

# Information-Theoretic 2-Round MPC without Round Collapsing: Adaptive Security, and More

Rachel Lin

University of Washington

Tianren Liu

University of Washington

Hoeteck Wee

NTT Research & ENS

TCC 2020

Information-Theoretic 2-Round MPC without Round  
Collapsing: Adaptive Security, and More

# Simple 2-Round MPC

Rachel Lin

University of Washington

Tianren Liu

University of Washington

Hoeteck Wee

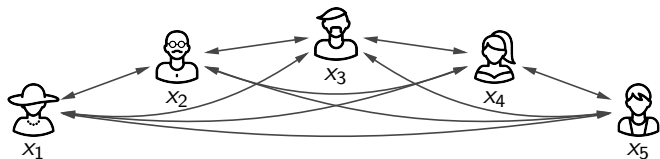
NTT Research & ENS

TCC 2020

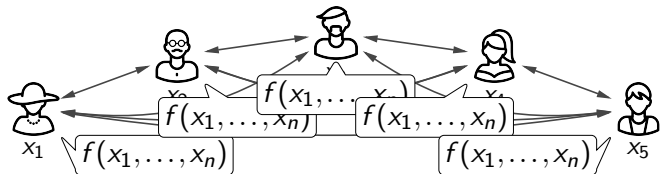
# Multi-Party Computation



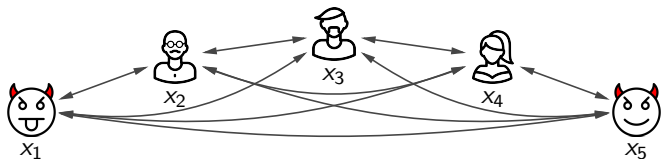
# Multi-Party Computation



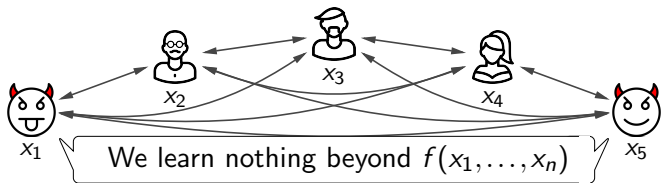
# Multi-Party Computation



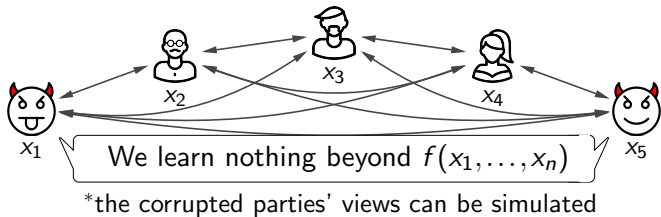
# Multi-Party Computation



# Multi-Party Computation

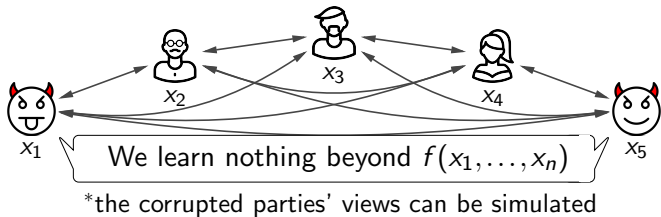


# Multi-Party Computation



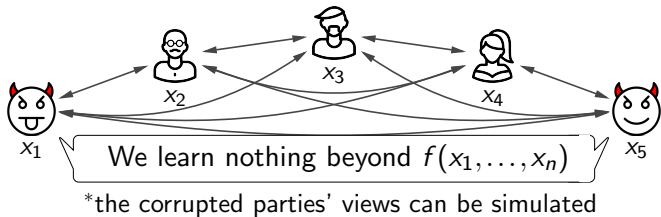


# Multi-Party Computation



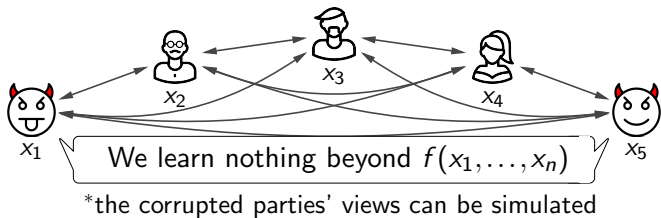
Adversary Semi-honest vs Malicious

# Multi-Party Computation



Adversary Semi-honest vs ~~Malicious~~

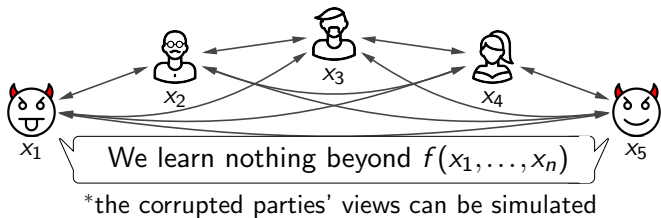
# Multi-Party Computation



Adversary Semi-honest vs ~~Malicious~~

Corruption Static vs Adaptive

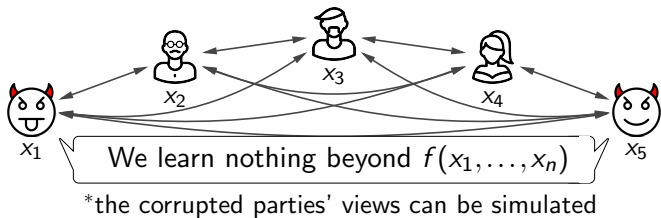
# Multi-Party Computation



Adversary Semi-honest vs ~~Malicious~~

Corruption ~~Static~~ vs Adaptive

# Multi-Party Computation

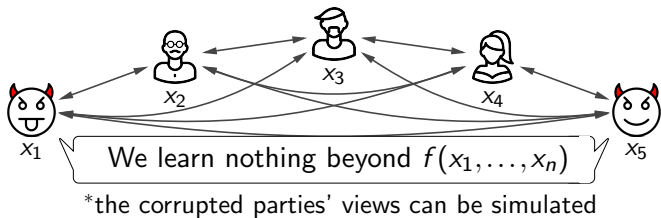


Adversary Semi-honest vs ~~Malicious~~

Corruption ~~Static~~ vs Adaptive

Security Computational vs Information-theoretic

# Multi-Party Computation

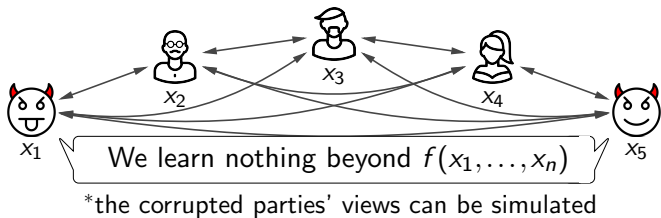


Adversary ~~Semi-honest~~ vs ~~Malicious~~

Corruption ~~Static~~ vs Adaptive

Security ~~Computational~~ vs Information-theoretic (NC1)

# Multi-Party Computation



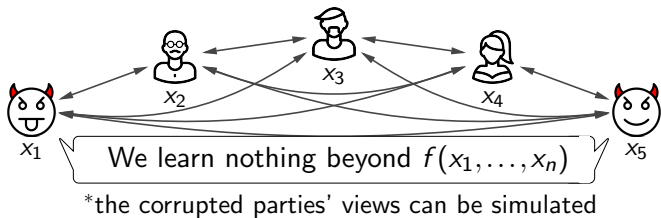
Adversary Semi-honest vs ~~Malicious~~

Corruption ~~Static~~ vs Adaptive

Security ~~Computational~~ vs Information-theoretic (NC1)

Computation Boolean vs Arithmetic

# Multi-Party Computation



Adversary ~~Semi-honest~~ vs ~~Malicious~~

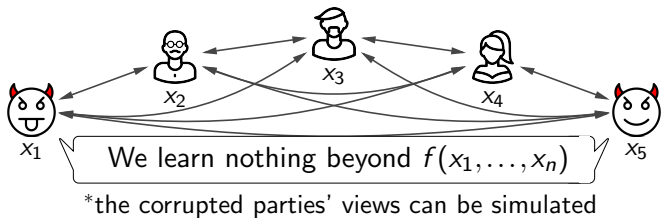
Corruption ~~Static~~ vs Adaptive

Security ~~Computational~~ vs Information-theoretic (NC1)

Computation ~~Boolean~~ vs Arithmetic (Black-box field)



# Multi-Party Computation



Adversary ~~Semi-honest~~ vs ~~Malicious~~

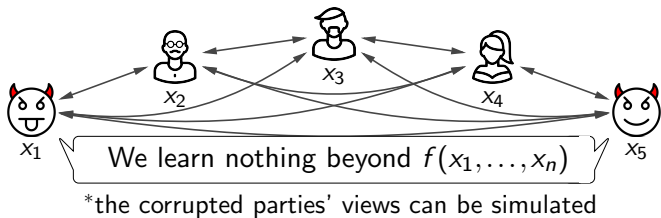
Corruption ~~Static~~ vs Adaptive

Security ~~Computational~~ vs Information-theoretic (NC1)

Computation ~~Boolean~~ vs Arithmetic (Black-box field)

Model

# Multi-Party Computation



Adversary ~~Semi-honest~~ vs ~~Malicious~~

Corruption ~~Static~~ vs Adaptive

Security ~~Computational~~ vs Information-theoretic (NC1)

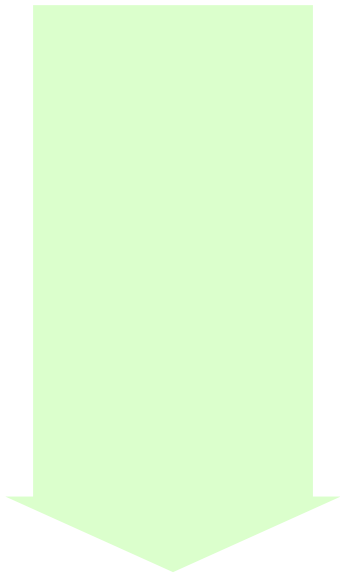
Computation ~~Boolean~~ vs Arithmetic (Black-box field)

Model Plain model, Correlated randomness model  
honest majority honest minority

# Optimal Round Complexity of Semi-Honest MPC

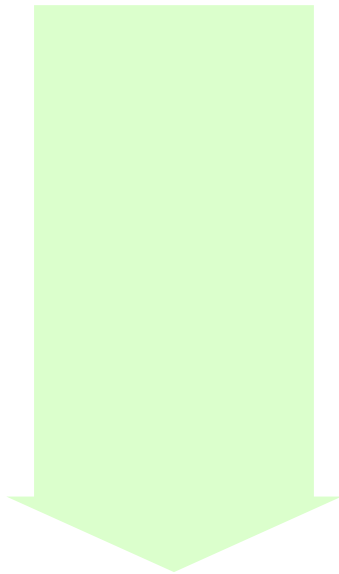
Honest majority

---



Honest minority

---





# Optimal Round Complexity of Semi-Honest MPC

Honest majority

[Yao,BGW,DI,BMR]

[IK00,IK02]

3-round & info-theoretic

Honest minority

3 rounds

2 rounds

# Optimal Round Complexity of Semi-Honest MPC

Honest majority

[Yao,BGW,DI,BMR]

[IK00,IK02]

3-round & info-theoretic

3 rounds

2 rounds

Honest minority

[GGHR14]

assume iO

# Optimal Round Complexity of Semi-Honest MPC

Honest majority

[Yao,BGW,DI,BMR]

[IK00,IK02]

3-round & info-theoretic

3 rounds

2 rounds

Honest minority

[GGHR14]

assume iO

[MW16]

MKFHE+CRS

# Optimal Round Complexity of Semi-Honest MPC

Honest majority

[Yao,BGW,DI,BMR]

[IK00,IK02]

3-round & info-theoretic

3 rounds

2 rounds

Honest minority

[GGHR14]

assume iO

[MW16]

MKFHE+CRS

[BL18,GS18]

2-round OT



# Optimal Round Complexity of Semi-Honest MPC

Honest majority

[Yao,BGW,DI,BMR]

[IK00,IK02]

3-round & info-theoretic

3 rounds

2 rounds

Honest minority

[GGHR14]

assume iO

[MW16]

MKFHE+CRS

[BL18,GS18]

2-round OT

[BLPV18,

GIS18,IMO18]

# Optimal Round Complexity of Semi-Honest MPC

Honest majority

[Yao,BGW,DI,BMR]

[IK00,IK02]

3-round & info-theoretic

[ACGJ18]  
assume OWF

Honest minority

3 rounds

2 rounds

[GGHR14]

assume iO

[MW16]

MKFHE+CRS

[BL18,GS18]

2-round OT

[BLPV18,  
GIS18,IMO18]

# Optimal Round Complexity of Semi-Honest MPC

Honest majority

[Yao,BGW,DI,BMR]

[IK00,IK02]

3-round & info-theoretic

[ACGJ18]  
assume OWF

[ABT18,GIS18]  
info-theoretic

3 rounds

2 rounds

Honest minority

[GGHR14]  
assume iO

[MW16]  
MKFHE+CRS

[BL18,GS18]  
2-round OT

[BLPV18,  
GIS18,IMO18]

# Optimal Round Complexity of Semi-Honest MPC

Honest majority

[Yao,BGW,DI,BMR]

[IK00,IK02]

3-round & info-theoretic

3 rounds

2 rounds

[ACGJ18]  
assume OWF

[ABT18,GIS18]  
info-theoretic

Honest minority

[GGHR14]  
assume iO

[MW16]  
MKFHE+CRS

[BL18,GS18]  
2-round OT

[BLPV18,  
GIS18,IMO18]

# Our Results

Honest majority

---

Honest minority

---

# Our Results

Honest majority

---

info-theoretic 2-round MPC for NC1

tolerating  $\lfloor \frac{n-1}{2} \rfloor$  corruptions

in plain model

Honest minority

---

## Our Results

### Honest majority

---

info-theoretic 2-round MPC for NC1  
tolerating  $\lfloor \frac{n-1}{2} \rfloor$  corruptions  
in plain model

### Honest minority

---

info-theoretic 2-round MPC for NC1  
tolerating  $n - 1$  corruptions  
in OLE correlated randomness model

# Our Results

## Honest majority

---

info-theoretic 2-round MPC for NC1  
tolerating  $\lfloor \frac{n-1}{2} \rfloor$  corruptions  
in plain model

## Honest minority

---

info-theoretic 2-round MPC for NC1  
tolerating  $n - 1$  corruptions  
in OLE correlated randomness model



# Our Results

Honest majority

---

info-theoretic 2-round MPC for NC1

tolerating  $\lfloor \frac{n-1}{2} \rfloor$  corruptions

in plain model

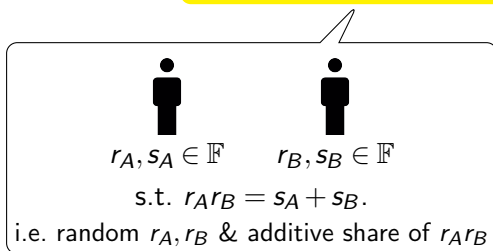
Honest minority

---

info-theoretic 2-round MPC for NC1

tolerating  $n - 1$  corruptions

in OLE correlated randomness model



# Our Results

## Honest majority

---

info-theoretic 2-round MPC for NC1

tolerating  $\lfloor \frac{n-1}{2} \rfloor$  corruptions

in plain model

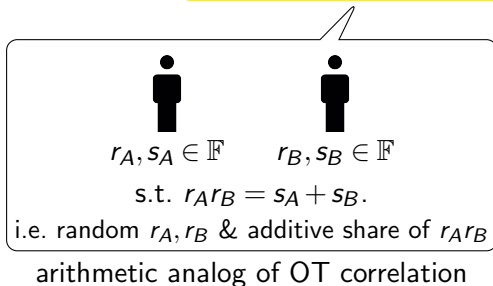
## Honest minority

---

info-theoretic 2-round MPC for NC1

tolerating  $n - 1$  corruptions

in OLE correlated randomness model



## Our Results

### Honest majority

---

info-theoretic 2-round MPC for NC1  
tolerating  $\lfloor \frac{n-1}{2} \rfloor$  corruptions  
in plain model

### Honest minority

---

info-theoretic 2-round MPC for NC1  
tolerating  $n - 1$  corruptions  
in OLE correlated randomness model

# Our Results

## Honest majority

---

info-theoretic 2-round MPC for NC1  
tolerating  $\lfloor \frac{n-1}{2} \rfloor$  corruptions  
in plain model

## Honest minority

---

info-theoretic 2-round MPC for NC1  
tolerating  $n - 1$  corruptions  
in OLE correlated randomness model

**Key Contribution: Simplicity**

# Our Results

## Honest majority

---

info-theoretic 2-round MPC for NC1  
tolerating  $\lfloor \frac{n-1}{2} \rfloor$  corruptions  
in plain model

## Honest minority

---

info-theoretic 2-round MPC for NC1  
tolerating  $n - 1$  corruptions  
in OLE correlated randomness model

### Key Contribution: Simplicity

- ▶ **new** adaptive security w/ explicit adaptive simulator\*

# Our Results

## Honest majority

---

info-theoretic 2-round MPC for NC1  
tolerating  $\lfloor \frac{n-1}{2} \rfloor$  corruptions  
in plain model

## Honest minority

---

info-theoretic 2-round MPC for NC1  
tolerating  $n - 1$  corruptions  
in OLE correlated randomness model

### Key Contribution: Simplicity

- ▶ **new** adaptive security w/ explicit adaptive simulator\*
- ▶ **new** support arithmetic NC1 w/ black-box field access

# Our Results

## Honest majority

---

info-theoretic 2-round MPC for NC1  
tolerating  $\lfloor \frac{n-1}{2} \rfloor$  corruptions  
in plain model

## Honest minority

---

info-theoretic 2-round MPC for NC1  
tolerating  $n - 1$  corruptions  
in OLE correlated randomness model

### Key Contribution: Simplicity

- ▶ **new** adaptive security w/ explicit adaptive simulator\*
- ▶ **new** support arithmetic NC1 w/ black-box field access
- ▶ more efficient

# Our Results

## Honest majority

---

info-theoretic 2-round MPC for NC1  
tolerating  $\lfloor \frac{n-1}{2} \rfloor$  corruptions  
in plain model

## Honest minority

---

info-theoretic 2-round MPC for NC1  
tolerating  $n - 1$  corruptions  
in OLE correlated randomness model

### Key Contribution: Simplicity

- ▶ **new** adaptive security w/ explicit adaptive simulator\*
- ▶ **new** support arithmetic NC1 w/ black-box field access
- ▶ more efficient

extension to P/poly with black-box use of PRG



# Our Results

## Honest majority

---

info-theoretic 2-round MPC for NC1  
tolerating  $\lfloor \frac{n-1}{2} \rfloor$  corruptions  
in plain model

## Honest minority

---

info-theoretic 2-round MPC for NC1  
tolerating  $n - 1$  corruptions  
in OLE correlated randomness model

### Key Contribution: Simplicity

- ▶ **new** adaptive security w/ explicit adaptive simulator\*
- ▶ **new** support arithmetic NC1 w/ black-box field access
- ▶ more efficient

extension to P/poly with black-box use of PRG

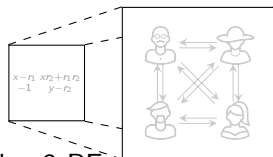
### Key Technique: Direct Construction w/o Round Collapsing

# What is Round Collapsing (here we illustrate the honest majority variant)

$$\begin{array}{cc} x-r_1 & x_2+r_1r_2 \\ -1 & y-r_2 \end{array}$$

deg-3 RE  
for NC1

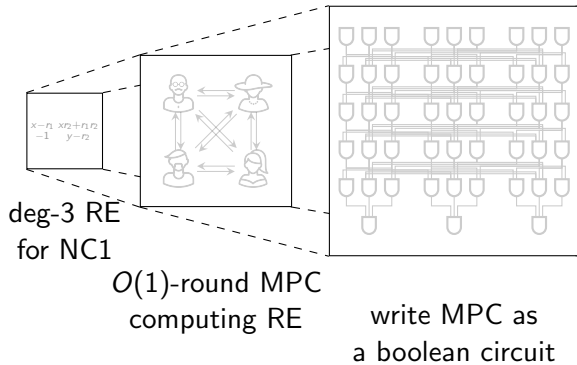
# What is Round Collapsing (here we illustrate the honest majority variant)



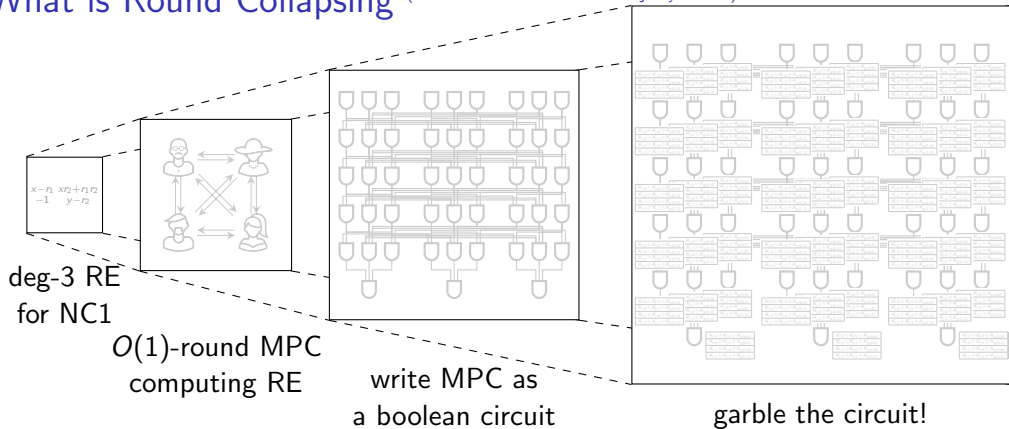
deg-3 RE  
for NC1

$O(1)$ -round MPC  
computing RE

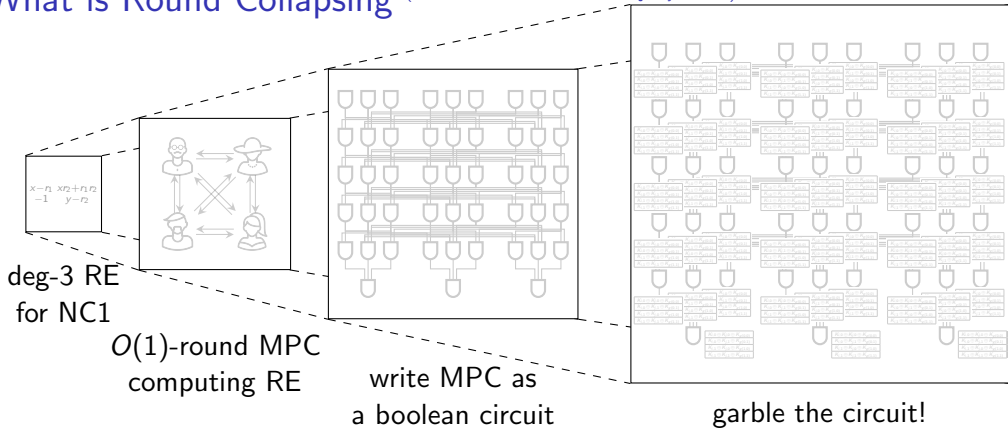
# What is Round Collapsing (here we illustrate the honest majority variant)



# What is Round Collapsing (here we illustrate the honest majority variant)



# What is Round Collapsing (here we illustrate the honest majority variant)

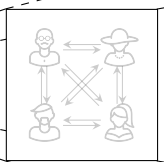


[ABT18]

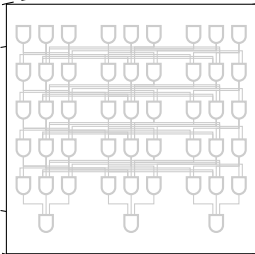
The garbled circuit is “effectively” degree-2 on *preprocessed* local input and randomness

# What is Round Collapsing (here we illustrate the honest majority variant)

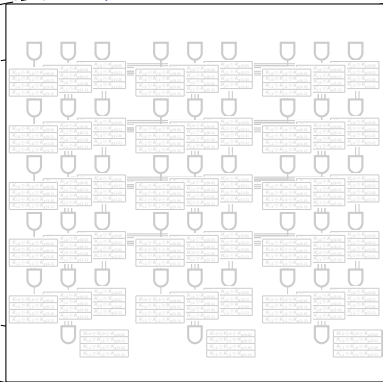
deg-3 RE  
for NC1



$O(1)$ -round MPC  
computing RE



write MPC as  
a boolean circuit



garble the circuit!

2-round BGW

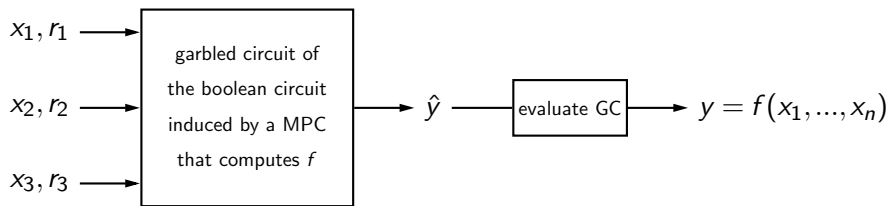


[ABT18]

The garbled circuit is  
"effectively" degree-2  
on *preprocessed*  
local input and randomness

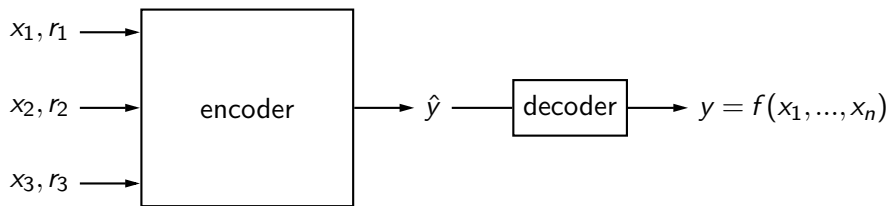
The garbled circuit  
can be computed  
by 2-round BGW  
assume honest major

## Multi-Party Randomized Encoding (MPRE) [ABT18]

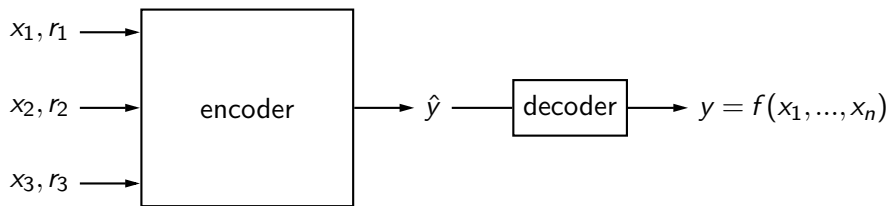




## Multi-Party Randomized Encoding (MPRE) [ABT18]

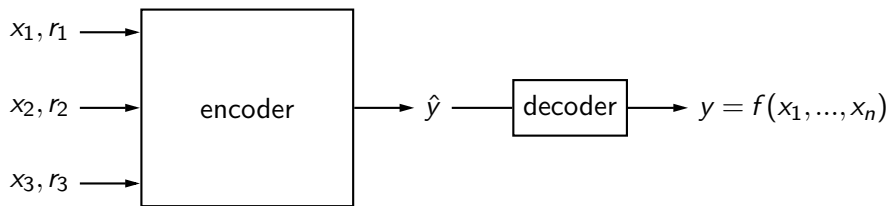


## Multi-Party Randomized Encoding (MPRE) [ABT18]



Correctness  $\hat{y}$  is decoded to  $f(x_1, \dots, x_n)$

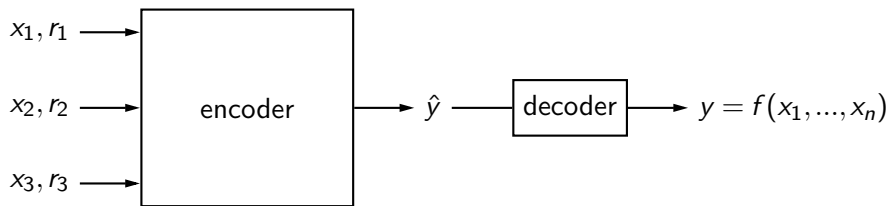
## Multi-Party Randomized Encoding (MPRE) [ABT18]



**Correctness**  $\hat{y}$  is decoded to  $f(x_1, \dots, x_n)$

**Privacy**  $\hat{y} \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n))$

## Multi-Party Randomized Encoding (MPRE) [ABT18]

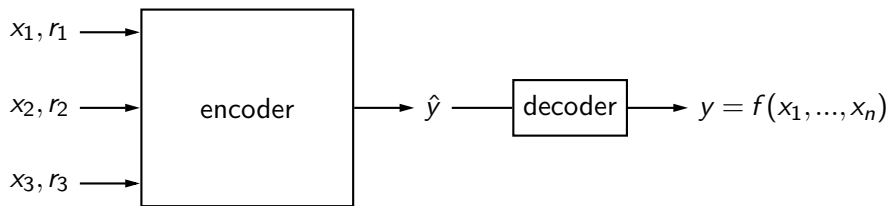


**Correctness**  $\hat{y}$  is decoded to  $f(x_1, \dots, x_n)$

**Privacy**  $\hat{y} \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n))$

**$t$ -Privacy**  $(\hat{y}, \underbrace{r_{i_1}, \dots, r_{i_t}}_{\text{up to threshold } t}) \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n), x_{i_1}, \dots, x_{i_t})$

# Multi-Party Randomized Encoding (MPRE) [ABT18]

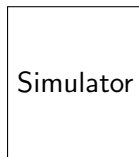
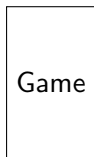


**Correctness**  $\hat{y}$  is decoded to  $f(x_1, \dots, x_n)$

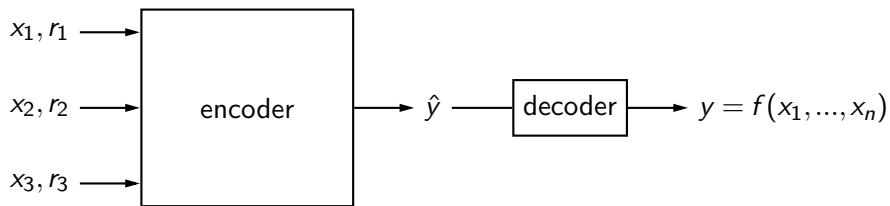
**Privacy**  $\hat{y} \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n))$

**$t$ -Privacy**  $(\hat{y}, \underbrace{r_{i_1}, \dots, r_{i_t}}_{\text{up to threshold } t}) \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n), x_{i_1}, \dots, x_{i_t})$

**Adaptive  $t$ -Privacy**



# Multi-Party Randomized Encoding (MPRE) [ABT18]

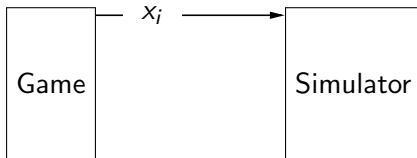


**Correctness**  $\hat{y}$  is decoded to  $f(x_1, \dots, x_n)$

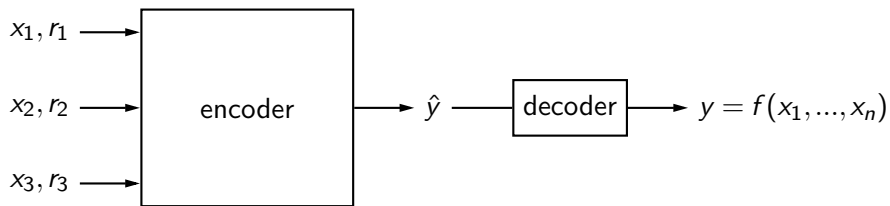
**Privacy**  $\hat{y} \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n))$

**$t$ -Privacy**  $(\hat{y}, \underbrace{r_{i_1}, \dots, r_{i_t}}_{\text{up to threshold } t}) \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n), x_{i_1}, \dots, x_{i_t})$

**Adaptive  $t$ -Privacy**



# Multi-Party Randomized Encoding (MPRE) [ABT18]

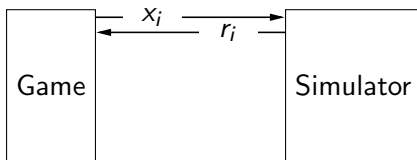


**Correctness**  $\hat{y}$  is decoded to  $f(x_1, \dots, x_n)$

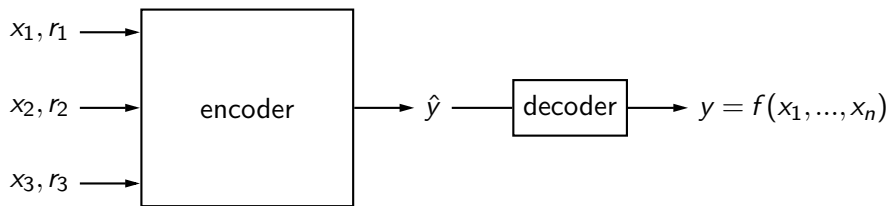
**Privacy**  $\hat{y} \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n))$

**$t$ -Privacy**  $(\hat{y}, \underbrace{r_{i_1}, \dots, r_{i_t}}_{\text{up to threshold } t}) \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n), x_{i_1}, \dots, x_{i_t})$

**Adaptive  $t$ -Privacy**



# Multi-Party Randomized Encoding (MPRE) [ABT18]

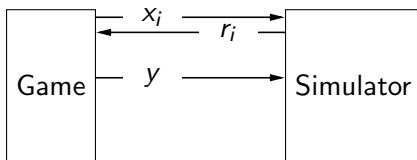


**Correctness**  $\hat{y}$  is decoded to  $f(x_1, \dots, x_n)$

**Privacy**  $\hat{y} \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n))$

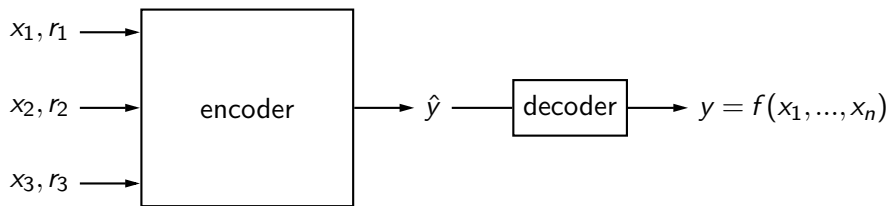
**$t$ -Privacy**  $(\hat{y}, \underbrace{r_{i_1}, \dots, r_{i_t}}_{\text{up to threshold } t}) \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n), x_{i_1}, \dots, x_{i_t})$

**Adaptive  $t$ -Privacy**





# Multi-Party Randomized Encoding (MPRE) [ABT18]

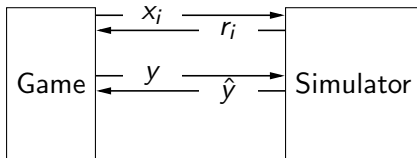


**Correctness**  $\hat{y}$  is decoded to  $f(x_1, \dots, x_n)$

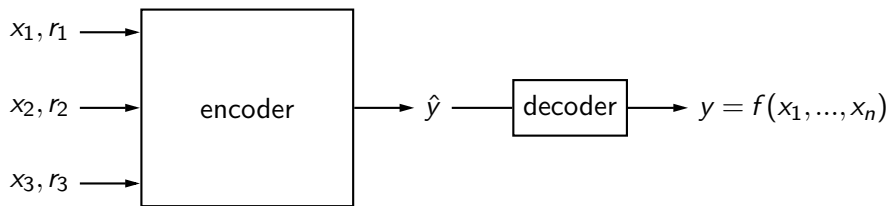
**Privacy**  $\hat{y} \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n))$

**$t$ -Privacy**  $(\hat{y}, \underbrace{r_{i_1}, \dots, r_{i_t}}_{\text{up to threshold } t}) \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n), x_{i_1}, \dots, x_{i_t})$

**Adaptive  $t$ -Privacy**



# Multi-Party Randomized Encoding (MPRE) [ABT18]

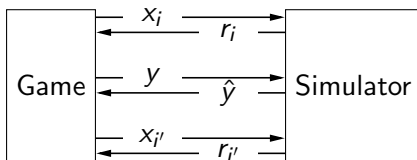


**Correctness**  $\hat{y}$  is decoded to  $f(x_1, \dots, x_n)$

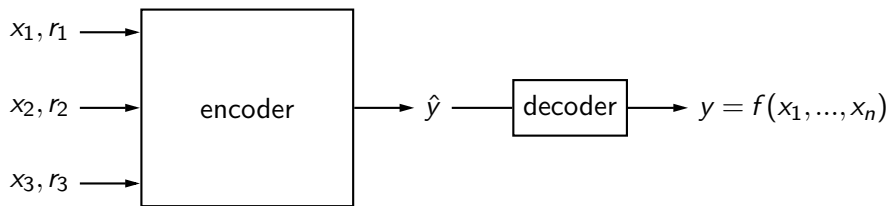
**Privacy**  $\hat{y} \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n))$

**$t$ -Privacy**  $(\hat{y}, \underbrace{r_{i_1}, \dots, r_{i_t}}_{\text{up to threshold } t}) \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n), x_{i_1}, \dots, x_{i_t})$

**Adaptive  $t$ -Privacy**



## Multi-Party Randomized Encoding (MPRE) [ABT18]

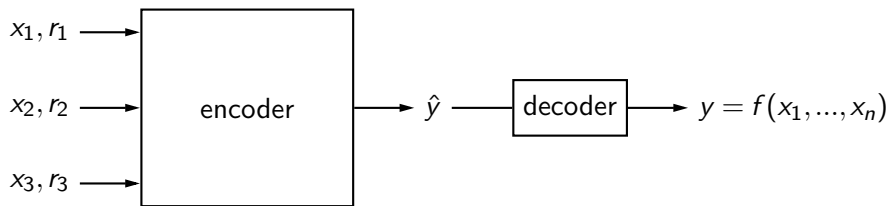


**Correctness**  $\hat{y}$  is decoded to  $f(x_1, \dots, x_n)$

**Privacy**  $\hat{y} \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n))$

**$t$ -Privacy**  $(\hat{y}, \underbrace{r_{i_1}, \dots, r_{i_t}}_{\text{up to threshold } t}) \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n), x_{i_1}, \dots, x_{i_t})$

## Multi-Party Randomized Encoding (MPRE) [ABT18]



**Correctness**  $\hat{y}$  is decoded to  $f(x_1, \dots, x_n)$

**Privacy**  $\hat{y} \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n))$

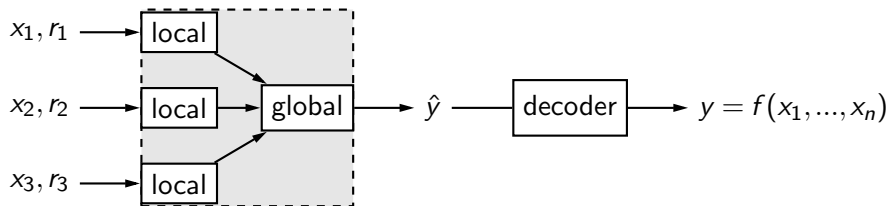
**$t$ -Privacy**  $(\hat{y}, \underbrace{r_{i_1}, \dots, r_{i_t}}_{\text{up to threshold } t}) \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n), x_{i_1}, \dots, x_{i_t})$



[IK00]

$\forall$  encoder has  
degree  $\geq 3$

# Multi-Party Randomized Encoding (MPRE) [ABT18]



**Correctness**  $\hat{y}$  is decoded to  $f(x_1, \dots, x_n)$

**Privacy**  $\hat{y} \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n))$

**$t$ -Privacy**  $(\hat{y}, \underbrace{r_{i_1}, \dots, r_{i_t}}_{\text{up to threshold } t}) \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n), x_{i_1}, \dots, x_{i_t})$



[IK00]

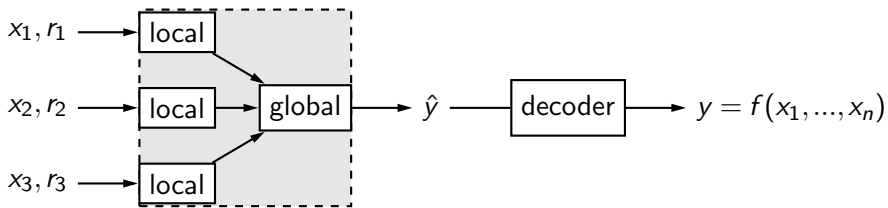
∇ encoder has  
degree  $\geq 3$

local pre-processing  
& global computation



[ABT18]

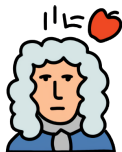
# Multi-Party Randomized Encoding (MPRE) [ABT18]



**Correctness**  $\hat{y}$  is decoded to  $f(x_1, \dots, x_n)$

**Privacy**  $\hat{y} \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n))$

**$t$ -Privacy**  $(\hat{y}, \underbrace{r_{i_1}, \dots, r_{i_t}}_{\text{up to threshold } t}) \stackrel{d}{=} \text{Sim}(f(x_1, \dots, x_n), x_{i_1}, \dots, x_{i_t})$



[IK00]

$\forall$  encoder has  
degree  $\geq 3$

$\exists$  encoder has degree 2  
after pre-processing



[ABT18]

## Multi-Party Randomized Encoding (MPRE) [ABT18]

Theorem  
[ABT10]

degree-2 MPRE  
for NC1

+

2-round MPC  
for degree-2 poly

$\Rightarrow$

2-round MPC  
for NC1

# Multi-Party Randomized Encoding (MPRE) [ABT18]

Theorem  
[ABT10]

degree-2 MPRE  
for NC1

+

2-round MPC  
for degree-2 poly

$\Rightarrow$

2-round MPC  
for NC1

Proof.



$x_1$



$x_2$



$x_3$



$x_4$



$x_5$



# Multi-Party Randomized Encoding (MPRE) [ABT18]

Theorem  
[ABT10]

degree-2 MPRE  
for NC1

+

2-round MPC  
for degree-2 poly

$\Rightarrow$

2-round MPC  
for NC1

Proof.



$x_1$

sample  $r_1$



$x_2$

sample  $r_2$



$x_3$

sample  $r_3$



$x_4$

sample  $r_4$



$x_5$

sample  $r_5$

# Multi-Party Randomized Encoding (MPRE) [ABT18]

Theorem  
[ABT10]

degree-2 MPRE  
for NC1

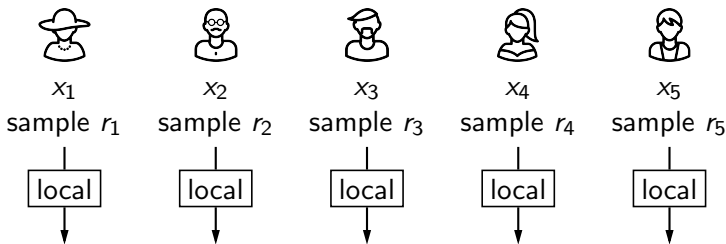
+

2-round MPC  
for degree-2 poly

$\Rightarrow$

2-round MPC  
for NC1

Proof.



# Multi-Party Randomized Encoding (MPRE) [ABT18]

Theorem  
[ABT10]

degree-2 MPRE  
for NC1

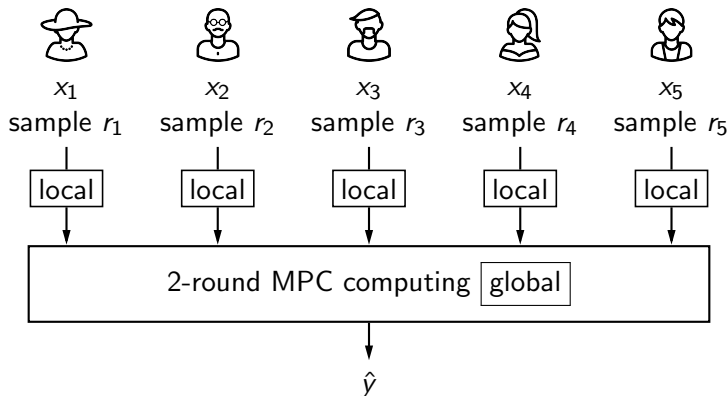
+

2-round MPC  
for degree-2 poly

$\Rightarrow$

2-round MPC  
for NC1

Proof.



# Multi-Party Randomized Encoding (MPRE) [ABT18]

Theorem  
[ABT10]

degree-2 MPRE  
for NC1

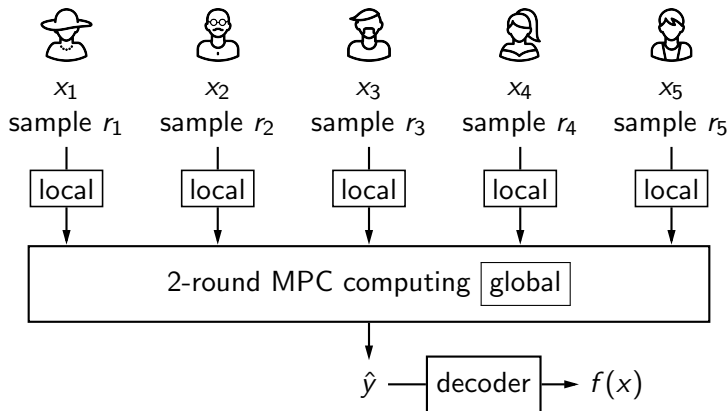
+

2-round MPC  
for degree-2 poly

$\Rightarrow$

2-round MPC  
for NC1

Proof.



## The Rest of the Talk...

Theorem  
[ABT10]

degree-2 MPRE  
for NC1

+

2-round MPC  
for degree-2 poly

$\Rightarrow$

2-round MPC  
for NC1

## The Rest of the Talk...

Theorem  
[ABT10]

degree-2 MPRE  
for NC1

+

2-round MPC  
for degree-2 poly

$\Rightarrow$

2-round MPC  
for NC1

---

Honest majority

## The Rest of the Talk...

Theorem  
[ABT10]

degree-2 MPRE  
for NC1

+

2-round MPC  
for degree-2 poly

$\Rightarrow$

2-round MPC  
for NC1

Honest majority

---

$\lfloor \frac{n-1}{2} \rfloor$ -private degree-2 MPRE  
for NC1

## The Rest of the Talk...

Theorem  
[ABT10]

degree-2 MPRE  
for NC1

+

2-round MPC  
for degree-2 poly

$\Rightarrow$

2-round MPC  
for NC1

Honest majority

---

$\lfloor \frac{n-1}{2} \rfloor$ -private degree-2 MPRE  
for NC1

$\lfloor \frac{n-1}{2} \rfloor$ -private 2-round MPC  
for degree-2 polynomial  
in plain model



## The Rest of the Talk...

Theorem  
[ABT10]

degree-2 MPRE  
for NC1

+

2-round MPC  
for degree-2 poly

$\Rightarrow$

2-round MPC  
for NC1

Honest majority

---

$\lfloor \frac{n-1}{2} \rfloor$ -private degree-2 MPRE  
for NC1

$\lfloor \frac{n-1}{2} \rfloor$ -private 2-round MPC  
in the honest majority model

# BGW

## The Rest of the Talk...

Theorem  
[ABT10]

degree-2 MPRE  
for NC1

+

2-round MPC  
for degree-2 poly

$\Rightarrow$

2-round MPC  
for NC1

---

Honest majority

$\lfloor \frac{n-1}{2} \rfloor$ -private degree-2 MPRE  
for NC1

$\lfloor \frac{n-1}{2} \rfloor$ -private 2-round MPC  
in the semi-honest model

# BGW

---

Honest minority

# The Rest of the Talk...

Theorem  
[ABT10]

degree-2 MPRE  
for NC1

+

2-round MPC  
for degree-2 poly

$\Rightarrow$

2-round MPC  
for NC1

Honest majority

$\lfloor \frac{n-1}{2} \rfloor$ -private degree-2 MPRE  
for NC1

Honest minority

$(n-1)$ -private degree-2 MPRE  
for NC1  
using OLE correlated randomness

$\lfloor \frac{n-1}{2} \rfloor$ -private 2-round MPC  
in the honest majority model

# BGW

# The Rest of the Talk...

Theorem  
[ABT10]

degree-2 MPRE  
for NC1

+

2-round MPC  
for degree-2 poly

$\Rightarrow$

2-round MPC  
for NC1

Honest majority

$\lfloor \frac{n-1}{2} \rfloor$ -private degree-2 MPRE  
for NC1

**BGW**

Honest minority

$(n-1)$ -private degree-2 MPRE  
for NC1  
using OLE correlated randomness

$(n-1)$ -private 2-round MPC  
for degree-2 polynomial  
using OLE correlated randomness

# The Rest of the Talk...

Theorem  
[ABT10]

degree-2 MPRE  
for NC1

+

2-round MPC  
for degree-2 poly

$\Rightarrow$

2-round MPC  
for NC1

Honest majority

$\lfloor \frac{n-1}{2} \rfloor$ -private degree-2 MPRE  
for NC1

**BGW**

Honest minority

$(n-1)$ -private degree-2 MPRE  
for NC1  
using OLE correlated randomness

$(n-1)$ -private degree-2 MPRE  
using OLE correlated randomness  
 $\approx$  arithmetic analog of  
passive-secure GMW



# The Rest of the Talk...

Theorem  
[ABT10]

de

Brief review of  
IK randomized encoding for NC1



2-round MPC  
for NC1

Honest majority

$\lfloor \frac{n-1}{2} \rfloor$ -private degree-2 MPRE  
for NC1

$\lfloor \frac{n-1}{2} \rfloor$ -private 2-round MPC  
for degree-2 polynomial  
in plain model

BGW

Honest minority

$(n-1)$ -private degree-2 MPRE  
for NC1  
using OLE correlated randomness

$(n-1)$ -private 2-round MPC  
for degree-2 polynomial  
using OLE correlated randomness

arithmetic analog of  
passive secure GMW

# The Rest of the Talk...

1

Theorem  
[ABT10]

de

Brief review of  
IK randomized encoding for NC1



2-round MPC  
for NC1

Honest majority

$\lfloor \frac{n-1}{2} \rfloor$ -private degree-2 MPRE  
for NC1

$\lfloor \frac{n-1}{2} \rfloor$ -private 2-round MPC  
for degree-2 polynomial  
in plain model

BGW

Honest minority

$(n-1)$ -private degree-2 MPRE  
for NC1  
using OLE correlated randomness

$(n-1)$ -private 2-round MPC  
for degree-2 polynomial  
using OLE correlated randomness

arithmetic analog of  
passive secure GMW



# The Rest of the Talk...

1

Theorem  
[ABT10]

de

Brief review of  
IK randomized encoding for NC1



2-round MPC  
for NC1

Honest majority

2

$\lfloor \frac{n-1}{2} \rfloor$ -private degree-2 MPRE  
for NC1

$\lfloor \frac{n-1}{2} \rfloor$ -private 2-round MPC  
for degree-2 polynomial  
in plain model

BGW

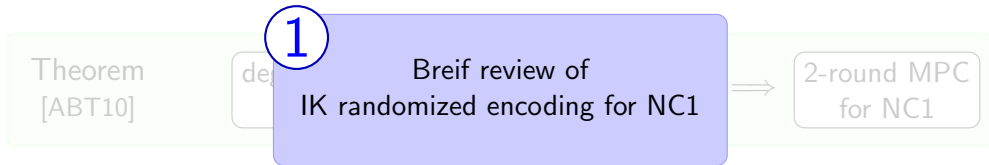
Honest minority

$(n-1)$ -private degree-2 MPRE  
for NC1  
using OLE correlated randomness

$(n-1)$ -private 2-round MPC  
for degree-2 polynomial  
using OLE correlated randomness

arithmetic analog of  
passive secure GMW

# The Rest of the Talk...



## Honest majority

2

$\lfloor \frac{n-1}{2} \rfloor$ -private degree-2 MPRE  
for NC1

$\lfloor \frac{n-1}{2} \rfloor$ -private 2-round MPC  
for degree-2 polynomial  
in plain model

BGW

## Honest minority

3

$(n-1)$ -private degree-2 MPRE  
for NC1  
using OLE correlated randomness

$(n-1)$ -private 2-round MPC  
for degree-2 polynomial  
using OLE correlated randomness

arithmetic analog of  
passive secure GMW

## Briefly Recall IK Randomized Encoding

## Briefly Recall IK Randomized Encoding

Any NC1 function  $f$  can be evaluated as a determinant

$$f(\vec{x}) = \det \begin{bmatrix} L_{1,1}(\vec{x}) & L_{1,2}(\vec{x}) & L_{1,3}(\vec{x}) & L_{1,4}(\vec{x}) \\ -1 & L_{2,2}(\vec{x}) & L_{2,3}(\vec{x}) & L_{2,4}(\vec{x}) \\ & -1 & L_{3,3}(\vec{x}) & L_{3,4}(\vec{x}) \\ & & -1 & L_{4,4}(\vec{x}) \end{bmatrix}$$

*linear in  $\vec{x}$*

## Briefly Recall IK Randomized Encoding

Any NC1 function  $f$  can be evaluated as a determinant

$$f(\vec{x}) = \det \begin{bmatrix} L_{1,1}(\vec{x}) & L_{1,2}(\vec{x}) & L_{1,3}(\vec{x}) & L_{1,4}(\vec{x}) \\ -1 & L_{2,2}(\vec{x}) & L_{2,3}(\vec{x}) & L_{2,4}(\vec{x}) \\ & -1 & L_{3,3}(\vec{x}) & L_{3,4}(\vec{x}) \\ & & -1 & L_{4,4}(\vec{x}) \end{bmatrix}$$

*linear in  $\vec{x}$*

Example:  $xyz + s = \det \begin{bmatrix} x & s \\ -1 & y \\ & -1 & z \end{bmatrix}$

## Briefly Recall IK Randomized Encoding

Any NC1 function  $f$  can be evaluated as a determinant

$$f(\vec{x}) = \det \begin{bmatrix} L_{1,1}(\vec{x}) & L_{1,2}(\vec{x}) & L_{1,3}(\vec{x}) & L_{1,4}(\vec{x}) \\ -1 & L_{2,2}(\vec{x}) & L_{2,3}(\vec{x}) & L_{2,4}(\vec{x}) \\ & -1 & L_{3,3}(\vec{x}) & L_{3,4}(\vec{x}) \\ & & -1 & L_{4,4}(\vec{x}) \end{bmatrix}$$

*linear in  $\vec{x}$*

## Briefly Recall IK Randomized Encoding

Any NC1 function  $f$  can be evaluated as a determinant

$$f(\vec{x}) = \det \begin{bmatrix} L_{1,1}(\vec{x}) & L_{1,2}(\vec{x}) & L_{1,3}(\vec{x}) & L_{1,4}(\vec{x}) \\ -1 & L_{2,2}(\vec{x}) & L_{2,3}(\vec{x}) & L_{2,4}(\vec{x}) \\ & -1 & L_{3,3}(\vec{x}) & L_{3,4}(\vec{x}) \\ & & -1 & L_{4,4}(\vec{x}) \end{bmatrix}$$

randomized encoding

IK02

$$RE = \begin{bmatrix} 1 & r_{12} & r_{13} & r_{14} \\ & 1 & r_{23} & r_{24} \\ & & 1 & r_{34} \\ & & & 1 \end{bmatrix} \begin{bmatrix} L_{1,1}(\vec{x}) & L_{1,2}(\vec{x}) & L_{1,3}(\vec{x}) & L_{1,4}(\vec{x}) \\ -1 & L_{2,2}(\vec{x}) & L_{2,3}(\vec{x}) & L_{2,4}(\vec{x}) \\ & -1 & L_{3,3}(\vec{x}) & L_{3,4}(\vec{x}) \\ & & -1 & L_{4,4}(\vec{x}) \end{bmatrix} \begin{bmatrix} 1 & r_{13} & r_{14} \\ & 1 & r_{24} \\ & & 1 & r_{34} \\ & & & 1 \end{bmatrix}$$

## Briefly Recall IK Randomized Encoding

Any NC1 function  $f$  can be evaluated as a determinant

$$f(\vec{x}) = \det \begin{bmatrix} L_{1,1}(\vec{x}) & L_{1,2}(\vec{x}) & L_{1,3}(\vec{x}) & L_{1,4}(\vec{x}) \\ -1 & L_{2,2}(\vec{x}) & L_{2,3}(\vec{x}) & L_{2,4}(\vec{x}) \\ & -1 & L_{3,3}(\vec{x}) & L_{3,4}(\vec{x}) \\ & & -1 & L_{4,4}(\vec{x}) \end{bmatrix}$$

*linear in  $\vec{x}$*

randomized encoding

IK02

$$RE = \begin{bmatrix} 1 & r_{12} & r_{13} & r_{14} \\ & 1 & r_{23} & r_{24} \\ & & 1 & r_{34} \\ & & & 1 \end{bmatrix} \begin{bmatrix} L_{1,1}(\vec{x}) & L_{1,2}(\vec{x}) & L_{1,3}(\vec{x}) & L_{1,4}(\vec{x}) \\ -1 & L_{2,2}(\vec{x}) & L_{2,3}(\vec{x}) & L_{2,4}(\vec{x}) \\ & -1 & L_{3,3}(\vec{x}) & L_{3,4}(\vec{x}) \\ & & -1 & L_{4,4}(\vec{x}) \end{bmatrix} \begin{bmatrix} 1 & r_{13} & r_{14} \\ & 1 & r_{24} \\ & & 1 & r_{34} \\ & & & 1 \end{bmatrix}$$

*randomness*

*linear in  $\vec{x}$*

*randomness*

properties

1)  $\det(RE) = f(\vec{x})$



## Briefly Recall IK Randomized Encoding

Any NC1 function  $f$  can be evaluated as a determinant

$$f(\vec{x}) = \det \begin{bmatrix} L_{1,1}(\vec{x}) & L_{1,2}(\vec{x}) & L_{1,3}(\vec{x}) & L_{1,4}(\vec{x}) \\ -1 & L_{2,2}(\vec{x}) & L_{2,3}(\vec{x}) & L_{2,4}(\vec{x}) \\ & -1 & L_{3,3}(\vec{x}) & L_{3,4}(\vec{x}) \\ & & -1 & L_{4,4}(\vec{x}) \end{bmatrix}$$

*linear in  $\vec{x}$*

randomized encoding

IK02

$$RE = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix} \begin{bmatrix} L_{1,1}(\vec{x}) & L_{1,2}(\vec{x}) & L_{1,3}(\vec{x}) & L_{1,4}(\vec{x}) \\ -1 & L_{2,2}(\vec{x}) & L_{2,3}(\vec{x}) & L_{2,4}(\vec{x}) \\ & -1 & L_{3,3}(\vec{x}) & L_{3,4}(\vec{x}) \\ & & -1 & L_{4,4}(\vec{x}) \end{bmatrix} \begin{bmatrix} 1 & r_{13} & r_{14} \\ & 1 & r_{24} \\ & & 1 & r_{34} \\ & & & 1 \end{bmatrix}$$

*randomness*

*linear in  $\vec{x}$*

*randomness*

properties

- 1)  $\det(RE) = f(\vec{x})$
- 2)  $RE \stackrel{d}{=} \text{Sim}(f(\vec{x}))$

## Briefly Recall IK Randomized Encoding

Any NC1 function  $f$  can be evaluated as a determinant

$$f(\vec{x}) = \det \begin{bmatrix} L_{1,1}(\vec{x}) & L_{1,2}(\vec{x}) & L_{1,3}(\vec{x}) & L_{1,4}(\vec{x}) \\ -1 & L_{2,2}(\vec{x}) & L_{2,3}(\vec{x}) & L_{2,4}(\vec{x}) \\ & -1 & L_{3,3}(\vec{x}) & L_{3,4}(\vec{x}) \\ & & -1 & L_{4,4}(\vec{x}) \end{bmatrix}$$

*linear in  $\vec{x}$*

randomized encoding

IK02

$$RE = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix} \begin{bmatrix} L_{1,1}(\vec{x}) & L_{1,2}(\vec{x}) & L_{1,3}(\vec{x}) & L_{1,4}(\vec{x}) \\ -1 & L_{2,2}(\vec{x}) & L_{2,3}(\vec{x}) & L_{2,4}(\vec{x}) \\ & -1 & L_{3,3}(\vec{x}) & L_{3,4}(\vec{x}) \\ & & -1 & L_{4,4}(\vec{x}) \end{bmatrix} \begin{bmatrix} 1 & r_{13} & r_{14} \\ & 1 & r_{24} \\ & & 1 & r_{34} \\ & & & 1 \end{bmatrix}$$

*randomness*

properties

- 1)  $\det(RE) = f(\vec{x})$
- 2)  $RE \stackrel{d}{=} \text{Sim}(f(\vec{x}))$
- 3) RE is arithmetic

## Briefly Recall IK Randomized Encoding

Any NC1 function  $f$  can be evaluated as a determinant

$$f(\vec{x}) = \det \begin{bmatrix} L_{1,1}(\vec{x}) & L_{1,2}(\vec{x}) & L_{1,3}(\vec{x}) & L_{1,4}(\vec{x}) \\ -1 & L_{2,2}(\vec{x}) & L_{2,3}(\vec{x}) & L_{2,4}(\vec{x}) \\ & -1 & L_{3,3}(\vec{x}) & L_{3,4}(\vec{x}) \\ & & -1 & L_{4,4}(\vec{x}) \end{bmatrix}$$

*linear in  $\vec{x}$*

randomized encoding

IK02

$$RE = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix} \begin{bmatrix} L_{1,1}(\vec{x}) & L_{1,2}(\vec{x}) & L_{1,3}(\vec{x}) & L_{1,4}(\vec{x}) \\ -1 & L_{2,2}(\vec{x}) & L_{2,3}(\vec{x}) & L_{2,4}(\vec{x}) \\ & -1 & L_{3,3}(\vec{x}) & L_{3,4}(\vec{x}) \\ & & -1 & L_{4,4}(\vec{x}) \end{bmatrix} \begin{bmatrix} 1 & r_{13} & r_{14} \\ & 1 & r_{24} \\ & & 1 & r_{34} \\ & & & 1 \end{bmatrix}$$

*randomness*

*linear in  $\vec{x}$*

*randomness*

properties

- 1)  $\det(RE) = f(\vec{x})$
- 2)  $RE \stackrel{d}{=} \text{Sim}(f(\vec{x}))$
- 3) RE is arithmetic
- 4) RE has degree 3

## Direct Construction of degree-2 MPRE

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$X, s_1$



$Y, s_2$



$Z, s_3$



## Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$X, s_1$



$Y, s_2$



$Z, s_3$



## Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$




$y, s_2, Q$



$z, s_3$



- ▶  samples random degree- $\lfloor \frac{n-1}{2} \rfloor$  poly  $P, Q$  s.t.  $P(0) = x, Q(0) = y$

## Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$




$y, s_2, Q$



$z, s_3$



- ▶  samples random degree- $\lfloor \frac{n-1}{2} \rfloor$  poly  $P, Q$  s.t.  $P(0) = x, Q(0) = y$
- ▶  $PQ$  is a degree- $(n-1)$  poly,

## Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$





$y, s_2, Q$



$z, s_3$



- ▶   samples random degree- $\lfloor \frac{n-1}{2} \rfloor$  poly  $P, Q$  s.t.  $P(0) = x, Q(0) = y$
- ▶  $PQ$  is a degree- $(n-1)$  poly,  
 $xy = (PQ)(0) = \text{linear}((PQ)(1), \dots, (PQ)(n))$



## Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$




$y, s_2, Q$



$z, s_3$



- ▶  samples random degree- $\lfloor \frac{n-1}{2} \rfloor$  poly  $P, Q$  s.t.  $P(0) = x, Q(0) = y$
- ▶  $PQ$  is a degree- $(n-1)$  poly,  
 $xy = (PQ)(0) = \text{linear}((PQ)(1), \dots, (PQ)(n))$
- ▶ Thus  $xyz + s_1 + s_2 + s_3 = \text{linear}((PQ)(1) \cdot z, \dots, (PQ)(n) \cdot z) + s_1 + s_2 + s_3$

## Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$




$y, s_2, Q$



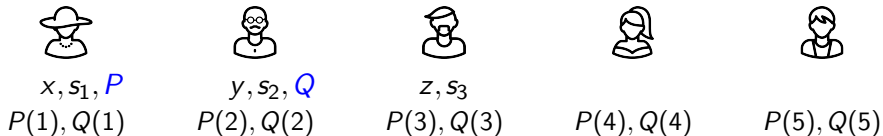
$z, s_3$





- ▶  samples random degree- $\lfloor \frac{n-1}{2} \rfloor$  poly  $P, Q$  s.t.  $P(0) = x, Q(0) = y$
- ▶  $PQ$  is a degree- $(n-1)$  poly,  
 $xy = (PQ)(0) = \text{linear}((PQ)(1), \dots, (PQ)(n))$
- ▶ Thus  $xyz + s_1 + s_2 + s_3 = \text{linear}((PQ)(1) \cdot z, \dots, (PQ)(n) \cdot z) + s_1 + s_2 + s_3$
- ▶ Shamir Sharing: Safe to let  $i$ -th party know  $P(i), Q(i)$

## Direct Construction of degree-2 MPRE with Honest Majority

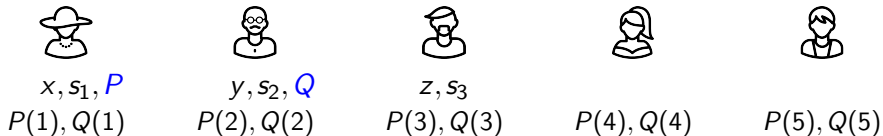
MPRE for the complete function  $xyz + s_1 + s_2 + s_3$





- ▶   samples random degree- $\lfloor \frac{n-1}{2} \rfloor$  poly  $P, Q$  s.t.  $P(0) = x, Q(0) = y$
- ▶  $PQ$  is a degree- $(n-1)$  poly,  
 $xy = (PQ)(0) = \text{linear}((PQ)(1), \dots, (PQ)(n))$
- ▶ Thus  $xyz + s_1 + s_2 + s_3 = \text{linear}((PQ)(1) \cdot z, \dots, (PQ)(n) \cdot z) + s_1 + s_2 + s_3$
- ▶ Shamir Sharing: Safe to let  $i$ -th party know  $P(i), Q(i)$   
Magically,  $i$ -th party gets  $P(i), Q(i)$

## Direct Construction of degree-2 MPRE with Honest Majority

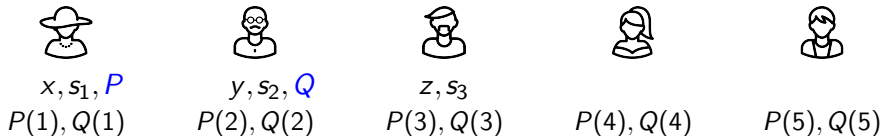
MPRE for the complete function  $xyz + s_1 + s_2 + s_3$





- ▶   samples random degree- $\lfloor \frac{n-1}{2} \rfloor$  poly  $P, Q$  s.t.  $P(0) = x, Q(0) = y$
- ▶  $PQ$  is a degree- $(n-1)$  poly,  
 $xy = (PQ)(0) = \text{linear}((PQ)(1), \dots, (PQ)(n))$
- ▶ Thus  $xyz + s_1 + s_2 + s_3 = \text{linear}((PQ)(1) \cdot z, \dots, (PQ)(n) \cdot z) + s_1 + s_2 + s_3$
- ▶ Shamir Sharing: Safe to let  $i$ -th party know  $P(i), Q(i)$   
Magically,  $i$ -th party gets  $P(i), Q(i)$ , locally computes  $(PQ)(i)$

## Direct Construction of degree-2 MPRE with Honest Majority

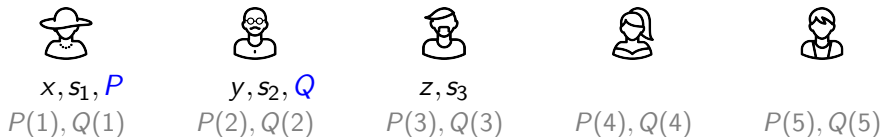
MPRE for the complete function  $xyz + s_1 + s_2 + s_3$





- ▶   samples random degree- $\lfloor \frac{n-1}{2} \rfloor$  poly  $P, Q$  s.t.  $P(0) = x, Q(0) = y$
- ▶  $PQ$  is a degree- $(n-1)$  poly,  
 $xy = (PQ)(0) = \text{linear}((PQ)(1), \dots, (PQ)(n))$
- ▶ Thus  $xyz + s_1 + s_2 + s_3 = \underbrace{\text{linear}((PQ)(1) \cdot z, \dots, (PQ)(n) \cdot z)}_{\text{degree 2 if } (PQ)(i) \text{ is locally computed}} + s_1 + s_2 + s_3$
- ▶ Shamir Sharing: Safe to let  $i$ -th party know  $P(i), Q(i)$   
Magically,  $i$ -th party gets  $P(i), Q(i)$ , locally computes  $(PQ)(i)$

# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



- ▶   samples random degree- $\lfloor \frac{n-1}{2} \rfloor$  poly  $P, Q$  s.t.  $P(0) = x, Q(0) = y$
- ▶  $PQ$  is a degree- $(n-1)$  poly,  
 $xy = (PQ)(0) = \text{linear}((PQ)(1), \dots, (PQ)(n))$
- ▶ Thus  $xyz + s_1 + s_2 + s_3 = \underbrace{\text{linear}((PQ)(1) \cdot z, \dots, (PQ)(n) \cdot z) + s_1 + s_2 + s_3}_{\text{degree 2 if } (PQ)(i) \text{ is locally computed}}$
- ▶ Shamir Sharing: Safe to let  $i$ -th party know  $P(i), Q(i)$   
~~Magically,  $i$ -th party gets  $P(i), Q(i)$ , locally computes  $(PQ)(i)$~~

## Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$   
 $P(1), Q(1)$



$y, s_2, Q$   
 $P(2), Q(2)$



$z, s_3$   
 $P(3), Q(3)$



$P(4), Q(4)$



$P(5), Q(5)$

- ▶ Thus  $xyz + s_1 + s_2 + s_3 = \underbrace{\text{linear}((PQ)(1) \cdot z, \dots, (PQ)(n) \cdot z)}_{\text{degree 2 if } (PQ)(i) \text{ is locally computed}} + s_1 + s_2 + s_3$
- ▶ Shamir Sharing: Safe to let  $i$ -th party know  $P(i), Q(i)$   
~~Magically,  $i$ -th party gets  $P(i), Q(i)$ , locally computes  $(PQ)(i)$~~

# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$   
 $P(1), Q(1)$



$y, s_2, Q$   
 $P(2), Q(2)$



$z, s_3$   
 $P(3), Q(3)$



$P(4), Q(4)$



$P(5), Q(5)$

NEW complete function:  $P(i) \cdot Q(i) \cdot z + \text{some linear terms}$

- ▶ Thus  $xyz + s_1 + s_2 + s_3 = \underbrace{\text{linear}((PQ)(1) \cdot z, \dots, (PQ)(n) \cdot z)}_{\text{degree 2 if } (PQ)(i) \text{ is locally computed}} + s_1 + s_2 + s_3$
- ▶ Shamir Sharing: Safe to let  $i$ -th party know  $P(i), Q(i)$   
~~Magically,  $i$ -th party gets  $P(i), Q(i)$ , locally computes  $(PQ)(i)$~~



## Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$   
 $P(1), Q(1)$



$y, s_2, Q$   
 $P(2), Q(2)$



$z, s_3$   
 $P(3), Q(3)$



$P(4), Q(4)$



$P(5), Q(5)$

NEW complete function:  $P(i) \cdot Q(i) \cdot z + \text{some linear terms}$

## Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$

$P(1), Q(1)$



$y, s_2, Q$

$P(2), Q(2)$



$z, s_3$

$P(3), Q(3)$




$P(4), Q(4)$



$P(5), Q(5)$

NEW complete function:  $P(i) \cdot Q(i) \cdot z + \text{some linear terms}$

▶  holds  $P(i)$

## Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$   
 $P(1), Q(1)$



$y, s_2, Q$   
 $P(2), Q(2)$



$z, s_3$   
 $P(3), Q(3)$



$P(4), Q(4)$



$P(5), Q(5)$

NEW complete function:  $P(i) \cdot Q(i) \cdot z + \text{some linear terms}$

- ▶  holds  $P(i)$
- ▶  holds  $Q(i)$

## Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$   
 $P(1), Q(1)$



$y, s_2, Q$   
 $P(2), Q(2)$



$z, s_3$   
 $P(3), Q(3)$






$P(4), Q(4)$



$P(5), Q(5)$

NEW complete function:  $P(i) \cdot Q(i) \cdot z + \text{some linear terms}$

- ▶  holds  $P(i)$
- ▶  holds  $Q(i)$
- ▶  holds  $z$

# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$   
 $P(1), Q(1)$



$y, s_2, Q$   
 $P(2), Q(2)$



$z, s_3$   
 $P(3), Q(3)$






$P(4), Q(4)$



$P(5), Q(5)$

NEW complete function:  $P(i) \cdot Q(i) \cdot z + \text{some linear terms}$

- ▶  holds  $P(i)$
- ▶  holds  $Q(i)$
- ▶  holds  $z$

*new*  $i$ -th party “gets” leakage  $P(i), Q(i)$

# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$   
 $P(1), Q(1)$



$y, s_2, Q$   
 $P(2), Q(2)$



$z, s_3$   
 $P(3), Q(3)$






$P(4), Q(4)$



$P(5), Q(5)$

NEW complete function:  $P(i) \cdot Q(i) \cdot z + \text{some linear terms}$

- ▶  holds  $P(i)$
- ▶  holds  $Q(i)$
- ▶  holds  $z$

*new*  $i$ -th party “gets” leakage  $P(i), Q(i)$

formalized as “MPRE w/ leakage”

# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$   
 $P(1), Q(1)$



$y, s_2, Q$   
 $P(2), Q(2)$



$z, s_3$   
 $P(3), Q(3)$






$P(4), Q(4)$



$P(5), Q(5)$

NEW complete function:  $P(i) \cdot Q(i) \cdot z + \text{some linear terms}$

- ▶  holds  $P(i)$
- ▶  holds  $Q(i)$
- ▶  holds  $z$

*new*  $i$ -th party “gets” leakage  $P(i), Q(i)$

formalized as “MPRE w/ leakage”

adversary & simulator gets  $P(i), Q(i)$  if  $i$ -th party is corrupted

# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$   
 $P(1), Q(1)$



$y, s_2, Q$   
 $P(2), Q(2)$



$z, s_3$   
 $P(3), Q(3)$



$P(4), Q(4)$



$P(5), Q(5)$

NEW complete function:  $P(i) \cdot Q(i) \cdot z + \text{some linear terms}$

$$\text{function} = \det \begin{bmatrix} P(i) & \text{terms} \\ -1 & z \\ -1 & Q(i) \end{bmatrix}$$



# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$   
 $P(1), Q(1)$



$y, s_2, Q$   
 $P(2), Q(2)$



$z, s_3$   
 $P(3), Q(3)$



$P(4), Q(4)$



$P(5), Q(5)$

NEW complete function:  $P(i) \cdot Q(i) \cdot z + \text{some linear terms}$

$$\text{function} = \det \begin{bmatrix} P(i) & \text{terms} \\ -1 & z \\ & -1 & Q(i) \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ & 1 & \\ & & 1 \end{bmatrix} \begin{bmatrix} P(i) & \text{terms} \\ -1 & z \\ & -1 & Q(i) \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ & 1 & r_5 \\ & & 1 \end{bmatrix}$$

# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$   
 $P(1), Q(1)$



$y, s_2, Q$   
 $P(2), Q(2)$



$z, s_3$   
 $P(3), Q(3)$



$P(4), Q(4)$



$P(5), Q(5)$

NEW complete function:  $P(i) \cdot Q(i) \cdot z + \text{some linear terms}$

$$\begin{aligned} \text{function} &= \det \begin{bmatrix} P(i) & \text{terms} \\ -1 & z \\ -1 & Q(i) \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} P(i) & \text{terms} \\ -1 & z \\ -1 & Q(i) \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ 1 & 1 & r_5 \\ 1 & 1 & 1 \end{bmatrix} \\ &= \begin{bmatrix} P(i) - r_1 & r_3 P(i) + r_1 z - r_1 r_3 - r_2 & r_1 r_5 z + r_4 P(i) + r_2 Q(i) - r_1 r_4 - r_2 r_5 + \text{terms} \\ -1 & z - r_3 & r_5 z - r_4 \\ -1 & -1 & Q(i) - r_5 \end{bmatrix} \end{aligned}$$

# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$   
 $P(1), Q(1)$



$y, s_2, Q$   
 $P(2), Q(2)$



$z, s_3$   
 $P(3), Q(3)$



$P(4), Q(4)$



$P(5), Q(5)$

NEW complete function:  $P(i) \cdot Q(i) \cdot z + \text{some linear terms}$

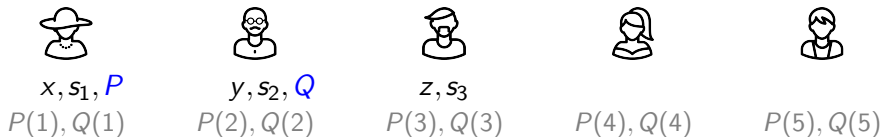
$$\text{function} = \det \begin{bmatrix} P(i) & \text{terms} \\ -1 & z \\ -1 & Q(i) \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} P(i) & \text{terms} \\ -1 & z \\ -1 & Q(i) \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ 1 & 1 & r_5 \\ 1 & 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} P(i) - r_1 & r_3 P(i) + r_1 z - r_1 r_3 - r_2 & r_1 r_5 z + r_4 P(i) + r_2 Q(i) - r_1 r_4 - r_2 r_5 + \text{terms} \\ -1 & z - r_3 & r_5 z - r_4 \\ -1 & -1 & Q(i) - r_5 \end{bmatrix}$$

How to Handle degree-3 term?

# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



NEW complete function:  $P(i) \cdot Q(i) \cdot z + \text{some linear terms}$

$$\text{function} = \det \begin{bmatrix} P(i) & \text{terms} \\ -1 & z \\ & -1 & Q(i) \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ & 1 & \\ & & 1 \end{bmatrix} \begin{bmatrix} P(i) & \text{terms} \\ -1 & z \\ & -1 & Q(i) \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ & 1 & r_5 \\ & & 1 \end{bmatrix}$$

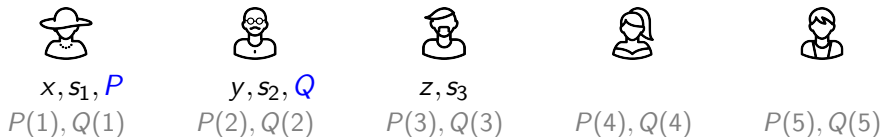
$$= \begin{bmatrix} P(i) - r_1 & r_3 P(i) + r_1 z - r_1 r_3 - r_2 & r_1 r_5 z + r_4 P(i) + r_2 Q(i) - r_1 r_4 - r_2 r_5 + \text{terms} \\ -1 & z - r_3 & r_5 z - r_4 \\ & -1 & Q(i) - r_5 \end{bmatrix}$$

How to Handle degree-3 term?

How to Sample  $r_1, \dots, r_5$ ?

# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



NEW complete function:  $P(i) \cdot Q(i) \cdot z + \text{some linear terms}$

$$\text{function} = \det \begin{bmatrix} P(i) & \text{terms} \\ -1 & z \\ -1 & Q(i) \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} P(i) & \text{terms} \\ -1 & z \\ -1 & Q(i) \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ 1 & 1 & r_5 \\ 1 & 1 & 1 \end{bmatrix}$$

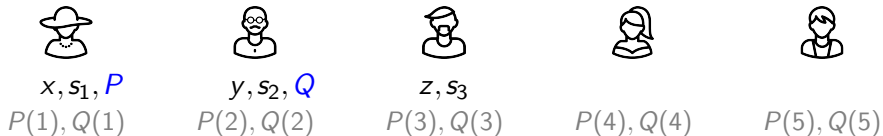
$$= \begin{bmatrix} P(i) - r_1 & r_3 P(i) + r_1 z - r_1 r_3 - r_2 & r_1 r_5 z + r_4 P(i) + r_2 Q(i) - r_1 r_4 - r_2 r_5 + \text{terms} \\ -1 & z - r_3 & r_5 z - r_4 \\ -1 & -1 & Q(i) - r_5 \end{bmatrix}$$

How to Handle degree-3 term?

How to Sample  $r_1, \dots, r_5$ ? Let  $i$ -th party sample  $r_1, r_5$

# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



NEW complete function:  $P(i) \cdot Q(i) \cdot z + \text{some linear terms}$

$$\text{function} = \det \begin{bmatrix} P(i) & \text{terms} \\ -1 & z \\ & -1 & Q(i) \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ & 1 & \\ & & 1 \end{bmatrix} \begin{bmatrix} P(i) & \text{terms} \\ -1 & z \\ & -1 & Q(i) \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ & 1 & r_5 \\ & & 1 \end{bmatrix}$$

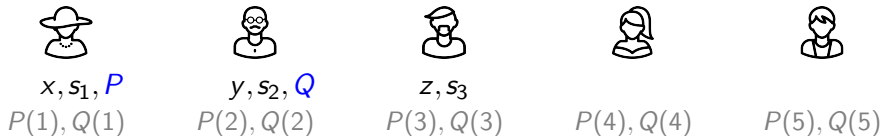
$$= \begin{bmatrix} P(i) - r_1 & r_3 P(i) + r_1 z - r_1 r_3 - r_2 & r_1 r_5 z + r_4 P(i) + r_2 Q(i) - r_1 r_4 - r_2 r_5 + \text{terms} \\ -1 & z - r_3 & r_5 z - r_4 \\ & -1 & Q(i) - r_5 \end{bmatrix}$$

How to Handle degree-3 term?

How to Sample  $r_1, \dots, r_5$ ? Let  $i$ -th party sample  $r_1, r_5$

# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



NEW complete function:  $P(i) \cdot Q(i) \cdot z + \text{some linear terms}$

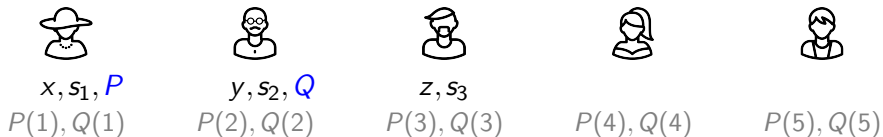
$$\begin{aligned}
 \text{function} &= \det \begin{bmatrix} P(i) & \text{terms} \\ -1 & z \\ & -1 & Q(i) \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ & 1 & \\ & & 1 \end{bmatrix} \begin{bmatrix} P(i) & \text{terms} \\ -1 & z \\ & -1 & Q(i) \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ & 1 & r_5 \\ & & 1 \end{bmatrix} \\
 &= \begin{bmatrix} P(i) - r_1 & r_3 P(i) + r_1 z - r_1 r_3 - r_2 & r_1 r_5 z + r_4 P(i) + r_2 Q(i) - r_1 r_4 - r_2 r_5 + \text{terms} \\ -1 & z - r_3 & r_5 z - r_4 \\ & -1 & Q(i) - r_5 \end{bmatrix}
 \end{aligned}$$

How to Handle degree-3 term?

How to Sample  $r_1, \dots, r_5$ ? Let  $i$ -th party sample  $r_1, r_5$  because  $P(i), Q(i)$  can be leaked to  $i$ -th party

# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



NEW complete function:  $P(i) \cdot Q(i) \cdot z + \text{some linear terms}$

$$\text{function} = \det \begin{bmatrix} P(i) & \text{terms} \\ -1 & z \\ & -1 & Q(i) \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ & 1 & \\ & & 1 \end{bmatrix} \begin{bmatrix} P(i) & \text{terms} \\ -1 & z \\ & -1 & Q(i) \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ & 1 & r_5 \\ & & 1 \end{bmatrix}$$

$$= \begin{bmatrix} P(i) - r_1 & r_3 P(i) + r_1 z - r_1 r_3 - r_2 & r_1 r_5 z + r_4 P(i) + r_2 Q(i) - r_1 r_4 - r_2 r_5 + \text{terms} \\ -1 & z - r_3 & r_5 z - r_4 \\ & -1 & Q(i) - r_5 \end{bmatrix}$$

How to Handle degree-3 term?  $i$ -th party locally computes  $r_1 r_5$

How to Sample  $r_1, \dots, r_5$ ? Let  $i$ -th party sample  $r_1, r_5$   
 because  $P(i), Q(i)$  can be leaked to  $i$ -th party



# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$



$y, s_2, Q$



$z, s_3$



← Putting-pieces-together →

# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$



$y, s_2, Q$



$z, s_3$



← Putting-pieces-together →

The encoding consists of

$$\begin{bmatrix} P(i) - r_1 & r_3 P(i) + r_1 z - r_1 r_3 - r_2 & r_1 r_5 z + r_4 P(i) + r_2 Q(i) - r_1 r_4 - r_2 r_5 + \text{terms} \\ -1 & z - r_3 & r_5 z - r_4 \\ & -1 & Q(i) - r_5 \end{bmatrix} \text{ for each } i.$$

# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$



$y, s_2, Q$





$z, s_3$



Putting-pieces-together

The encoding consists of

$$\begin{bmatrix} P(i) - r_1 & r_3 P(i) + r_1 z - r_1 r_3 - r_2 & r_1 r_5 z + r_4 P(i) + r_2 Q(i) - r_1 r_4 - r_2 r_5 + \text{terms} \\ -1 & z - r_3 & r_5 z - r_4 \\ & -1 & Q(i) - r_5 \end{bmatrix} \text{ for each } i.$$

▶   sample  $P, Q$  resp.

# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$



$y, s_2, Q$




$z, s_3$



Putting-pieces-together

The encoding consists of

$$\begin{bmatrix} P(i) - r_1 & r_3 P(i) + r_1 z - r_1 r_3 - r_2 & r_1 r_5 z + r_4 P(i) + r_2 Q(i) - r_1 r_4 - r_2 r_5 + \text{terms} \\ -1 & z - r_3 & r_5 z - r_4 \\ & -1 & Q(i) - r_5 \end{bmatrix} \text{ for each } i.$$

- ▶  sample  $P, Q$  resp.
- ▶  $i$ -th party samples  $r_{i,1}, r_{i,5}$  and locally compute  $r_{i,1} r_{i,5}$

# Direct Construction of degree-2 MPRE with Honest Majority

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1, P$



$y, s_2, Q$





$z, s_3$



Putting-pieces-together

The encoding consists of

$$\begin{bmatrix} P(i)-r_1 & r_3P(i)+r_1z-r_1r_3-r_2 & r_1r_5z+r_4P(i)+r_2Q(i)-r_1r_4-r_2r_5+\text{terms} \\ -1 & z-r_3 & r_5z-r_4 \\ & -1 & Q(i)-r_5 \end{bmatrix} \text{ for each } i.$$

- ▶   sample  $P, Q$  resp.
- ▶  $i$ -th party samples  $r_{i,1}, r_{i,5}$  and locally compute  $r_{i,1}r_{i,5}$
- ▶  $r_{i,2}, r_{i,3}, r_{i,4}$  are jointly sampled

NEXT

MPRE w/ OLE correlated randomness

## Direct Construction of degree-2 MPRE with OLE Correlations

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$X, s_1$



$Y, s_2$



$Z, s_3$



## Direct Construction of degree-2 MPRE with OLE Correlations

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$X, s_1$



$Y, s_2$



$Z, s_3$



$$\text{function} = \det \begin{bmatrix} x & s_1 + s_2 + s_3 \\ -1 & z \\ z & -1 \\ & & y \end{bmatrix}$$



# Direct Construction of degree-2 MPRE with OLE Correlations

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$X, s_1$



$Y, s_2$



$Z, s_3$



$$\text{function} = \det \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ & -1 & y \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ & 1 & 1 \\ & & 1 \end{bmatrix} \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ & -1 & y \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ & 1 & r_5 \\ & & 1 \end{bmatrix}$$

# Direct Construction of degree-2 MPRE with OLE Correlations

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$X, s_1$



$Y, s_2$



$Z, s_3$



$$\text{function} = \det \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ z & -1 \\ & y \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ & 1 & 1 \\ & & 1 \end{bmatrix} \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ & -1 \\ & y \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ & 1 & r_5 \\ & & 1 \end{bmatrix}$$

$$= \begin{bmatrix} x - r_1 (r_3 x + r_1 z) & (r_1 r_5 z + r_4 x + r_2 y) \\ -1 & z - r_3 \\ & -1 \\ & -1 \end{bmatrix} \begin{bmatrix} r_1 r_5 z + r_4 x + r_2 y \\ -r_1 r_4 - r_2 r_5 + s_1 + s_2 + s_3 \\ r_5 z - r_4 \\ y - r_5 \end{bmatrix}$$

# Direct Construction of degree-2 MPRE with OLE Correlations

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$X, s_1$



$Y, s_2$



$Z, s_3$



$$\text{function} = \det \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ z & -1 \\ -1 & y \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ -1 & y \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ 1 & r_5 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} x - r_1 & \begin{pmatrix} r_3x + r_1z \\ -r_1r_3 - r_2 \end{pmatrix} & \begin{pmatrix} r_1r_5z + r_1x + r_2y \\ -r_1r_4 - r_2r_5 + s_1 + s_2 + s_3 \end{pmatrix} \\ -1 & z - r_3 & r_5z - r_4 \\ -1 & -1 & y - r_5 \end{bmatrix}$$

How to Handle degree-3 term?

# Direct Construction of degree-2 MPRE with OLE Correlations

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$X, s_1$



$Y, s_2$



$Z, s_3$



$$\text{function} = \det \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ z & -1 \\ -1 & y \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ & 1 & \\ & & 1 \end{bmatrix} \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ z & -1 \\ -1 & y \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ & 1 & r_5 \\ & & 1 \end{bmatrix}$$

$$= \begin{bmatrix} x - r_1 & \begin{pmatrix} r_3x + r_1z \\ -r_1r_3 - r_2 \end{pmatrix} & \begin{pmatrix} r_1r_5z + r_1x + r_2y \\ -r_1r_4 - r_2r_5 + s_1 + s_2 + s_3 \end{pmatrix} \\ -1 & z - r_3 & r_5z - r_4 \\ -1 & -1 & y - r_5 \end{bmatrix}$$

How to Handle degree-3 term?

How to Sample  $r_1, \dots, r_5$ ?

# Direct Construction of degree-2 MPRE with OLE Correlations

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1$



$y, s_2$




$z, s_3$



$$\text{function} = \det \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ -1 & y \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ 1 & & 1 \end{bmatrix} \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ -1 & y \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ 1 & r_5 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} x - r_1 & \begin{pmatrix} r_3x + r_1z \\ -r_1r_3 - r_2 \end{pmatrix} & \begin{pmatrix} r_1r_5z + r_1x + r_2y \\ -r_1r_4 - r_2r_5 + s_1 + s_2 + s_3 \end{pmatrix} \\ -1 & z - r_3 & r_5z - r_4 \\ -1 & -1 & y - r_5 \end{bmatrix}$$

How to Handle degree-3 term?

How to Sample  $r_1, \dots, r_5$ ? Let  sample  $r_1$ .

# Direct Construction of degree-2 MPRE with OLE Correlations

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$X, s_1$



$Y, s_2$




$Z, s_3$



$$\text{function} = \det \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ -1 & y \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ 1 & & 1 \end{bmatrix} \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ -1 & y \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ 1 & r_5 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} x - r_1 & r_3x + r_1z & r_1r_5z + r_1x + r_2y \\ -1 & -r_1r_3 - r_2 & -r_1r_4 - r_2r_5 + s_1 + s_2 + s_3 \\ -1 & z - r_3 & r_5z - r_4 \\ & -1 & y - r_5 \end{bmatrix}$$

How to Handle degree-3 term?

How to Sample  $r_1, \dots, r_5$ ? Let  sample  $r_1$ .

# Direct Construction of degree-2 MPRE with OLE Correlations

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$X, s_1$



$Y, s_2$



$Z, s_3$



$$\text{function} = \det \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ -1 & y \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ 1 & & 1 \end{bmatrix} \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ -1 & y \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ 1 & r_5 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} x - r_1 & r_3x + r_1z & r_1r_5z + r_1x + r_2y \\ -1 & z - r_3 & -r_1r_4 - r_2r_5 + s_1 + s_2 + s_3 \\ -1 & -1 & r_5z - r_4 \\ & & y - r_5 \end{bmatrix}$$

How to Handle degree-3 term?

How to Sample  $r_1, \dots, r_5$ ? Let  sample  $r_1$ . Let  sample  $r_5$ .

# Direct Construction of degree-2 MPRE with OLE Correlations

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$X, s_1$



$Y, s_2$



$Z, s_3$



$$\text{function} = \det \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ -1 & y \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ 1 & & 1 \end{bmatrix} \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ -1 & y \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ 1 & r_5 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} x - r_1 & r_3x + r_1z & r_1r_5z + r_1x + r_2y \\ -1 & z - r_3 & -r_1r_4 - r_2r_5 + s_1 + s_2 + s_3 \\ -1 & -1 & r_5z - r_4 \\ & & y - r_5 \end{bmatrix}$$

How to Handle degree-3 term?   sample  $r_1, r_5$  from OLE Correlation!

How to Sample  $r_1, \dots, r_5$ ? Let  sample  $r_1$ . Let  sample  $r_5$ .



# Direct Construction of degree-2 MPRE with OLE Correlations

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$$\text{function} = \det \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ -1 & y \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ 1 & & 1 \end{bmatrix} \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ -1 & y \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ 1 & r_5 \\ 1 \end{bmatrix} \\
 = \begin{bmatrix} x - r_1 & r_3x + r_1z & r_1r_5z + r_1x + r_2y \\ -1 & -r_1r_3 - r_2 & -r_1r_4 - r_2r_5 + s_1 + s_2 + s_3 \\ -1 & z - r_3 & r_5z - r_4 \\ & -1 & y - r_5 \end{bmatrix}$$

How to Handle degree-3 term?   sample  $r_1, r_5$  from OLE Correlation!

How to Sample  $r_1, \dots, r_5$ ? Let  sample  $r_1$ . Let  sample  $r_5$ .

# Direct Construction of degree-2 MPRE with OLE Correlations

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1$

$r_1, a_1$



$y, s_2$

$r_5, a_2$

s.t.  $r_1 r_5 = a_1 + a_2$



$z, s_3$



$$\text{function} = \det \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ -1 & y \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ 1 & & 1 \end{bmatrix} \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ -1 & y \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ 1 & r_5 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} x - r_1 & r_3x + r_1z & r_1r_5z + r_1x + r_2y \\ -1 & -r_1r_3 - r_2 & -r_1r_4 - r_2r_5 + s_1 + s_2 + s_3 \\ -1 & z - r_3 & r_5z - r_4 \\ & & y - r_5 \end{bmatrix}$$

How to Handle degree-3 term?   sample  $r_1, r_5$  from OLE Correlation!

How to Sample  $r_1, \dots, r_5$ ? Let  sample  $r_1$ . Let  sample  $r_5$ .

# Direct Construction of degree-2 MPRE with OLE Correlations

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1$

$r_1, a_1$



$y, s_2$

$r_5, a_2$

s.t.  $r_1 r_5 = a_1 + a_2$



$z, s_3$



$$\text{function} = \det \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ -1 & y \end{bmatrix} \xrightarrow{\text{IK RE}} \begin{bmatrix} 1 & r_1 & r_2 \\ 1 & & 1 \end{bmatrix} \begin{bmatrix} x & s_1+s_2+s_3 \\ -1 & z \\ -1 & y \end{bmatrix} \begin{bmatrix} 1 & r_3 & r_4 \\ 1 & r_5 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} x - r_1 & r_3x + r_1z & (a_1 + a_2)z + r_1x + r_2y \\ -1 & -r_1r_3 - r_2 & -r_1r_4 - r_2r_5 + s_1 + s_2 + s_3 \\ -1 & z - r_3 & r_5z - r_4 \\ & & y - r_5 \end{bmatrix}$$

How to Handle degree-3 term?   sample  $r_1, r_5$  from OLE Correlation!

How to Sample  $r_1, \dots, r_5$ ? Let  sample  $r_1$ . Let  sample  $r_5$ .

# Direct Construction of degree-2 MPRE with OLE Correlations

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1$

$r_1, a_1$



$y, s_2$

$r_5, a_2$



$z, s_3$



s.t.  $r_1 r_5 = a_1 + a_2$

In short

The encoding is 
$$\begin{bmatrix} x-r_1 & \begin{pmatrix} r_3x+r_1z \\ -r_1r_3-r_2 \end{pmatrix} & \begin{pmatrix} (a_1+a_2)z+r_4x+r_2y \\ -r_1r_4-r_2r_5+s_1+s_2+s_3 \end{pmatrix} \\ -1 & z-r_3 & r_5z-r_4 \\ & -1 & y-r_5 \end{bmatrix}$$

# Direct Construction of degree-2 MPRE with OLE Correlations

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1$

$r_1, a_1$



$y, s_2$

$r_5, a_2$




$z, s_3$



s.t.  $r_1 r_5 = a_1 + a_2$

In short

The encoding is 
$$\begin{bmatrix} x - r_1 & \begin{pmatrix} r_3 x + r_1 z \\ -r_1 r_3 - r_2 \end{pmatrix} & \begin{pmatrix} (a_1 + a_2)z + r_4 x + r_2 y \\ -r_1 r_4 - r_2 r_5 + s_1 + s_2 + s_3 \end{pmatrix} \\ -1 & z - r_3 & r_5 z - r_4 \\ & -1 & y - r_5 \end{bmatrix}$$

-  sample  $(r_1, a_1), (r_5, a_2)$  from OLE correlated randomness

# Direct Construction of degree-2 MPRE with OLE Correlations

MPRE for the complete function  $xyz + s_1 + s_2 + s_3$



$x, s_1$

$r_1, a_1$



$y, s_2$

$r_5, a_2$




$z, s_3$



s.t.  $r_1 r_5 = a_1 + a_2$

In short

The encoding is 
$$\begin{bmatrix} x - r_1 & \begin{pmatrix} r_3 x + r_1 z \\ -r_1 r_3 - r_2 \end{pmatrix} & \begin{pmatrix} (a_1 + a_2)z + r_4 x + r_2 y \\ -r_1 r_4 - r_2 r_5 + s_1 + s_2 + s_3 \end{pmatrix} \\ -1 & \begin{pmatrix} z - r_3 \\ -1 \end{pmatrix} & \begin{pmatrix} r_5 z - r_4 \\ y - r_5 \end{pmatrix} \end{bmatrix}$$

- ▶  sample  $(r_1, a_1), (r_5, a_2)$  from OLE correlated randomness
- ▶  $r_2, r_3, r_4$  are jointly sampled

# Simple 2-round MPC

**Our Results:** information-theoretic 2-round MPC for NC1

(i) in plain model, w/ honest majority

(ii) in OLE correlation model, w/ honest minority

extension to P/poly with black-box use of PRG

**new** support arithmetic NC1 with black-box field access

**new** adaptive security with explicit simulator\*

more efficient

# Simple 2-round MPC

**Our Results:** information-theoretic 2-round MPC for NC1

(i) in plain model, w/ honest majority

(ii) in OLE correlation model, w/ honest minority

extension to P/poly with black-box use of PRG

**new** support arithmetic NC1 with black-box field access

**new** adaptive security with explicit simulator\*

more efficient

**Technique:**

a new **direct** construction of degree-2 MPRE with no round collapsing

$$xyz + \text{terms} = \det \begin{bmatrix} x - r_1 & \begin{pmatrix} r_3x + r_1z \\ -r_1r_3 - r_2 \end{pmatrix} & \begin{pmatrix} r_1r_5z + r_4x + r_2y \\ -r_1r_4 - r_2r_5 + \text{terms} \end{pmatrix} \\ -1 & z - r_3 & r_5z - r_4 \\ & -1 & y - r_5 \end{bmatrix}$$



# Simple 2-round MPC

**Our Results:** information-theoretic 2-round MPC for NC1

(i) in plain model, w/ honest majority

(ii) in OLE correlation model, w/ honest minority

extension to P/poly with black-box use of PRG

**new** support arithmetic NC1 with black-box field access

**new** adaptive security with explicit simulator\*

more efficient

**Technique:**

a new **direct** construction of degree-2 MPRE with no round collapsing

$$xyz + \text{terms} = \det \begin{bmatrix} x - r_1 & \begin{pmatrix} r_3x + r_1z \\ -r_1r_3 - r_2 \end{pmatrix} & \begin{pmatrix} r_1r_5z + r_4x + r_2y \\ -r_1r_4 - r_2r_5 + \text{terms} \end{pmatrix} \\ -1 & z - r_3 & r_5z - r_4 \\ & -1 & y - r_5 \end{bmatrix}$$

# Thank you!

*"So simple that can be taught in class."*