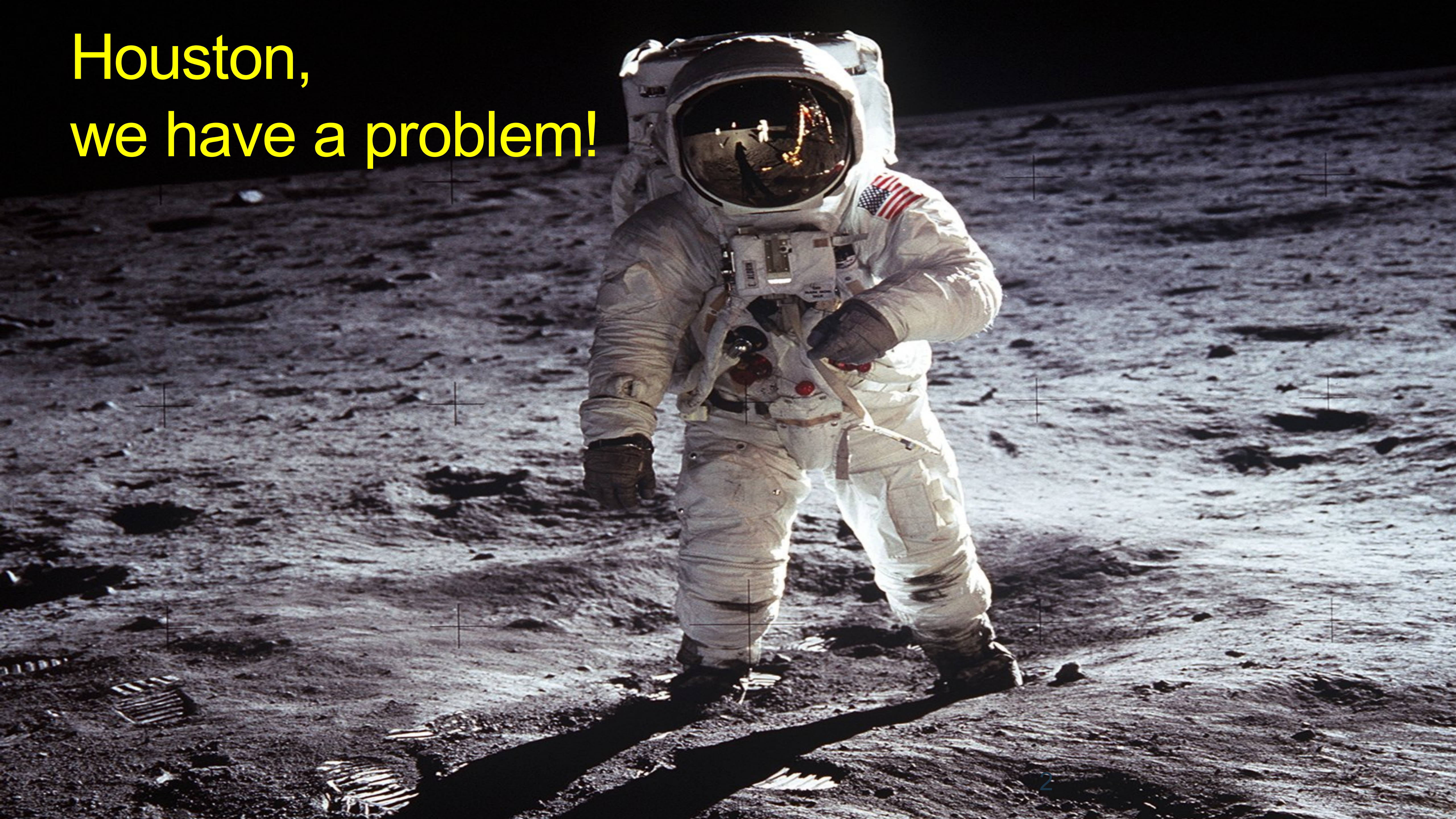
IBM Research: Shaping the Future of Cybersecurity

Dr. Maria Dubovitskaya
Cryptographer, IBM Research - Zurich

ICC Moscow, 2018



Houston, we have a problem!

Houston,
we have a problem!

“Buzz Aldrin's footprints are still up there”

(Robin Wilton)

Computers do not forget!

- Data storage ever cheaper
- Data mining ever better
- Internet is not a sandy beach
- But people build apps with the paper-based world in mind :-(
  - if it works it works
  - security too often still an afterthought
  - implementers too often have no crypto education
- Huge security problem!
  - Millions of hacked passwords
  - Stolen identities ($150 - 2005, $15 - 2009, $5 – 2013)

Facts

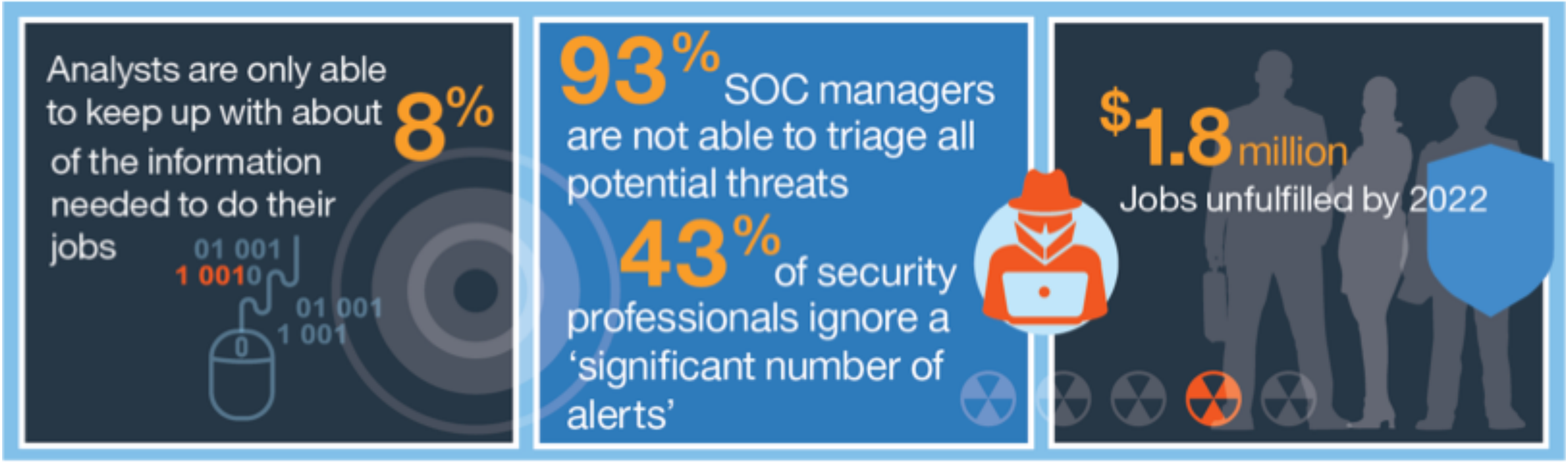
10 Years ago your personal data on the black market was worth $150. Today….

Facts

33% of cyber crimes, including identity theft, take less time than to make a cup of tea.

Did the data got out of our control?

Data Overload **Unaddressed Threats** **Skills Shortage**



Analysts are only able to keep up with about 8% of the information needed to do their jobs

93% SOC managers are not able to triage all potential threats

43% of security professionals ignore a ‘significant number of alerts’

$1.8 million Jobs unfulfilled by 2022

Let us take a look at Present and Future of Cybersecurity

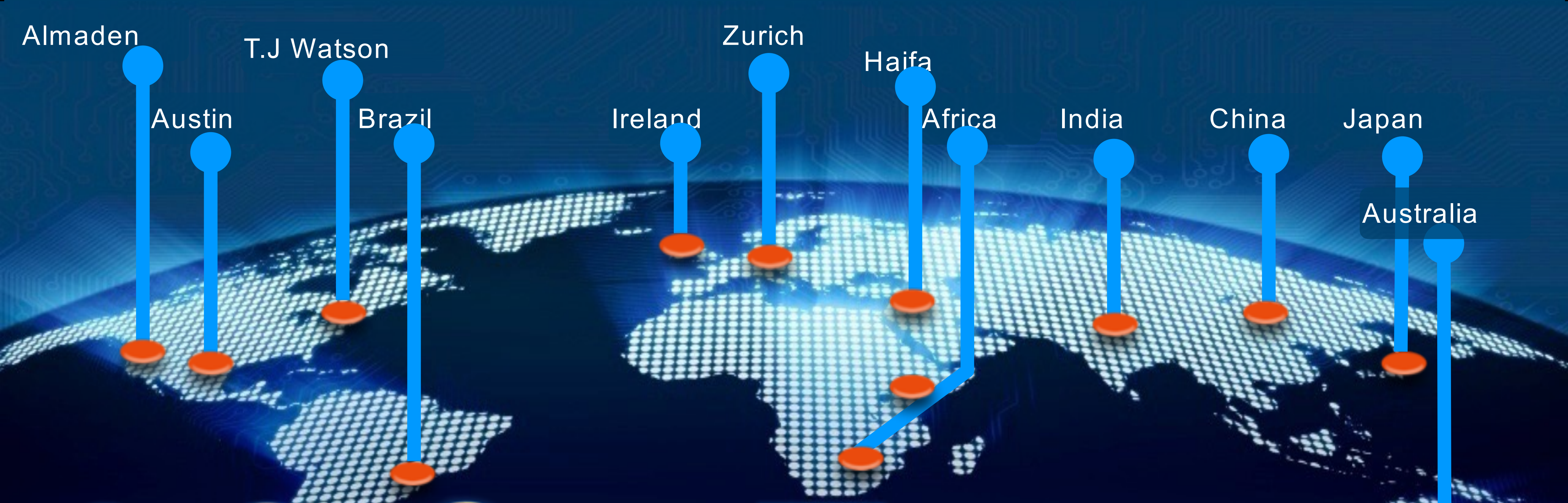
What is IBM Research?

The World is Our Lab

World's largest information technology research organisation

More than 3,000 scientists and engineers

IBM invested 6% of revenue on R&D in 2015



Six Nobel Laureates

Ten Medals of Technology

Five National Medals of Science

Three Kavli Prizes

Six Turing Awards

NATIONAL ACADEMY OF ENGINEERING

69 Members

IEEE

123 IEEE Fellows

acm

28 ACM Fellows

IBM

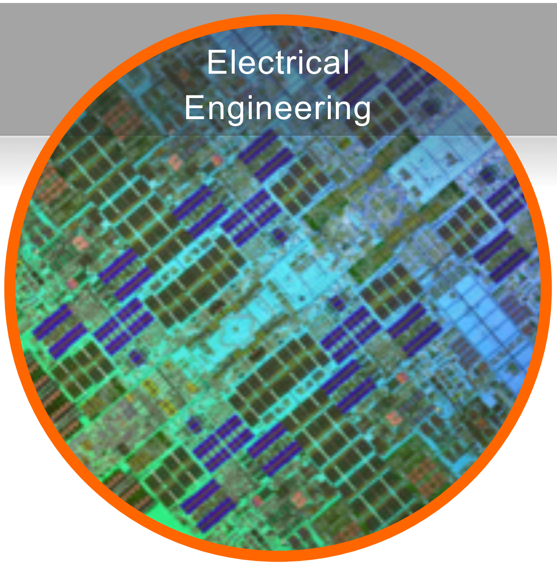
98 IBM Fellows

IBM Research: A diversity of core academic disciplines

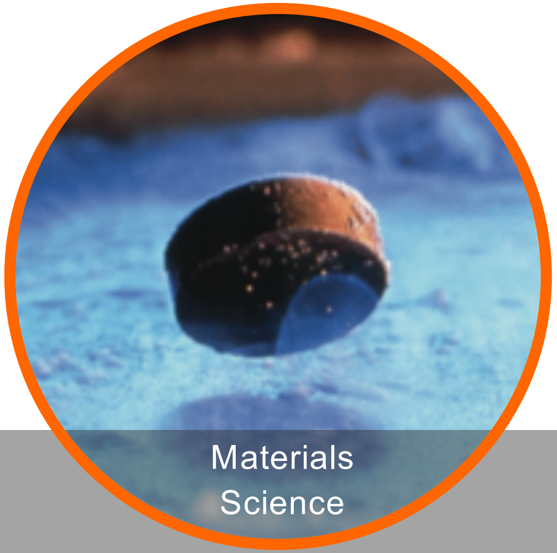
Behavioral Science

Chemistry

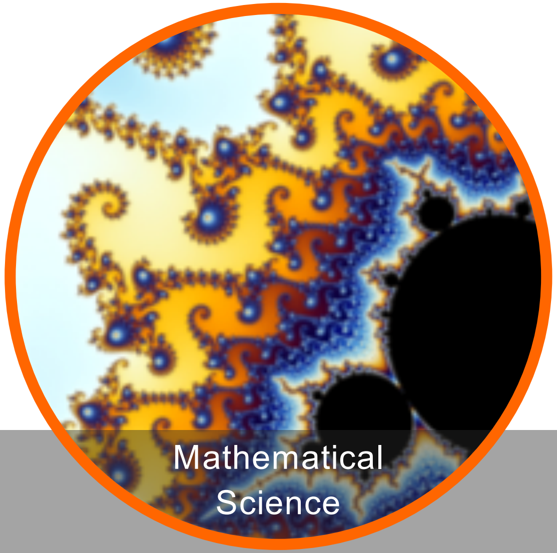
Computer Science



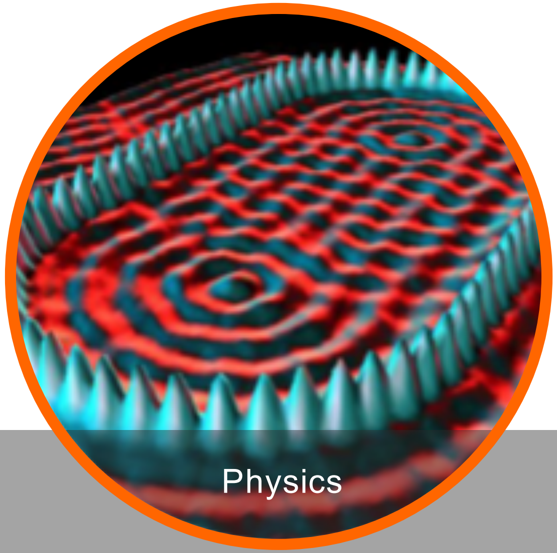
Electrical Engineering



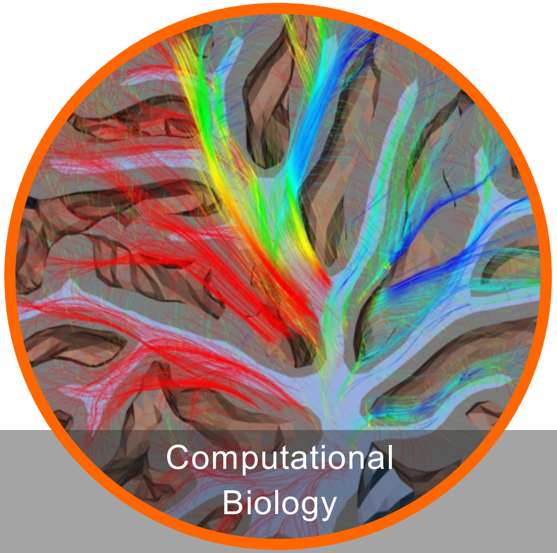
Materials Science



Mathematical Science



Physics



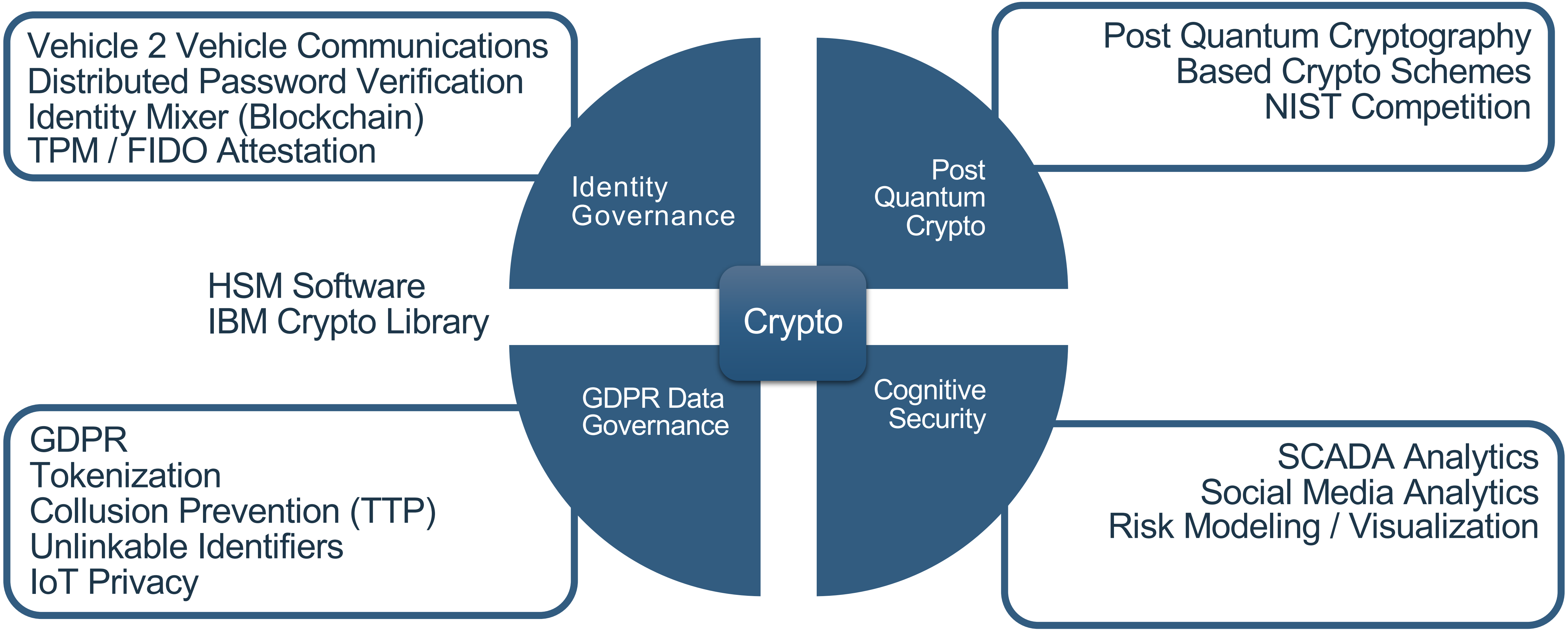
Computational Biology

IBM Research - Zurich

- Established in 1956
- 45+ different nationalities
- Open Collaboration:
  - Horizon2020: 43 funded projects and 500+ partners
- Two Nobel Prizes:
  - 1986: Nobel Prize in Physics for the invention of the scanning tunneling microscope by Heinrich Rohrer and Gerd K. Binnig
  - 1987: Nobel Prize in Physics for the discovery of high-temperature superconductivity by K. Alex Müller and J. Georg Bednorz
- Binnig and Rohrer Nanotechnology Centre opened in 2011 (Public Private Partnership with ETH Zürich and EMPA)
- 9 European Research Council Grants

IBM Security Research Overview

Security Research Overview



Vehicle 2 Vehicle Communications
Distributed Password Verification
Identity Mixer (Blockchain)
TPM / FIDO Attestation

Identity Governance

Post Quantum Crypto

Post Quantum Cryptography
Based Crypto Schemes
NIST Competition

HSM Software
IBM Crypto Library

Crypto

GDPR Data Governance

Cognitive Security

GDPR
Tokenization
Collusion Prevention (TTP)
Unlinkable Identifiers
IoT Privacy

SCADA Analytics
Social Media Analytics
Risk Modeling / Visualization

Cognitive Security and Risk Modelling

Security operations team are fundamental to business

Protect critical systems & data

Respond to incidents accurately and quickly

Outthink cyber criminals

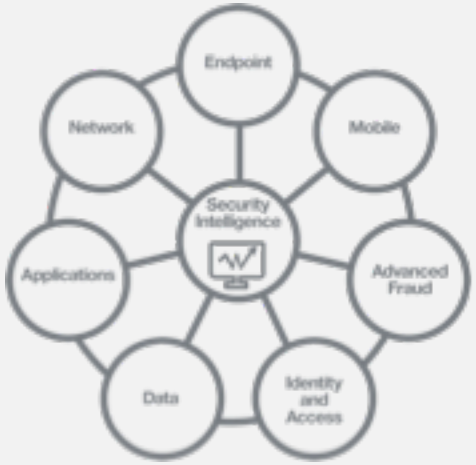
Cognitive is ushering in a new era of security

Moats and Castles
Pre-2005

Security Intelligence
2005+

Cognitive Security
2015+

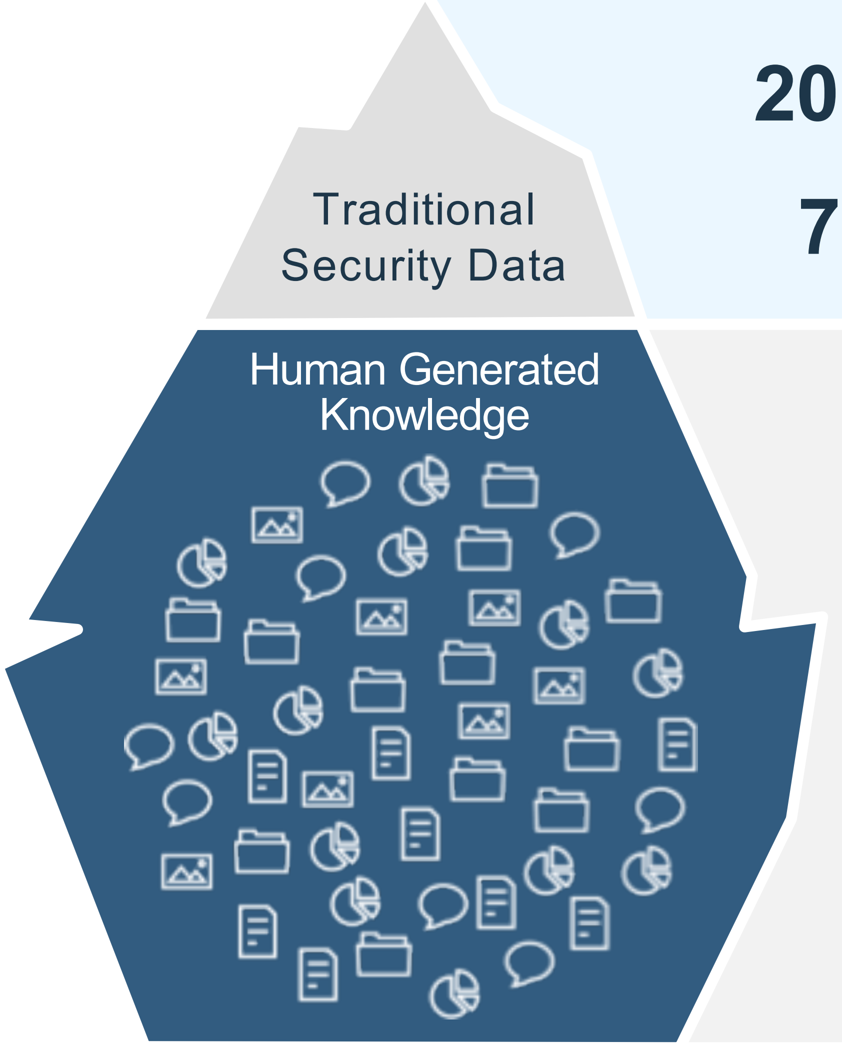
Deploy static defenses to guard or limit the flow of data, including firewalls, antivirus software and web gateways



Leverage analytics to collect and make sense of massive amounts of real-time data flow, prioritizing events and detecting high-risk threats in real-time

Interpret, learn and process security intelligence that was designed by and for humans, at speed and scale like never before

A tremendous amount of security knowledge is created for human consumption, but most of it is untapped



200K+ security events viewed each day

75K+ reported software vulnerabilities

- Security events and alerts
- Logs and configuration data
- User and network activity
- Threat and vulnerability feeds

A universe of security knowledge Dark to your defenses

Typical organizations leverage only 8% of this content*

720K security blogs / year

180K security related news articles / year

10K security research papers / year

- Industry publications
- Forensic information
- Threat intelligence commentary
- Analyst reports
- Conference presentations
- News sources
- Newsletters
- Tweets
- Wikis

[1] Forrester Research : Can You Give The Business The Data That It Needs? , 2013

A day in the life of investigating threats…

Rafael
Security Analyst

1 HOUR
Gets caught up on the latest security news through bulletins and social networks in order to identify new threats

3 HOURS
Repeatedly investigates potential security incidents via online sources

4 HOURS
Manually copies and pastes information from disparate and siloed tools to correlate data

All this mundane time spent, yet
STILL SO MANY FALSE POSITIVES!

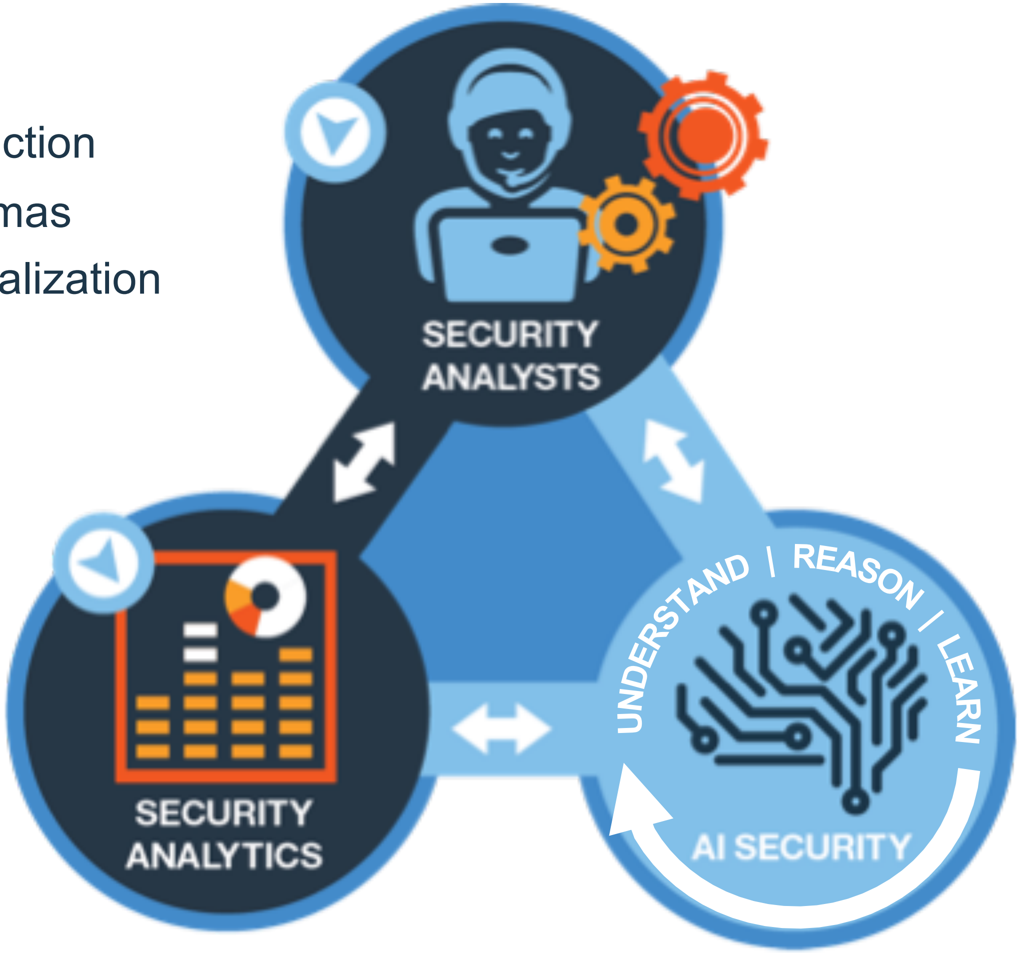
Artificial intelligence bridges this gap and unlocks a new partnership between security analysts and their technology

Human Expertise

- Common sense
- Morals
- Compassion
- Abstraction
- Dilemmas
- Generalization

Security Analytics

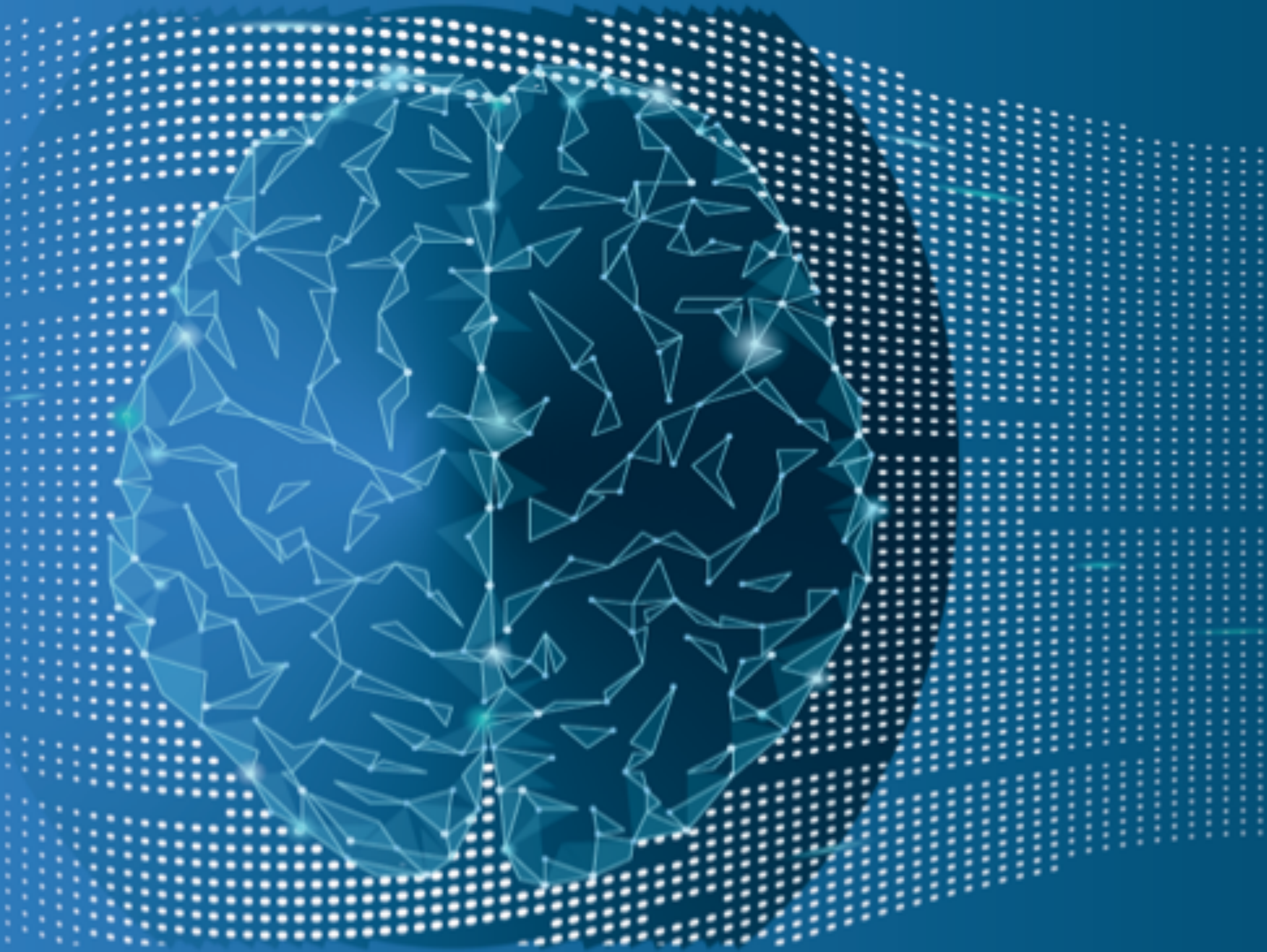
- Data correlation
- Pattern identification
- Anomaly detection
- Prioritization
- Data visualization
- Workflow



AI: Cognitive Security

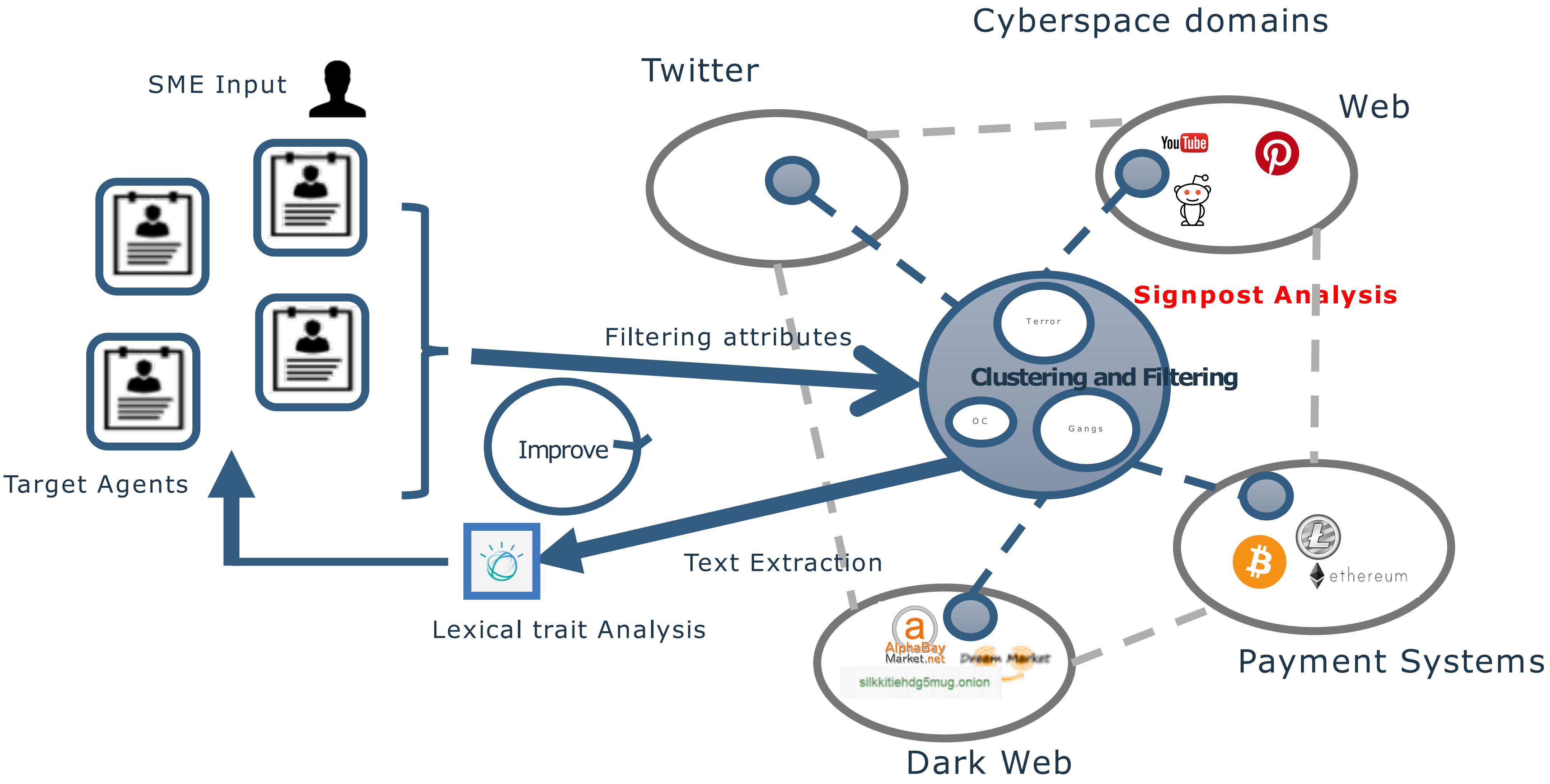
- Unstructured analysis
- Natural language
- Question and answer
- Machine learning
- Bias elimination
- Tradeoff analytics

How it works – Cognitive applied for cybersecurity



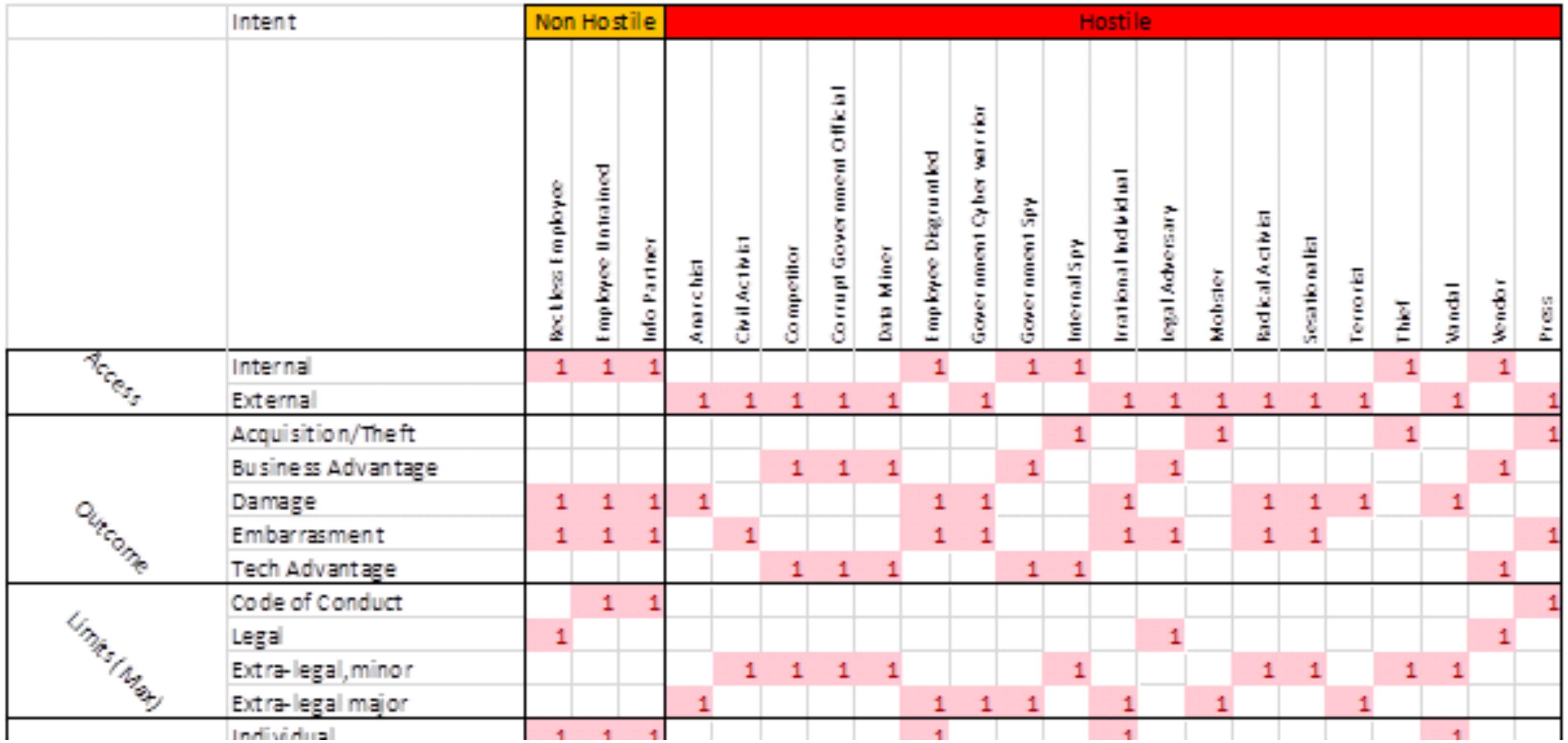
- Ingest mass amounts of data
- Classify, select, and normalize data
- Natural language processing for security context
- Training and learning with feedback
- Relational analysis visualized through knowledge graphs

PROTON Project: Searching for cybercriminals



Threat Agent Library

- The TAL tool defines a set of attacker profiles with attributes.
- Profiles are forms of personas that include:
  - Reckless Employee
  - Employee Untrained
  - Info Partner
  - Anarchist
  - Civil Activist
  - Competitor
  - …….
- Defined Attributes
- Simple Metrics



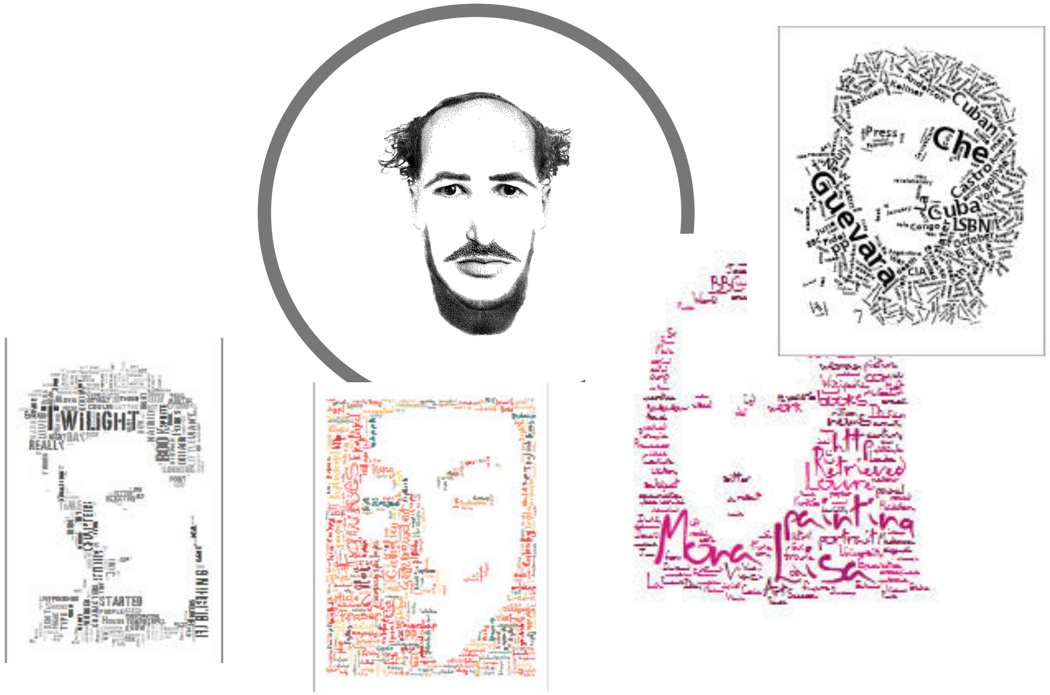
	Intent	Non Hostile			Hostile																		
		Reckless Employee	Employee Untrained	Info Partner	Anarchist	Civil Activist	Competitor	Corrupt Government Official	Data Miner	Employee Disgruntled	Government Cyber warrior	Government Spy	Internal Spy	Irrational Individual	legal Adversary	Mobster	Radical Activist	Sensationalist	Terrorist	Thief	Vandal	Vendor	Press
Access	Internal	1	1	1						1		1	1							1		1	
	External				1	1	1	1	1		1			1	1	1	1	1	1		1		1
Outcome	Acquisition/Theft												1			1				1			1
	Business Advantage						1	1	1			1			1							1	
	Damage	1	1	1	1					1	1			1			1	1	1		1		
	Embarrasment	1	1	1		1				1	1			1	1		1	1					1
	Tech Advantage						1	1	1			1	1									1	
Limits (Max)	Code of Conduct		1	1																			1
	Legal	1													1							1	
	Extra-legal,minor					1	1	1	1				1				1	1		1	1		
	Extra-legal major				1					1	1	1		1		1			1				
	Individual	1	1	1						1				1							1		

Modelling Agent Behavior / Personas

Combination of 3 concepts :

1. Persona concept originating in the usability design space
2. The Threat Agent Library (TAL) model used in the Threat Assessment & Remediation Analysis (TARA) for cyber risk modelling methodology
3. Lexical Analysis used for behavioral and /personality modeling

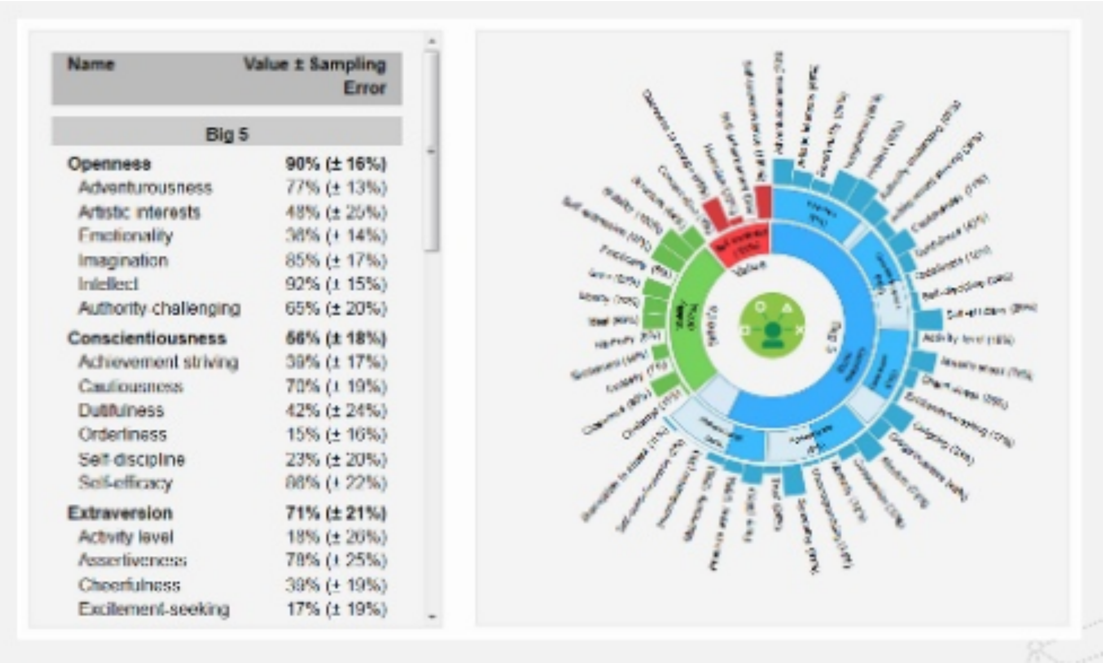
- By modelling agent traits we can :
  - Develop better risk models
  - Focus on prevention
  - Develop better search algorithms for cyberspace
  - Help bridge the gap between criminologists and cyber security/risk experts



Cognitive Interfaces

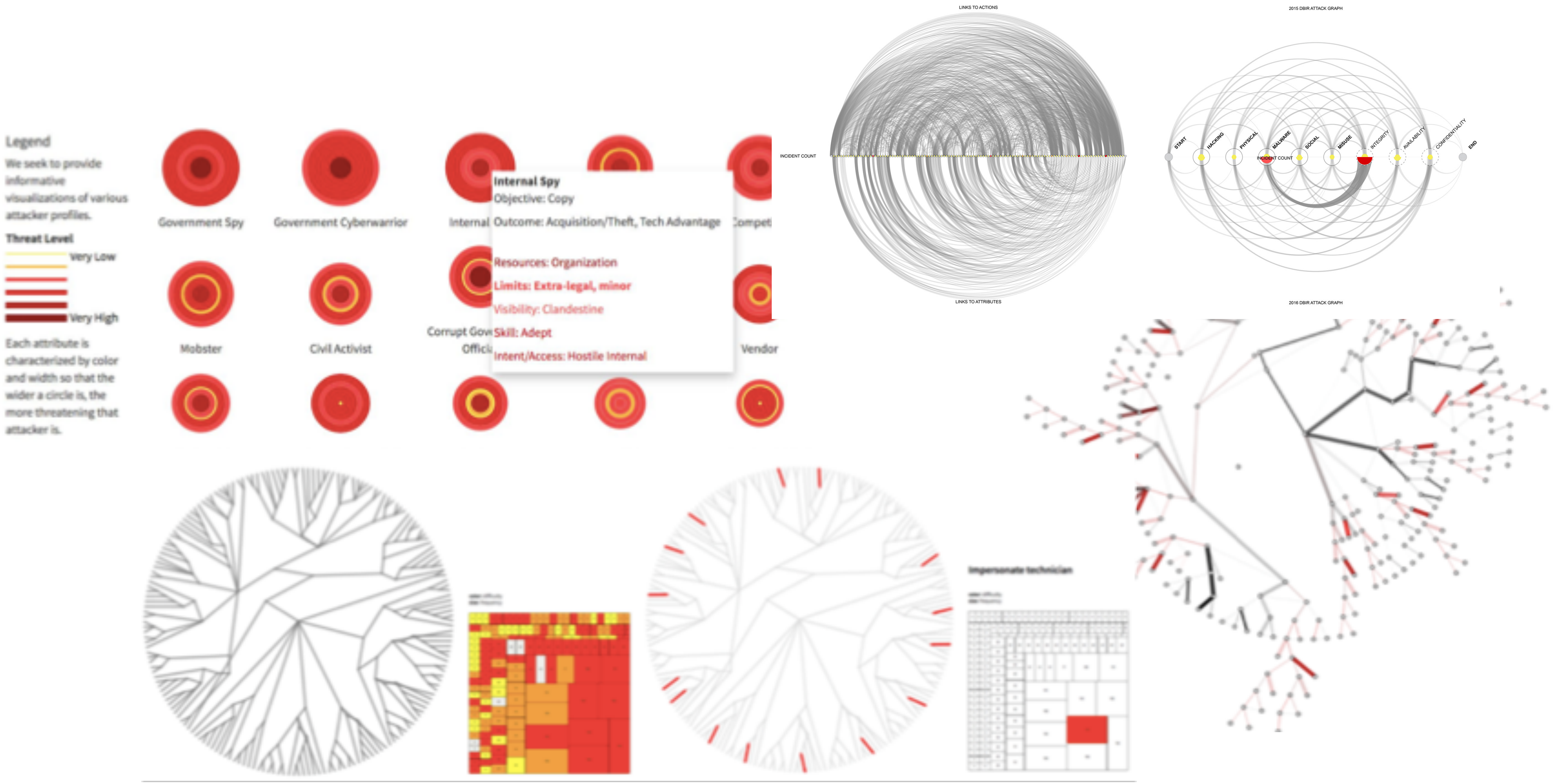
Watson Personality Traits
Linguistic Analytics
Big 5 Traits Classification

- Agreeableness
  - A person's tendency to be compassionate and cooperative toward others
- Conscientiousness
  - A person's tendency to act in an organized or thoughtful way
- Extraversion
  - A person's tendency to seek stimulation in the company of others
- Emotional Range
  - The extent to which a person's emotions are sensitive to the individual's environment
- Openness
  - The extent to which a person is open to experiencing a variety of activities



Name	Value ± Sampling Error
Big 5	
Openness	**90% (± 16%)**
Adventurousness	77% (± 13%)
Artistic interests	48% (± 25%)
Emotionality	38% (± 14%)
Imagination	85% (± 17%)
Intellect	92% (± 15%)
Authority-challenging	65% (± 20%)
Conscientiousness	**66% (± 18%)**
Achievement striving	39% (± 17%)
Cautiousness	70% (± 19%)
Dutifulness	42% (± 24%)
Orderliness	15% (± 16%)
Self-discipline	23% (± 20%)
Self-efficacy	08% (± 22%)
Extraversion	**71% (± 21%)**
Activity level	18% (± 20%)
Assertiveness	78% (± 25%)
Cheerfulness	39% (± 19%)
Excitement-seeking	17% (± 19%)

Visualizing Risk



Legend

We seek to provide informative visualizations of various attacker profiles.

Threat Level

Very Low

Very High

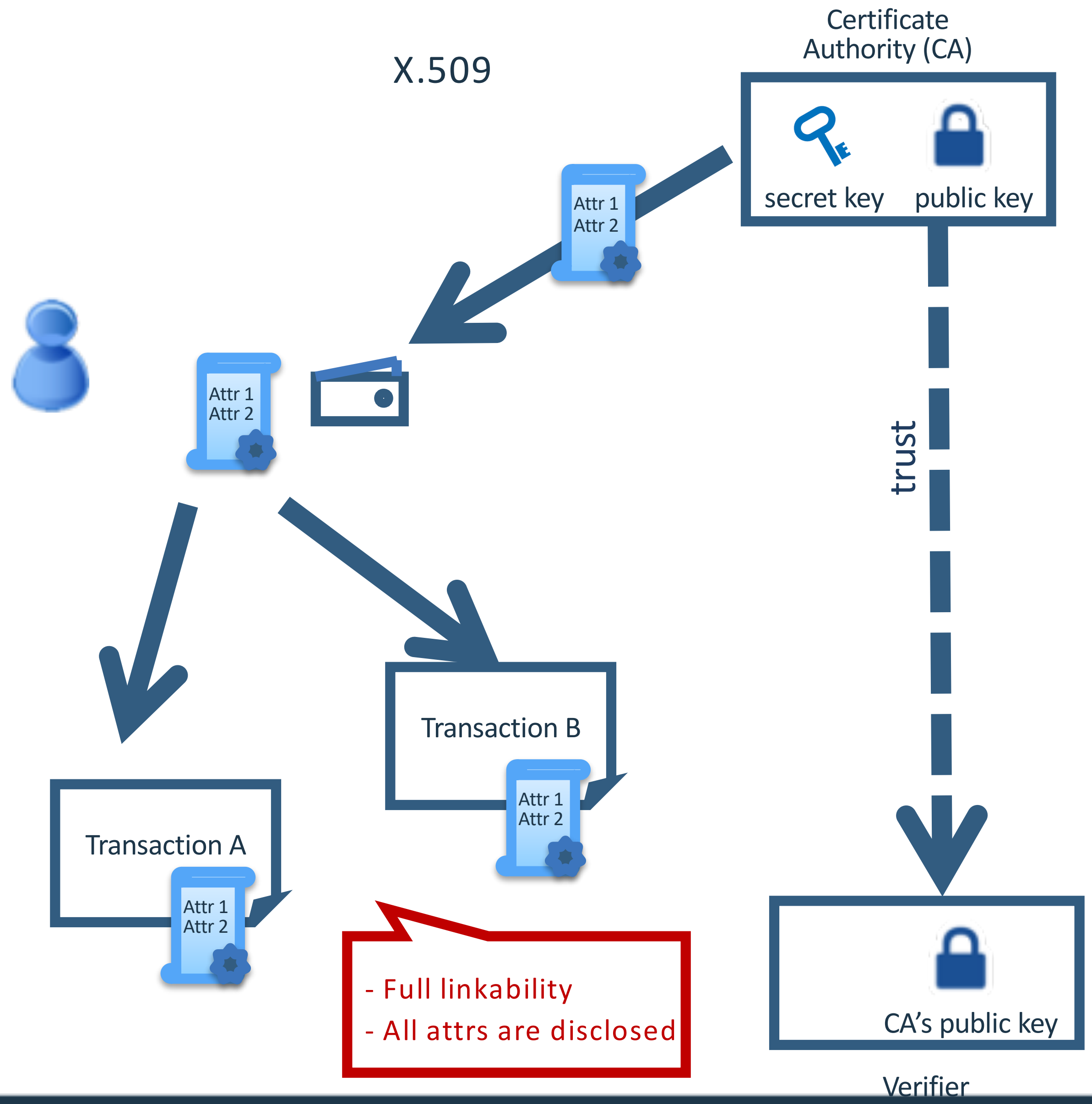
Each attribute is characterized by color and width so that the wider a circle is, the more threatening that attacker is.

Internal Spy
Objective: Copy
Outcome: Acquisition/Theft, Tech Advantage
Resources: Organization
Limits: Extra-legal, minor
Visibility: Clandestine
Skill: Adept
Intent/Access: Hostile Internal

Identity Governance

How can I trust you without knowing who you are?

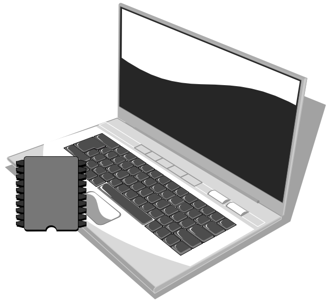
Signing transactions with a single X.509 Certificate



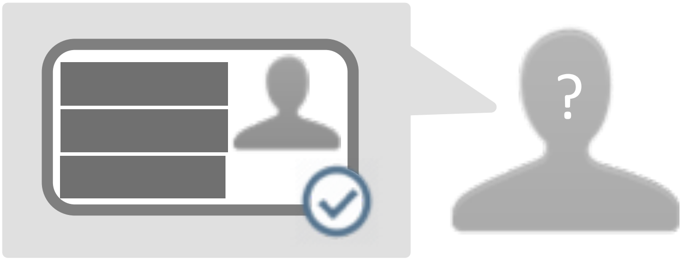
- Full linkability
- All attrs are disclosed

How can I trust you?

Computers

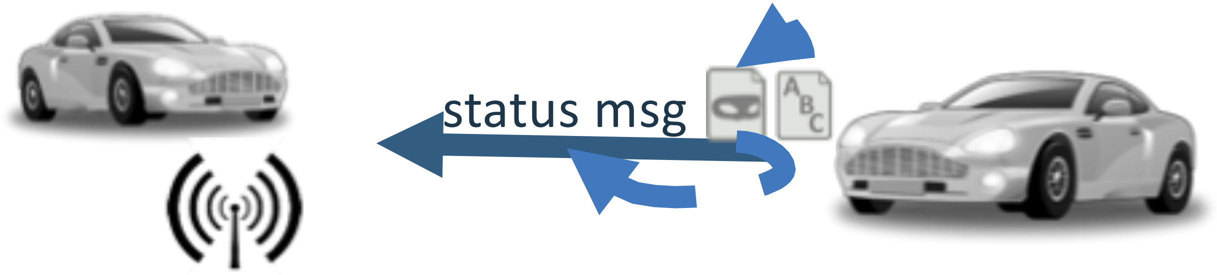


Electronic Identites



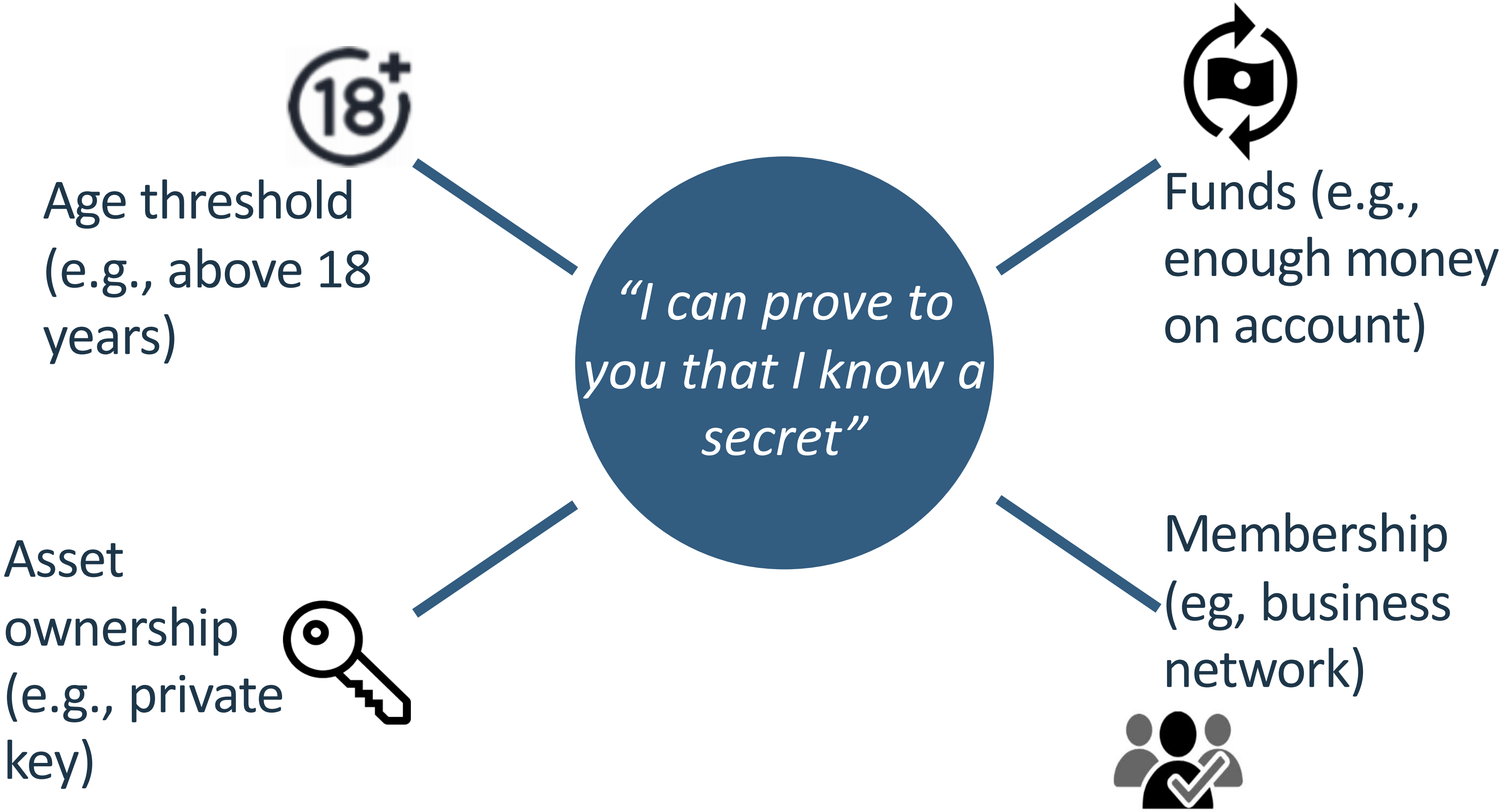
?

Vehicles



Blockchain transactors

How to combine public verifiability with privacy?
Using Zero-Knowledge Proofs (ZKP)!



“I can prove to you that I know a secret”

Age threshold (e.g., above 18 years)

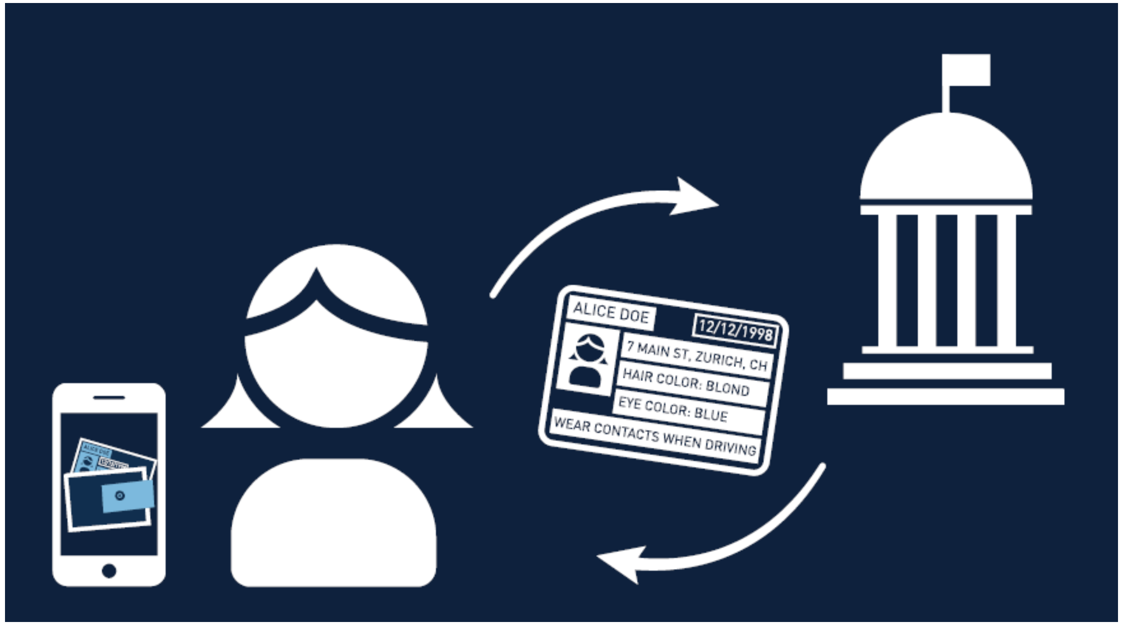
Funds (e.g., enough money on account)

Asset ownership (e.g., private key)

Membership (eg, business network)

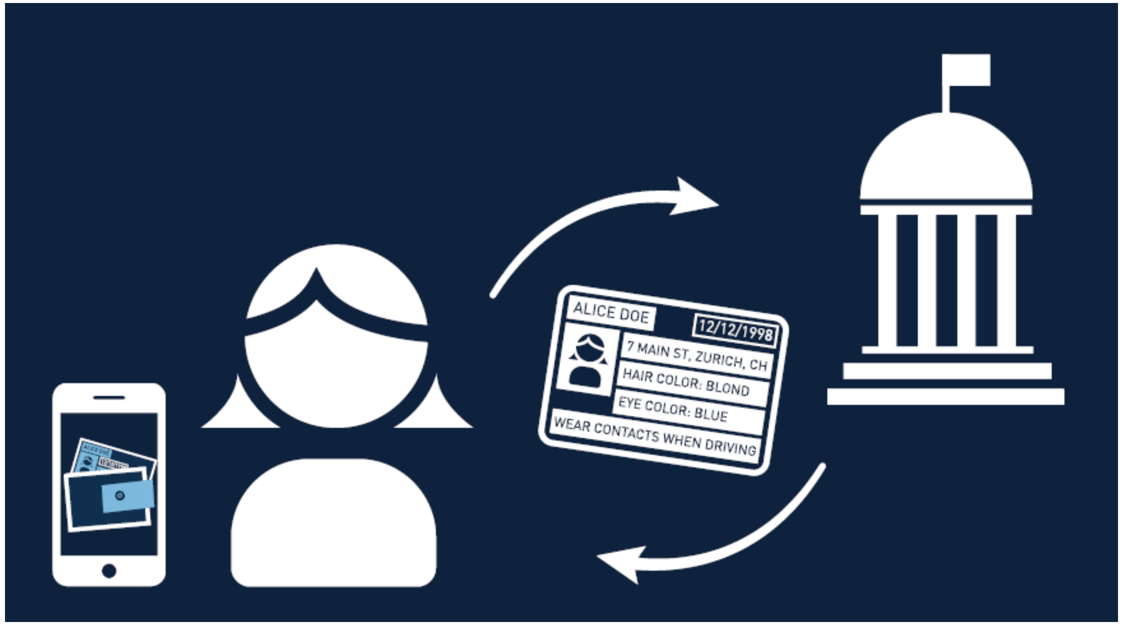
Identity Mixer

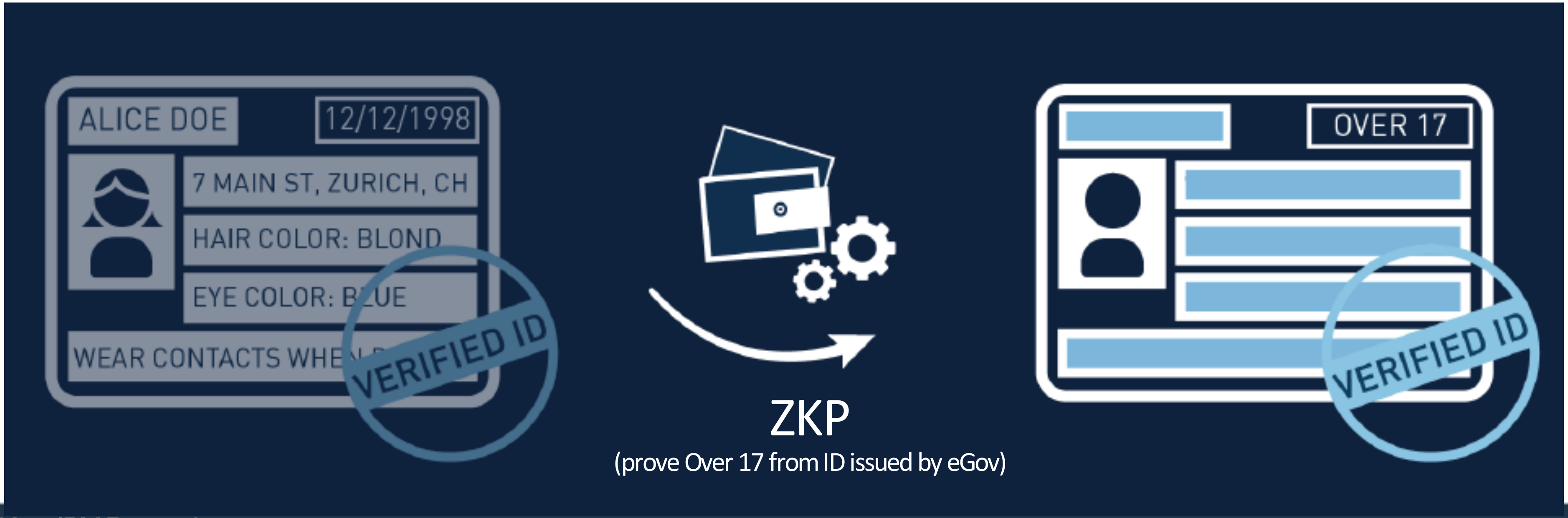
- Attribute-based credentials
- Strong authentication (signatures)
- Privacy-preserving Access Control
  - Selective disclosure of attributes, predicates over attributes, full unlinkability
- Auditability
- Revocation
  - Preserving privacy and unlinkability



Identity Mixer

- Attribute-based credentials
- Strong authentication (signatures)
- Privacy-preserving Access Control
  - Selective disclosure of attributes, predicates over attributes, full unlinkability
- Auditability
- Revocation
  - Preserving privacy and unlinkability



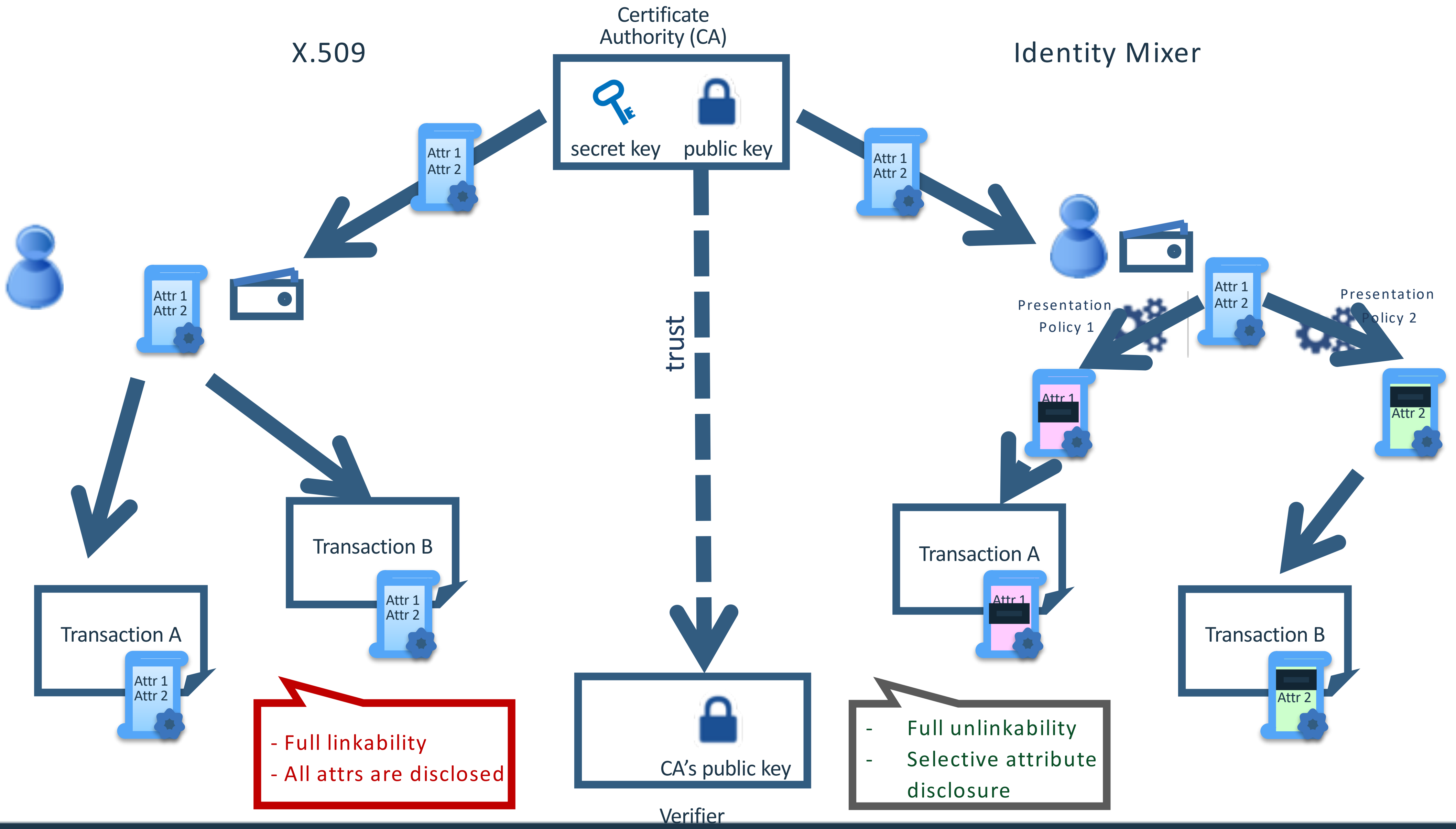


ZKP

(prove Over 17 from ID issued by eGov)

- Verification is done with the public key of the CA only

x.509 vs. Identity Mixer: better privacy with Identity Mixer



- Full linkability
- All attrs are disclosed

- Full unlinkability
- Selective attribute disclosure

Direct Anonymous Attestation for (IoT) devices

Protocol standardized by Trusted Computing Group

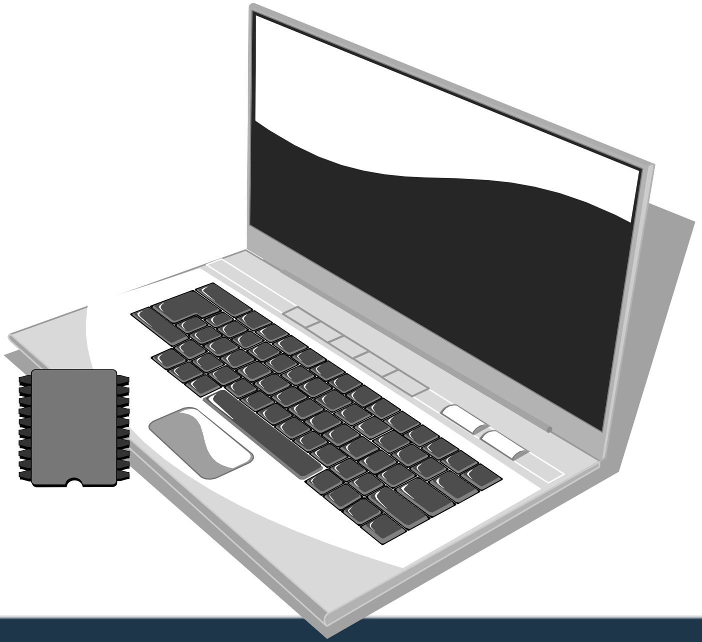
to attest boot sequence by TPM (root of trust) to third party

Other use cases:

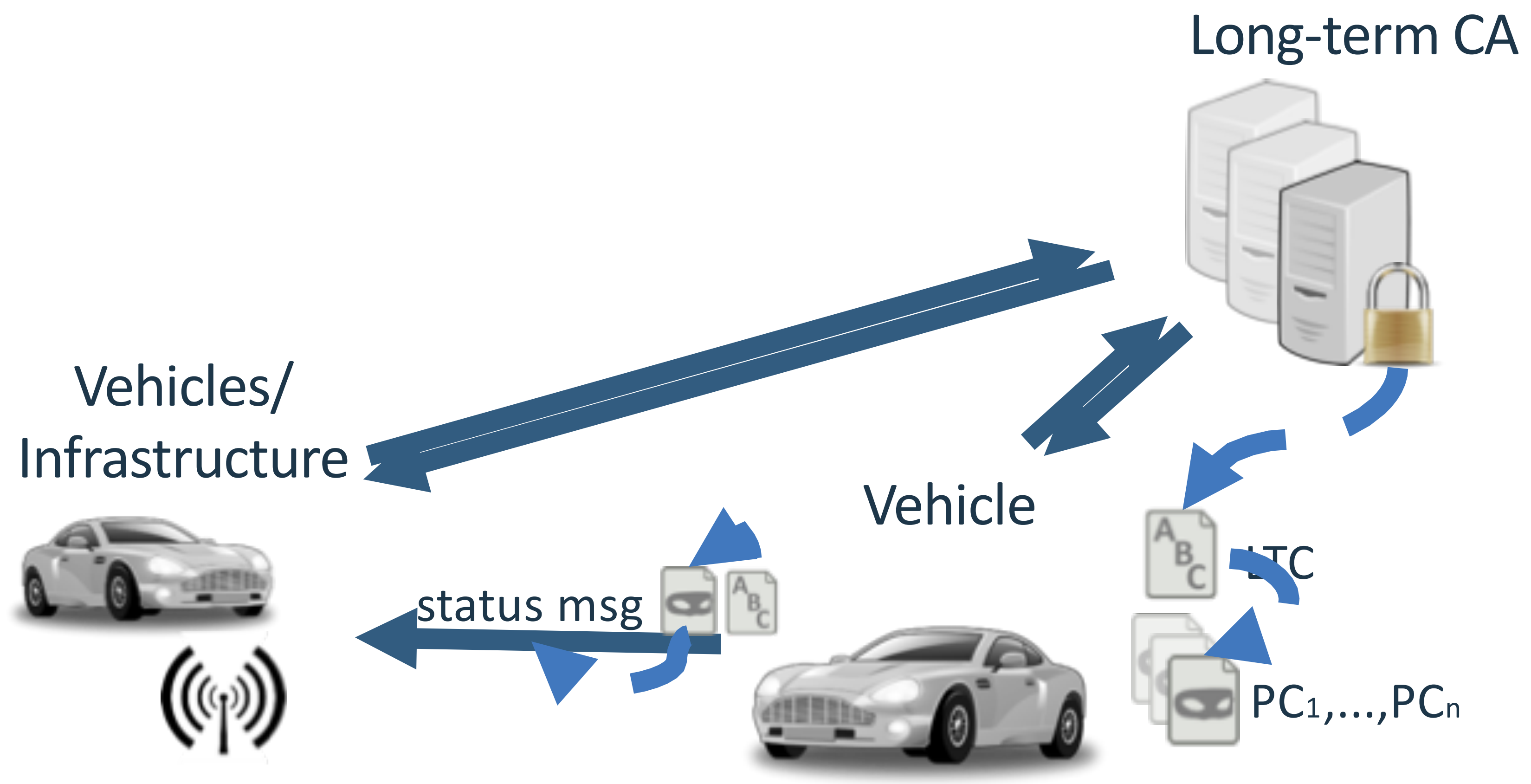
- Secure access to networks, services, any resources
- Secure mobile devices
- FIDO authentication

Security requirements:

- unforgeability,
- non-frameability,
- anonymity,
- revocability



Identity Mixer in V2V: privacy and security can co-exist



Identity and Blockchain:

much more than consensus and hashing

Hyperledger Fabric: Distributed ledger platform

HYPERLEDGER FABRIC 1.0
27 ORGANIZATIONS
159 DEVELOPERS
3,500 CHANGE SETS

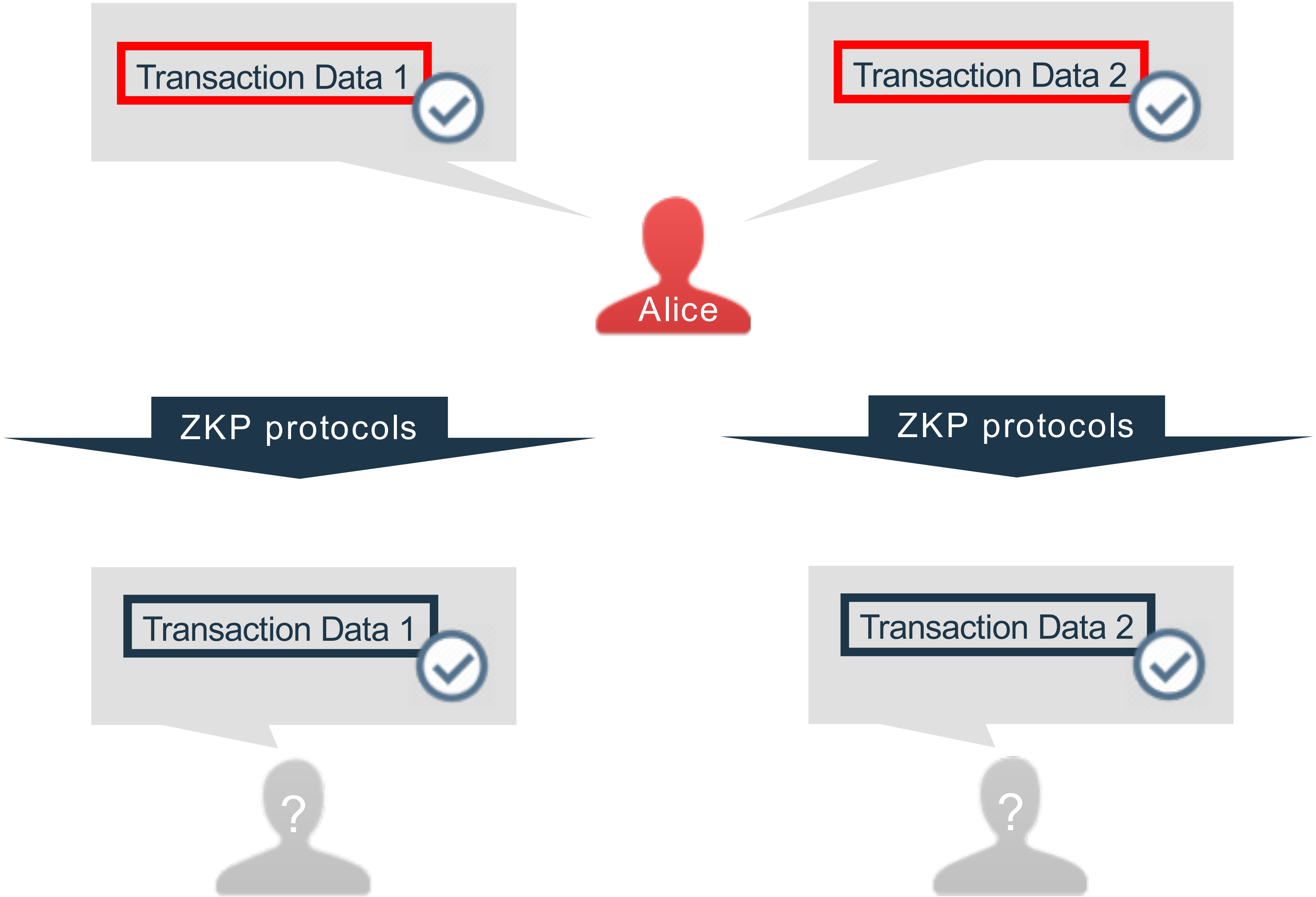
- **Channels** for sharing confidential information
- **Ordering Service** delivers transactions consistently to peers in the network
- **Endorsement policies** for transactions
- **CouchDB** world state supports wide range of queries
- Bring-your-own **Membership Service Provider (MSP)**

A significant milestone for the open source business blockchain community. Hyperledger

- A general-purpose permissioned blockchain system for enterprise applications.
- Modular approach: pluggable consensus, membership providers, crypto providers and so on.
- Based on the execute-order-validate paradigm.
- V1.1 released March 2018
  - 159 developers from 27 organizations
  - IBM is one contributor of code, IP and development effort to Hyperledger Fabric

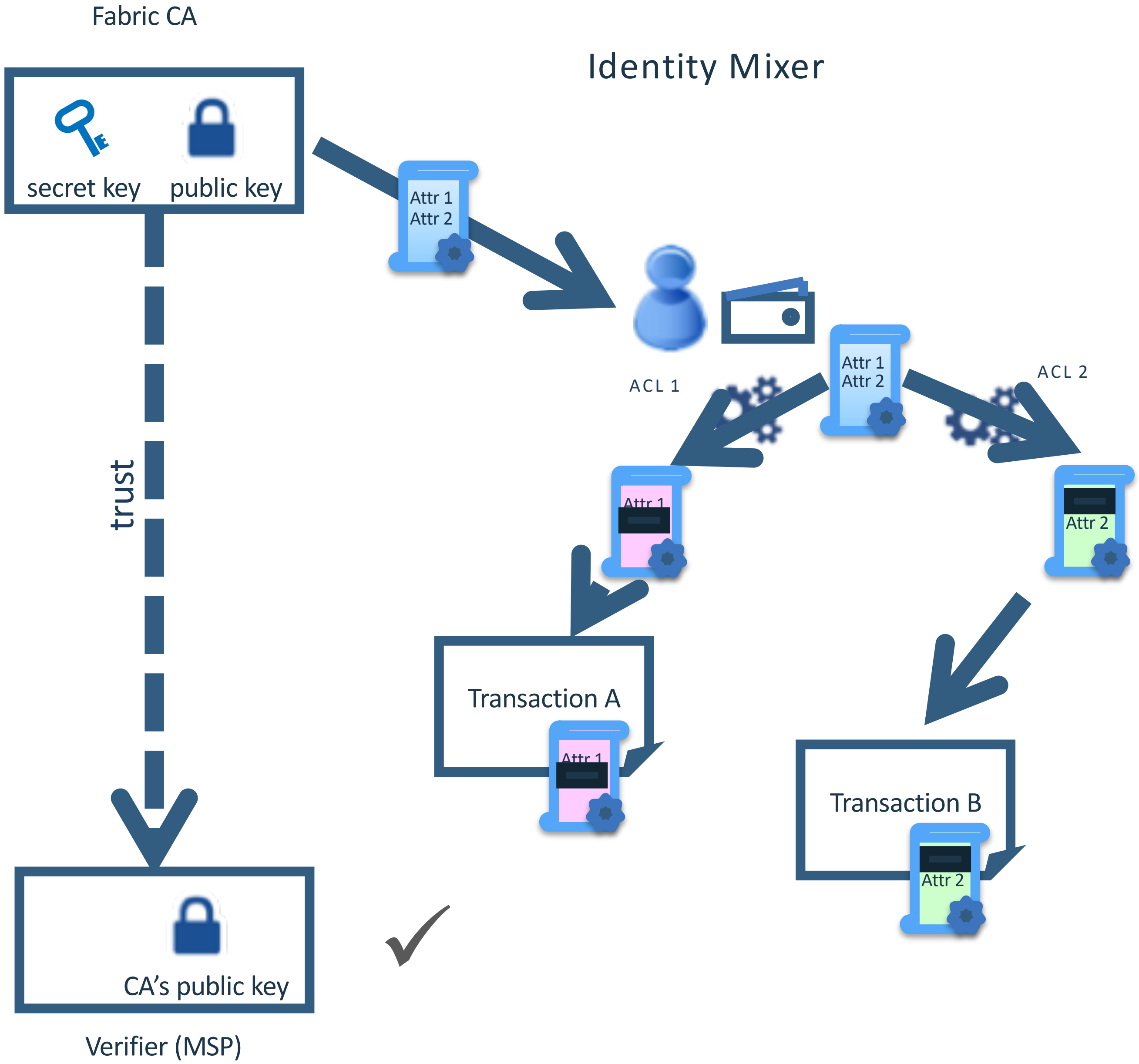
http://hyperledger-fabric.readthedocs.io/

Privacy-Preserving Transactions

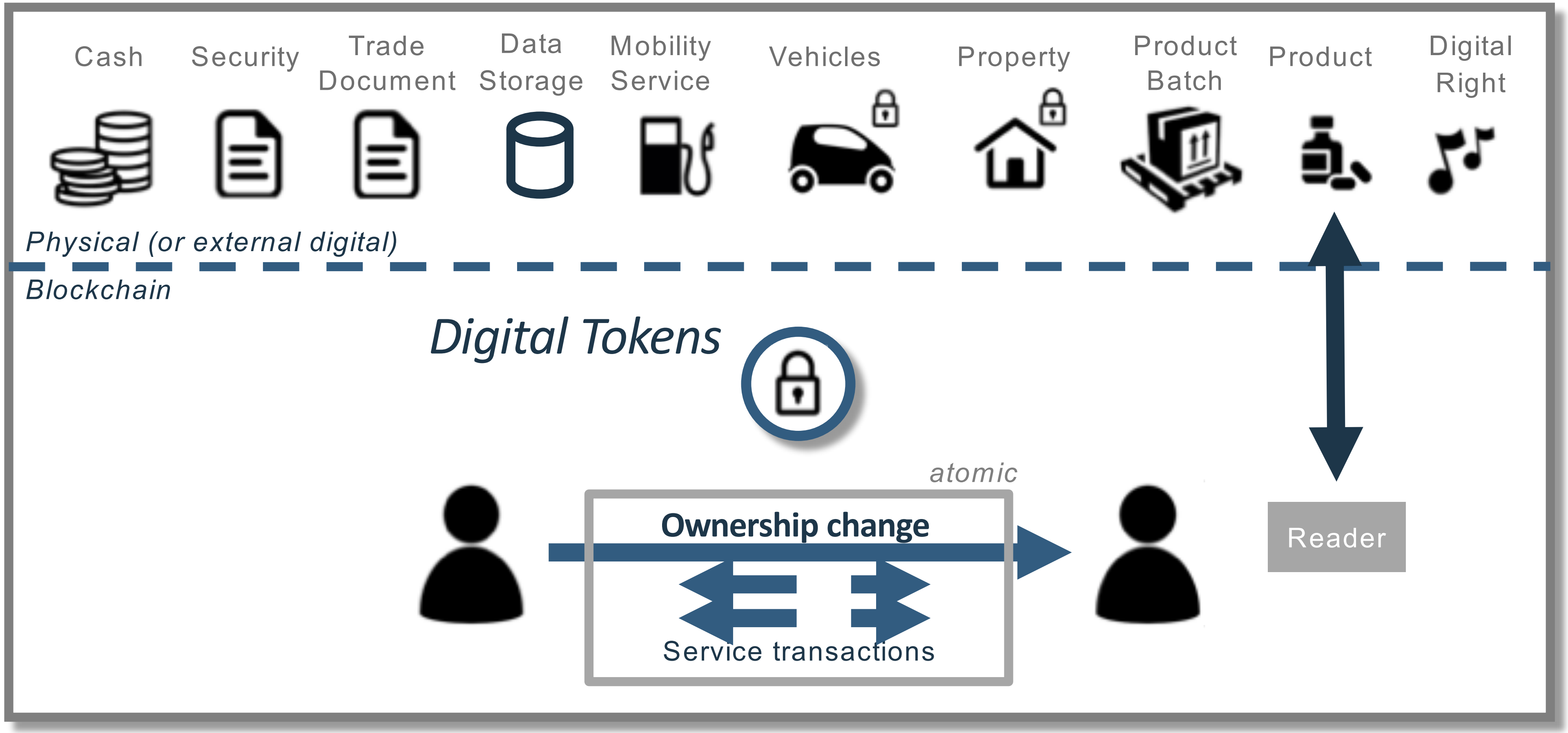


Identity Mixer in HL Fabric

- Approach:
  - Enrollment certificate = Identity Mixer Credential
  - Transaction certificate = ZKP of Enrollment Certificate
- Features:
  - Unlinkability and Privacy
  - Revocation (future release)
  - Auditing (future release)
- Components:
  - MSP (Membership Service Provider)
  - Fabric-CA
  - Client SDK



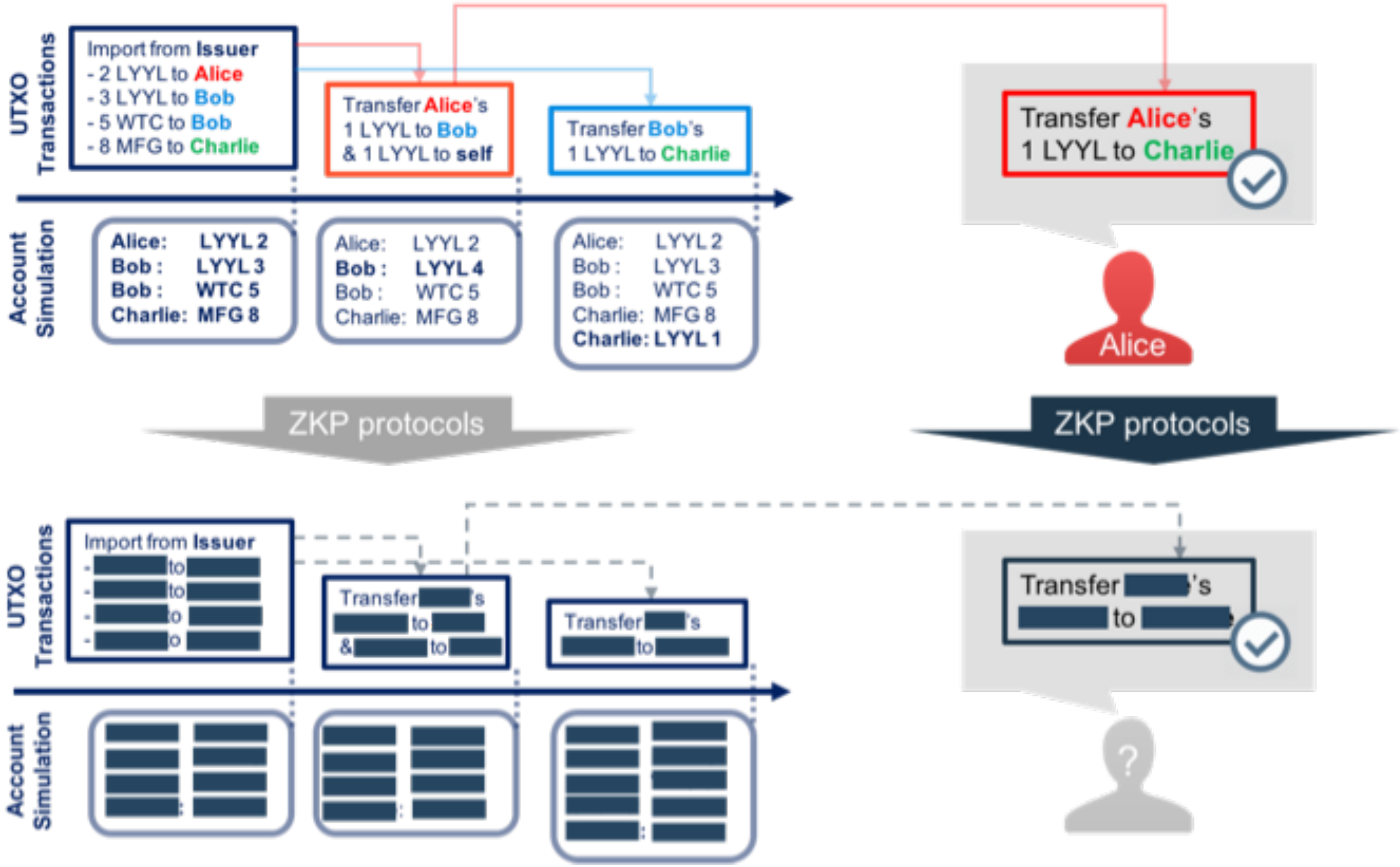
Assets can be conveniently represented with digital tokens



Use cases

- Securities trading
- Asset transfer
- Digital currency
- Supply chain
- Provenance
- …

Hiding Transaction Owner AND Content

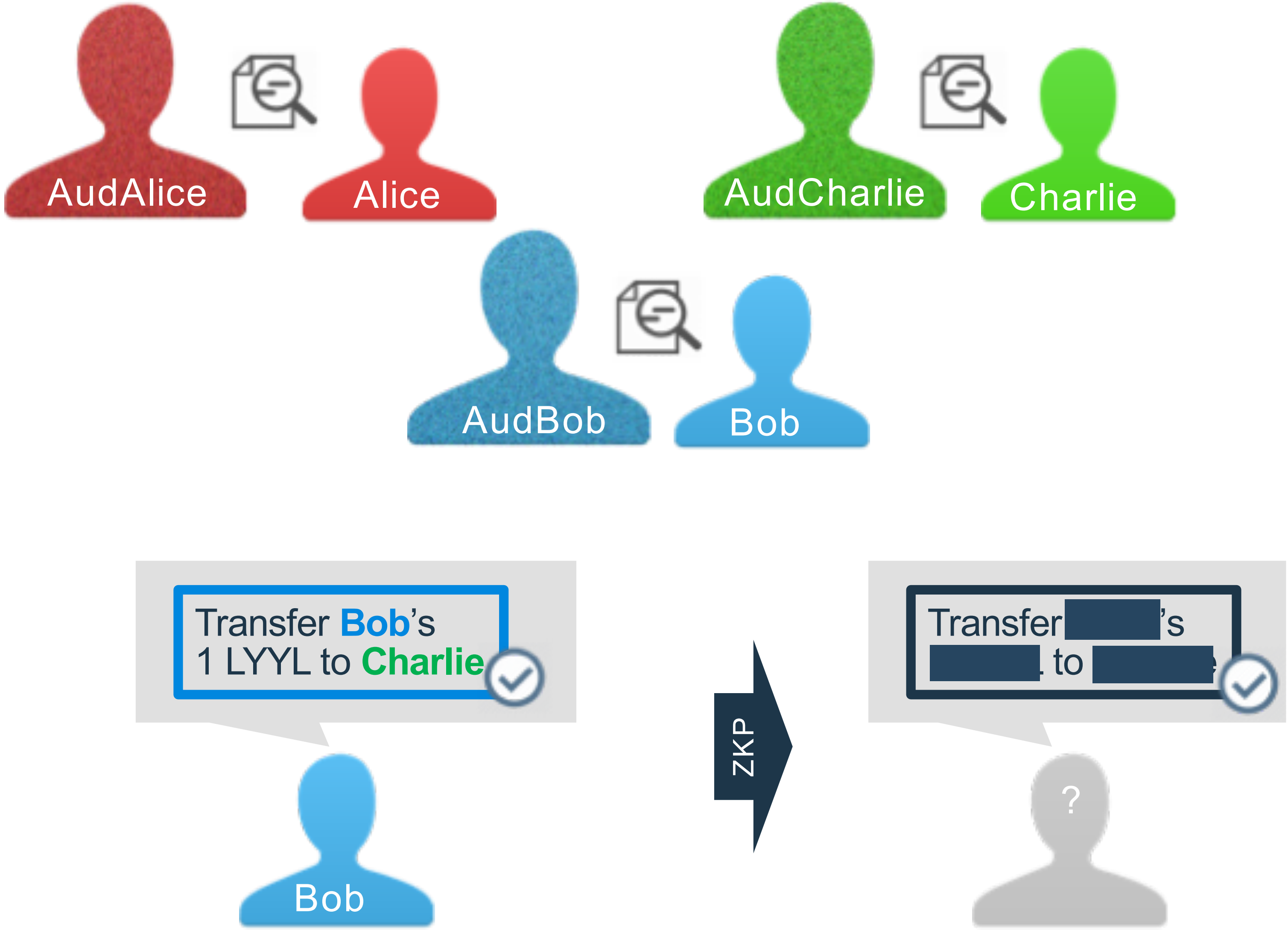


Auditability in privacy-preserving asset management can be served with Zero-Knowledge proofs

Alice and her friends have agreed on a shared ledger and user-authentication mechanisms; ***auditor assignment takes place.***

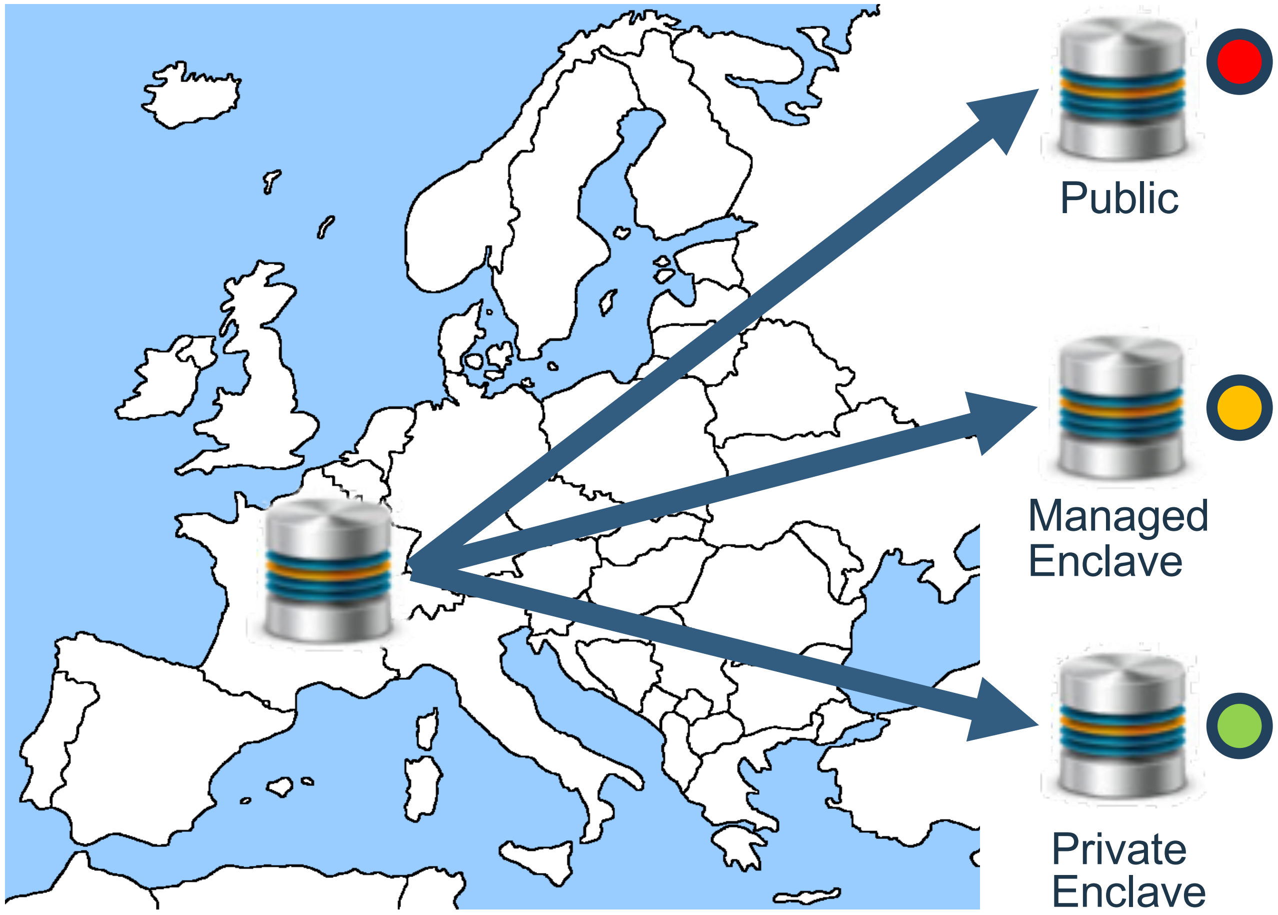
The statement:
Anonymous claims that private transaction ***grants access to the transactor's assigned auditor***

Zero-knowledge proof:
How can Anonymous (e.g., ***Bob****) prove the statement* ***without revealing*** *her identity, or the asset, or the auditor identity?*


AudAlice
Alice
AudCharlie
Charlie
AudBob
Bob
Transfer Bob's 1 LYYL to Charlie
Bob
ZKP
Transfer [redacted]'s [redacted] to [redacted]
?

Data Security and Governance: Storing Data Safely

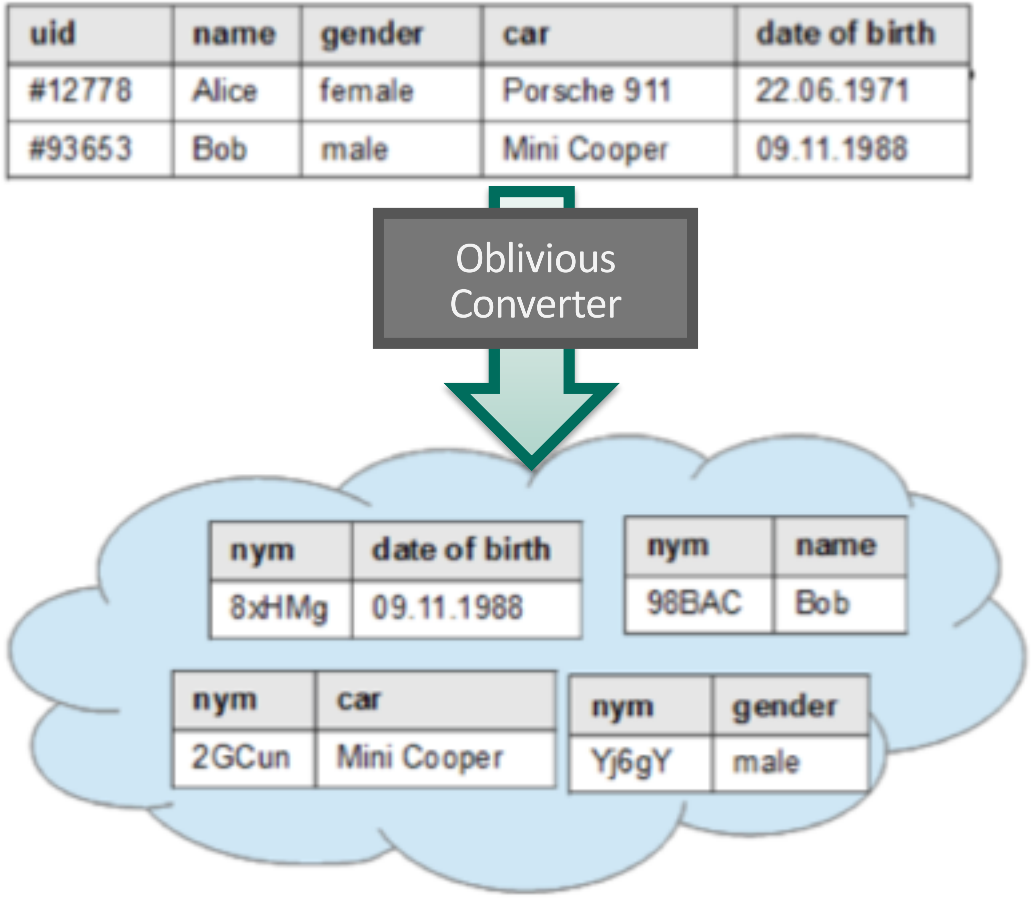
Data Location, Control and Risk



Example Scenarios	Technology
Open Data Data Publishing Fire and Forget	Full Anonymisation
Cloud Hosting Offsite Outsourcing Supply Chain Integration Partnerships/Collaborations Mergers & Acquisitions External Analytics	Tokenisation with Partial Anonymization
Off-shoring within an Organisation International consolidation of activities Centralised Processes Companywide Analytics Internal Segregation (HR Data)	Tokenisation

Data Security: storing data safely

- Data is scattered into (un)linkable pieces
- Secure even if data is stolen
- Requirement for compliance with GDPR



uid	name	gender	car	date of birth
#12778	Alice	female	Porsche 911	22.06.1971
#93653	Bob	male	Mini Cooper	09.11.1988

nym	date of birth
8xHMg	09.11.1988

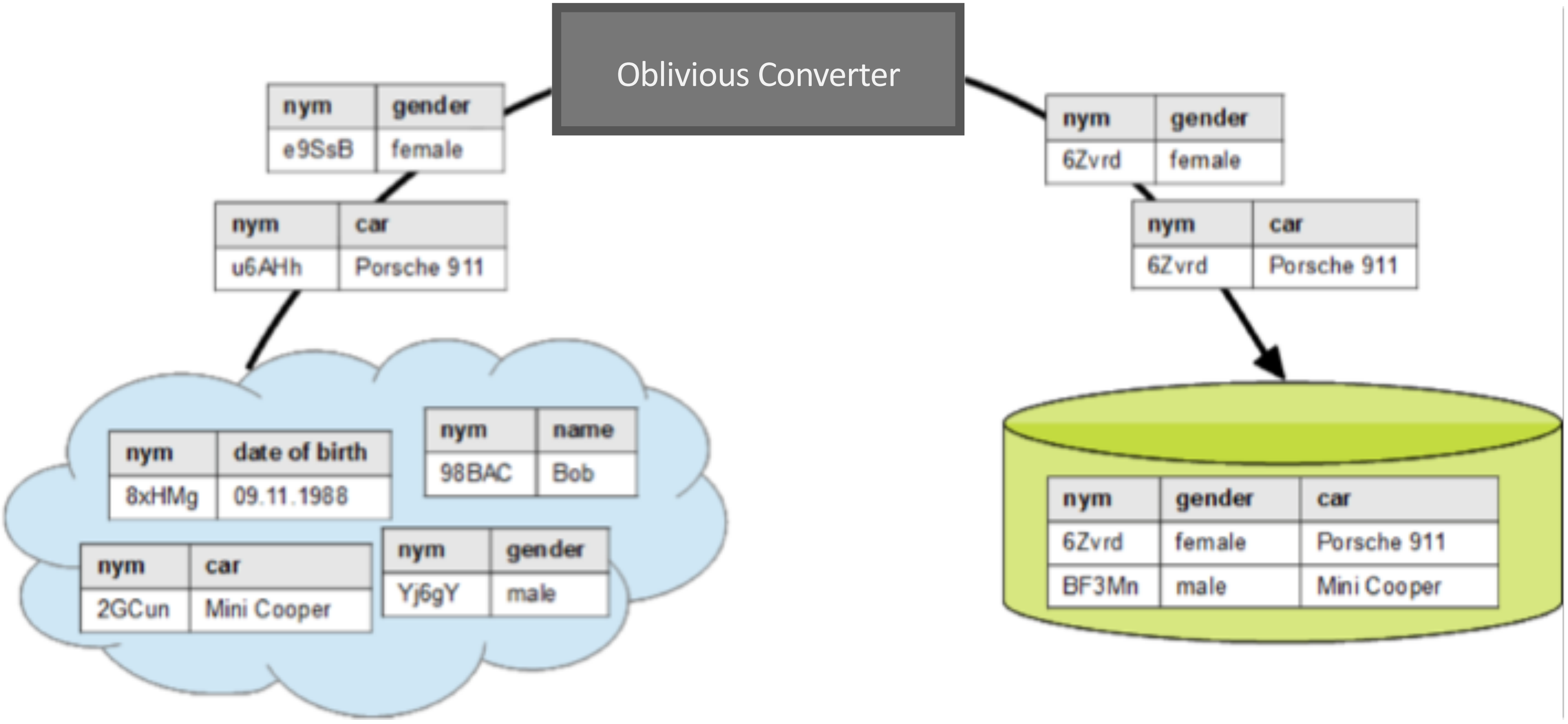
nym	name
98BAC	Bob

nym	car
2GCun	Mini Cooper

nym	gender
Yj6gY	male

Data Security and Compliance: retrieving the data

- „Unlinkable“ sub-sets are made linkable w.r.t. new pseudonym
- User consent can be enforced



nym	gender
e9SsB	female

nym	car
u6AHh	Porsche 911

nym	date of birth
8xHMg	09.11.1988

nym	name
98BAC	Bob

nym	car
2GCun	Mini Cooper

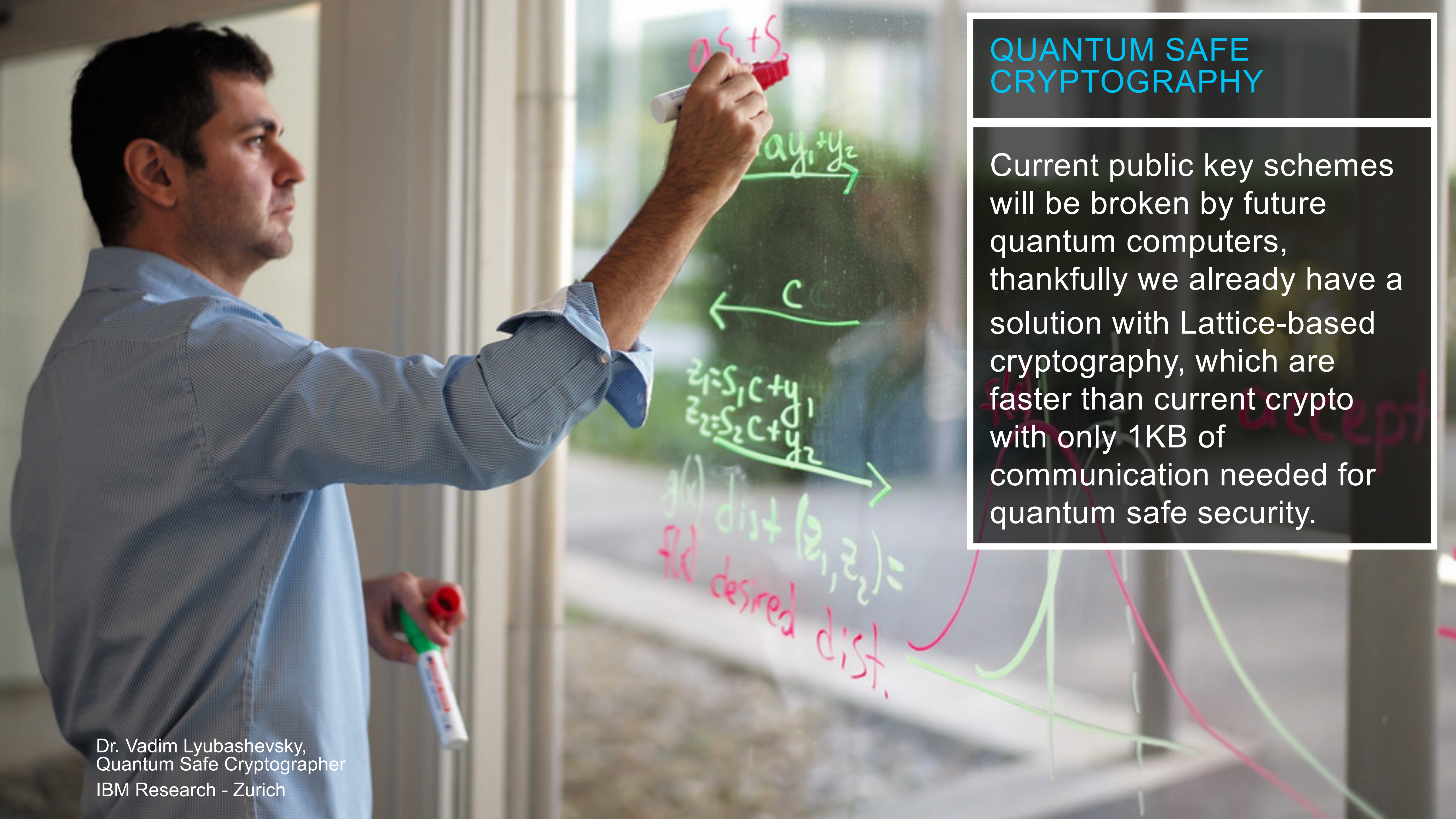
nym	gender
Yj6gY	male

nym	gender
6Zvrd	female

nym	car
6Zvrd	Porsche 911

nym	gender	car
6Zvrd	female	Porsche 911
BF3Mn	male	Mini Cooper

Quantum-safe Cryptography



QUANTUM SAFE CRYPTOGRAPHY

Current public key schemes will be broken by future quantum computers, thankfully we already have a solution with Lattice-based cryptography, which are faster than current crypto with only 1KB of communication needed for quantum safe security.

Dr. Vadim Lyubashevsky,
Quantum Safe Cryptographer
IBM Research - Zurich

IBM Q

Two new processors
IBM Q has successfully built and tested two of its most powerful universal quantum computing processors to date: 16 qubits for public use and a 17 qubit prototype commercial processor.

Quantum Computer Approaches

Quantum Annealer

Least powerful and most restrictive
Simplest to build

Computation Power
Same as traditional computers

Application
Optimization Problems

Analogue Quantum

Simulates complex quantum interactions that conventual computers cannot

Computational Power
High

Application
Quantum Chemistry
Material Science
Optimization Problems
Sampling
Quantum Dynamics

Universal Quantum

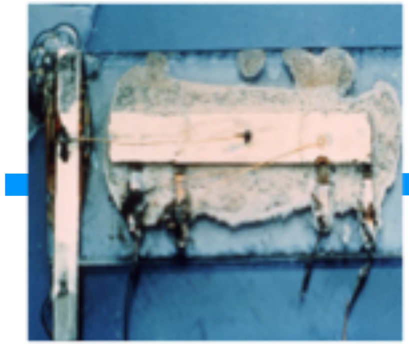
Most powerful, most general and the hardest to build powerful and least restrictive

Computation Power
High

Application
Secure Computing
Machine Learning
Cryptography
Quantum Chemistry
Material Science
Optimization Problems
Sampling
Quantum Dynamics
Searching

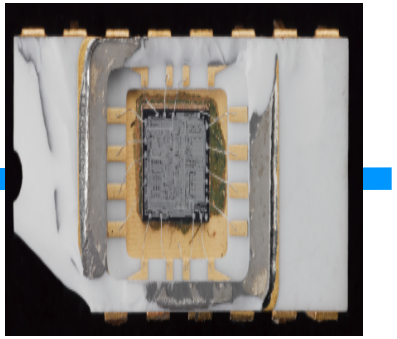
When will the threat to cryptography become real?

1958



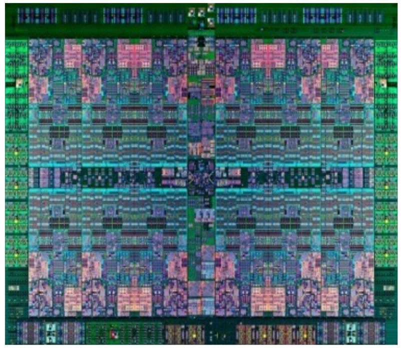
First integrated circuit
Size ~1cm^2
2 Transistors

1971



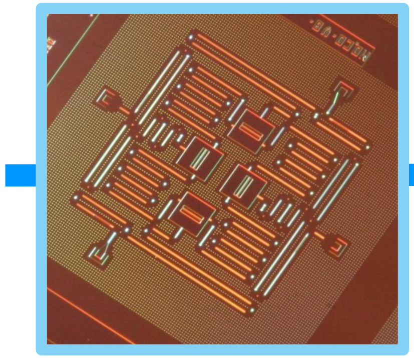
Moore's Law is Born
Intel 4004
2,300 transistors

2014



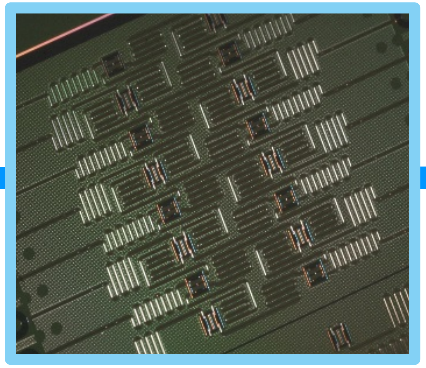
IBM P8 Processor ~ 650 mm^2
22 nm feature size, 16 cores
> 4.2 Billion Transistors

2016



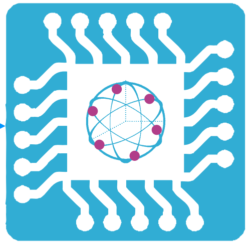
Chip with 4 superconducting qubits and resonators

2017



Chip with 16 superconducting qubits and resonators

Large
Quantum
Computer



?

But we have been in the same situation before

The Impact for cryptographic schemes

Algorithm	Key Length	Security level on conventional computer	Security level on quantum computer
RSA-1024	1024 bits	80 bits	0
RSA 12048	2048 bits	120 bits	0
ECC 256	256 bits	128 bits	0
ECC 384	384 bits	192 bits	0
AES 128	128 bits	128 bits	64 bits
AES 256	256 bits	256 bits	128 bits

Quantum Algorithms

Shor's algorithm

Exponential improvement in brute-force attacks on asymmetric encryption schemes like RSA, ECC, Elgamel.

Grover's algorithm

Quadratic improvement in brute-force attacks on symmetric encryption schemes like AES.

In asymmetric public key algorithms the security evaporates
In symmetric key algorithms the effective security is halved

Review of quantum resistant algorithms

Code-based systems: difficulty of recovering state from error-correction residuals [McEliece – 1978]

Multivariate equations (Rainbow Signatures) Signature Only

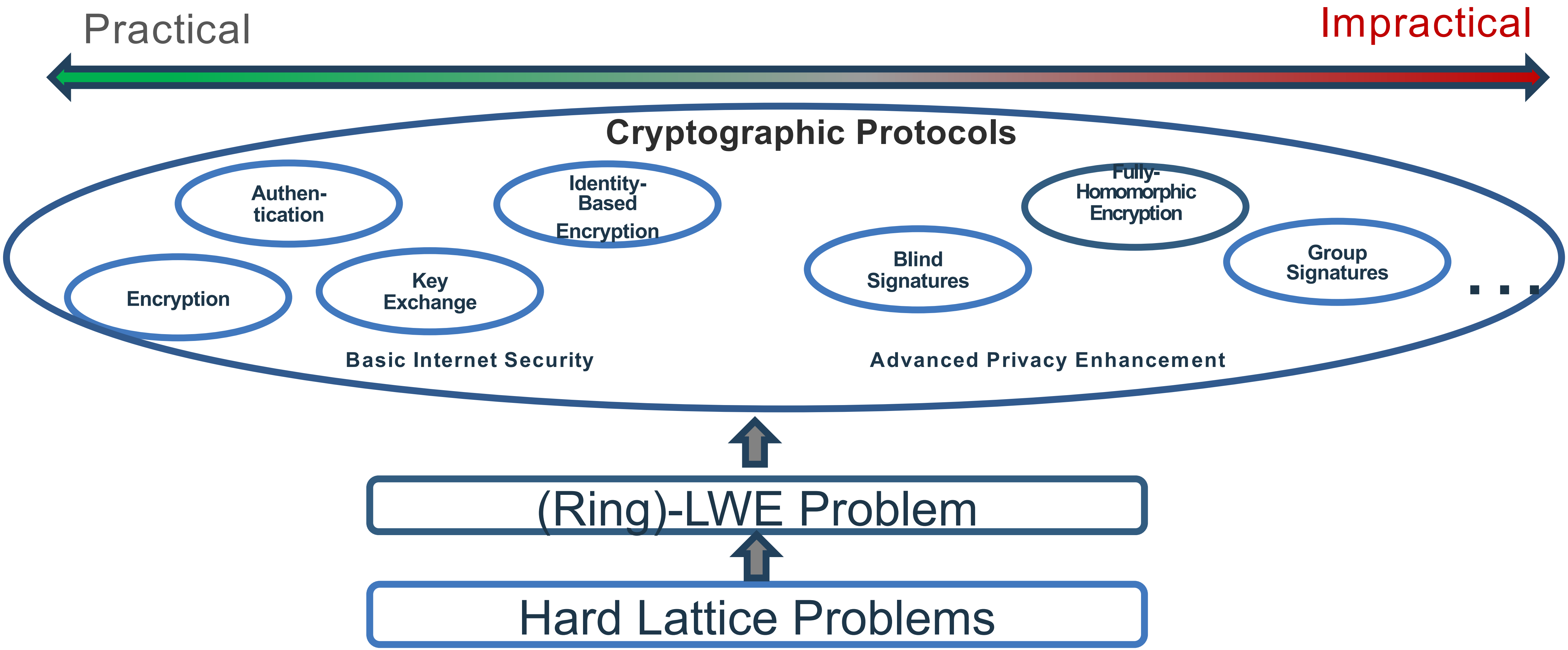
Hash-tree based: secret is knowledge of original input, plus hash function

Supersingular Isogeny DH (SIDH): difficulty of reconstructing ``large enough'' permutations from indirect samples

Lattice-based trapdoors: difficulty of finding coordinate base only from projected points [LWE, Ring-LWE, NTRU]

These are all *algorithm categories, not specific algorithms*

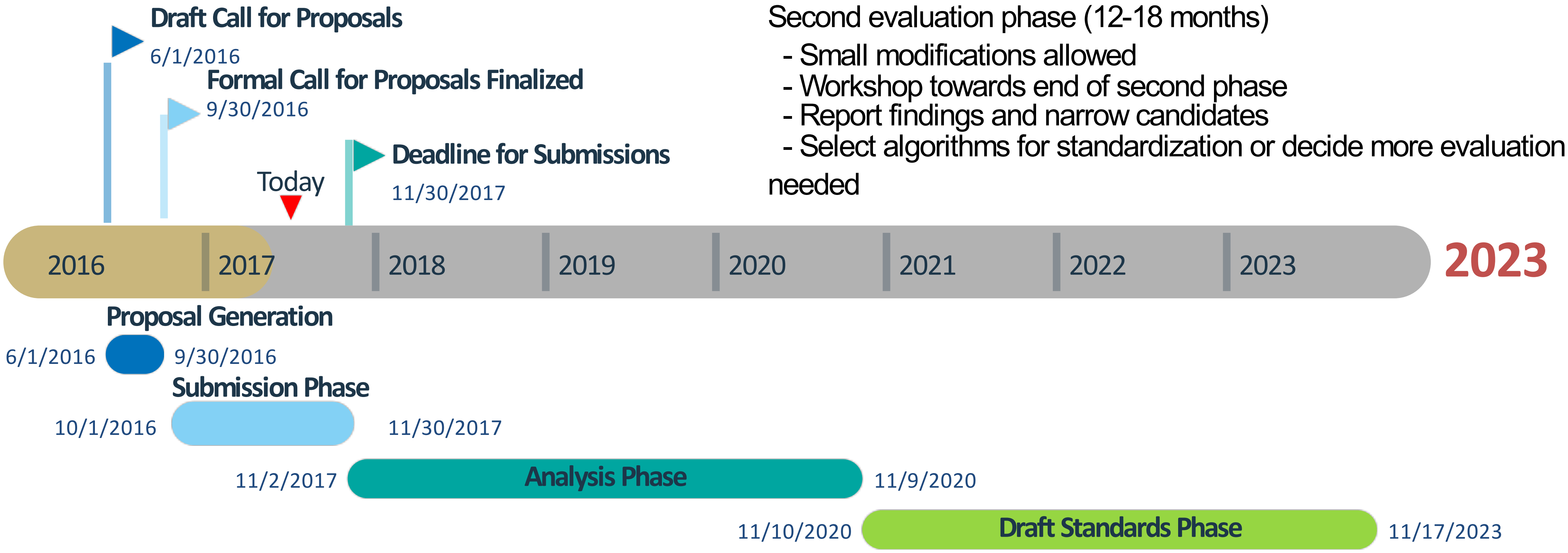
Lattice-based Schemes



NIST PQC Standardization : Timeline and Phases

Second evaluation phase (12-18 months)

- Small modifications allowed
- Workshop towards end of second phase
- Report findings and narrow candidates
- Select algorithms for standardization or decide more evaluation needed



IBM

ICC
International
Cybersecurity
Congress

Thank you!

mdu@zurich.ibm.com

www.research.ibm.com