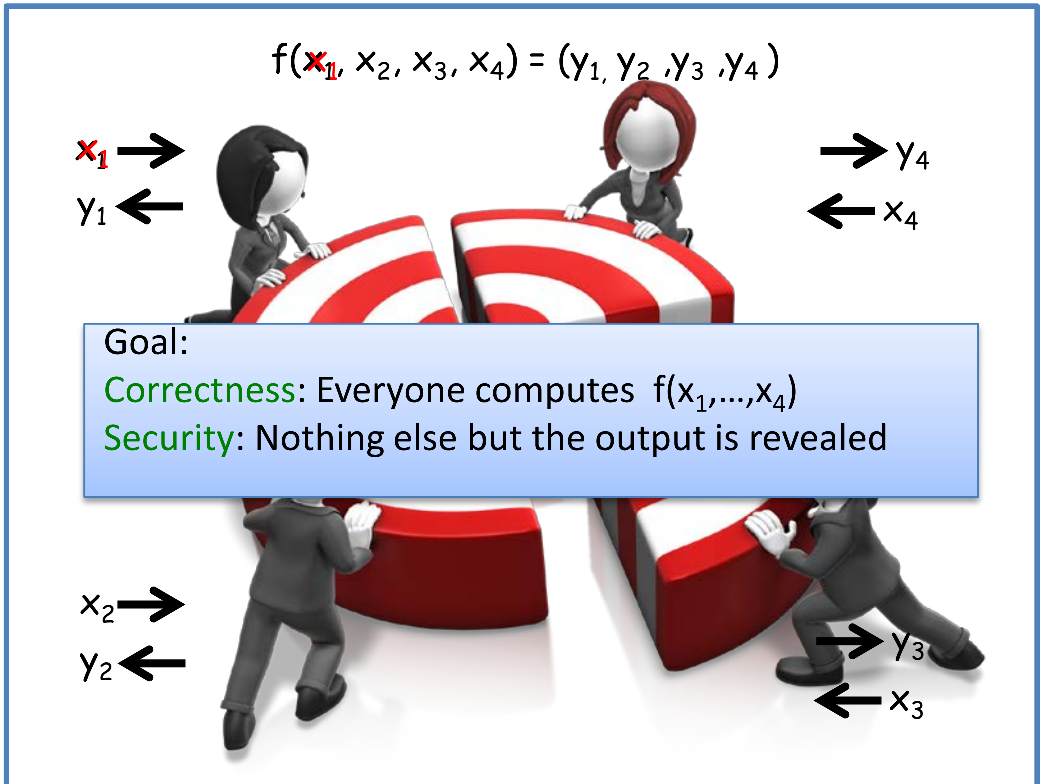
Round-Optimal Secure Multi-Party Computation

CRYPTO 2018

Shai Halevi, IBM
Carmit Hazay, Bar Ilan University
Antigoni Polychroniadou, Cornell Tech
Muthuramakrishnan Venkitasubramaniam, University of Rochester

Secure Multi-Party Computation (MPC)



Goal:

Correctness: Everyone computes $f(x_1,\ldots,x_4)$

Security: Nothing else but the output is revealed

Adversary

PPT

Malicious

Static

4-round

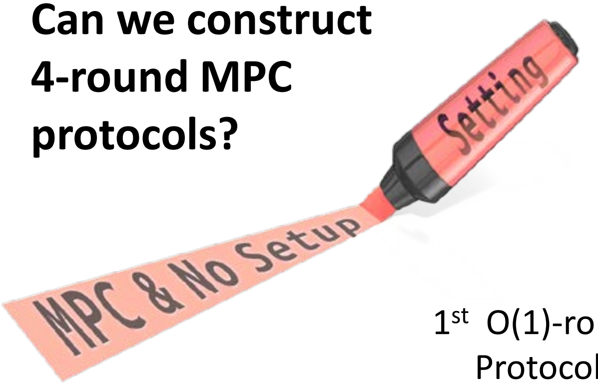
Can we construct ~~round optimal~~ MPC protocols?

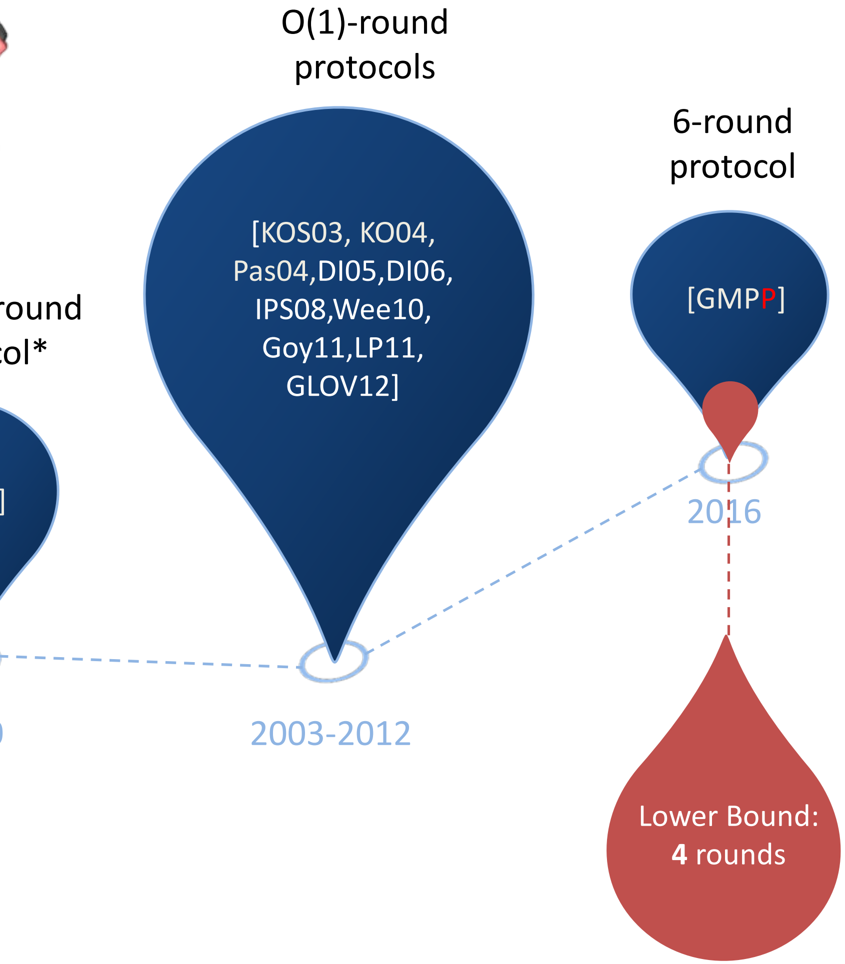
- ☑ Without setup
- ☑ In the presence of malicious adversaries
- ☑ Under standard (polytime) assumptions

[GMPP16]: 4 rounds are necessary with black box simulation

State-of-the-Art Until 2016

Can we construct 4-round MPC protocols?





*Honest majority

State-of-the-Art Since 2016

- ✗ Without setup (requires CRS)
- ✓ In the presence of malicious adversaries
- ✓ Under standard (polytime) assumptions

2-round: [MW16, BP16, PS16,GS17, GS18,BL18]

- ✓ Without setup
- ✗ In the presence of malicious adversaries
- ✓ Under standard (polytime) assumptions

2-round semi-malicious: [BL18,GS18] from DDH, QR,DCR

3-round semi-malicious: [BHP17] from LWE

- ✓ Without setup
- ✓ In the presence of malicious adversaries
- ✗ Under standard (polytime) assumptions

4-round: [ACJ17,BHP17]

- ✓ Without setup
- ✓ In the presence of malicious adversaries
- ✓ Under standard (polytime) assumptions

4-round 2PC and MPC coin-flipping: [COSV17a,b]

5-round: [ACJ17,BL18]

Can we construct 4-round MPC protocols?

Can we construct ~~round optimal~~ **4-round** MPC protocols?

- ☑ Without setup
- ☑ In the presence of malicious adversaries
- ☑ Under standard (polytime) assumptions

[GMPP16]: 4 rounds are necessary with black box simulation

Our Results

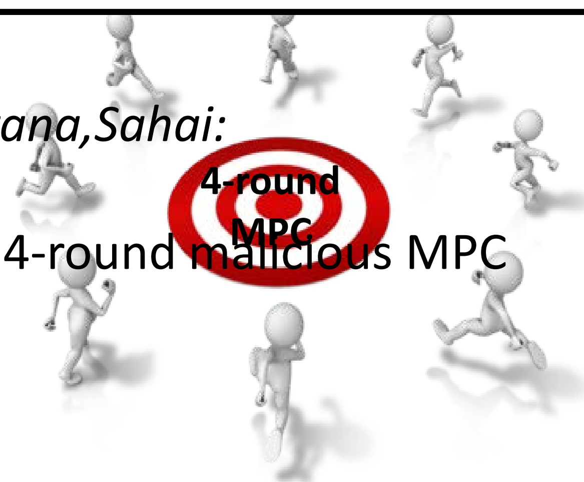
Theorem (informal)
Injective OWFs + ZAPS **+** AHE ➔ 4-round malicious MPC

Corollary (informal)
ETDP **+** QR/LWE/DDH/DCR ➔ 4-round malicious MPC

QR ➔ 4-round malicious MPC

Concurrent work *Badrinarayanan,Goyal,Jain,Kalai,Khurana,Sahai:*

Injective OWFs + dense cryptosystems + 2-round OT ➔ 4-round malicious MPC



MPC with Setup to MPC without Setup compilation

[GMP**P**16]:

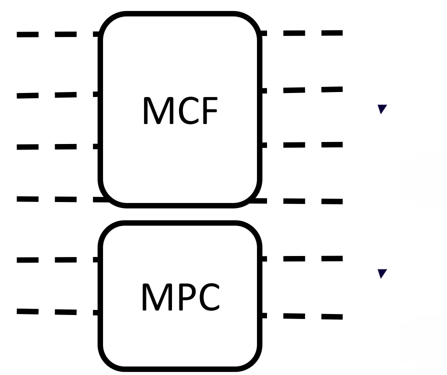
2-round malicious MPC in the CRS model [MW16,…]

+

4-round malicious multi-party coin flipping (MCF) [GMPP16,COSV17a]

↓

6-round malicious MPC



GMW paradigm compilation (1)

[ACJ17]:

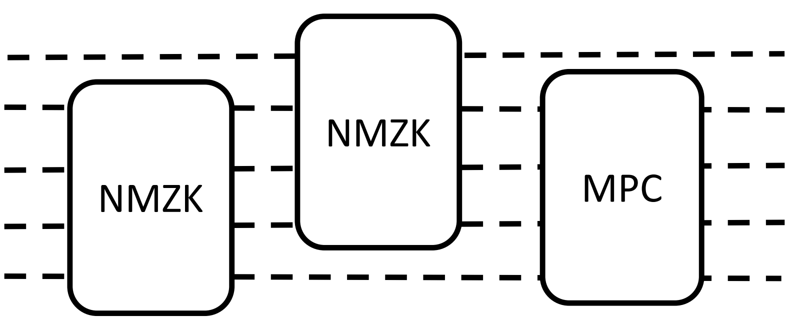
4-round semi-malicious MPC

+

Delayed input 4-round NMZK

⇓

5-round malicious MPC



[BL18]:

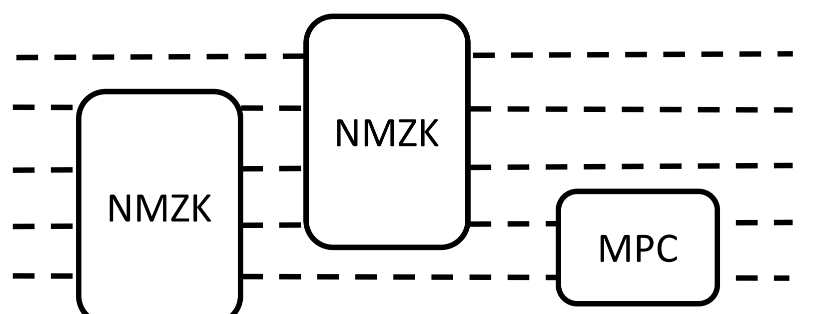
2-round semi-malicious MPC [GS18, BL18]

+

Delayed input 4-round NMZK

⇓

5-round malicious MPC



GMW paradigm compilation (2)

[ACJ17]:

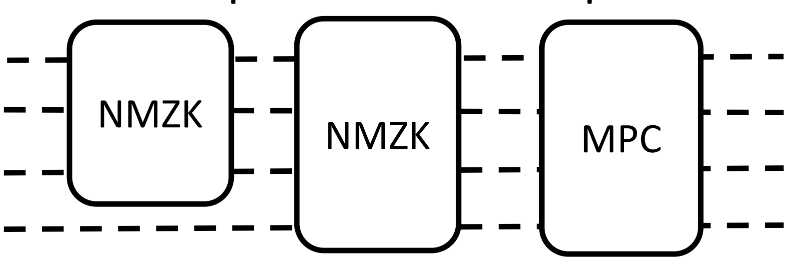
4-round semi-malicious MPC

+

Delayed input 3-round 'NMZK' with complexity leveraging

↓

4-round malicious MPC from sub-exponential assumptions



[BHP17]:

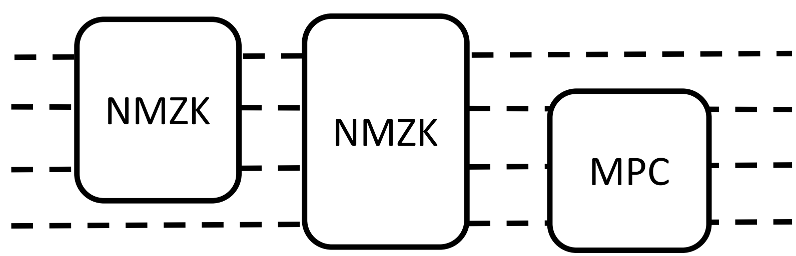
3-round semi-malicious MPC

+

Delayed input 3-round 'NMZK' with complexity leveraging

↓

4-round malicious MPC from sub-exponential assumptions



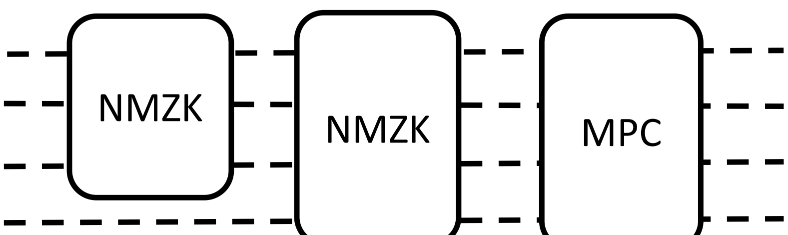
GMW paradigm compilation (2)

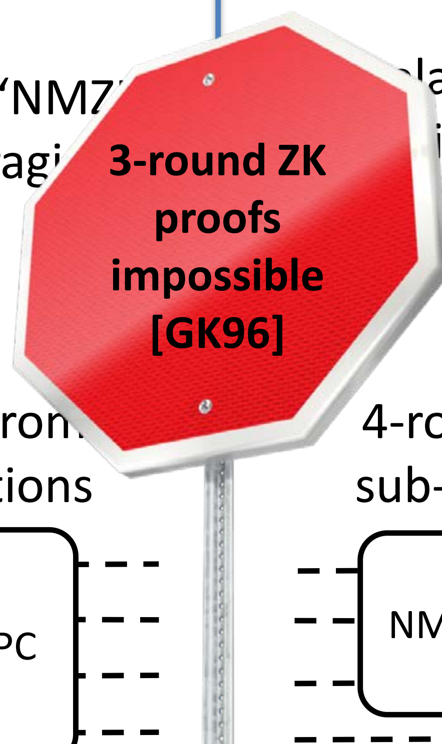
[ACJ17]:

4-round semi-malicious MPC

Delayed input 3-round 'NMZ
with complexity leveragi

4-round malicious MPC fro
sub-exponential assumptions



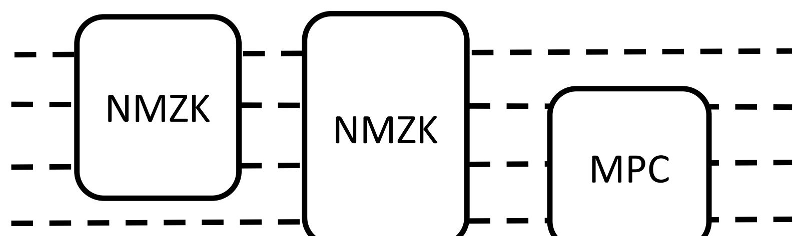


[BHP17]:

3-round semi-malicious MPC

layed input 3-round 'NMZK'
ith complexity leveraging

4-round malicious MPC from
sub-exponential assumptions



Our Approach: replace ZK by WI proofs in the 3rd round

Even if we use weaker tools, we still need to design a protocol that guarantees the same level of security.

Our Approach

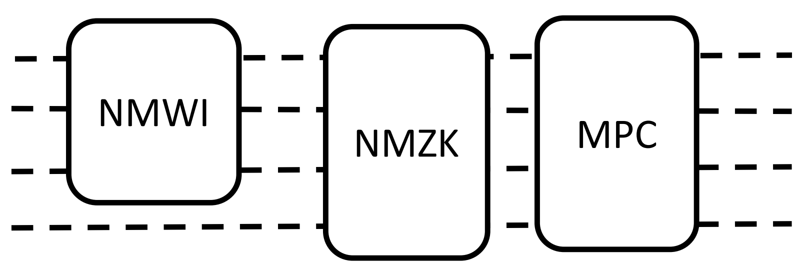
4-round WI-friendly
semi-malicious MPC

+

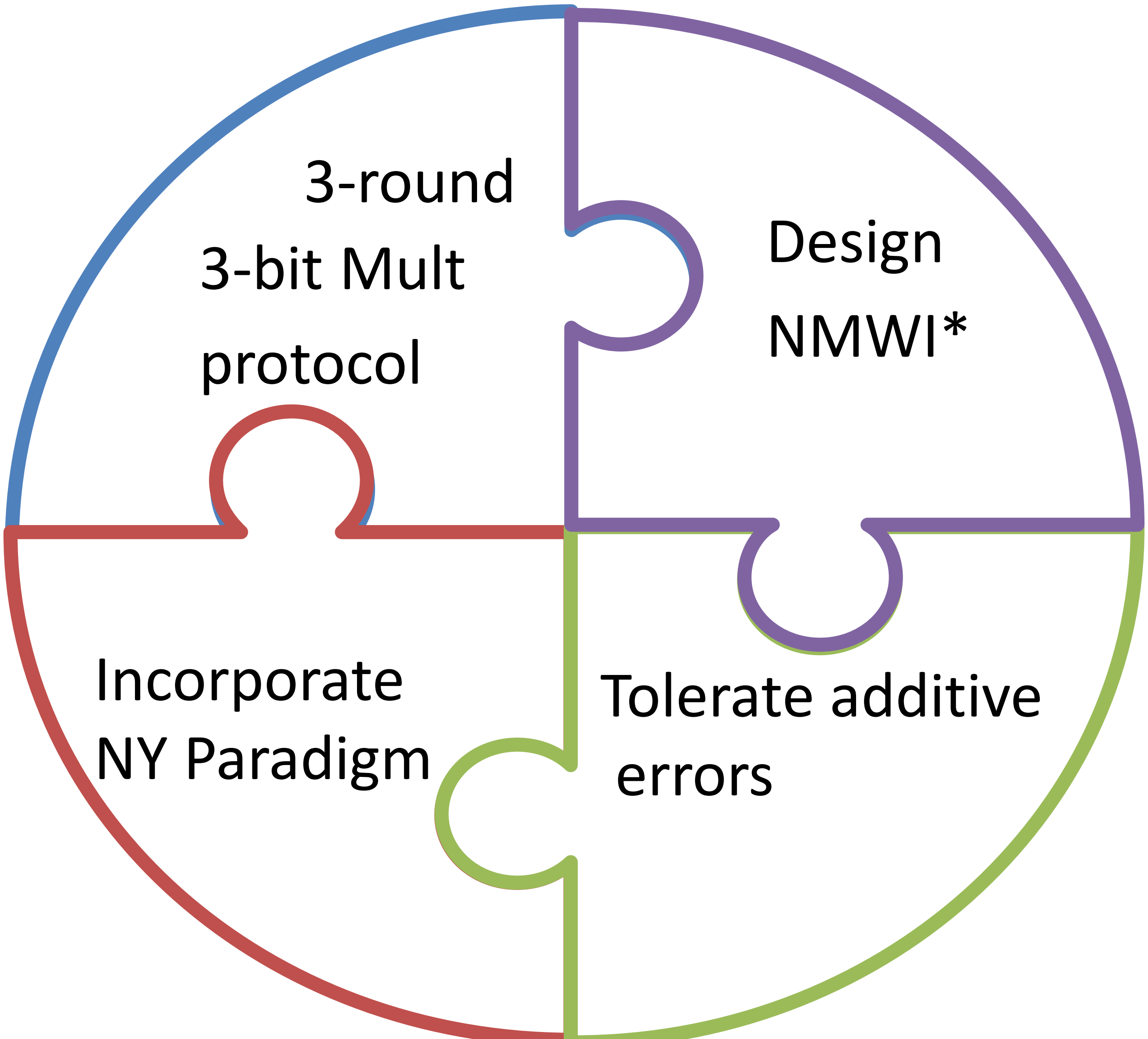
3-round NMWI primitive

↓

4-round malicious MPC



Our Approach *in a nutshell*

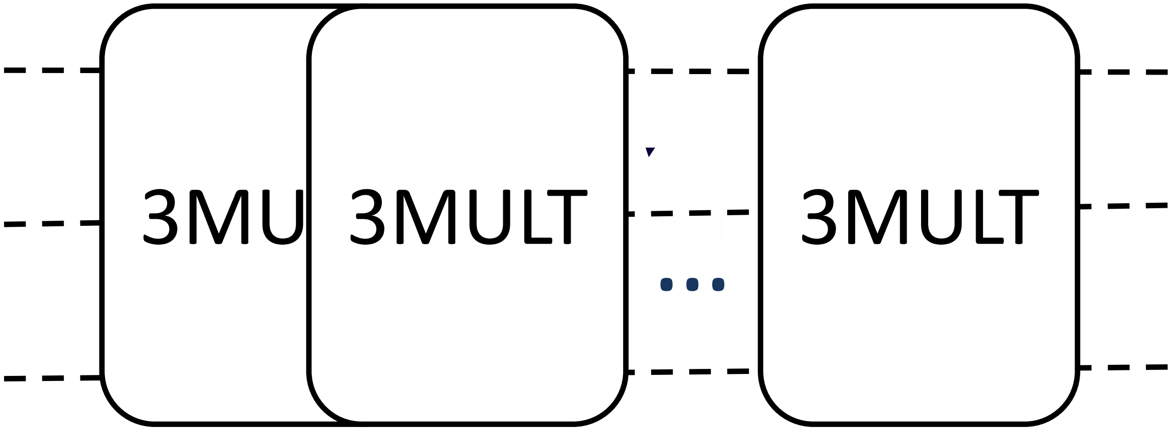


Our Approach *in a nutshell*

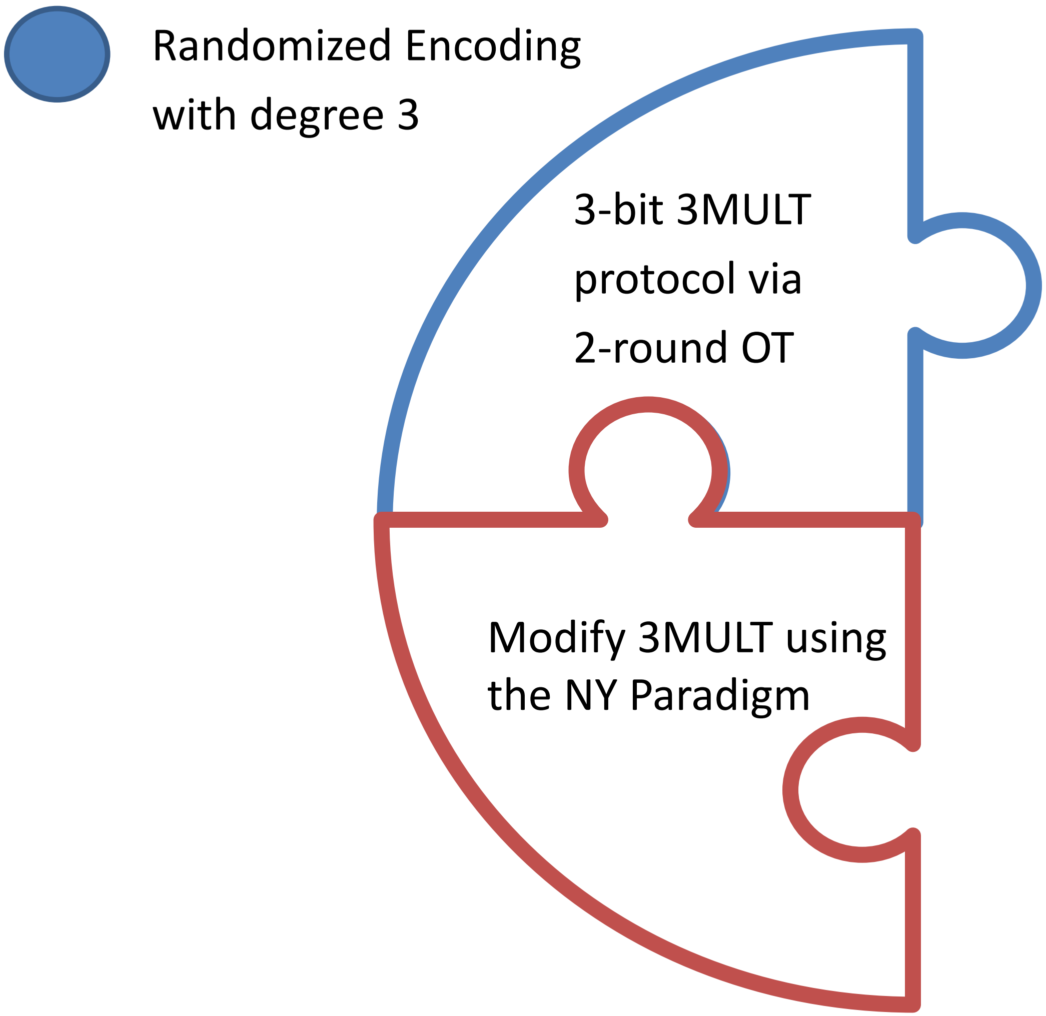
Secure comp. of f reduces to secure comp. of randomized encoding (RE) of f $[AIK06]$.

Q: Randomized Encoding with degree 3?

A: 3-bit multiplication protocol 3MULT based on 2-round OT [ACJ17]



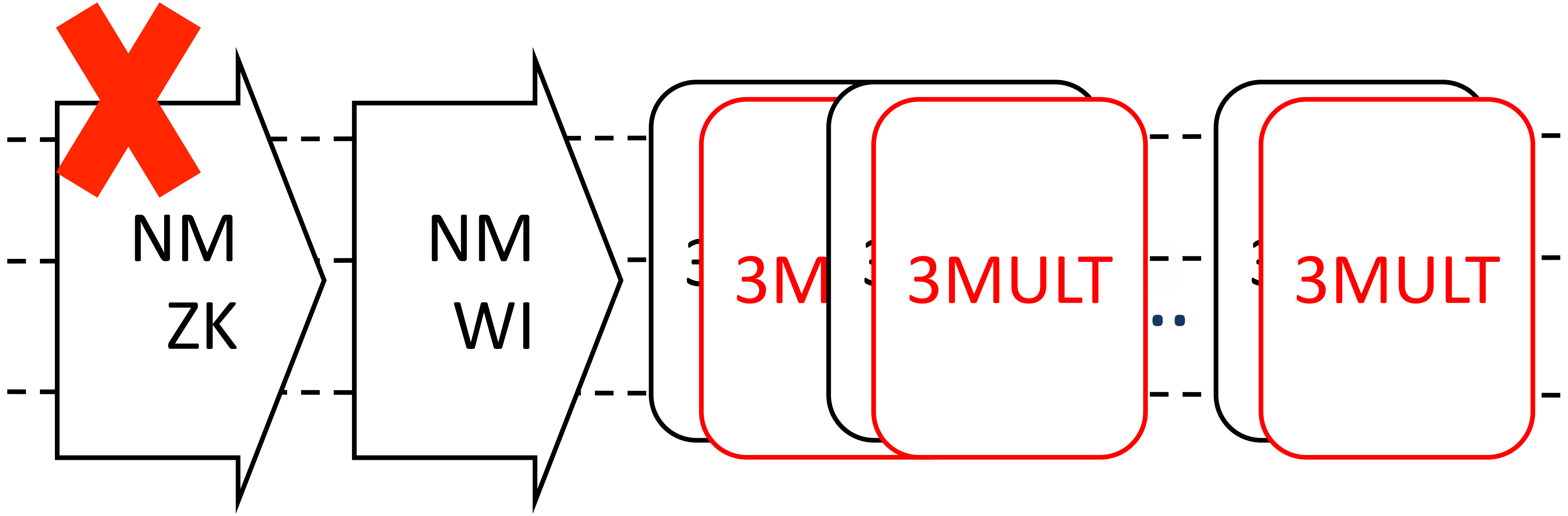
Our Approach *in a nutshell*



Our Approach *in a nutshell*

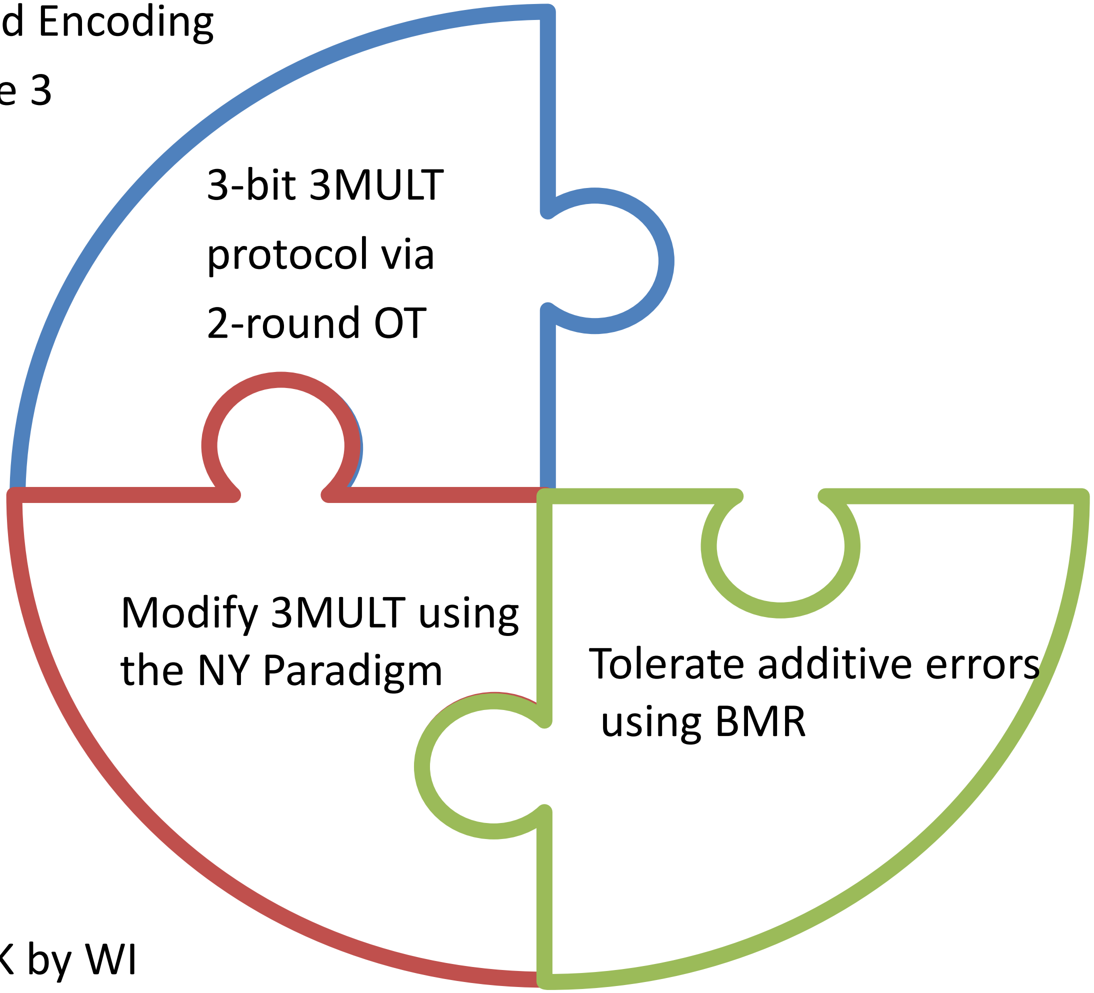
Q: Can we replace ZK by WI?
(Unlike ZK proofs, in WI proofs the simulator must follow the real prover strategy with a real witness)

A: Modify 3MULT using the Naor-Yung paradigm



Our Approach *in a nutshell*

Randomized Encoding with degree 3



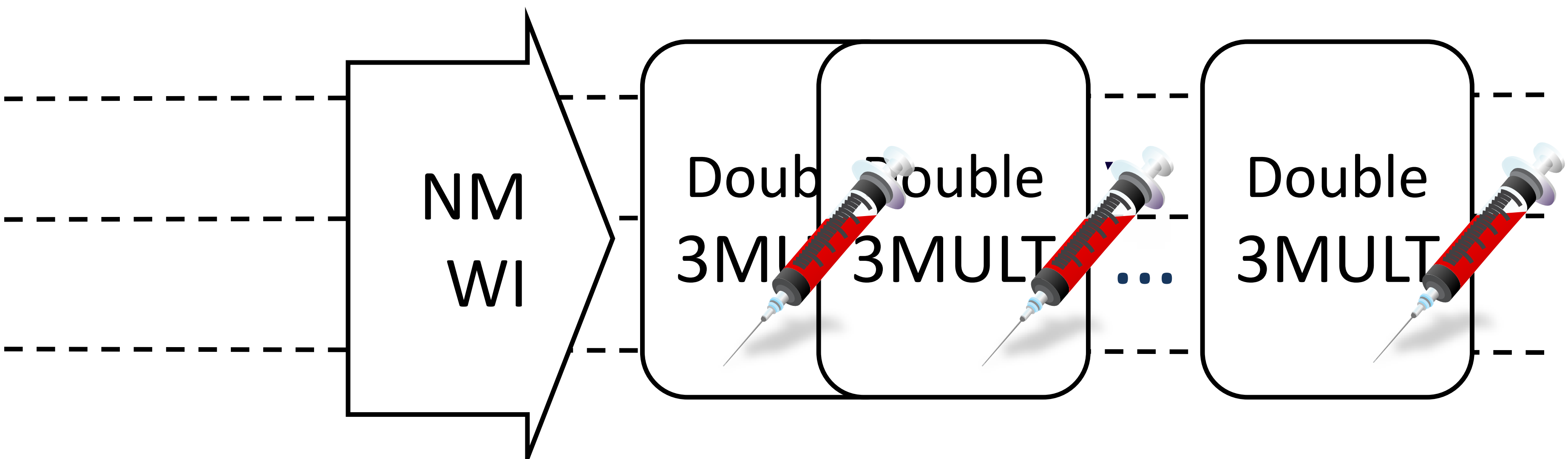
Replace ZK by WI

Our Approach *in a nutshell*

To accommodate WI proofs we need to weaken the correctness guarantees

Q: Can we protect against all adversarial attacks?

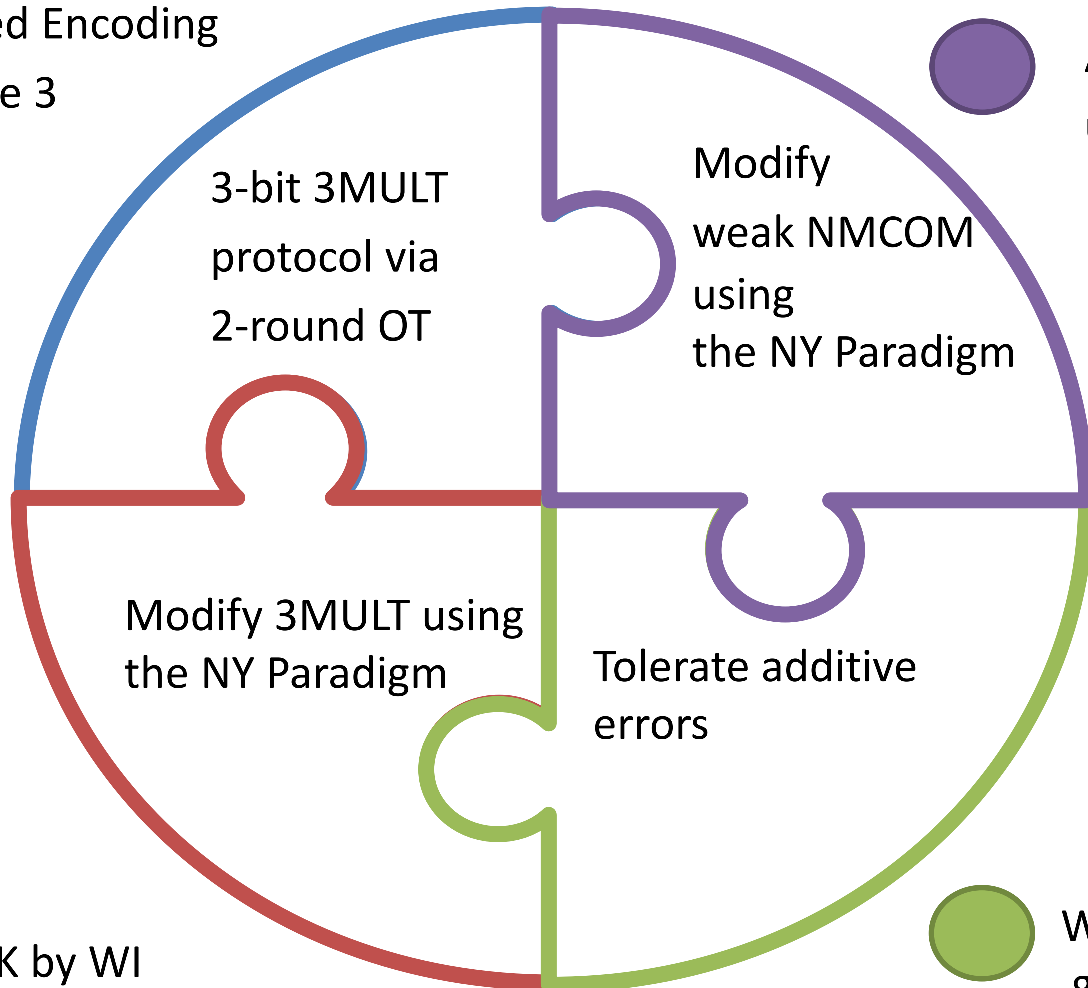
A: Adversary can include additive errors in the computation.



Our Approach *in a nutshell*

Randomized Encoding with degree 3

Achieve 'NMWI' using 3-round weak NMCOMs

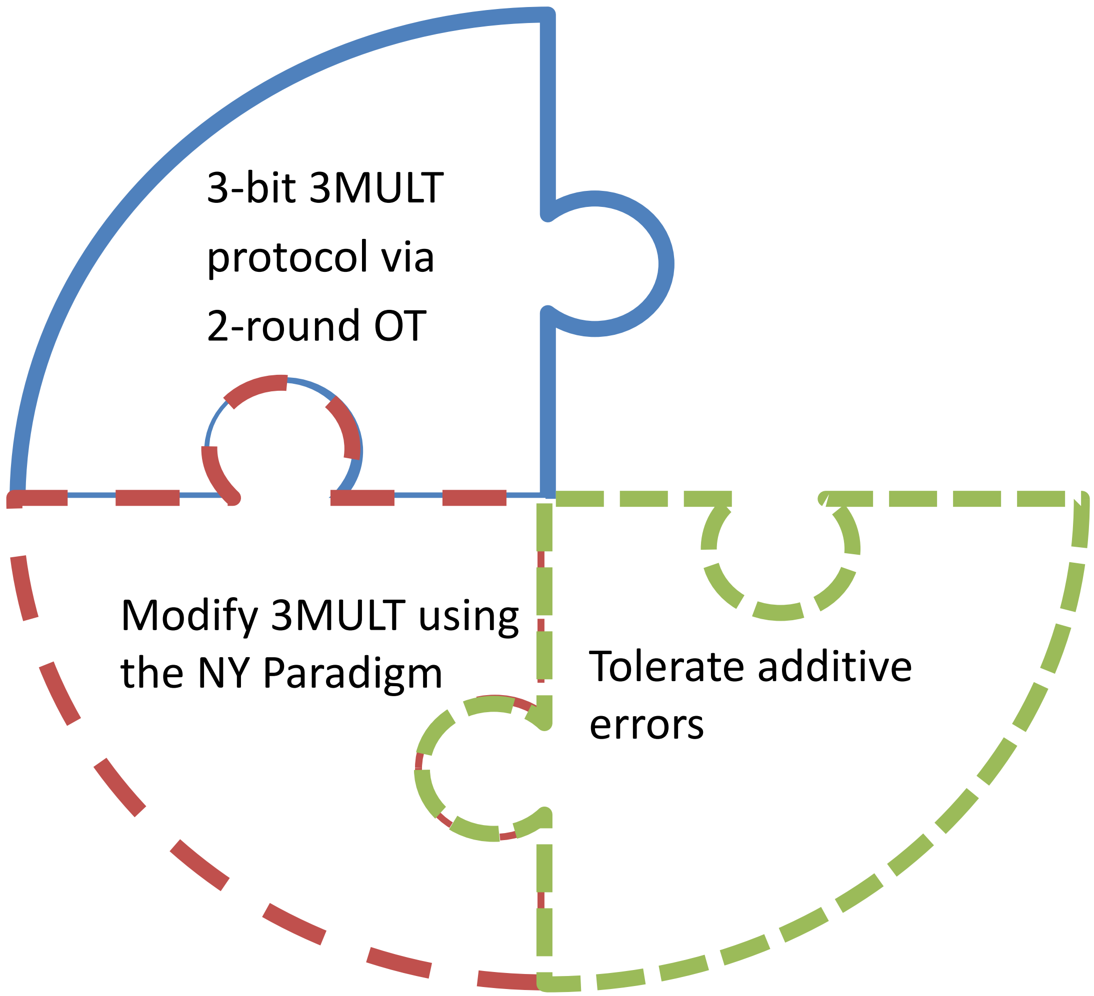


Replace ZK by WI

Weaken correctness guarantees in WI proofs do not protect against all adversarial attacks.

+ Require Sender Equivocal OT (via Additive HE)

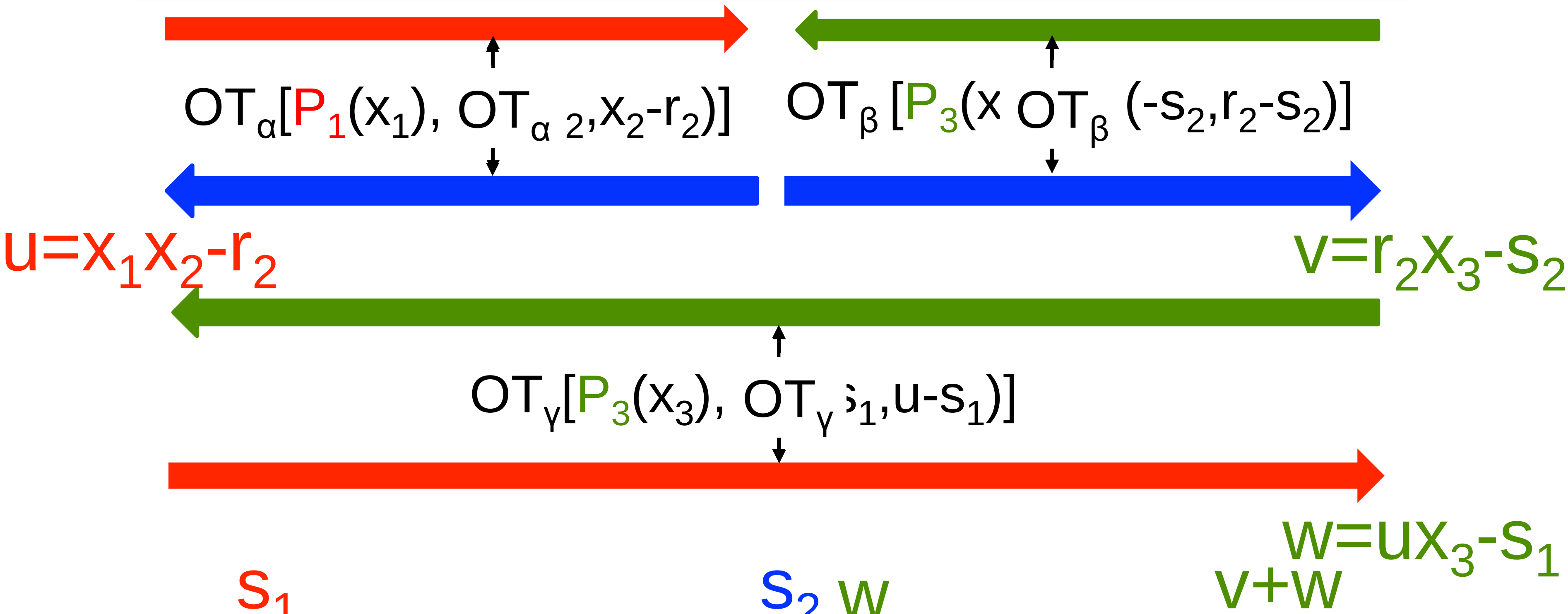
Outline



3-bit 3MULT protocol via 2-round OT
Modify 3MULT using the NY Paradigm
Tolerate additive errors

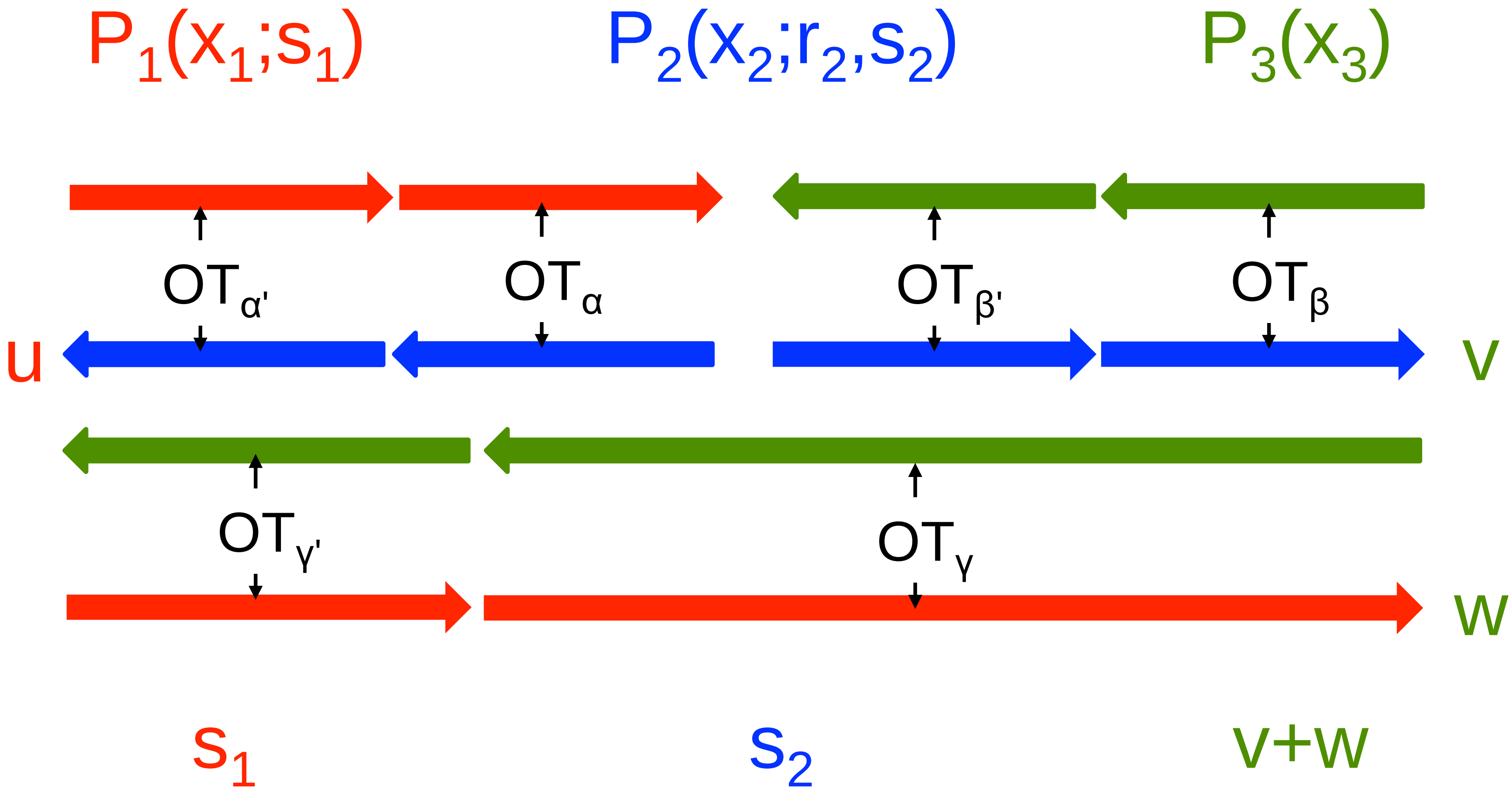
Starting Point: 3-party 3-bit multiplication protocol (3MULT) [Yuval+ACJ17]

Theorem (informal) [ACJ17]: Assuming 2-round OT, there is a 3-round 3-bit multiplication protocol



Output $s_2 + s_1 + \underbrace{r_2 x_3 - s_2}_{v} + \underbrace{(\underbrace{x_1 x_2 - r_2}_{u})\, x_3 - s_1}_{w} = x_1 x_2 x_3$

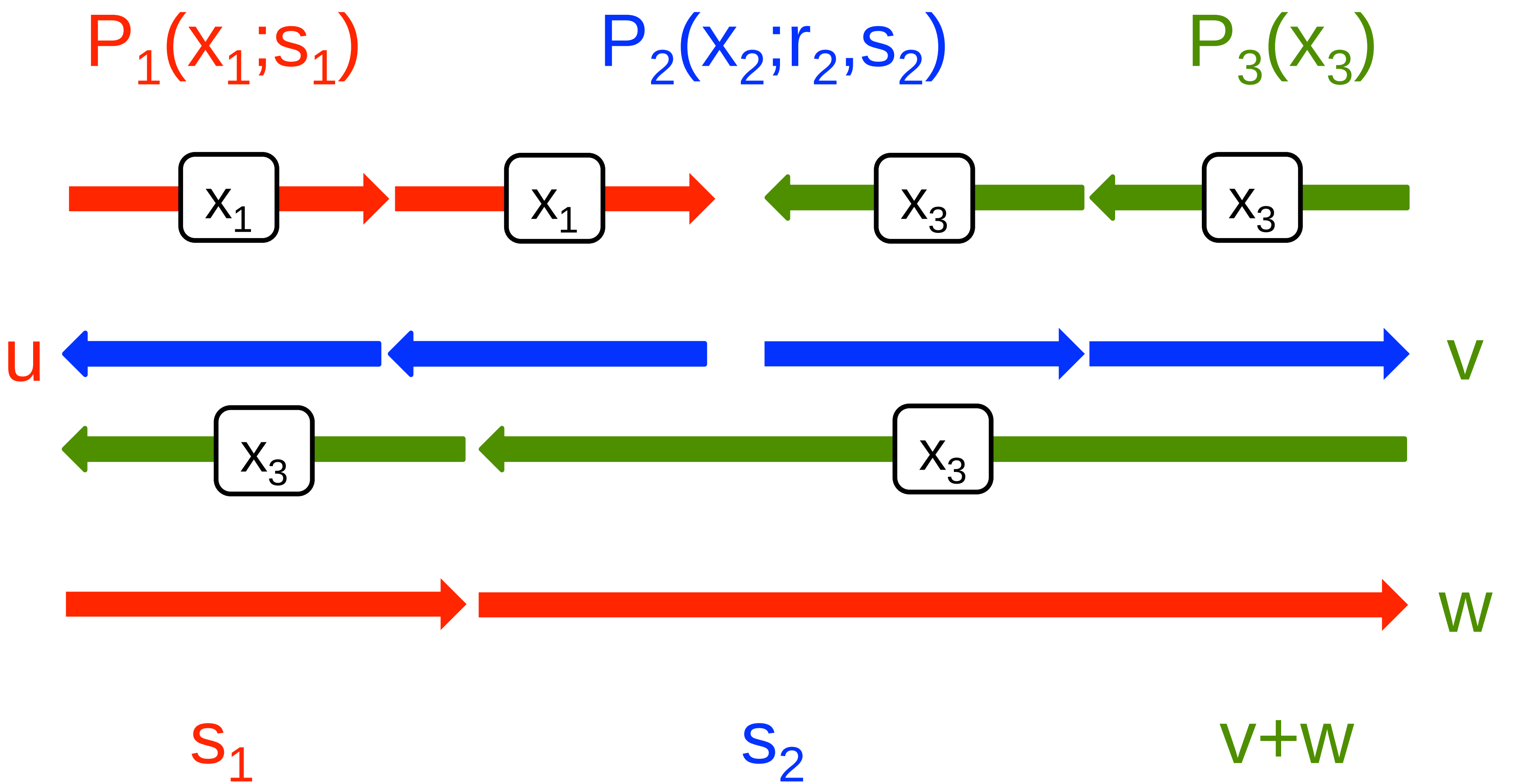
Double 3MULT using the NY Paradigm



Receiver sets **same input** in both OTs

Sender **secret shares** its input across the OTs

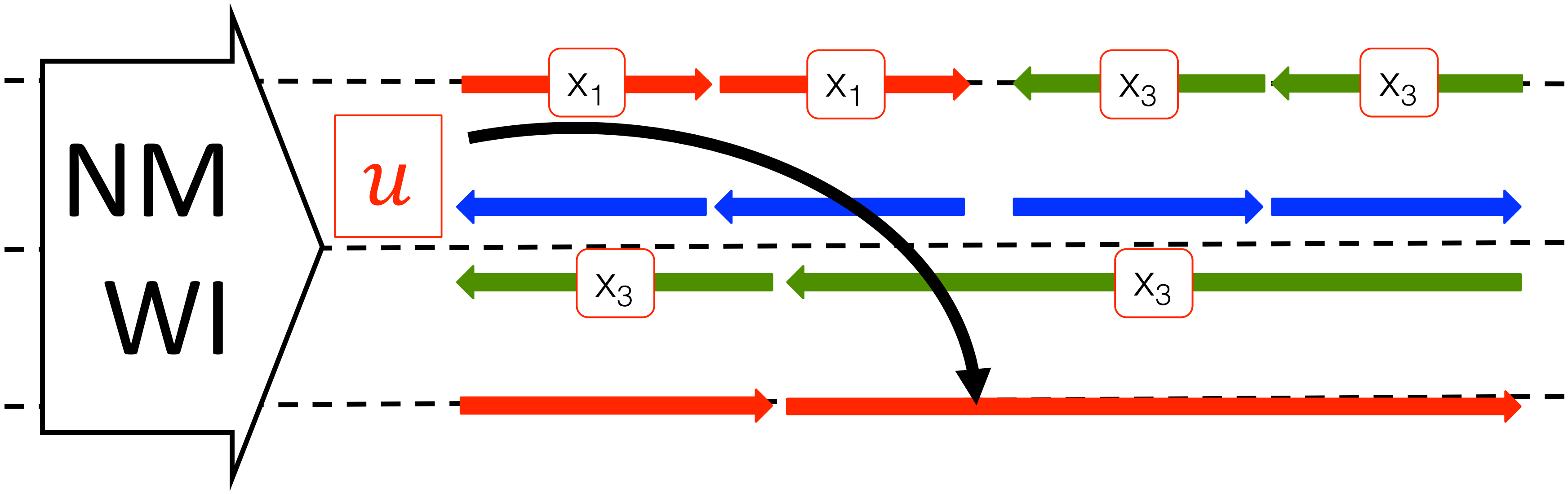
Double 3MULT using the NY Paradigm



Receiver sets **same input** in both OTs

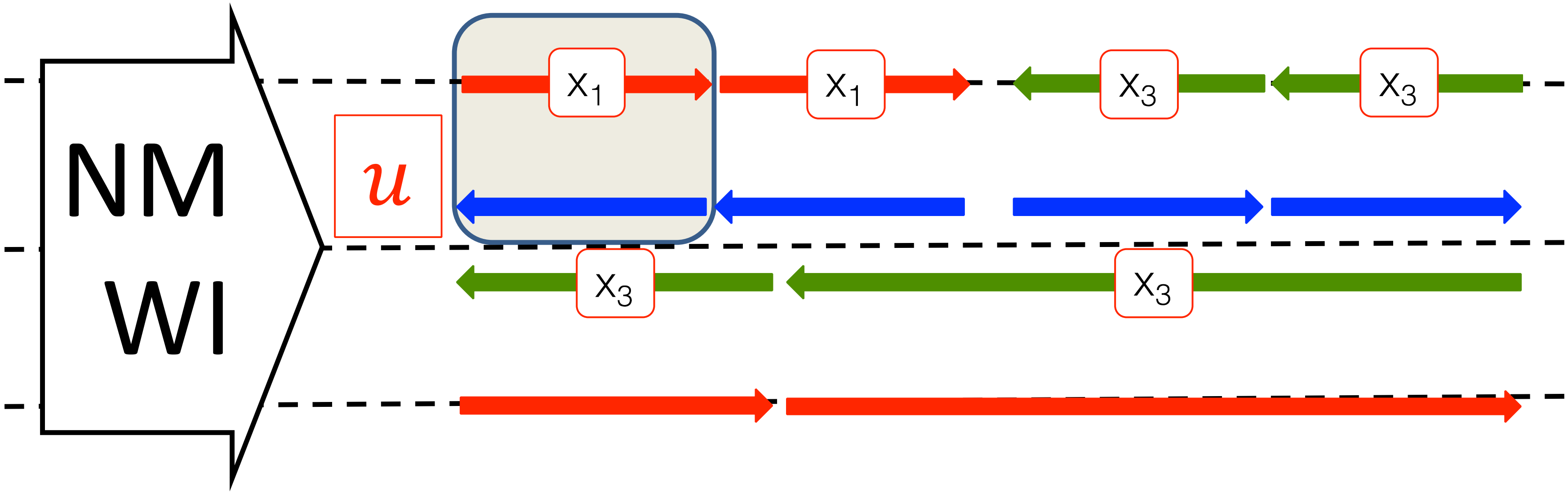
Sender **secret shares** its input across the OTs

Incorporating NMWI



There is a “u” problem

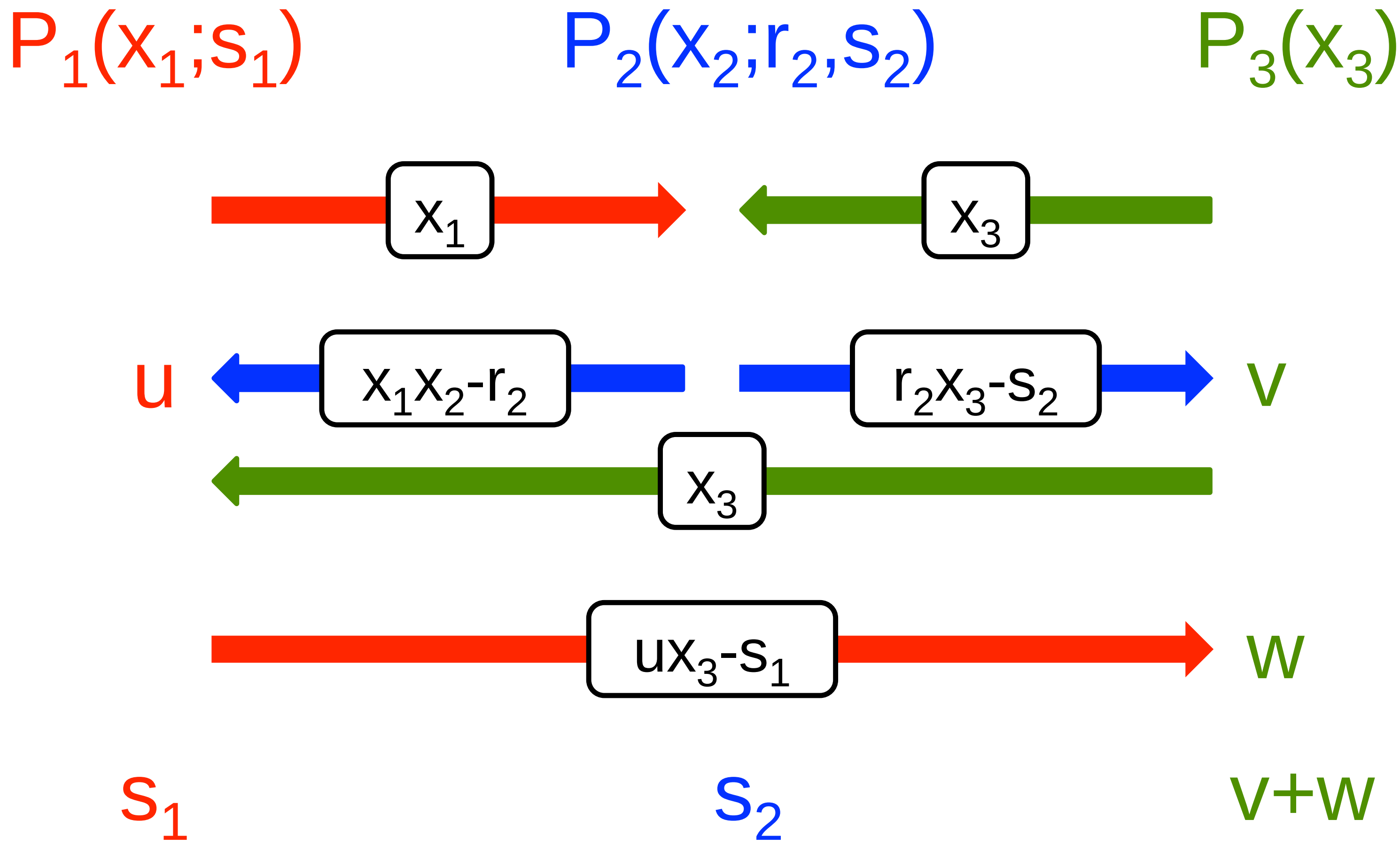
Incorporating NMWI



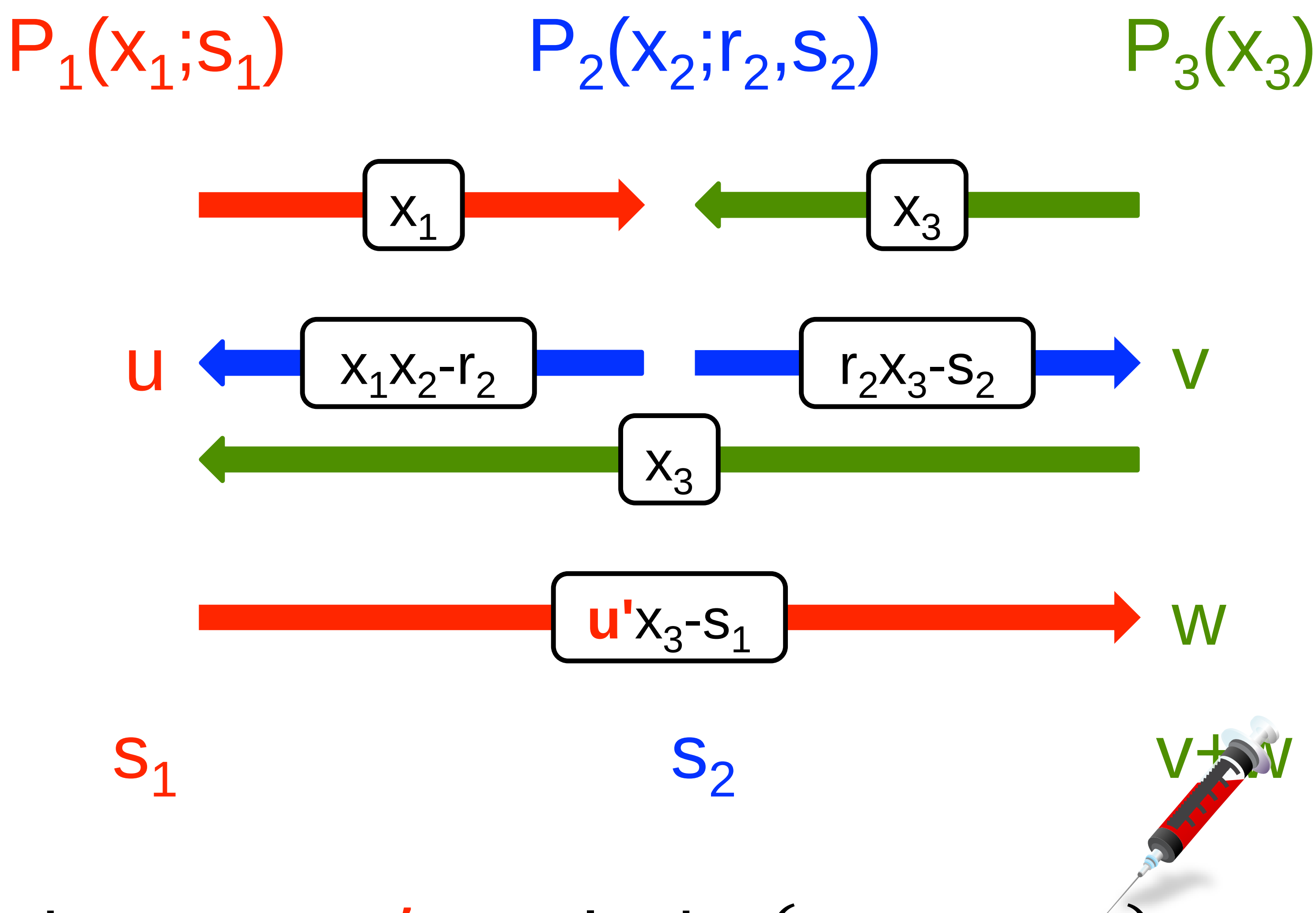
Problem: 3^{rd}-round message depends on u

Solution: Don't enforce correctness with u

So what if u is not correct



So what if u is not correct



An incorrect u' results in $(x_1 \cdot x_2 + e) \cdot x_3$

So what if u is not correct

$P_1(x_1;s_1)$ $P_2(x_2;r_2,s_2)$ $P_3(x_3)$

x_1 → ← x_3

Tolerating Additive errors using BMR

Choose ~~RE~~ Distributed Yao (BMR) and massage double 3MULT so that additive errors reduce to additive errors on the underlying computation.

An incorrect u' results in $(x_1 \cdot x_2 + u - u') \cdot x_3$

Conclusion

Round-optimal MPC protocol:

- ☑ Without setup
- ☑ In the presence of malicious adversaries
- ☑ Under standard (polytime) assumptions

Theorem (informal)

ETDP + QR/LWE/DDH/DCR ➔ 4-round malicious MPC

QR ➔ 4-round malicious MPC

Open Problems

4-round malicious MPC from minimal assumptions (4-round malicious OT)

With CRS: 2-round [GS18]

4-round malicious MPC in the *adaptive setting*

With CRS: 2-round [BLPV18]

[GS12] Adaptive security without setup requires non-black box techniques.

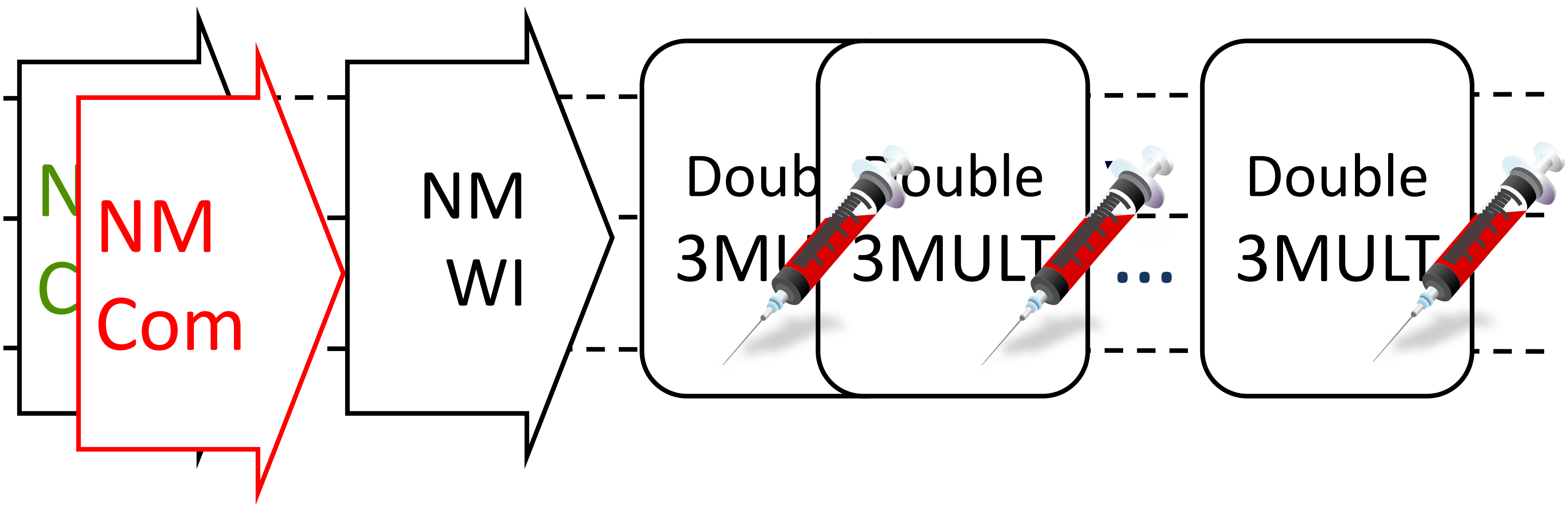
Tak!

Our Approach *in a nutshell*

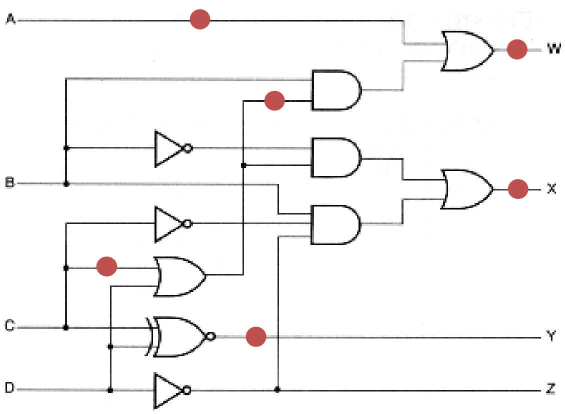
Q: How can we achieve extraction and WI with non-malleability guarantees?

A:

1. Extract via a 3-round weak non-malleable commitment [GRRV14]
2. Modify 3-round weak NMCOM using the Naor-Yung paradigm
3. Make weak NMCOM rewinding safe

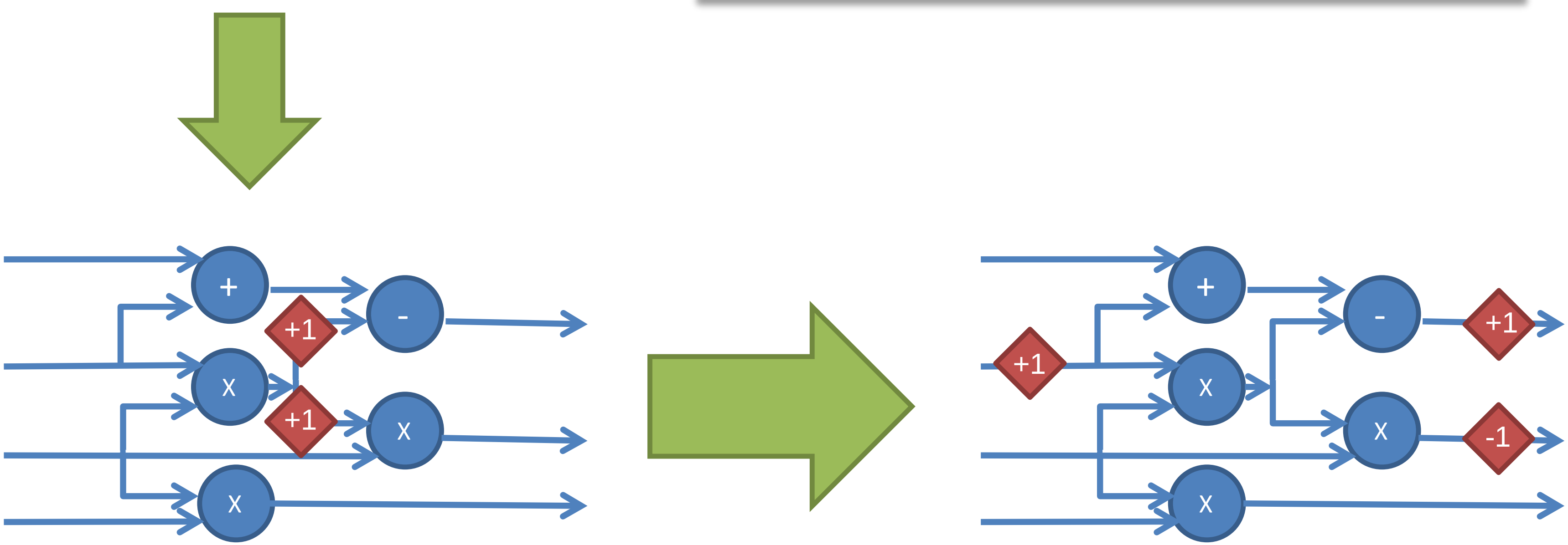


Circuits resilient to additive attacks [GIPST14,GIP15,GIW16]



C

Any additive attack on C’ translates to an equivalent additive attack on the inputs of C’



C’