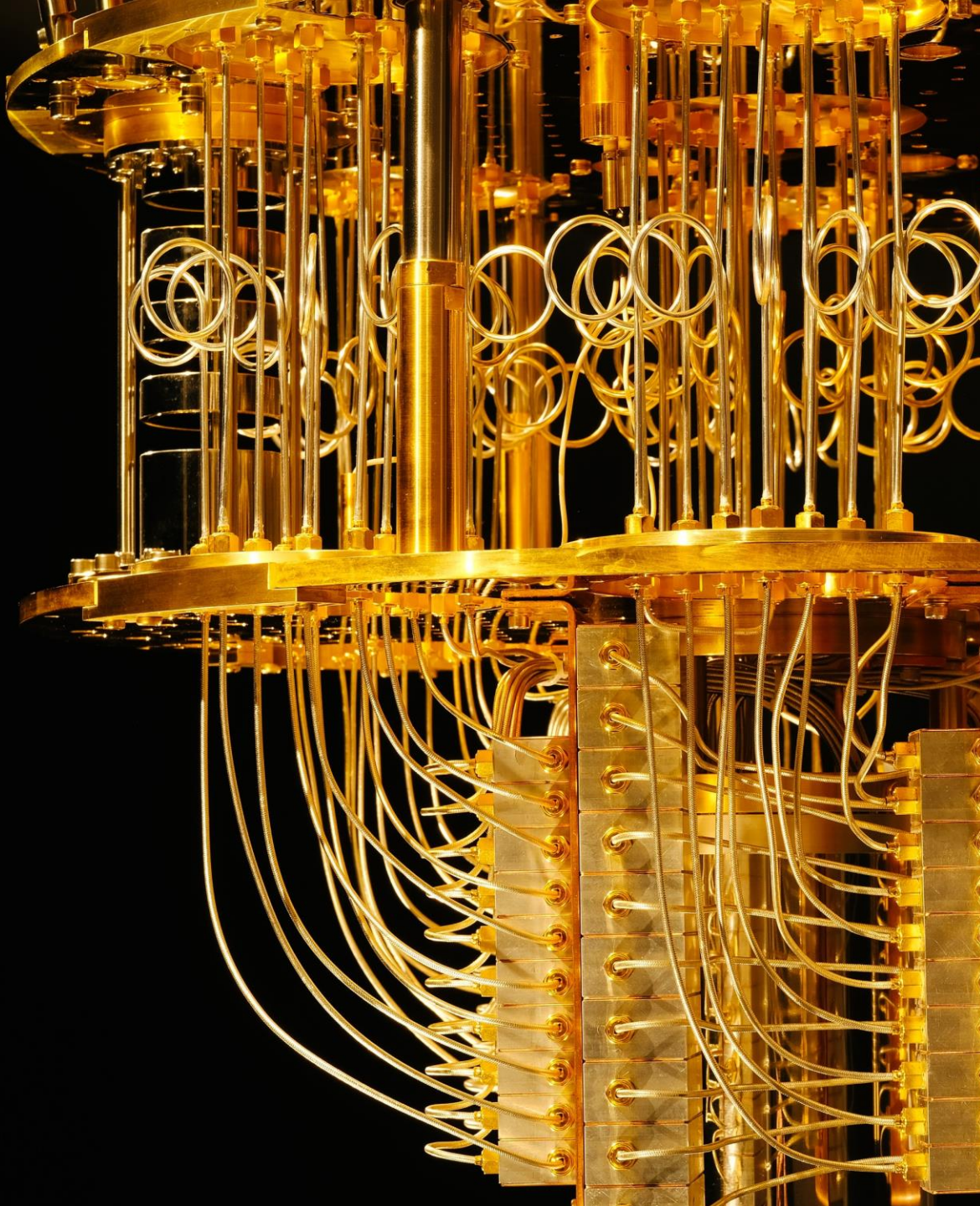
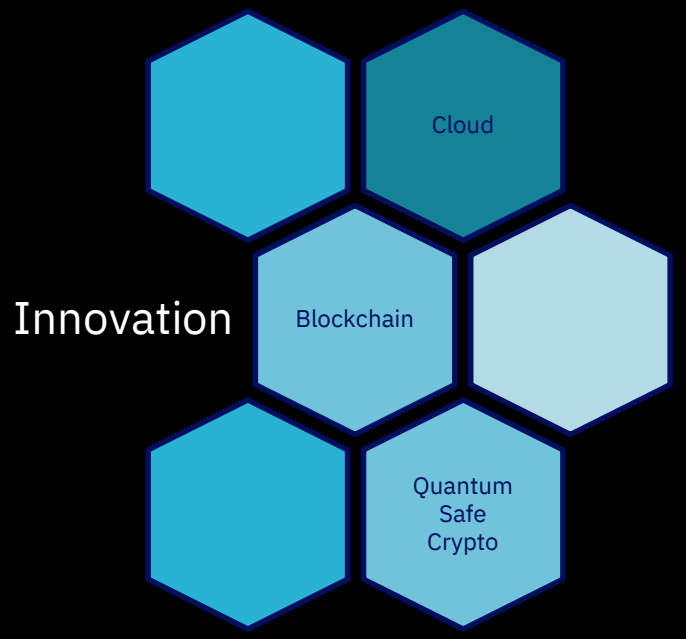
Security of the future:
Addressing today the challenges of tomorrow

Cecilia Boschini
Predoctoral Researcher
IBM Research





Can we improve the security infrastructure *while* adopting new technologies?

What vulnerability took more than 800 days to identify, cost more than $500 million to fix, and years later, nearly 200,000 websites are still at risk?

(CVE-2014-0160) OpenSSL Heartbleed Vulnerability (April 2014)

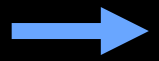
Jan 2017: (https://thehackernews.com/2017/01/heartbleed-openssl-vulnerability.html).

This is an example of ‘lack of Cybersecurity agility’

In this specific case ‘lack of cryptographic agility’

Problems in cryptography today

An Analysis of OpenSSL common vulnerabilities and exposures (CVEs) between 2002 to 2016. Implementation flaws accounted for far and away the greatest number



- Algorithm flaws, including block ciphers and cryptographic primitives;
- Protocol problems, meaning fixes that require changes to the protocol;
- Side channel attacks, where secret keys leak out;
- Padding attacks, which may overlap protocols and implementations; and
- Implementation flaws, where there is a bug in the code that is often not revealed until it is too late to rewrite it.

Problems in cryptography today

- Algorithm flaws, including block ciphers and cryptographic primitives;
- Protocol problems, meaning fixes that require changes to the protocol;
- Side channel attacks, where secret keys leak out;
- Padding attacks, which may overlap protocols and implementations; and
- Implementation flaws, where there is a bug in the code that is often not revealed until it is too late to rewrite it.

The threat from Quantum Computers

- A Change in Mathematical Hardness Assumptions

NSA Says It “Must Act Now” Against the Quantum Computing Threat

The National Security Agency is worried that quantum computers will neutralize our best encryption – but doesn’t yet know what to do about that problem.

February 3, 2016

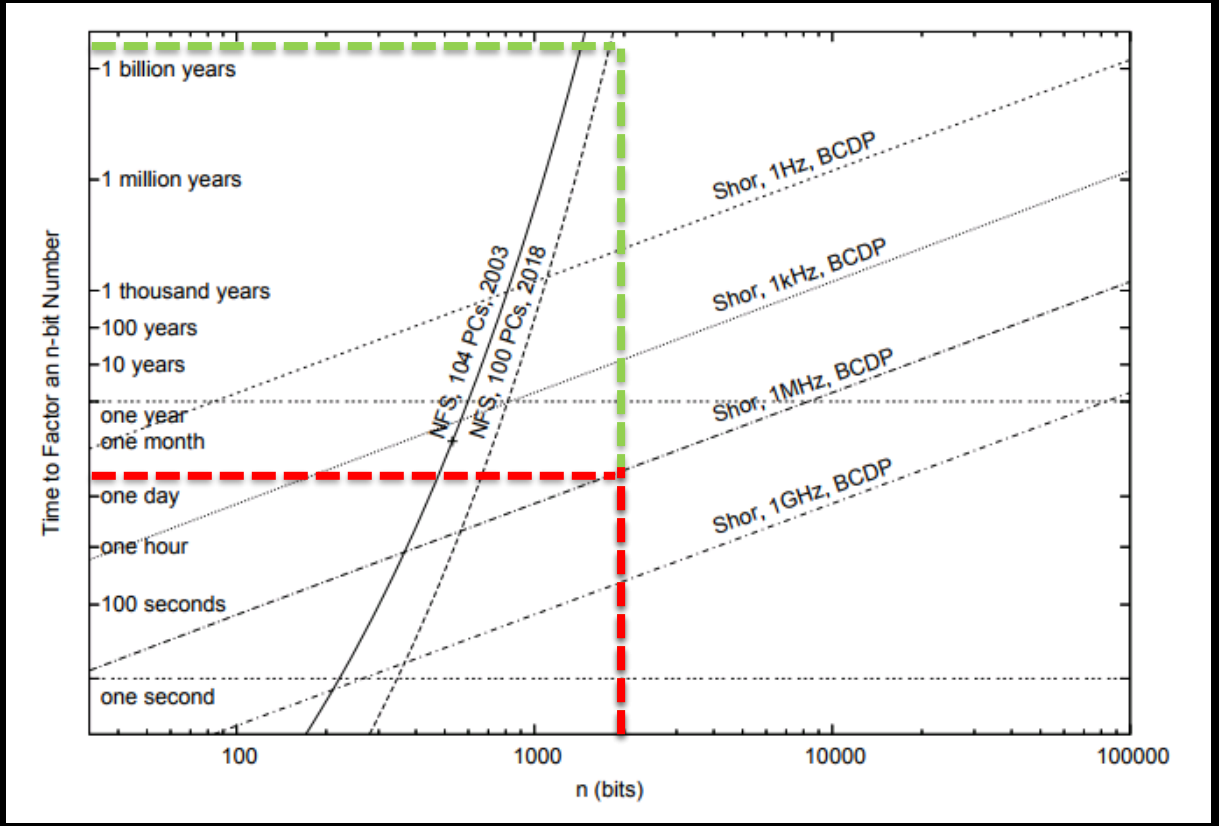
Current popular public key algorithms rely on one of three hard mathematical problems:

Public key cryptography relies on the fact that there is a huge difference in the difficulty of a forward mathematical operation compared to the reverse operation

	RSA	DSA	ECC
Forward Operation	Integer Multiplication	Discrete exponentiation	Point multiplication
Inverse Operation	**Integer Factorisation Problem**	**Discrete Logarithm Problem**	**Elliptic curve discrete logarithm problem**

Quantum computers are especially good at factoring integers (Shor's Algorithm)

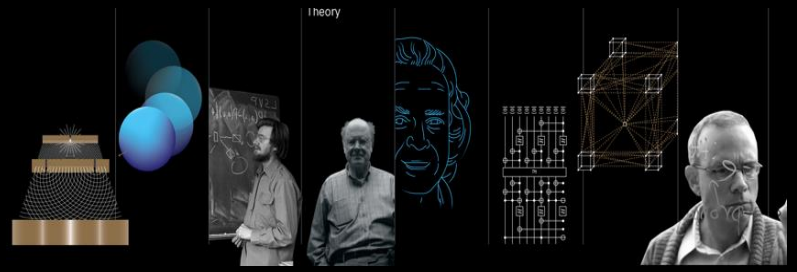
From a billion years to hours – exponantial speedup



Quantum computers can factor large numbers much faster than even the best classical computers. Source data from R. Van Meter, K. M. Itoh, and T. D. Ladd, "Architecture-dependent execution of Shor's algorithm," in https://arxiv.org/pdf/quant-ph/0507023.pdf

The quantum journey

Quantum foundations

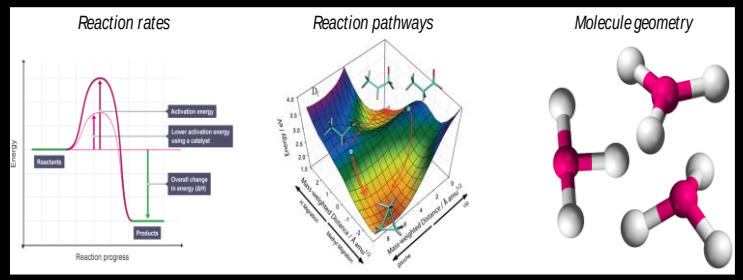


Quantum computing as the exclusive domain of scientists and theoreticians

Quantum-ready

Exploration of use cases and potential for quantum advantage

Quantum advantage



Extracting value out of quantum computing for business and science

Today

Why is the impact so high?

+Chinese Algorithms
+Russian Algorithms
+Korean Algorithms

Name	function	pre-quantum security level	post-quantum security level
Symmetric cryptography			
AES-128 [1]	block cipher	128	64 (Grover)
AES-256 [1]	block cipher	256	
Salsa20 [2]	stream cipher	256	
GMAC [3]	MAC	128	
Poly1305 [4]	MAC	128	
SHA-256 [5]	hash function	256	128 (Grover)
SHA-3 [6]	hash function	256	128 (Grover)
Public-key cryptography			
RSA-3072 [7]	encryption	128	broken (Shor)
RSA-3072 [7]	signature	128	
DH-3072 [8]	key exchange	128	
DSA-3072 [9, 10]	signature	128	
256-bit ECDH [11, 12, 13]	key exchange	128	broken (Shor)
256-bit ECDSA [14, 15]	signature	128	broken (Shor)

Security Halved

Security Broken

Cryptographic systems and their security levels against the best pre-quantum and post-quantum attacks known

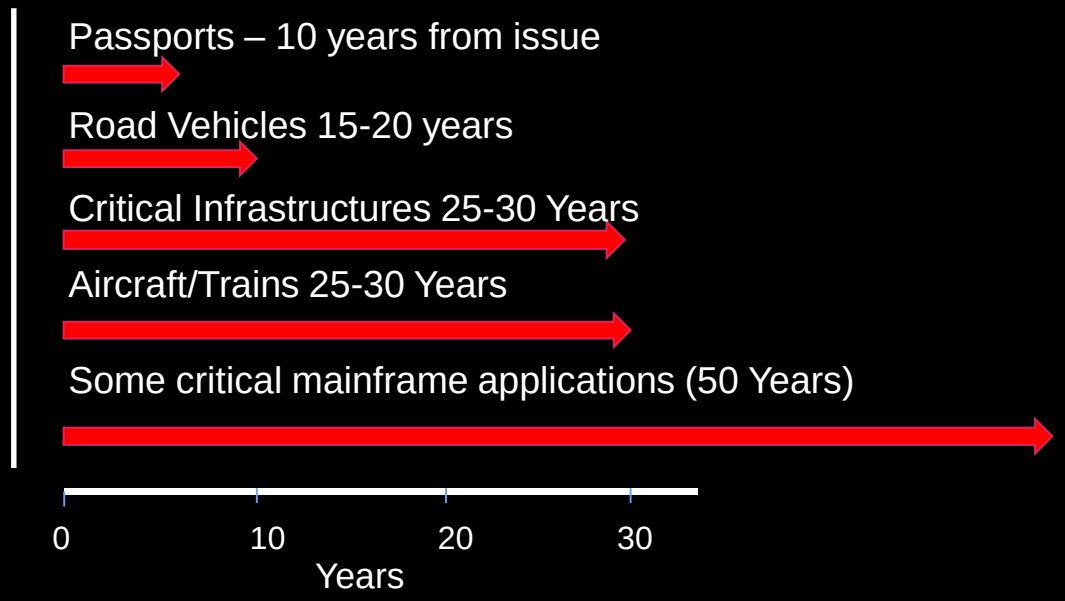
Why is this a problem today ?

Security time value of data

Certain data stored today must remain confidential for decades

Infrastructure Update Cycles

Many applications and infrastructures have long update cycles



Key Takeaways

Sensitive Data and Systems need to migrate to quantum safe cryptography

The window is closing for introducing new cryptographic schemes that are not quantum resistant

What does quantum safe cryptography mean?

- Cryptography based on hard mathematical problems thought to be difficult for both classical and quantum computers
- Cryptography that runs on todays classical computers that can be used to replace our existing cryptographic schemes

quantum-safe = post-quantum

A number of candidate hard problems

Solving multivariate quadratic equations
- Multivariate Crypto

Bounded-distance decoding (BDD)
- Code-based crypto

Learning with Errors and Short Integer Solution problem (LWE, SIS)
- Lattice-based crypto

Breaking security of symmetric primitives (SHAx-, AES-, Keccak-,... problem)
- Hash-based signatures / symmetric crypto

Inverting isogenies between elliptic curves
- Supersingular Isogeny Elliptic Curve Cryptography

PQC Standards

NIST

The NIST Post-Quantum Cryptography (PQC) Standardization Project, and focuses on asymmetric algorithms for: data encryption, digital signatures, and key encapsulation. 80 Submissions being evaluated.

Standard drafting planned to start in 2020

Multiple schemes likely

IETF and IRTF

A second Internet-Draft in the domain of hash-based signatures- Leigthon-Micali signature scheme (LMS).

Quantum-safe hybrid TLS cipher-suite. A current Internet-Draft describes a quantum-safe hybrid cipher suite for the Transport Layer Security (TLS) protocol version 1.3

Internet-Draft describes an extension of the Internet key exchange protocol IKEv2

IEEE

Std 1363.1-2008 provides specifications of several public key cryptographic techniques based on hard problems over lattices, including primitives for key establishment, public-key encryption, authentication and digital signatures, as well as cryptographic schemes based on those primitives

ISO/IEC JTC 1 SC27

Working Group for Quantum-Safe Cryptography (WG QSC) was founded 2015. Includes Identification of quantum-safe cryptographic primitives, and the development of a framework for quantum safe algorithms.

ANSI

X9 Quantum Computing Risk Study Group creating a white paper

NIST PQC Submissions: Update

Candidate	Type
BIKE	Code
Classic McEliece	Code
HQC	Code
Ouroboros-R	Code
RLCE-KEM	Code
QC-MDPC KEM	Code
LEDAkem	Code
LEDApkc	Code
DAGS	Code
McNie	Code
LOCKER	Code
LAKE	Code
Edon-K	Code
RQC	Code
NTS-KEM	Code
BIG QUAKE	Code
Ramstake	Lattice
Odd Manhattan	Lattice
NTRU Prime	Lattice
Three Bears	Lattice
CRYSTALS- KYBER	**Lattice**
LOTUS	Lattice
NTRUEncrypt	Lattice
SABER	Lattice
Compact LWE	Lattice

Key Exchange

Candidate	Type
Round5	Lattice

Candidate	Type
LEDAcrypt	Code

Candidate	Type
ROLLO	Code

Candidate	Type
NTRU	Lattice

IBM Supported Submissions

Candidate	Type
Ding Key Exchange	Lattice
KINDI	Lattice
Lizard	Lattice
Round 2	Lattice
LIMA	Lattice
EMBLEM and R.EMBLEM	Lattice
NewHope	Lattice
Titanium	Lattice
HILA5	Lattice
KCL (OKCN/AKCN/CNKE)	Lattice
LAC	Lattice
FrodoKEM	Lattice
Giophantus	Lattice
NTRU-HRSS-KEM	Lattice
Mersenne-756839	Lattice
Lepton	LPN (Lattice/Code)
DME	Multivariate Quadratic
SRTPI	Multivariate Quadratic
RVB	Chebyshev polynomials
HK17	Hypercomplex numbers
Guess Again	Random Walk
Post-Quantum RSA Encryption	RSA
SIKE	SIDH

NIST PQC Submissions: Update

IBM Supported Submissions

Signature

Candidate	Type
DualModeMS	Multivariate Quadratic
LUOV	Multivariate Quadratic
GeMSS	Multivariate Quadratic
MQDSS	Multivariate Quadratic
HiMQ-3	Multivariate Quadratic
Gui	Multivariate Quadratic
Rainbow	Multivariate Quadratic
SRTPI	Multivariate Quadratic
CFPKM	Multivariate
WalnutDSA	Braids
Post-Quantum RSA Signature	RSA

Candidate	Type
RaCoSS	Code
RankSign	Code
pqsigRM	Code
Picnic	Other
Gravity-SPHINCS	Hash
SPHINCS+	Hash
pqNTRUsign	Lattice
qTESLA	Lattice
CRYSTALS- DILITHIUM	**Lattice**
DRS	Lattice
FALCON	Lattice

Four Phases to Quantum Safe Migration

1. What does it mean for me ? — Security Risk Assessment
2. What do I need to do ? — Security Strategy
3. Preparing and Planning — Quantum Safe Enablement
4. Execution — Quantum Safe Migration

Cryptographic Agility

By making our system crypto agile we can improve our Cybersecurity stance at the same time as making it simple to move to quantum safe algorithms.

NIST, Report on Post-Quantum Cryptography (2016)

Cryptographic Agility

- It should be simple and transparent for applications to change underlying cryptography
- Applications should only require a clean interface and be driven by policy
- Policy can be selected based on sensitivity of the data being protected
- Migrating cryptography should be a simple as installing a provider and changing the policy

Algorithm Agility

Implementation Agility

Retirement Agility

Protocol Agility

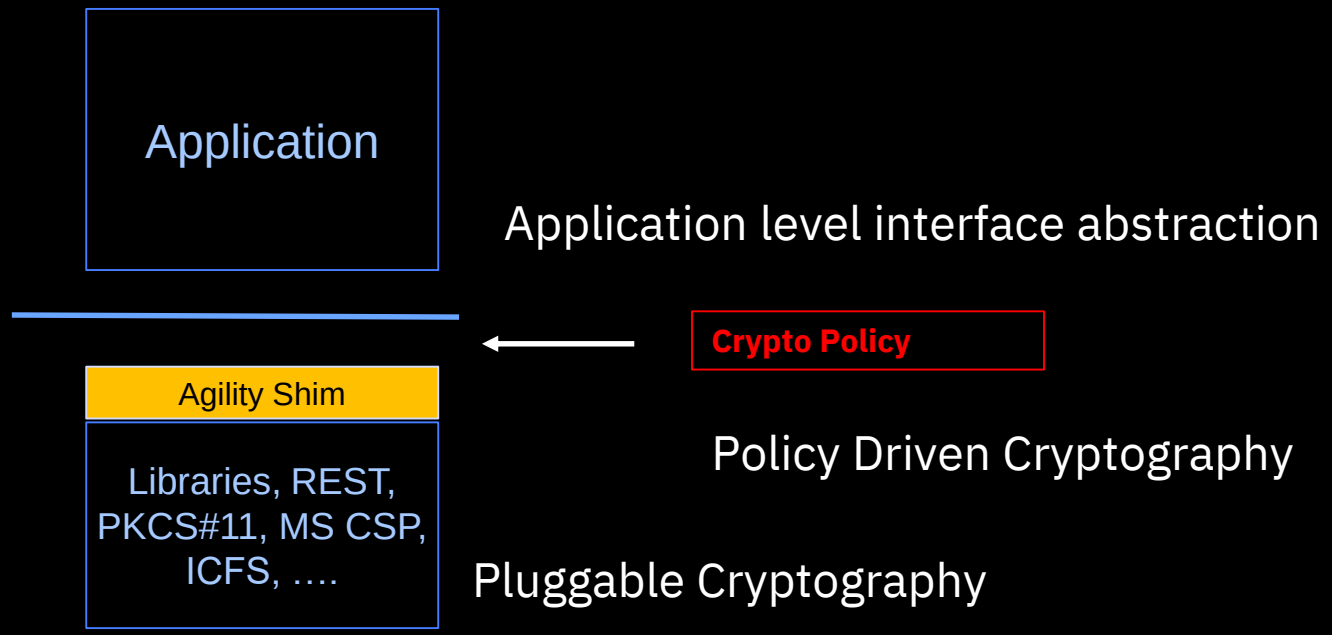
Platform Agility

Cryptographic Agility – Overview

Todays non agile approach

Tightly coupled, system level crypto providers, application internal configuration

Future Agility



Pluggable application level interface, crypto providers abstracted by an agility shim, external policy driven

Key Takeaways

Cryptographic Agility is something that we need to today

Built into new products

Added to legacy systems

Built into legacy system migration strategies

Built into cloud migration strategies

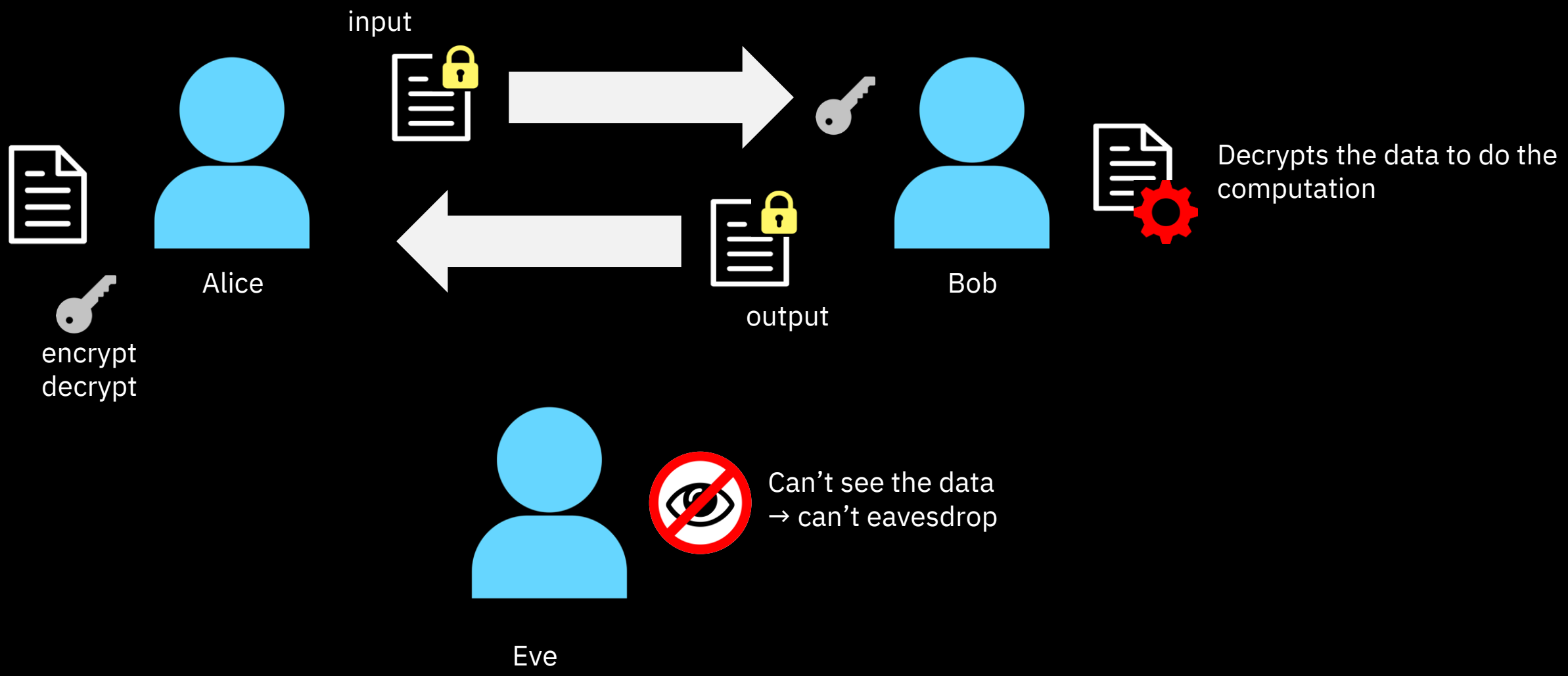
Peeking into the Future

PROBLEM:

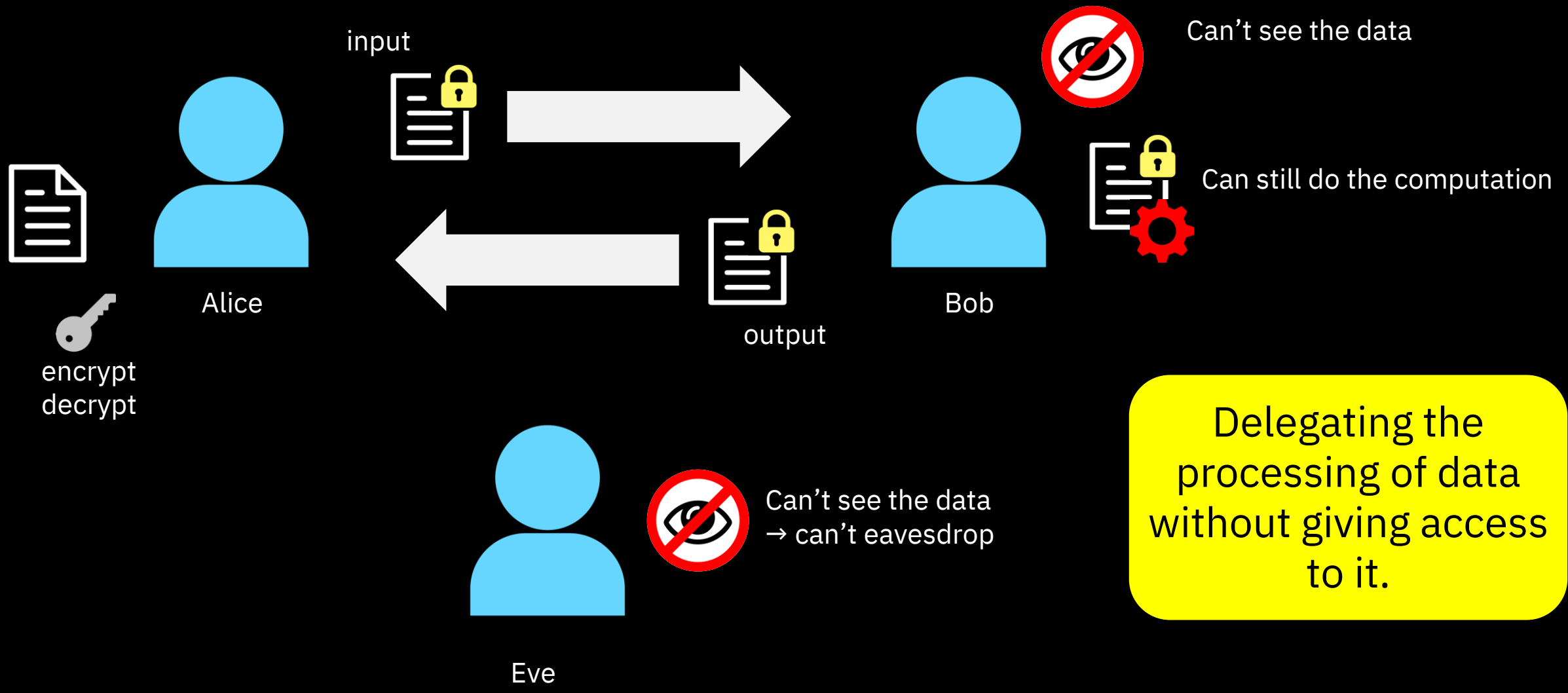
- I have sensitive data
- I cannot share this with everyone
- But value comes from sharing

Can we use cutting-edge cryptographic algorithms to reduce liability of statistical analysis of sensitive data?

Computing on data



Fully Homomorphic Encryption

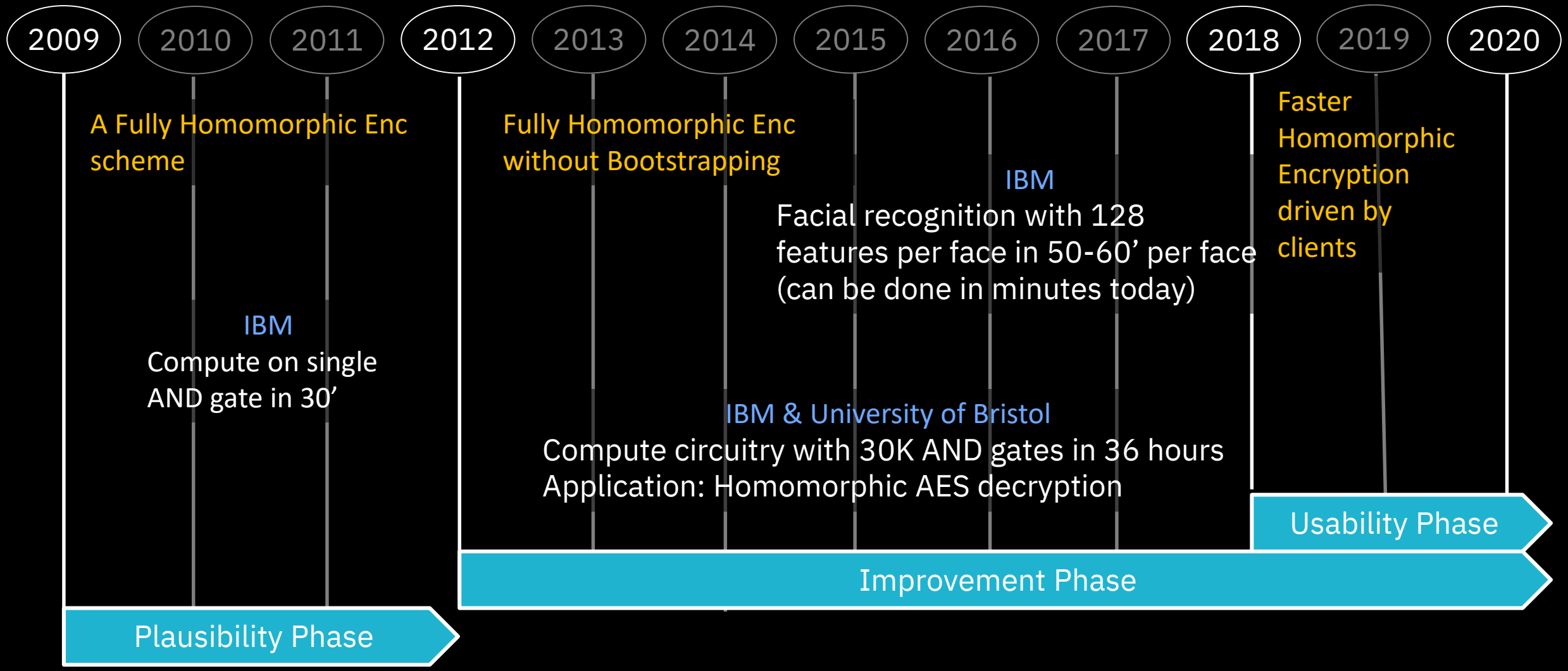


Delegating the processing of data without giving access to it.

Analytics through Safe Aggregation

Reduces liability/risk of statistical analysis of sensitive data

Timeline



Conclusion: Addressing Today the Challenges of Tomorrow

- Quantum-safe cryptography will safeguard the confidentiality of data.
- Cryptoagility will allow fast updates of the security infrastructure.
- FHE will help in reducing the liability of handling sensitive data.