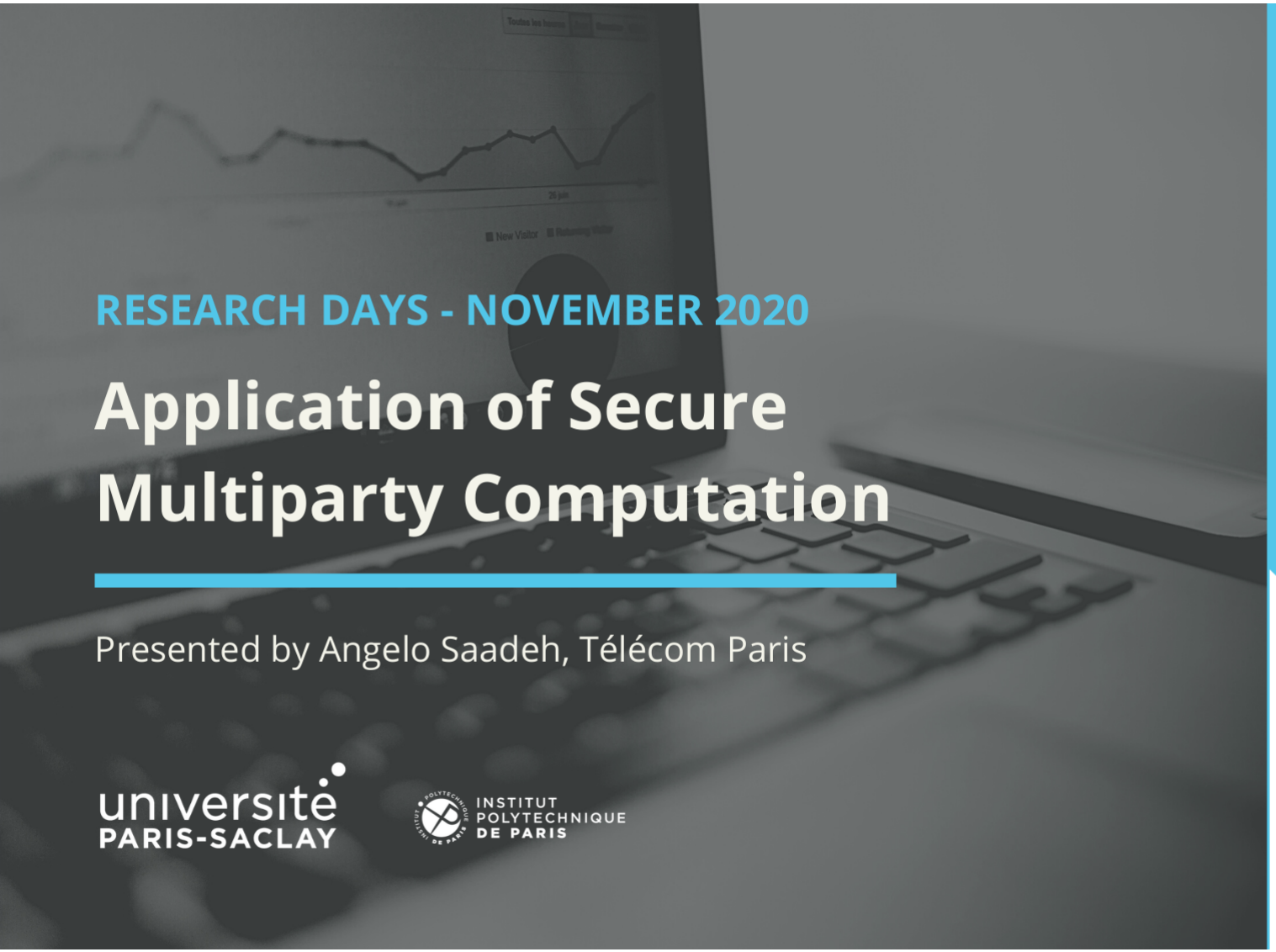


RESEARCH DAYS - NOVEMBER 2020

Application of Secure Multiparty Computation

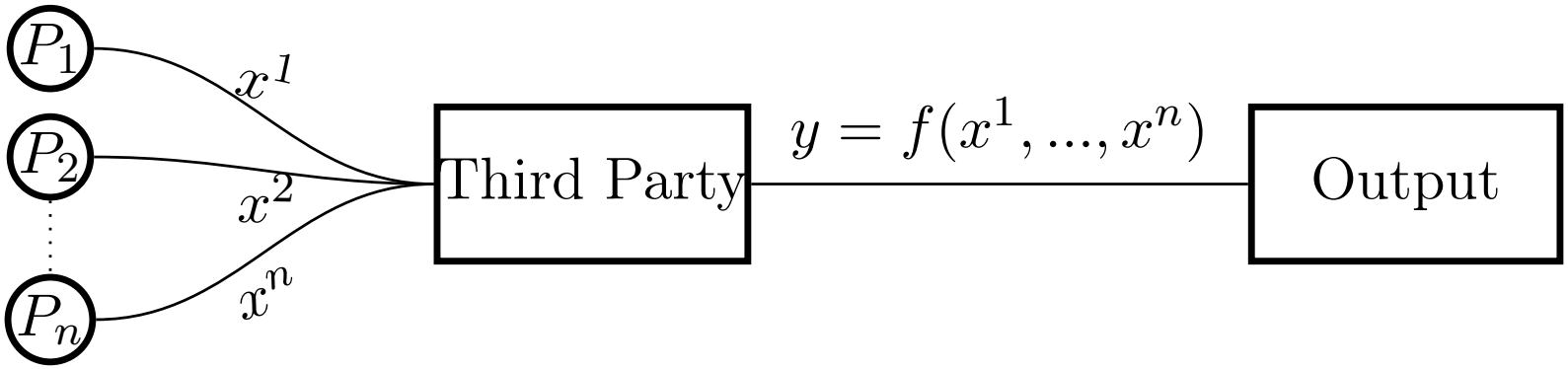
Presented by Angelo Saadeh, Télécom Paris

université PARIS-SACLAY

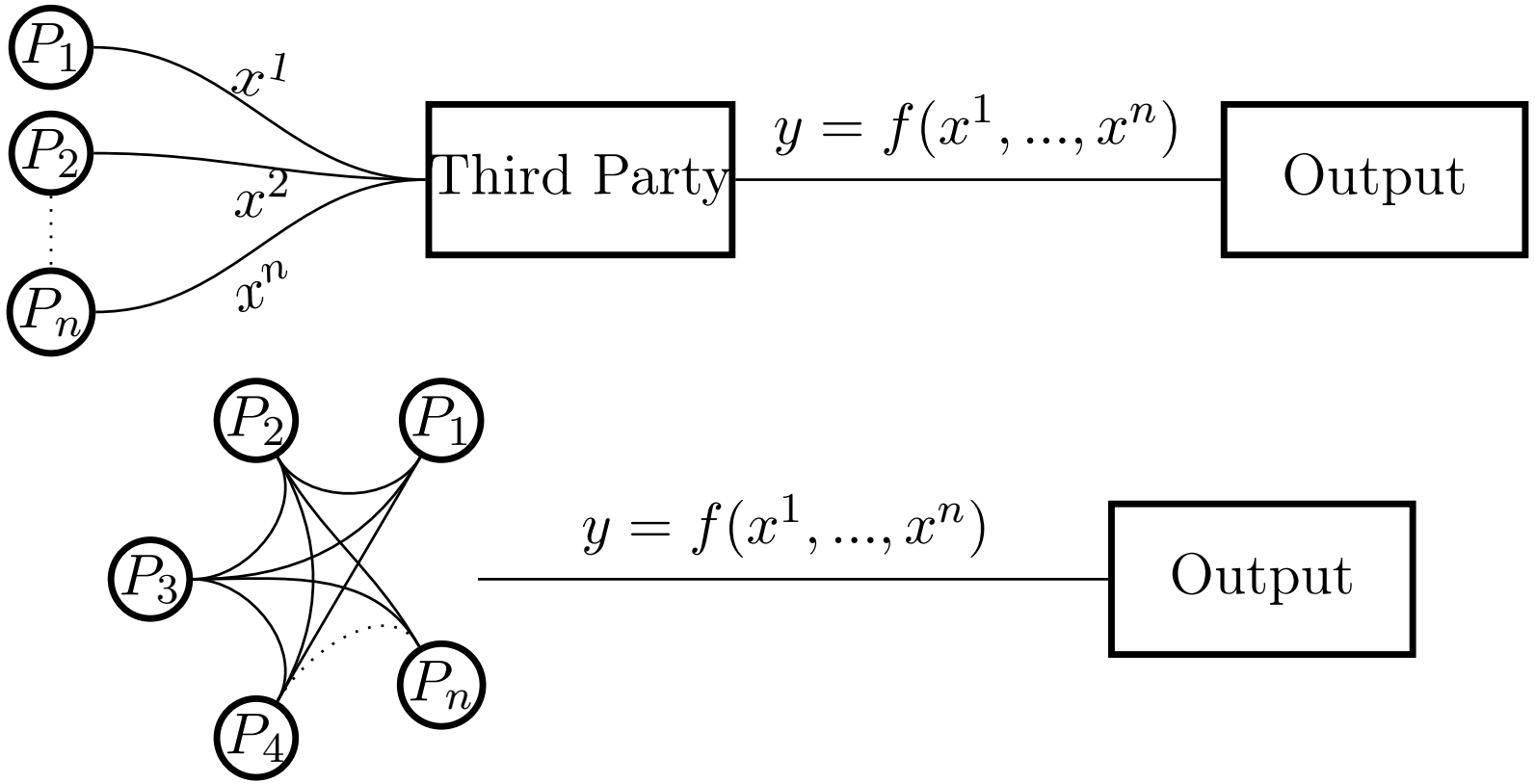
INSTITUT POLYTECHNIQUE DE PARIS

Labex DigiCosme université PARIS-SACLAY

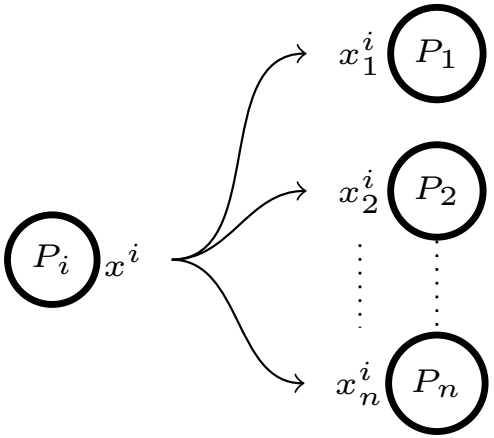
What is Secure Multiparty Computation ?



What is Secure Multiparty Computation ?



Secret Sharing



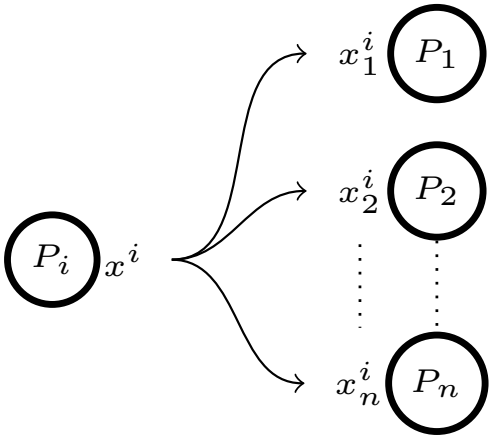
Additive Secret Sharing :

$$\sum_{j=1}^{n} x_j^i = x^i$$

MPC Protocols

			P_1	P_2	P_3	
$x^1 = 1000$	P_1	$\rightarrow$	$x_1^1 = 500$	$x_2^1 = 500$	$x_3^1 = 0$	
$x^2 = 1500$	P_2	$\rightarrow$	$x_1^2 = 1500$	$x_2^2 = 500$	$x_3^2 = -500$	
$x^3 = 750$	P_3	$\rightarrow$	$x_1^3 = 250$	$x_2^3 = 250$	$x_3^3 = 250$	
			2250	1250	-250	3250

Secret Sharing



Additive Secret Sharing :

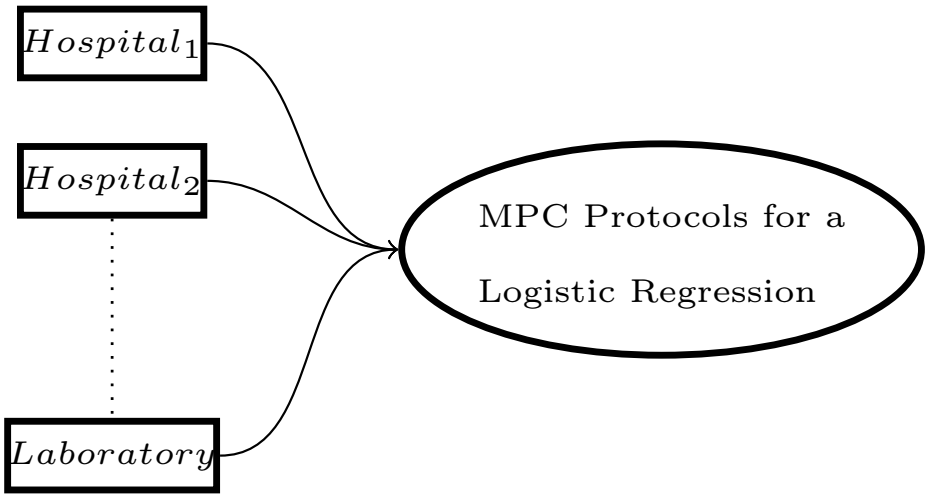
$$\sum_{j=1}^{n} x_j^i = x^i$$

MPC Protocols

			P_1	P_2	P_3	
$x^1 = 1000$	P_1	$\rightarrow$	$x_1^1 = 500$	$x_2^1 = 500$	$x_3^1 = 0$	
$x^2 = 1500$	P_2	$\rightarrow$	$x_1^2 = 1500$	$x_2^2 = 500$	$x_3^2 = -500$	
$x^3 = 750$	P_3	$\rightarrow$	$x_1^3 = 250$	$x_2^3 = 250$	$x_3^3 = 250$	
			2250	1250	-250	3250

How can it be Used ?

In Machine Learning



Step 1 : Secret-share client's private data

Step 2 : Evaluate the protocols

Research

Create MPC-protocols that are
- Efficient
- Secure

to compute functions used in machine learning

Applications of Secure Multiparty Computation

Angelo Saadeh

Télécom Paris

Supervised by

Daniel Augot - Inria Saclay
Matthieu Rambaud - Télécom Paris

November 2020