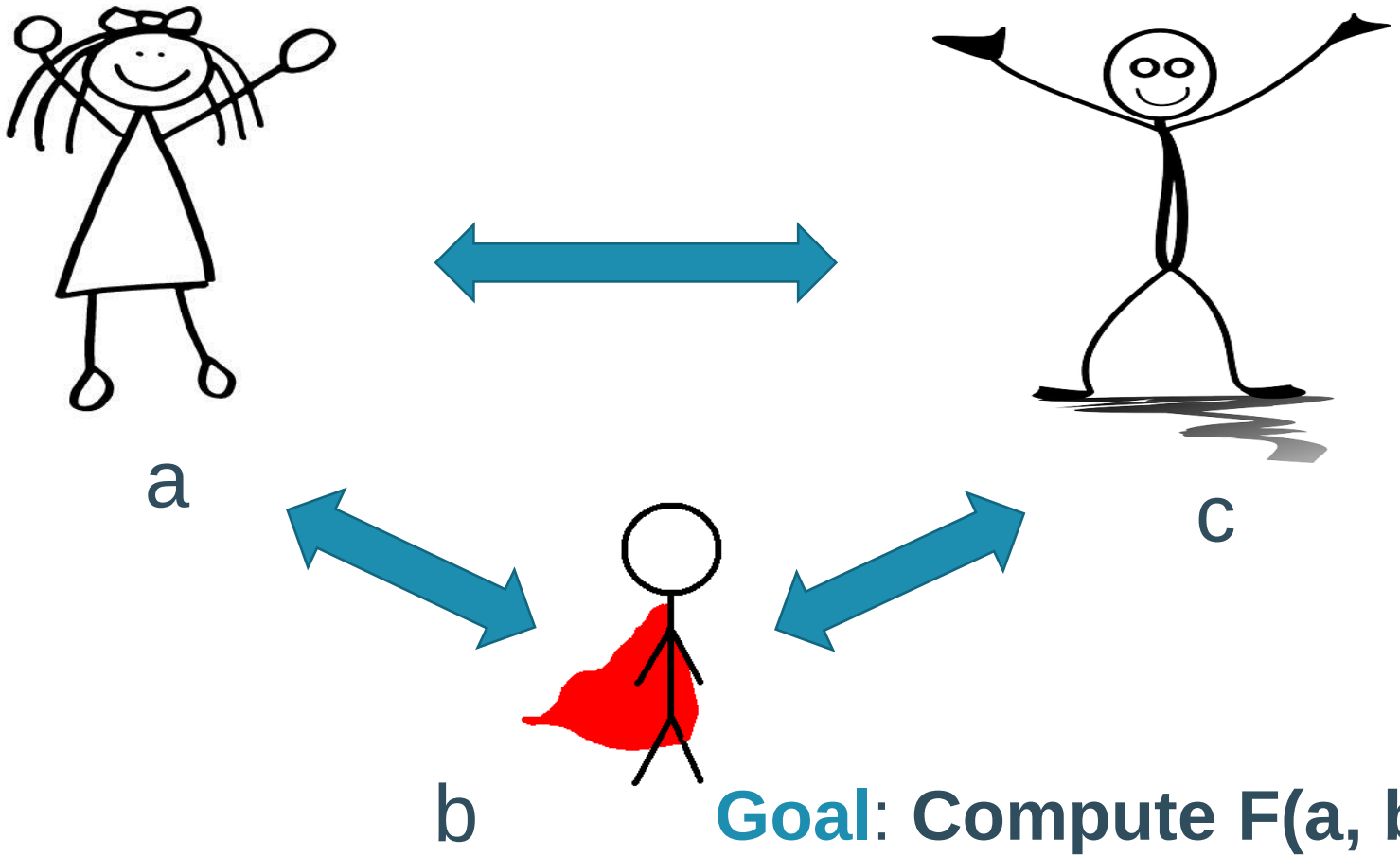
FSE 2018

Modes of operations for computing on encrypted data

Dragos Rotaru, N.P. Smart, and Martijn Stam

KU Leuven, University of Bristol

Multiparty computation hijacks FSE'18



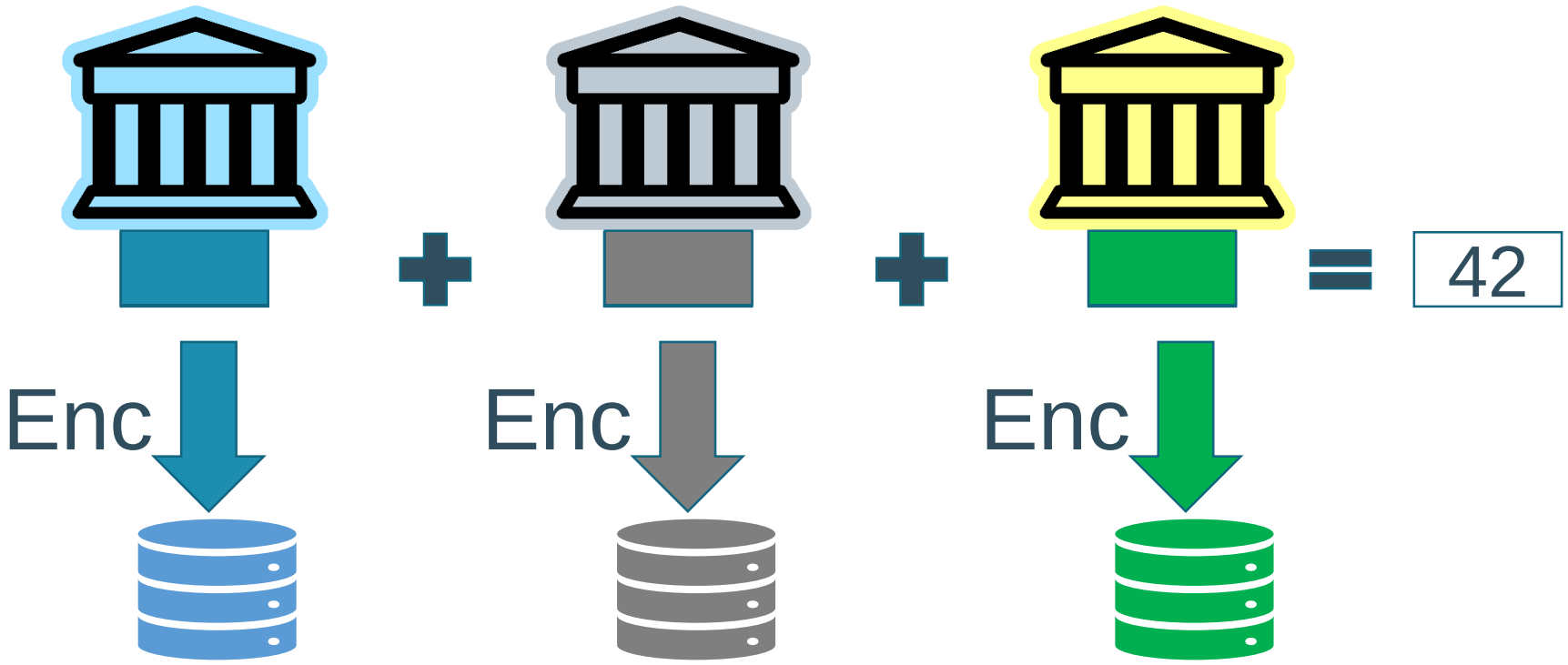
Goal: **Compute F(a, b, c)**

What is the problem?

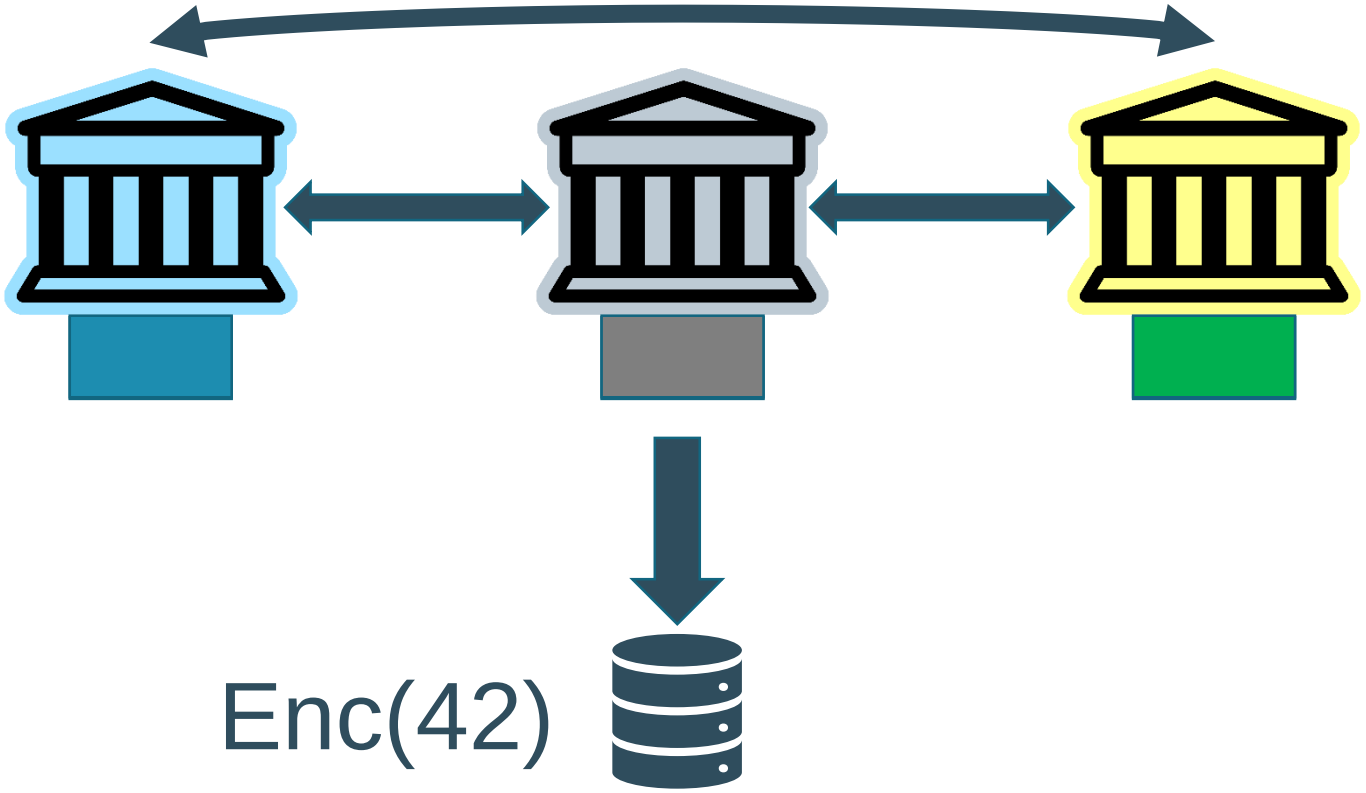
What is the problem?

Dragos Rotaru, N.P. Smart, M. Stam imec-Cosic, Dept. Electrical Engineering KU LEUVEN

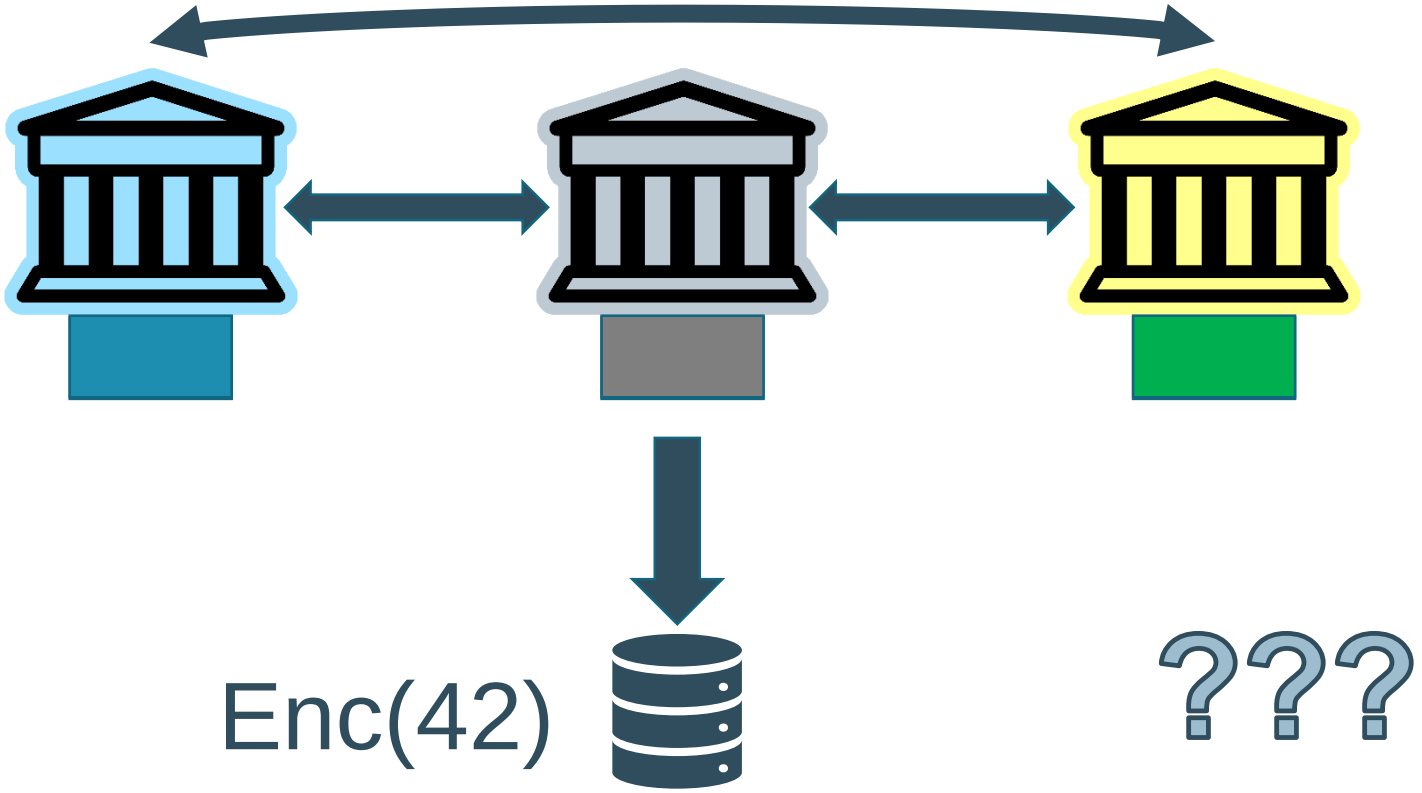
What is the problem?



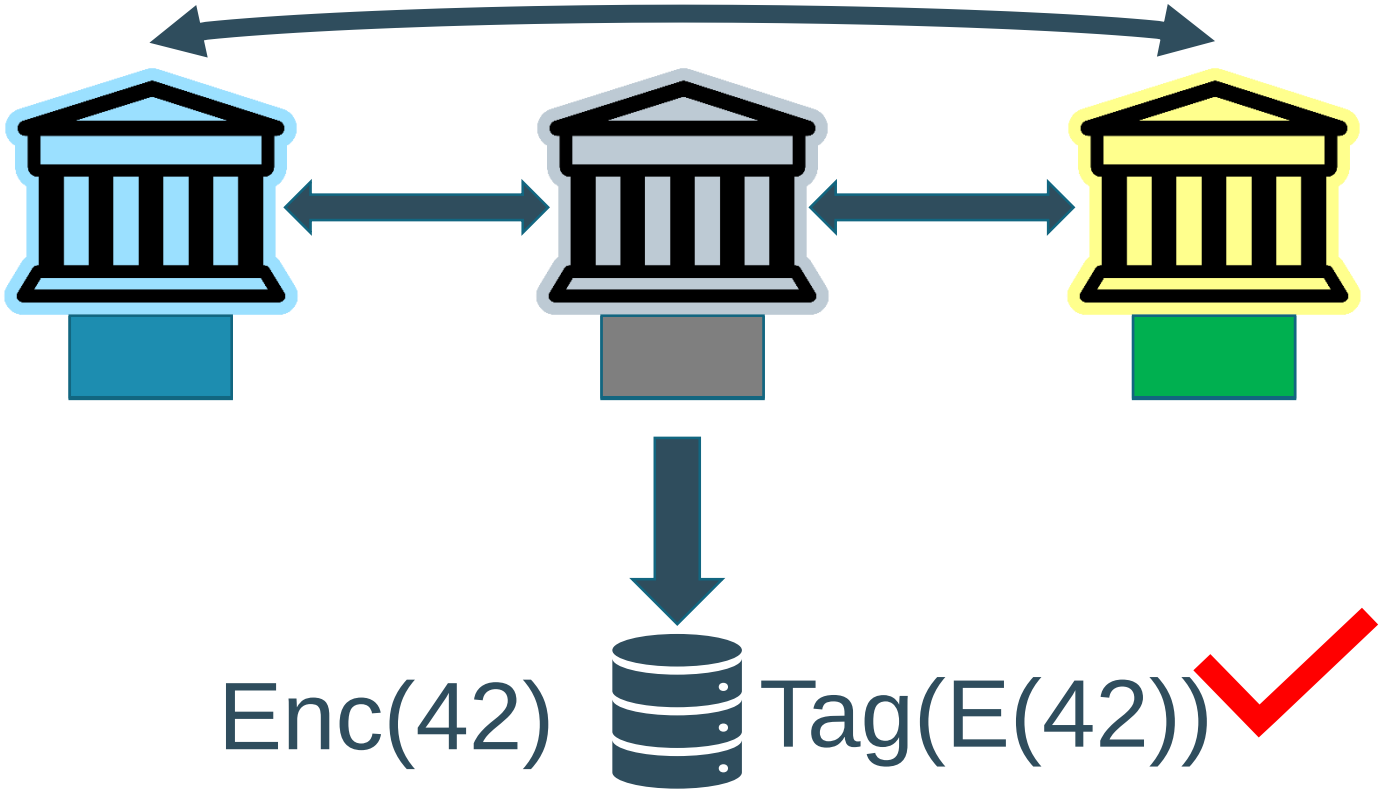
What is the problem?



What is the problem?



What is the problem?



What is the problem?

For free: detect malicious encryption keys.

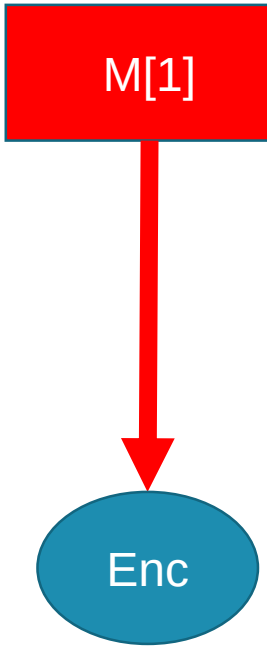
Prior work – PRFs in MPC (CCS'16)

Enc(42)  Tag(Enc(42))

- MiMC
- Legendre PRF

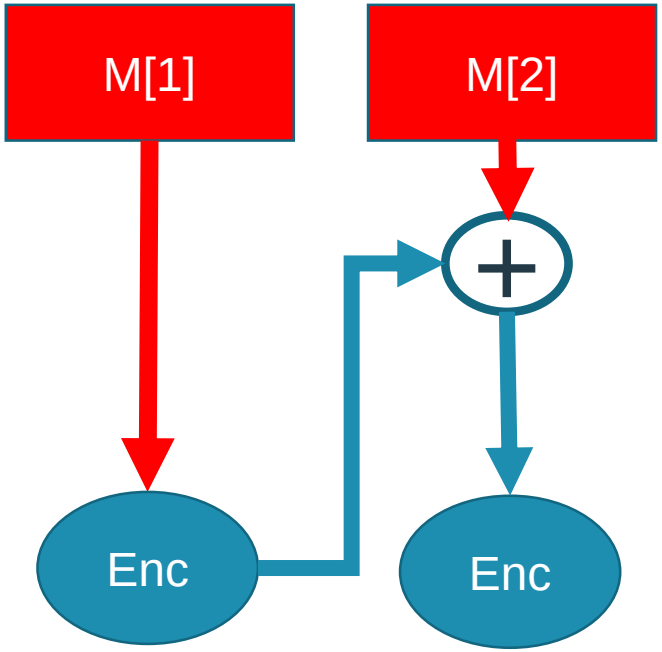
Prior work – PRFs in MPC (CCS'16)

Enc(42)  Tag(Enc(42))



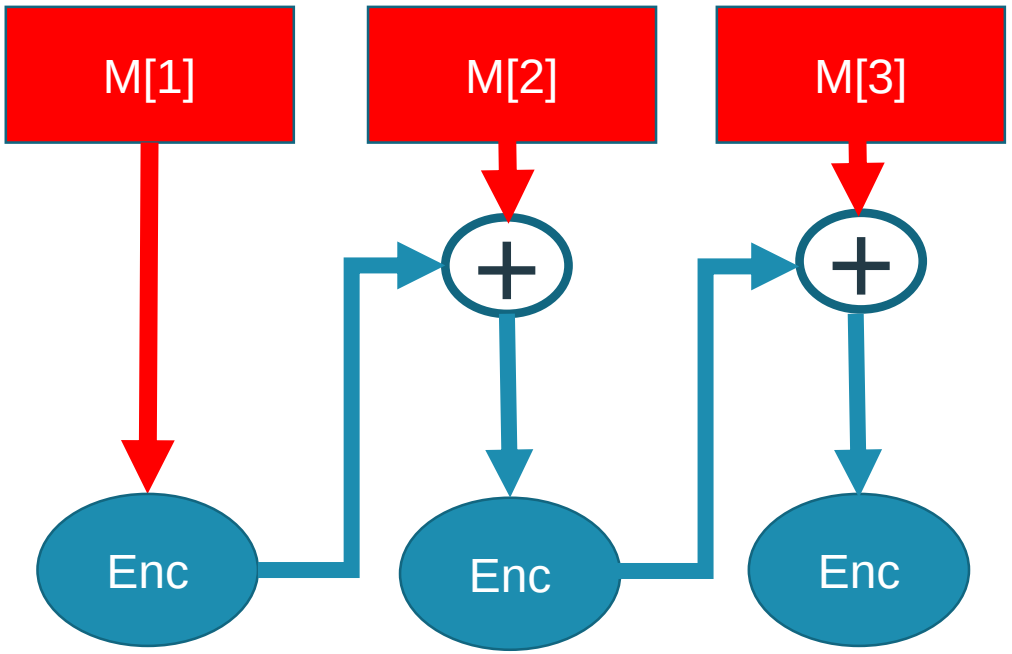
Prior work – PRFs in MPC (CCS'16)

Enc(42)  Tag(Enc(42))



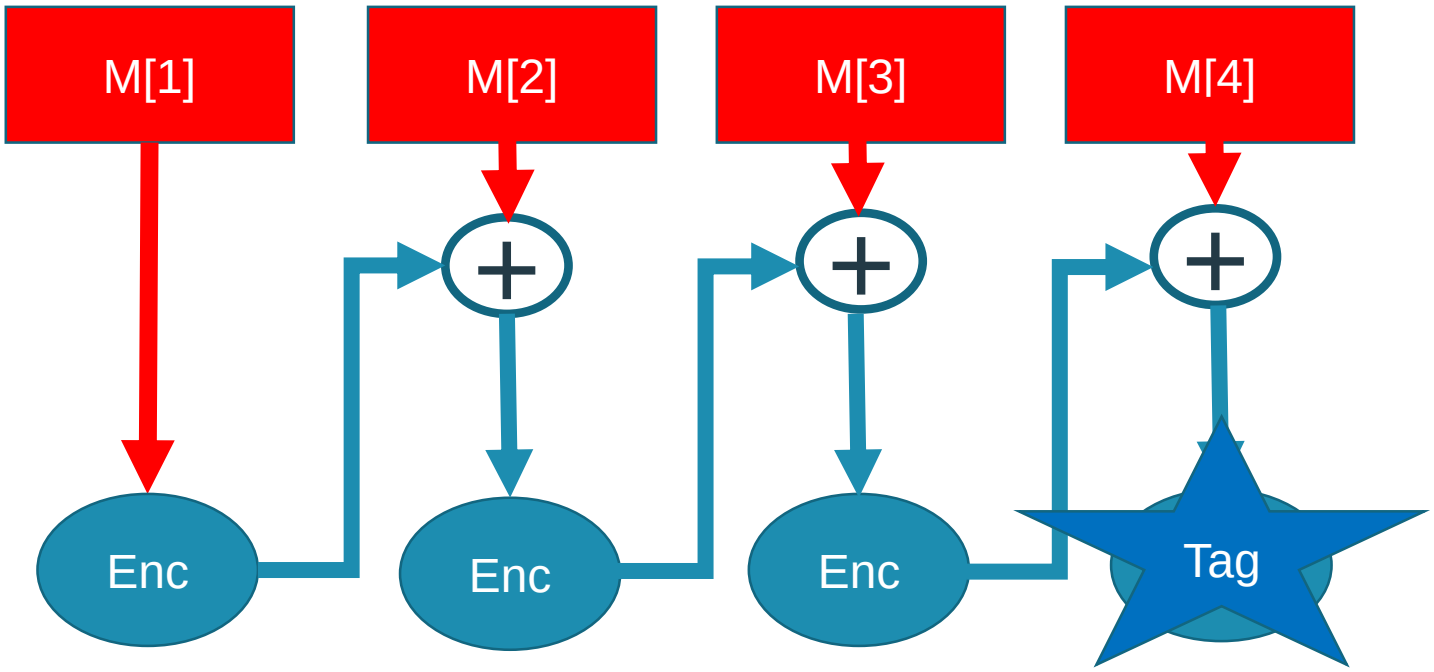
Prior work – PRFs in MPC (CCS'16)

Enc(42)  Tag(Enc(42))



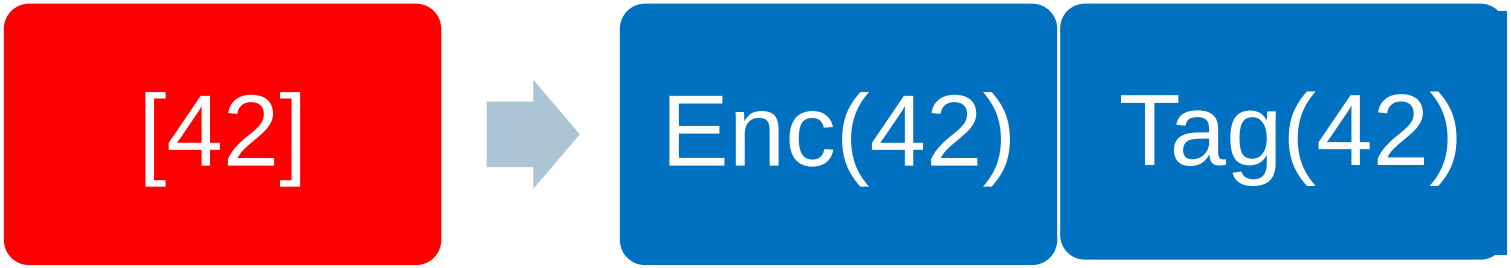
Prior work – PRFs in MPC (CCS'16)

Enc(42)  Tag(Enc(42))



Dragos Rotaru, N.P. Smart, M. Stam imec-Cosic, Dept. Electrical Engineering

What we have done



- Analyze AE in Multiparty Computation (MPC).
- Useful MPC happens in Fp => Need AE and PRFs modp.
- Look for parallel AE: CTR+PMAC, OTR.

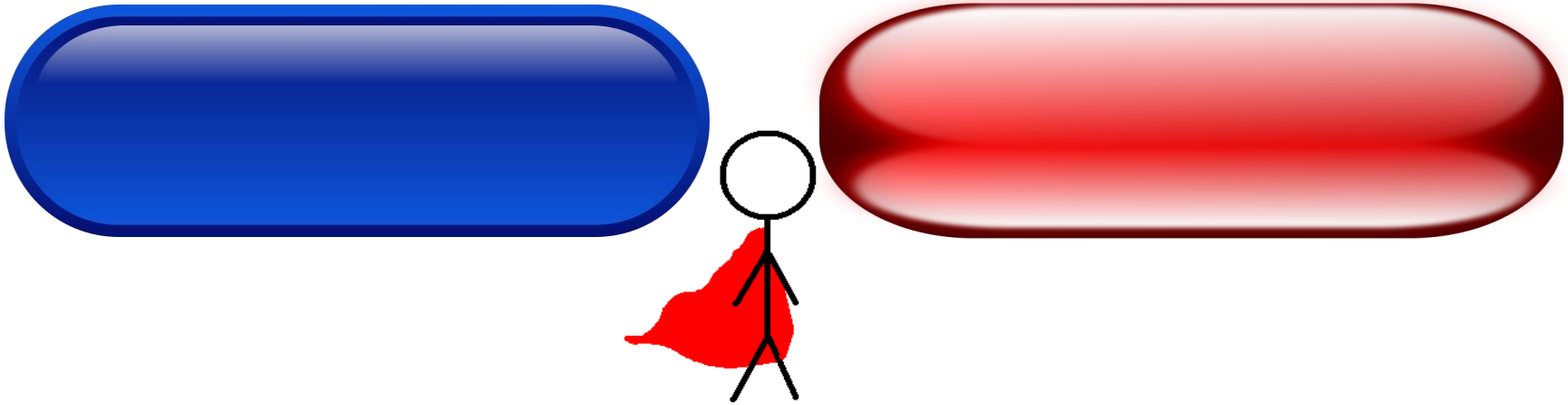
The story

The story

‘You take the blue pill—the story ends, you wake up in your bed and believe whatever you want to believe.

You take the *red* pill—you stay in Wonderland, and I show you how deep the rabbit hole goes.’

The story



‘You take the blue pill—the story ends, you wake up in your bed and believe whatever you want to believe.

You take the *red* pill—you stay in Wonderland, and I show you how deep the rabbit hole goes.’

Down the rabbit hole - MPC with Secret Sharing

$$x = x_1 + \cdots + x_n$$

Each P_i has $[x] \leftarrow x_i$

$[x] \leftarrow x_1$

$[x] \leftarrow x_2$

$[x] \leftarrow x_3$

MPC Preprocessing Phase

Generate triples
[c] = [a][b]

MPC Preprocessing Phase

Generate triples

[c] = [a][b]

MPC Preprocessing Phase

Dragos Rotaru, N.P. Smart, M. Stam imec-Cosic, Dept. Electrical Engineering

MPC Preprocessing Phase

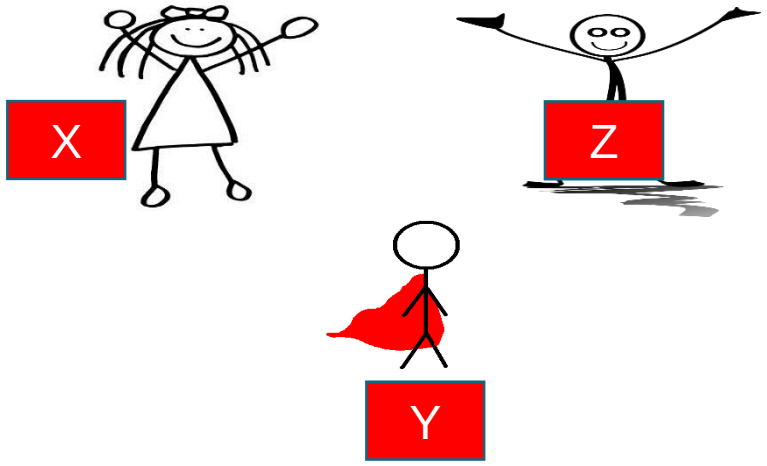
Dragos Rotaru, N.P. Smart, M. Stam imec-Cosic, Dept. Electrical Engineering

MPC Online Phase

Use Triples.

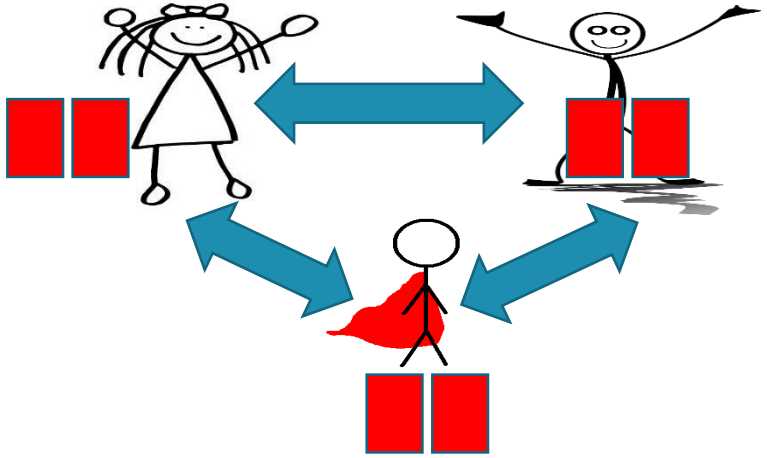
MPC Online Phase

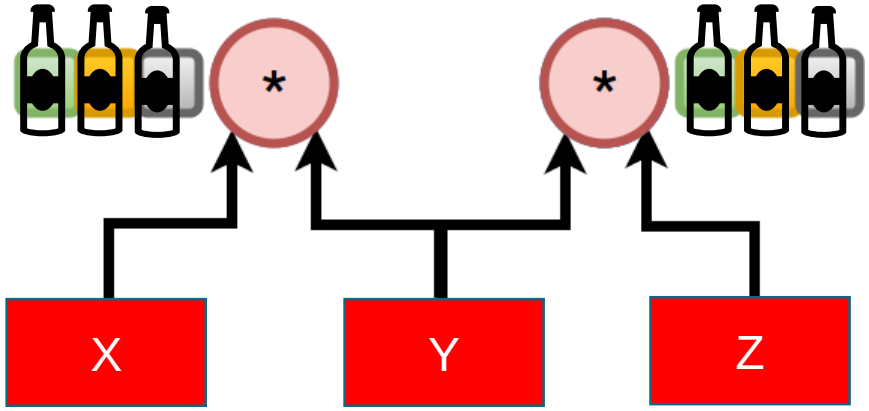
MPC Circuit Evaluation



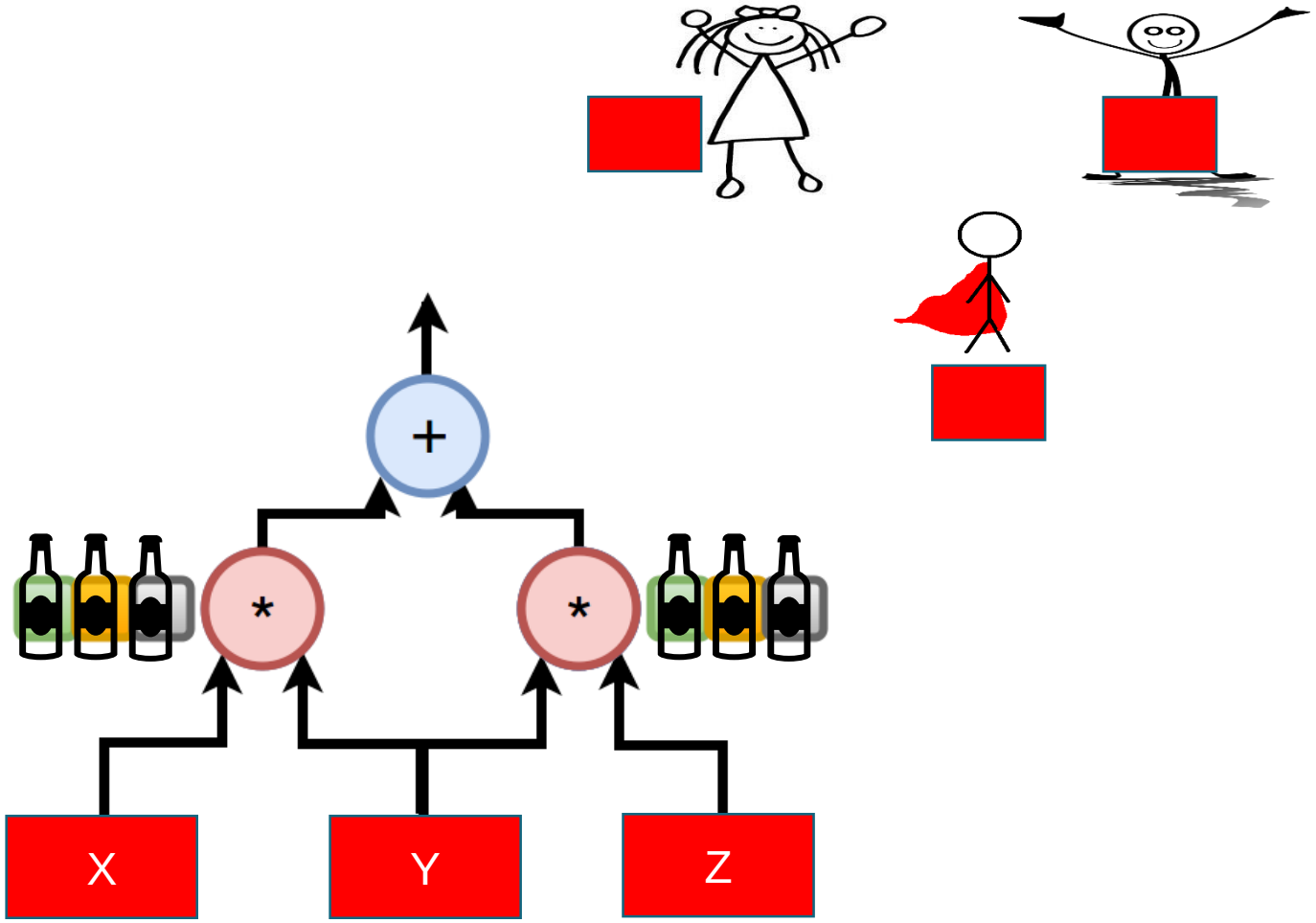
X Y Z

MPC Circuit Evaluation

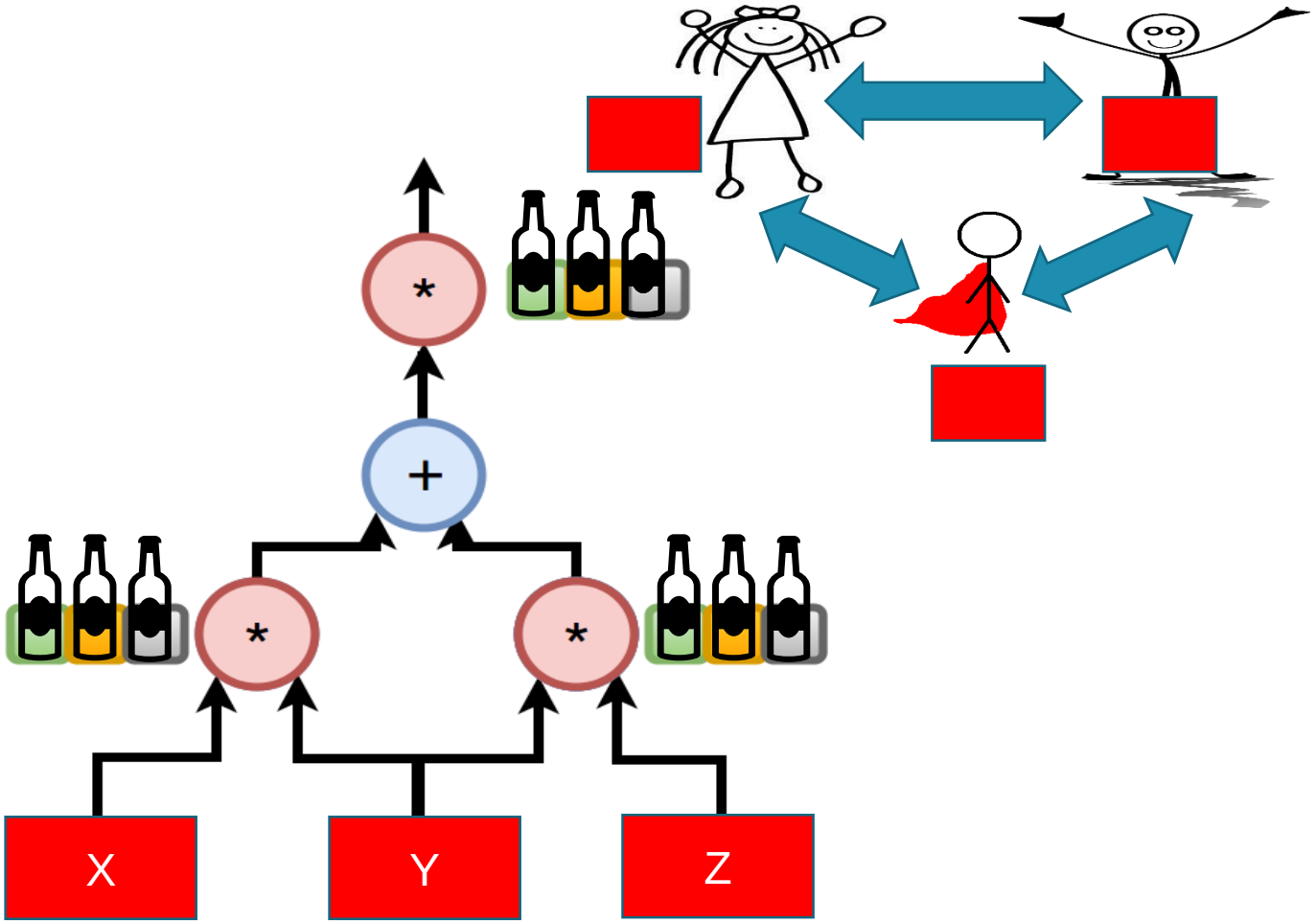




MPC Circuit Evaluation

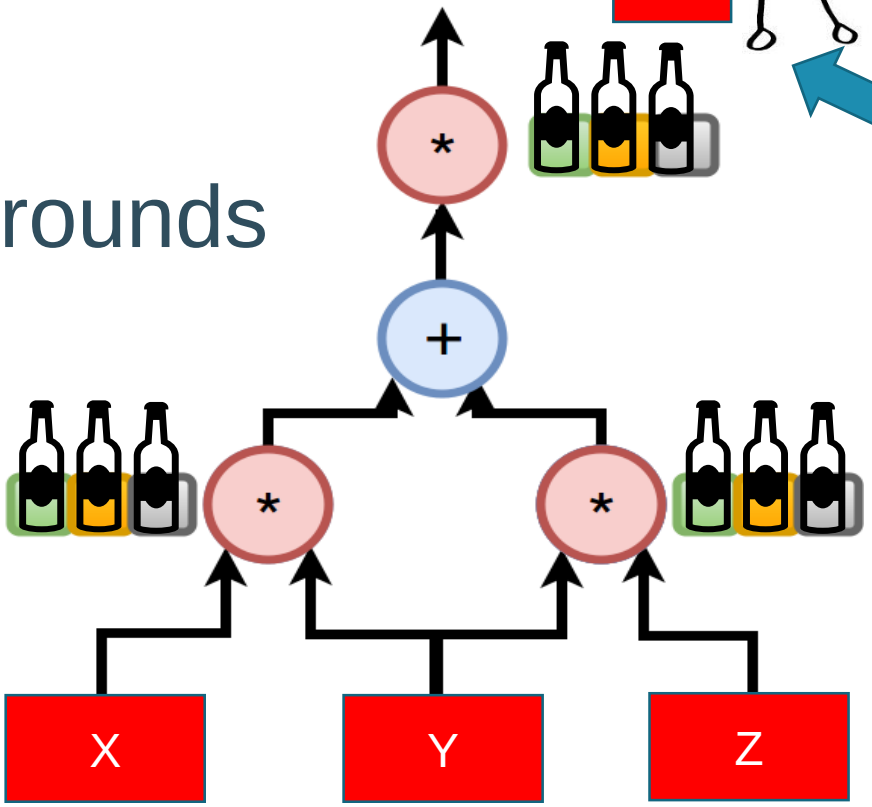


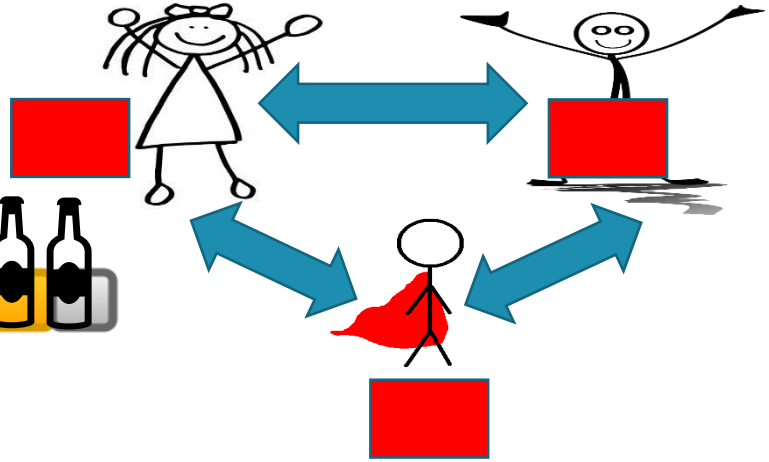
MPC Circuit Evaluation



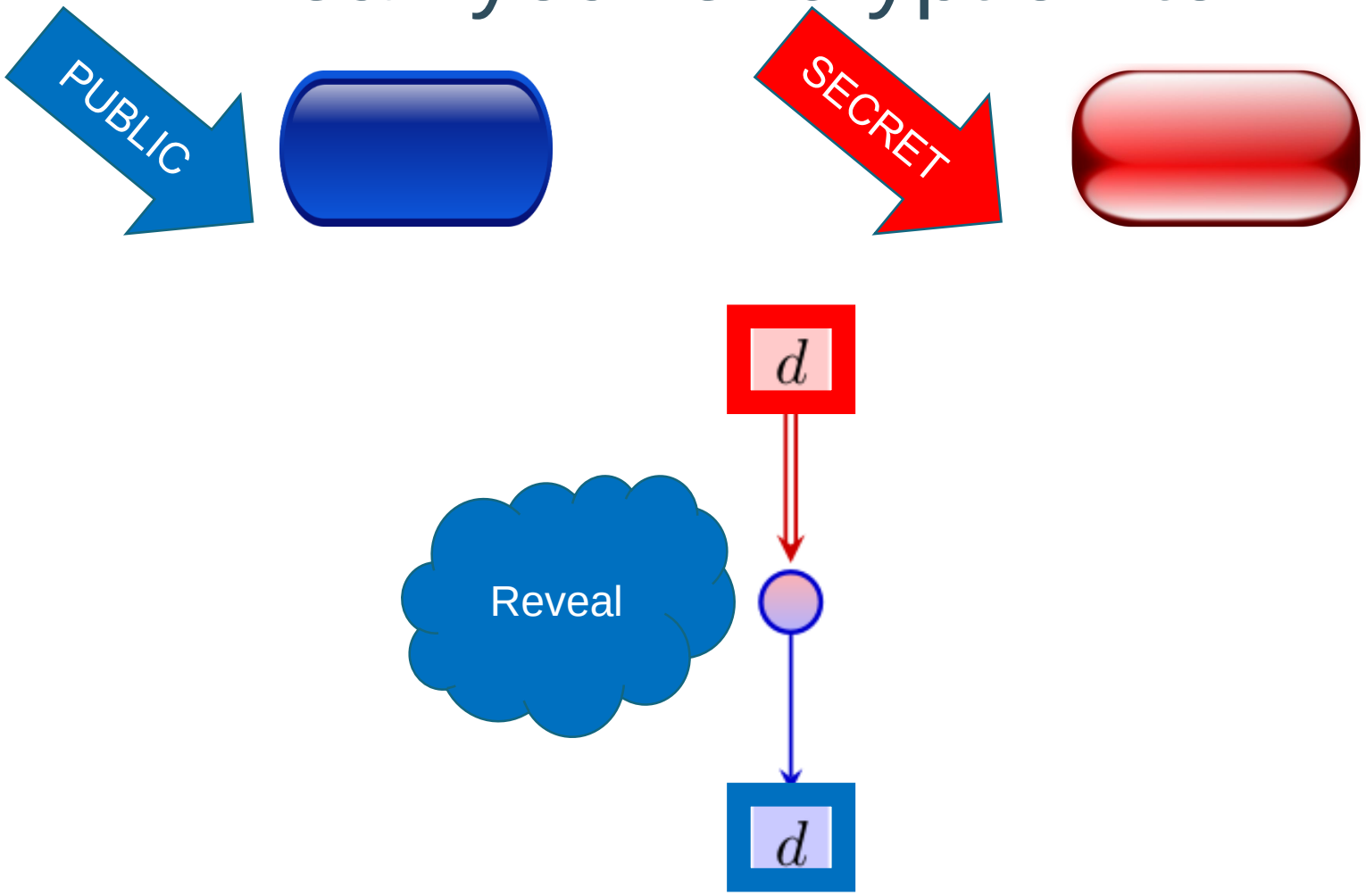
MPC Circuit Evaluation

3 triples.
2 comm. rounds

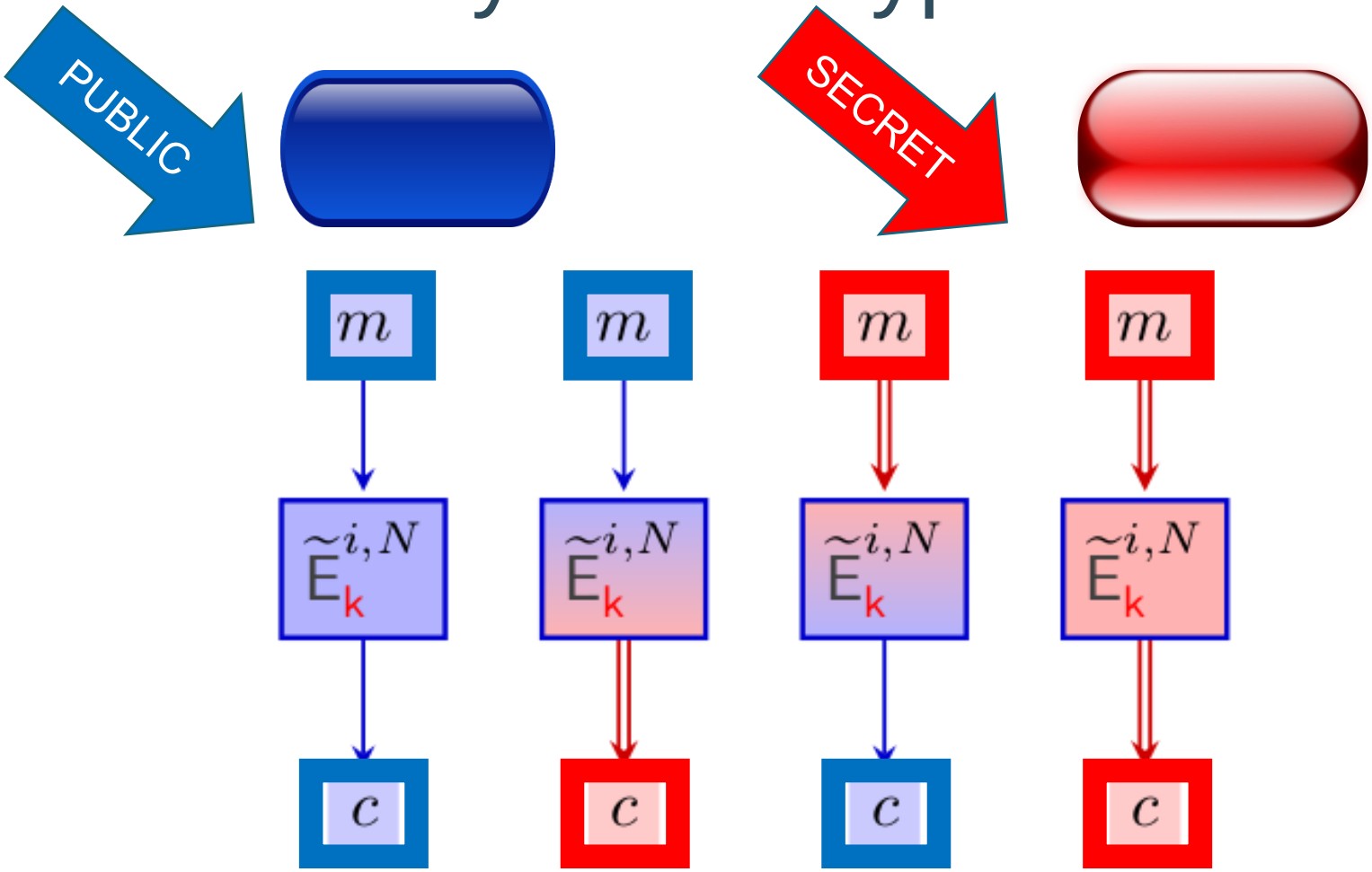




Tweak your encryption to MPC

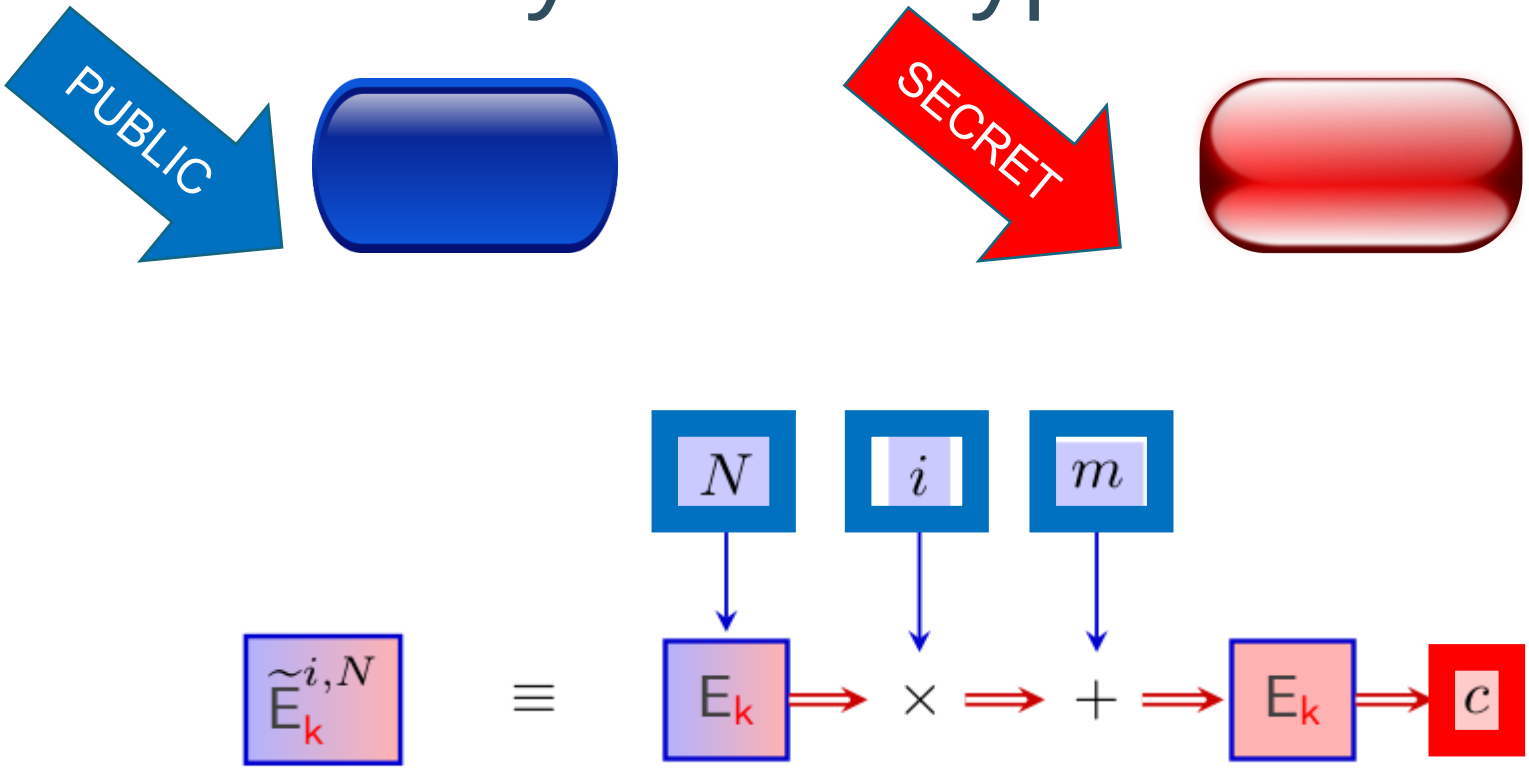


Tweak your encryption to MPC

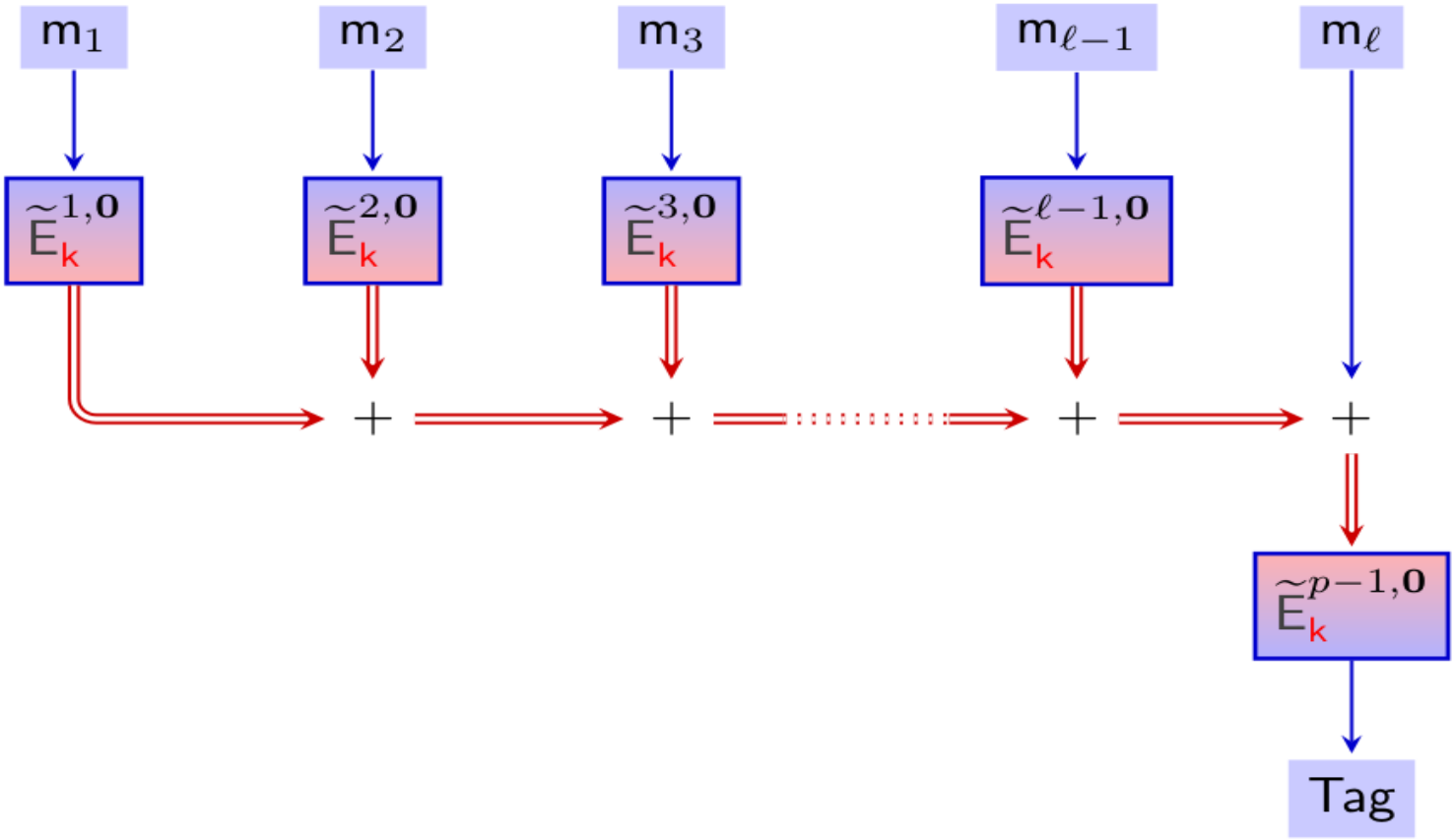


Dragos Rotaru, N.P. Smart, M. Stam imec-Cosic, Dept. Electrical Engineering KU LEUVEN

Tweak your encryption to MPC

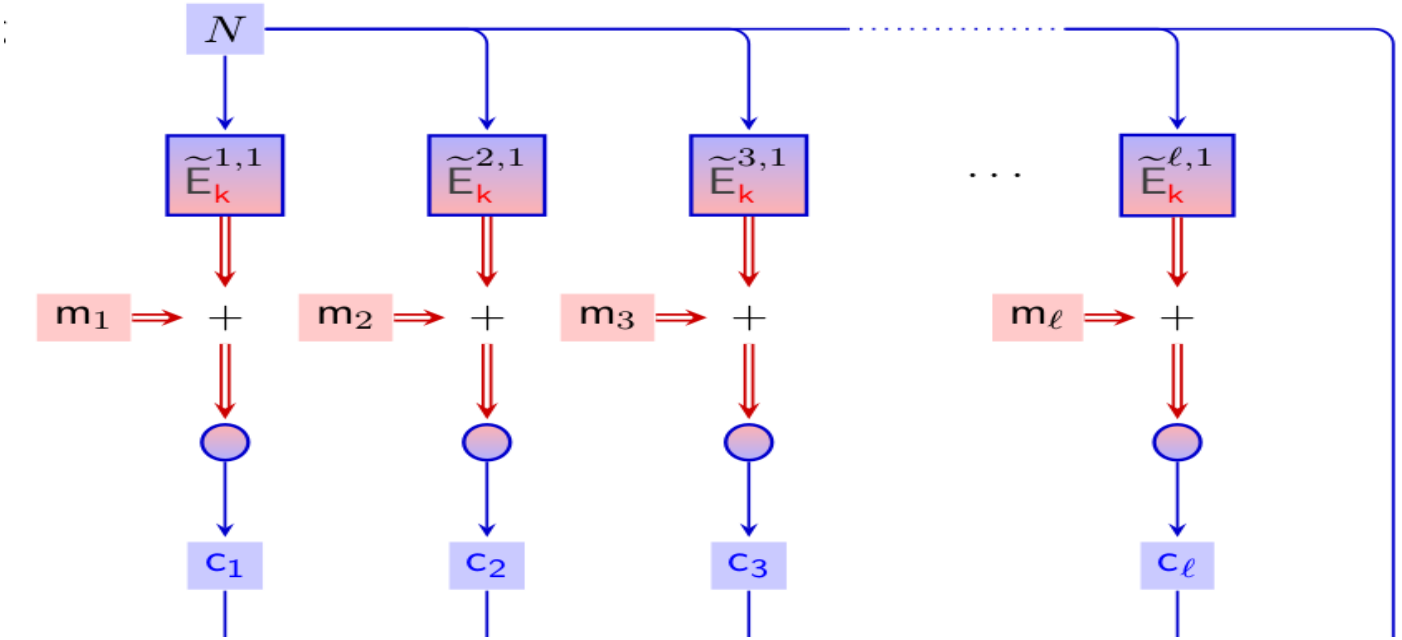


How-to compute PMAC



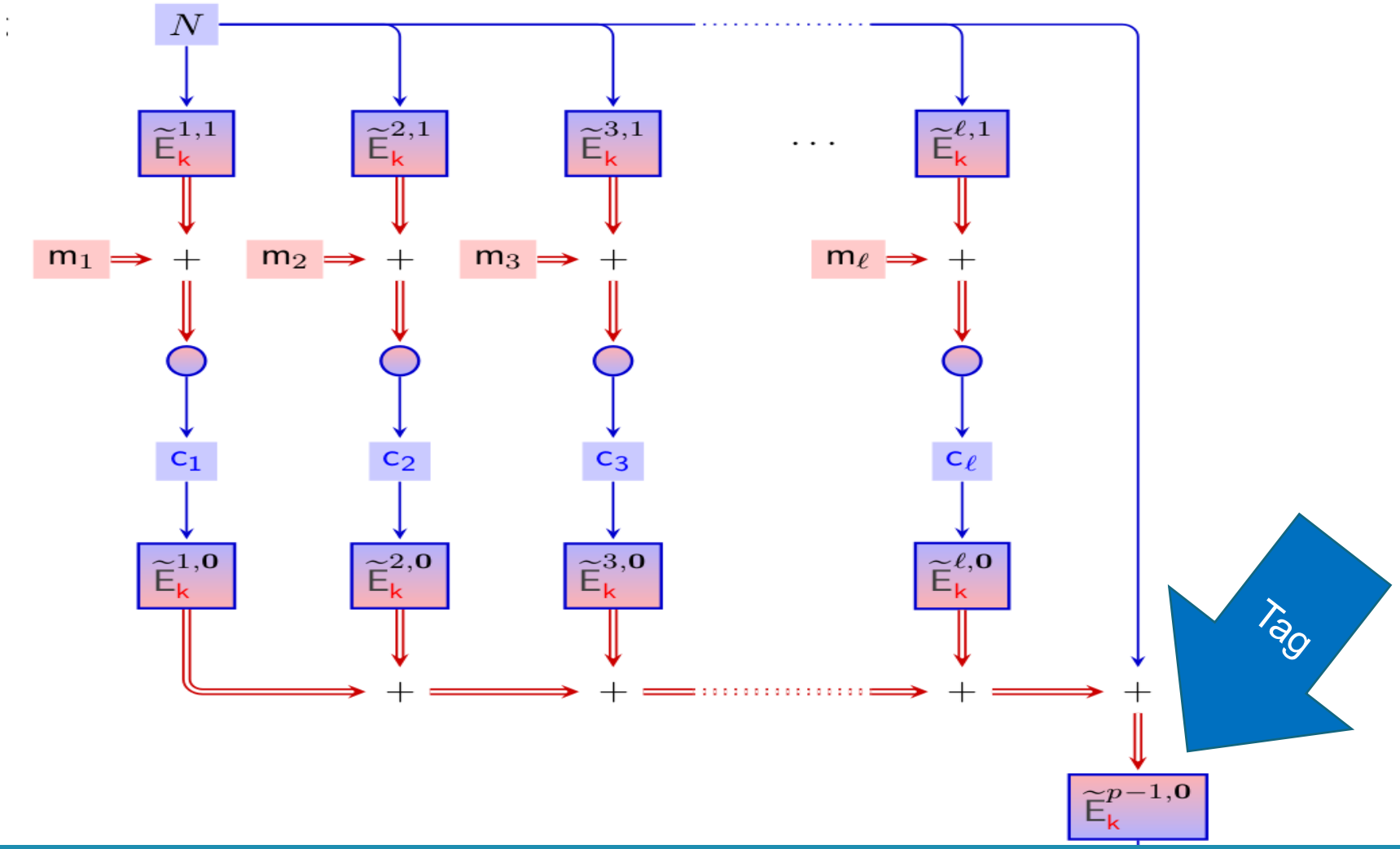
Dragos Rotaru, N.P. Smart, M. Stam imec-Cosic, Dept. Electrical Engineering

Let's do AE with CTR+pPMAC



Dragos Rotaru, N.P. Smart, M. Stam imec-Cosic, Dept. Electrical Engineering KU LEUVEN

Let's do AE with CTR+pPMAC

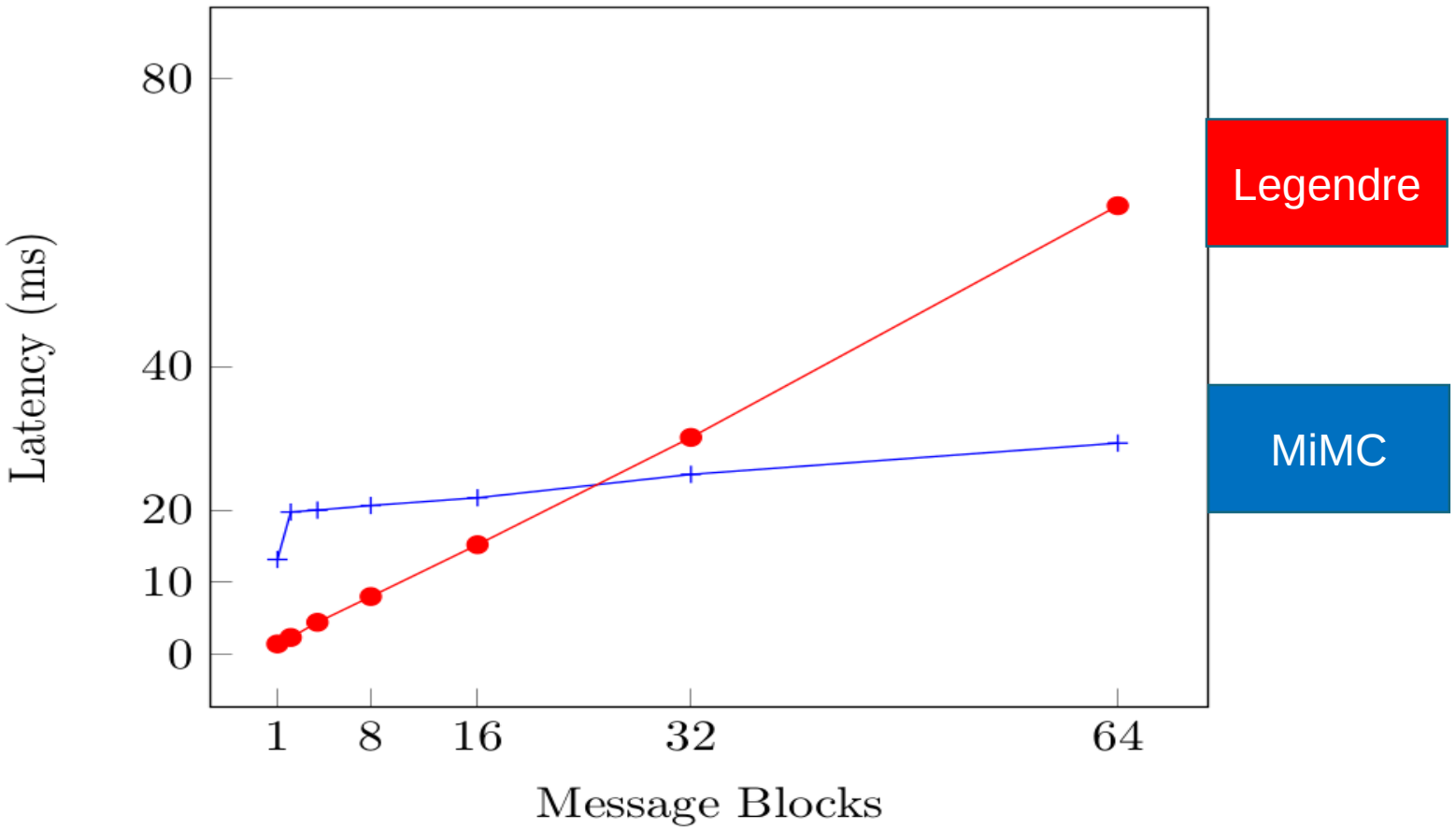


Dragos Rotaru, N.P. Smart, M. Stam imec-Cosic, Dept. Electrical Engineering KU LEUVEN

When ideal meets real

When ideal meets real – surprise!

When ideal meets real – surprise!



Dragos Rotaru, N.P. Smart, M. Stam imec-Cosic, Dept. Electrical Engineering KU LEUVEN

Other competitive modes

PRF	Mode	Online cost	
		Rounds (Enc/Dec)	Openings
Leg	CTR+pPMAC	7/6	$768 \cdot \ell + \ell$
MiMC	CTR+pPMAC	221/147	$146 \cdot \ell + \ell + 1$
Leg	CTR+HtMAC	5/4	$384 \cdot (\ell + 1) + \ell$
MiMC	CTR+HtMAC	148/75	$73 \cdot (\ell + 1) + \ell + 1$
Leg	OTR	6/9	$384 \cdot (\ell + 128) + \ell$
MiMC	OTR	220/295	$73 \cdot (\ell + 2) + \ell + 1$

Other competitive modes

PRF	Mode	Online cost	
		Rounds (Enc/Dec)	Openings
Leg	CTR+pPMAC	7/6	$768 \cdot \ell + \ell$
MiMC	CTR+pPMAC	221/147	$146 \cdot \ell + \ell + 1$
Leg	CTR+HtMAC	5/4	$384 \cdot (\ell + 1) + \ell$
MiMC	CTR+HtMAC	148/75	$73 \cdot (\ell + 1) + \ell + 1$
Leg	OTR	6/9	$384 \cdot (\ell + 128) + \ell$
MiMC	OTR	220/295	$73 \cdot (\ell + 2) + \ell + 1$

Some open problems

- Preprocessing scales linearly in terms of number of message blocks - roughly n PRFs for n messages.
- Number of rounds of a cipher vs. multiplicative depth in MPC.

Thank you!

Thank you!

- Questions?