Fully Homomorphic Encryption

An overview of techniques and applications

Malika Izabachène

Cosmian, Paris, France

EU Cyber Week , 15/11-17/11

What is Fully Homomorphic Encryption (FHE) ?

Alice

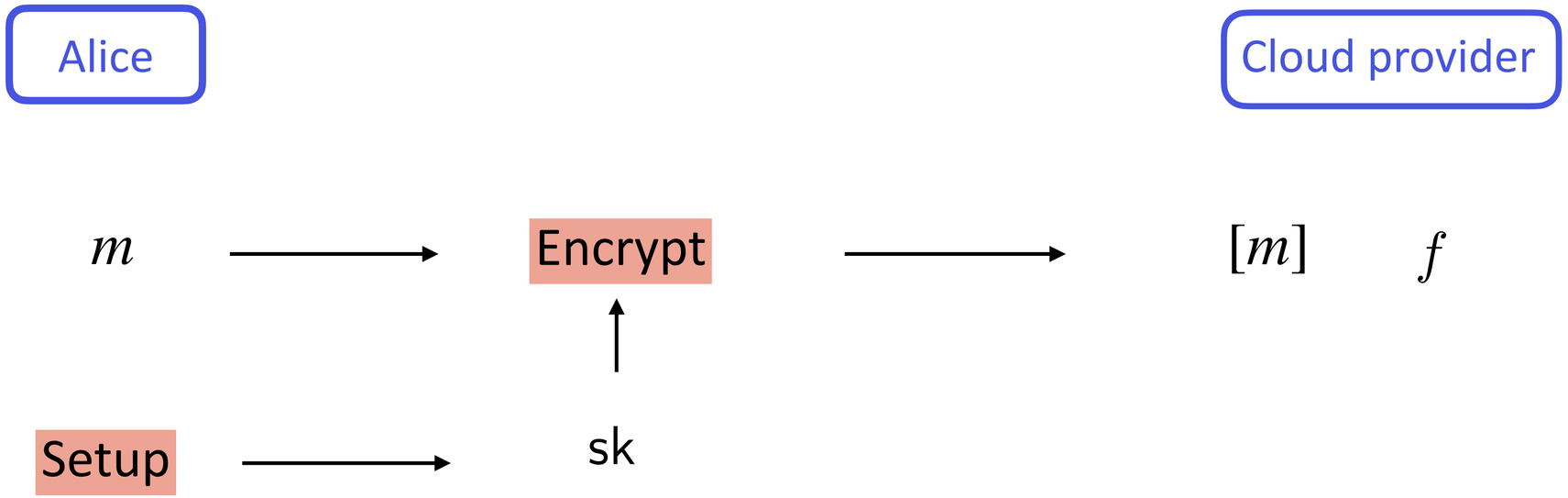
m

Cloud provider

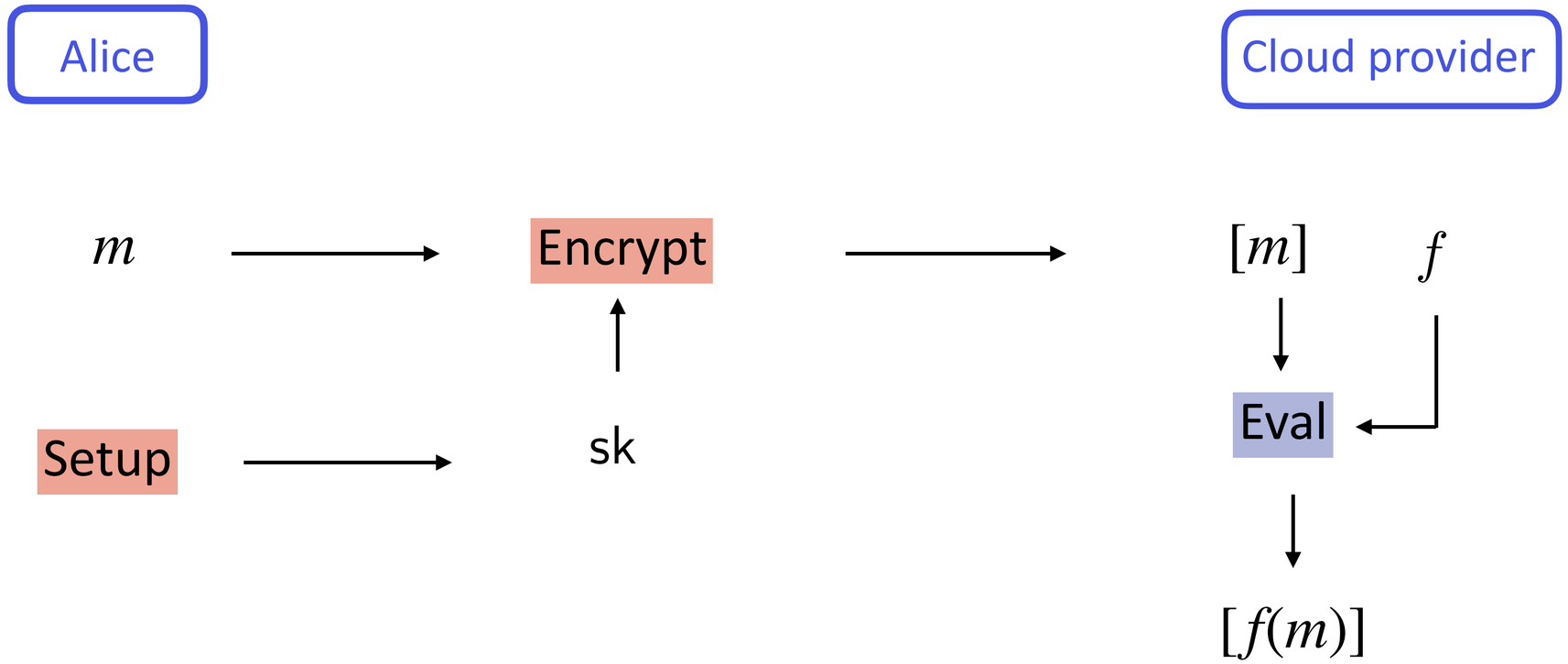
f

What is Fully Homomorphic Encryption (FHE) ?

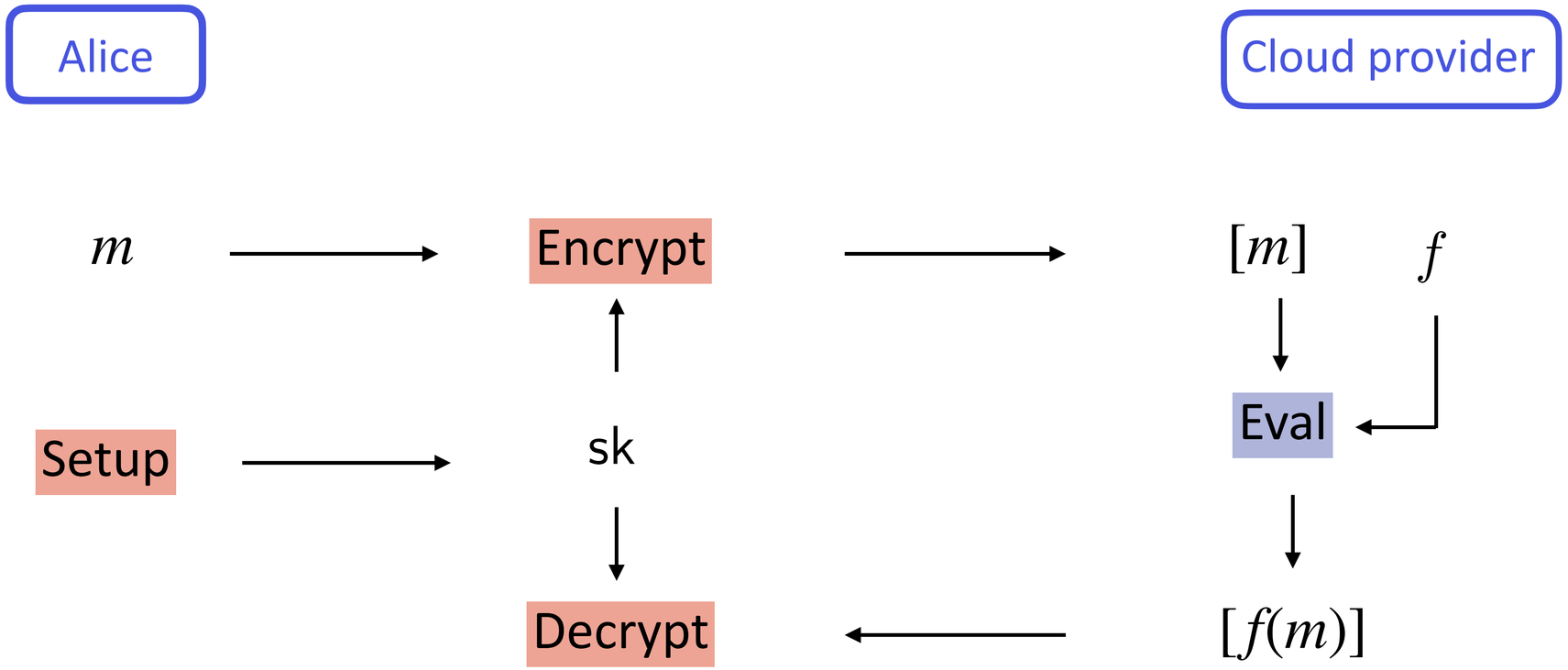
What is Fully Homomorphic Encryption (FHE) ?



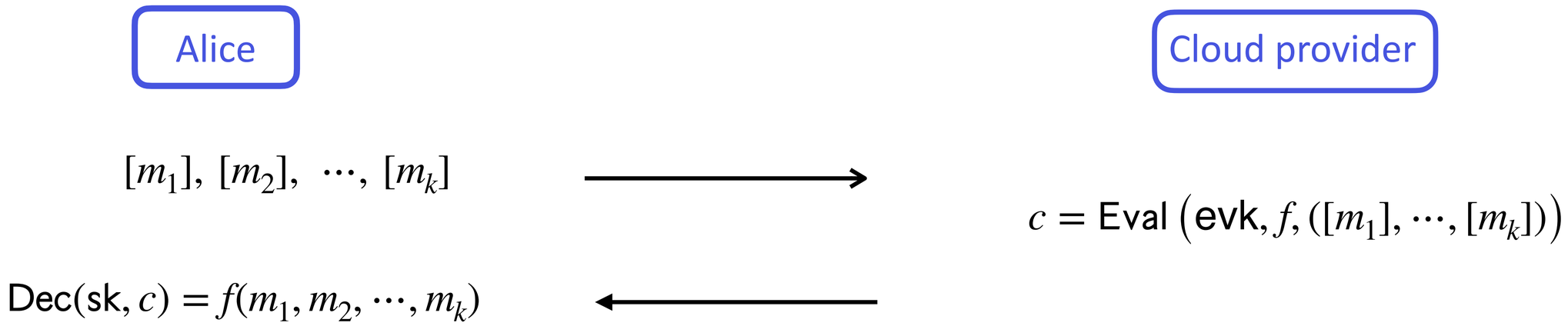
What is Fully Homomorphic Encryption (FHE) ?



What is Fully Homomorphic Encryption (FHE) ?

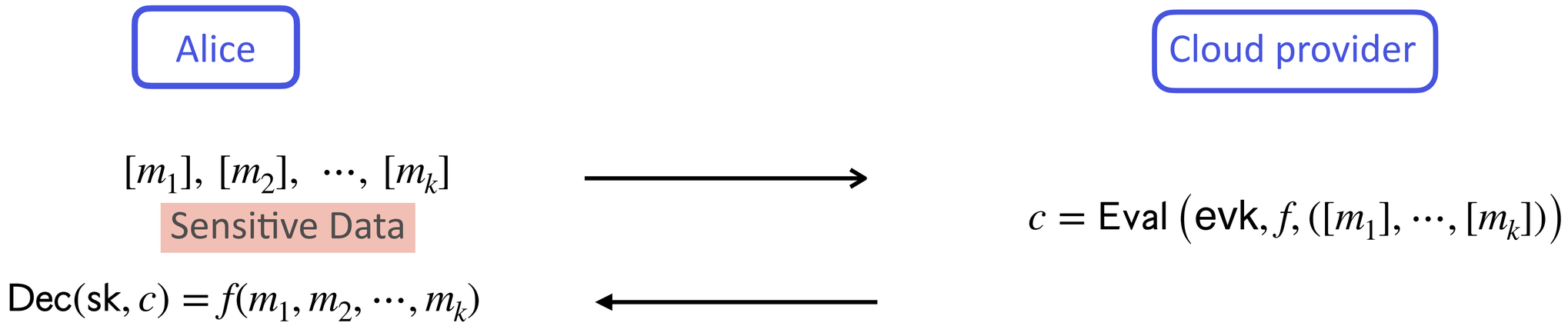


Fully Homomorphic Encryption



Message privacy: Alice's messages are kept unknown to the cloud provider.

Fully Homomorphic Encryption



Message privacy: Alice's messages are kept unknown to the cloud provider.

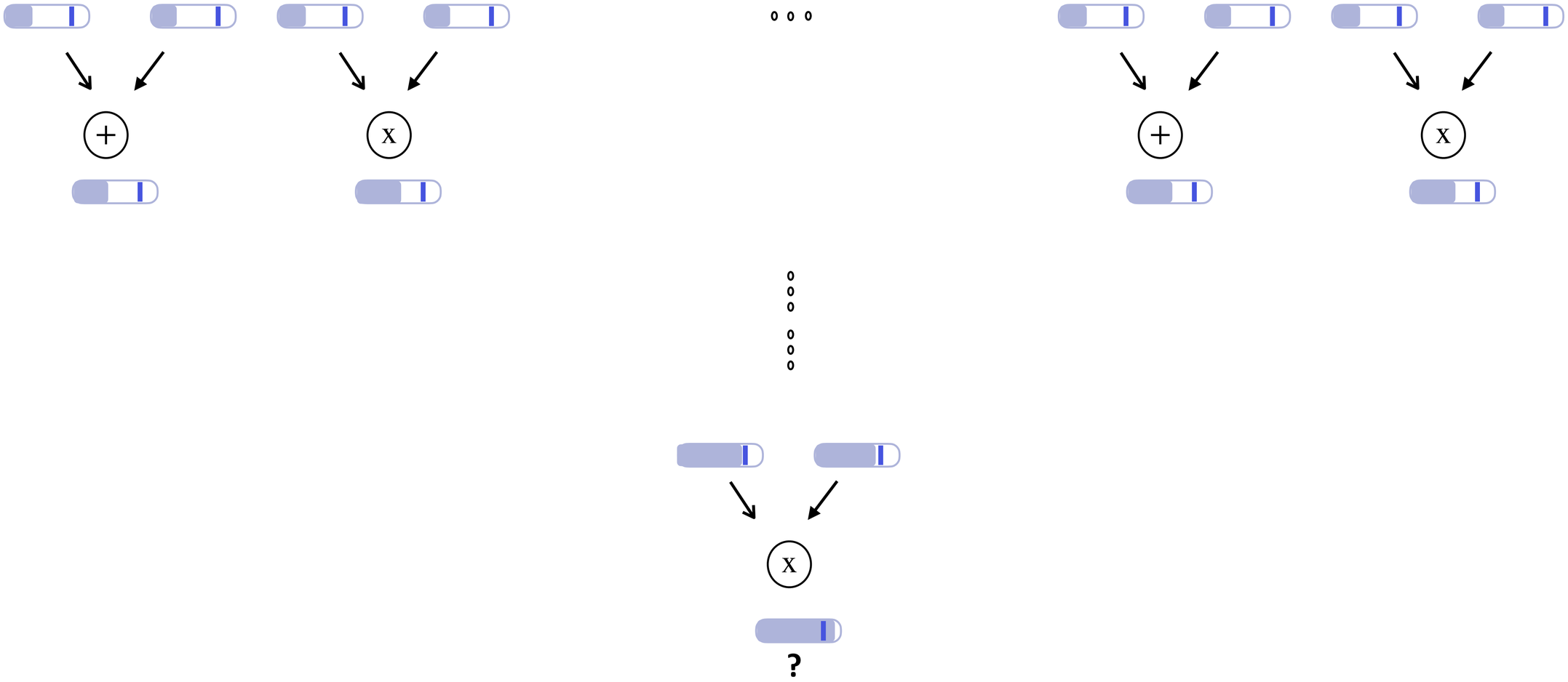
Evoting
Fraud detection
Medical diagnosis
Financial Risk Prevention
Market Analysis, …

Outline

- Definitions
- FHE (noisy) ciphertexts
- Homomorphic Evaluation Paradigms
- Homomorphic Heatmap computation

FHE ciphertexts (noisy ciphertexts)

FHE ciphertexts (noisy ciphertexts)



Noise management

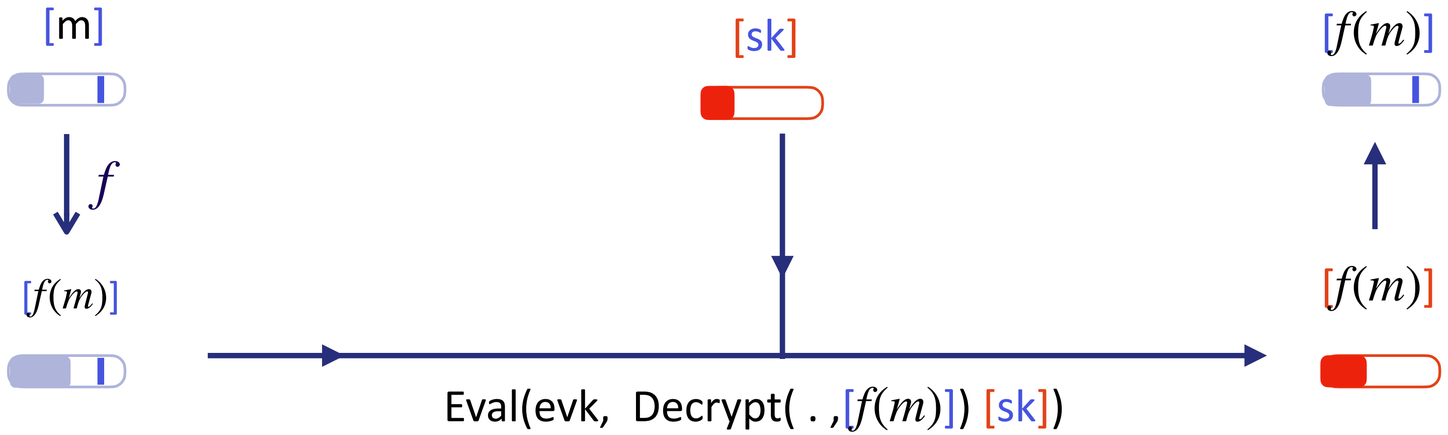
Level Mode

- Circuit depth d known in advance
- Parameters are set relatively to d
- Bounded number of operations

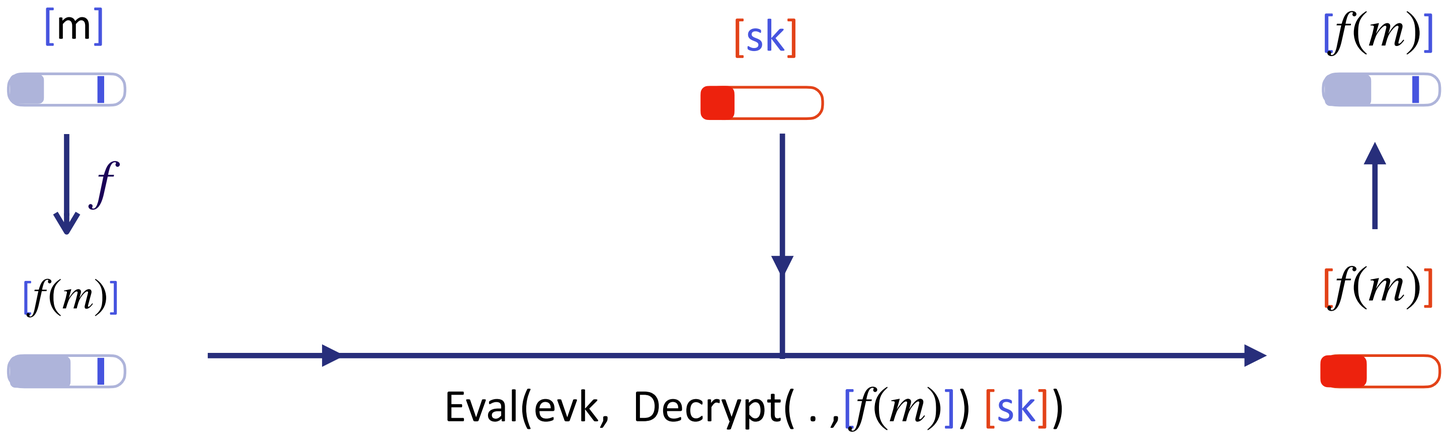
Bootstrapped Mode

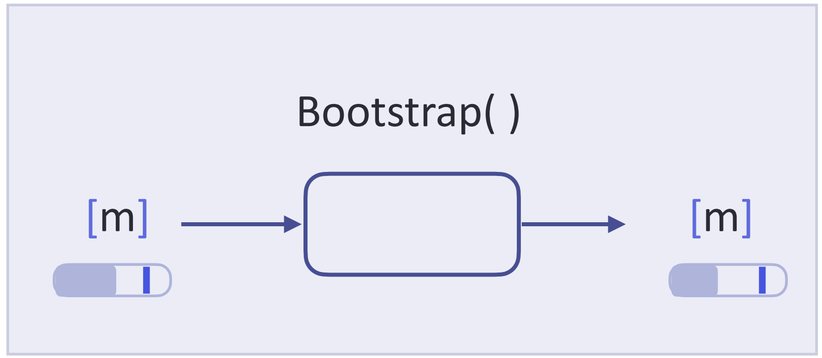
- Depth circuit can be set dynamically
- Unlimited depth
- Flexibility: bootstrap (set of) gate(s) by gate.

Bootstrapping noise growth, [Gentry09]

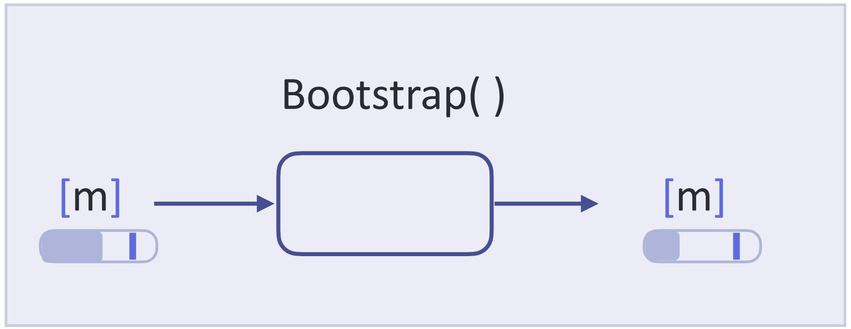


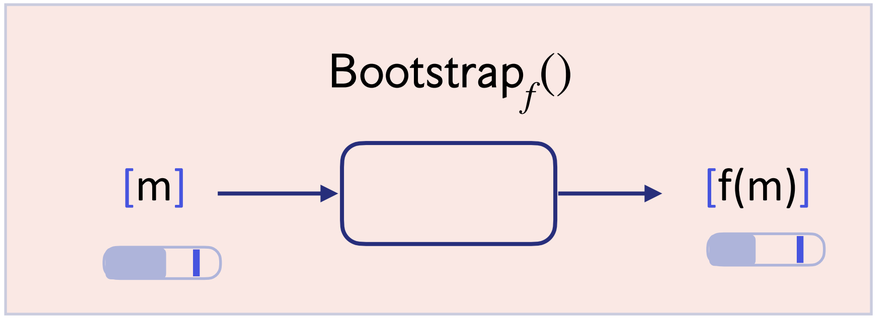
Bootstrapping noise growth, [Gentry09]





Functional Bootstrapping



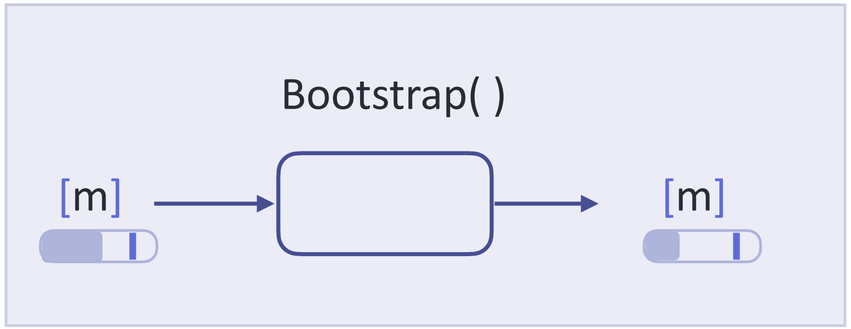


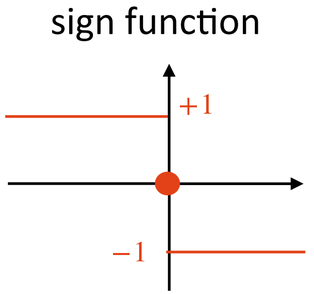
$$f : \{0,\ldots,B\} \mapsto \{0,\ldots,B\},\ \mathrm{dom}(f) \subset \mathscr{M}$$

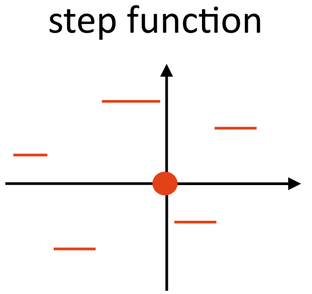
$$m \rightarrow f(m)$$

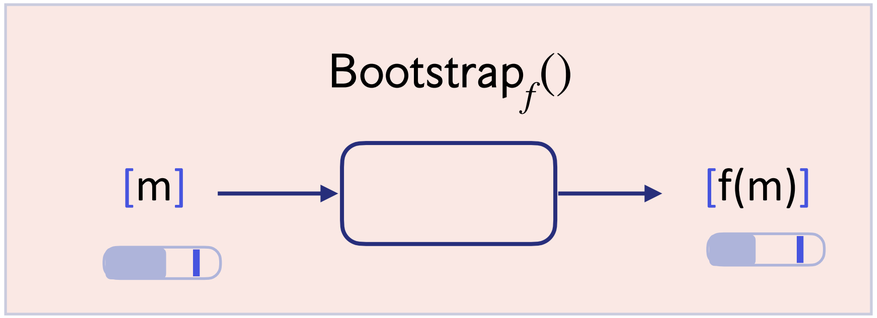
$$\mathrm{coeff}_0(T_f \cdot X^{\mathrm{encode}(m)}) = [f(m)]$$

Functional Bootstrapping









$$f : \{0,\ldots,B\} \mapsto \{0,\ldots,B\},\ \mathrm{dom}(f) \subset \mathscr{M}$$

$$m \rightarrow f(m)$$

$$\mathrm{coeff}_0(T_f \cdot X^{\mathrm{encode}(m)}) = [f(m)]$$

Homomorphic Evaluation Paradigm

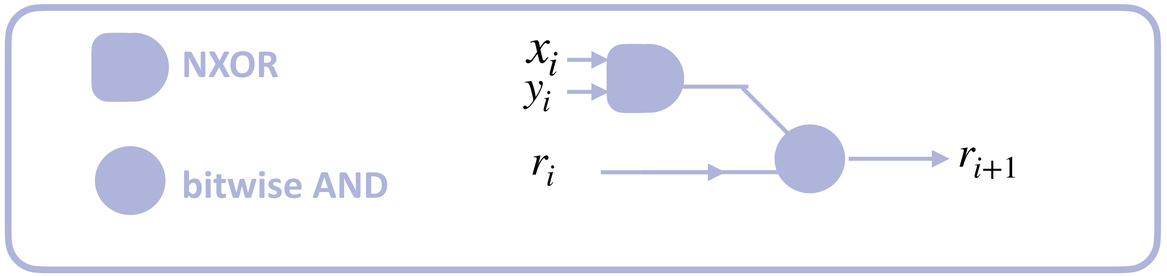
Example: homomorphic equality

Example: homomorphic equality test (1/2)

boolean circuit for equality test

input: $[x]$ and $[y]$, with $x = \sum_{i=0}^{d-1} x_i 2^i$, $y = \sum_{i=0}^{d-1} y_i 2^i$

output: $[1]$ if $x = y$ and $[0]$ if $x \neq y$



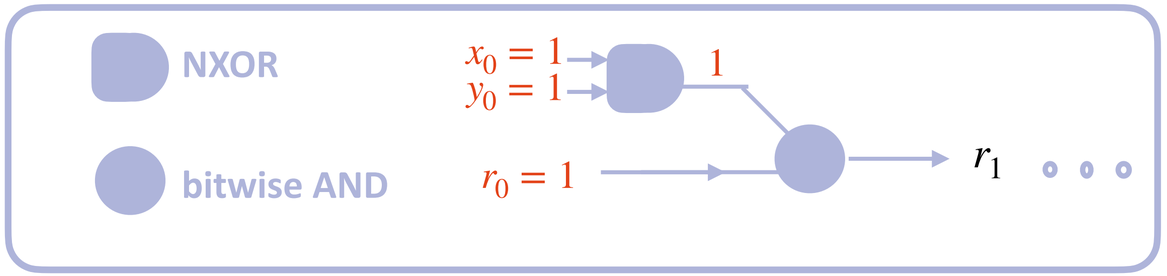
Example: homomorphic equality test (1/2)

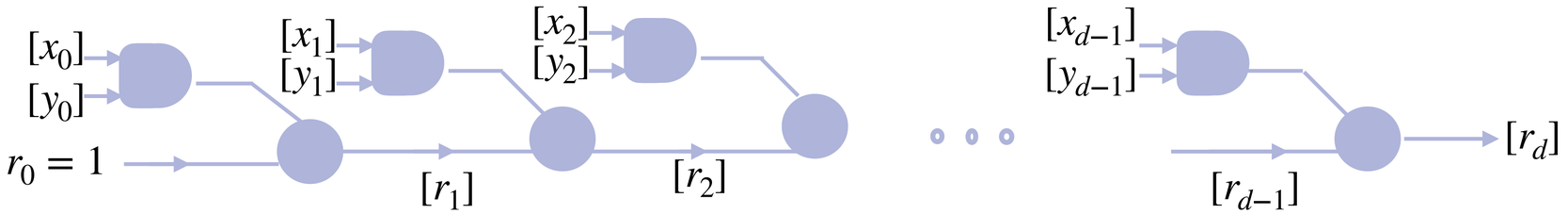
boolean circuit for equality test

input: $[x]$ and $[y]$, with $x = \sum_{i=0}^{d-1} x_i 2^i$, $y = \sum_{i=0}^{d-1} y_i 2^i$

output: $[1]$ if $x = y$ and $[0]$ if $x \neq y$

$x = 110$
$y = 111$
$r_0 = 1$





Example: homomorphic equality test (2/2)

hom. equality test over $\mathbb{F}_p$

input: $[x]$ and $[y]$, $x, y \in \mathbb{F}_p$

output: $[1]$ if $x = y$ and $[0]$ if $x \neq y$

Fermat's Little Theorem, compute , $1 - (x - y)^{p-1}$ over $\mathbb{F}_p$

hom. equality test over $\mathbb{Z}_q$

input: $[x]$ and $[y]$, $x, y \in \{0, \ldots, B\} \subseteq \mathbb{Z}_q$

output: $[1]$ if $x - y = 0$ and $[0]$ if $x - y \neq 0$

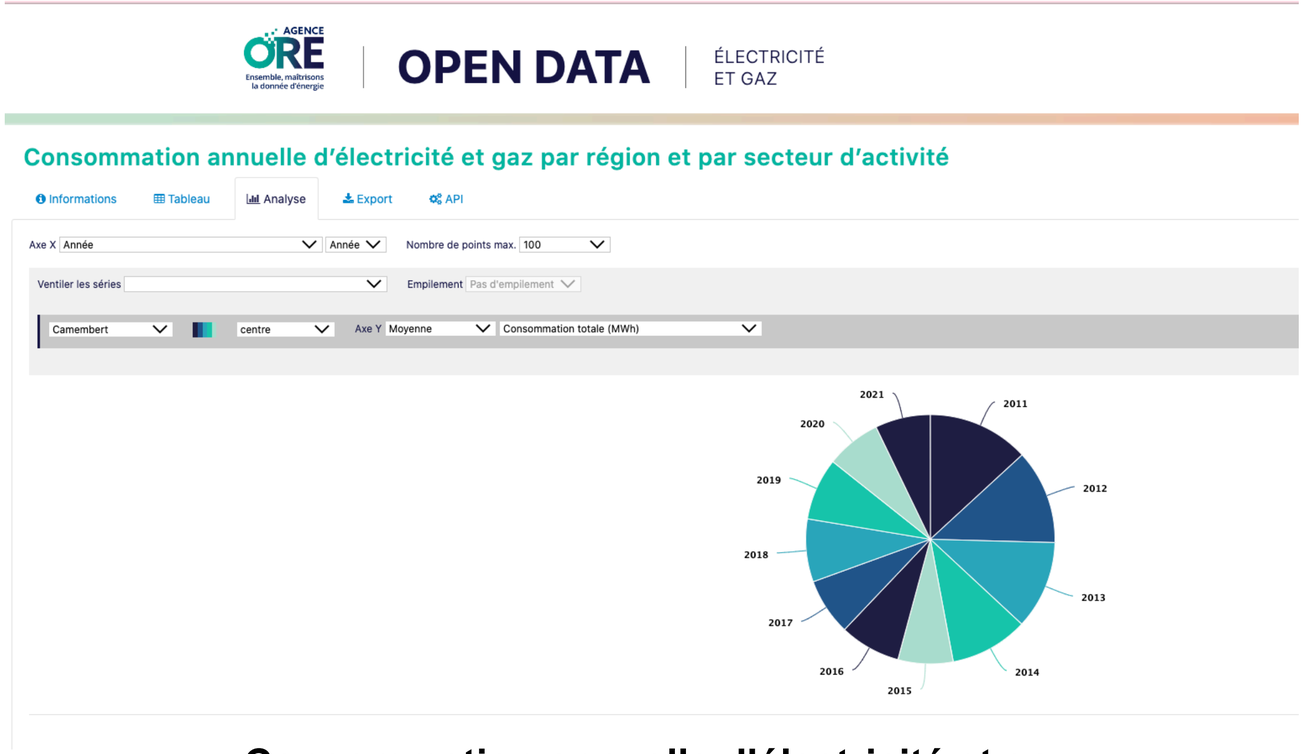
$$f : \{-B, \ldots, B\} \mapsto \{0,1\}$$

$$x - y \rightarrow \begin{matrix} 0 \text{ if } x - y \neq 0 \\ 1 \text{ if } x - y = 0 \end{matrix}$$

Bootstrap$_f()$ with appropriate $T_f(X)$

Homomorphic Heatmap computation

Heatmap: example



Consommation annuelle d'électricité et gaz par région et par secteur d'activité

Agence ORE & Gestionnaires de réseaux électricité et gaz
Data from https://opendata.agenceore.fr/
Dernière modification, 3 novembre 2022

Description of the problem

- Client: ask for a Heatmap function over encrypted coordinates
- Server: a list $[x_i]$, $[y_i]$ (latitude, longitude)

  1. map x_i, y_i to a cell in the grid: $f(x_i, y_i) = \lfloor \frac{x_i}{b} \rfloor + k \lfloor \frac{y_i}{h} \rfloor$

  2. count number of points in each cell

Description of the problem

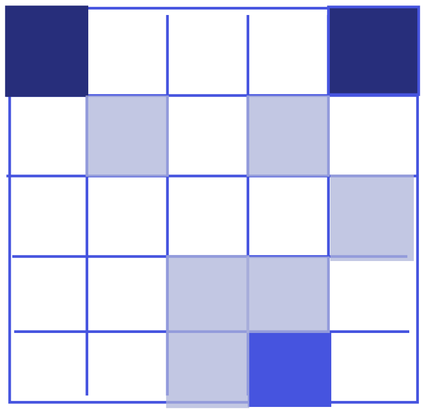
- Client: ask for a Heatmap function over encrypted coordinates

- Server: a list $[x_i]$, $[y_i]$ (latitude, longitude)

  1. map x_i, y_i to a cell in the grid: $f(x_i, y_i) = \lfloor \frac{x_i}{b} \rfloor + k \lfloor \frac{y_i}{h} \rfloor$

  $f(x_i, y_i) : \{[23], [5], [15], [7], [1], [18], [9], [19], [5], [1], [5], [24], [24], [1]\}$

  2. count number of points in each cell



A possible solution: homomorphic comparison

$f(x_i, y_i)$: { [23] , [5], [5], [7], [1], [18], [9], [19], [15], [1], [5], [24], [24], [1]}

$\stackrel{?}{=} 1$

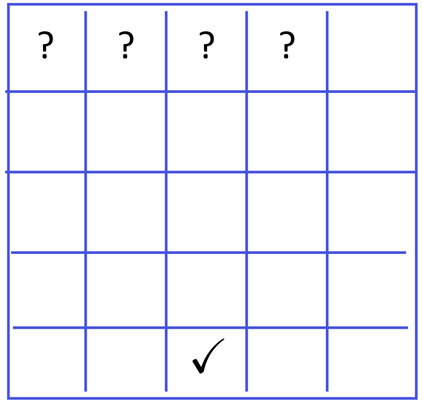
$\stackrel{?}{=} 2$

$\vdots$

$\stackrel{?}{=} 23$

$\stackrel{?}{=} 24$

$\stackrel{?}{=} 25$



1	2	3	4																		23	24	25
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[1]	[0]	[0]

Table of the frequencies

A possible solution: homomorphic comparison

$f(x_i, y_i) : \{[23], [5], [5], [7], [1], [18], [9], [19], [15], [1], [5], [24], [24], [1]\}$

$\stackrel{?}{=} 1$

$\vdots$

$\stackrel{?}{=} 5$

$\vdots$

$\stackrel{?}{=} 24$

$\stackrel{?}{=} 25$

?	?	?	?	✓

1	2	3	4	5																	23	24	25
[0]	[0]	[0]	[0]	[1]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[1]	[0]	[0]

Table of the frequencies

Encoding in the exponent

$$f(x_i, y_i) : \{[23], [5], [5], [7], [18], [9], [19], [15], [1], [5], [24], [24], [1]\}$$

$$X^{f(x_i,y_i)} : \{[X^{23}], [X^5], [X^5], [X^7], [X^{18}], [X^9], [X^{19}], [X^{15}], [X^1], [X^5], [X^{24}], [X^{24}], [X^1]\}$$

Adding the components (the first three ones):

$$[X^{23}] + [X^5] + [X^{23}] \quad \longrightarrow \quad [2X^{23} + X^5]$$

Full domain solution

- Start with $[X^{x_i}]$
- Retrieve all the bits of $[f(x_i)]$: $[f(x_i)_0], \ldots, [f(x_i)_{\ell-1}]$
- Homomorphically compute $[X^{f(x_i)_0 \cdot 2^0}], \ldots, [X^{f(x_i)_{\ell-1} 2^{\ell-1}}]$
- Get $[X^{f(x_i)_0 \cdot 2^0} + \ldots + X^{f(x_i)_{\ell-1} 2^{\ell-1}}] \longrightarrow [X^{f(x_i)}]$

Testvector polynomial

Homomorphic CMux

Homomorphic Mulitplication

Polynomials are modulo $X^N + 1$

$N \geq \max(|\mathbf{dom}(f)|, |\mathbf{img}(f)|)$

Split Domain Method

$N \approx |\mathbf{img}(f)|$

Benchmarks for Heatmap computation

$N \geq \max(|\text{dom}(f)|, |\text{img}(f)|)$

$N = 2^{12}$

$N = x_{\max}$

$x_{\max}$ and $y_{\max}$	b and h	Full domain	Split domain
2^{10}	2^6	0.174 s	0.507 s
2^{11}	2^7	0.174 s	0.507 s
2^{12}	2^8	0.174 s	0.512 s
2^{13}	2^9	0.394 s	0.568 s
2^{14}	2^9	1.0617 s	0.635 s
2^{15}	2^9	2.832 s	0.820 s

Timing to process a point (x_i, y_i) for different heatmap instances.

joint work with Ilia Iliashienko, Alex Mertens and Hilder V. L. Pereira
https://github.com/KULeuven-COSIC/Homomorphic-Heatmap

Conclusion

- Powerful paradigms to compute over encrypted data;
- Combined approaches (Levelled and/or Bootstrapped modes);
- Reasonable performance in many scenarios …
- .. and very efficient tailor-made solution in some cases;
- Scaling with large datasets remains challenging;
- Good representational choice can make a huge difference.

Thank you

malika.izabachene@cosmian.com