Two Round Information-Theoretic MPC with Malicious Security

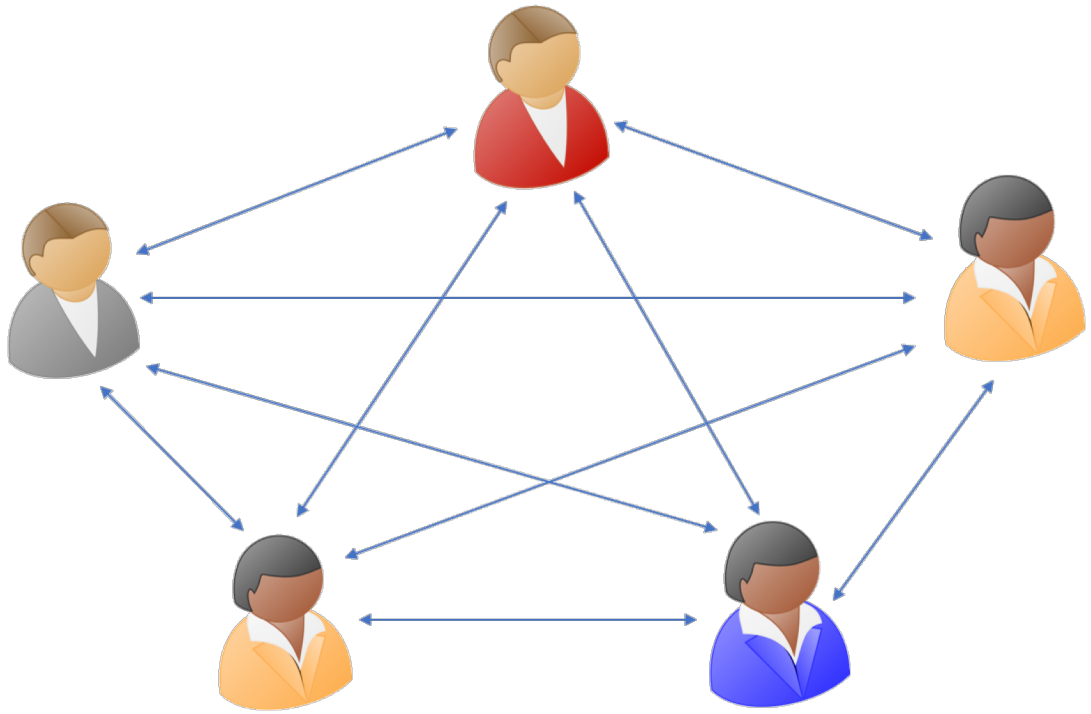
Prabhanjan Ananth Arka Rai Choudhuri Aarushi Goel Abhishek Jain

Massachusetts Institute of Technology

JOHNS HOPKINS UNIVERSITY

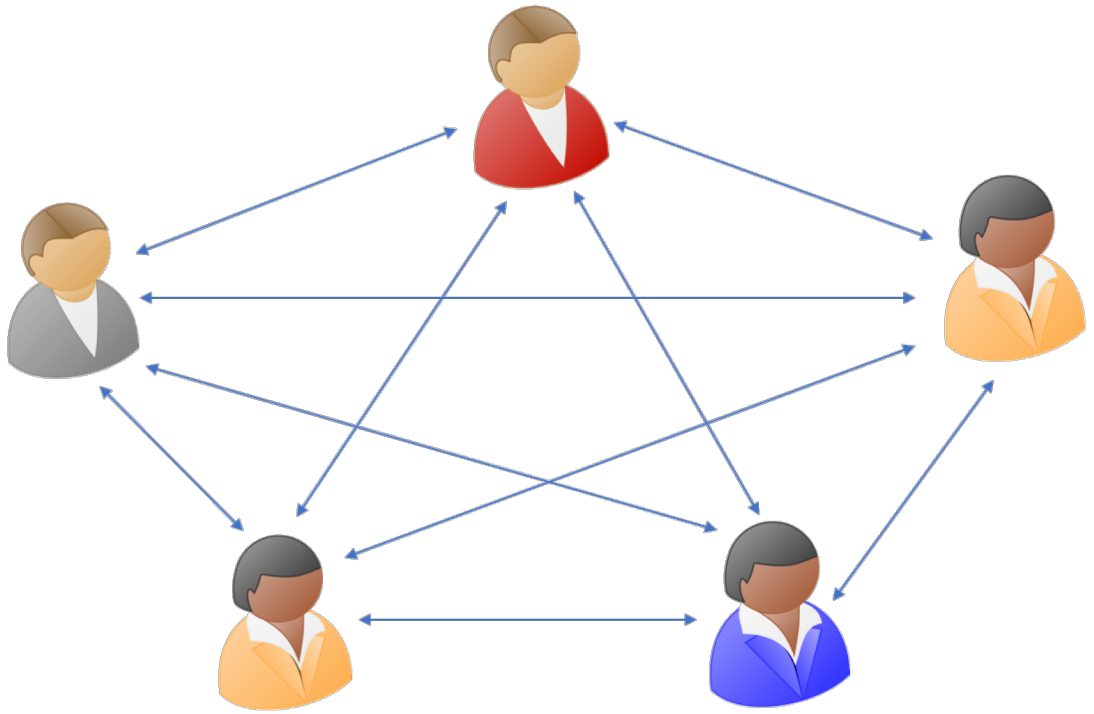
EUROCRYPT 2019

Adversarial Model



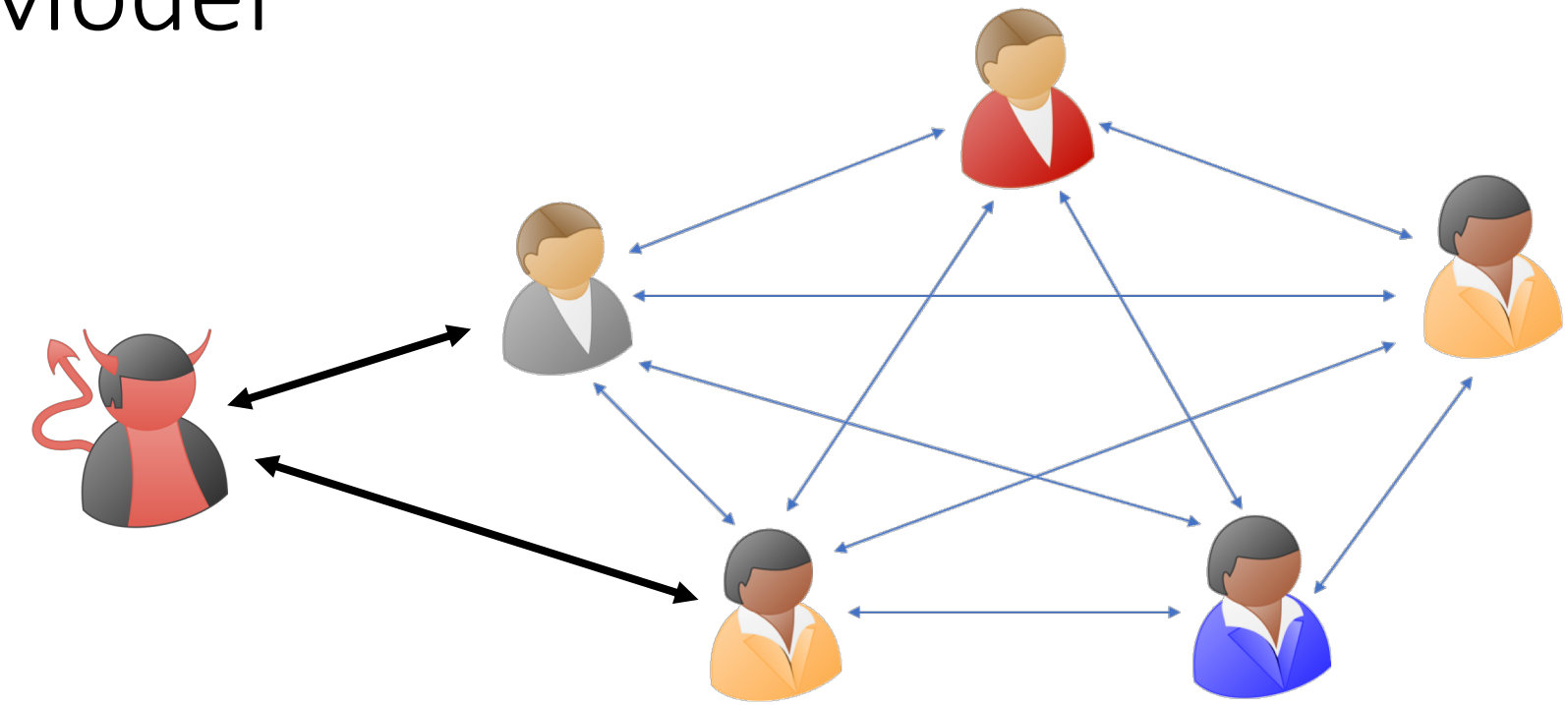
Adversarial Model

Malicious Adversary



Adversarial Model

Malicious Adversary



Corrupts $< n/2$ parties (Honest Majority)

Honest Majority MPC

Honest Majority MPC

Information-Theoretic security is possible.

[Ben-Or, Goldwasser, Widgerson'88]

Honest Majority MPC

Information-Theoretic security is possible.

[Ben-Or, Goldwasser, Widgerson'88]

Typically UC secure

Simulation proofs are typically straight-line

Honest Majority MPC

Information-Theoretic security is possible.

[Ben-Or, Goldwasser, Widgerson'88]

Typically UC secure

Simulation proofs are typically straight-line

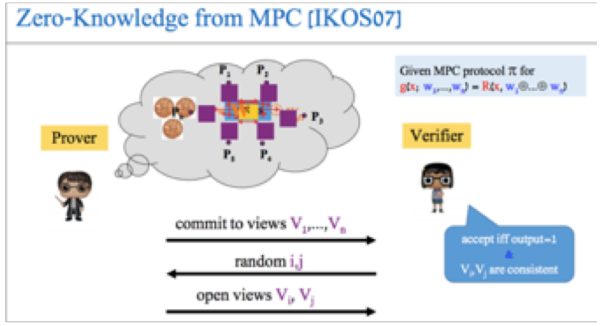
Round complexity lower bounds of dishonest majority do not apply.

4 rounds necessary for dishonest majority in the plain model

[Garg- Mukherjee-Pandey-Polychroniadou16]

Honest Majority MPC: Applications

Efficient Zero-Knowledge
[IKOS'07,…]

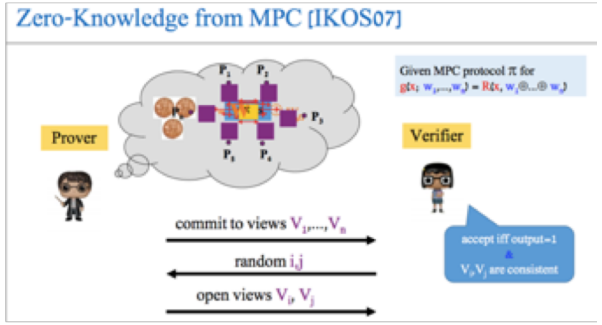


(Courtesy: Carmit Hazay's talk)

Useful for constructing efficient ZK-protocols.

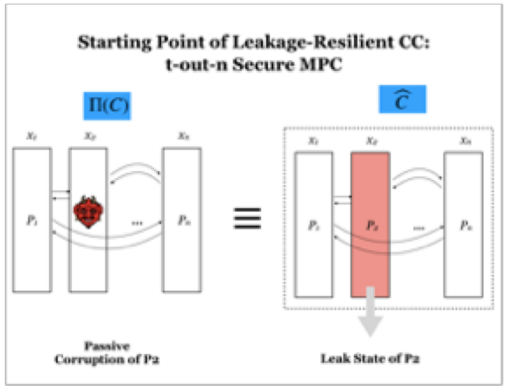
Honest Majority MPC: Applications

Efficient Zero-Knowledge
[IKOS'07,…]

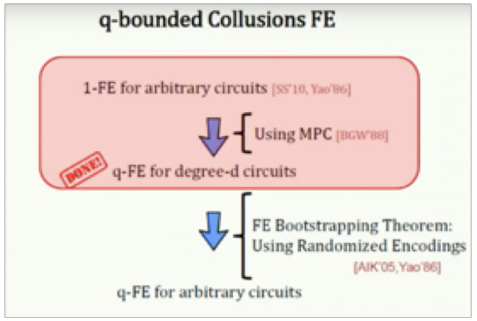


(Courtesy: Carmit Hazay's talk)

Leakage-Resilient Circuit Compilers
[ISW03,FKKNV10,AIS18]



Bounded-Key Functional Encryption
[GVW12,AV18]



(Courtesy: Sergey Gorbunov's talk)

History of IT-MPC

	Round Complexity	Class of Functions	Corruption Threshold	Adversary	
[BGW'88]	> # of multiplications	P/Poly	t<n/2	Malicious	
[BB'89, IK'00, AIK'06]	constant	NC^1	t<n/2	Malicious	
[IKP'10]	2	NC^1	t<n/3	Malicious	Security with selective abort
[GIS'18, ABT'18]	2	NC^1	t<n/2	Semi-honest	
[ABT'19]	2	NC^1	t<n/2	Malicious	Security with selective abort

Our Results

Round Complexity	Class of Functions	Corruption Threshold	Adversary
2	NC^1	$t<n/2$	Malicious

Security with Abort over
Broadcast + P2P

Security with Selective Abort over
P2P

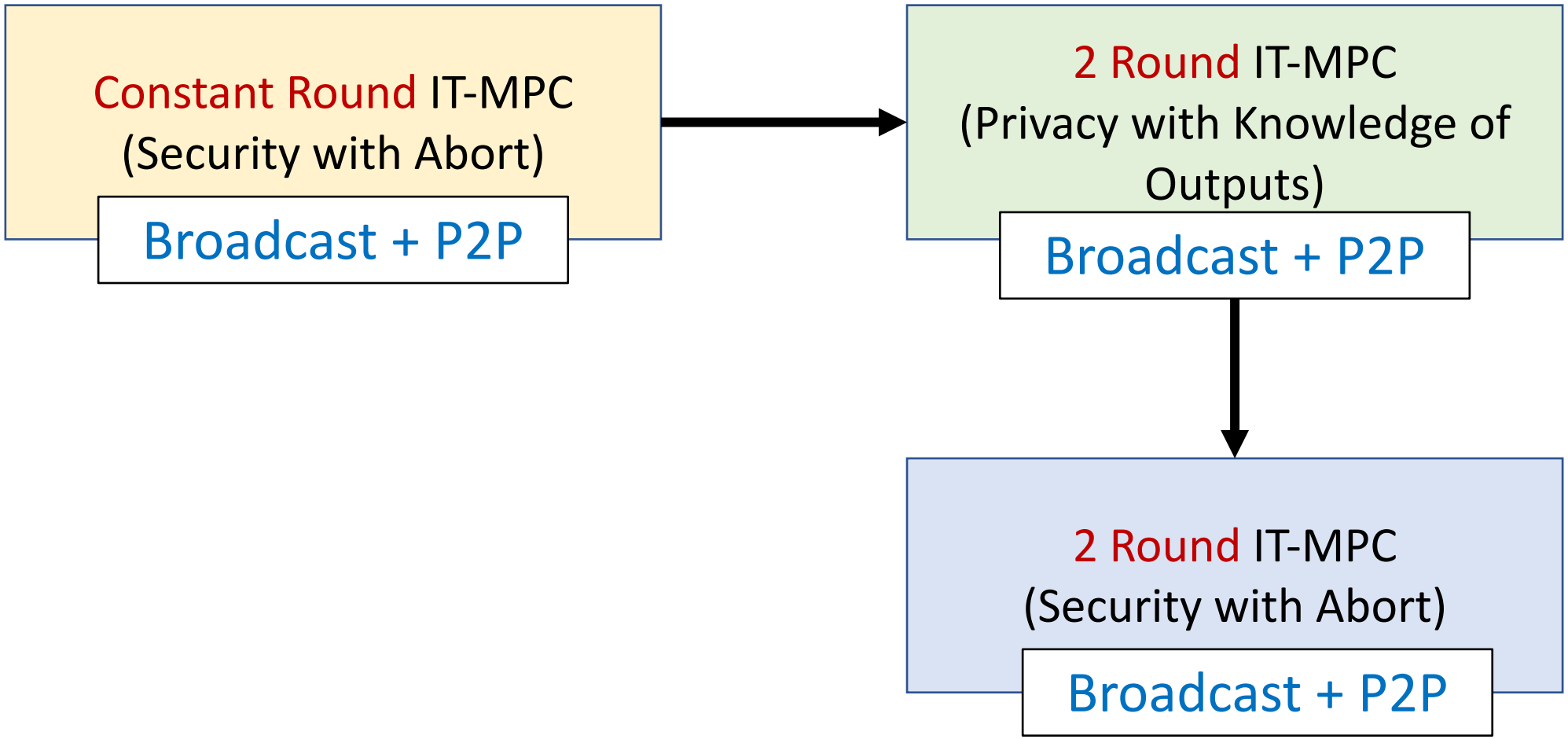
This Talk

Round Complexity	Class of Functions	Corruption Threshold	Adversary
2	NC^1	$t<n/2$	Malicious

Security with Abort over
Broadcast + P2P

Security with Selective Abort over
P2P

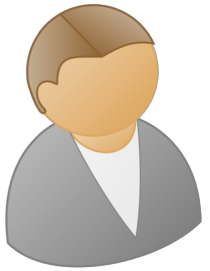
Our Strategy



Security with Abort

Party 1

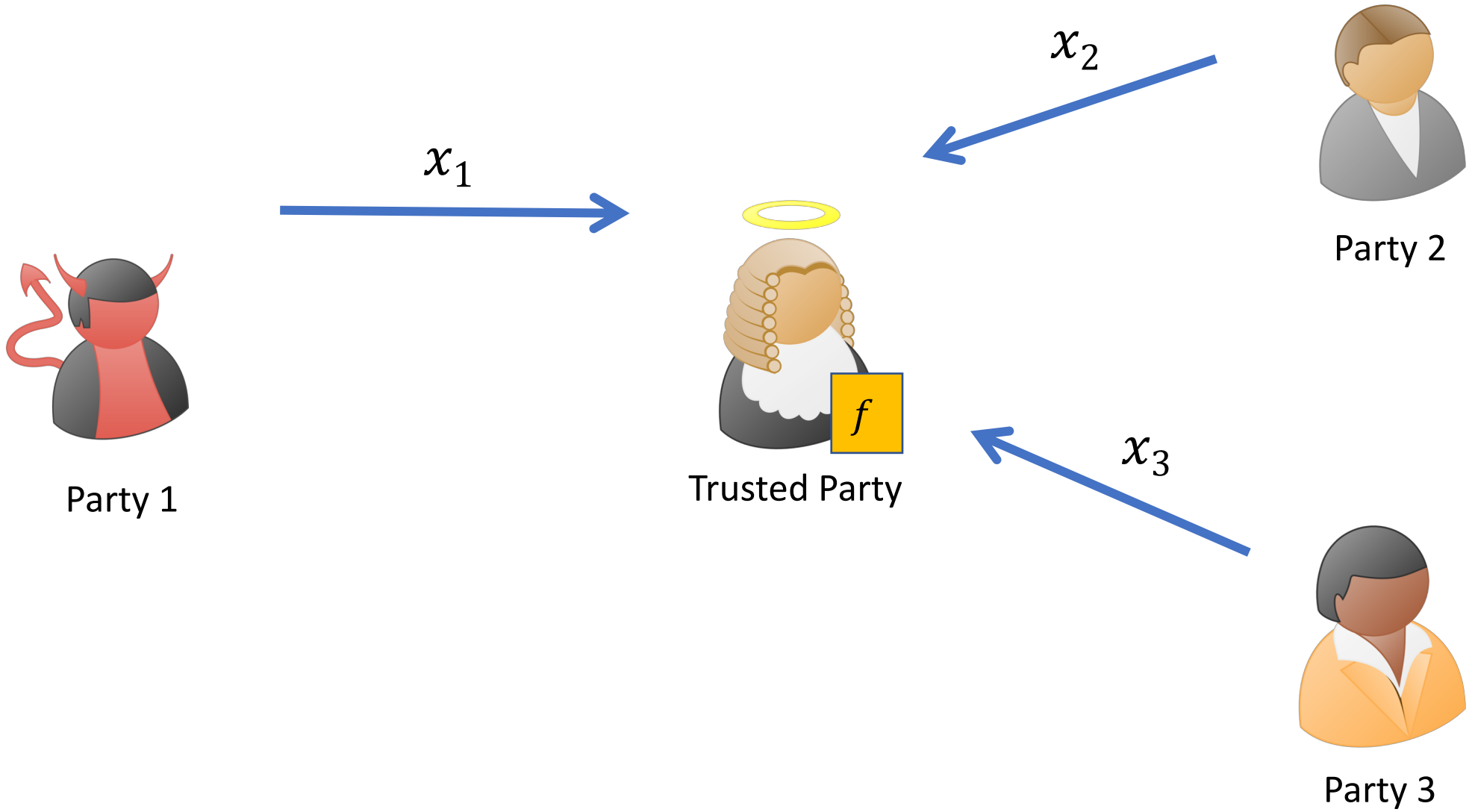
Trusted Party



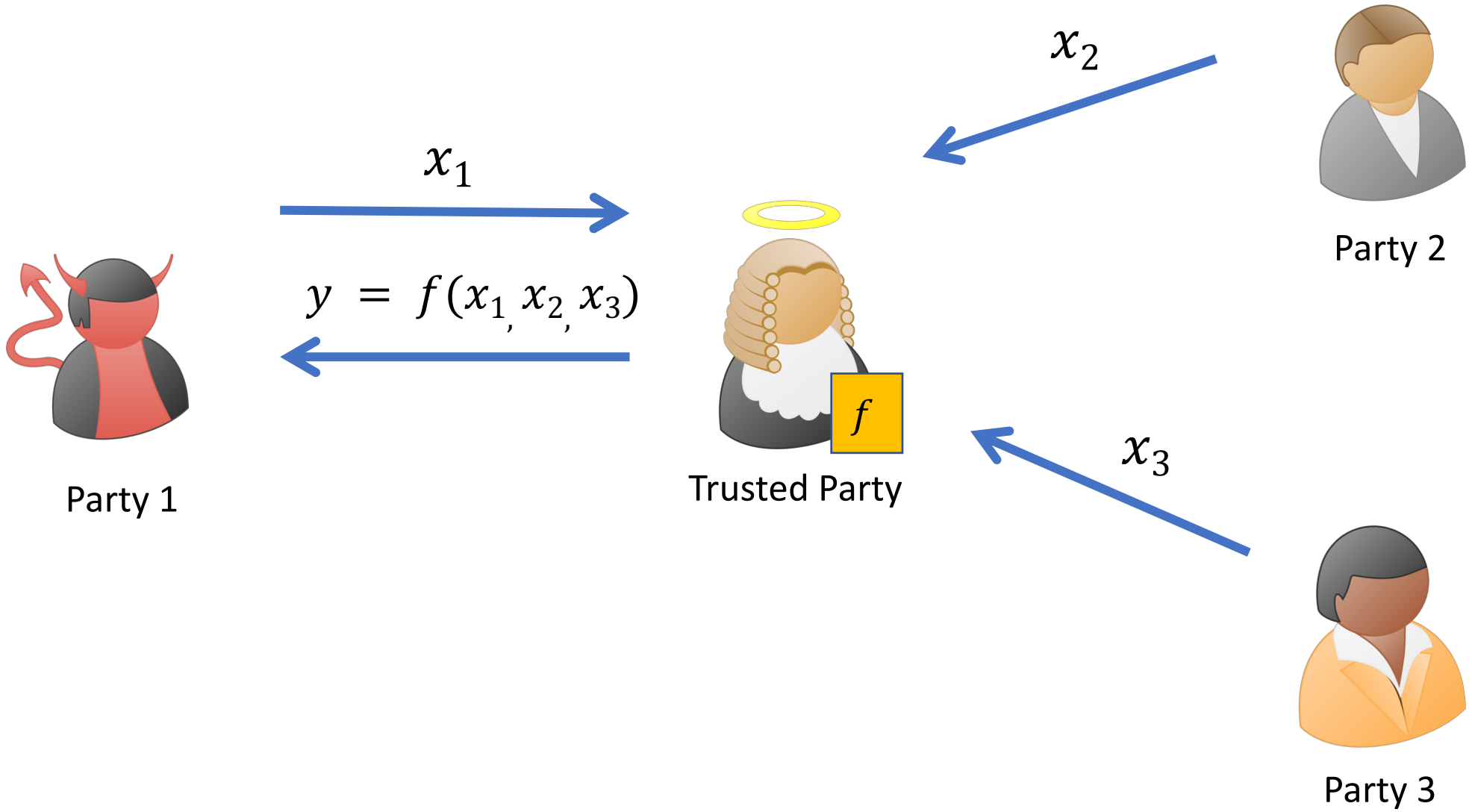
Party 2

Party 3

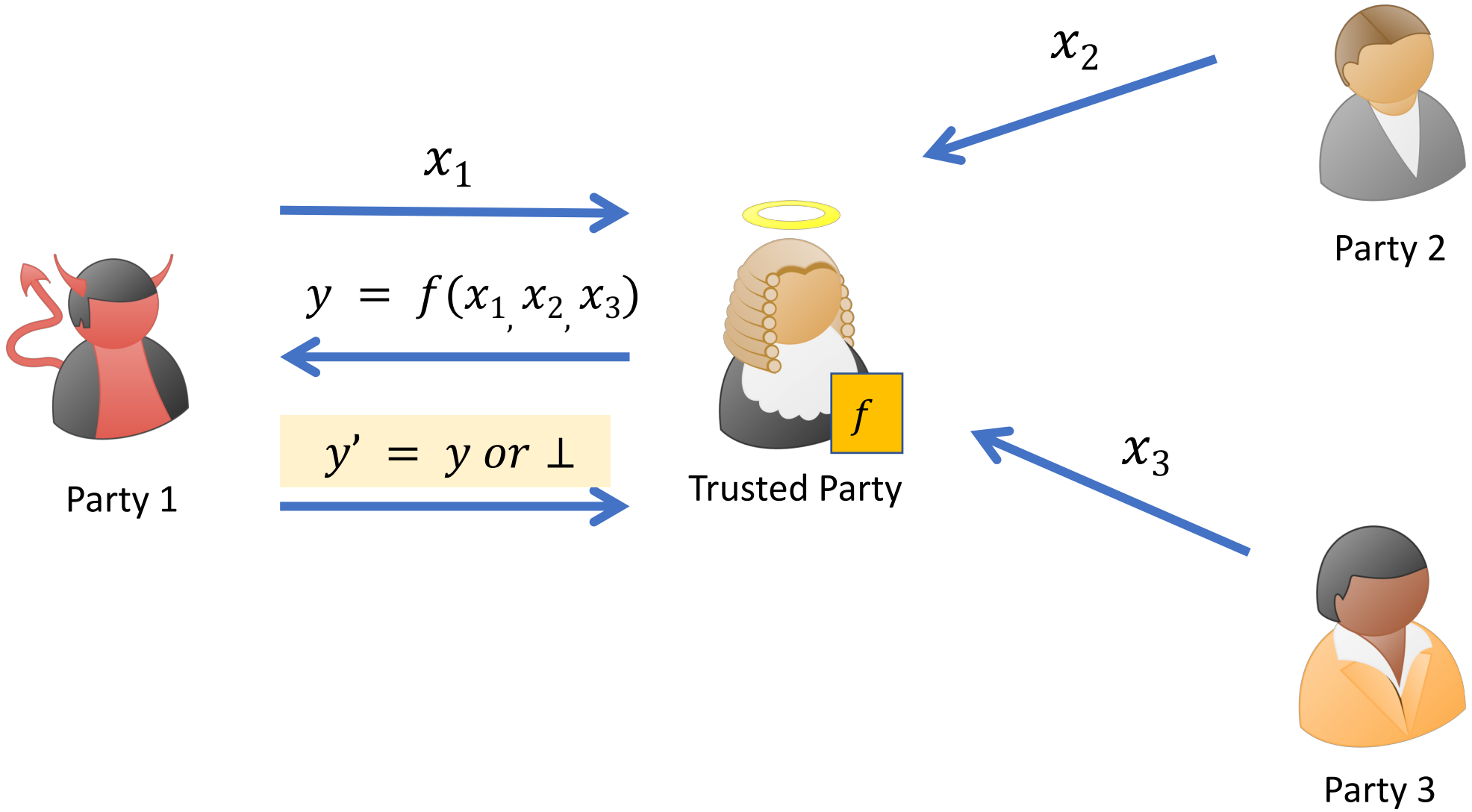
Security with Abort



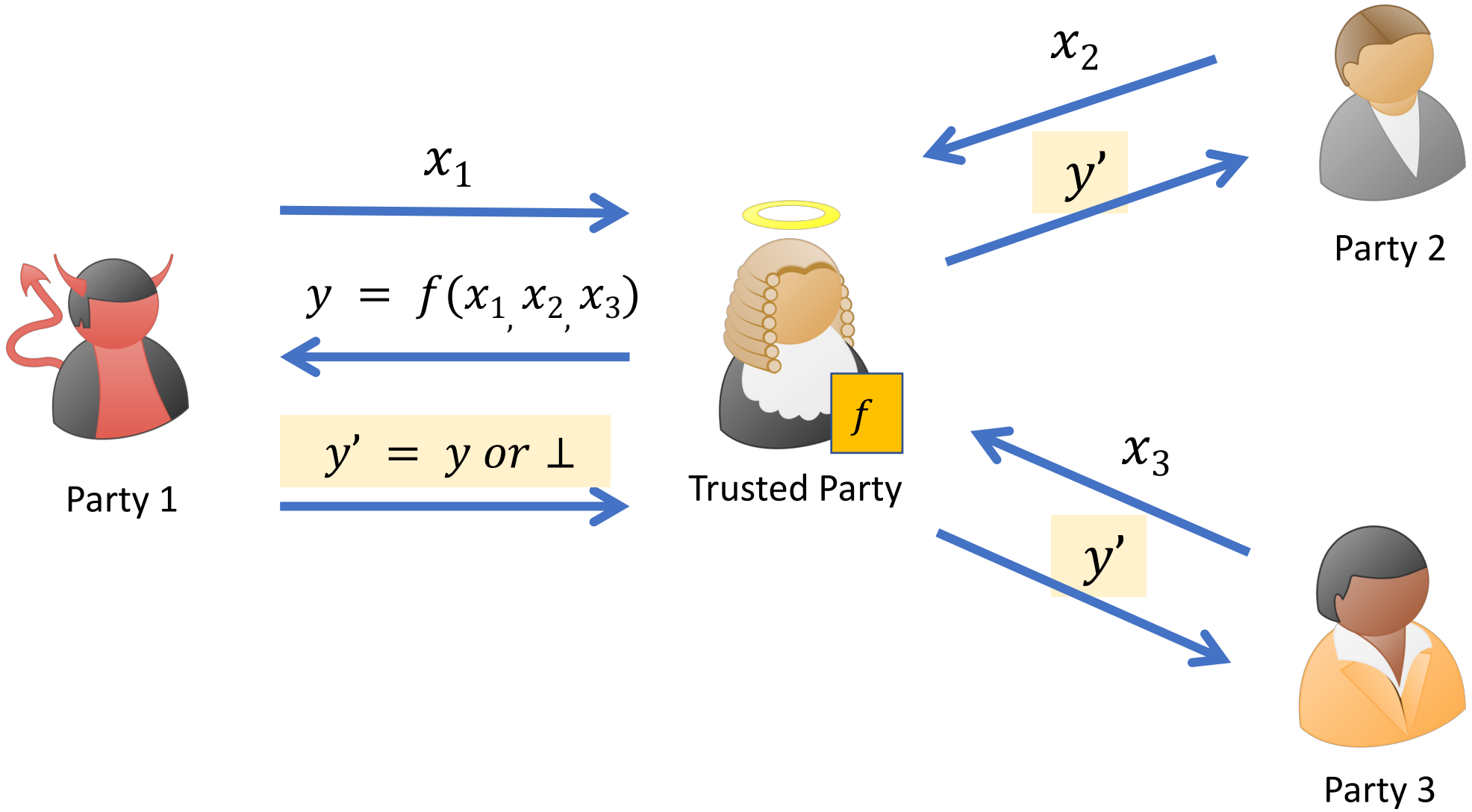
Security with Abort



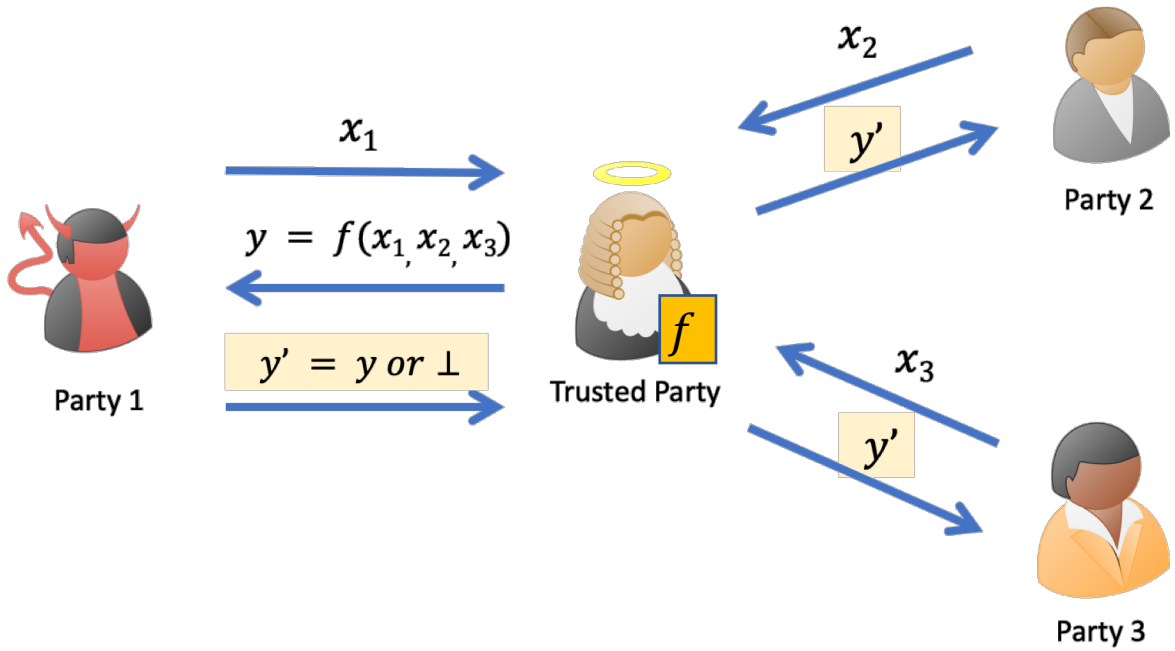
Security with Abort



Security with Abort



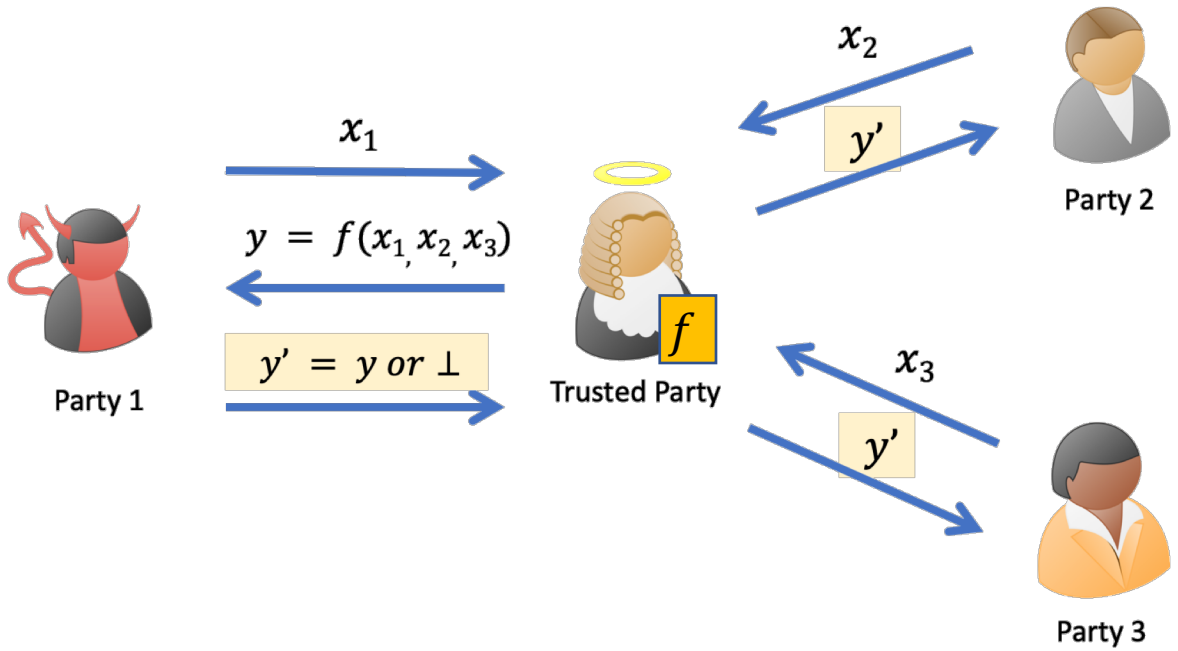
Security with Abort



Privacy

x_2 and x_3 remain hidden

Security with Abort



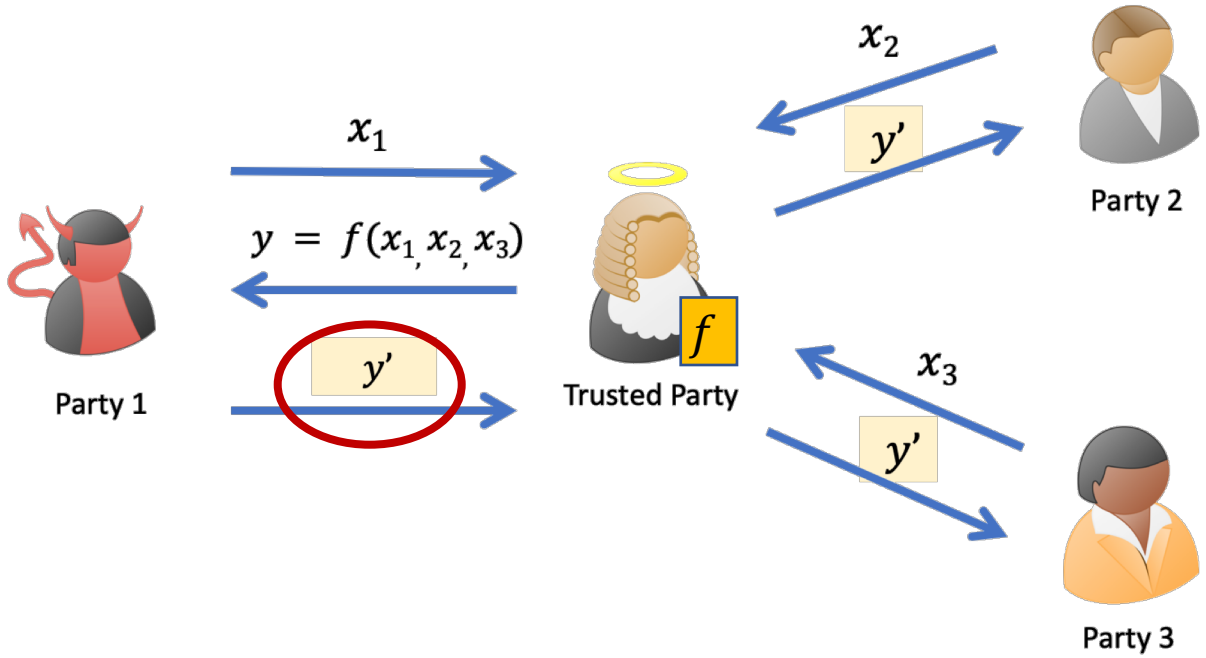
Privacy

x_2 and x_3 remain hidden

Output Correctness

Honest Parties either output $f(x_1, x_2, x_3)$ or $\perp$

Privacy with Knowledge of Outputs



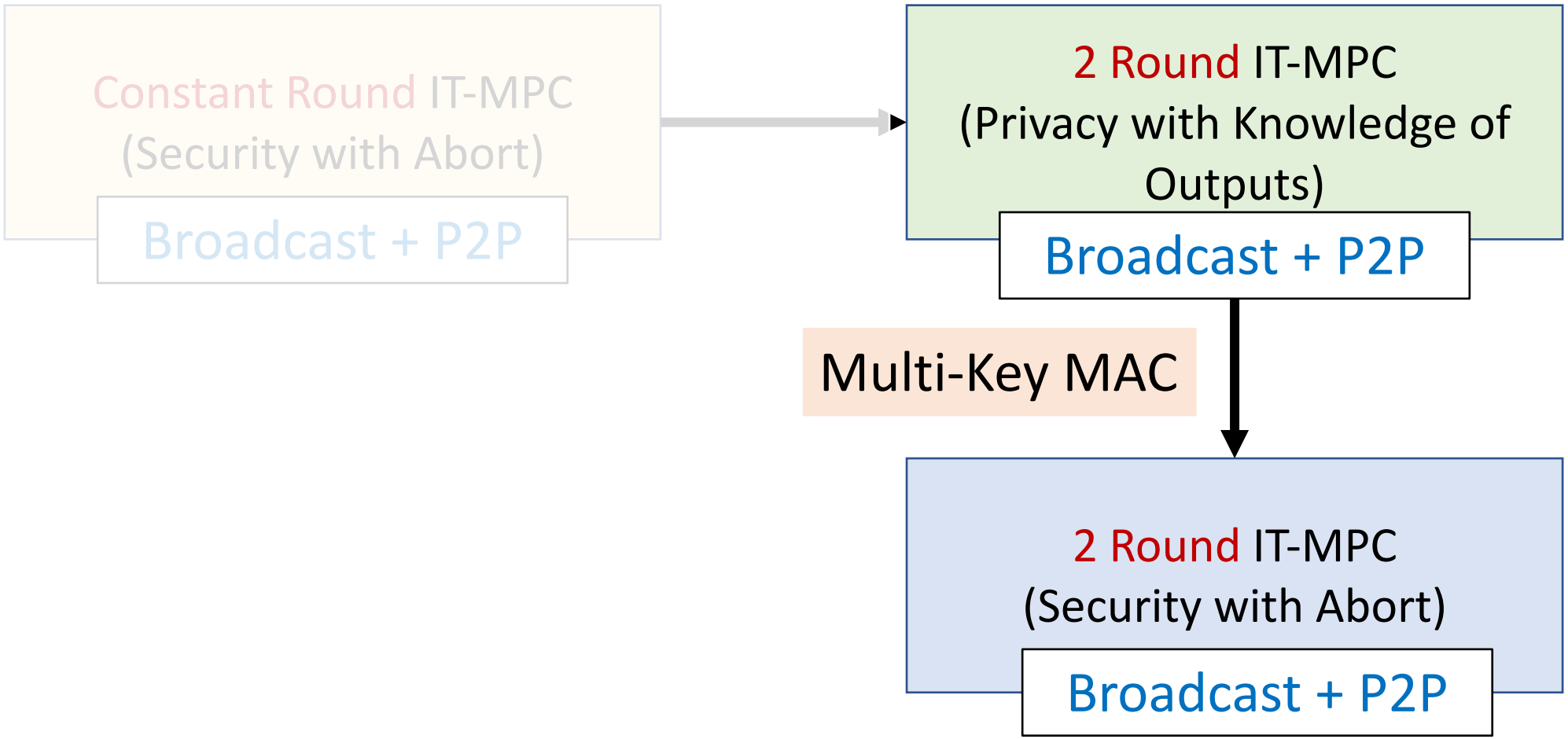
Privacy

x_2 and x_3 remain hidden

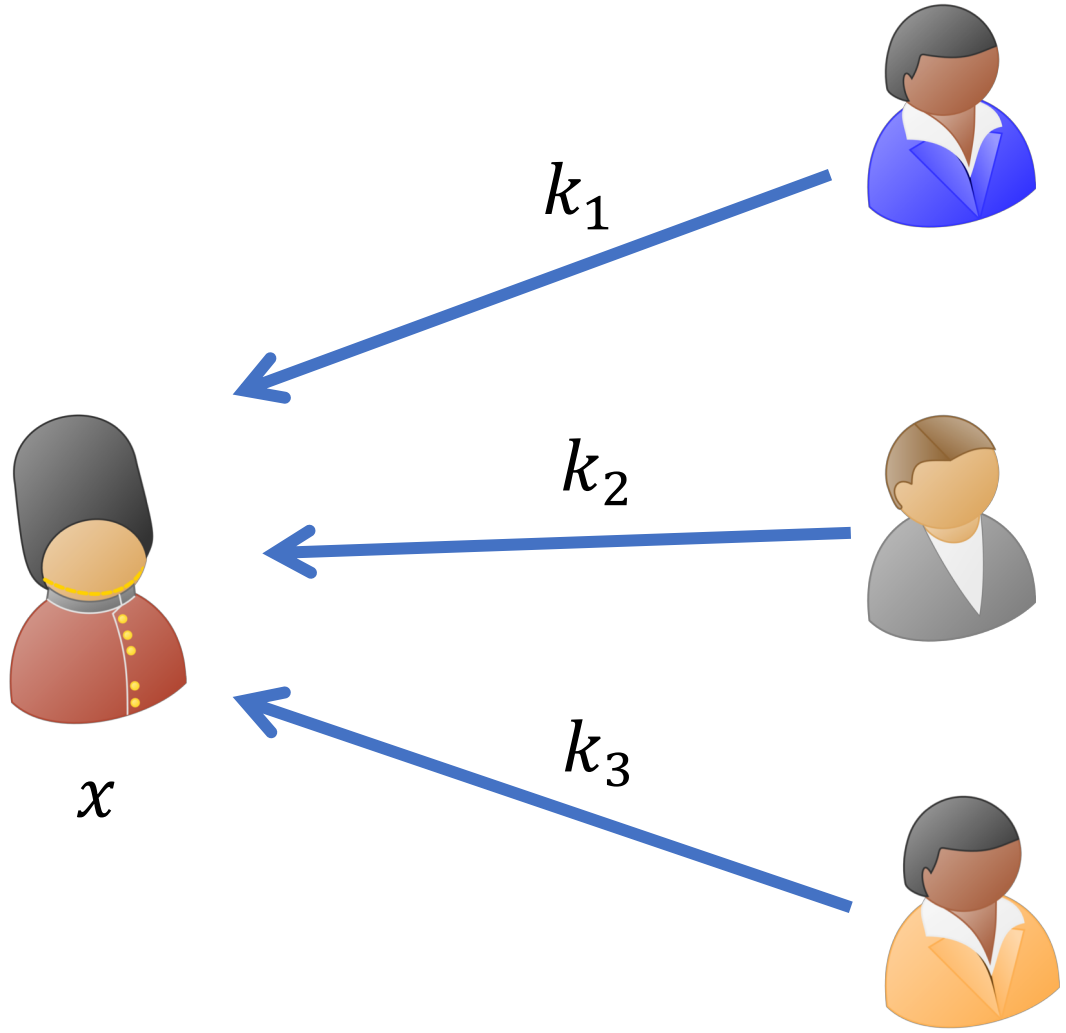
Output Correctness

Honest Parties either output $f(x_1, x_2, x_3)$ or $\perp$

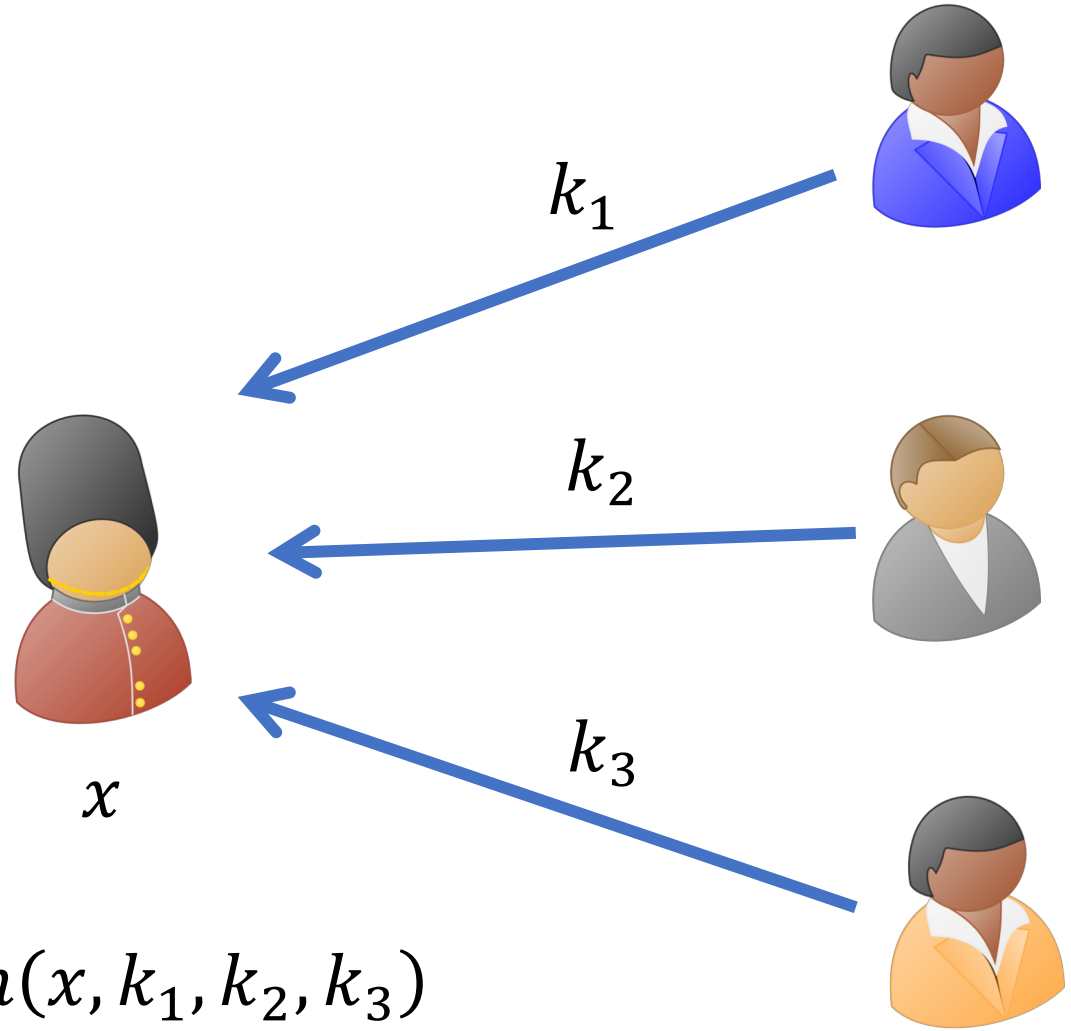
First Step


Constant Round IT-MPC
(Security with Abort)
Broadcast + P2P
2 Round IT-MPC
(Privacy with Knowledge of Outputs)
Broadcast + P2P
Multi-Key MAC
2 Round IT-MPC
(Security with Abort)
Broadcast + P2P

Our Tool: Multi-Key MAC

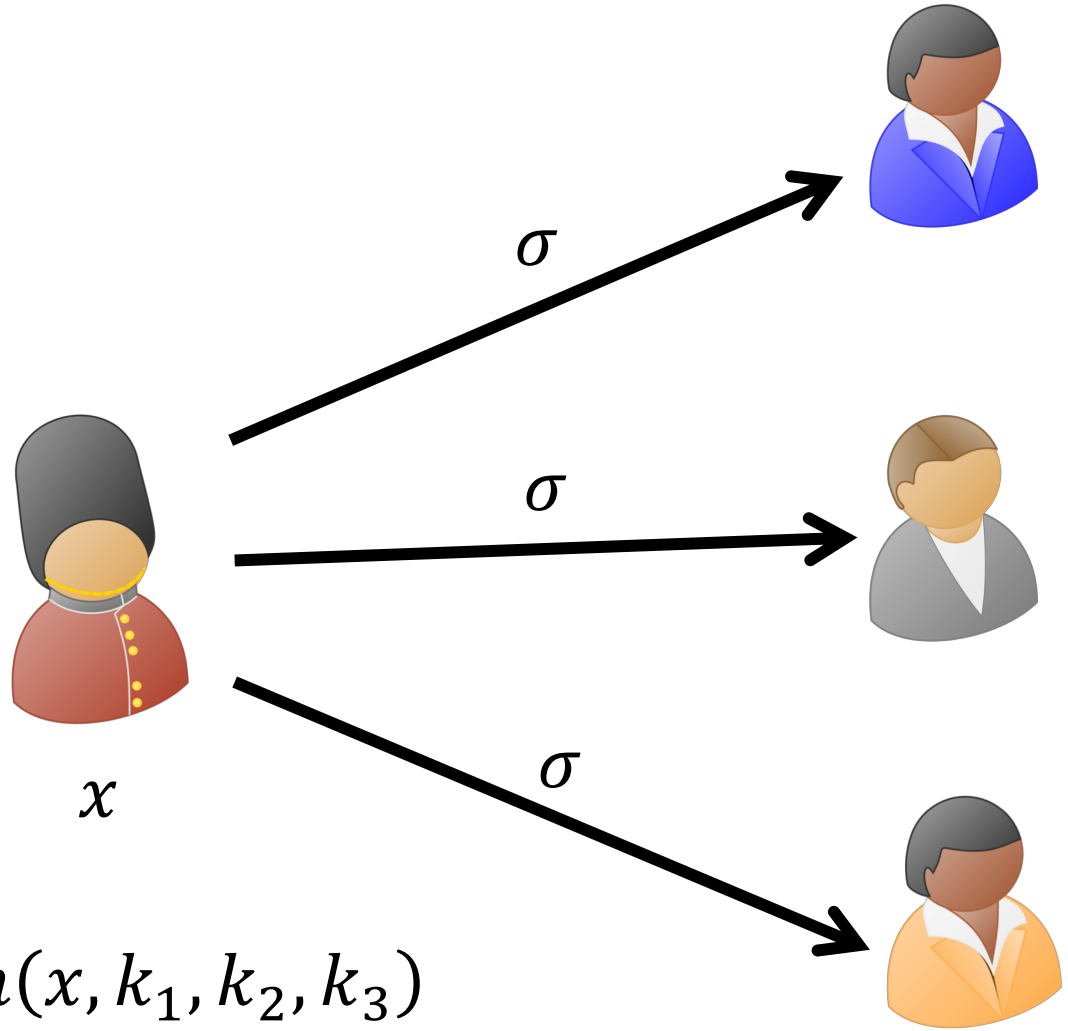


Our Tool: Multi-Key MAC



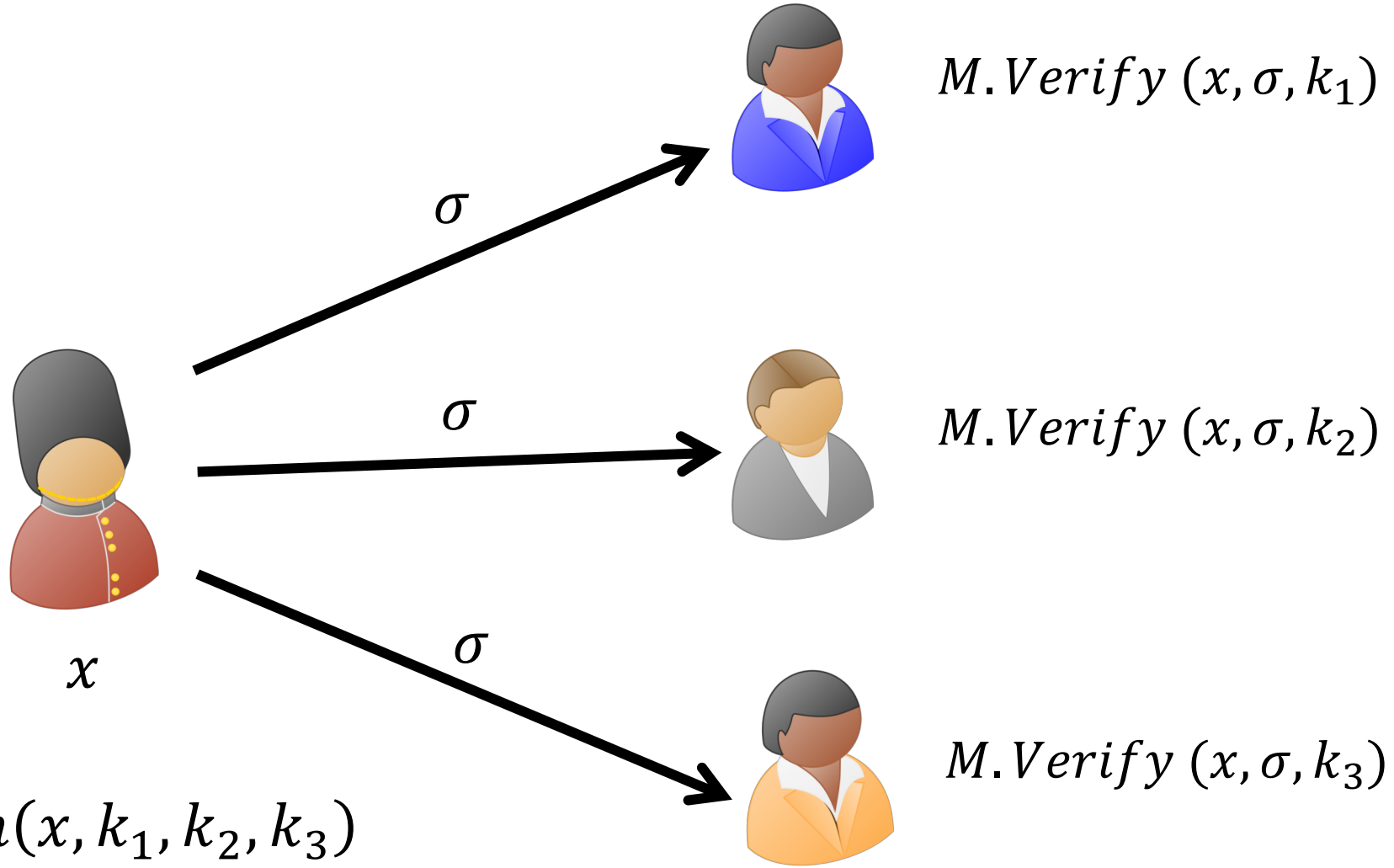
$$\sigma = Sign(x, k_1, k_2, k_3)$$

Our Tool: Multi-Key MAC



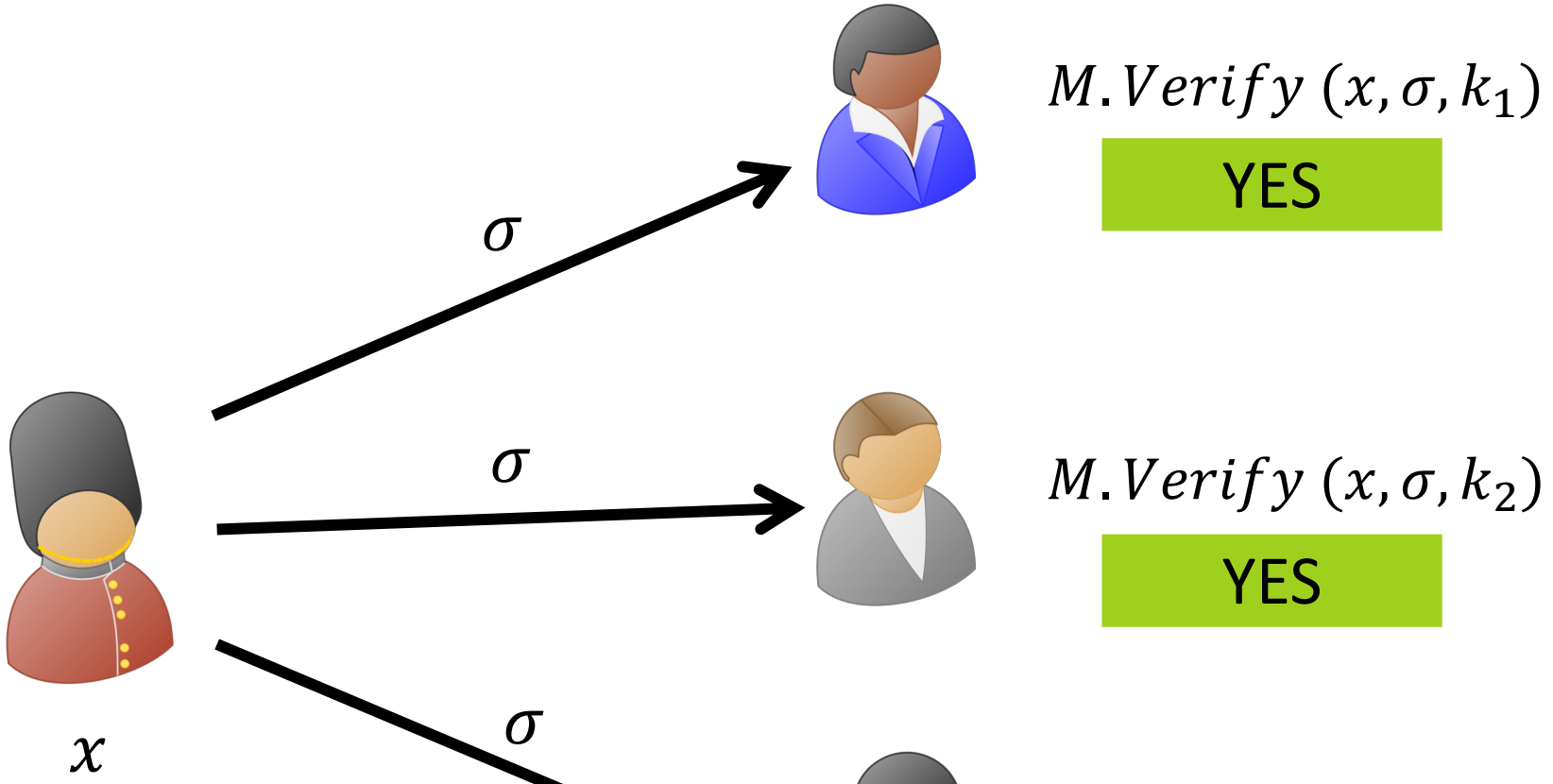
$\sigma = Sign(x, k_1, k_2, k_3)$

Our Tool: Multi-Key MAC



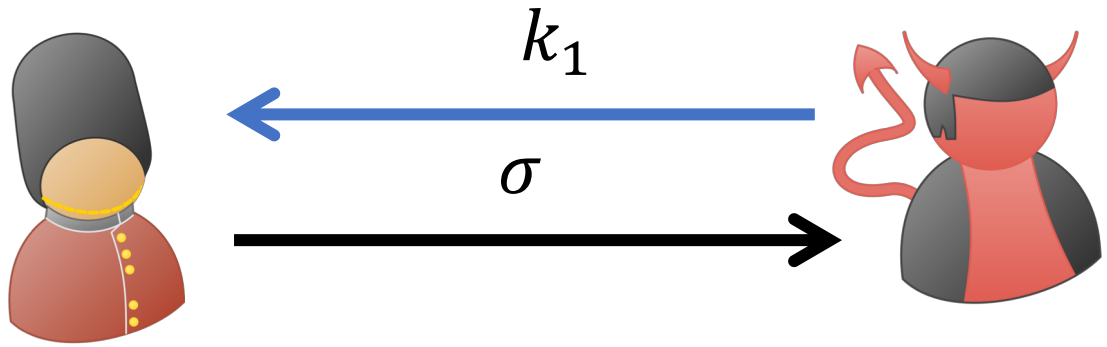
$\sigma = Sign(x, k_1, k_2, k_3)$

Our Tool: Multi-Key MAC (Correctness)



$$\sigma = Sign(x, k_1, k_2, k_3)$$

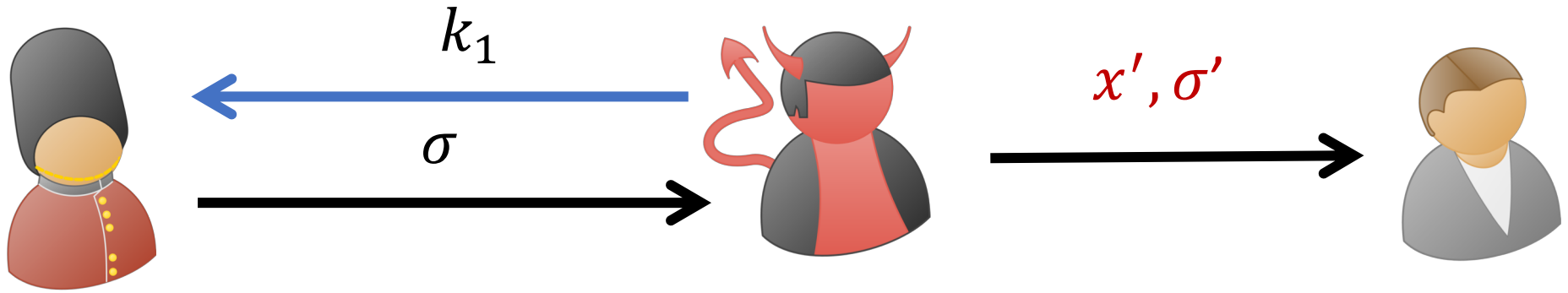
Our Tool: Multi-Key MAC (Security)



x, k_2, k_3

$\sigma = Sign(x, k_1, k_2, k_3)$

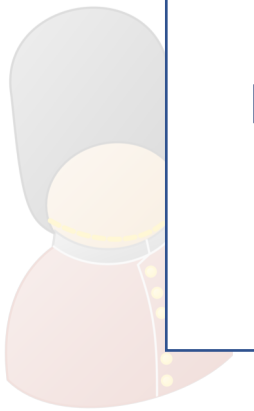
Our Tool: Multi-Key MAC (Security)



$\sigma = Sign(x, k_1, k_2, k_3)$

Our Tool: Multi-Key MAC (Security)

An adversary cannot output any valid message-signature pair other than the one it received



x, k_2, k_3

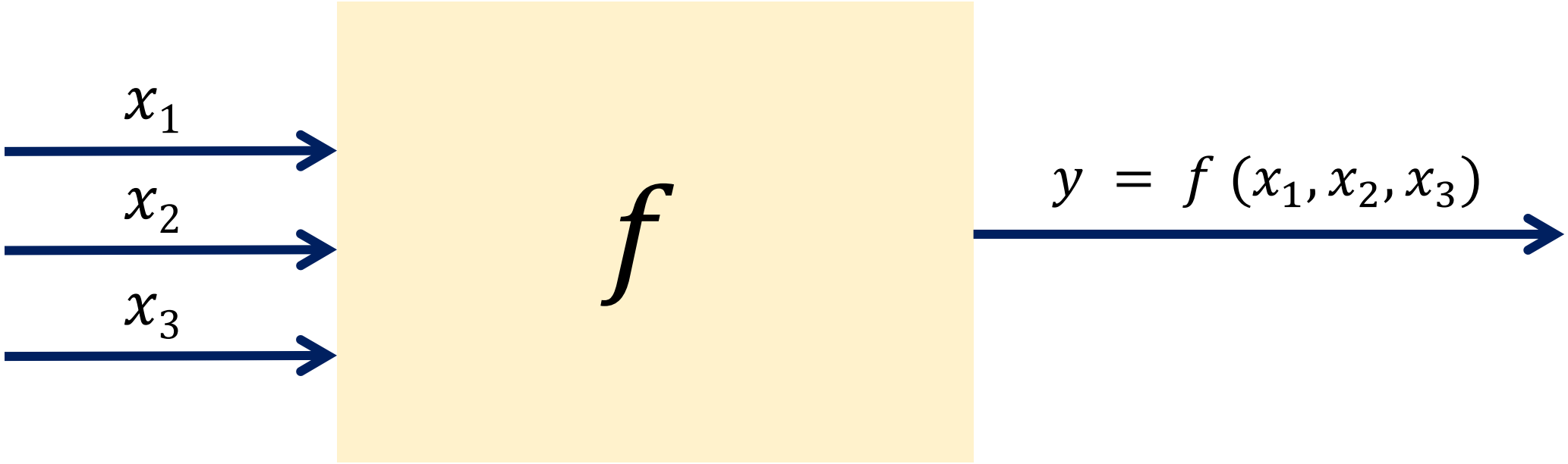
$\sigma = Sign(x, k_1, k_2, k_3)$

k_2

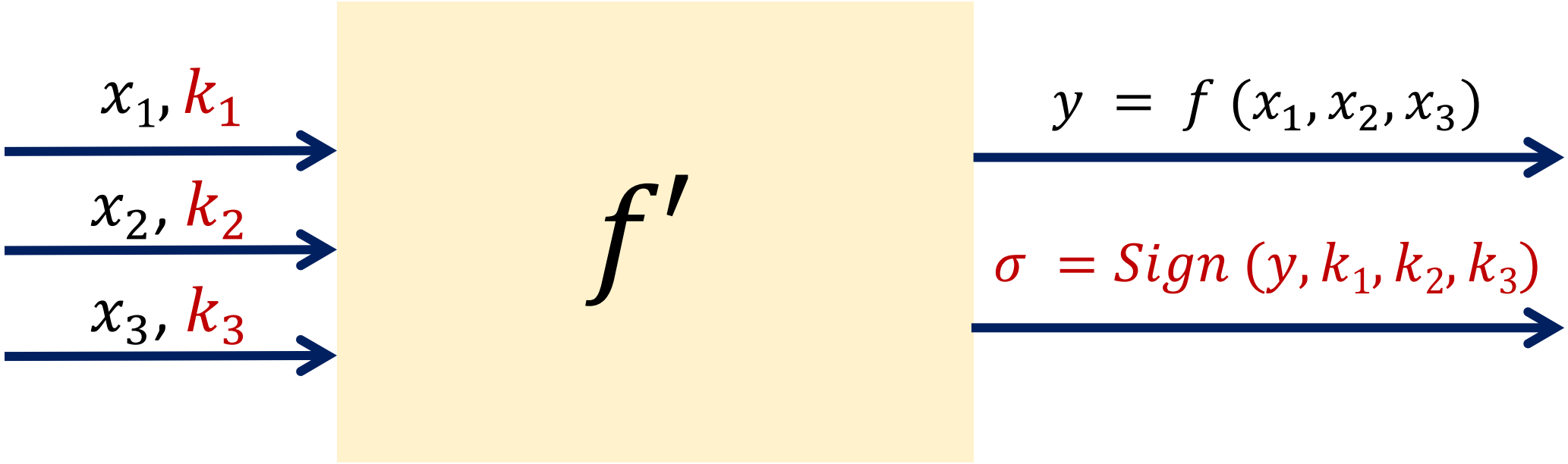
$M.Verify\ (x', \sigma', k_2)$

NO

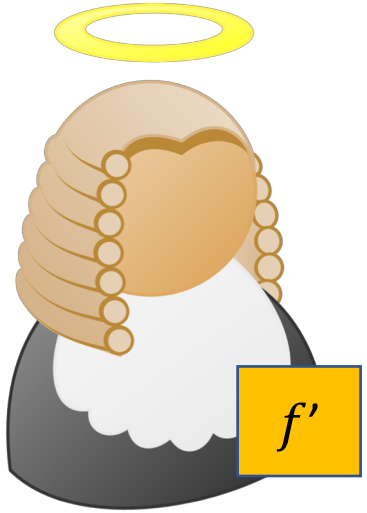
Using Multi-Key MAC



Using Multi-Key MAC

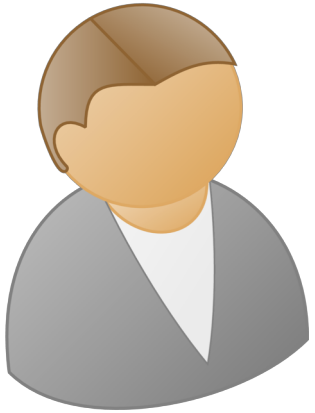


Using Multi-Key MAC



x_2, k_2

y, σ

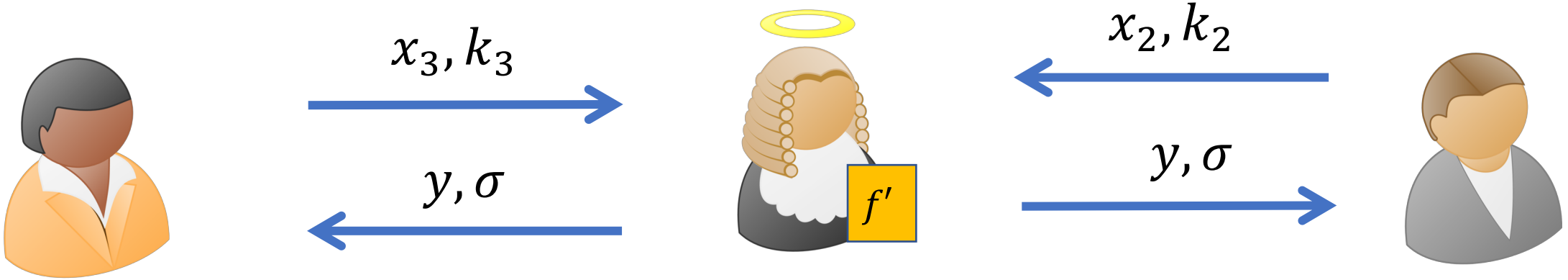


$M.Verify(y, \sigma, k_2)$

Trusted Party

Party 2

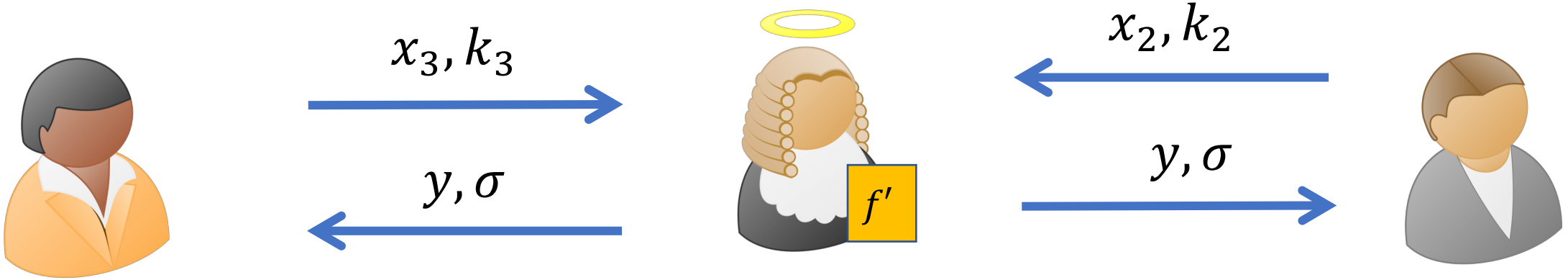
Security with abort: Using Multi-Key MAC



Honest Party 3 Trusted Party Honest Party 2

IF $y, \sigma = f'((x_1 k_1), (x_2, k_2), (x_3, k_3))$

Security with abort: Using Multi-Key MAC



Honest Party 3

Trusted Party

Honest Party 2

$M.Verify(y, \sigma, k_3)$

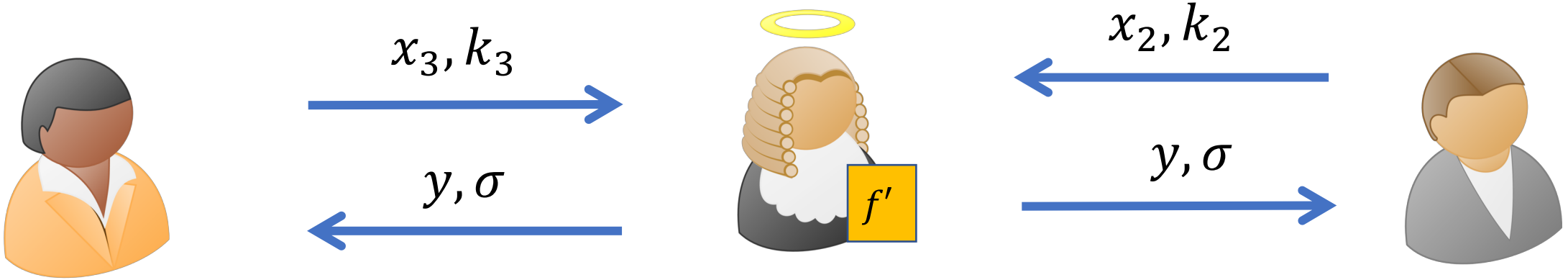
YES

IF $y, \sigma = f'((x_1 k_1), (x_2, k_2), (x_3, k_3))$

$M.Verify(y, \sigma, k_2)$

YES

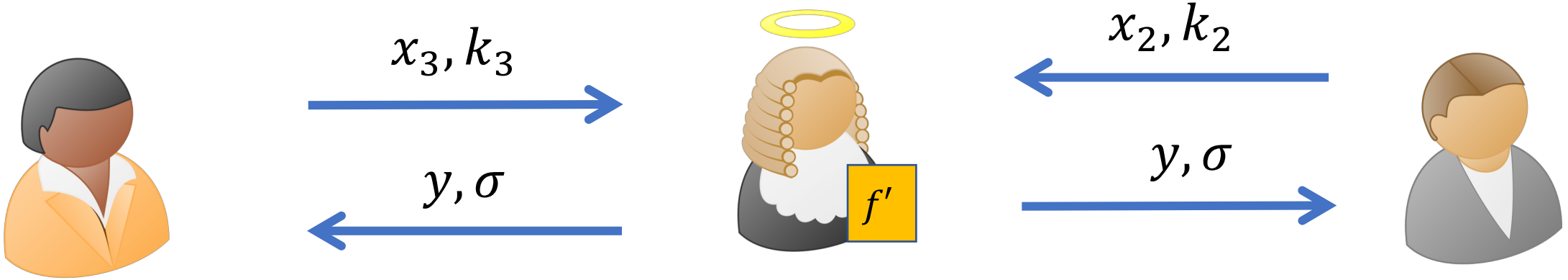
Security with abort: Using Multi-Key MAC



Honest Party 3 Trusted Party Honest Party 2

IF $y, \sigma \neq f'((x_1 k_1), (x_2, k_2), (x_3, k_3))$

Security with abort: Using Multi-Key MAC



Honest Party 3

Trusted Party

Honest Party 2

$M.Verify(y, \sigma, k_3)$

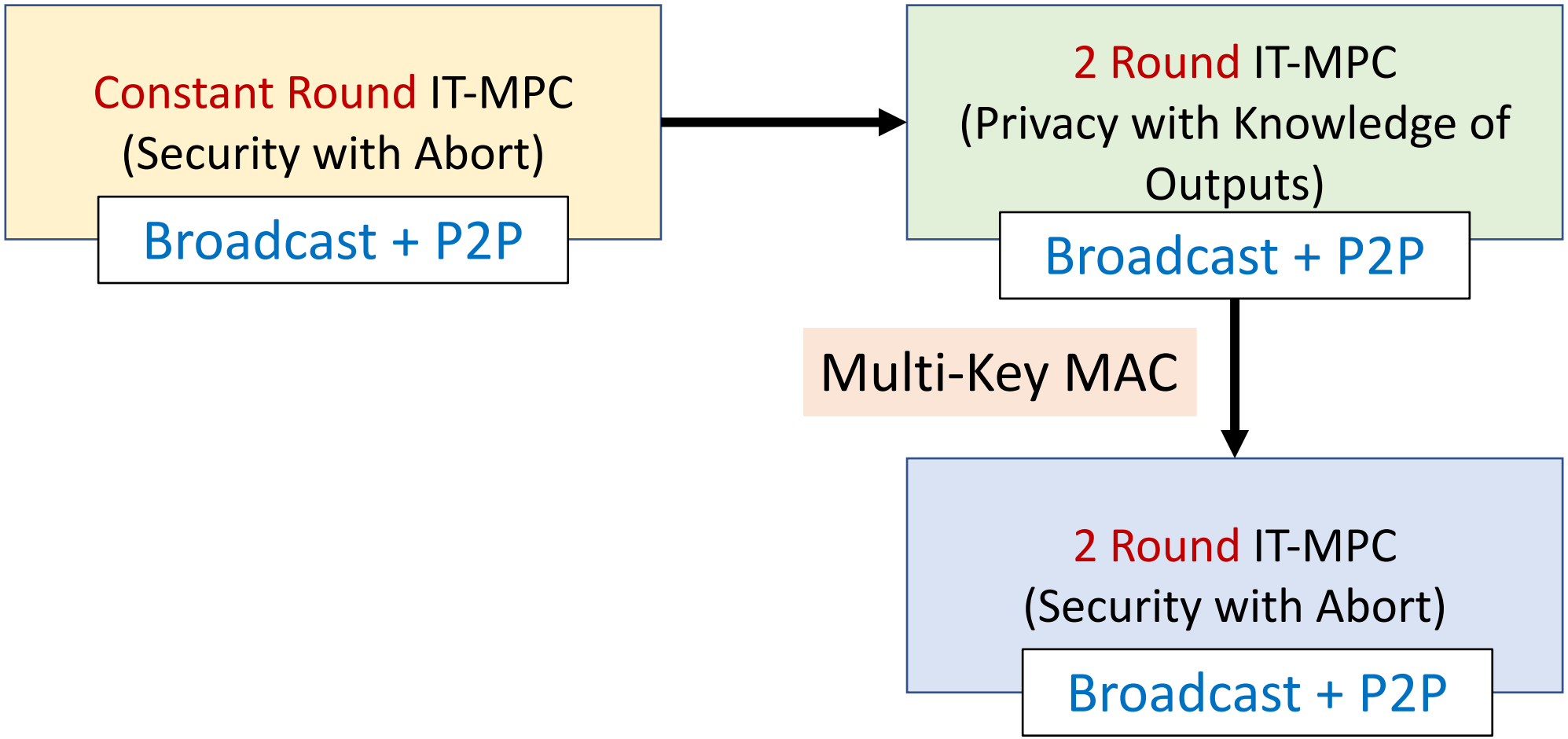
NO

IF $y, \sigma \neq f'((x_1 k_1), (x_2, k_2), (x_3, k_3))$

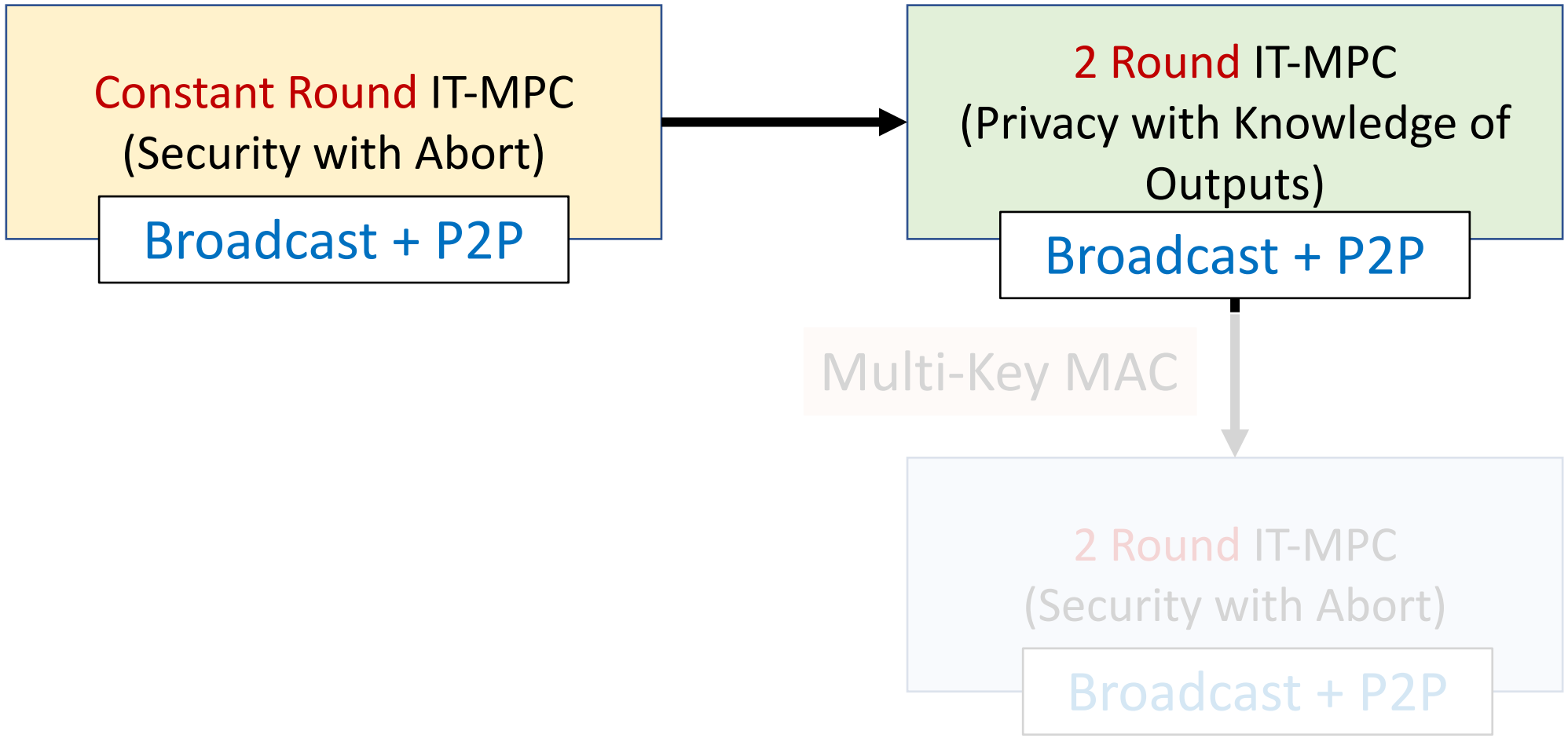
$M.Verify(y, \sigma, k_2)$

NO

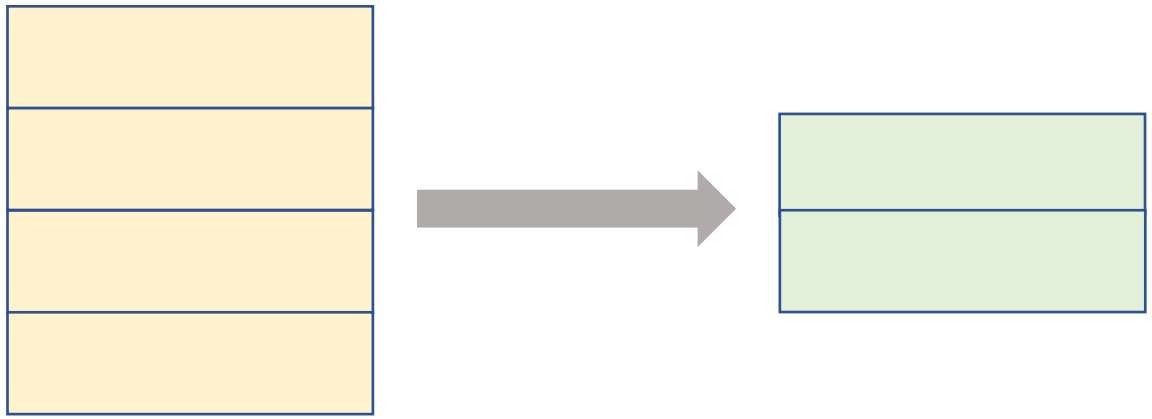
Recall: Our Strategy



Second Step


Constant Round IT-MPC
(Security with Abort)
Broadcast + P2P
2 Round IT-MPC
(Privacy with Knowledge of Outputs)
Broadcast + P2P
Multi-Key MAC
2 Round IT-MPC
(Security with Abort)
Broadcast + P2P

Technique: Round Compression



Interactive secure MPC

2 round secure MPC

[GGHR'13]
Indistinguishability Obfuscation

[GLS'15]
Witness Encryption + Garbled circuits

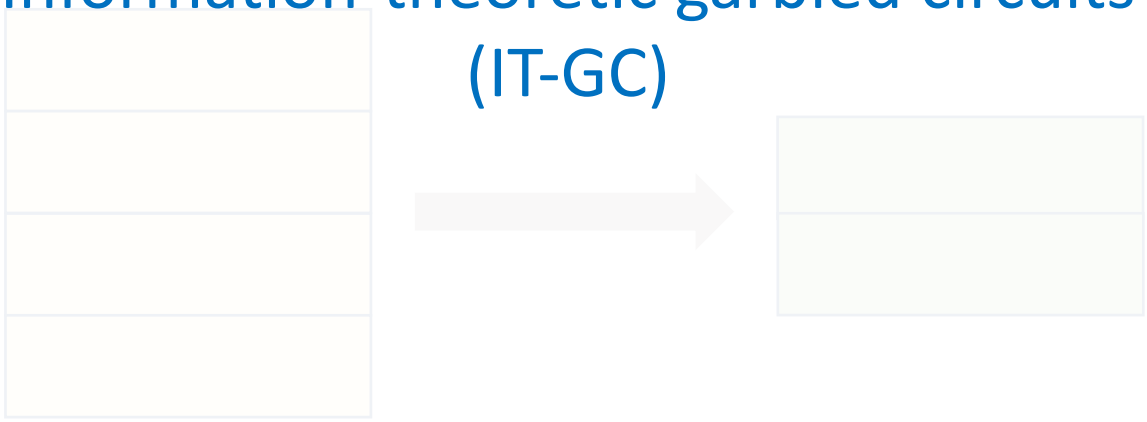
[GS'17]
Bilinear Maps + Garbled circuits

[GS'18, BL'18]
OT + Garbled Circuits

[ACGJ'18]
Garbled circuits

Initial Idea

Replace garbled circuits with
Information-theoretic garbled circuits
(IT-GC)



Interactive secure MPC

2 round secure MPC

[GGHR'13]
Indistinguishability Obfuscation

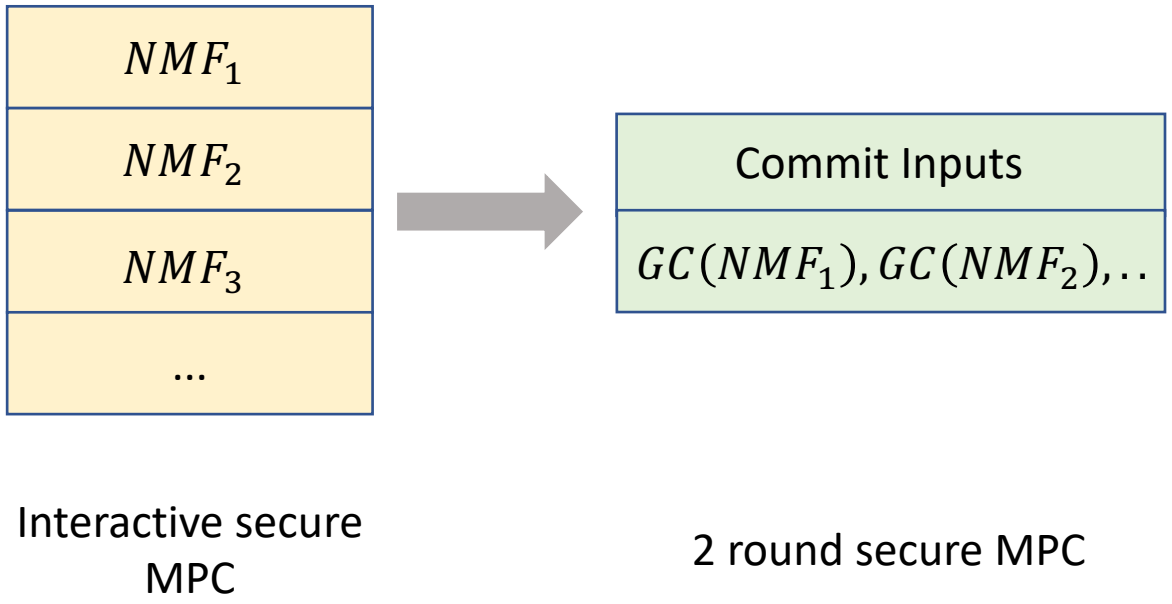
[GLS'15]
Witness Encryption + Garbled circuits

[GS'17]
Bilinear Maps + Garbled circuits

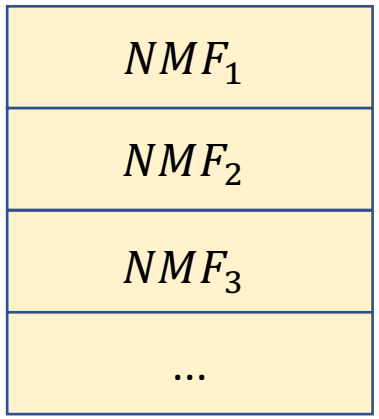
[GS'18, BL'18]
OT + Garbled Circuits

[ACGJ'18]
Garbled circuits

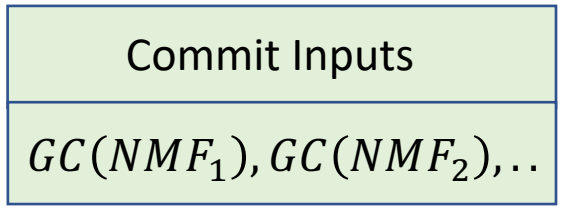
Round Compression Template



Round Compression Template

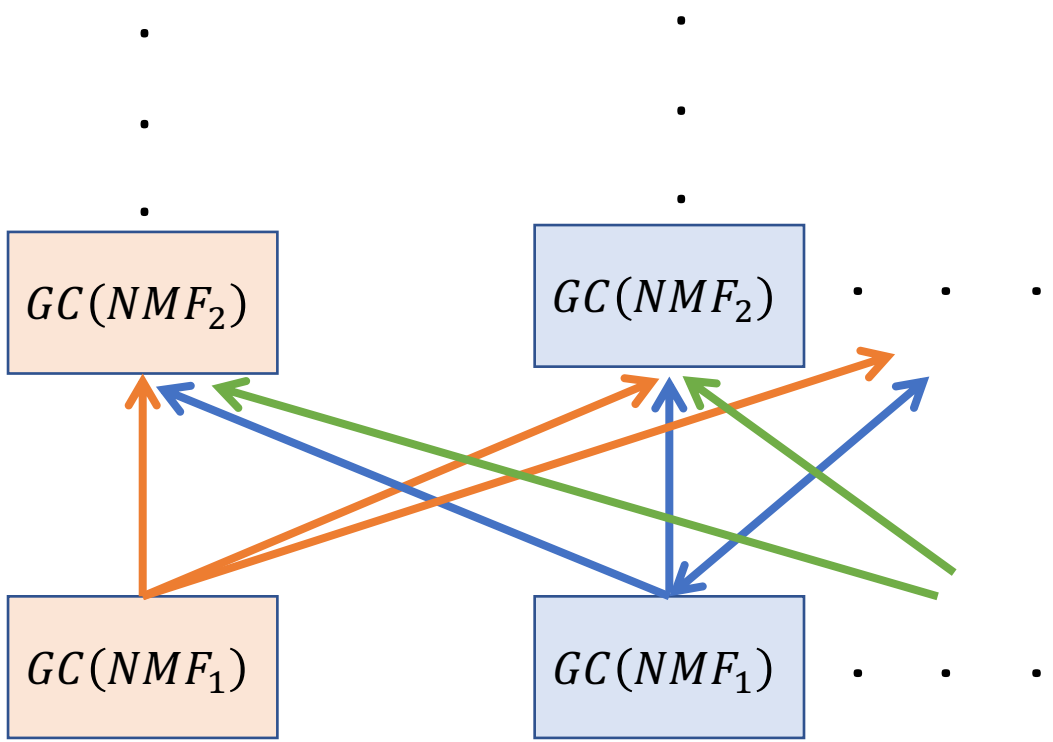


Interactive secure MPC



2 round secure MPC

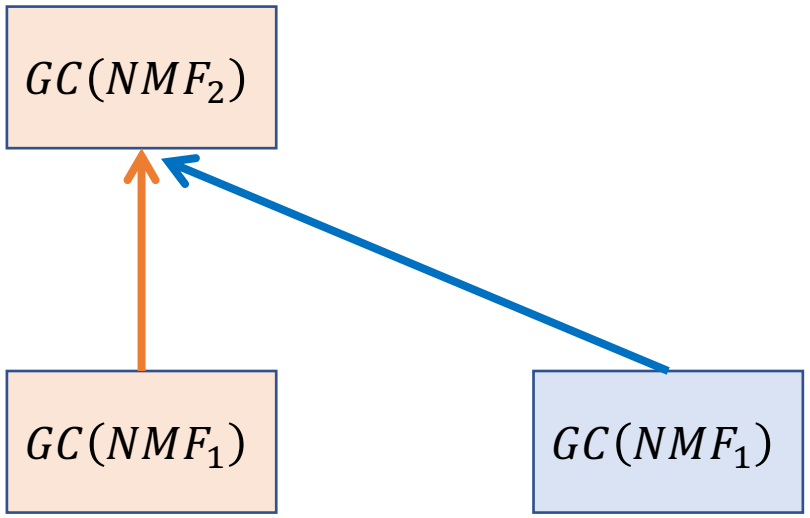
After Round 2



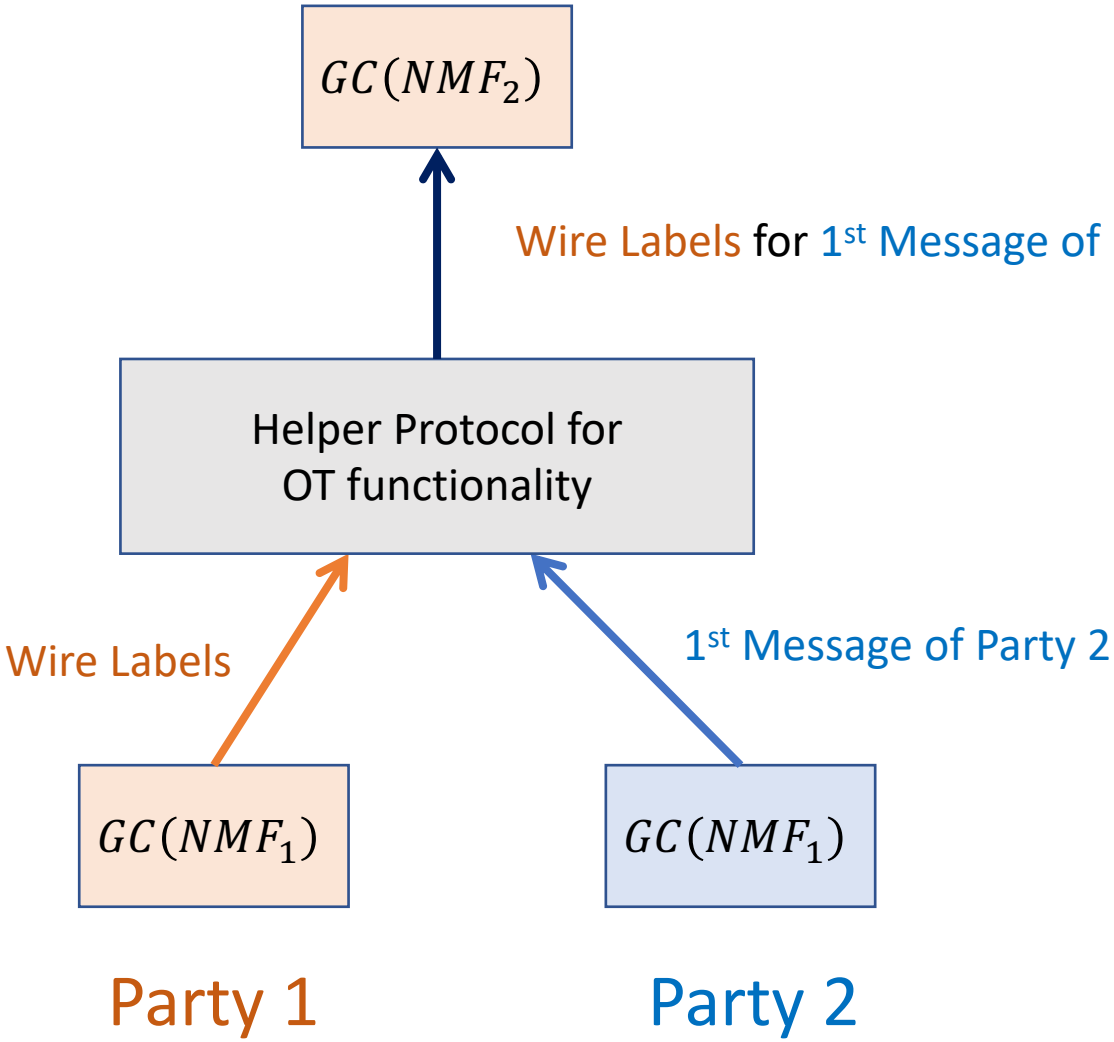
Party 1

Party 2

Round Compression Template: After Round 2



Round Compression Template: After Round 2



Initial Idea: Doesn't Work

Replace garbled circuits with
Information-theoretic garbled circuits
(IT-GC)

Problem

Size of the input wire labels in IT-GC grows exponentially in the depth of the circuit being garbled.

[GGHR'13]
Indistinguishability Obfuscation

[GLS'15]
Witness Encryption + Garbled circuits

[GS'17]
Bilinear Maps + Garbled circuits

[GS'18, BL'18]
OT + Garbled Circuits

Interactive secure MPC

2 round secure MPC

[ACGJ'18]
Garbled circuits

Initial Idea: Doesn't Work

Replace garbled circuits with
Information-theoretic garbled circuits
(IT-GC)

Problem

Size of the input wire labels in IT-GC grows exponentially in the depth of the circuit being garbled.

$$Size(NMF) \approx |C|$$

[ACGJ'18]
Garbled circuits

[GGHR'13]
Indistinguishability Obfuscation

[GLS'15]
Witness Encryption + Garbled circuits

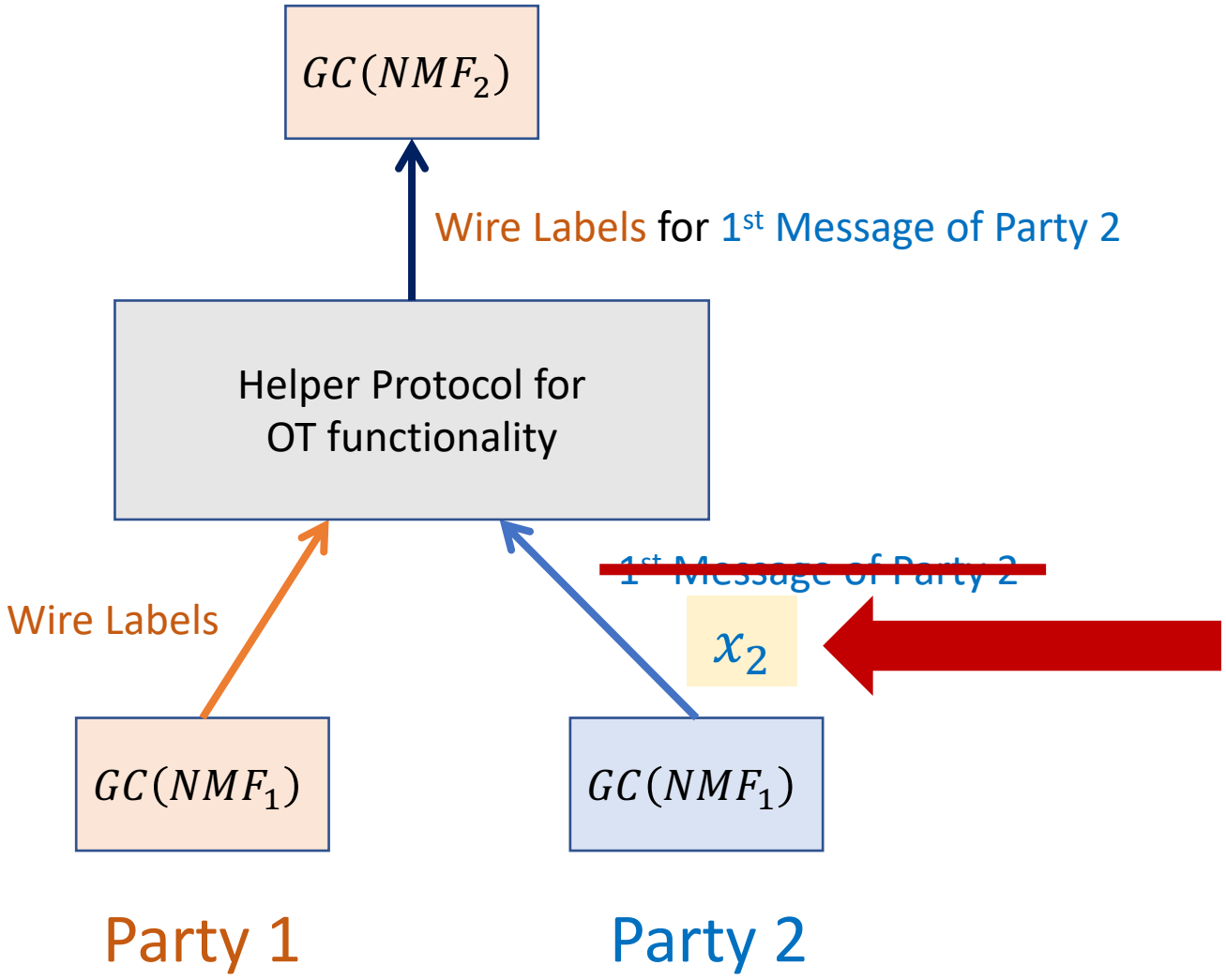
[GS'17]
Bilinear Maps + Garbled circuits

[GS'18, BL'18]
OT + Garbled Circuits

Interactive secure MPC

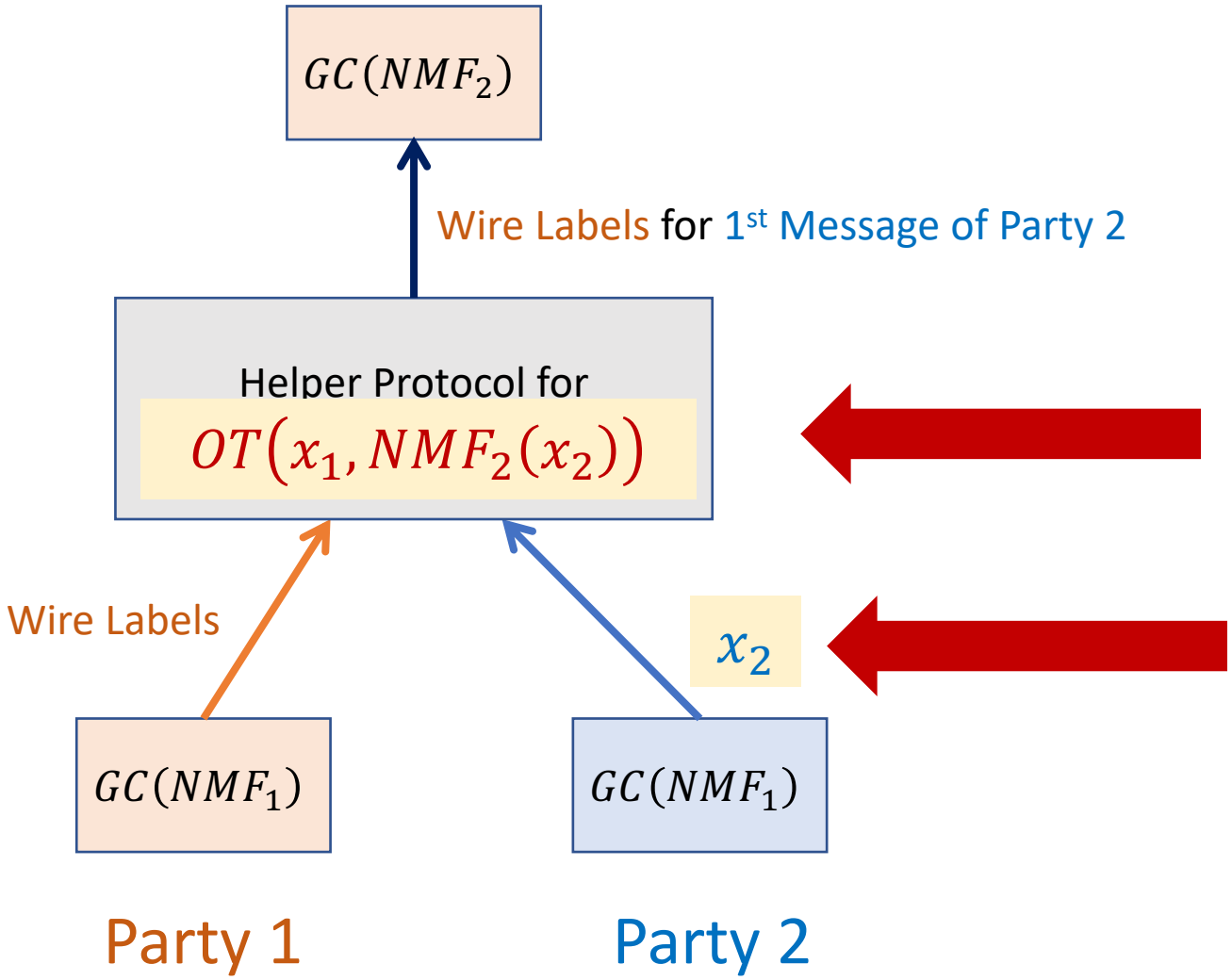
2 round secure MPC

Our Approach



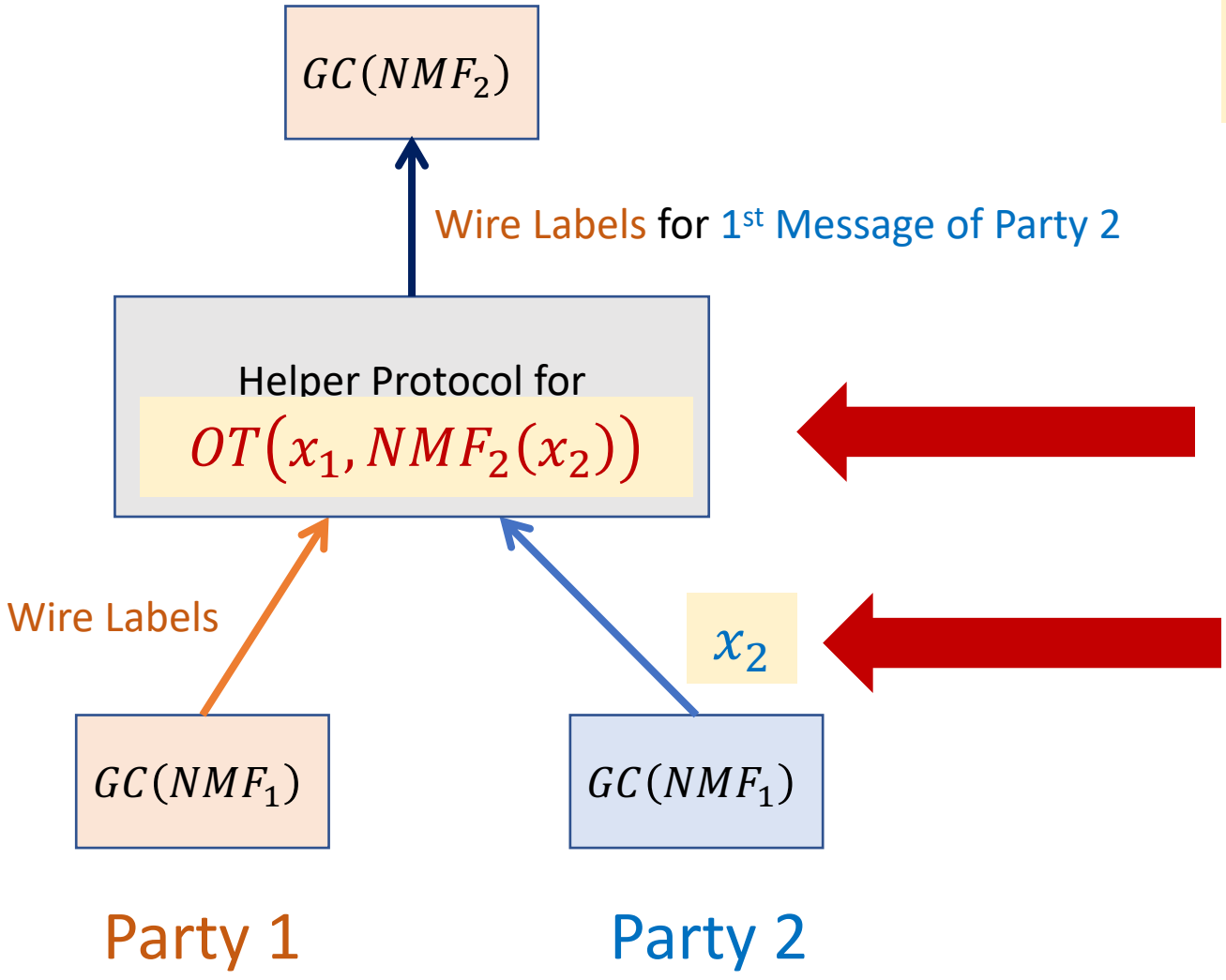
Similar to the approach used in [BL'18]

Our Approach



Our Approach

Design a 2 round helper protocol for $OT\left(x_1, NMF_2(x_2)\right)$



Challenges in Designing such a protocol

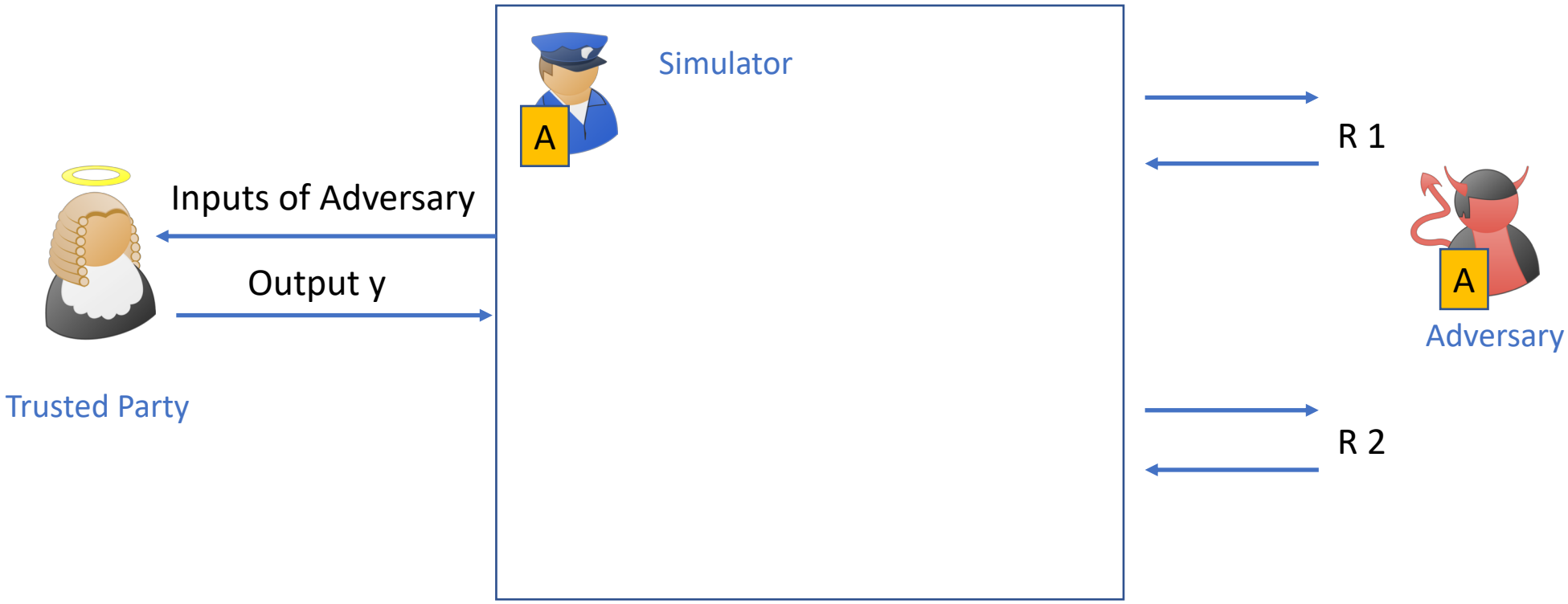
2 Round MPC Template using a 2 Round Helper Protocol

R 1 — 1st round of Helper Protocol (implicitly commits to inputs)

R 2 — 2nd round of Helper Protocol & $GC(NMF_1), GC(NMF_2), ..$

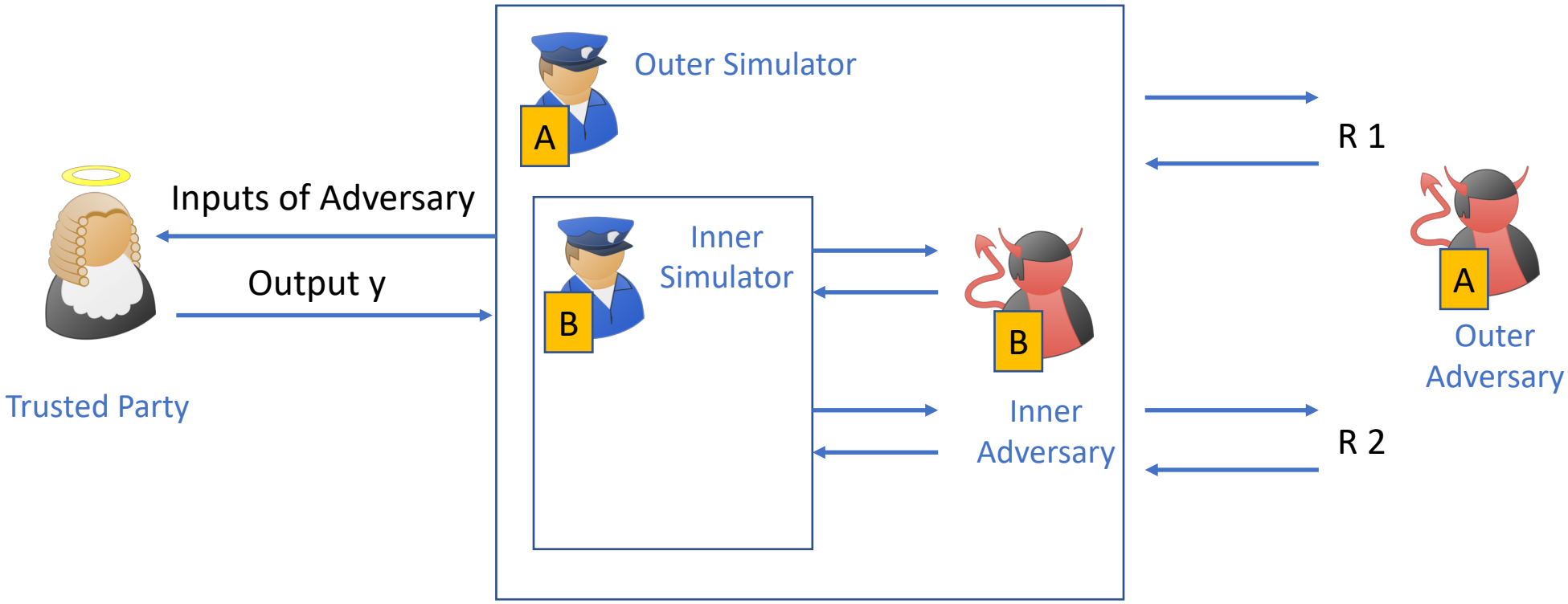
Challenges in Designing such a protocol

Malicious Security



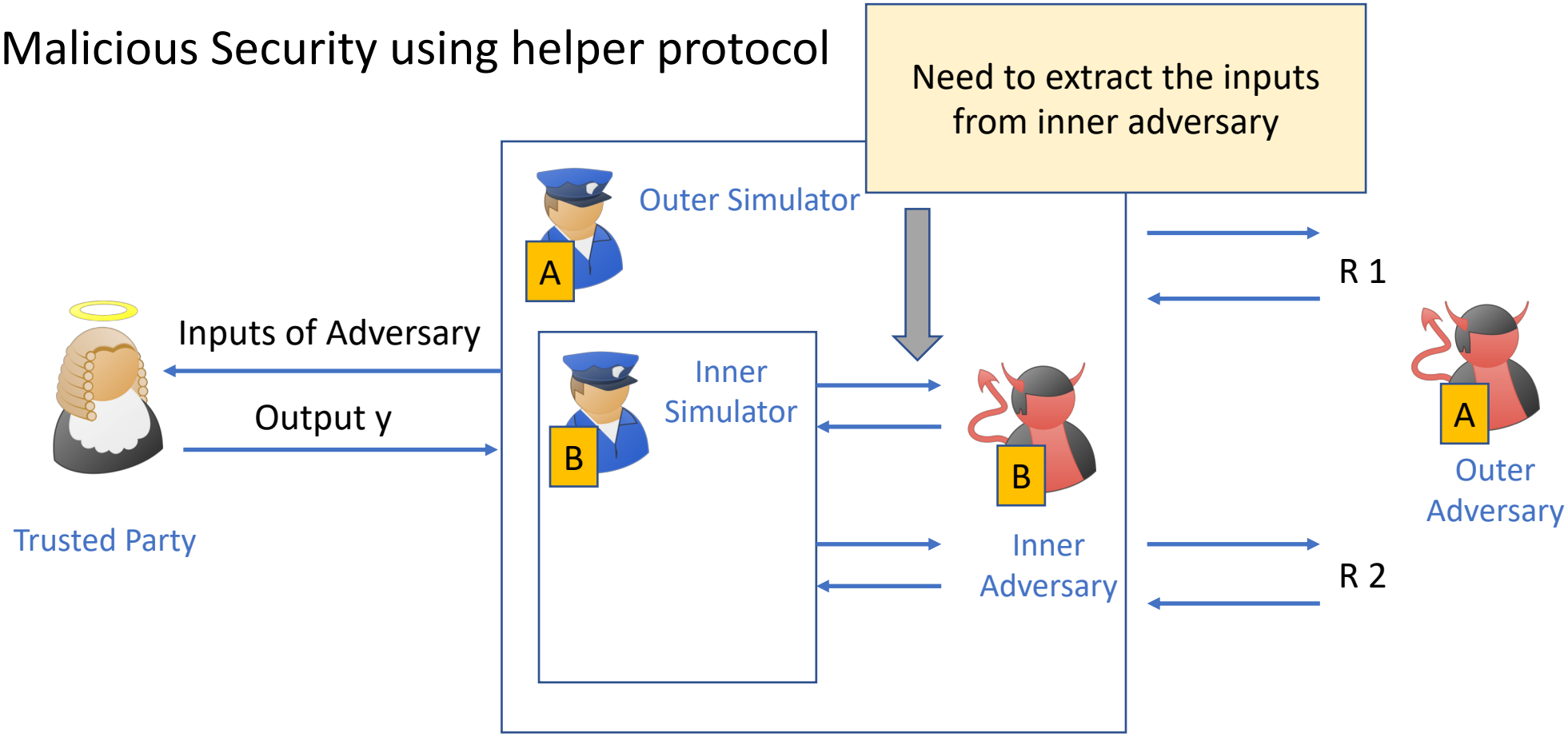
Challenges in Designing such a protocol

Malicious Security using helper protocol

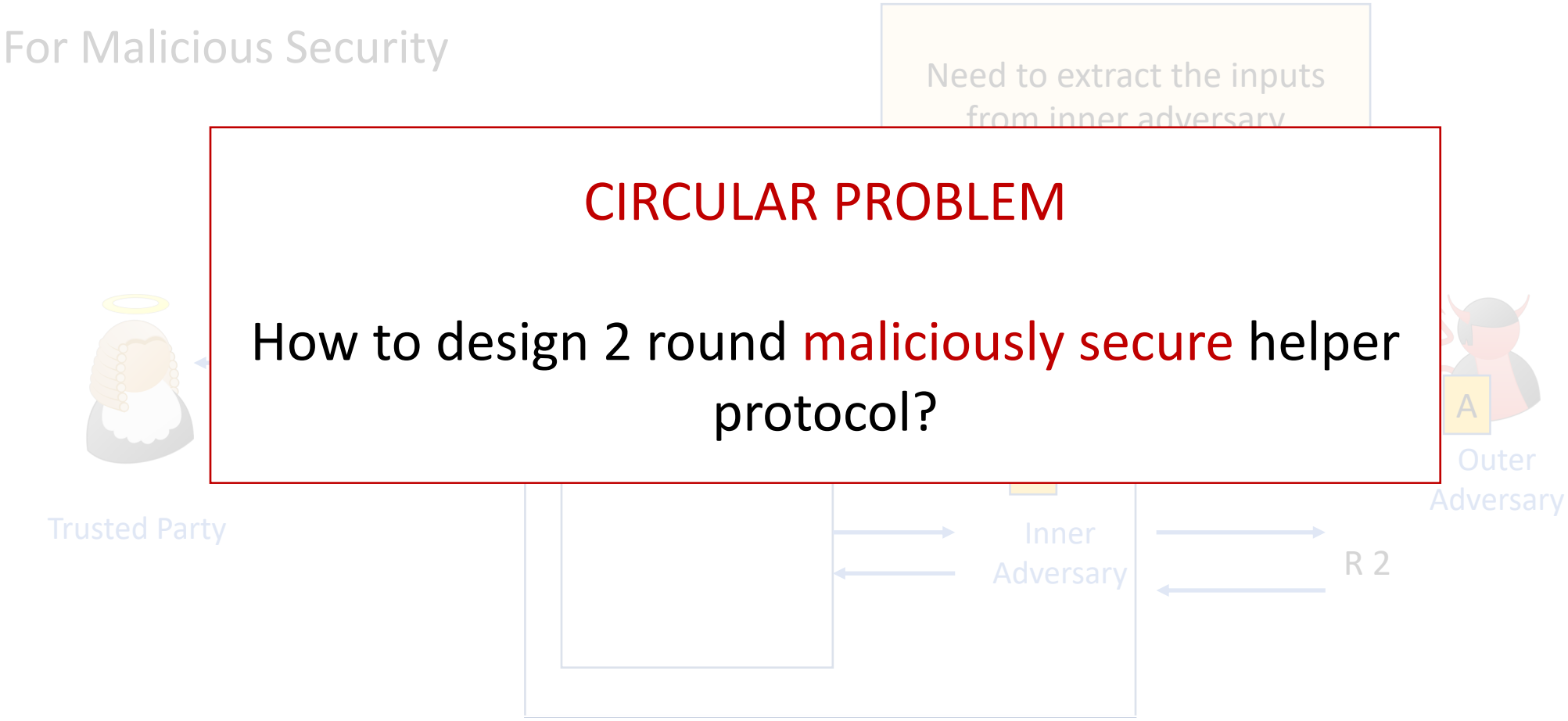


Challenges in Designing such a protocol

Malicious Security using helper protocol



Challenges in Designing such a protocol



Thank You

https://eprint.iacr.org/2018/1078

aarushig@cs.jhu.edu