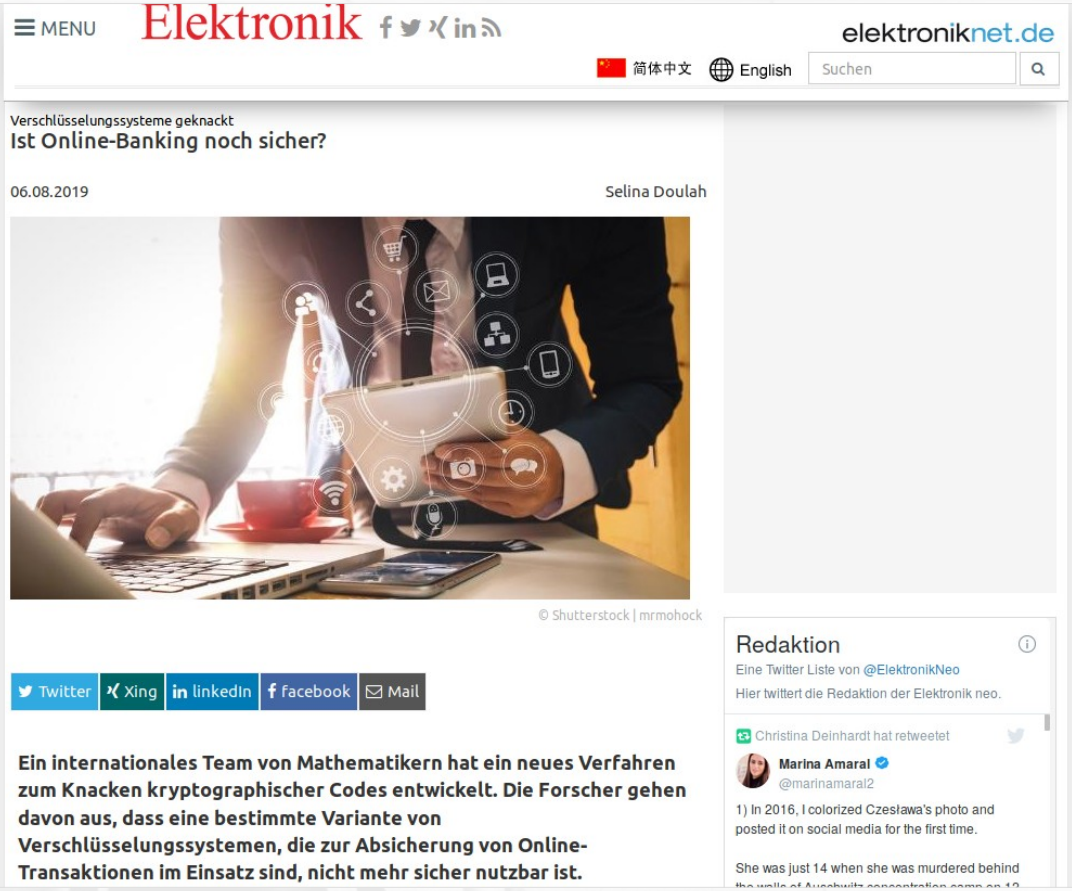
The stack:



Cryptography

Confidentiality, Integrity and Authentication

New Mathematical Solutions: Cryptanalysis



MENU Elektronik elektroniknet.de

简体中文 English Suchen

Verschlüsselungssysteme geknackt

Ist Online-Banking noch sicher?

06.08.2019 Selina Doulah

© Shutterstock | mrmohock

Twitter Xing linkedIn facebook Mail

Ein internationales Team von Mathematikern hat ein neues Verfahren zum Knacken kryptographischer Codes entwickelt. Die Forscher gehen davon aus, dass eine bestimmte Variante von Verschlüsselungssystemen, die zur Absicherung von Online-Transaktionen im Einsatz sind, nicht mehr sicher nutzbar ist.

Redaktion

Eine Twitter Liste von @ElektronikNeo

Hier twittert die Redaktion der Elektronik neo.

Christina Deinhardt hat retweetet

Marina Amaral

@marinamaral2

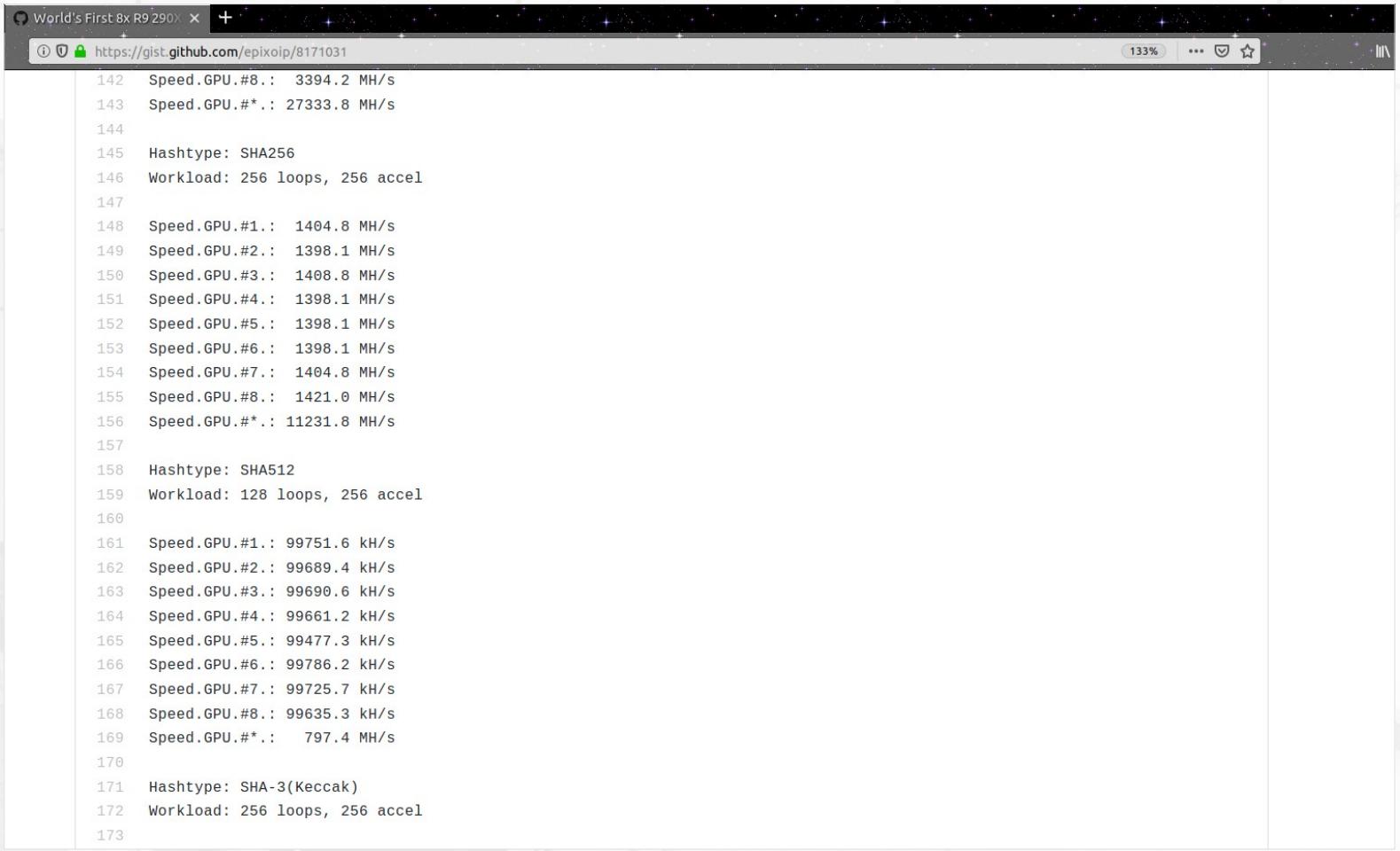
1) In 2016, I colorized Czesława's photo and posted it on social media for the first time.

She was just 14 when she was murdered behind

Cryptography

Confidentiality, Integrity and Authentication

Increased Performance:




```
Speed.GPU.#8.:  3394.2 MH/s
Speed.GPU.#*.: 27333.8 MH/s

Hashtype: SHA256
Workload: 256 loops, 256 accel

Speed.GPU.#1.:  1404.8 MH/s
Speed.GPU.#2.:  1398.1 MH/s
Speed.GPU.#3.:  1408.8 MH/s
Speed.GPU.#4.:  1398.1 MH/s
Speed.GPU.#5.:  1398.1 MH/s
Speed.GPU.#6.:  1398.1 MH/s
Speed.GPU.#7.:  1404.8 MH/s
Speed.GPU.#8.:  1421.0 MH/s
Speed.GPU.#*.: 11231.8 MH/s

Hashtype: SHA512
Workload: 128 loops, 256 accel

Speed.GPU.#1.: 99751.6 kH/s
Speed.GPU.#2.: 99689.4 kH/s
Speed.GPU.#3.: 99690.6 kH/s
Speed.GPU.#4.: 99661.2 kH/s
Speed.GPU.#5.: 99477.3 kH/s
Speed.GPU.#6.: 99786.2 kH/s
Speed.GPU.#7.: 99725.7 kH/s
Speed.GPU.#8.: 99635.3 kH/s
Speed.GPU.#*.:   797.4 MH/s

Hashtype: SHA-3(Keccak)
Workload: 256 loops, 256 accel
```

Cryptography

Confidentiality, Integrity and Authentication

Quantum Computing:

c|net

IBM's new 53-qubit quantum computer is its biggest yet

Stephen Shankland 9/18/2019

IBM's 14th quantum computer is its most powerful so far, a model with 53 of the qubits that form the fundamental data-processing element at the heart of the system. The system, available online to quantum computing customers in October, is a big step up from the last IBM Q machine with 20 qubits and should help advance the marriage of classical computers with the crazy realm of quantum physics.

Cryptography

Confidentiality, Integrity and Authentication

The world reacts!

- Research for new cryptographic algorithms (Post-Quantum Crypto)
- Standardization

Why now, if we don't know when potent enough quantum Computers exist?

- Catastrophic effects when they are available:
  Sensitive data which is sent now and has to remain secret in future
- Possible "Quantum" Leap in development
- Protection against evolving binary technologies and cryptanalysis of classical crypto
- Global integration takes years

My Message

Post-Quantum Crypto

… don’t wait too long to integrate it for data which has to remain secret

contact: xb@quant-x-sec.com
website: https://quant-x-sec.com

Additional Information

Check out the next slides

Further Articles and Presentations:

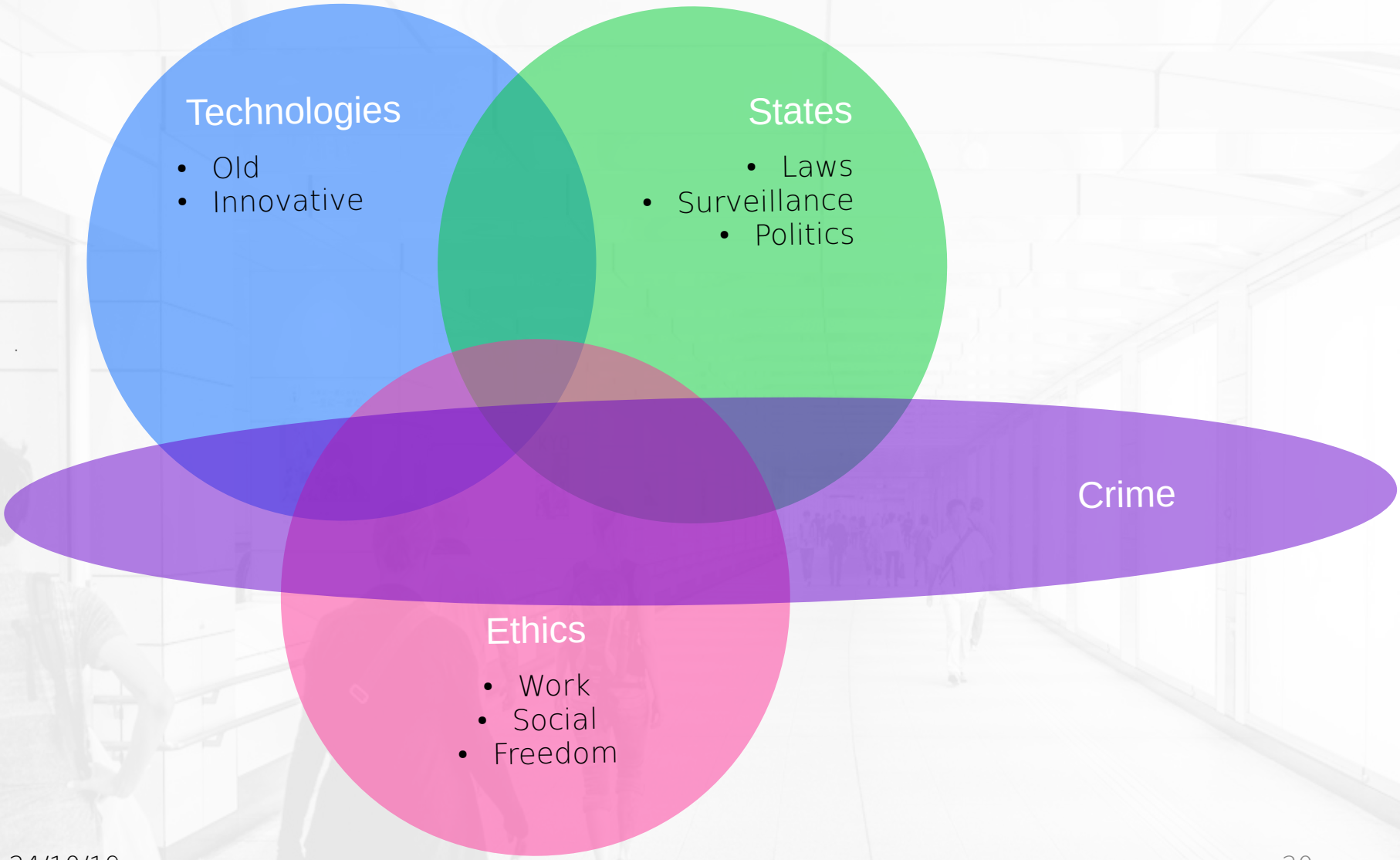
https://quant-x-sec.com/published.htm

Post-Quantum security as ISO standard candidate:
https://eprint.iacr.org/2019/1208

contact: xb@quant-x-sec.com
website: https://quant-x-sec.com

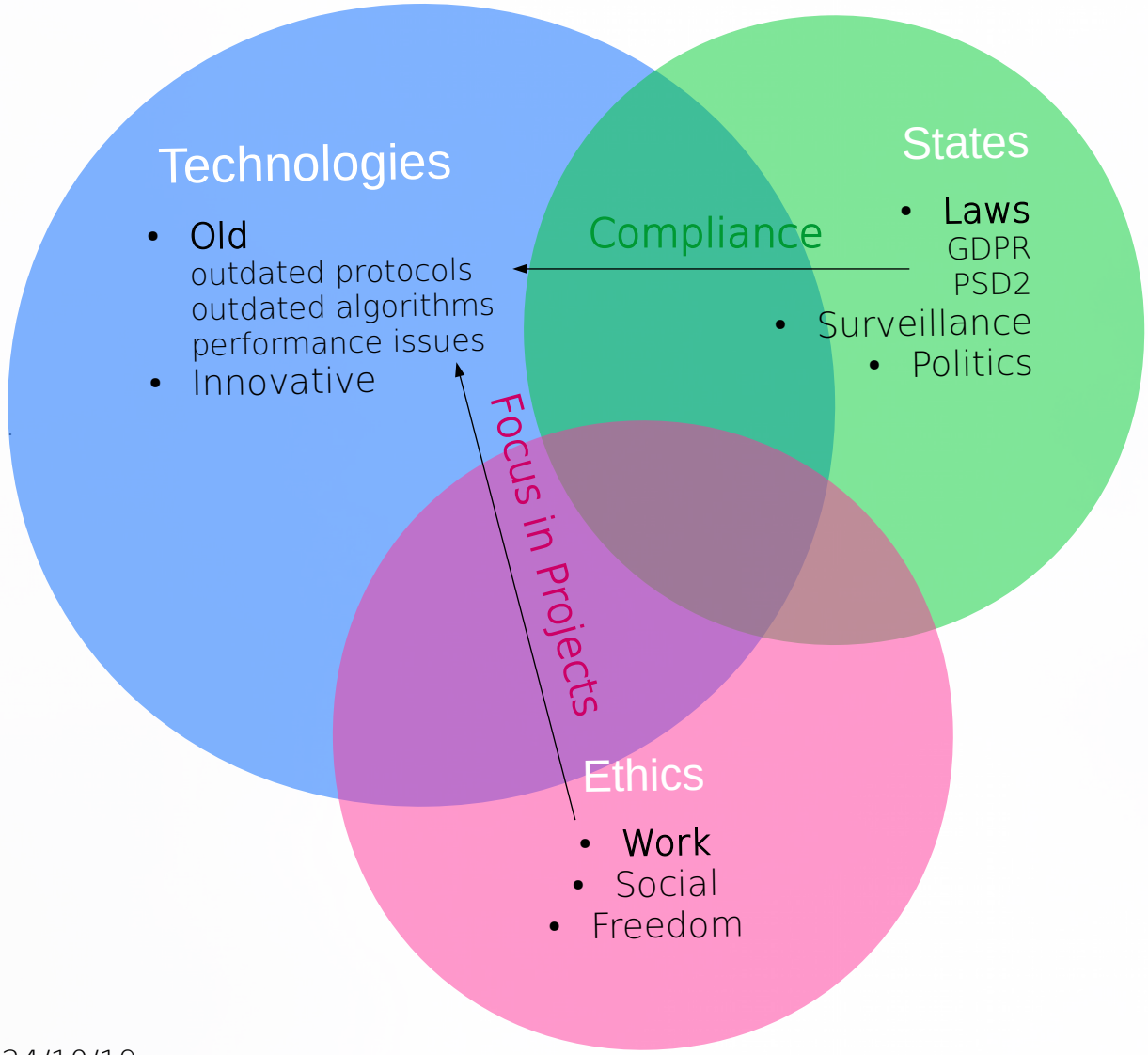
Information Security

Influences and Challenges



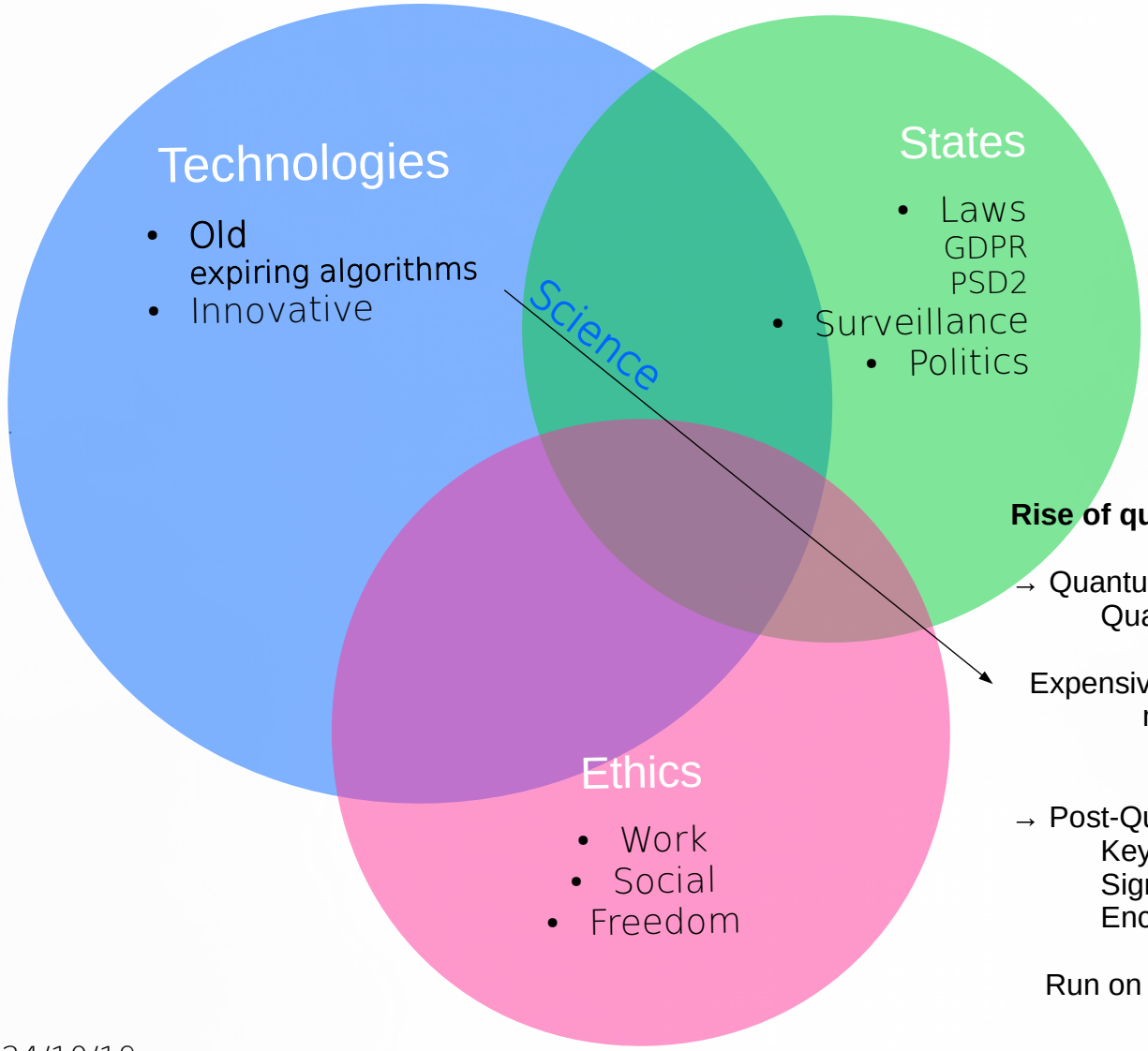
Information Security

Challenges for Old Technologies



Information Security

Challenges for Expiring Algorithms



Rise of quantum technology threats

→ Quantum Cryptology
Quantum Key Distribution

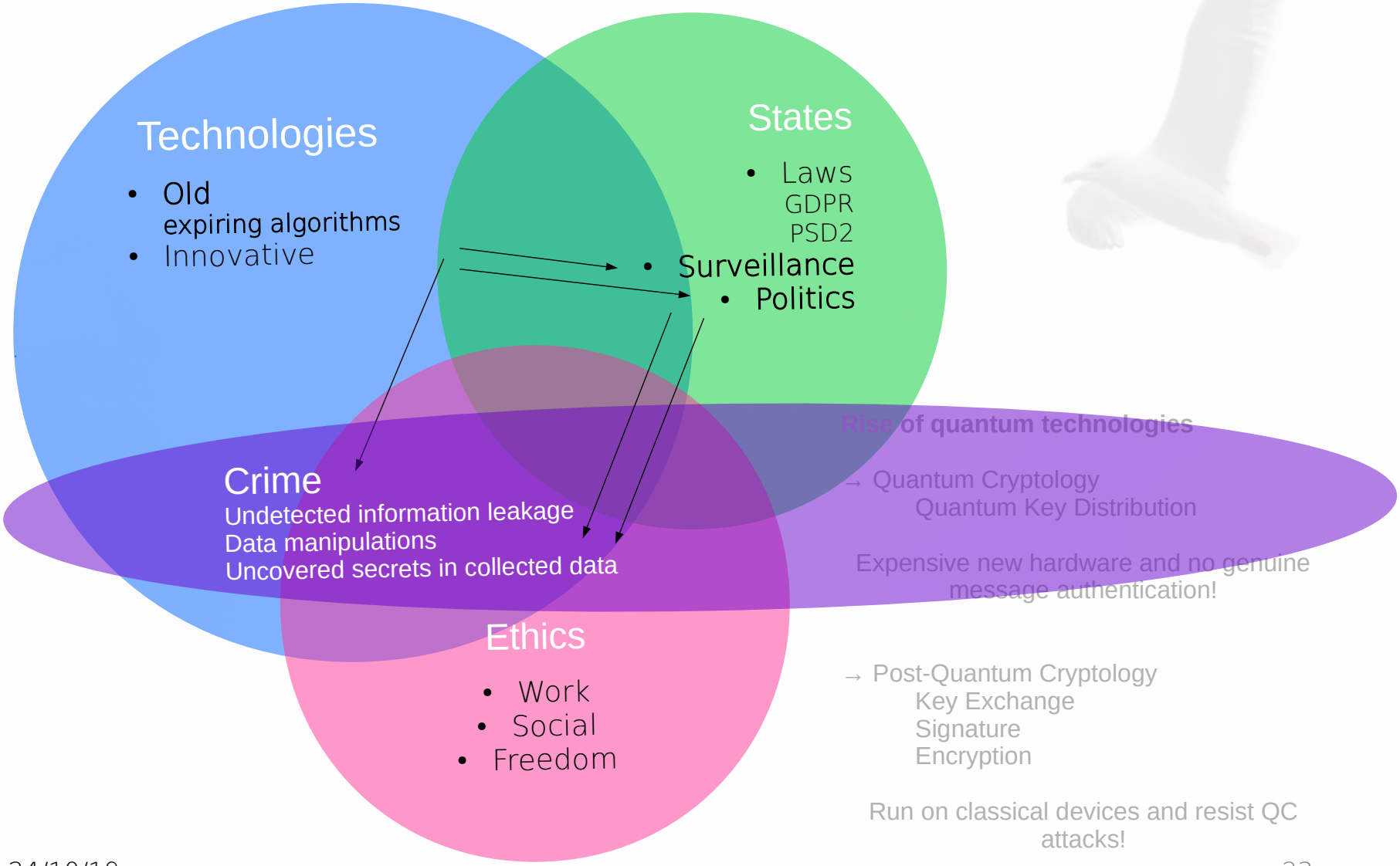
Expensive new hardware and no genuine message authentication!

→ Post-Quantum Cryptology
Key Exchange
Signature
Encryption

Run on classical devices and resist QC attacks!

Information Security

Challenges



Rise of quantum technologies

→ Quantum Cryptology
Quantum Key Distribution

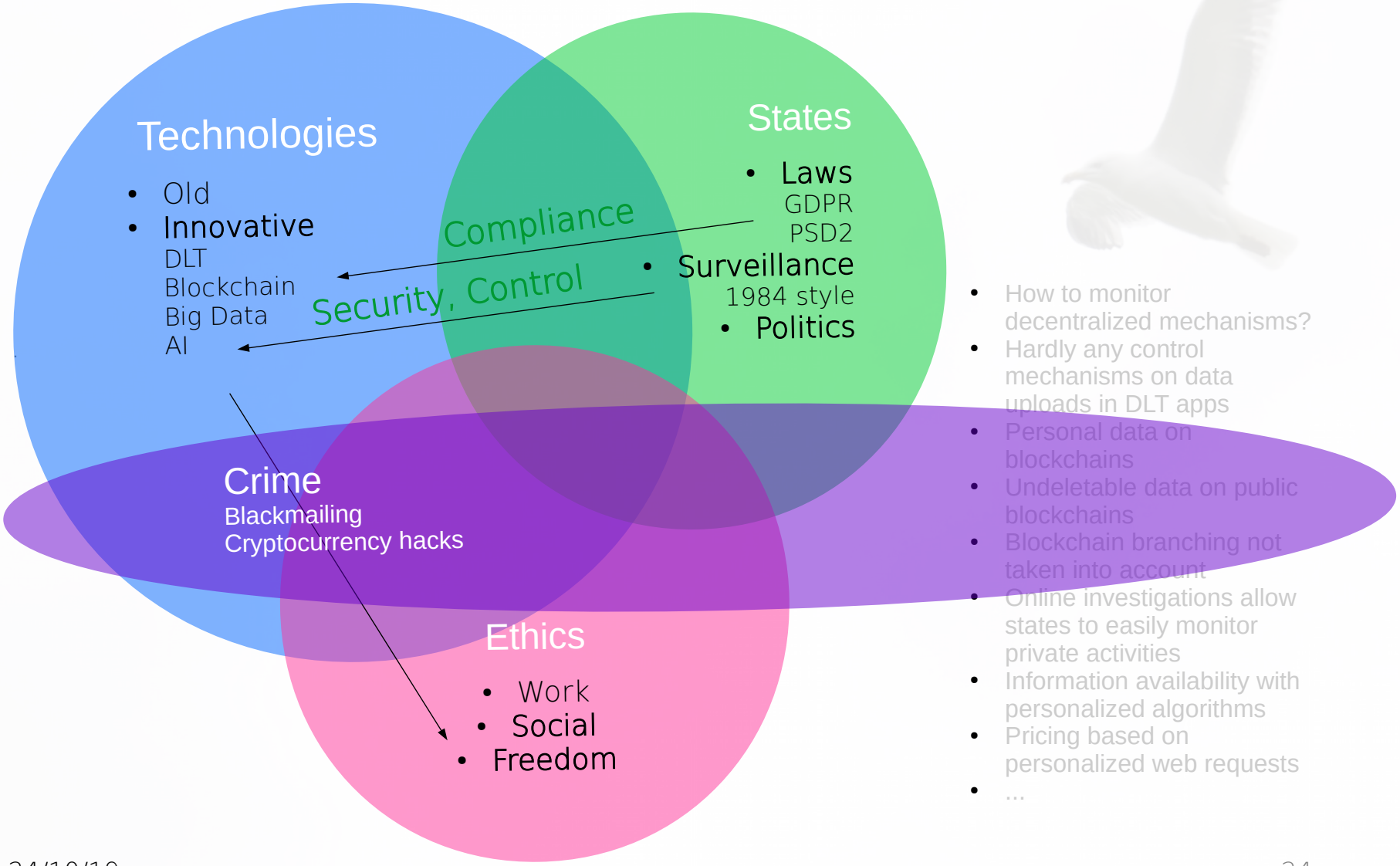
Expensive new hardware and no genuine message authentication!

→ Post-Quantum Cryptology
Key Exchange
Signature
Encryption

Run on classical devices and resist QC attacks!

Information Security

Challenges



- How to monitor decentralized mechanisms?
- Hardly any control mechanisms on data uploads in DLT apps
- Personal data on blockchains
- Undeletable data on public blockchains
- Blockchain branching not taken into account
- Online investigations allow states to easily monitor private activities
- Information availability with personalized algorithms
- Pricing based on personalized web requests
- ...

Quantum Computers and Crypto

An upcoming Bliss with side Effects

Rise of Quantum Computers Technology offers

- More computation power
- Possibility to build complex materials
- Different kind of algorithms to solve certain problems (integer factorization, needle in haystack, etc.)

As a consequence, classical asymmetric crypto is about to expire!

Official Quantum Tech Achievements

- IBM: 20 qubits QC commercially available in 2017
- IBM, Google: 50 qubits prototypes in 2017
- IBM: 53 qubits prototype in 2019
- Google: 72 qubit prototype bristlecone in March 2018!
- D-Wave 2048 qubits for quantum annealing to solve optimization problems in 2016
- Topological quantum bits announced in 2017
  (If successful, error correction problem which slows down quantum computation development will be considerably mitigated.)
  https://www.nist.gov/news-events/news/2019/08/newfound-superconductor-material-could-be-silicon-quantum-computers

Expiring Crypto Algorithms

Explaining a simple Term in a complex Context

What does “expire” mean in this context?

As soon as potent enough quantum computers are available, it will be possible to compute RSA, ECC and Diffie-Hellmann private keys with the knowledge of the public keys.

When will they expire?

We don’t know that and estimations vary. But IBM believes that they will be broken within 5 years:

https://www.afterdawn.com/news/article.cfm/2018/05/22/ibm-all-current-encryption-methods-will-be-broken-instantly-in-5-years-time

What will remain safe?

AES-256 is expected to be quantum computer attack proof with a security level comparable to AES-128 against binary computer attacks. So all encryption of static data is safe.

New Crypto Solutions

Replacements for up to 40 Years old Algorithms

Quantum Key Distribution

Quantum key distribution, key exchange based on quantum mechanical effects

- Expensive new hardware (ID quantique)
- Only for short distances (300-1200km in 2017)
- No genuine message authentication included, man in the middle is possible if no extra message authentication is added

QUESS: 2000km quantum communication channel between Shanghai and Bejing

SwissQuantum

SECQC Austria

Tokyo QDK Network

DARPA USA

Post-Quantum Cryptography

Alternative algorithms for key exchange based on hardness of mathematical problems other than integer factorization

- Being standardized by the NIST (2017-20219
- Some of them were already used for years and haven't been broken
- Run effectively on classical devices
- Can be enabled by software updates

Isara USA

KPN in Netherlands

Infineon

Microsofts experimental VPNs with algorithms that haven't been exposed publicly

some examples of established solutions

Post-Quantum Crypto

When does it make sense to start with Implementations?

When does it make sense to start with implementations?

If you are sending data out of your own network of which you think it might interesting enough for someone to collect now and decrypt it as soon as quantum computers are potent enough.

Signatures on documents which have to be valid longer than you believe it takes before the Quantum Computer threat becomes real and which cannot be easily updated. For example signatures on electronic passports.

Data on public blockchains which will have to remain private for longer than you believe it takes before the Quantum Computer threat becomes real. Think about the fact that copies of those chains are intended to exist forever.