HELLENIC DATA
PROTECTION AUTHORITY

PQC and PETs state of play

Konstantinos Limniotis

ICT Specialist, Head of Research and Studies, HDPA

WEBINAR

Engineering
Data Protection
in the wake of PQC

8th December

Overview

- Intro on basic notions of “classical” cryptography
    - Symmetric vs. Asymmetric and their interplay
    - Privacy Enhancing Cryptography
- Why post-quantum cryptography?
- Current post-quantum cryptographic standards
- Privacy Enhancing Cryptography in the post-quantum era
    - Challenges – Current state of play
- Conclusions – Future Steps

What is cryptography about?

- How can Alice send a message to Bob over the internet so that **only Bob** can read it? (even if they have never met in the past!)
  - And allowing Bob being sure that the message is genuine, sent indeed by Alice?
- How can Alice digitally **sign** a document so that everyone is sure that she is the one who signed and no one can forge her signature?
- How can I **protect files** stored in my device or the cloud?
- How can we **check that two files are identical**, without looking at their content?
- How can you **share a secret** between five people so that you do not get any information about the secret if you just have four of the shares?
- Can you **prove** you know a secret without revealing any information whatsoever about the nature or content of this secret?
- How can you perform **computations on data** without having direct access to the data per se?
- And others….

What is cryptography about?

Security - related

- How can Alice send a message to Bob over the internet so that **only Bob** can read it? (even if they have never met in the past!)
  - And allowing Bob being sure that the message is genuine, sent indeed by Alice?
- How can Alice digitally **sign** a document so that everyone is sure that she is the one who signed and no one can forge her signature?
- How can I **protect files** stored in my device or the cloud?
- How can we **check that two files are identical**, without looking at their content?
- How can you **share a secret** between five people so that you do not get any information about the secret if you just have four of the shares?
- Can you **prove** you know a secret without revealing any information whatsoever about the nature or content of this secret?
- How can you perform **computations on data** without having direct access to the data per se?
- And others….

What is cryptography about?

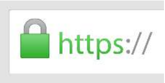
Security - related

- How can Alice send a message to Bob over the internet so that **only Bob** can read it? (even if they have never met in the past!)
  - And allowing Bob being sure that the message is genuine, sent indeed by Alice?
- How can Alice digitally **sign** a document so that everyone is sure that she is the one who signed and no one can forge her signature?
- How can I **protect files** stored in my device or the cloud?
- How can we **check that two files are identical**, without looking at their content?
- How can you **share a secret** between five people so that you do not get any information about the secret if you just have four of the shares?
- Can you **prove** you know a secret without revealing any information whatsoever about the nature or content of this secret?
- How can you perform **computations on data** without having direct access to the data per se?
- And others….

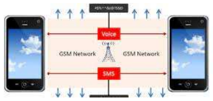
Privacy - related

Cryptography is present in…

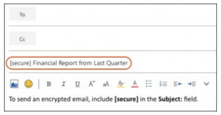
- Web browsing (π.χ. https) – digital signatures
- Teleconferences – Messaging apps etc. (VoIP, messanging apps κτλ.)
- Mobile communications
- Wireless networks (802.11x, Bluetooth, …)
- Electronic payments (e-commerce)
- E-mail
- Enterprise security – (Hard) disk security
- Electronic voting
- Virtual Private Networks (VPN)
- IoT communications
- Digital wallet – digital identities
- eHealth – mhealth
- Distributed Ledger Technology (Bitcoin, Ethereum…)
- … and many others


https://

KONSTANTINOS LIMNIOTIS
27/03/2024 08:59



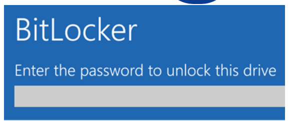
Secure credit card payment


To

Cc

[secure] Financial Report from Last Quarter

To send an encrypted email, include **[secure]** in the **Subject:** field.


BitLocker

Enter the password to unlock this drive

Check Point Endpoint Security

Endpoint Security

Check Point

Cryptography in data protection legislation

- Art. 32 GDPR: *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate the encryption of personal data (….)*
- Art. 34 (GDPR): In case of personal data breach, there is no obligation for the controller to communicate the breach to the affected data subjects, in case that *the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;*
- Cryptographic techniques could also provide the technical means to facilitate implementation of data protection principles, such as purpose limitation and data minimization
  - E.g. through cryptography-based pseudonymisation or advanced cryptographic techniques (see ENISA's reports)

Cryptography in data protection legislation

Security - related

- Art. 32 GDPR: *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate the encryption of personal data (….)*
- Art. 34 (GDPR): In case of personal data breach, there is no obligation for the controller to communicate the breach to the affected data subjects, in case that *the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;*
- Cryptographic techniques could also provide the technical means to facilitate implementation of data protection principles, such as purpose limitation and data minimization
    - E.g. through cryptography-based pseudonymisation or advanced cryptographic techniques (see ENISA's reports)

Cryptography in data protection legislation

Security - related

- Art. 32 GDPR: *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate the encryption of personal data (….)*
- Art. 34 (GDPR): In case of personal data breach, there is no obligation for the controller to communicate the breach to the affected data subjects, in case that *the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;*

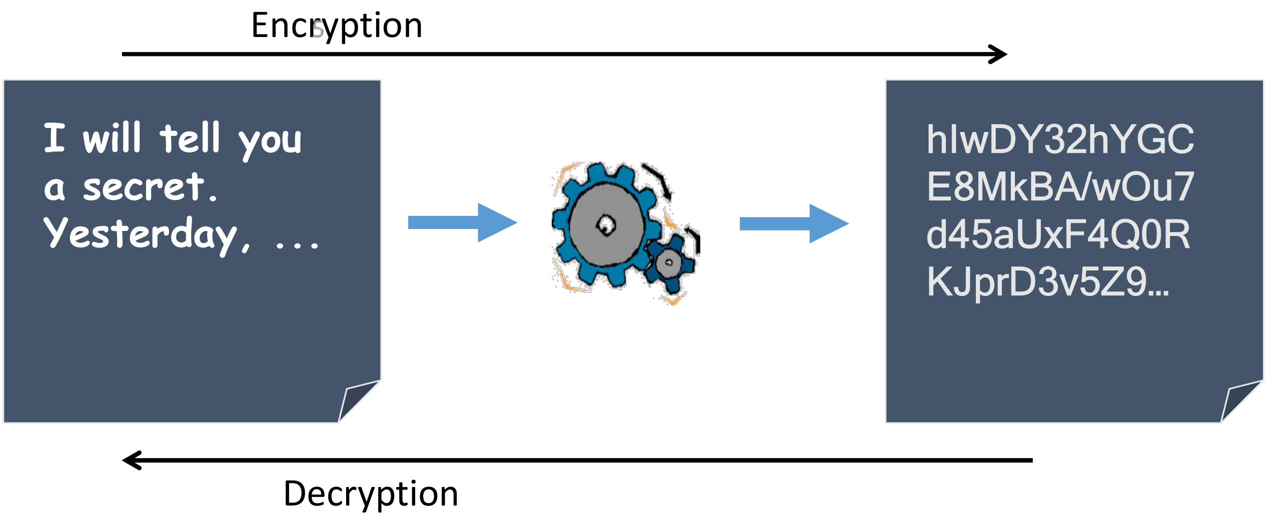
- Cryptographic techniques could also provide the technical means to facilitate implementation of data protection principles, such as purpose limitation and data minimization
  - E.g. through cryptography-based pseudonymisation or advanced cryptographic techniques (see ENISA's reports on data protection engineering)

Privacy - related

HELLENIC DATA PROTECTION AUTHORITY

The “traditional” definition of cryptography

- Focusing on confidentiality of data (i.e., a security-related aspect)
  - *This is not a robust definition today – cryptography goes far beyond encryption*



Encryption

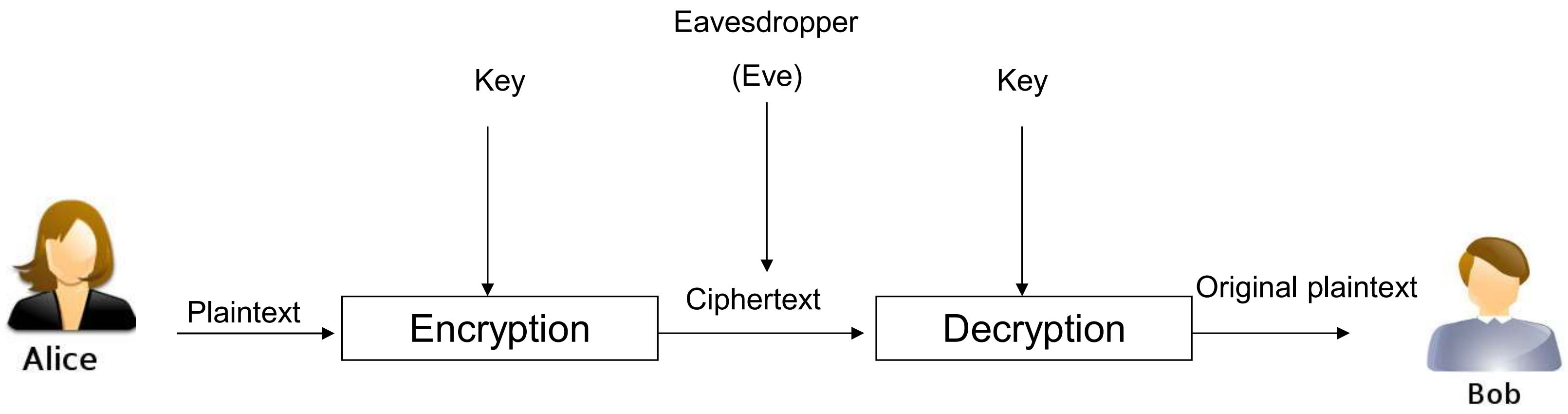
I will tell you a secret. Yesterday, ...

hIwDY32hYGC
E8MkBA/wOu7
d45aUxF4Q0R
KJprD3v5Z9…

Decryption

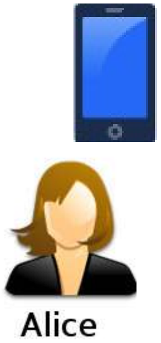
- *Independently from whether we focus on the “traditional” cryptography or on advanced cryptographic methods, a crucial factor is the* ***cryptographic key.***

Symmetric-key cryptography

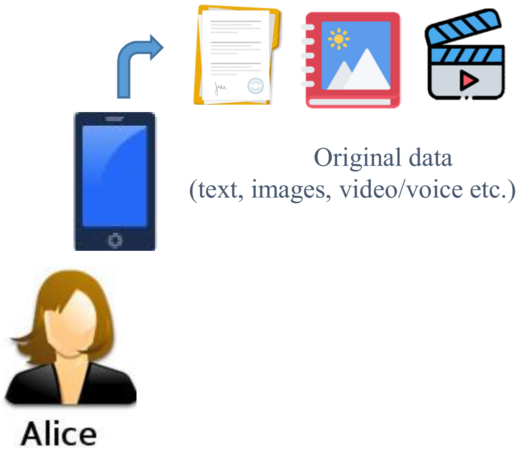


- The security rests with the secrecy of the key
  - The encryption and decryption algorithms can be publically known
  - That's why we have well-known cryptographic standards (e.g., the Advanced Encryption Standard (AES))

Encryption in practice



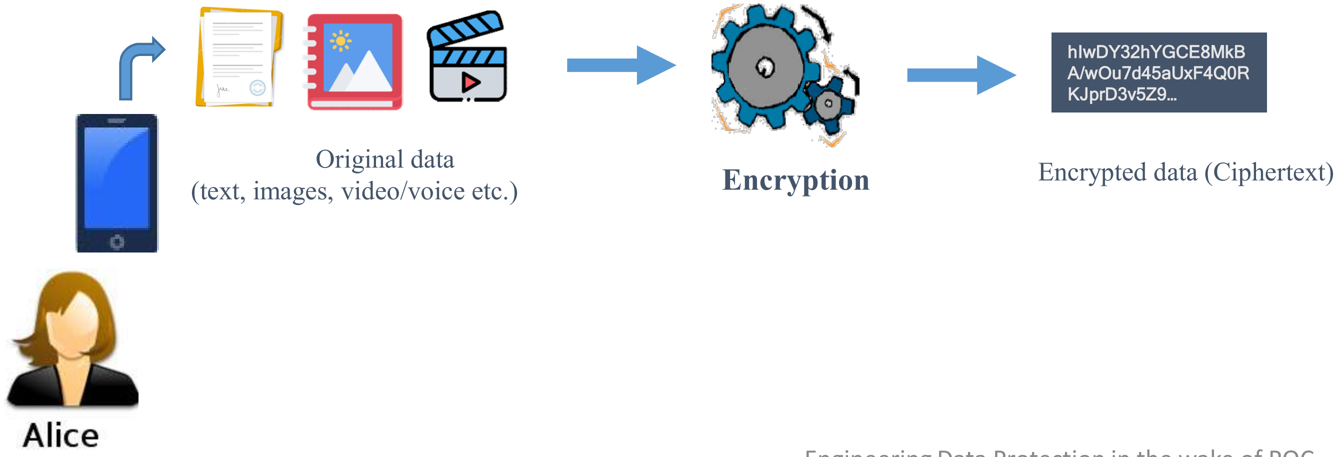
Encryption in practice



Original data
(text, images, video/voice etc.)

Alice

Encryption in practice



Original data
(text, images, video/voice etc.)

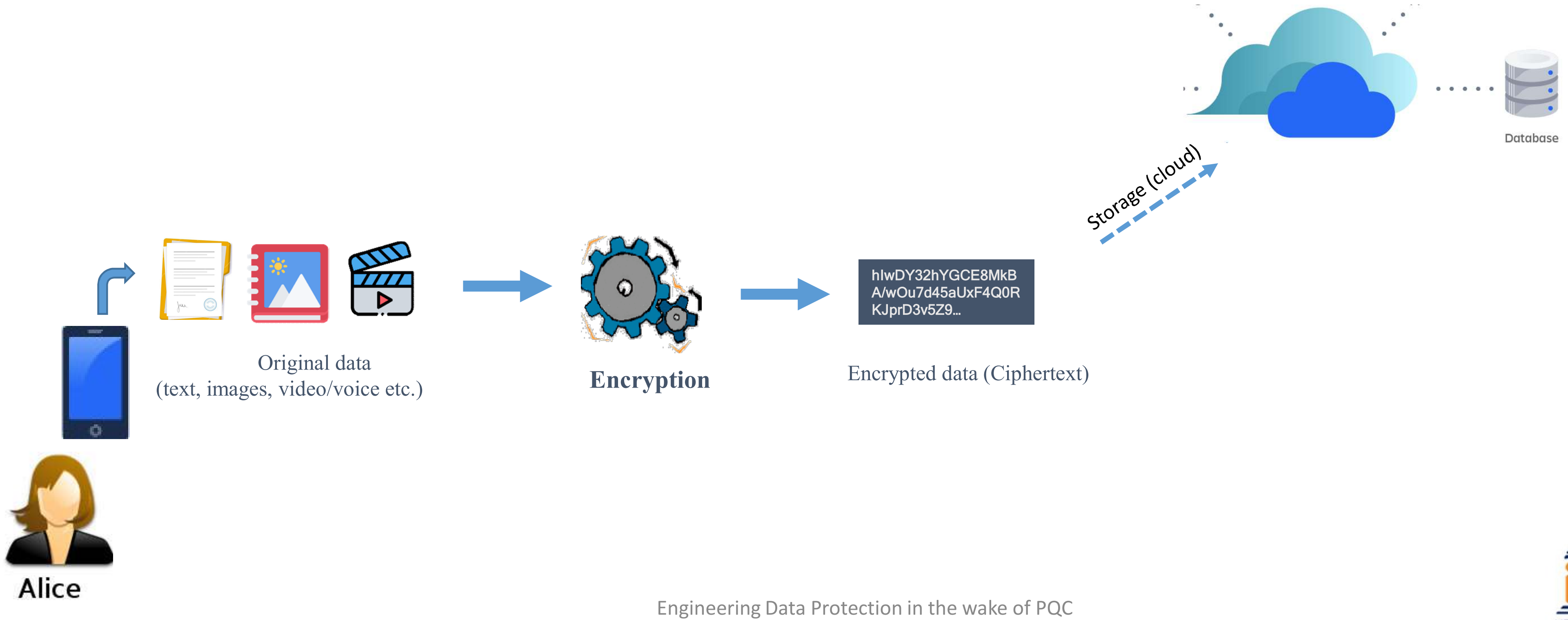
Encryption

hlwDY32hYGCE8MkB
A/wOu7d45aUxF4Q0R
KJprD3v5Z9...

Encrypted data (Ciphertext)

Alice

Encryption in practice



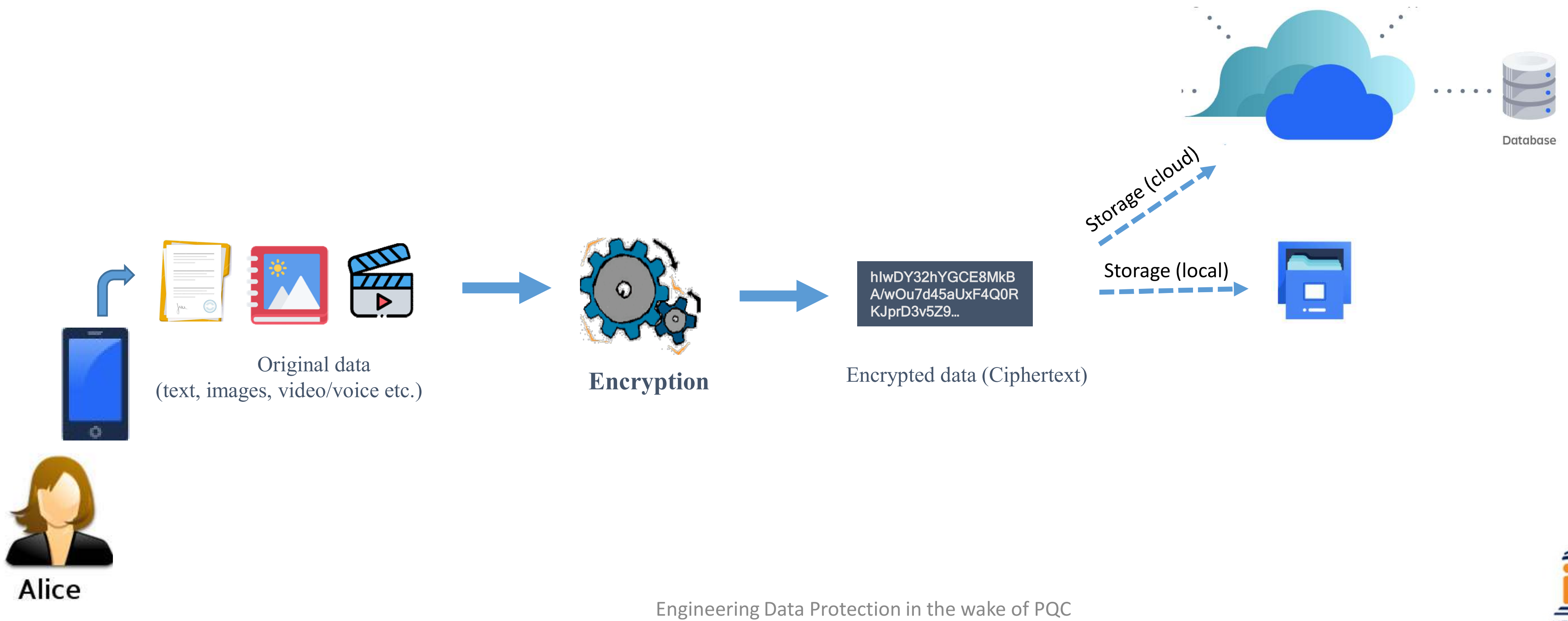
Original data
(text, images, video/voice etc.)

Encryption

hIwDY32hYGCE8MkB
A/wOu7d45aUxF4Q0R
KJprD3v5Z9...

Encrypted data (Ciphertext)

Encryption in practice



Original data
(text, images, video/voice etc.)

Encryption

hIwDY32hYGCE8MkB
A/wOu7d45aUxF4Q0R
KJprD3v5Z9...

Encrypted data (Ciphertext)

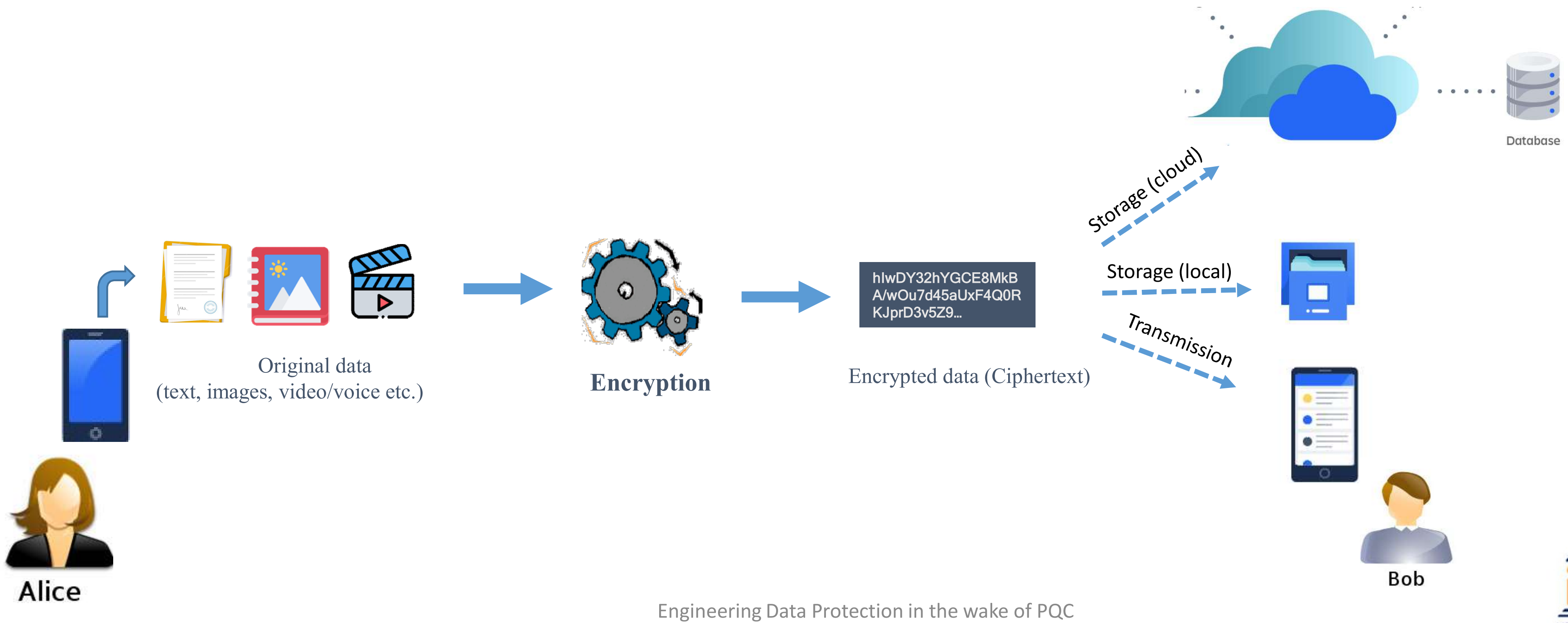
Storage (cloud)

Storage (local)

Database

Alice

Encryption in practice



Original data
(text, images, video/voice etc.)

Encryption

hlwDY32hYGCE8MkB
A/wOu7d45aUxF4Q0R
KJprD3v5Z9...

Encrypted data (Ciphertext)

Storage (cloud)

Storage (local)

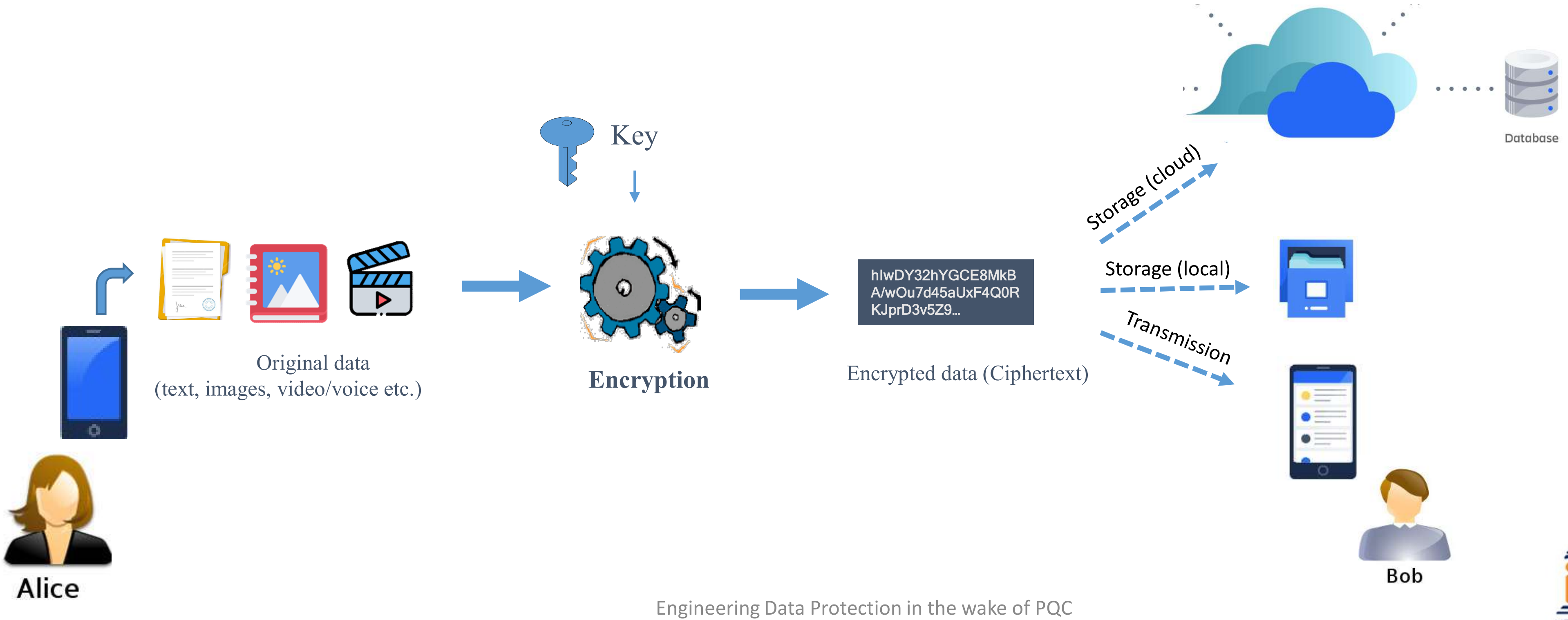
Transmission

Database

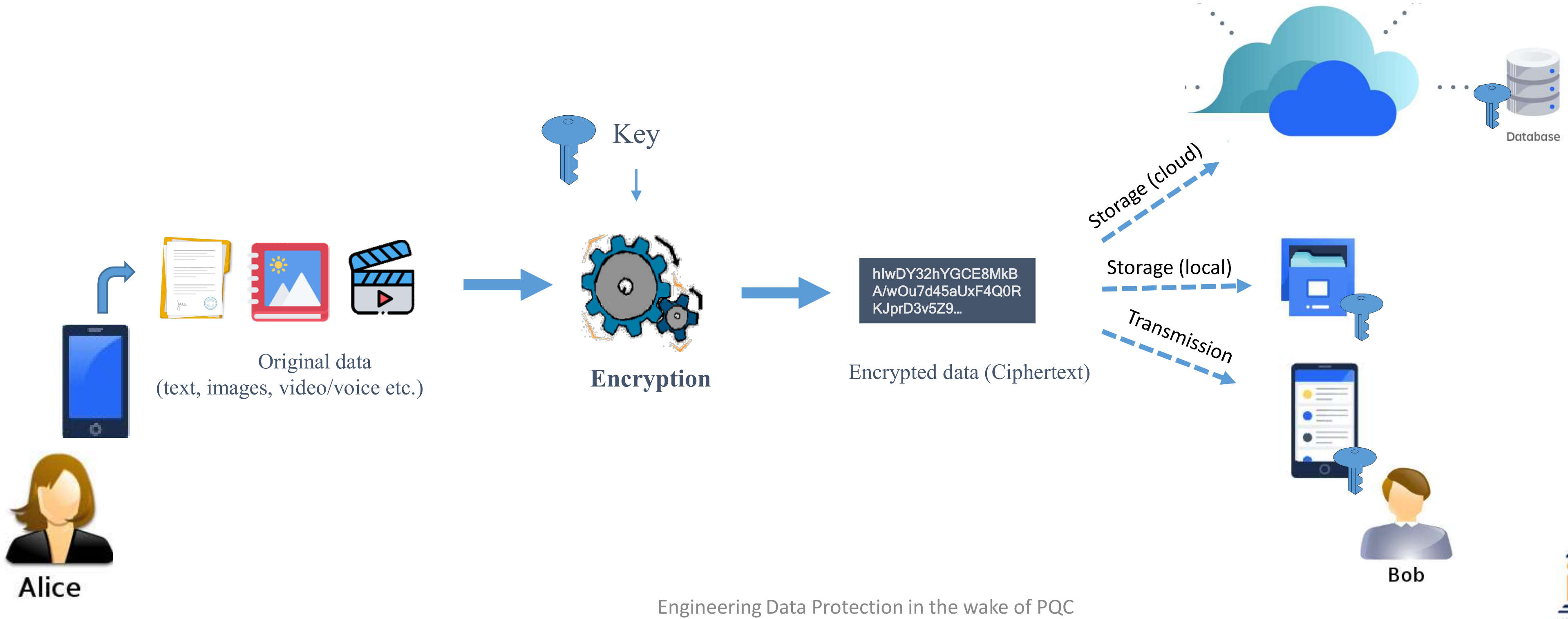
Alice

Bob

Encryption in practice



Encryption in practice



Key

Original data
(text, images, video/voice etc.)

Encryption

hlwDY32hYGCE8MkB
A/wOu7d45aUxF4Q0R
KJprD3v5Z9...

Encrypted data (Ciphertext)

Storage (cloud)

Storage (local)

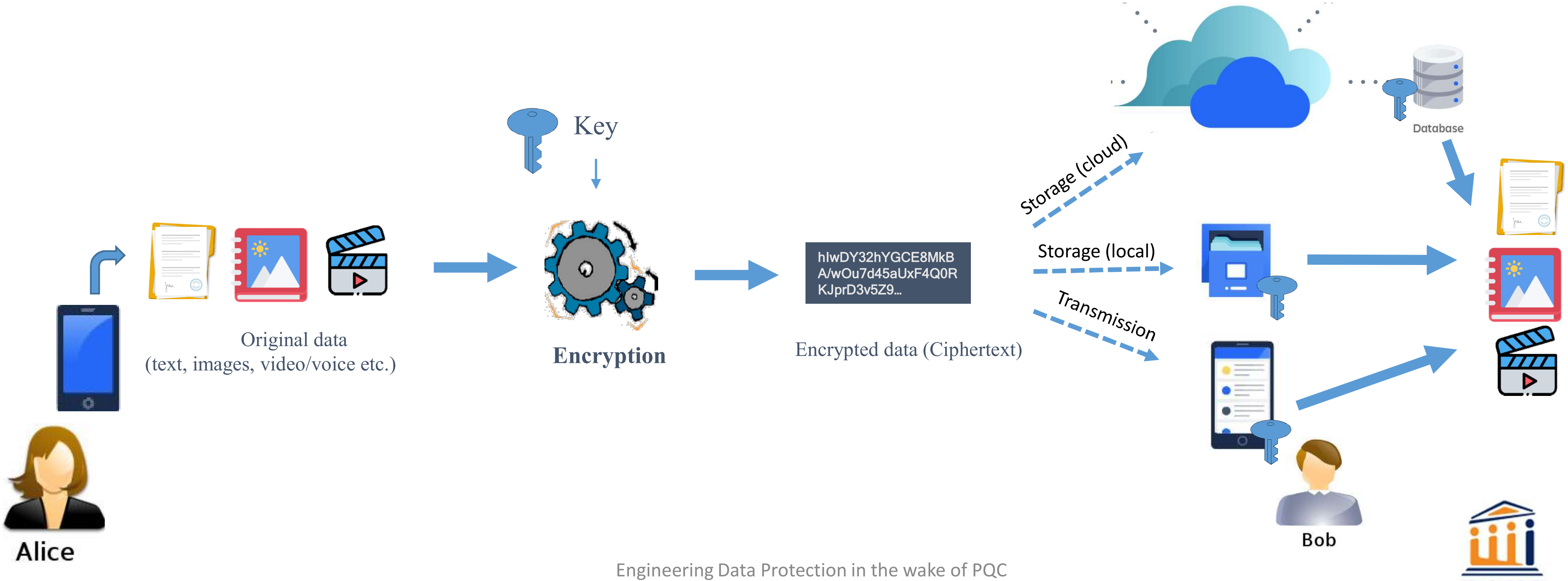
Transmission

Database

Alice

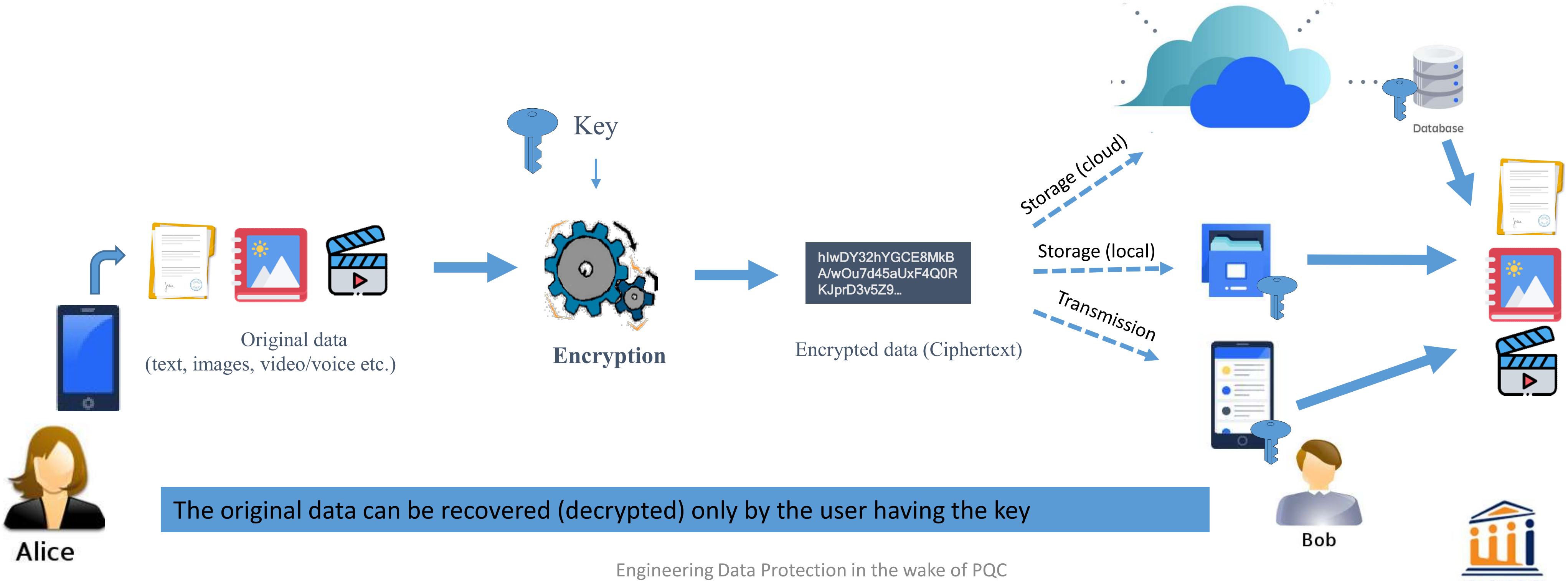
Bob

Encryption in practice



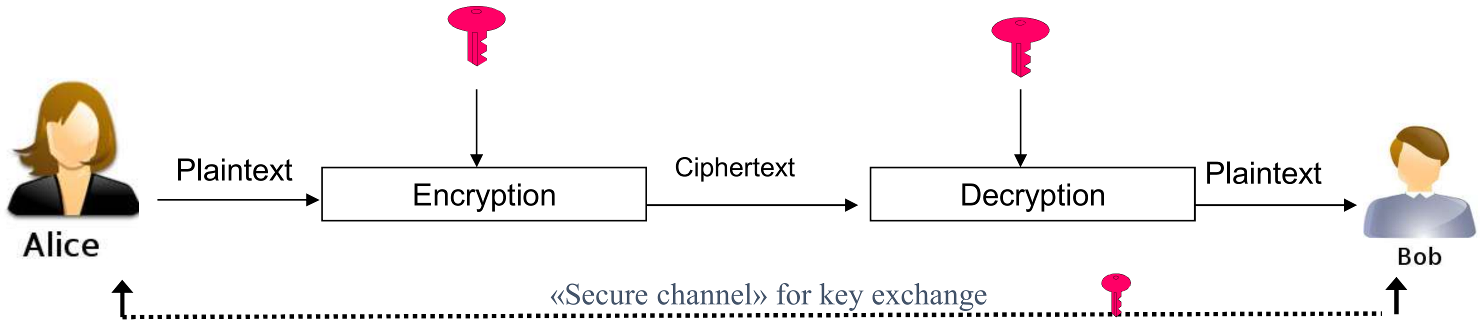
HELLENIC DATA
PROTECTION AUTHORITY

Encryption in practice



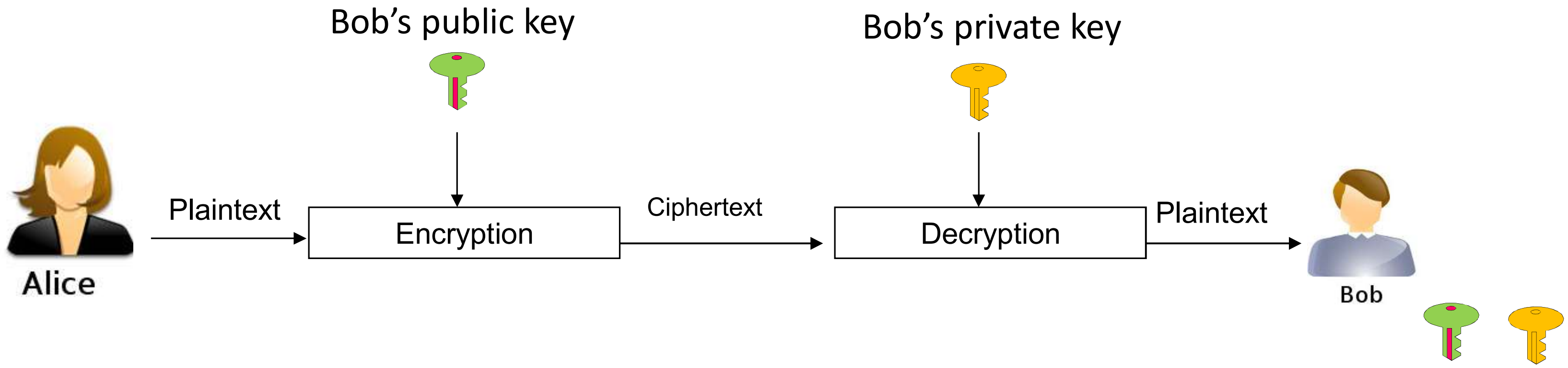
The original data can be recovered (decrypted) only by the user having the key

The key exchange problem



- To achieve this, we introduce the public-key (or asymmetric) cryptography
  - Mainly introduced to solve the following (Diffie-Hellman, 1976):
    - **Secure symmetric key exchange** (no need to a-priori secret communication)
    - **Digital signatures**
      - Verification of the authenticity of a “document” (it has not been modified)
      - Authentication of the “document” s creator (verification of the identity of the signer)

Public key (or asymmetric) encryption



Bob’s public key

Bob’s private key

Alice

Plaintext

Encryption

Ciphertext

Decryption

Plaintext

Bob

- Each user has a public key e and a private key d
  - The one “reverses” the other but they are different
  - The public key can be widely known
    - Typically, through digital certificates
  - It is practically infeasible to determine the private key from the public

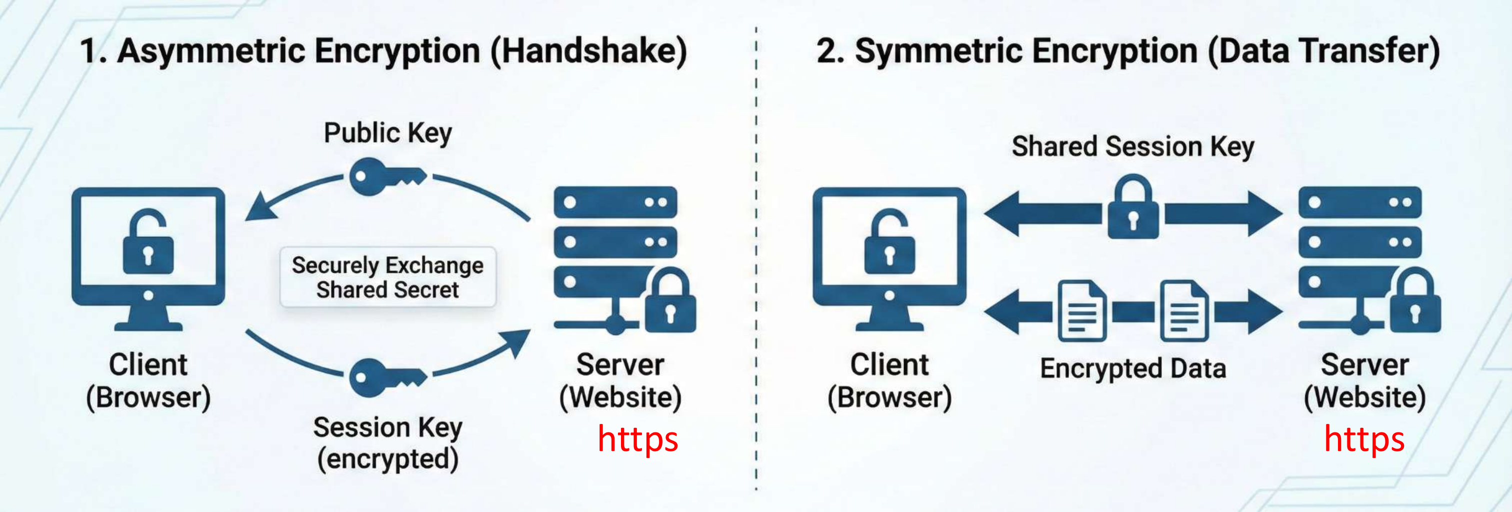
Such algorithms in practice:
RSA, Diffie–Hellman,
Elliptic Curve cryptographic algorithms

The security relies on known difficult mathematical problems

e.g. **integer factorization problem, (elliptic curve) discrete logarithm problem** etc.

A classical common real-world scenario

- Visiting an HTTPS website (TLS protocol) – a (very) simplified version



- The public key is obtained from a digital certificate that is **digitally signed** by a trusted authority
  - Hence, **asymmetric encryption** is again being used – in conjunction with the so-called cryptographic hash functions
  - The authenticity of the web site is also ensured by the validity of the certificate

HELLENIC DATA PROTECTION AUTHORITY

Privacy Enhancing Cryptography

- Lies in the wide class of Privacy Enhancing Technologies (PETs)
- A notion that includes a variety of cryptographic primitives as enablers for privacy
  - Zero-knowledge protocols
  - Homomorphic encryption
  - Secure multi-party computations
  - Attribute-based encryption
  - and others… (*e.g. searchable encryption, polymorphic encryption, proxy re-encryption etc.)*

They rely on asymmetric cryptography

enisa 20 years!

EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENGINEERING PERSONAL DATA PROTECTION IN EU DATA SPACES

JANUARY 2024

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENGINEERING PERSONAL DATA SHARING

Emerging Use Cases and Technologies

JANUARY 2023

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

DATA PROTECTION ENGINEERING

From Theory to Practice

JANUARY 2022

enisa

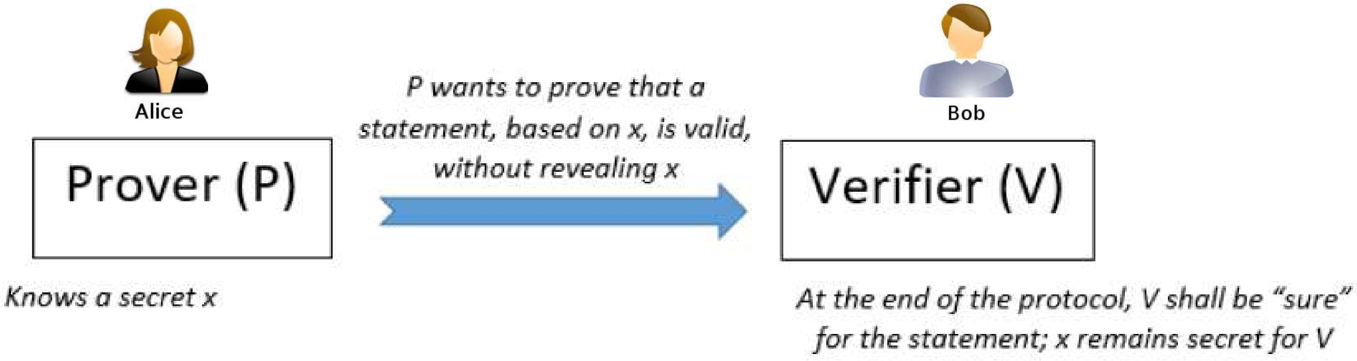
EUROPEAN UNION AGENCY FOR CYBERSECURITY

DATA PSEUDONYMISATION: ADVANCED TECHNIQUES & USE CASES

Technical analysis of cybersecurity measures in data protection and privacy

JANUARY 2021

Zero-knowledge (ZK) proofs


Alice

Prover (P)

Knows a secret x

P wants to prove that a statement, based on x, is valid, without revealing x

Bob

Verifier (V)

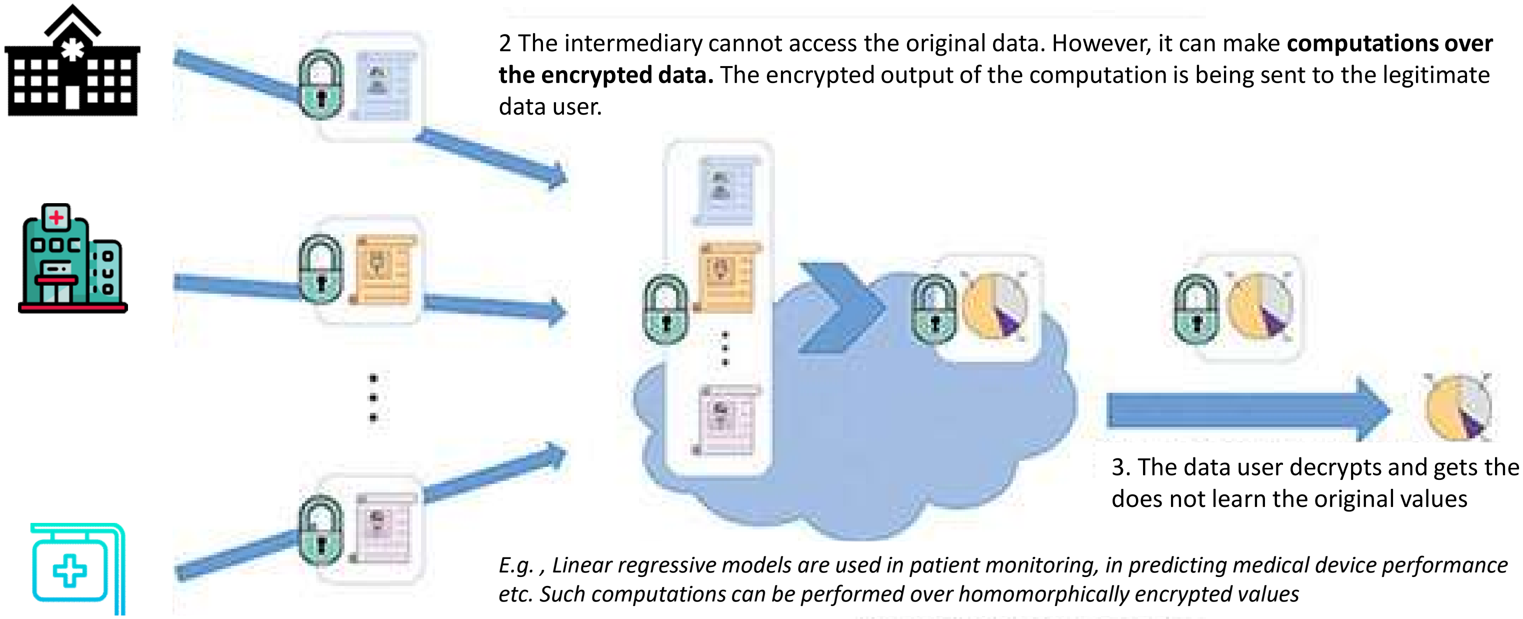
At the end of the protocol, V shall be "sure" for the statement; x remains secret for V

- Enabler for data minimization
  - E.g. For the age verification problem (envisioned by the European Commission)

- Well-known ZK protocols:
  - Feige – Fiat – Shamir (Identification of a user)
  - Schnorr (Identification of a user)
  - ZK-SNARKs (**succinct, non-interactive zero-knowledge proofs)**
    - Extremely short proofs and fast verification
    - They're widely used in blockchains

Homomorphic encryption (HE)

Computations over encrypted data, without having access to the original data



2 The intermediary cannot access the original data. However, it can make **computations over the encrypted data.** The encrypted output of the computation is being sent to the legitimate data user.

3. The data user decrypts and gets the output of the computation. It does not learn the original values

E.g. , Linear regressive models are used in patient monitoring, in predicting medical device performance etc. Such computations can be performed over homomorphically encrypted values

1. The data holders send encrypted data to the intermediary service; only the data user can decrypt.

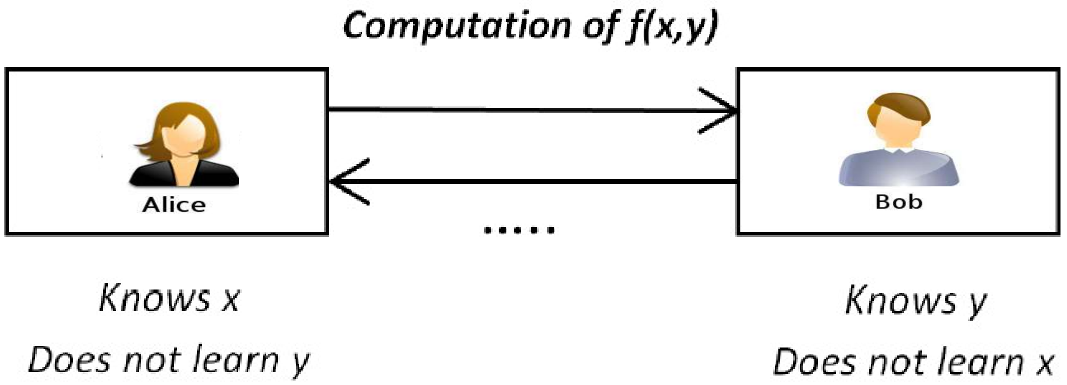
Applications in secure computations, private training in AI systems, private data sharing etc.

Types of HE

- Partially Homomorphic Encryption (PHE), which supports only addition or multiplication operation
  - E.g. the Paillier cryptosystem, the RSA homomorphism etc.
- Somewhat homomorphic encryption (SHE), which supports a limited number of homomorphic operations
- Fully homomorphic encryption (FHE), which supports an unbounded number of homomorphic operations
  - E.g. the pioneering work by Gentry in 2009
  - The BFV (Brakerski–Fan–Vercauteren) scheme
  - The BGV (Brakerski–Gentry–Vaikuntanathan) scheme
  - The CKKS (Cheon–Kim–Kim–Song) scheme
  - The Torus Fully Homomorphic Encryption (TFHE)

Used in known libraries (Seal, Palisade, Helib, Zama etc.)

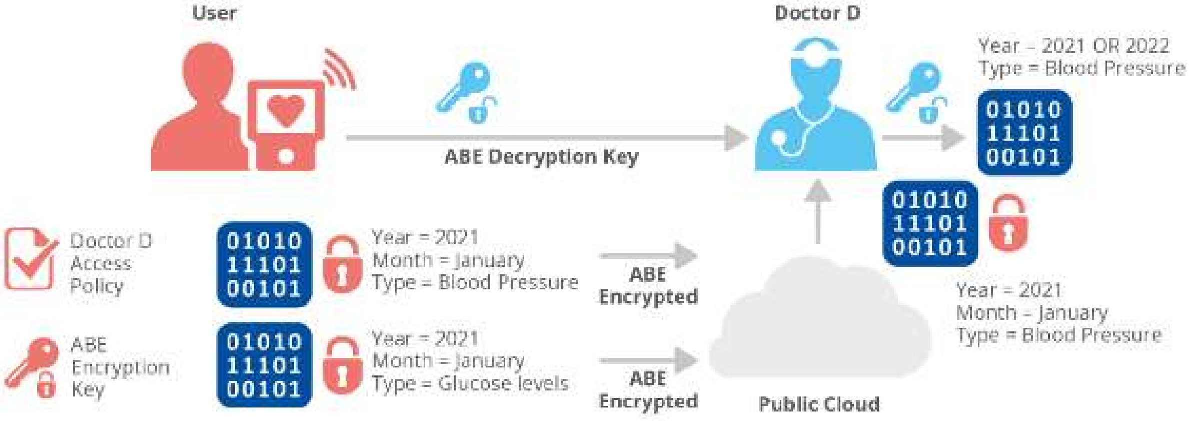
Secure multi-party computations (SMPC)



- Two or more parties jointly compute an outcome based on private pieces of information
  - E.g. comparing a person's DNA against a database with the goal of finding if the person is in a high risk group for this disease, without revealing anything on the person's DNA or the patients in the database
  - Used for "private" machine learning, private set intersection, collaborative analytics across enterprises etc.
    - See, e.g., the Eurostat's Joconde project
- Homomorphic encryption could be used to implement SMPC
- Other approaches: garbled circuits, secret sharing protocols, oblivious PRFs
- SMPC could be used to generate ZKP ('MPC-in-the-head' approach)

Attribute-based encryption (ABE)

An example (ENISA, 2023)



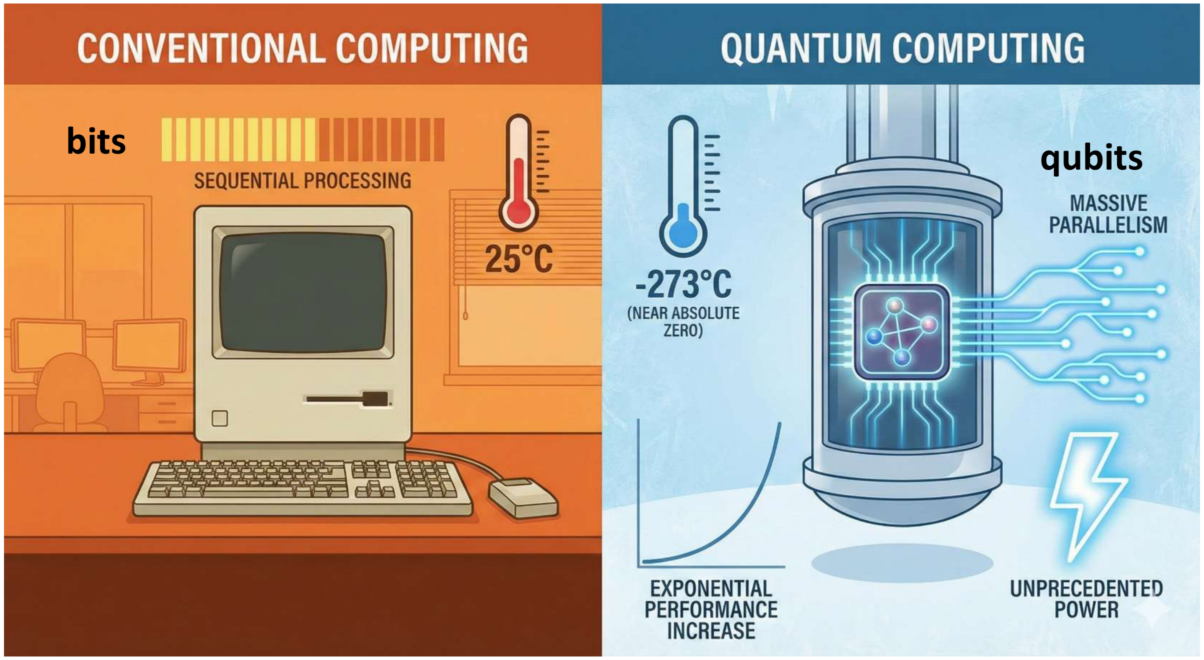
- Contrary to the classical notion of encryption, multiple keys can decrypt different parts of the encrypted data, based on the attributes of the corresponding original data
- The majority of them are based on security properties of bilinear pairings over elliptic curves

Privacy Enhancing Cryptography in AI systems

- ZK Proofs (ZKPs) may allow Machine Learning (ML) models to be trained and evaluated without exposing the underlying data. ZKPs also prove that training was based on valid datasets, making them ideal for outsourced or federated learning.
- HE can hide computations but, due to limitations in terms of computation functions, it is generally considered more suitable for the inference phase (which requires less computational resources than the training phase).
- SMPC allows different parties to train a model on combined datasets without revealing their proprietary data to one another (i.e. in federated learning). Additionally, SMPC can facilitate secure data labelling
- ABE is a special case of the so-called Functional Encryption (FE) – not widely used yet in AI systems due to practical limitations, but it is considered as an active research area.

Why we discuss about post-quantum cryptography?

Basic unit:
Bit
(0 or 1)



Basic unit:
Qubit
(0 or 1 or simultaneously both)

- It is still (?) infeasible to have quantum computes with significant number of qubits so as to be cryptographically-relevant
- However, what if we had?

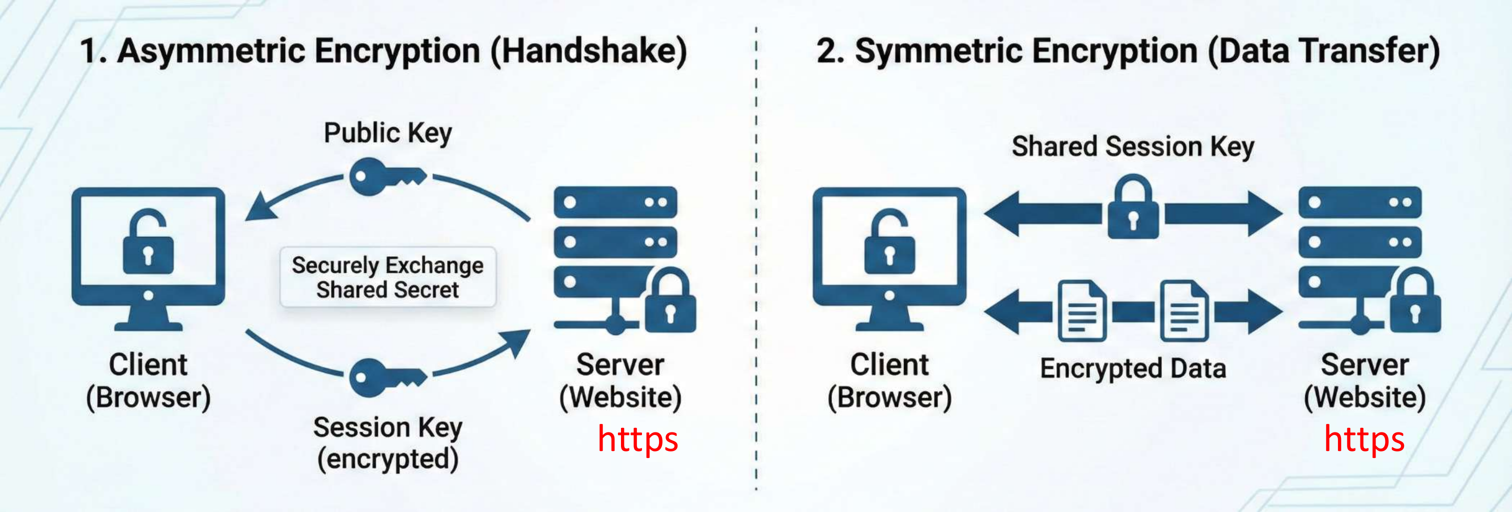
Famous algorithms for quantum computers

- Shor’s Algorithm — Efficiently factors large integers & solves discrete logarithms.
  - Breaks widely used schemes: RSA, Diffie–Hellman, Elliptic Curve cryptography
- Grover’s Algorithm — Speeds up brute-force key search
  - Weakens symmetric ciphers & hash functions by half the bit-security.
- **Impact:**
  - Due to the Grover’s algorithm, current symmetric cryptography will remain viable by **doubling key sizes** (e.g., AES-128 → AES-256).
  - Due to the Shor’s algorithm, current asymmetric cryptography **becomes fully insecure** (i.e., RSA, (Elliptic Curve) Diffie-Hellman, (Elliptic Curve) DSA etc.)

So, if we could have cryptographically-relevant quantum computers, well-known asymmetric (public key) algorithms would not provide security at all!

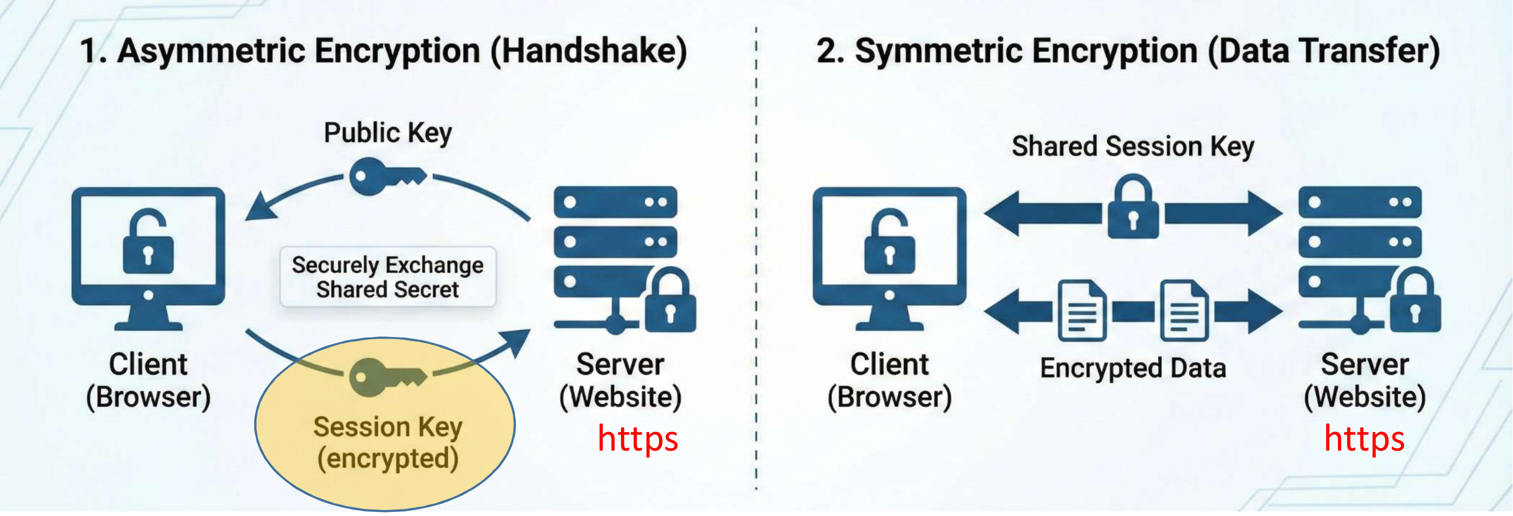
Revisiting the common real-world scenario

- Visiting an HTTPS website (TLS protocol) – a (very) simplified version



Revisiting the common real-world scenario

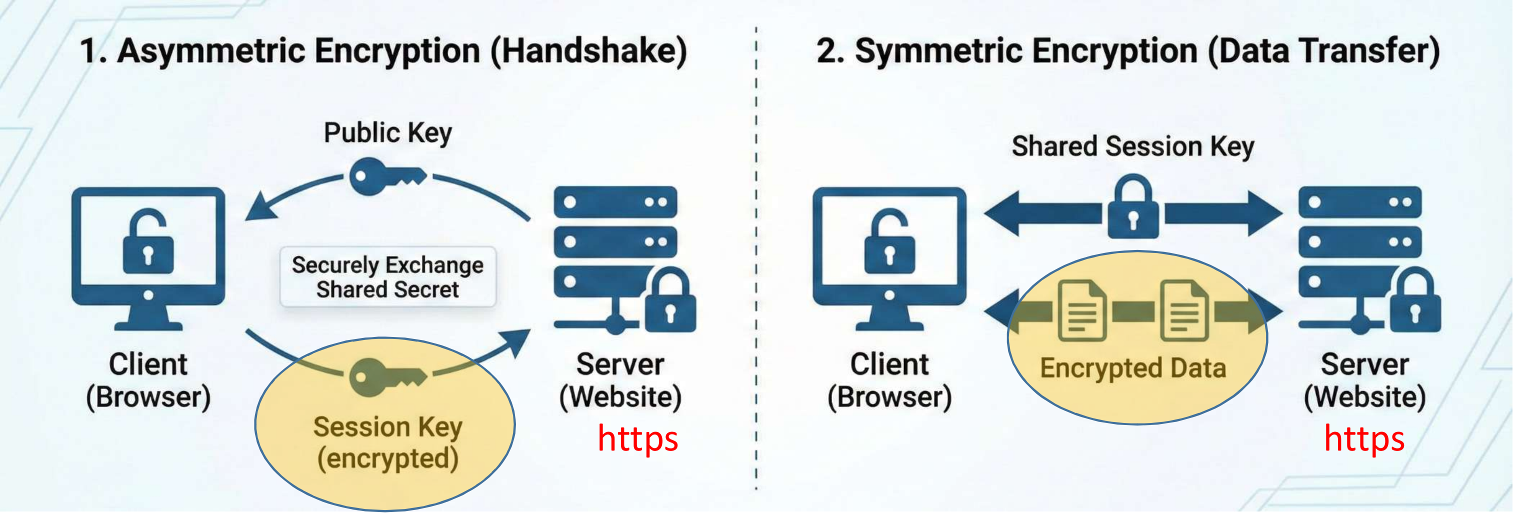
- Visiting an HTTPS website (TLS protocol) – a (very) simplified version



- With quantum computers:
  - Asymmetric encryption “collapses” – the session key can be compromised

Revisiting the common real-world scenario

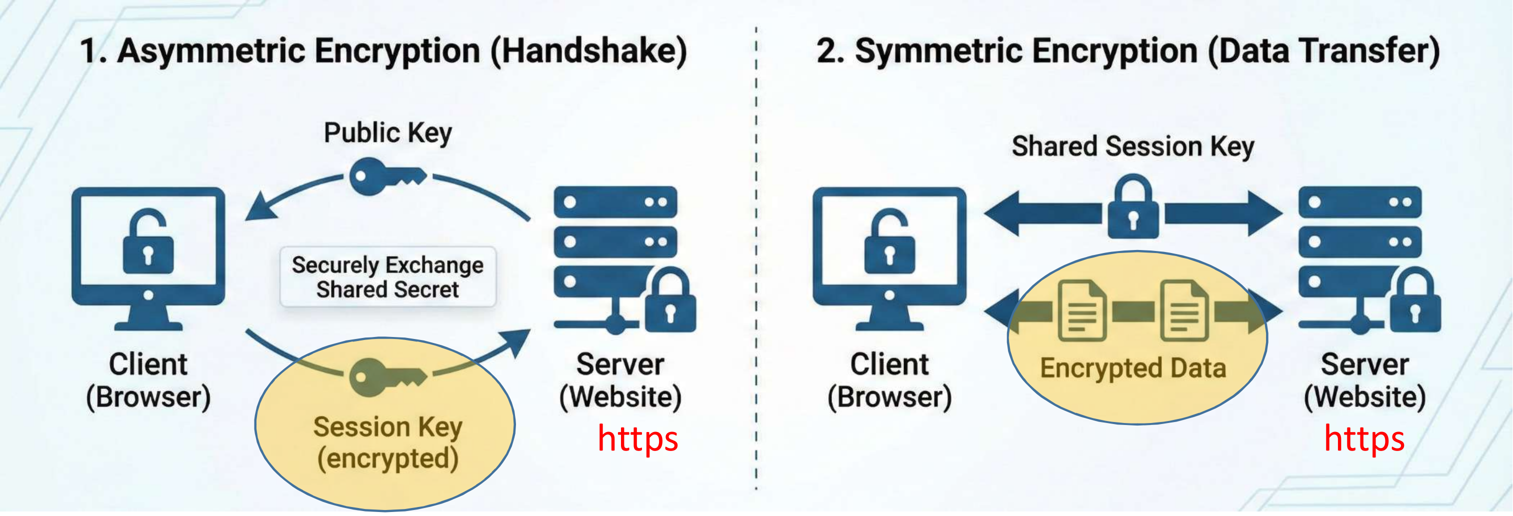
- Visiting an HTTPS website (TLS protocol) – a (very) simplified version



- With quantum computers:
  - Asymmetric encryption “collapses” – the session key can be compromised
  - The encrypted transferred data can be decrypted by any malicious party (the strength of the symmetric algorithm does not help…)

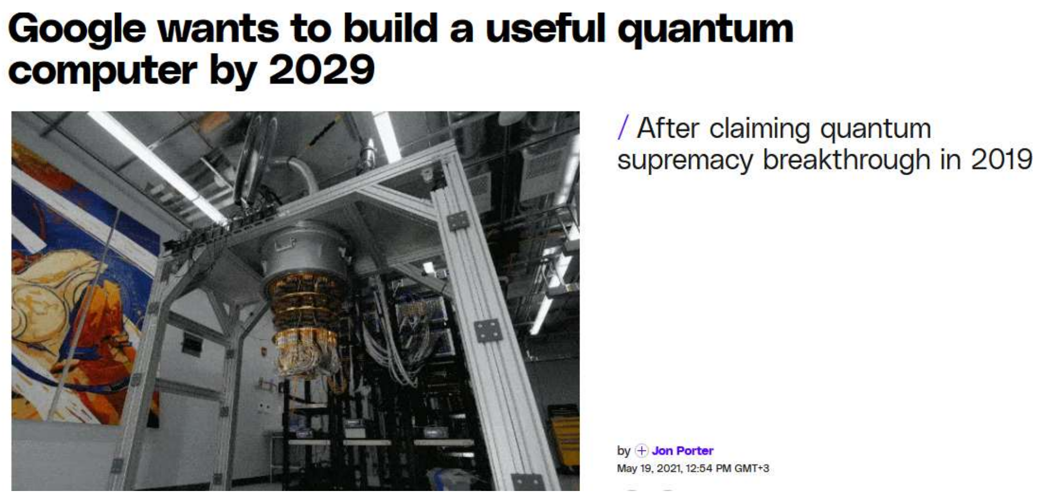
Revisiting the common real-world scenario

- Visiting an HTTPS website (TLS protocol) – a (very) simplified version



- Store (harvest) now – Decrypt later attack
  - If someone “writes down” all our today’s secure communications, she will be able to read them when cryptographically relevant quantum computes become a reality

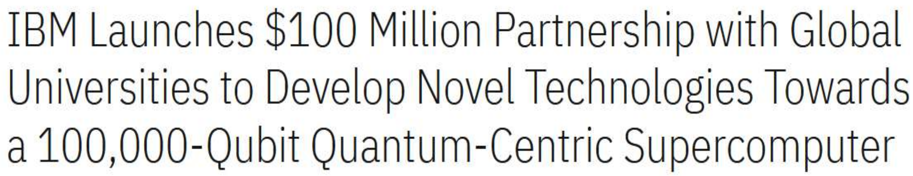
How far are we from quantum computers?



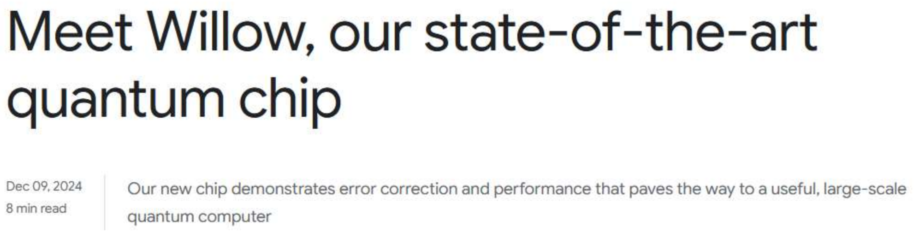
Google wants to build a useful quantum computer by 2029

/ After claiming quantum supremacy breakthrough in 2019

by Jon Porter
May 19, 2021, 12:54 PM GMT+3



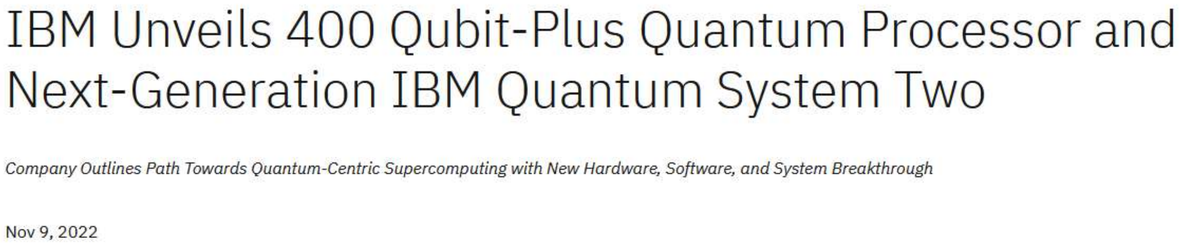
IBM Launches $100 Million Partnership with Global Universities to Develop Novel Technologies Towards a 100,000-Qubit Quantum-Centric Supercomputer



Meet Willow, our state-of-the-art quantum chip

Dec 09, 2024
8 min read

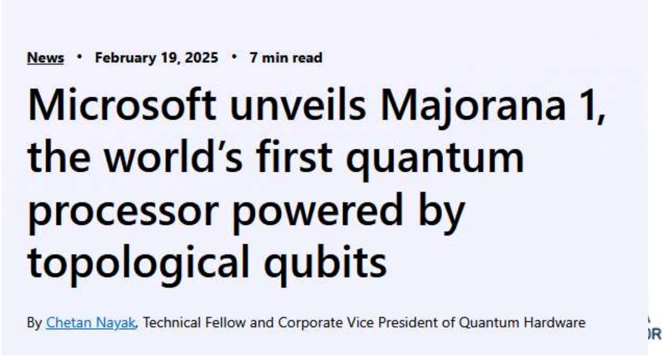
Our new chip demonstrates error correction and performance that paves the way to a useful, large-scale quantum computer



IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two

Company Outlines Path Towards Quantum-Centric Supercomputing with New Hardware, Software, and System Breakthrough

Nov 9, 2022



News • February 19, 2025 • 7 min read

Microsoft unveils Majorana 1, the world's first quantum processor powered by topological qubits

By Chetan Nayak, Technical Fellow and Corporate Vice President of Quantum Hardware

Why post-quantum cryptography?

- Recall the wide use of public key cryptography…
  - Key exchange
  - Digital signatures
  - Privacy Enhancing Cryptography (ZK proofs, homomorphic encryption, SMPC, ABE etc.)
- **The above will not remain secure if they rely on "difficult" problems that can be solved by quantum computers (as is the typical case)**
- Post-Quantum Cryptography (PQC): Asymmetric (Public key) cryptography that its security relies on mathematical problems that cannot be solved (up to our current knowledge) neither by quantum computers

PQC is not quantum cryptography!

- **Quantum cryptography is based on physics, by exploiting quantum properties to perform cryptographic operations**
  - Fully different from “classical” cryptography
  - Still with some limitations (distance, expensive etc.)

What is PQC?

- Post-quantum cryptography is a special class of the typical “public-key” (i.e., asymmetric) cryptography
  - **But** its security rests with mathematical problems that cannot be solved either by quantum computers
  - Main such mathematical problems:
    - Lattice-based
    - Code-based
    - Hash-based
    - Multivariate-quadratic
    - Supersingular elliptic curve isogeny cryptography

PQC worlwide standards

- NIST initiated in 2016 a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms
- The first standards have been selected in June 2022, after three rounds of evaluation:

Algorithm	Type	Mathematical problem that is based on
CRYSTALS-KYBER	Encryption – Key Encapsulation	Lattice
CRYSTALS-DILITHIUM	Signature	Lattice
FALCON	Signature	Lattice
SPHINCS+	Signature	Hash-based

A significant portion comes from European research teams.

PQC worldwide standards

- NIST continues for new standards (calling also for new submissions)
- 11 March 2025: A new standard was announced
  - The aim was to choose a standard relying on another difficult mathematical problem (i.e., not lattice-based)

Algorithm	Type	Mathematical problem that is based on
HQC	Encryption – Key Encapsulation	Code-based

By several research institutions, including European

  - It has been chosen as a backup standard
  - Its official document is expected in about a year from now
- The process continues for new standards for digital signatures

Performance of new PQC standards

- Extensive research has been performed during the last years, especially for the TLS
  - There are efficient purely post-quantum solutions for authentication and key exchange as well as efficient hybrid post-quantum solutions
    - **Hybrid = combination of classical algorithms with PQ**
  - The performances of post-quantum secure implementations seem to be restricted in ‘noisy’ environments with significant packet loss.
    - However, embedding post-quantum secure algorithms does not negatively affect the overall performance as substantially as poor network conditions.
- NIST concludes that PQC algorithms are expected to be acceptable for most general applications.

Challenges in adopting PQC into Privacy Enhancing Cryptography

- Existing protocols (ZK proofs, SMPC etc.) are built around specific assumptions
  - They need full re-design
    - It is not just a matter of just replacing algorithms
    - It is not just a matter of increasing the size of the keys

Post-quantum secure ZK proofs?

- Well-known ZK protocols:
  - Feige – Fiat – Shamir (Identification of a user)
  - Schnorr (Identification of a user)
  - ZK-SNARKs (**succinct, non-interactive zero-knowledge proofs)**

Post-quantum secure ZK proofs?

- ~~Well-known ZK protocols:~~
  - ~~Feige – Fiat – Shamir (Identification of a user)~~
  - ~~Schnorr (Identification of a user)~~
  - ~~ZK-SNARKs (**succinct, non-interactive zero-knowledge proofs)**~~

No post-quantum secure!

Post-quantum secure ZK proofs?

- ~~Well-known ZK protocols:~~
  - ~~Feige – Fiat – Shamir (Identification of a user)~~
  - ~~Schnorr (Identification of a user)~~
  - ~~ZK-SNARKs (**succinct, non-interactive zero-knowledge proofs)**~~

No post-quantum secure!

- **But…**
  - ZK-STARKs - Zero-knowledge Scalable Transparent ARguments of Knowledge
    - Security is based on cryptographic hash functions
  - PQ secure ZK-SNARKs
    - Mainly relied on either hash-based (e.g. Ligero) or lattice-based problems (e.g. Crescent, Ligetron)

Post-quantum secure ZK proofs?

- ~~Well-known ZK protocols:~~
  - ~~Feige – Fiat – Shamir (Identification of a user)~~
  - ~~Schnorr (Identification of a user)~~
  - ~~ZK-SNARKs (**succinct, non-interactive zero-knowledge proofs)**~~

No post-quantum secure!

- The European Commission, for the age verification solution, seems to have chosen* the solution from a recent paper [Frigo et. al., 2024] which builds upon the Ligero protocol
  - The paper has not peer-reviewed yet
  - Several possible solutions were examined, according to specific requirements
    - The PQ security was not one of them
    - Ligero is PQ secure, but a rigorous analysis for this new solution is needed….

* https://github.com/eu-digital-identity-wallet/av-doc-technical-specification/blob/main/docs/annexes/annex-B/annex-B-zkp.md

Post-quantum secure Homomorphic Encryption?

- The first known partially homomorphic ciphers (e.g., the Paillier's cryptosystem) are not PQ secure
- However:
  - Since 2009, by the Gentry's advancements, lattices have been mainly used to provide both additive and multiplicative homomorphisms (i.e. FHE schemes)
    - So, their security rests with an underlying lattice-based problem

↓

Due to this, they are generally considered as PQ secure

Post-quantum secure MPC?

- Typical "classical" implementations of garbled circuits and oblivious PRFs are no PQ-secure
- However:
  - Several SMPC protocols rely on FHE
    - If the FHE is PQ secure, the same (probably) holds for the SMPC
  - PQ secure oblivious PRFs have been proposed
    - LEAP (Eurocrypt 2025): A novel Oblivious PRF based on lattice assumptions, <u>with high performance</u>

Post-quantum ABE?

- Most ABE schemes are based on bilinear maps over elliptic curves

  → no PQ secure
- New ABE schemes are being developed that rely on difficulties of lattice-based problems
  - Research though highlights that such PQ secure solutions come at a cost
    - In many cases, these schemes are less efficient than classical ABE
      - Larger parameters, slower performance

Discussion on PQ security of Privacy Enhancing Cryptography

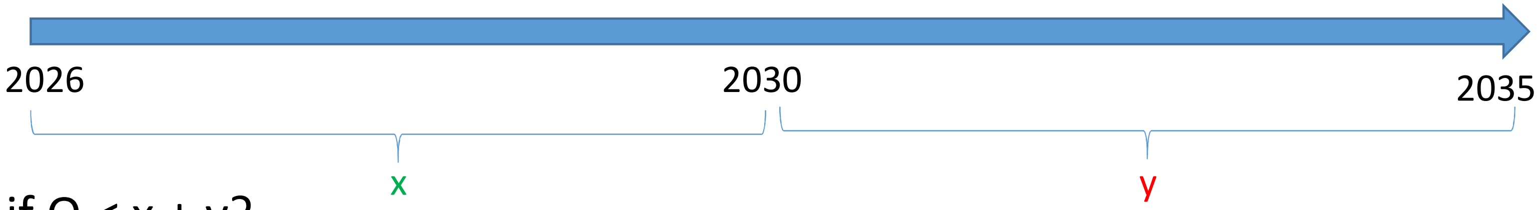
- There are no existing standards
  - Current PQ secure cryptographic standards correspond to key exchange and digital signatures
    - They are not “directly applicable” to PEC
- The security is not (always) well established under a formal proof
  - Combining primitives with proven security individually, does not ensure an overall security for their composition.
- In general, there are performance issues (extra computing and memory needs)
  - Although recent advances such as the LEAP are quite promising
- Implication challenges: How to mitigate the so-called side-channel attacks?
  - The math are here, but what about a non-secure implementation?
  - PQC is still quite new….

An academic timeline - So, when to start?

According to Mosca's work (https://eprint.iacr.org/2015/1075)

- **Q:** #years until first large (cryptographically relevant) quantum computer
- **x:** #years it take to switch
- **y:** #years data need to be confidential

- Need to start switching in the year 2026+Q-x-y
- If Q=10, x=5 and y=5?



- What if Q < x + y?

Summary - Conclusions

- Embedding PQC in real-time applications is indeed necessary
  - Not only in TLS (e.g. https) but also in other daily applications (video conferences, emails, encrypting software etc.)
    - Already a few video conferencing platforms started to use PQC
- Critical infrastructures shall also provide PQ security
  - We may assume that the “store now – decrypt later” attack already happens
- Efficiency issues for employing PQC for cybersecurity seem to not be a burden
  - Consider also hybrid implementations for the transition period
- The EC roadmap for PQC transition indicates this urgency

Summary - Conclusions

- However:
  - It is not only a matter of security, but also a matter of privacy
  - PEC must also be PQ secure
    - Not standards yet worldwide
  - PQ-secure PEC is now a sovereignty issue
  - Digital identities (e.g. digital wallets), AI systems, and data spaces shall follow the necessity of PQ security
    - For instance, ECDSA is not PQ secure…..
    - A requirement for the ZKP for age verification through the digital wallet seems to be that "*A ZKP scheme SHALL provide support for privacy-preserving proof of possession of a Proof of Age attestation by proving knowledge of a private key that corresponds to an ECDSA signature*".

«Cryptography is about the right to privacy, freedom of speech, freedom of political association, freedom of the press, freedom from unreasonable search and seizure, freedom to be left alone».

Phil Zimmermann

Useful sources

- ENISA, “Engineering personal data protection in EU Data Spaces”, 2024.
- ENISA, “Engineering personal data sharing – Emerging use cases and technologies”, 2023.
- Heimberger, L. et. al., “Leap: A fast, lattice-based OPRF with application to private set intersection*”,* In *Advances in Cryptology – EUROCRYPT 2025* (pp. 254–283), Springer, 2025
- Frigo, M., & Shelat, A., “Anonymous credentials from ECDSA*”,*. Cryptology ePrint Archive, Paper 2024/2010.
- G. Sravya et. al., “Survey of Post-Quantum Lattice-Based Ciphertext-Policy Attribute-Based Encryption Schemes,” *IEEE Security & Privacy*, vol. 22, no. 4, pp. 1–20, Oct. 2024.
- L. Malina *et al*., "Post-Quantum Era Privacy Protection for Intelligent Infrastructures," *IEEE Access*, vol. 9, pp. 36038-36077, 2021.
- R. Wang, C. Hazay and M. Venkitasubramaniam, "Ligetron: Lightweight Scalable End-to-End Zero-Knowledge Proofs Post-Quantum ZK-SNARKs on a Browser," *2024 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2024, pp. 1760-1776.
- Doan, T. V. T., Messai, ML., Gavin, G. *et al.*, “A survey on implementations of homomorphic encryption schemes”,. *J Supercomput* 79, 15098–15139, Springer, 2023.

HELLENIC DATA
PROTECTION AUTHORITY

Thank you for your attention!

Discussion / Questions ?