



Smart and Blind : Secure AI on Encrypted Data

Sofiane Azogagh

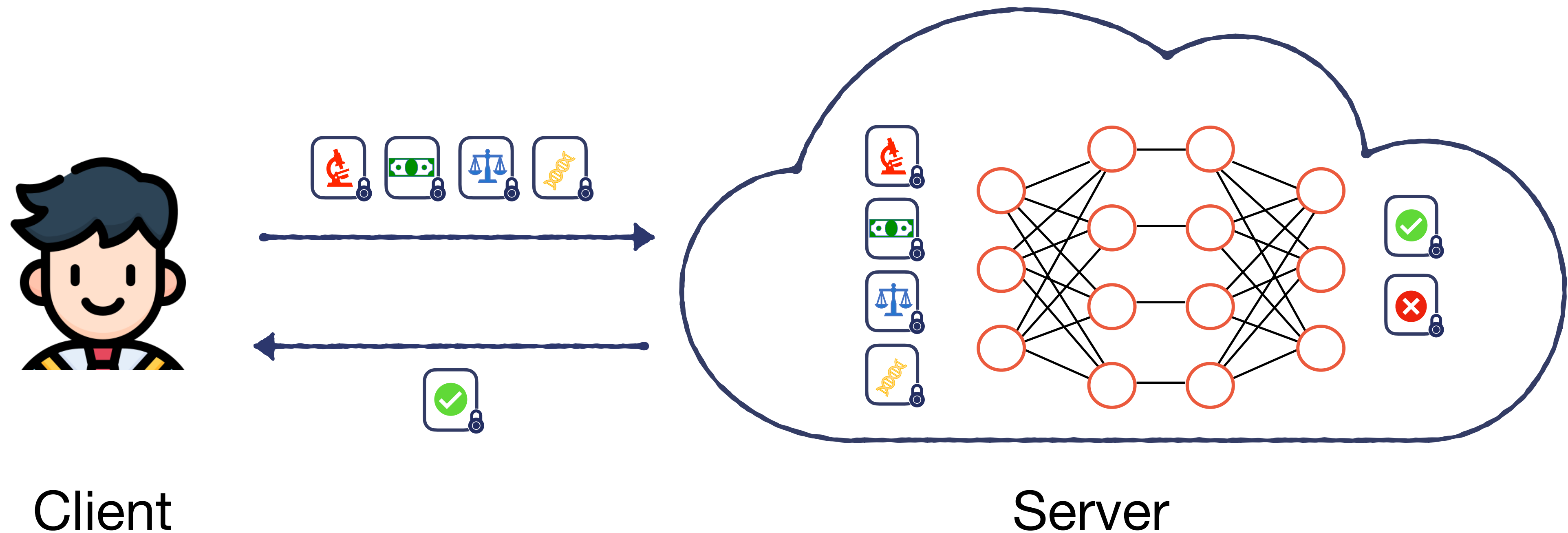
Supervised by Marc-Olivier Killijian and Sébastien Gambs

Responsible AI day - August 5th 2025

Imagine a world where...



Homomorphic encryption



Why it's hard ?

Addition

$$\boxed{x} + \boxed{y} = \boxed{x + y}$$

Multiplication

$$\boxed{x} \times \boxed{y} = \boxed{x \times y}$$

Function evaluation

$$f(\boxed{x}) = \boxed{f(x)}$$

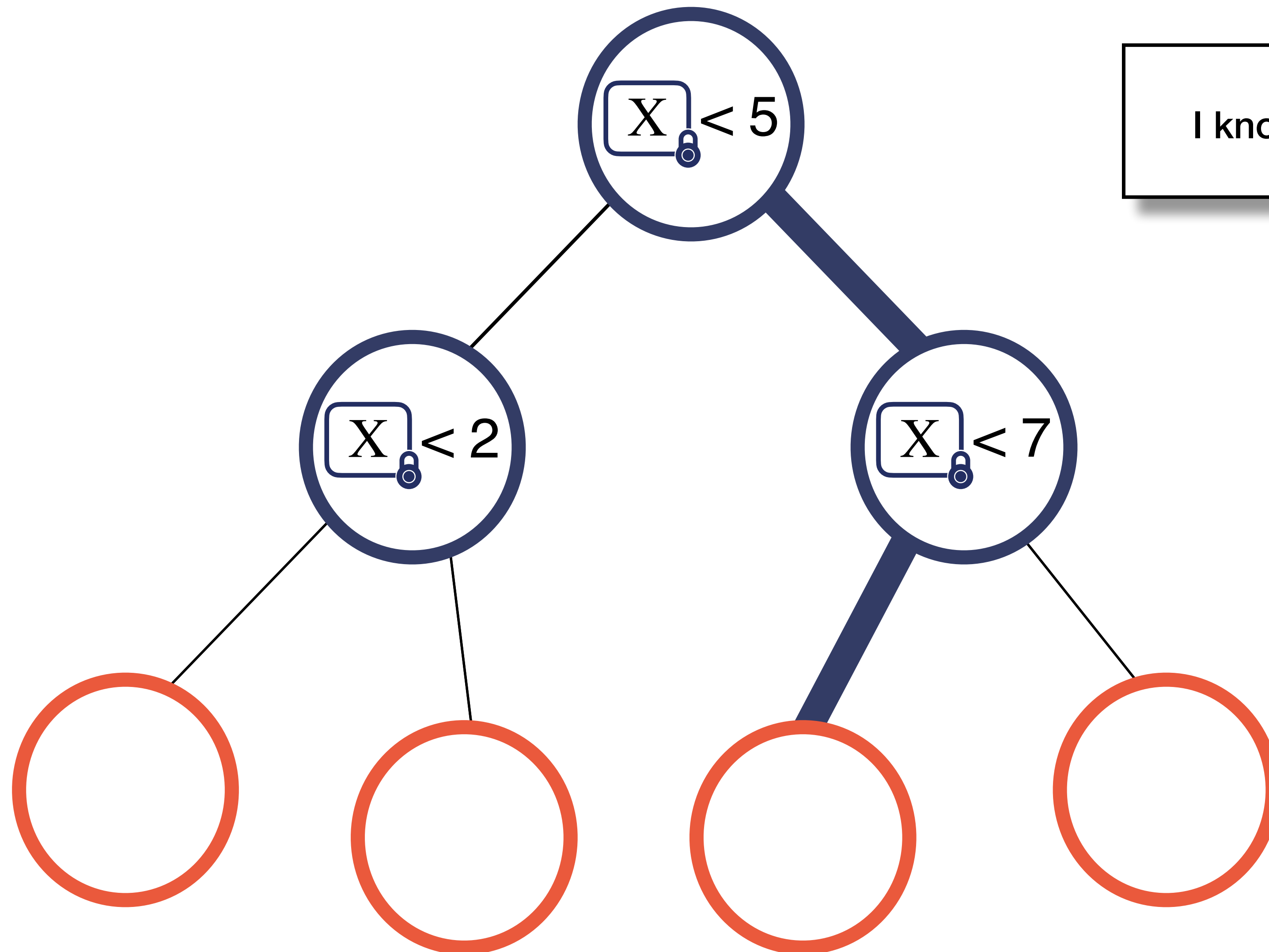
$f(0) \ f(1) \ f(2) \ \dots\dots\dots f(p-1)$

LUT : Look-Up-Table

Arithmetic operations

Non arithmetic operations

Why it's hard ?



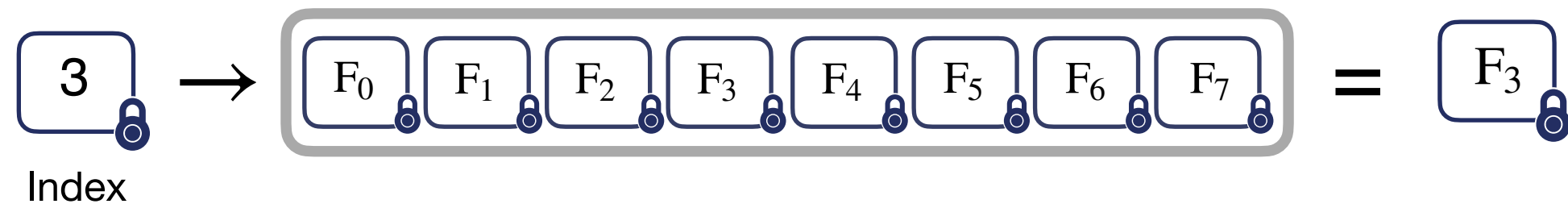
I know that $X = 6$



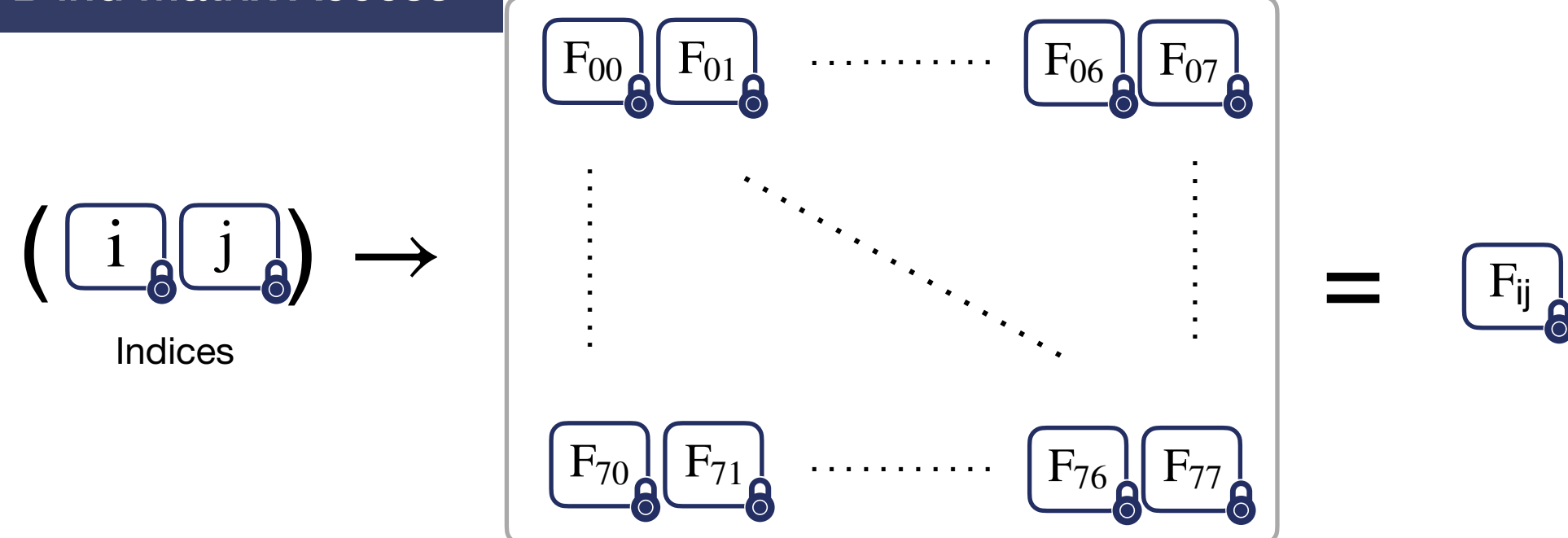
RevoLUT



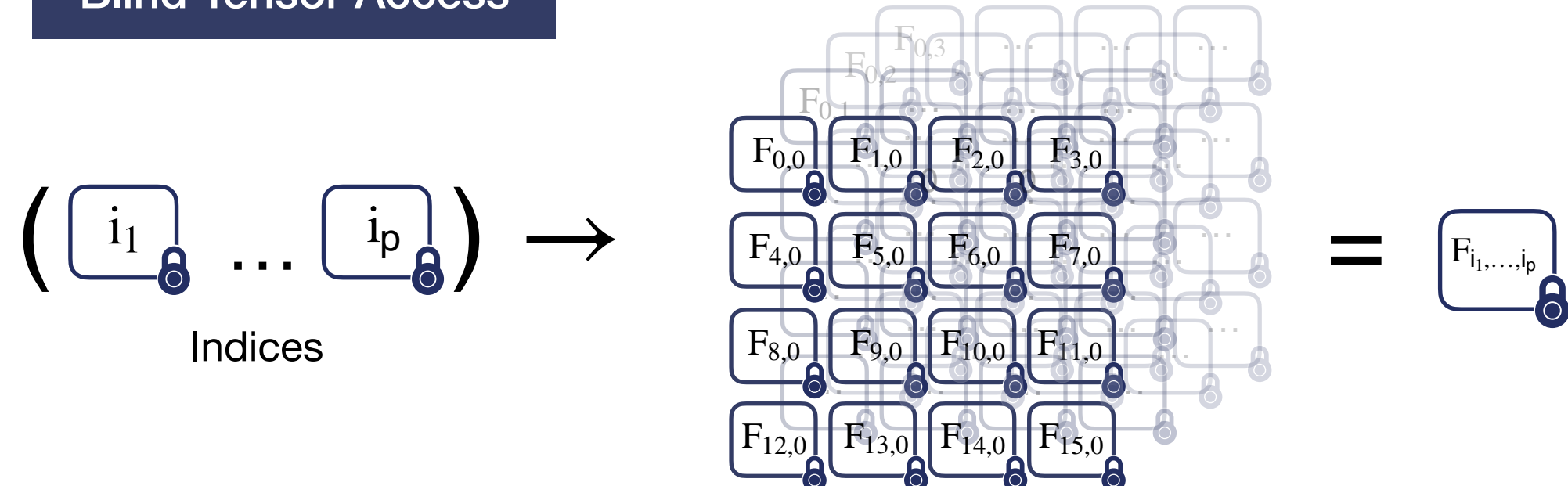
Blind Array Access



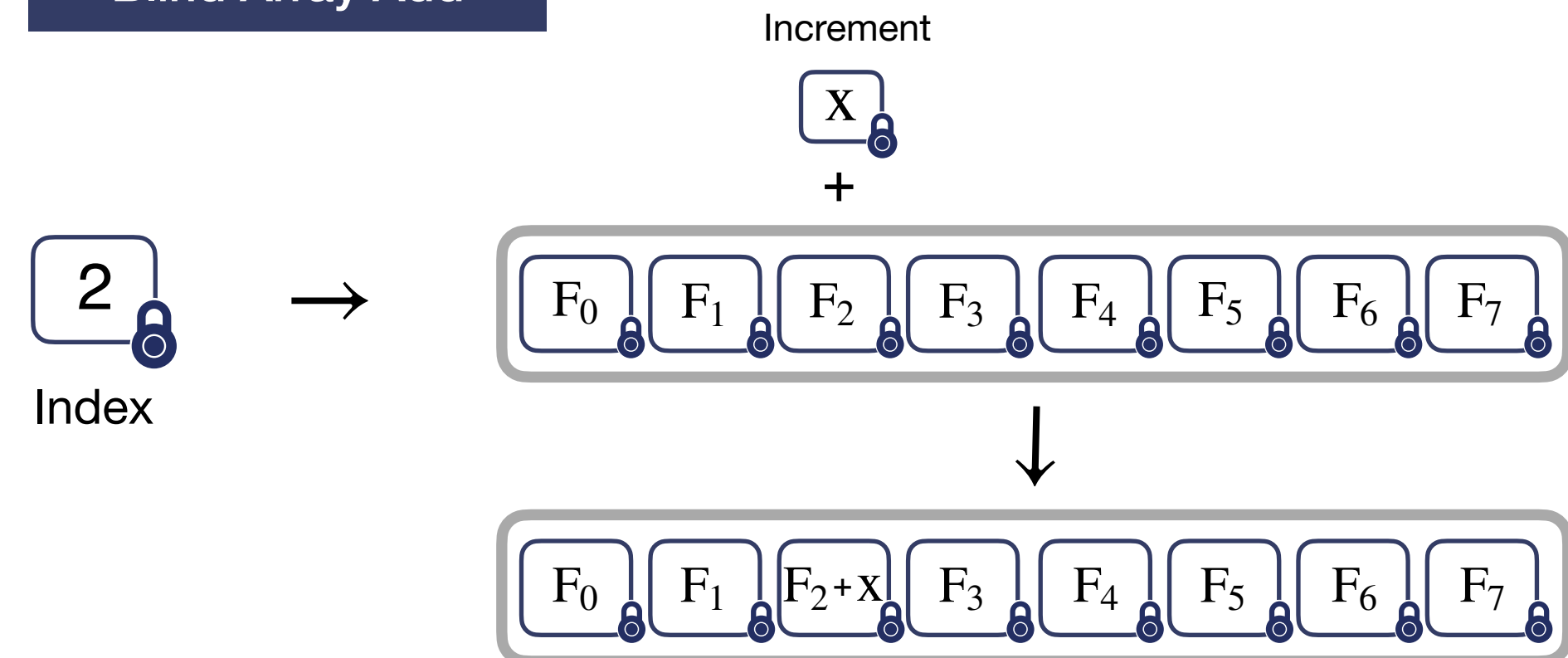
Blind Matrix Access



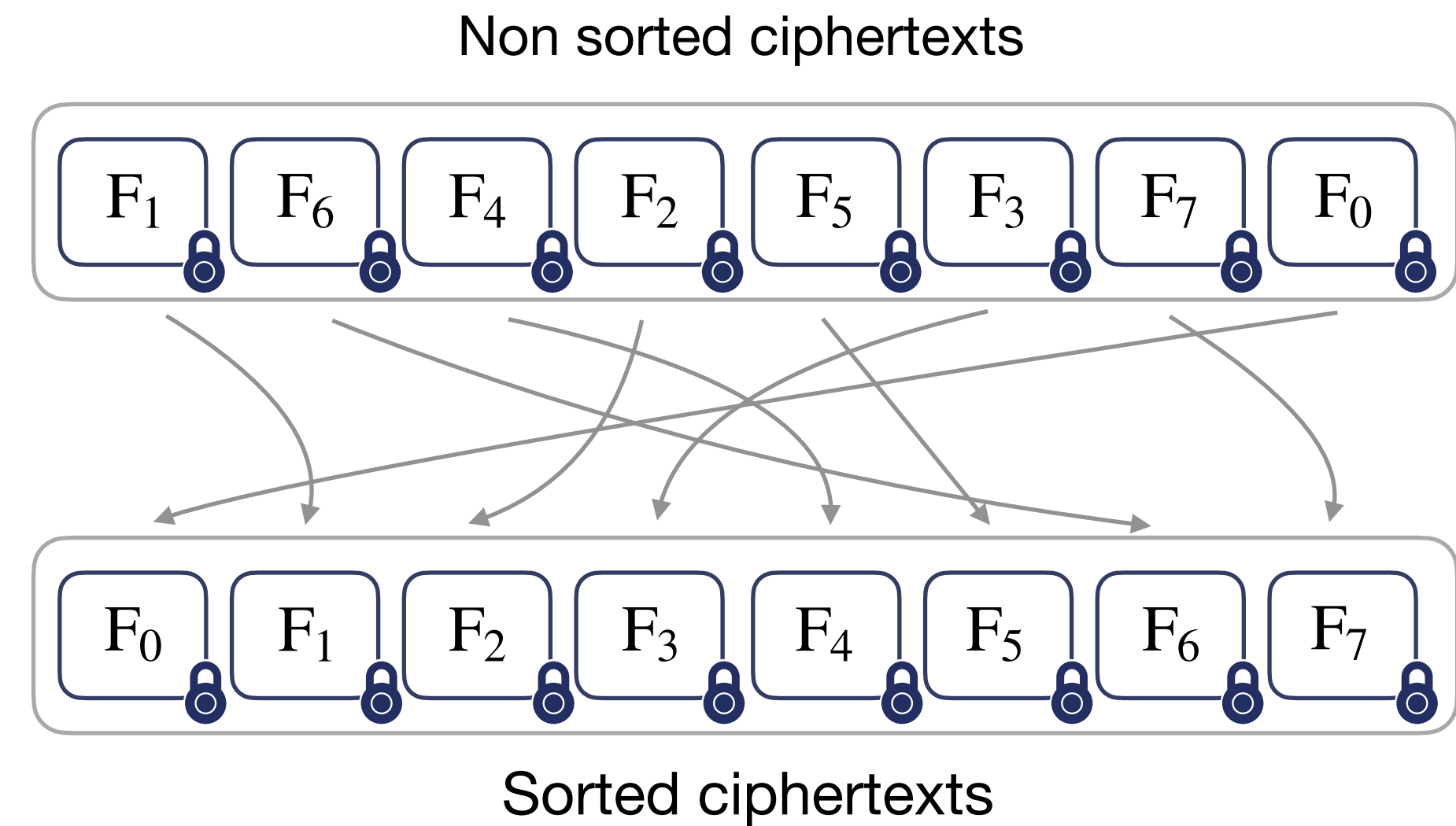
Blind Tensor Access



Blind Array Add



Blind Sort



Is it a Training or an Unlearning ?

Oblivious (Un)Learning of Extremely Randomized Trees

Sofiane Azogagh

azogagh.sofiane@courrier.uqam.ca

Univ Québec à Montréal

Montréal, Canada

Sébastien Gambs

gambs.sebastien@courrier.uqam.ca

Univ Québec à Montréal

Montréal, Canada

Zelma Aubin Birba

birba.zelma_aubin@courrier.uqam.ca

Univ Québec à Montréal

Montréal, Canada

Marc-Olivier Killijian

killijian.marc-olivier.2@uqam.ca

Univ Québec à Montréal

Montréal, Canada

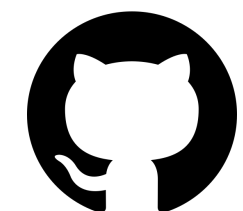
Thank you !



azogagh.sofiane@courrier.uqam.ca



sofianeazogagh.github.io



[sofianeazogagh/revoLUT](https://github.com/sofianeazogagh/revoLUT)



ia.cr/2024/1935