Leanear

Trusting the Cloud

Cécile Delerablée (CEO)

Our DNA

Leveraging expertises in Cryptography and Operational Security to tackle hard tech challenges and durably address customer concrete problems.

The Team

Backed by

Cécile Delerablée, PhD
CEO
(ENS, Orange, CryptoExperts)

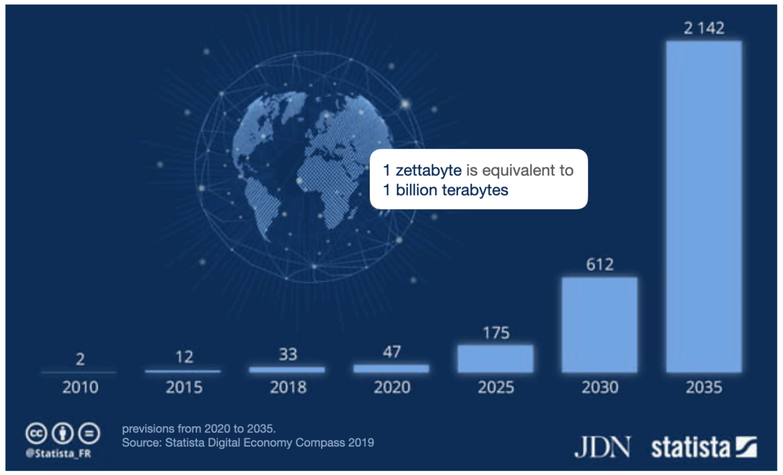
Yohann Thomas, PhD
CTO
(Orange, ANSSI)

Lénaïck Gouriou
PhD Student
(ENS)

Pierre Hardy
Lead Software
(Sopra, ANSSI)

Bérenger Rosat
Lead DevOps
(Cassidian, ANSSI)

Cloud (R)Evolution…

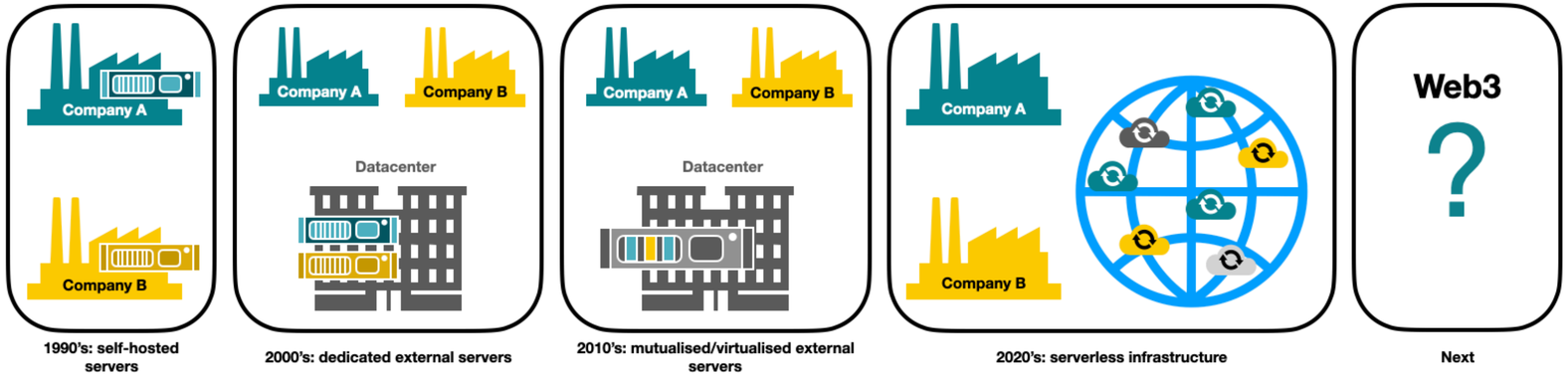


- More and more data

DATA is the new OIL

- More and more value

- Less and less control



...Cyberattacks Explosion

2021 Highlights

Number of victims whose data was posted on leak sites:
+85% to 2,566 organizations

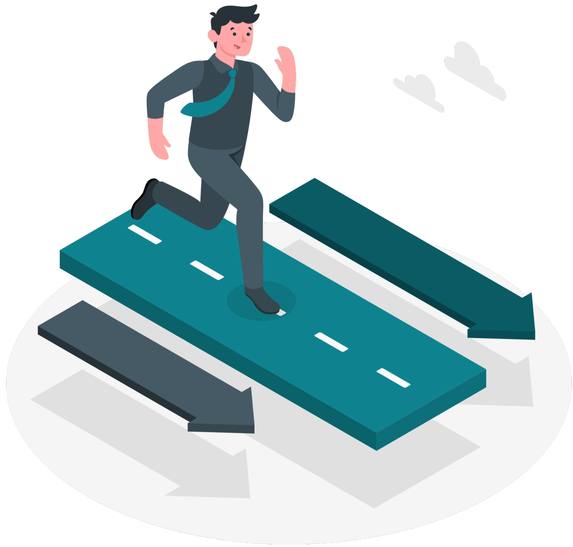
Cyber extortion ecosystem:
emergence of 35 new ransomware gangs

Frequency of ransomware attacks:
11 seconds (40 seconds in 2016)

Average ransom demand:
+144% to $2.2 million

Source: Palo Alto Networks - Unit 42, 2022 Ransomware Threat Report

Perimeter Security



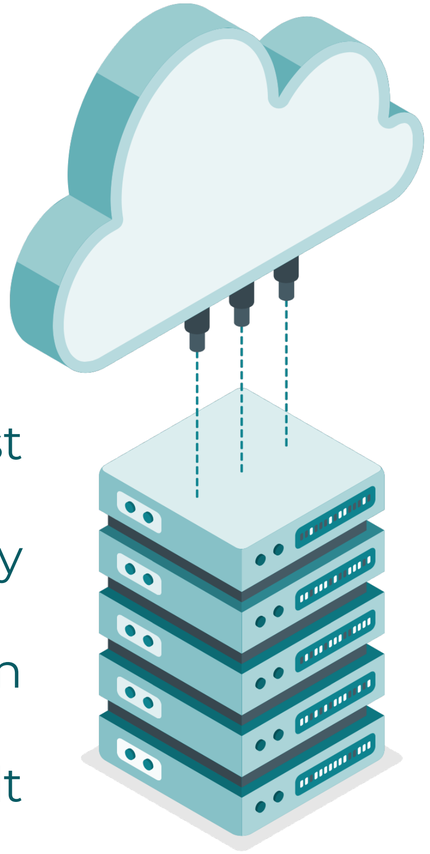
Data security is needed more than ever

Zero Trust

Data Centric Security

Privacy by Design

Privacy by Default

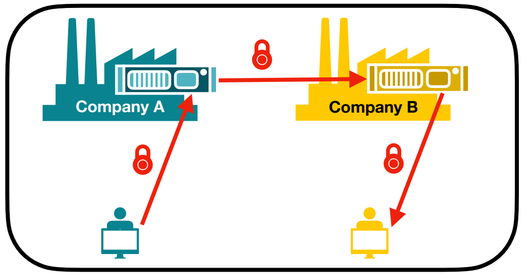


Solution: End-to-End Encryption (E2EE)

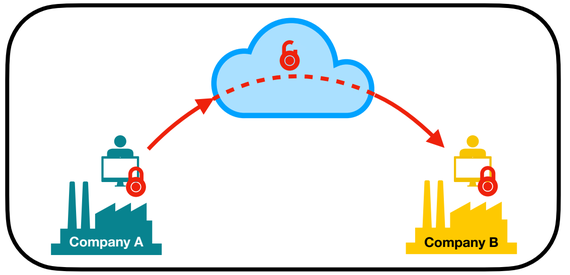
E2EE allows communications where only communicating users can read the content. It aims to prevent potential eavesdroppers[1] from being able to access the content (i.e the cryptographic keys needed to decrypt the content).

A technical means to address issues related to regulatory compliance, data leaks, data sovereignty, and more generally to data protection.

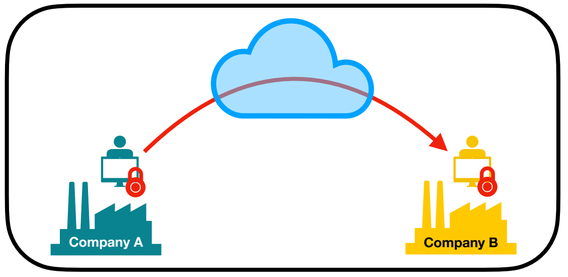
Related concepts / principles: Data-Centric Security, Privacy by Design, Zero-Trust, Web3.



Client-server / server-server security



« Traditional » Cloud security (relying on Cloud provider)



En-to-end security

(1) including telecom providers, Internet providers, malicious state bodies, and even the provider of the communication service

« Not Data Centric » Solutions

- VPNs
- Peer2Peer communications

E2EE: easily applicable to chat[1], but... Hard to generalize

(1) E2EE has become the norm for instant messaging applications (Signal, Whatsapp, etc.)

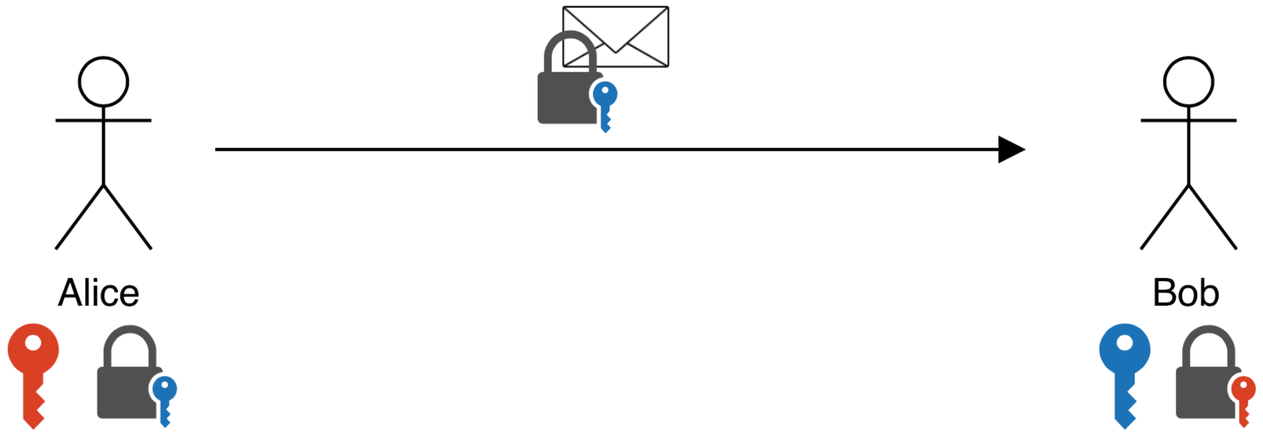
Our mission: bringing E2EE[1] generalization

(1) E2EE: End-to-end Encryption

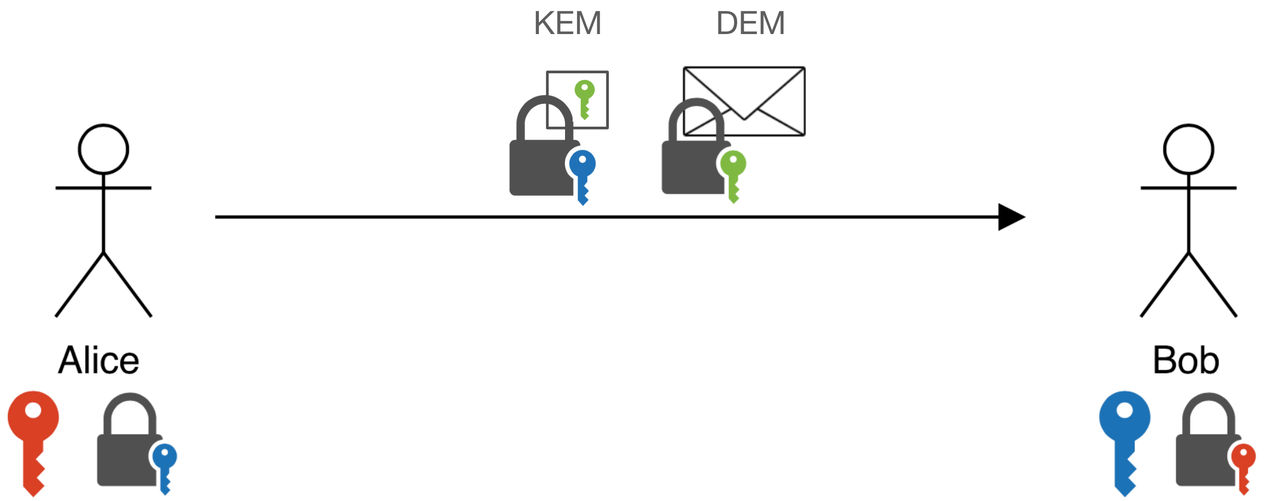
Back to the 70’s

Symmetric Encryption

Asymmetric Encryption



Hybrid Encryption

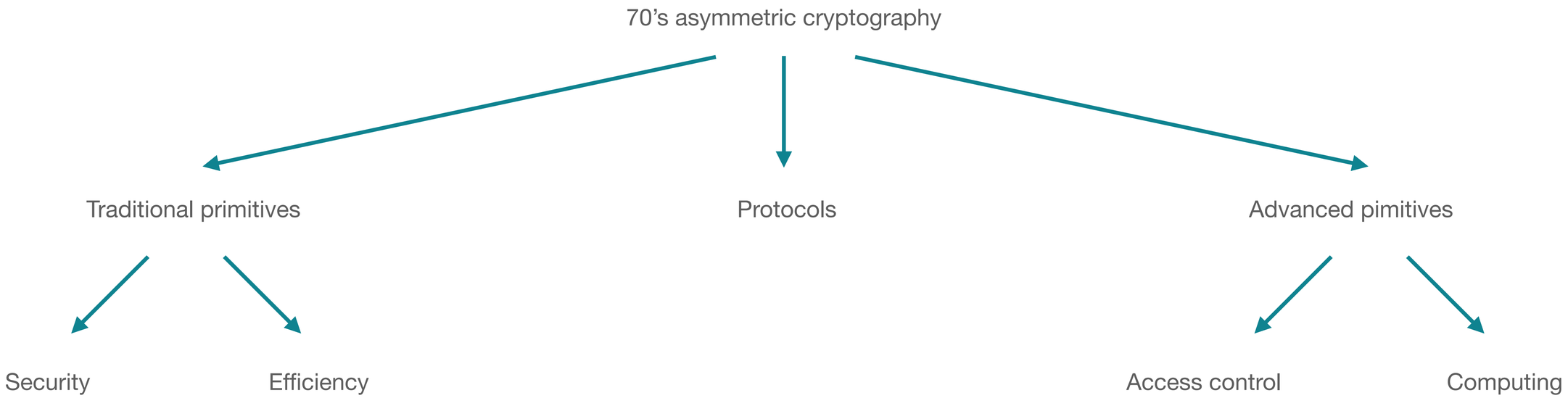


KEM: Key Encapsulation Mechanism

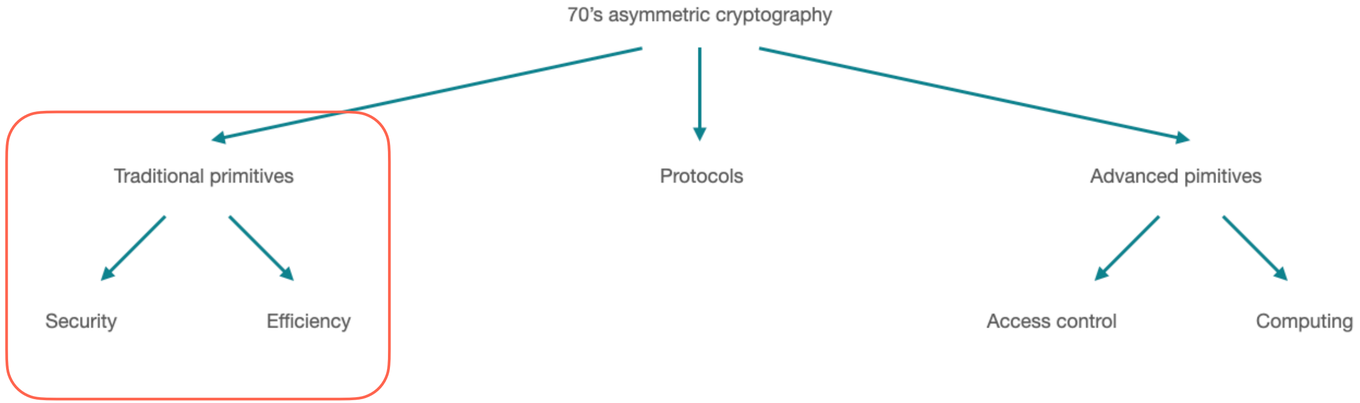
DEM: Data Encapsulation Mechanism

In the 2000's

Evolutions



Traditional Primitives



Traditional Primitives

Security

ex: Post-Quantum resistance

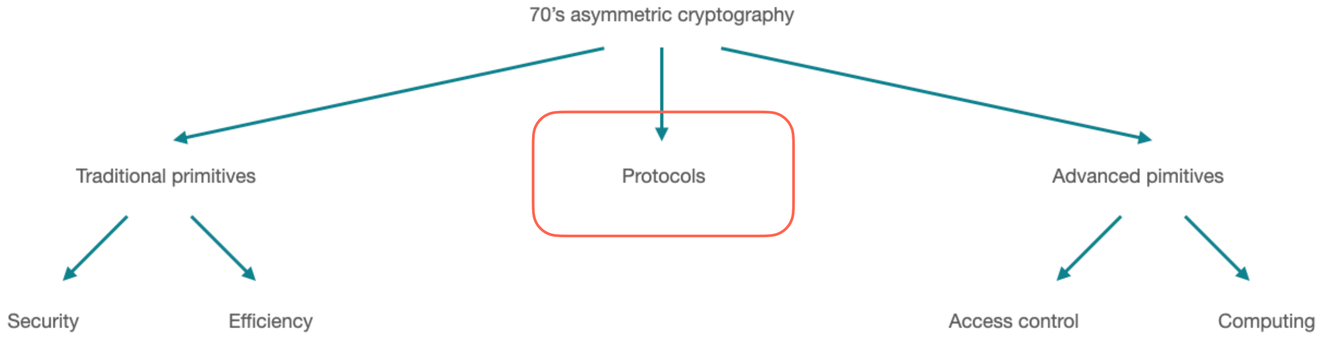
Efficiency

Keys size

Output size

Computing efficiency

Protocols



DH, TLS

Diffie–Hellman key exchange

From Wikipedia, the free encyclopedia

Diffie–Hellman key exchange[nb 1] is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as conceived by Ralph Merkle and named after Whitfield Diffie and Martin Hellman.[1][2] DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography.

Transport Layer Security

From Wikipedia, the free encyclopedia

Transport Layer Security (**TLS**) is a cryptographic protocol designed to provide communications security over a computer network. The protocol is widely used in applications such as email, instant messaging, and voice over IP, but its use in securing HTTPS remains the most publicly visible.

2004: OTR

Off-the-Record Communication,
or, Why Not To Use PGP

Nikita Borisov
UC Berkeley
nikitab@cs.berkeley.edu

Ian Goldberg
Zero-Knowledge Systems
ian@cypherpunks.ca

Eric Brewer
UC Berkeley
brewer@cs.berkeley.edu

...  ...

2005: SAS

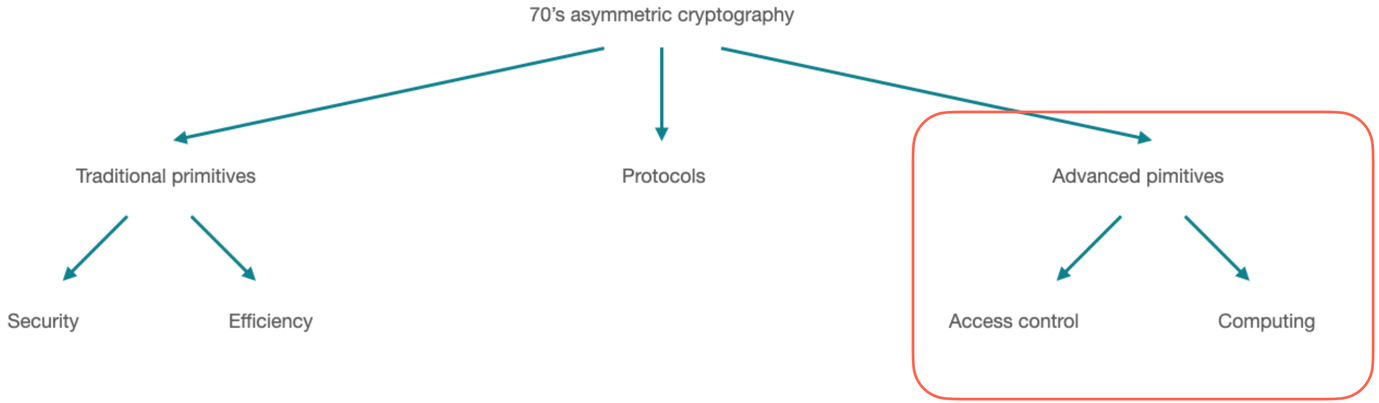
Ensuring the link between a cryptographic identity and a human being

Secure Communications over Insecure Channels Based on Short Authenticated Strings

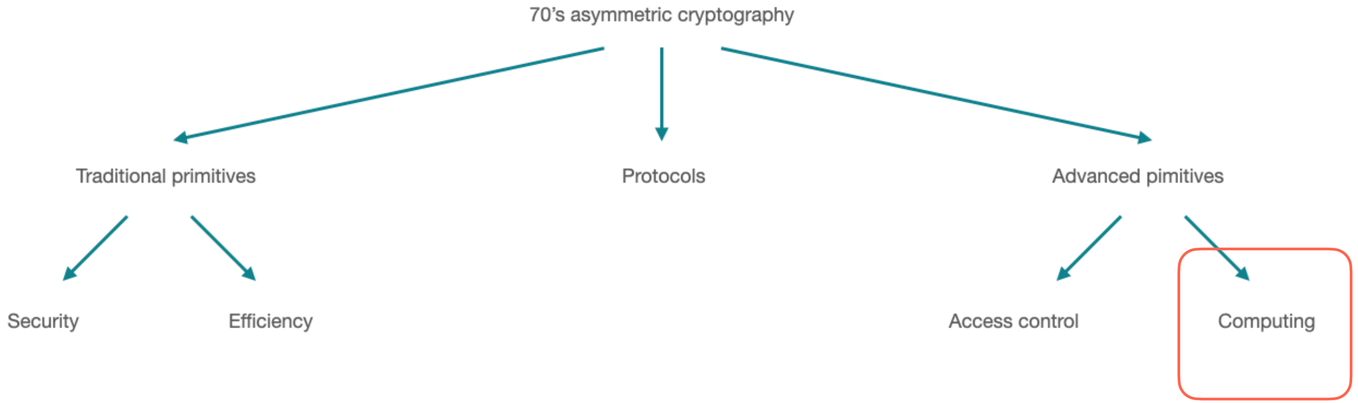
Serge Vaudenay

EPFL

Advanced Primitives



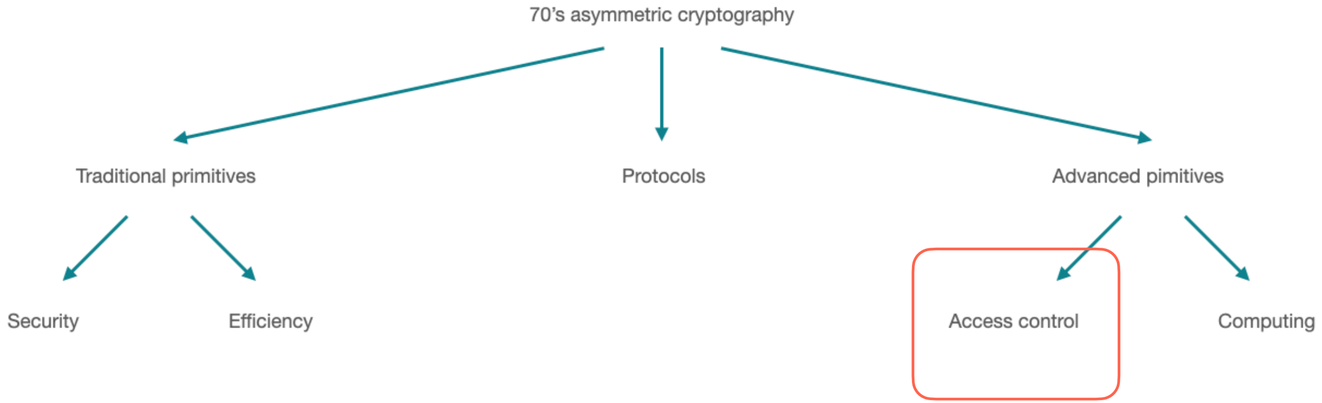
Computing



Computing

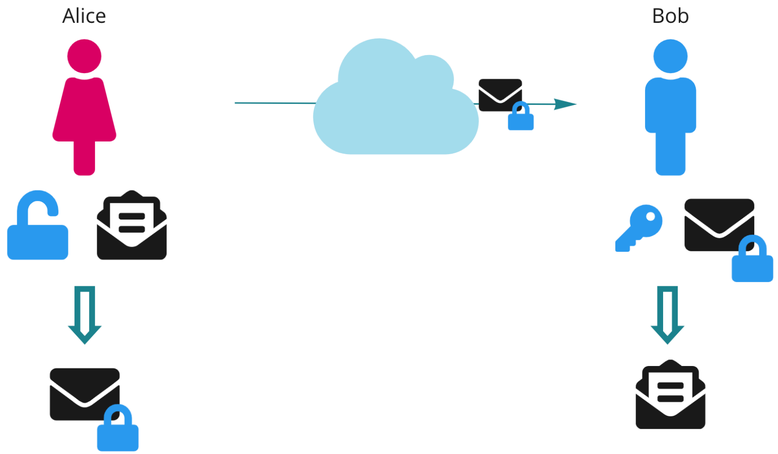
- Searchable Encryption (SE)
- Secure Multiparty Computation (MPC)
- Fully Homomorphic Encryption (FHE)

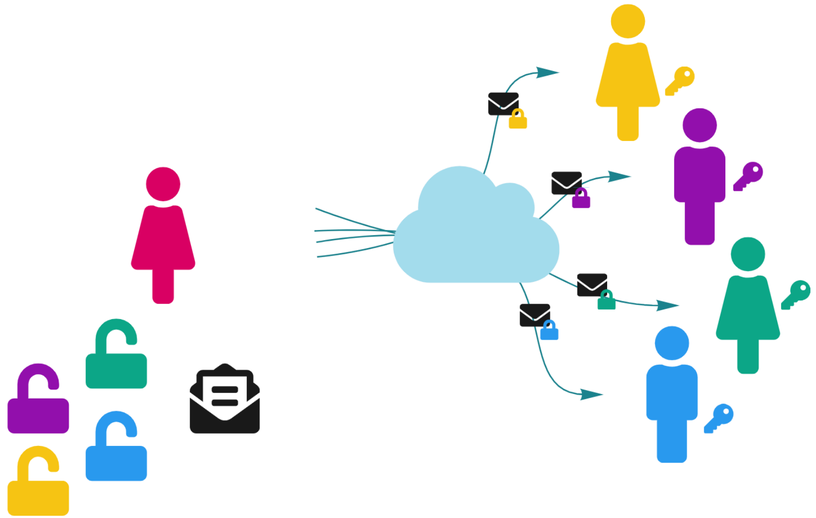
Access Control



Traditional Paradigm

1 encryption key <=> 1 (unique) decryption key



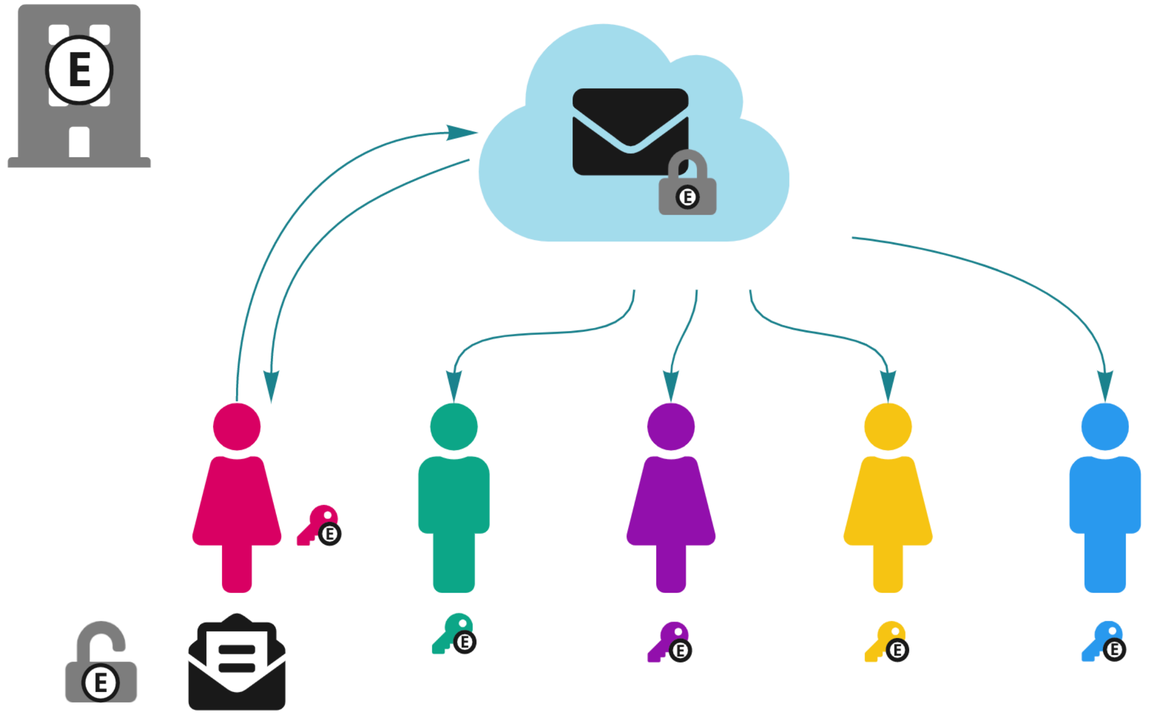


Various Access Policies

- 1 over n (inclusive / exclusive)
- Matching identity, hierarchical position, attributes, threshold…

Broadcast Encryption

1 encryption key <=> Multiple decryption keys



Some Technical Elements

El Gamal Encryption (KEM)

- Public key: $g, y = g^x$
- Secret key: x
- Encryption:
  - $C = y^r$
  - $K = g^r$
- Decryption: $K = C^{\frac{1}{x}} = g^{x \cdot r \cdot \frac{1}{x}} = g^r$

Underlying problem examples

Inverse problem

- Given: g, g^{γ}
- Find: $g^{\frac{1}{\gamma}}$

Underlying problems examples

Hard problem with multiple solutions

- Given: $g, Y = g^{\gamma}$
- Find: (x, A) such that $A = g^{\frac{1}{\gamma + x}}$

Verifiable Property

- Bilinear map: e such that $e(g^x, g^y) = e(g, g)^{x \cdot y}$
- (x, A) verifies: $e(A, Y) \cdot e(g^x, g) = e(g^{\frac{1}{\gamma + x}}, g^{\gamma}) \cdot e(A^x, g) = e(g, g)^{\frac{\gamma}{\gamma + x} + \frac{x}{\gamma + x}}$

$$= e(g, g)$$

Lots of other problems
Lots of Primitives

Some of Our Results

- Cécile Delerablée, Pascal Paillier, David Pointcheval:
  Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys (2007)
- Cécile Delerablée:
  Identity-Based Broadcast Encryption (2007)
- Cécile Delerablée, David Pointcheval:
  Dynamic Threshold Public-Key Encryption (2008)
- Cécile Delerablée, Lénaïck Gouriou, David Pointcheval:
  Key-Policy ABE with Delegation of Rights (2022)

Learn more?

Cécile Delerablée, CEO

cd@leanear.io

Leanear

Trusting the Cloud

Cécile Delerablée (CEO)