TPMPC 2018

MPC across the wire: There is something you require

Dragos Rotaru

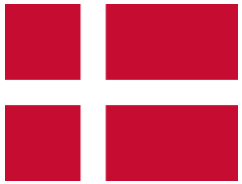
KU Leuven, University of Bristol

$6.3M question – Brandeis program

K

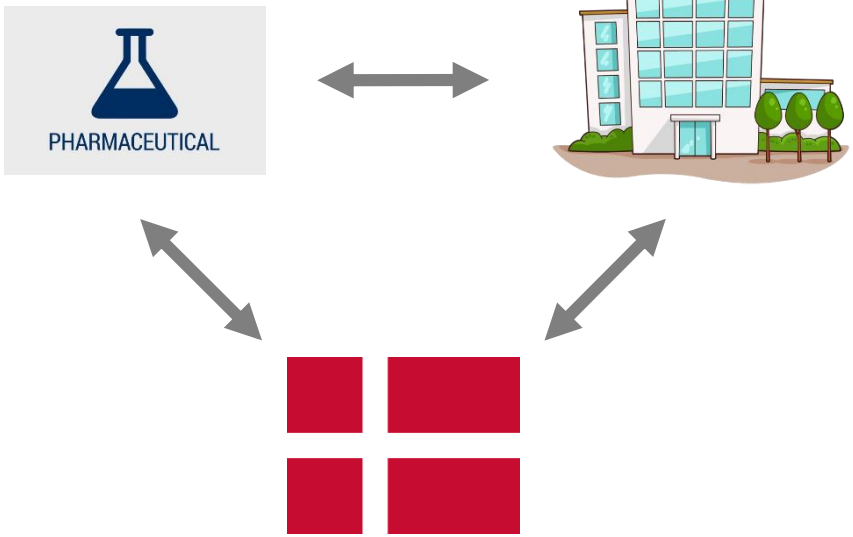
Enc(K, MEDICAL RECORD)

PHARMACEUTICAL



$6.3M question – Brandeis program

K



$6.3M question – Brandeis program

K

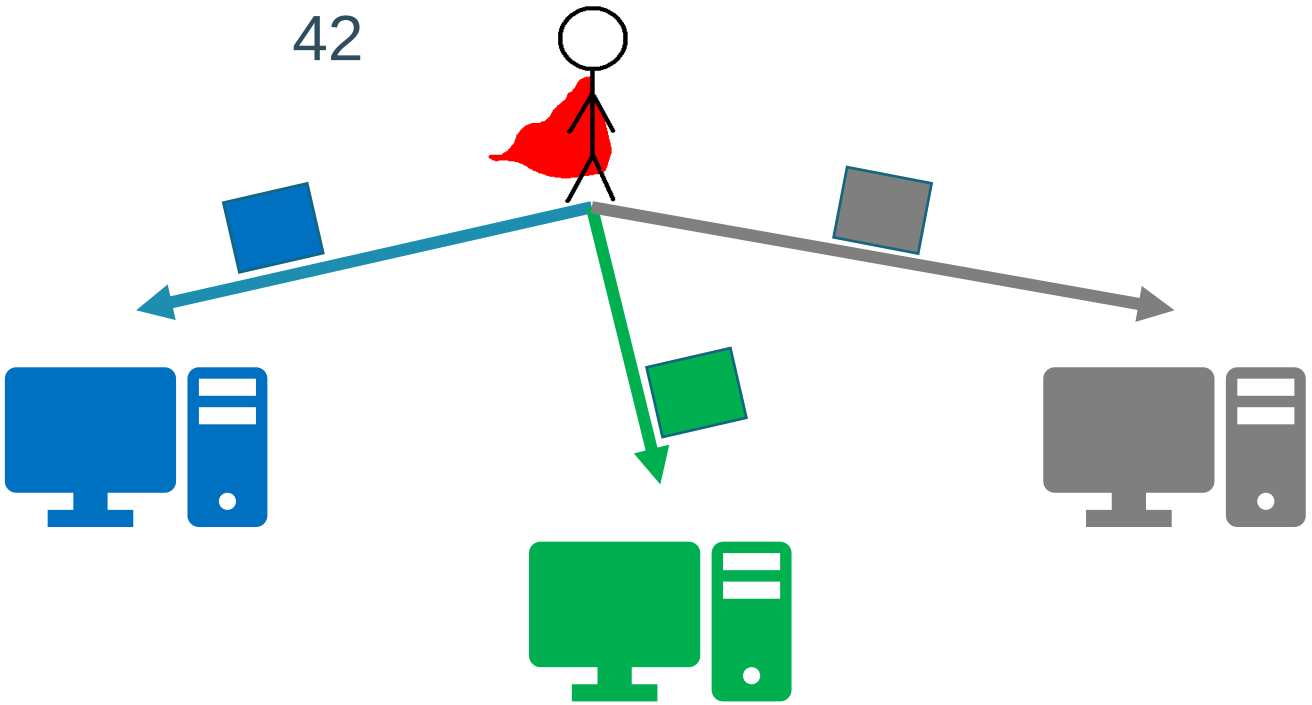
PHARMACEUTICAL

C = Enc(K, 

)

MPC and Long-term storage some research shortage…

Long-term storage



Long-term storage

42

$M_1 + M_2 + M_3 = 42$

M_1

M_2

M_3

Long-term storage

$M_1 + M_2 + M_3 = 42$

M_1

M_2

M_3

Long-term storage

K

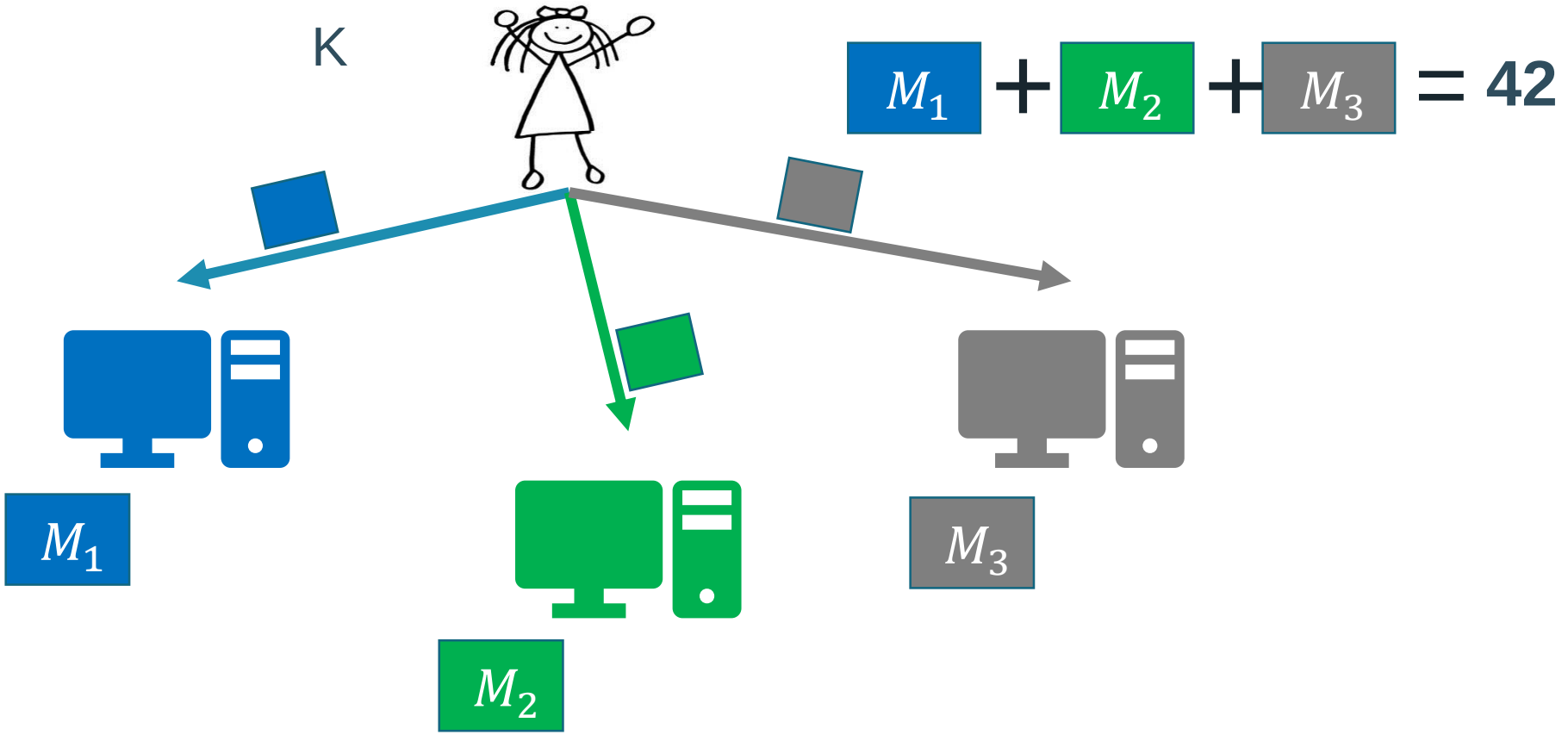
$M_1 + M_2 + M_3 = 42$

M_1

M_2

M_3

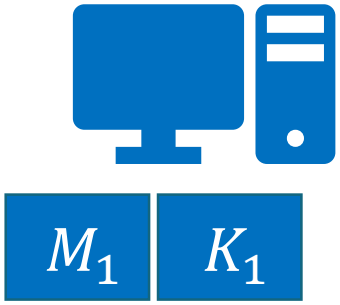
Long-term storage

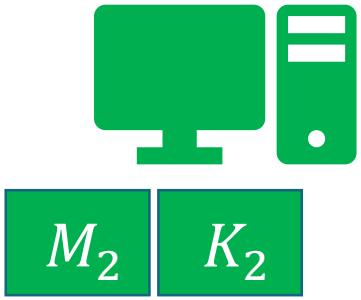


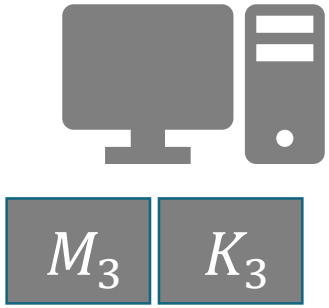
Long-term storage

$M_1 + M_2 + M_3 = 42$

$K_1 + K_2 + K_3 = K$



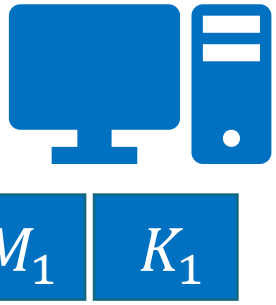


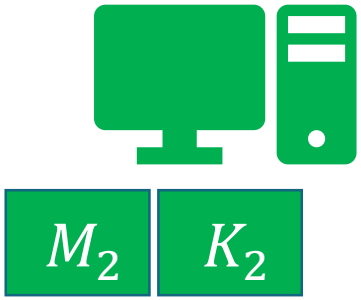


Long-term storage

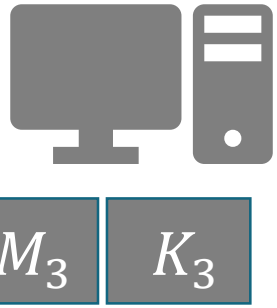
$M_1 + M_2 + M_3 = 42$

$K_1 + K_2 + K_3 = K$





Enc(K_2, M_2)

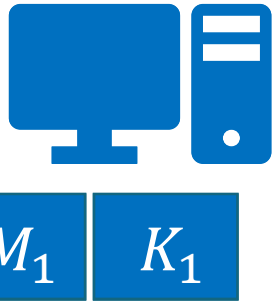


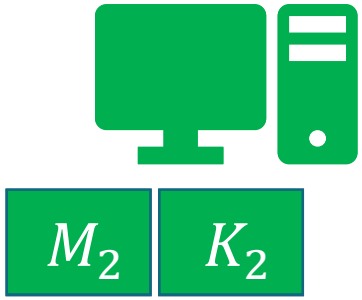
Long-term storage

Too many keys!
Let's keep it simple.

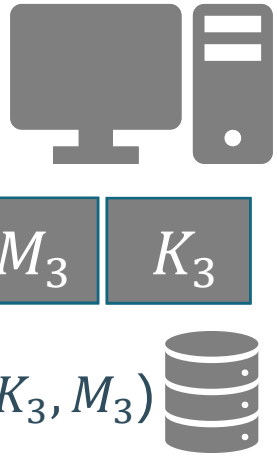
$M_1 + M_2 + M_3 = 42$

$K_1 + K_2 + K_3 = K$





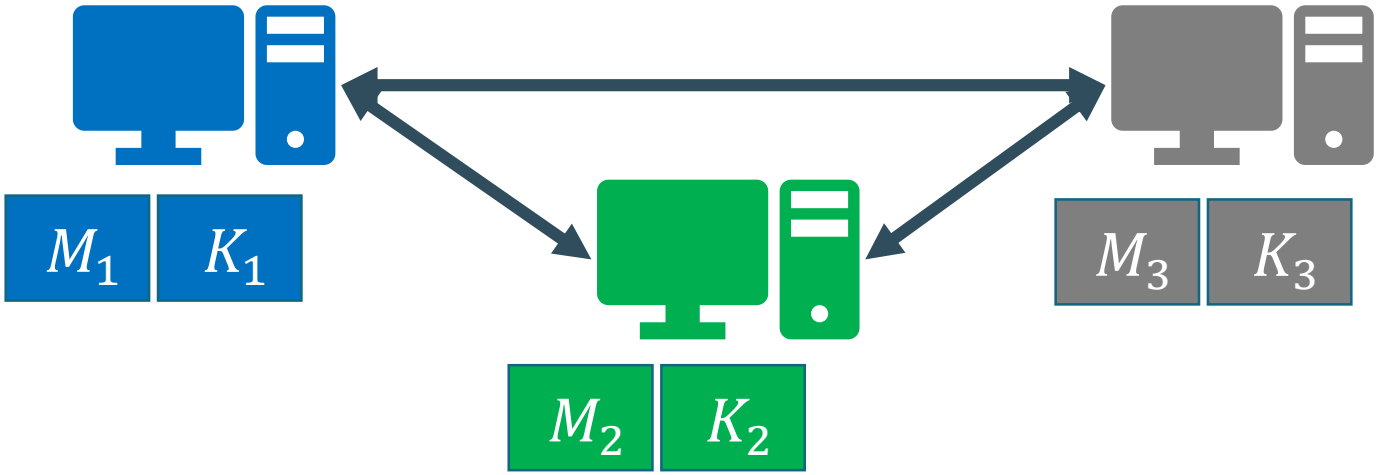
Enc(K_2, M_2)



Long-term storage

$M_1 + M_2 + M_3 = 42$

$K_1 + K_2 + K_3 = K$



Long-term storage

I can also detect whether parties used incorrect keys.

K

Enc(K,42)  Tag(Enc(K,42))

Long-term storage

I can also detect whether parties used incorrect keys.

K

- Can be used to remove interaction when providing inputs to SPDZ [DDN+15].

Enc(K,42)  Tag(Enc(K,42))

Tricks to get a PhD in crypto*

Line of work - mod p

Enc(42)  Tag(Enc(42))

PRFs: NR, MiMC, Leg.

CCS'16
[GRRSS]

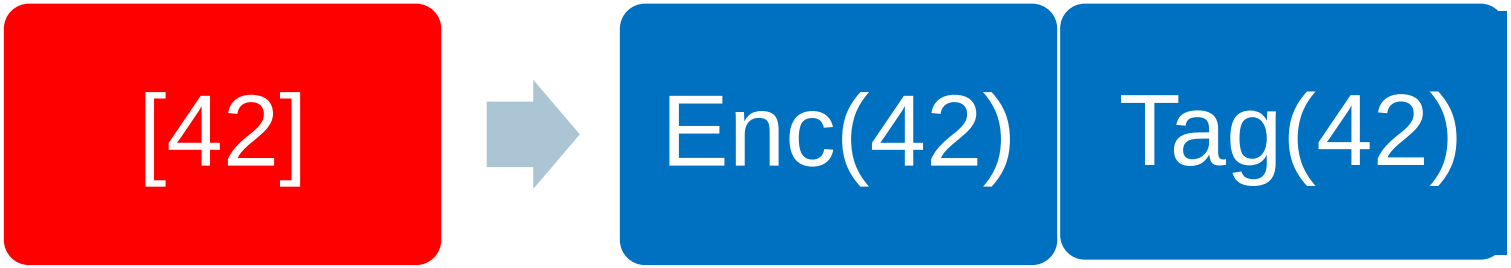
AE: OTR, PMAC.

FSE'18
[RSS]

Generalized MiMC,
Fewer triples per message block.

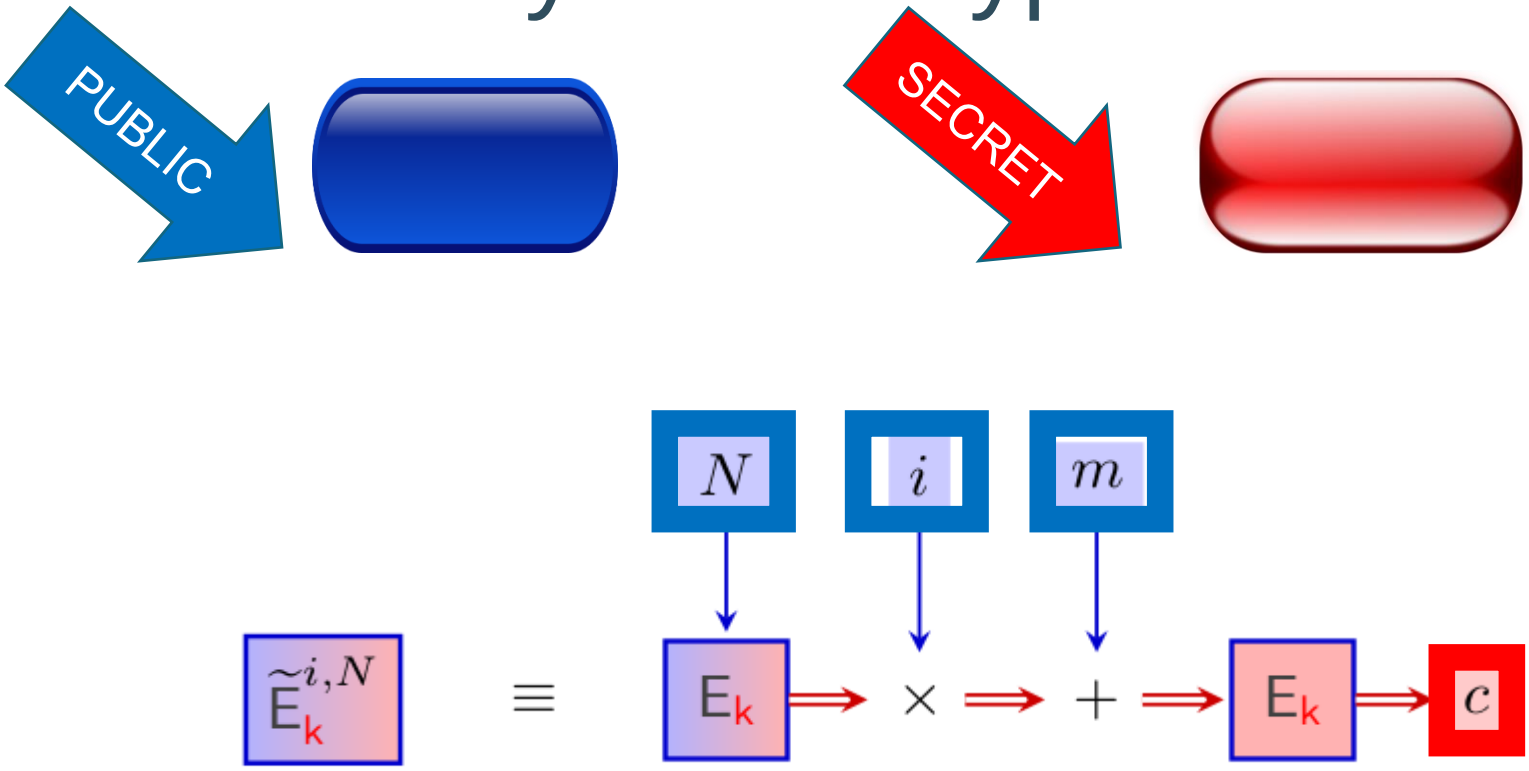
?'18
[AGPRRRRS]

Authenticated Encryption in MPC

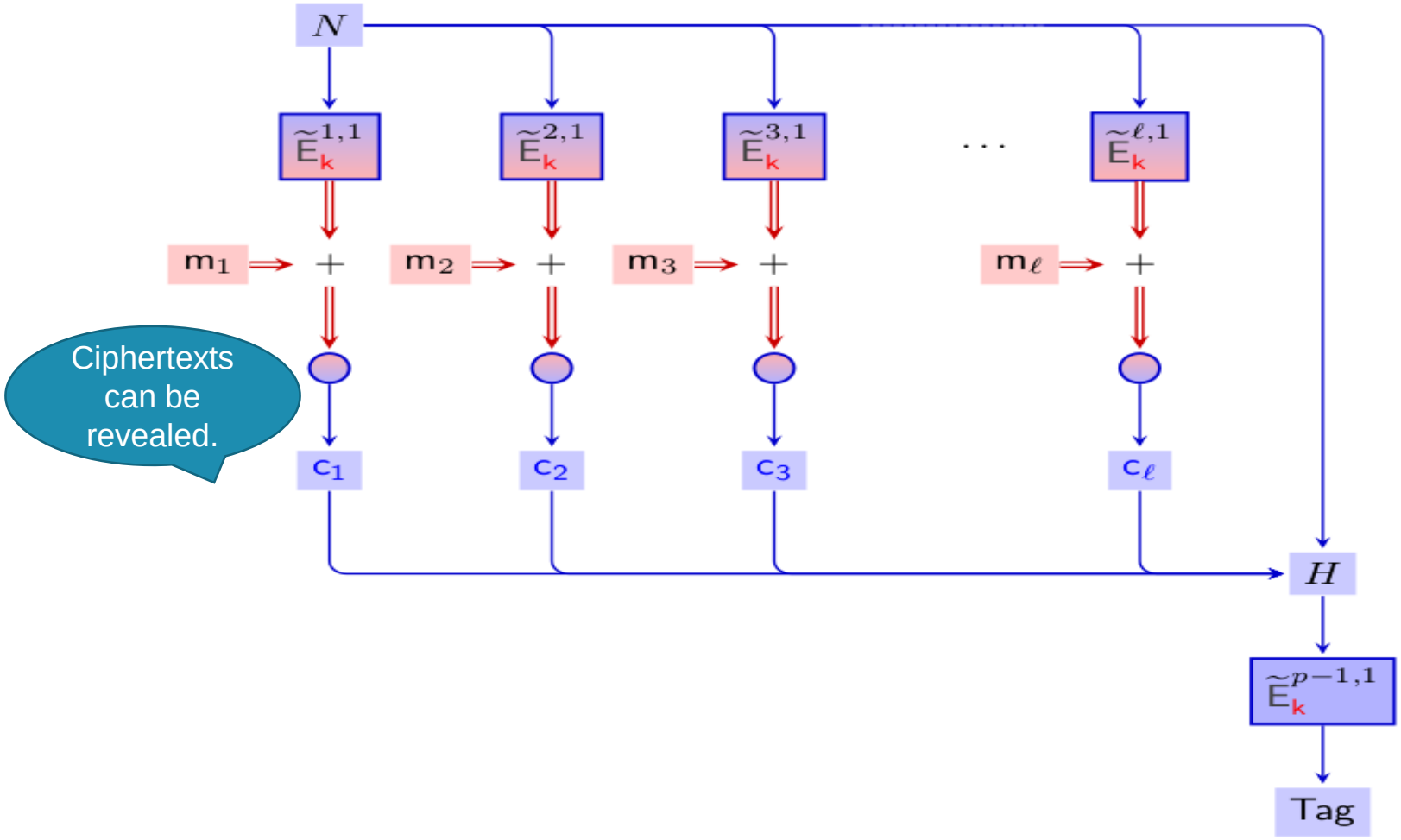


- Useful MPC happens in Fp => Need AE and PRFs modp.
- Look for parallel AE: CTR+PMAC, OTR.
- MPC framework splits computation in 2 phases:
  - Input independent pre-processing.
  - Online phase where inputs are used.

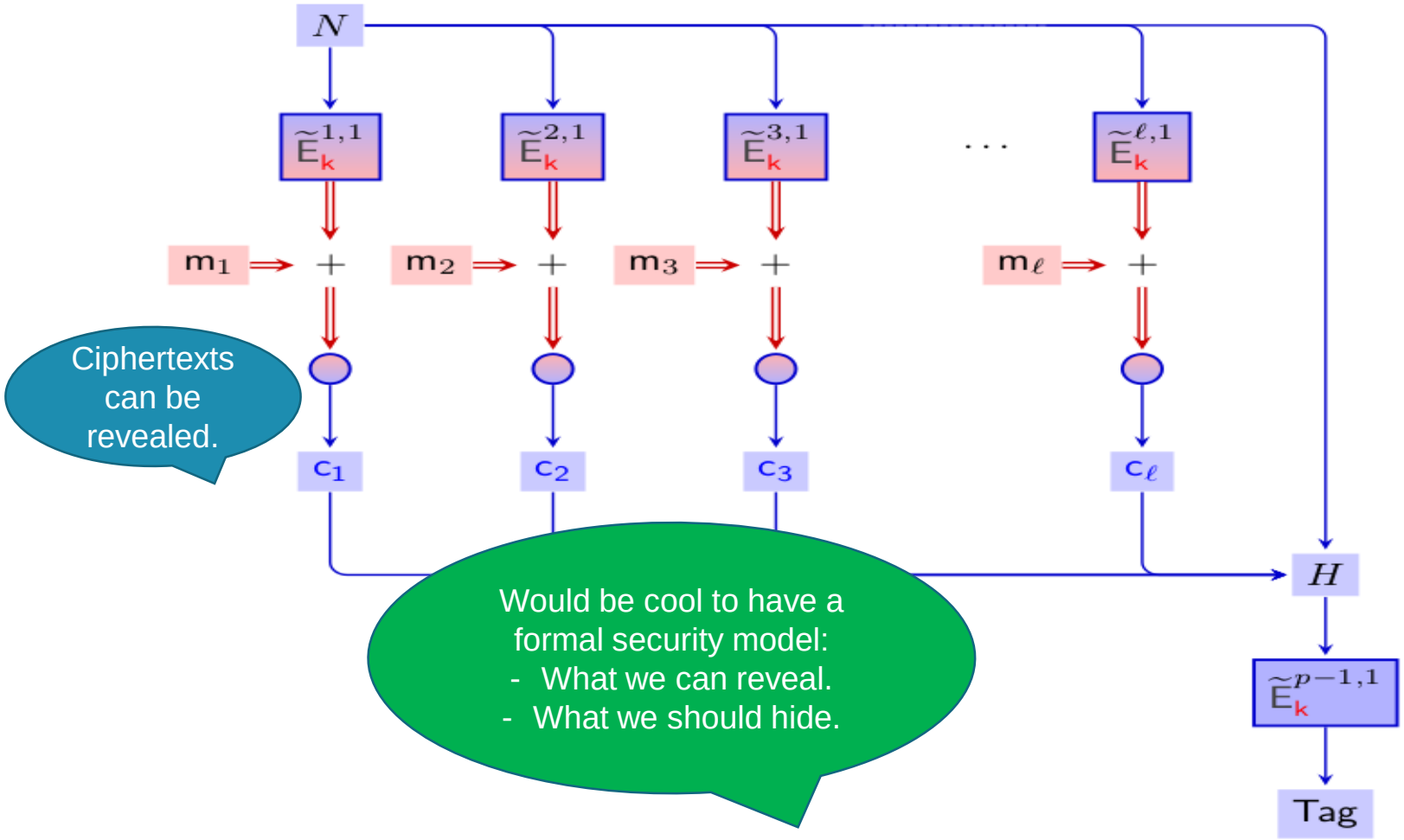
Tweak your encryption to MPC



And the winner is…CTR+HtMAC



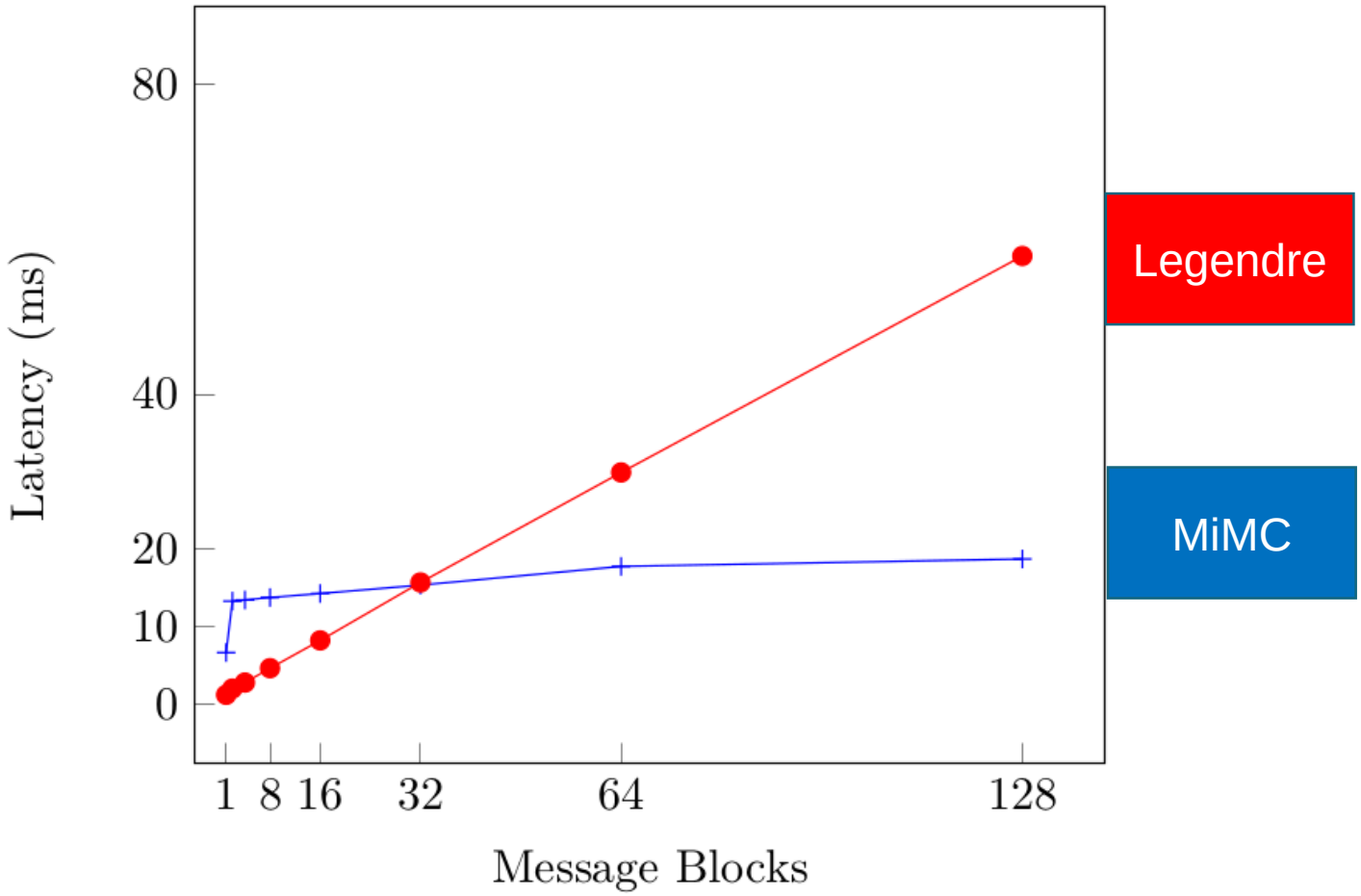
And the winner is…CTR+HtMAC



When ideal meets real

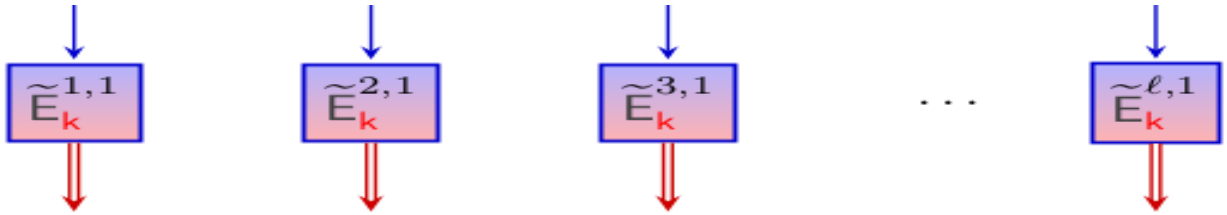
When ideal meets real – surprise!

When ideal meets real – surprise!

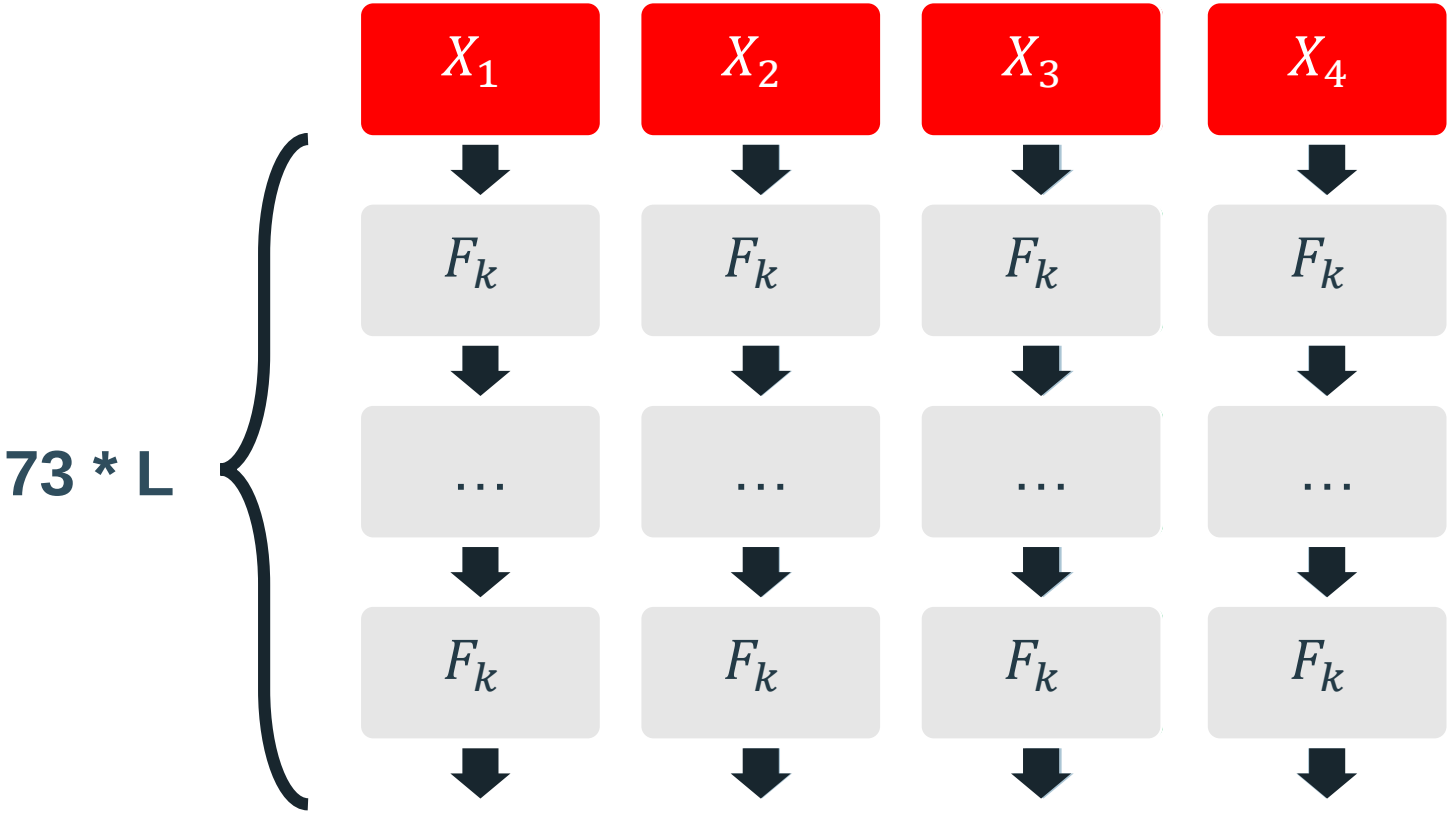


Can we cripple…the triple(s)?

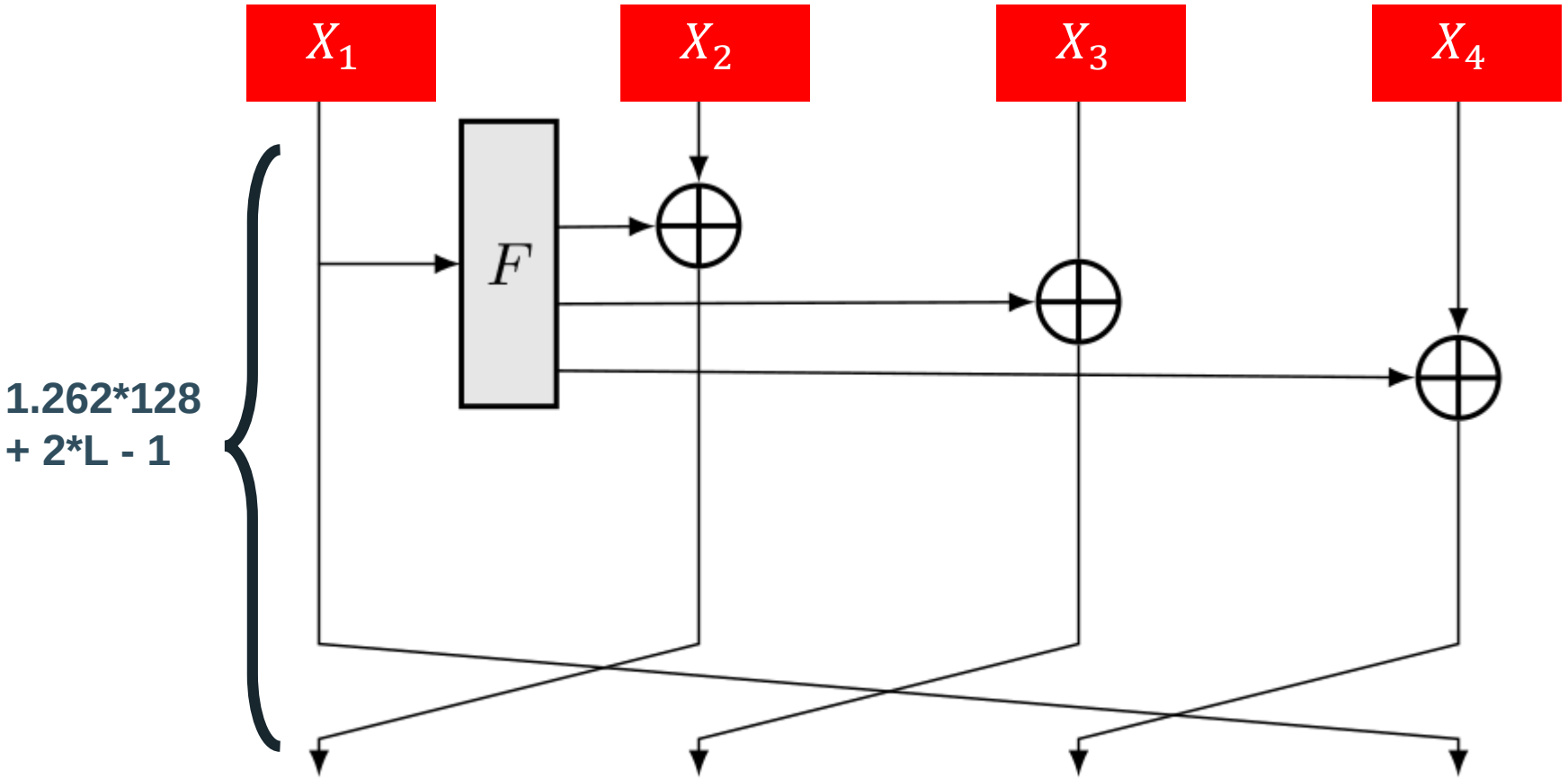
- Pre-processing cost scales linearly with the number of blocks.



MiMC



GMiMC



Putting the (GMi)MC into MPC

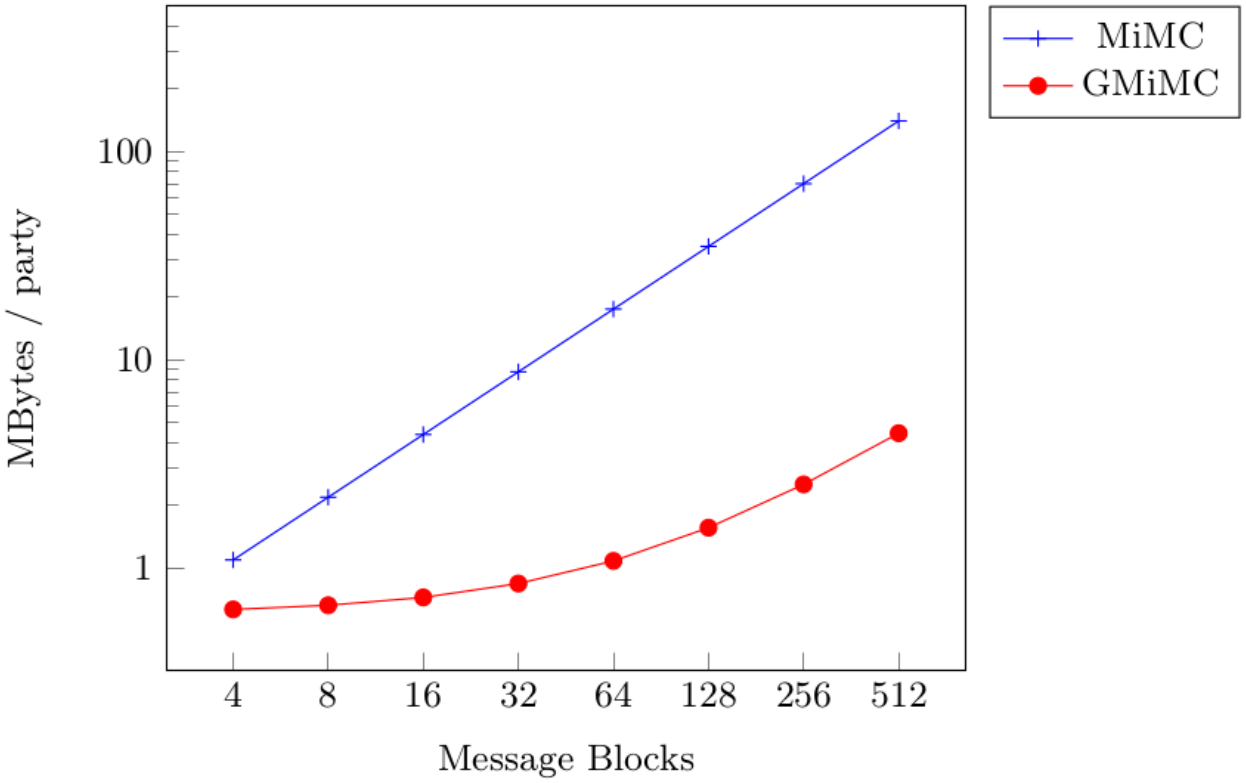


Fig. 1. One way preprocessing costs (MBytes) using 2 party Low Gear with 128 bit prime field from Overdrive for encrypting various message blocks.

Putting the (GMi)MC into MPC

	PRF	$\ell = 4$	8	16	32	64
Communication rounds	MiMC	146	146	146	146	146
	GMiMC	338	354	386	450	578
Openings	MiMC	876	1752	3504	7008	14016
	GMiMC	507	531	579	675	867

Table 2. Online cost for encrypting message blocks of size ℓ, with two parties

Putting the (GMi)MC into MPC

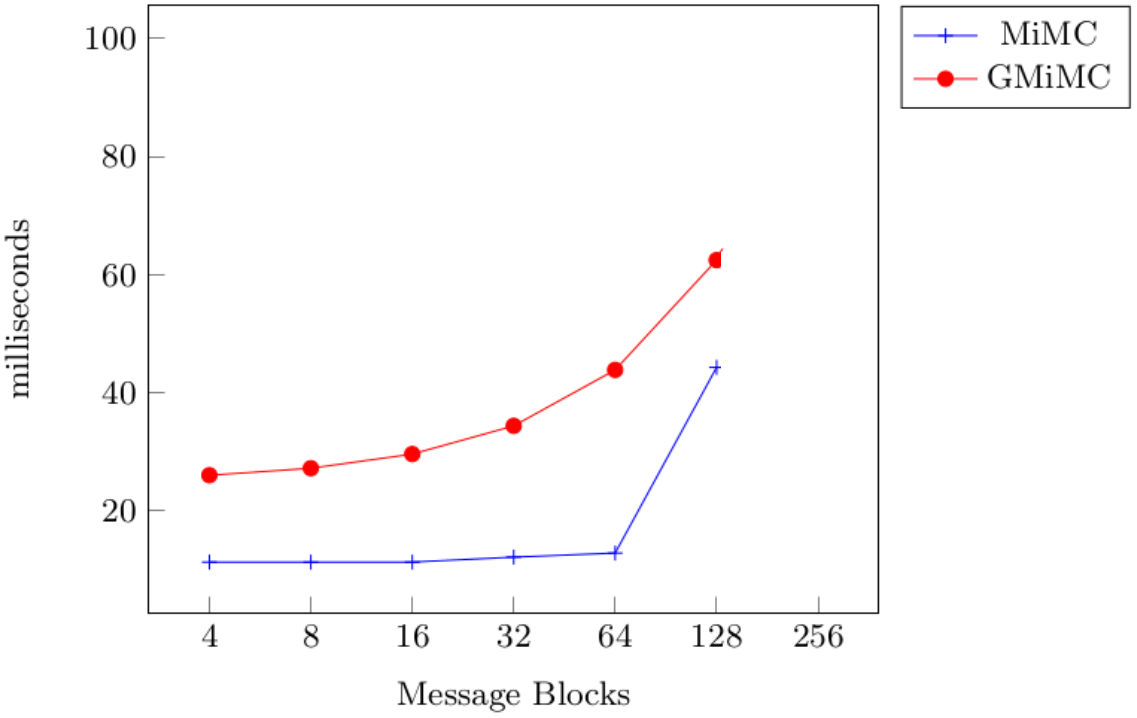


Fig. 3. Online latency for encrypting message blocks of size ℓ, with two parties.

Putting the (GMi)MC into MPC

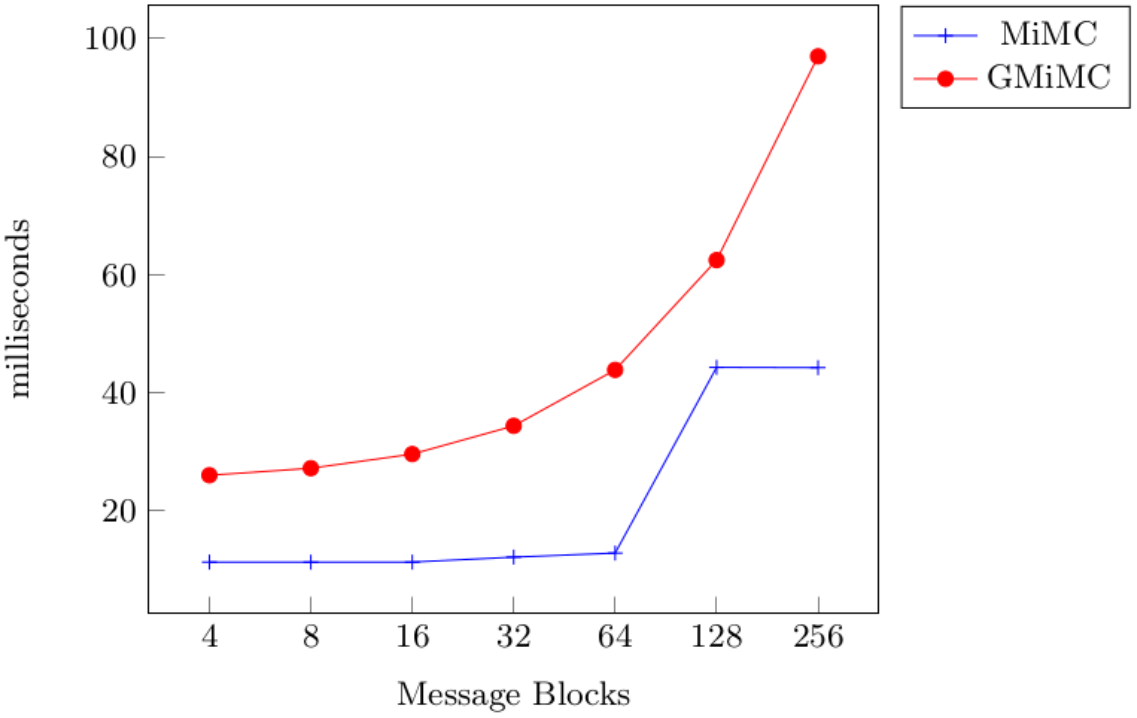
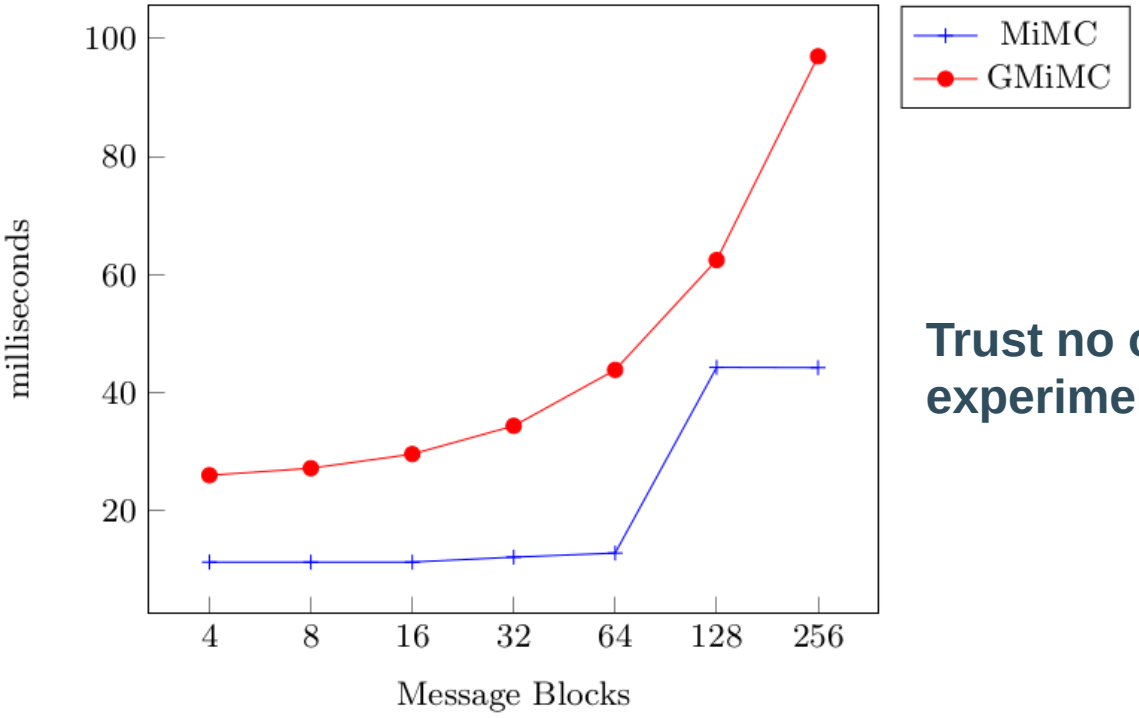


Fig. 3. Online latency for encrypting message blocks of size ℓ, with two parties.

Putting the (GMi)MC into MPC



Trust no one. Do your experiments.

Fig. 3. Online latency for encrypting message blocks of size ℓ, with two parties.

My lyrics get stolen by MiMCs,
I gotta ‘tag’ my rhymes with MPC;
But I keep on generatin' like a PRG
'Cause there's so much drama in the PhD. *

* Adapted from ‘So Much Drama in the PhD’ by Monzy

My lyrics get stolen by miMCs,
I gotta ‘tag’ my rhymes with MPC;
But I keep on generatin' like a PRG
'Cause there's so much drama in the PhD. *

Thank you!

* Adapted from ‘So Much Drama in the PhD’ by Monzy