On Perfectly Secure Two-Party Computation for Symmetric Functionalities with Correlated Randomness

Bar Alon
Ariel University

Olga Nissenbaum
Ariel University

Eran Omri
Ariel University

Anat Paskin-Cherniavsky
Ariel University

Arpita Patra
Indian Institute of Science

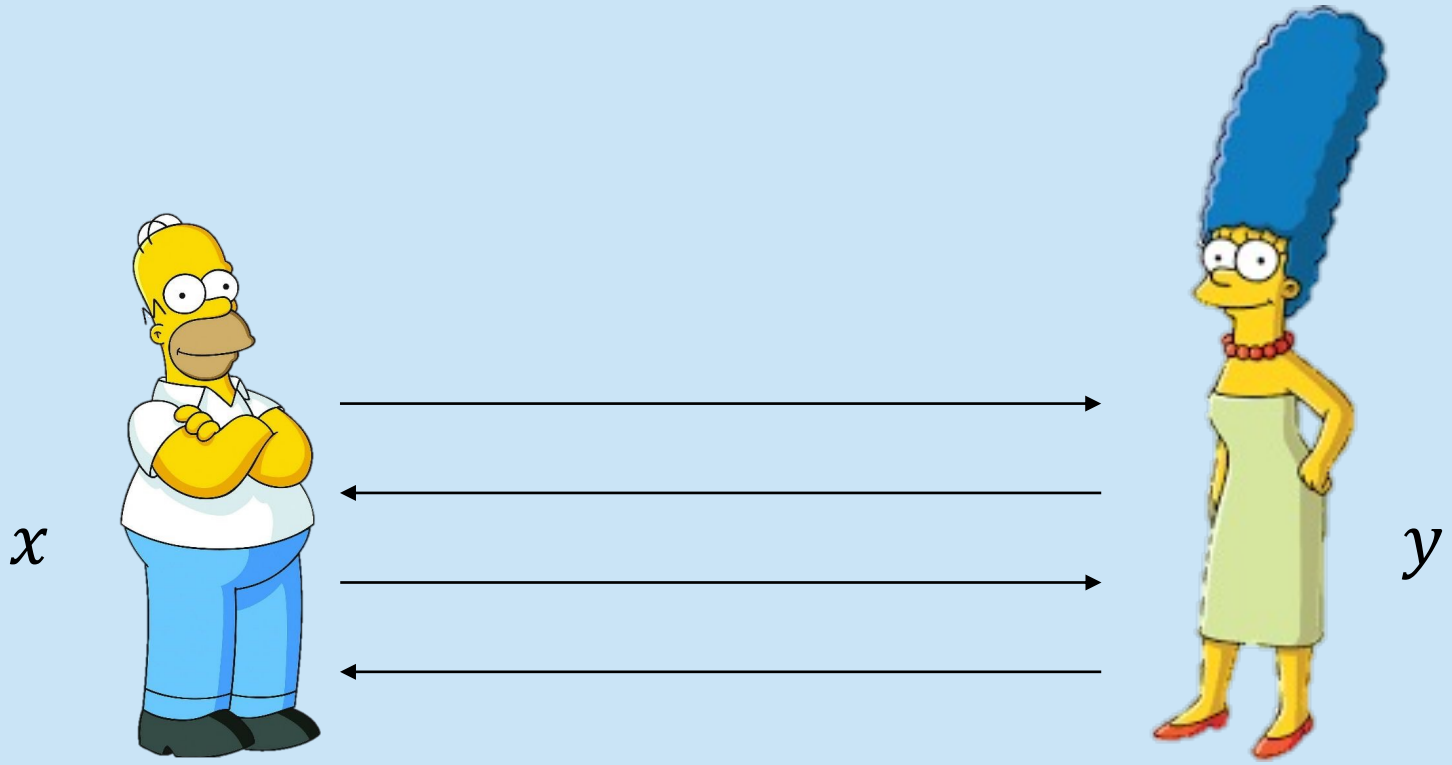
TCC 2022

Secure Two-Party Computation

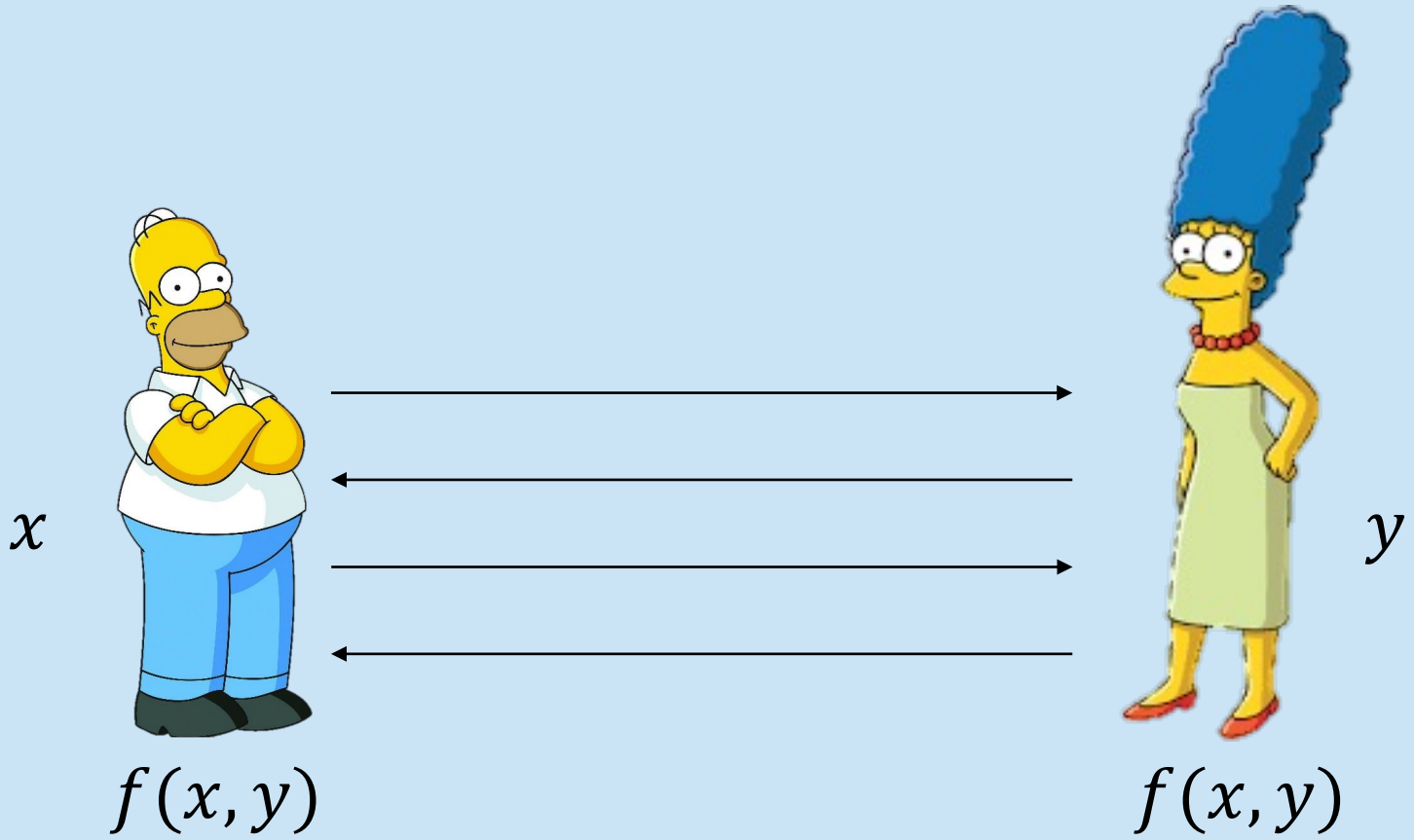
x

y

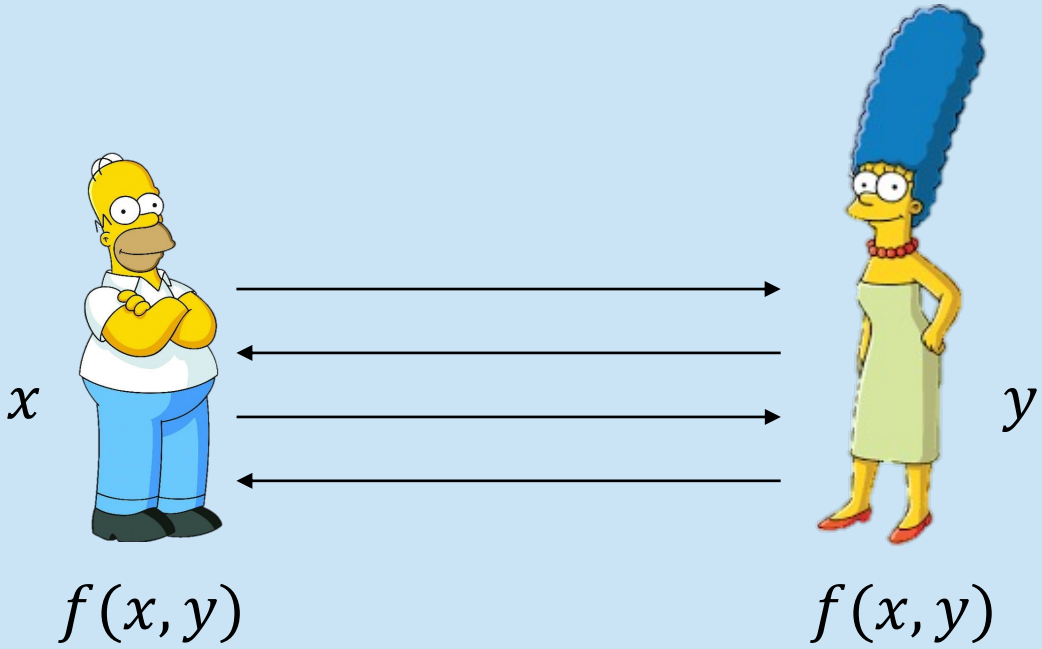
Secure Two-Party Computation



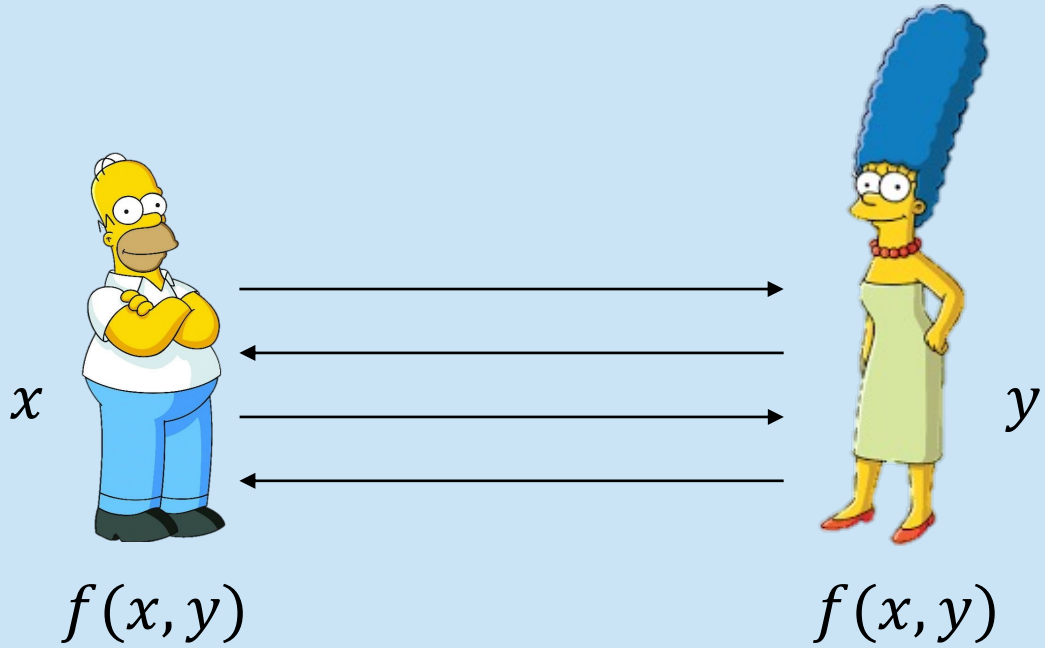
Secure Two-Party Computation

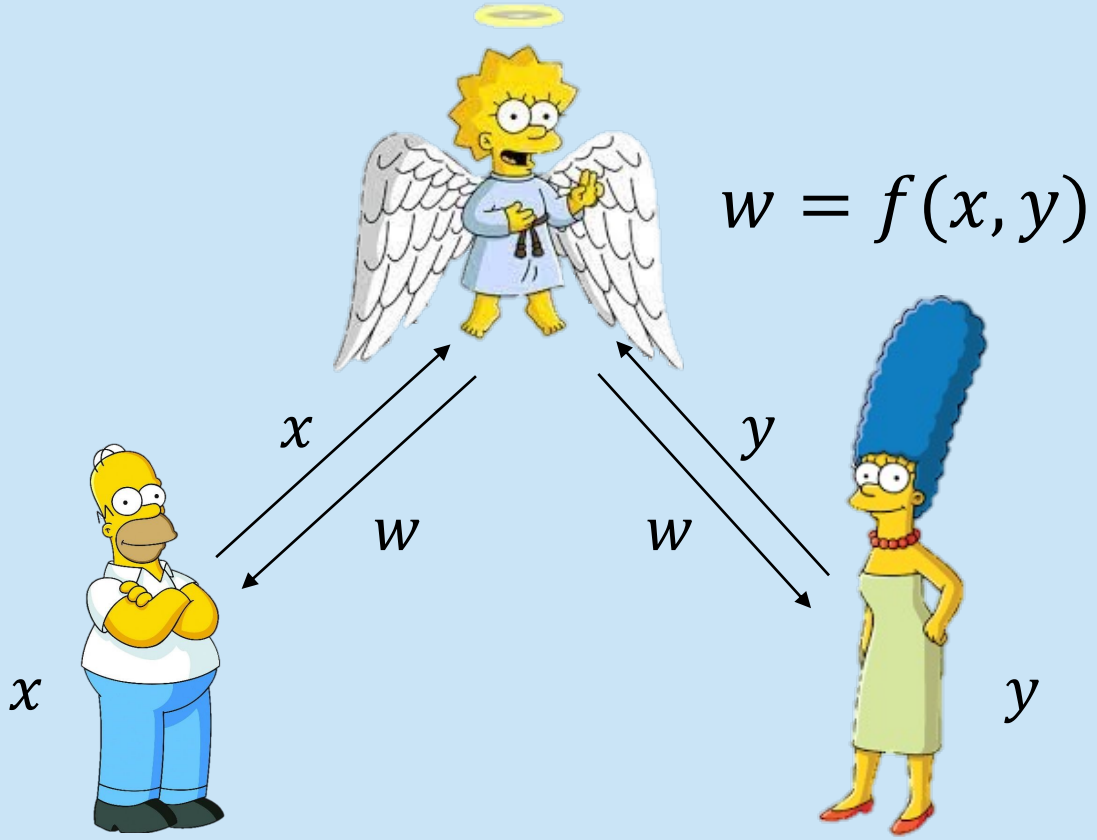


Perfect Security in a Nutshell

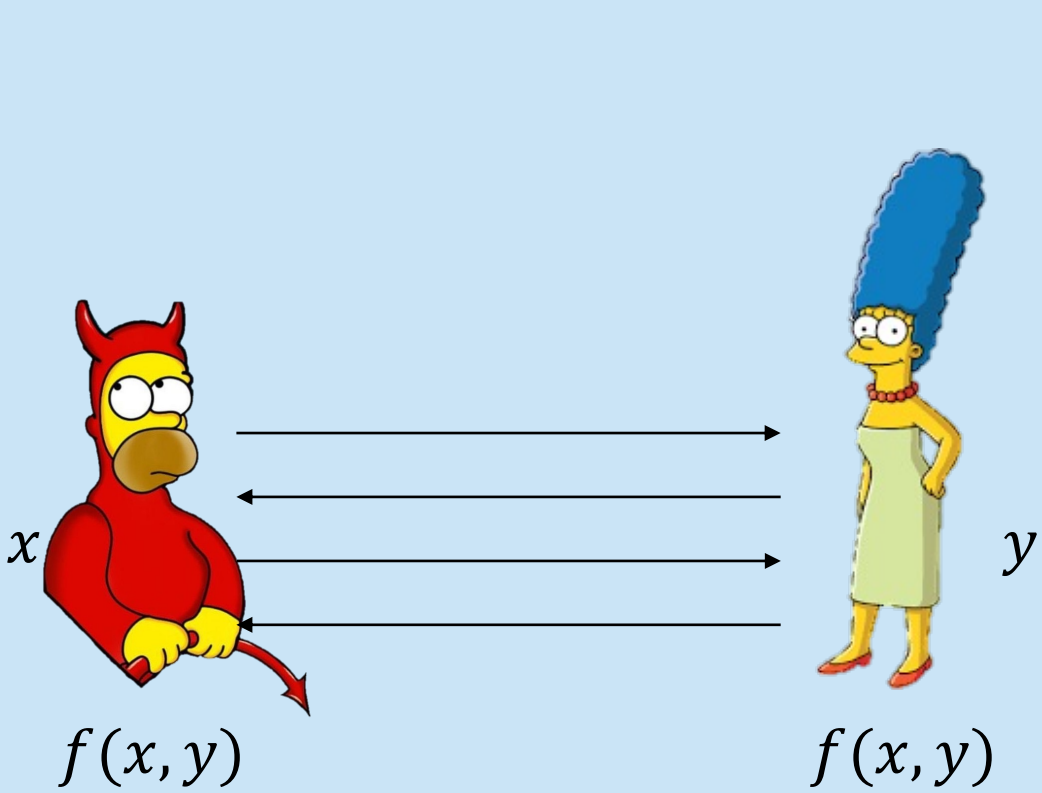


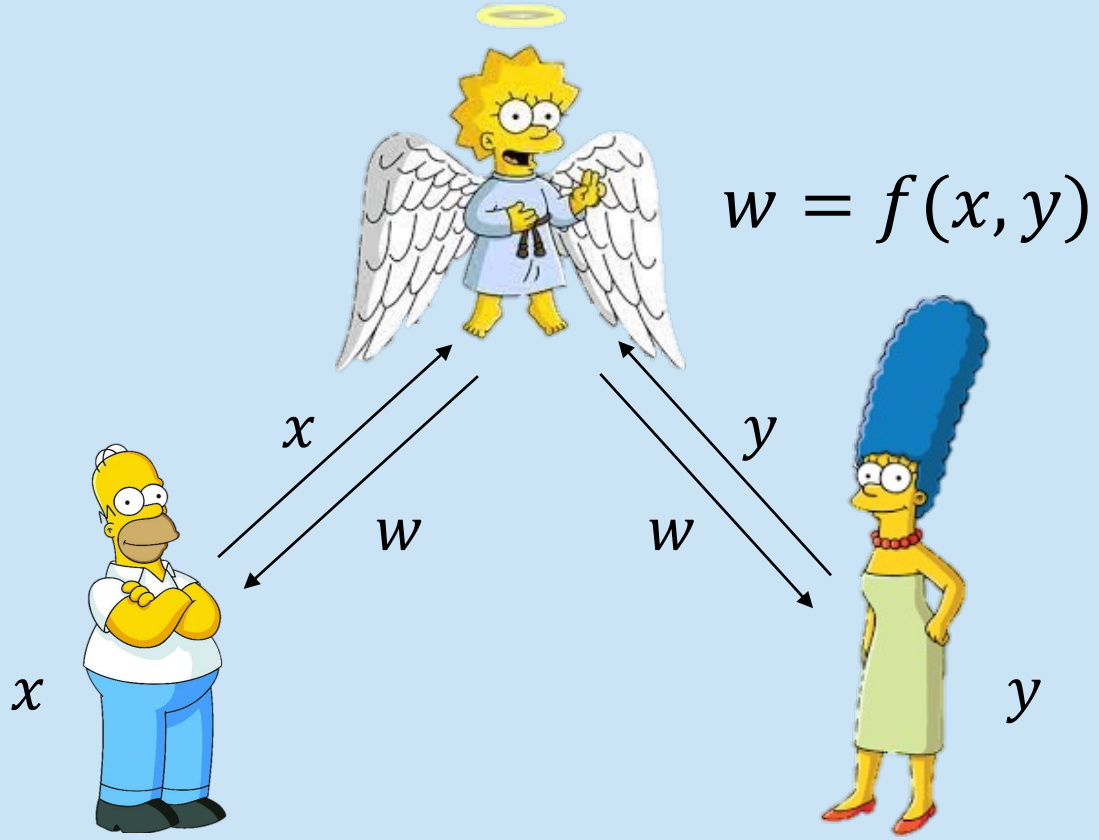
Perfect Security in a Nutshell



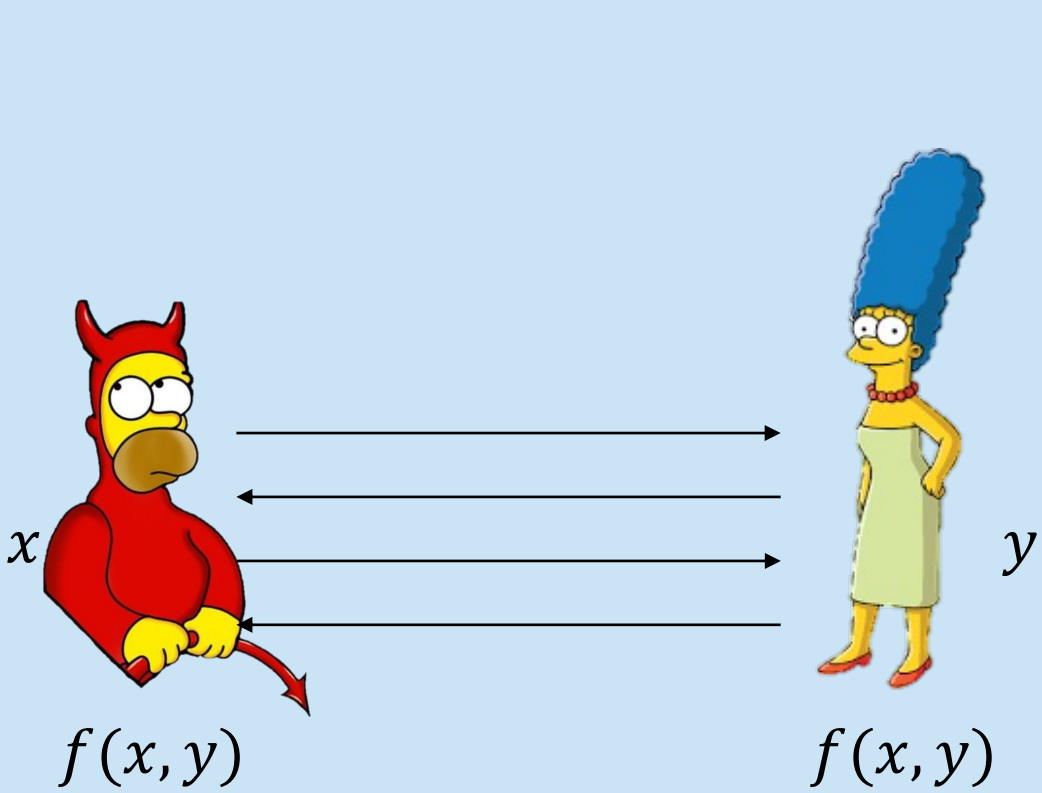


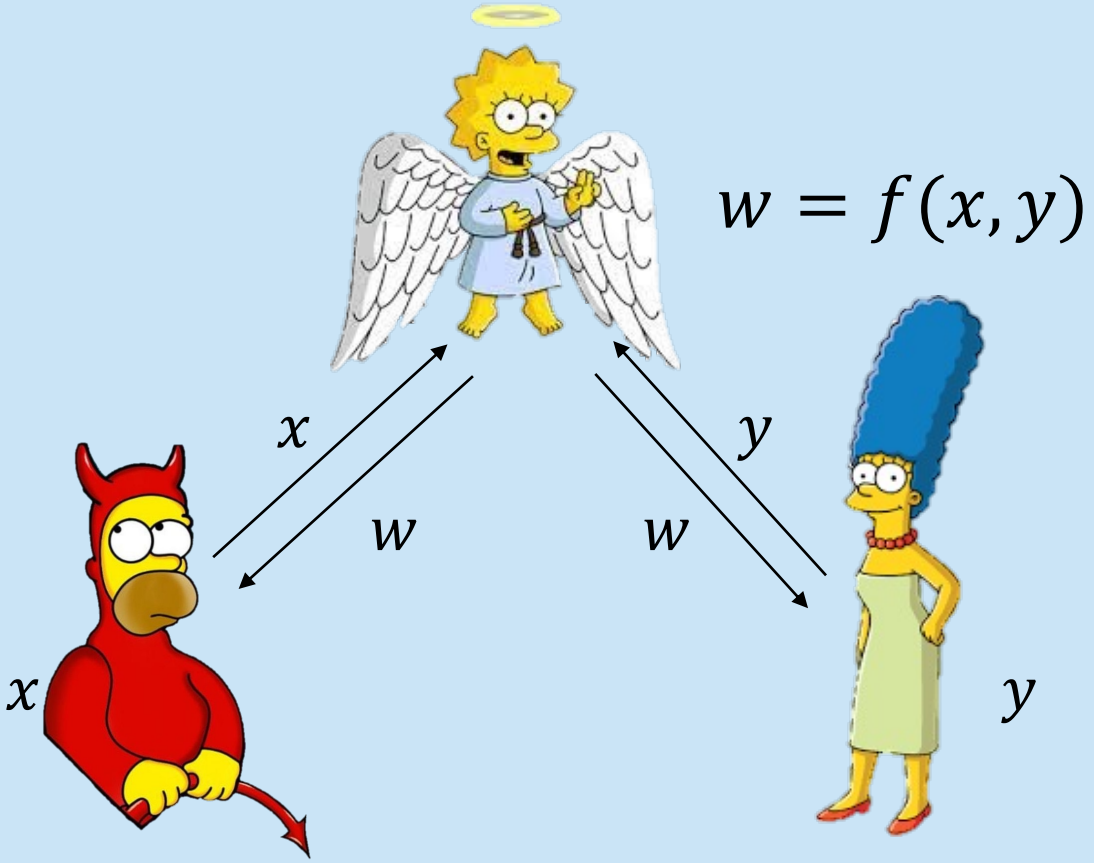
Perfect Security in a Nutshell



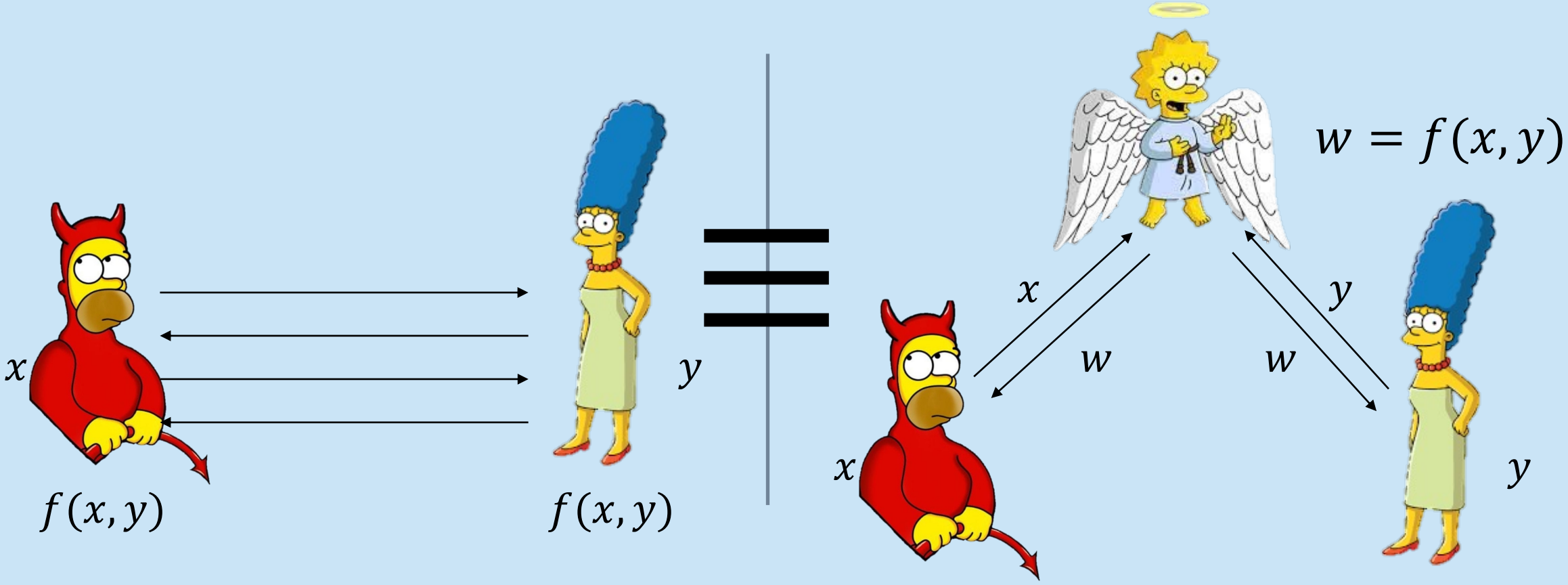


Perfect Security in a Nutshell

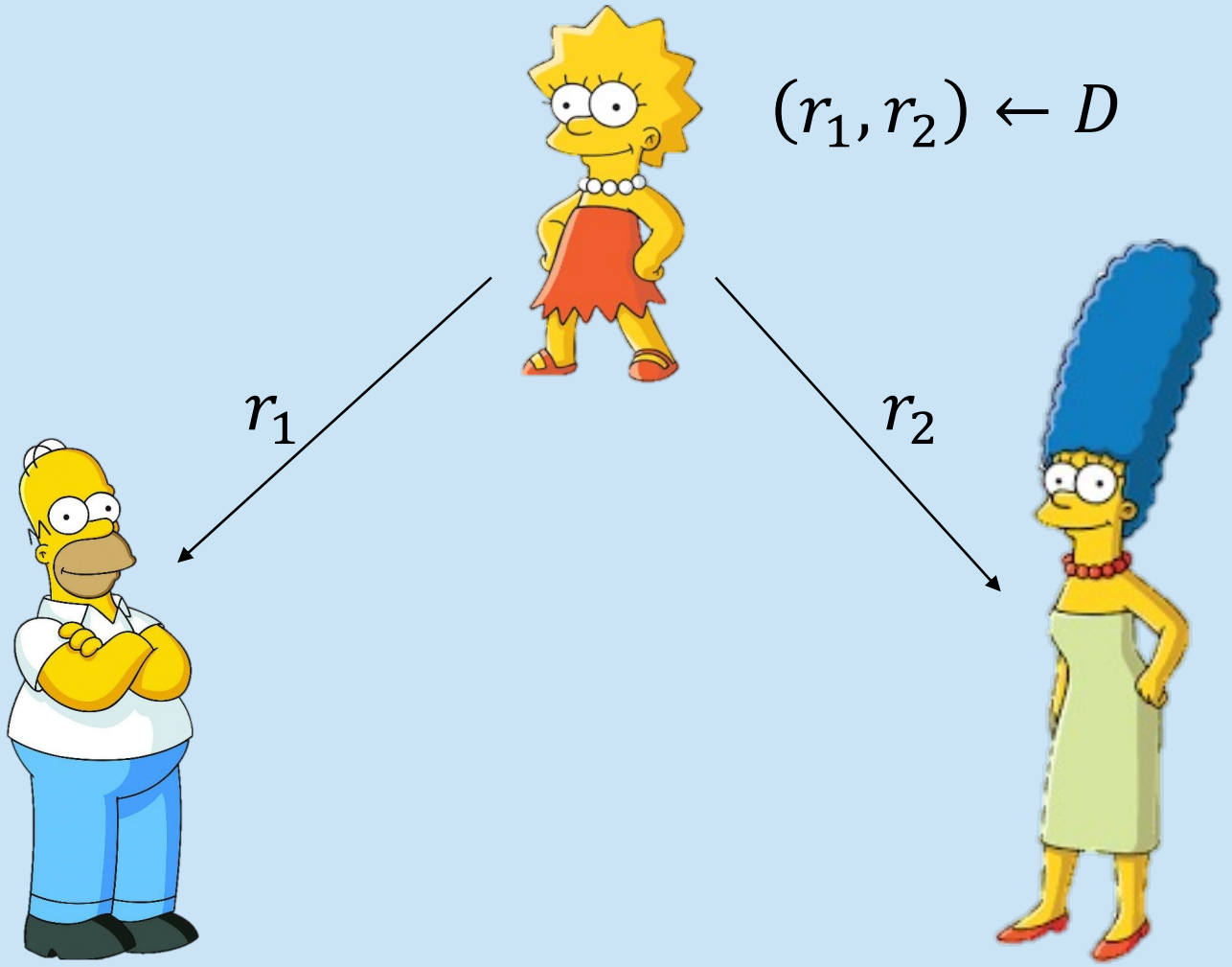




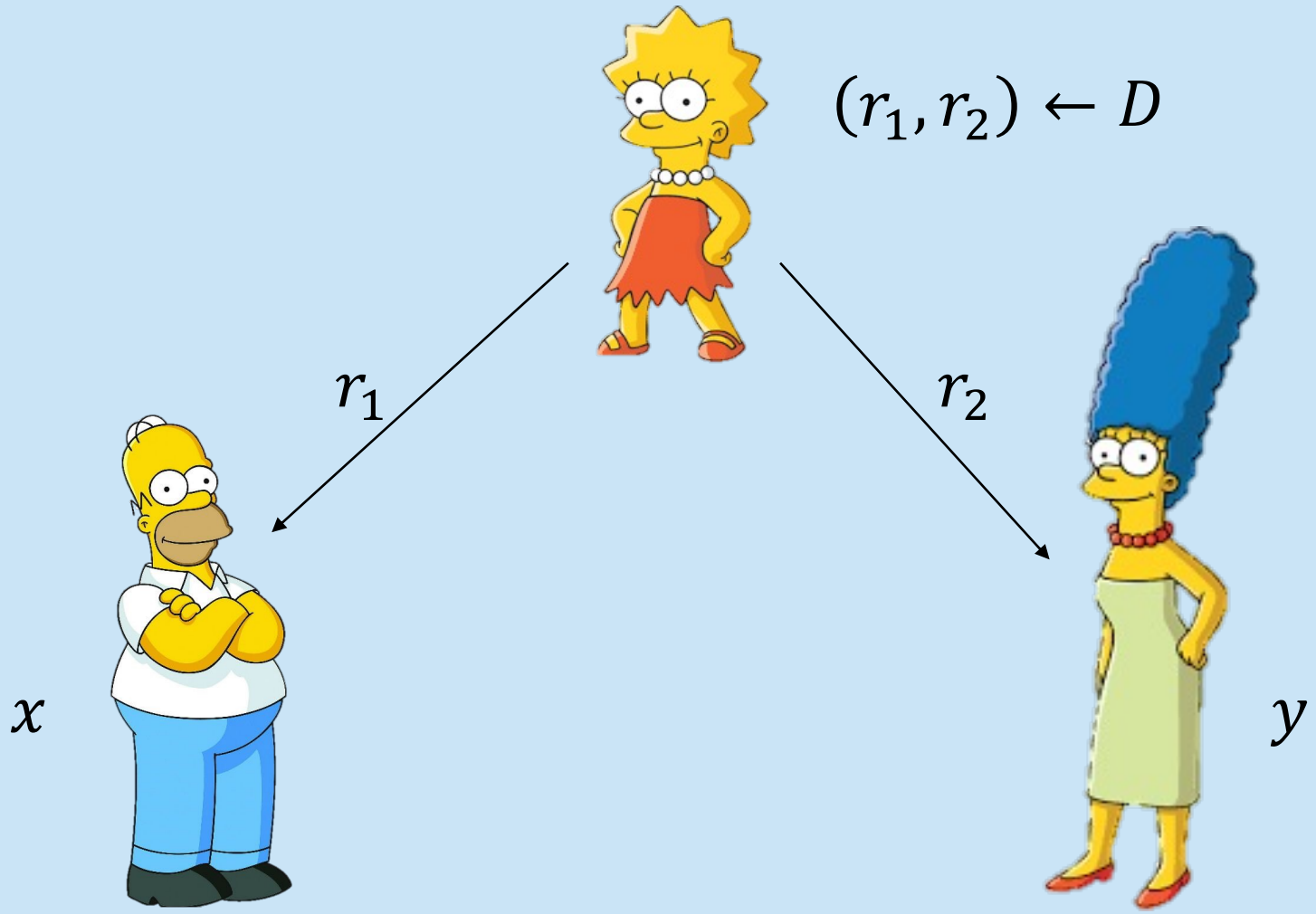
Perfect Security in a Nutshell



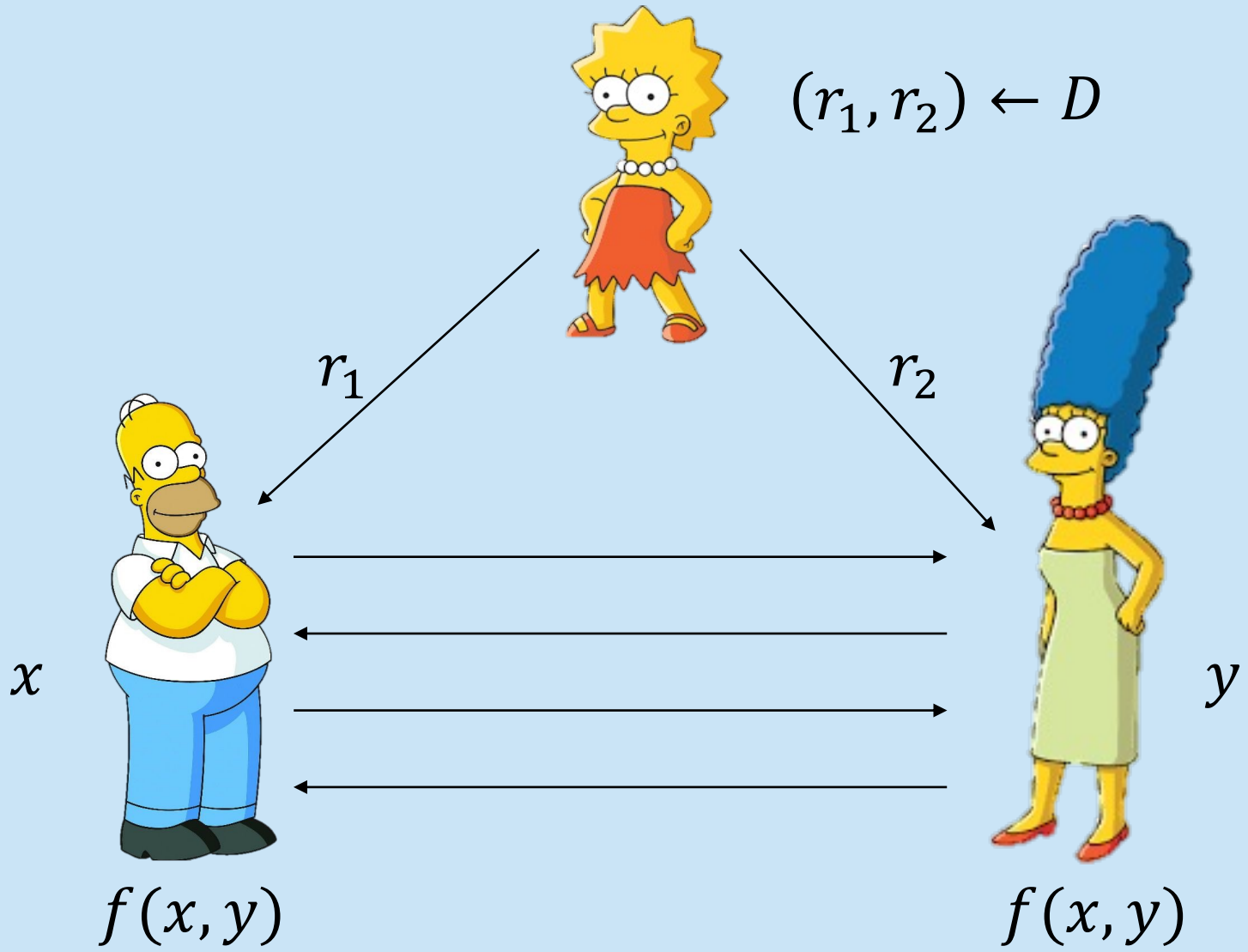
The Correlated Randomness Hybrid Model



The Correlated Randomness Hybrid Model



The Correlated Randomness Hybrid Model



Previous Results

[Ben-Or, Goldwasser, and Wigderson ’88],
[Chaum, Crépeau, Damgård ’88]

If $< 1/3$ are corrupted, everything is computable with perfect security

- In plain model, i.e., no correlated randomness (CR)

Previous Results

[Ben-Or, Goldwasser, and Wigderson '88], [Chaum, Crépeau, Damgård '88]

If $< 1/3$ are corrupted, everything is computable with perfect security

- In plain model, i.e., no correlated randomness (CR)

One party gets output

[Ishai, Kushilevitz, Meldgaard, Orlandi, Paskin-Cherniavsky '13]

1. Any two-party sender-receiver functionality can be computed with CR

Previous Results

[Ben-Or, Goldwasser, and Wigderson '88],
[Chaum, Crépeau, Damgård '88]

If $< 1/3$ are corrupted, everything is computable with perfect security

- In plain model, i.e., no correlated randomness (CR)

Both parties have same output

One party gets output

[Ishai, Kushilevitz, Meldgaard, Orlandi, Paskin-Cherniavsky '13]

1. Any two-party sender-receiver functionality can be computed with CR
2. Symmetric two-party XOR cannot be computed in CR-hybrid model
   - Works even for perfect security-with-abort (SWA)

Our Results

Our Results

- Characterization of symmetric functionalities

$$f: \mathcal{X} \times \mathcal{Y} \mapsto \{0,1,2,3\}$$

  - Positive results hold in plain model
  - Negative results hold in CR-hybrid model and SWA

Our Results

- Characterization of symmetric functionalities

$$f: \mathcal{X} \times \mathcal{Y} \mapsto \{0,1,2,3\}$$

  - Positive results hold in plain model
  - Negative results hold in CR-hybrid model and SWA

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

Trivial

Our Results

- Characterization of symmetric functionalities

$$f: \mathcal{X} \times \mathcal{Y} \mapsto \{0,1,2,3\}$$

  - Positive results hold in plain model
  - Negative results hold in CR-hybrid model and SWA

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

Trivial

$$\begin{pmatrix} 4 & 4 & 4 & 5 \\ 3 & 0 & 1 & 5 \\ 3 & 2 & 2 & 5 \\ 6 & 6 & 6 & 6 \end{pmatrix} \quad \begin{pmatrix} 2 & 2 \\ 1 & 0 \end{pmatrix}$$

Spiral

Our Results

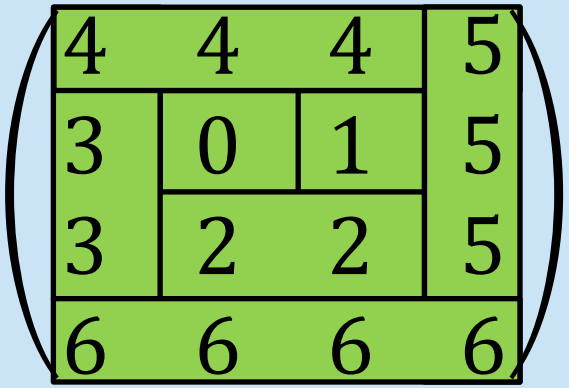
- Characterization of symmetric functionalities

$$f: \mathcal{X} \times \mathcal{Y} \mapsto \{0,1,2,3\}$$

  - Positive results hold in plain model
  - Negative results hold in CR-hybrid model and SWA

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

Trivial



$$\begin{pmatrix} 2 & 2 \\ 1 & 0 \end{pmatrix}$$

Spiral

Our Results

$$\big((m_0, m_1), b\big) \mapsto (m_b, b)$$

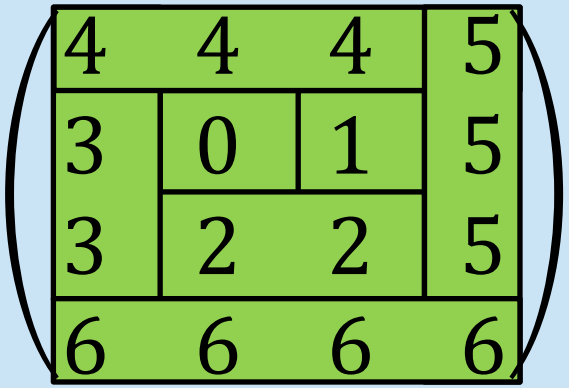
- Characterization of symmetric functionalities

$$f: \mathcal{X} \times \mathcal{Y} \mapsto \{0,1,2,3\}$$

  - Positive results hold in plain model
  - Negative results hold in CR-hybrid model and SWA

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

Trivial



$$\begin{pmatrix} 2 & 2 \\ 1 & 0 \end{pmatrix}$$

Spiral

$$\begin{pmatrix} 0 & 1 \\ 2 & 3 \\ 0 & 3 \\ 2 & 1 \end{pmatrix}$$

Transperent Transfer

Our Results

Our Results

- f contains an embedded XOR or an embedded AND
  $\Rightarrow$ f cannot be computed with perfect security
  - ➢ Works in CR-hybrid model and SWA
  - ➢ For any number of outputs

$$\begin{pmatrix} 0 & 1 & 2 \\ 2 & 3 & 3 \\ 2 & 4 & 0 \end{pmatrix}$$

Embedded XOR

$$\begin{pmatrix} 0 & 1 & 2 \\ 2 & 3 & 2 \\ 2 & 4 & 3 \end{pmatrix}$$

Embedded AND

Warmup: Impossibility of XOR [IKMOP ‘13]

Warmup: Impossibility of XOR [IKMOP ‘13]

x, r_1

$x \leftarrow \{0,1\}$

y, r_2

$y \leftarrow \{0,1\}$

Warmup: Impossibility of XOR [IKMOP '13]

First round where Homer knows output regardless of x, y, r_1, r_2

x, r_1

$x \leftarrow \{0,1\}$

y, r_2

$y \leftarrow \{0,1\}$

Warmup: Impossibility of XOR [IKMOP '13]

First round where Homer knows output regardless of x, y, r_1, r_2

First round where Marge knows output regardless of x, y, r_1, r_2

x, r_1

$x \leftarrow \{0,1\}$

y, r_2

$y \leftarrow \{0,1\}$

Warmup: Impossibility of XOR [IKMOP ‘13]

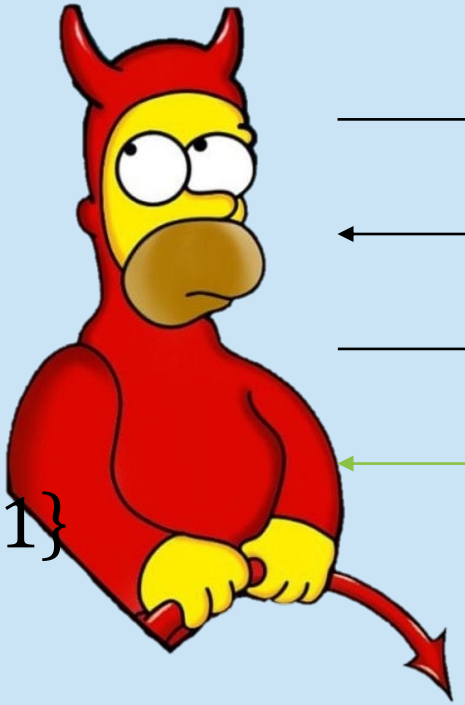
x, r_1

$x \leftarrow \{0,1\}$

y, r_2

$y \leftarrow \{0,1\}$

Warmup: Impossibility of XOR [IKMOP ‘13]



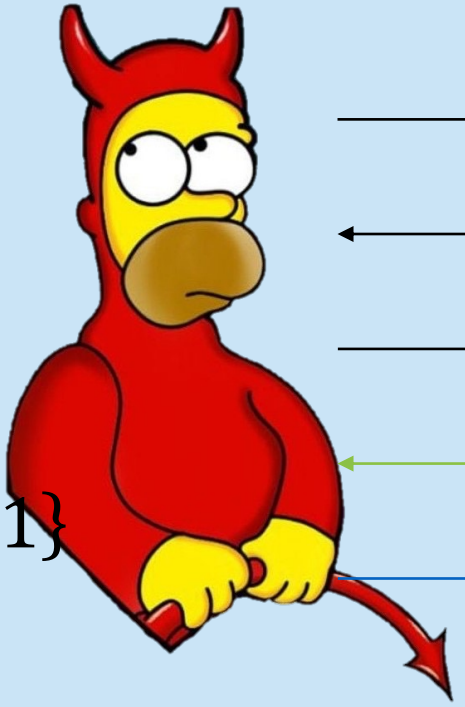
x, r_1

$x \leftarrow \{0,1\}$

y, r_2

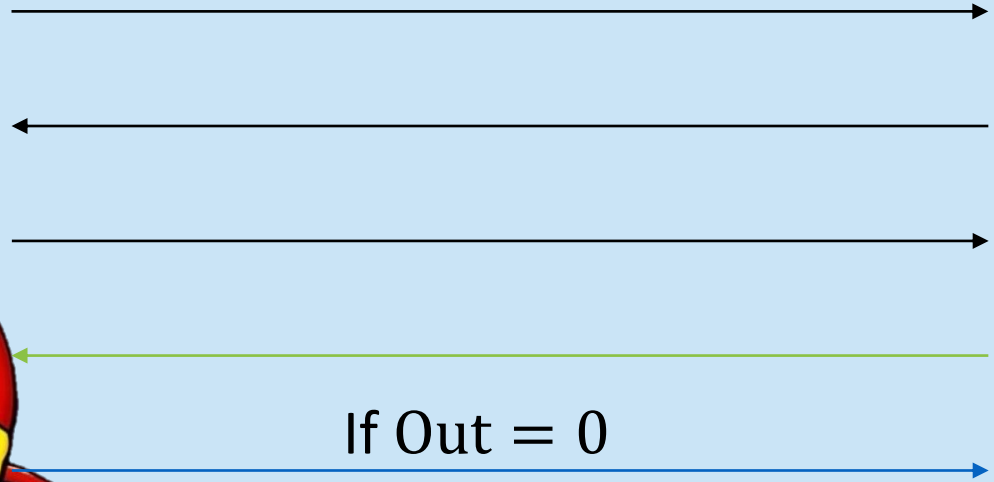
$y \leftarrow \{0,1\}$

Warmup: Impossibility of XOR [IKMOP ‘13]



x, r_1

$x \leftarrow \{0,1\}$

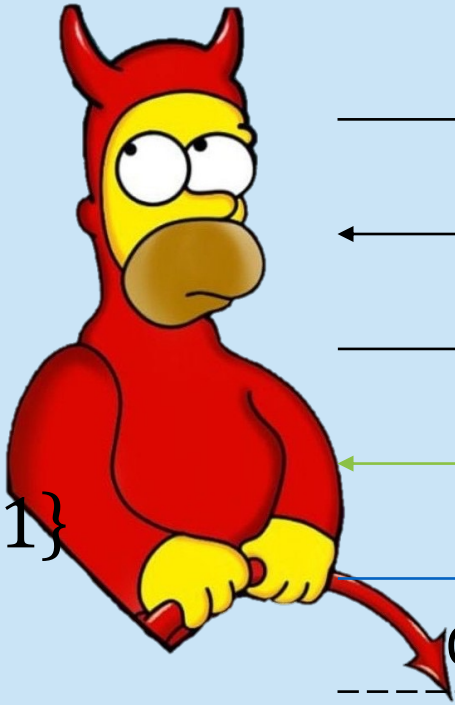


If Out $= 0$

y, r_2

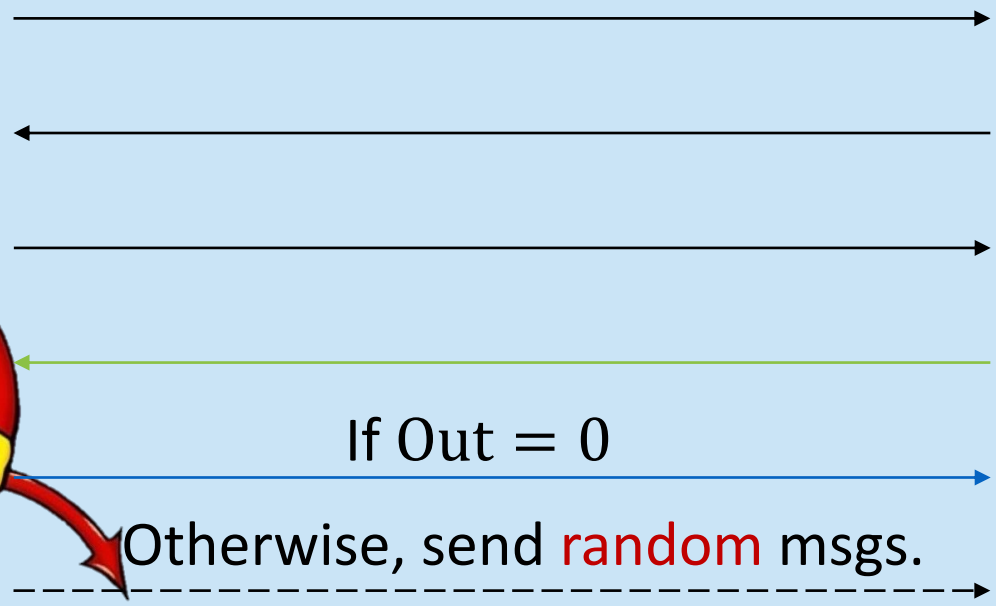
$y \leftarrow \{0,1\}$

Warmup: Impossibility of XOR [IKMOP ‘13]



x, r_1

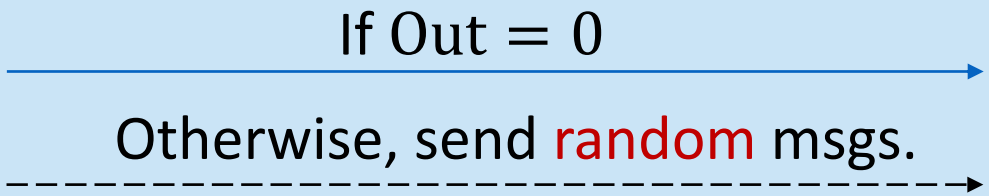
$x \leftarrow \{0,1\}$



y, r_2

$y \leftarrow \{0,1\}$

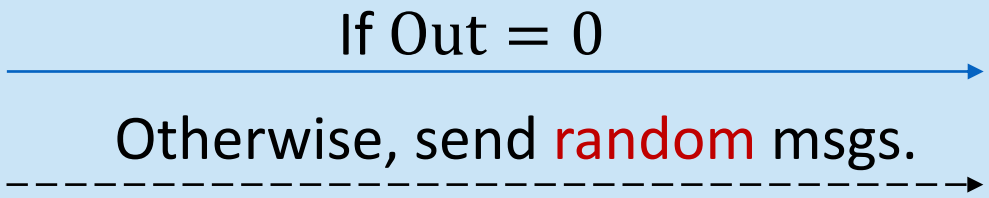
Warmup: Impossibility of XOR [IKMOP ‘13]



Intuitition:

- Marge doesn’t know the output for some y, r_2

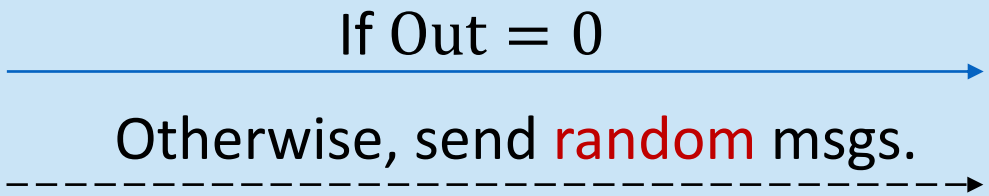
Warmup: Impossibility of XOR [IKMOP ‘13]



Intuitition:

- Marge doesn’t know the output for some y, r_2
- If $\mathrm{Out} = 1$ then $\exists$continuation causing her to output 0

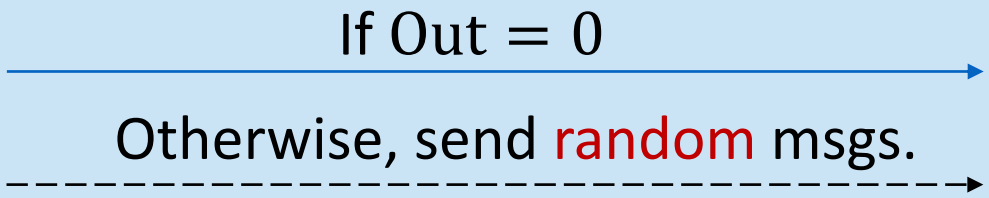
Warmup: Impossibility of XOR [IKMOP '13]



Intuitition:

- Marge doesn't know the output for some y, r_2
- If $\mathrm{Out} = 1$ then $\exists$continuation causing her to output 0
- $\Rightarrow$ non-zero probability of increasing chance of $\mathrm{Out} = 0$

Warmup: Impossibility of XOR [IKMOP ‘13]



Intuitition:

- Marge doesn’t know the output for some y, r_2
- If $\mathrm{Out} = 1$ then $\exists$continuation causing her to output 0
- $\Rightarrow$ non-zero probability of increasing chance of $\mathrm{Out} = 0$

$$\Pr[\mathrm{Out}_M = 0] = \Pr[x \oplus y = 0] + \Pr[x \oplus y = 1] \cdot \varepsilon$$
$$= 1/2 + \varepsilon/2$$

Warmup: Impossibility of XOR [IKMOP '13]

Real world:

$$\Pr[\mathrm{Out}_{\mathrm{M}} = 0] = \Pr[x \oplus y = 0] + \Pr[x \oplus y = 1] \cdot \varepsilon$$
$$= 1/2 + \varepsilon/2$$

Ideal world:

$$\Pr[\mathrm{Out}_{\mathrm{M}} = 0] = 1/2$$

y is uniform

Where Does The Argument Fails for AND?

Real world:

$$\Pr[\mathrm{Out}_{\mathrm{M}} = 0] = \Pr[x \wedge y = 0] + \Pr[x \wedge y = 1] \cdot \varepsilon$$
$$= 3/4 + \varepsilon/4$$

Where Does The Argument Fails for AND?

Real world:

$$\Pr[\mathrm{Out}_M = 0] = \Pr[x \wedge y = 0] + \Pr[x \wedge y = 1] \cdot \varepsilon$$
$$= 3/4 + \varepsilon/4$$

Ideal world:

- The simulator can change its input

Where Does The Argument Fails for AND?

Real world:

$$\Pr[\mathrm{Out}_{\mathrm{M}} = 0] = \Pr[x \wedge y = 0] + \Pr[x \wedge y = 1] \cdot \varepsilon$$
$$= 3/4 + \varepsilon/4$$

Ideal world:

- The simulator can change its input
- Sending $x^* = 0$ with certain probability might work

Where Does The Argument Fails for AND?

Real world:

$$\Pr[\mathrm{Out}_{\mathrm{M}} = 0] = \Pr[x \wedge y = 0] + \Pr[x \wedge y = 1] \cdot \varepsilon$$
$$= 3/4 + \varepsilon/4$$

Ideal world:

- The simulator can change its input
- Sending $x^* = 0$ with certain probability might work
- Biasing towrads 1 might also be simulatable

Where Does The Argument Fails for AND?

Real world:

$$\Pr[\mathrm{Out}_{\mathrm{M}} = 0] = \Pr[x \wedge y = 0] + \Pr[x \wedge y = 1] \cdot \varepsilon$$
$$= 3/4 + \varepsilon/4$$

Ideal world:

- The simulator can change its input
- Sending $x^* = 0$ with certain probability might work
- Biasing towrads 1 might also be simulatable

Observation: sending $x^* = 0$ reveals no info. to the simulator

Idea: adversary will also guess the input of Marge.

Impossiblity of AND

Guess of adversary

Real world:

$$\Pr[\mathrm{Out}_M = 0, y^* = y] = \Pr[x = 0] \cdot 1/2 + \Pr[x = 1, y = 0]$$
$$+ \Pr[x = y = 1] \cdot \varepsilon$$
$$= 1/2 + \varepsilon/4$$

Impossiblity of AND

Guess of adversary

Real world:

$$\Pr[\mathrm{Out}_{\mathrm{M}} = 0, y^* = y] = \Pr[x = 0] \cdot 1/2 + \Pr[x = 1, y = 0]$$
$$+ \Pr[x = y = 1] \cdot \varepsilon$$
$$= 1/2 + \varepsilon/4$$

Ideal world:

- If $x^* = 0$ then guessing works w.p. $1/2$

Impossiblity of AND

Guess of adversary

Real world:

$$\Pr[\mathrm{Out}_M = 0, y^* = y] = \Pr[x = 0] \cdot 1/2 + \Pr[x = 1, y = 0]$$
$$+ \Pr[x = y = 1] \cdot \varepsilon$$
$$= 1/2 + \varepsilon/4$$

Ideal world:

- If $x^* = 0$ then guessing works w.p. $1/2$
- If $x^* = 1$ then $\mathrm{Out}_M = 0$ w.p. $1/2$

Impossiblity of AND

Guess of adversary

Real world:

$$\Pr[\mathrm{Out}_M = 0, y^* = y] = \Pr[x = 0] \cdot 1/2 + \Pr[x = 1, y = 0] + \Pr[x = y = 1] \cdot \varepsilon = 1/2 + \varepsilon/4$$

Ideal world:

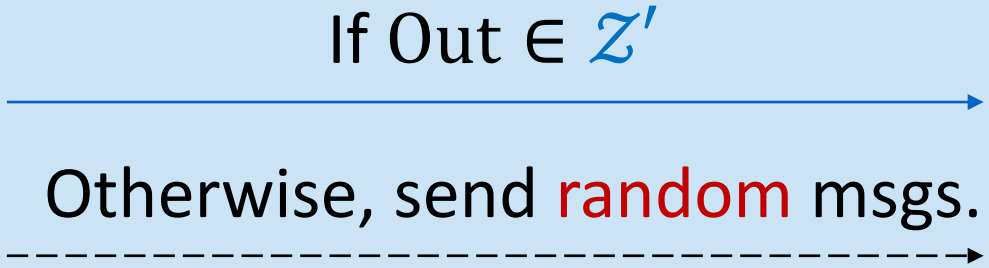
- If $x^* = 0$ then guessing works w.p. $1/2$
- If $x^* = 1$ then $\mathrm{Out}_M = 0$ w.p. $1/2$

$\Rightarrow$ Success probability is $1/2$

General Impossibility

For general $f: \mathcal{X} \times \mathcal{Y} \mapsto \mathcal{Z}$, fix $\mathcal{X}' \subseteq \mathcal{X}$, $\mathcal{Y}' \subseteq \mathcal{Y}$, and $\mathcal{Z}' \subset \mathcal{Z}$

For $x \leftarrow \mathcal{X}'$ and $y \leftarrow \mathcal{Y}'$, the attacker is as follows

1. Play honestly until "special" round
2. 

3. Guess the input of the other party

We identify when the attack cannot be simulated

Summary

- Perfect security for 2 parties with correlated randomness
- Characterized functionalities with 4 outputs
- Showed a general negative result
  - Embedded XOR/AND is impossible to compute with perfect security
  - Works for security-with-abort
- We gave several positive results
  - Work in the plain model

Thank You