Design and Analysis of Secure Cryptographic Implementations in the Random Probing Model

Sonia Belaïd

Habilitation Defense

February 9, Sorbonne Université

Introduction

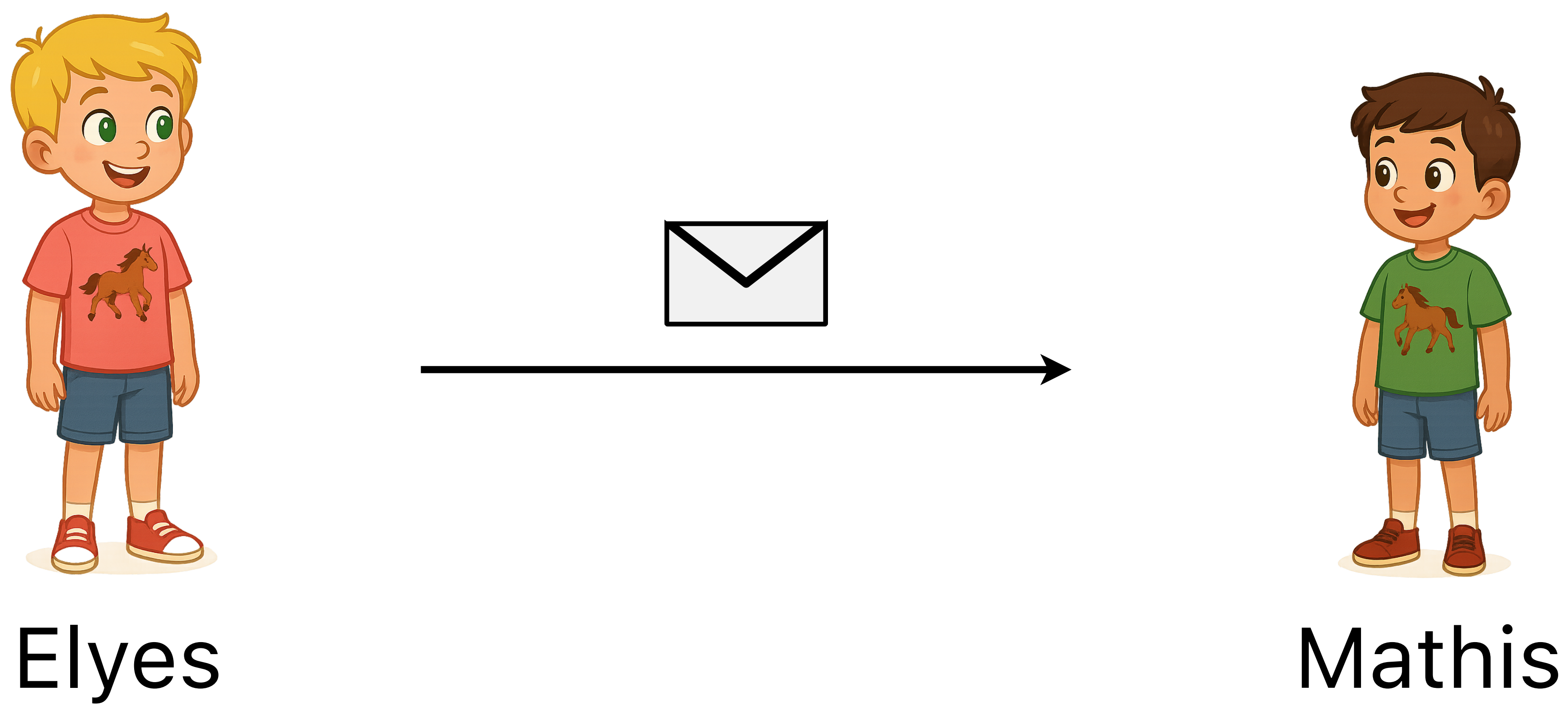
Cryptography

🔒 Confidentiality

✔ Integrity

👤 Authentication

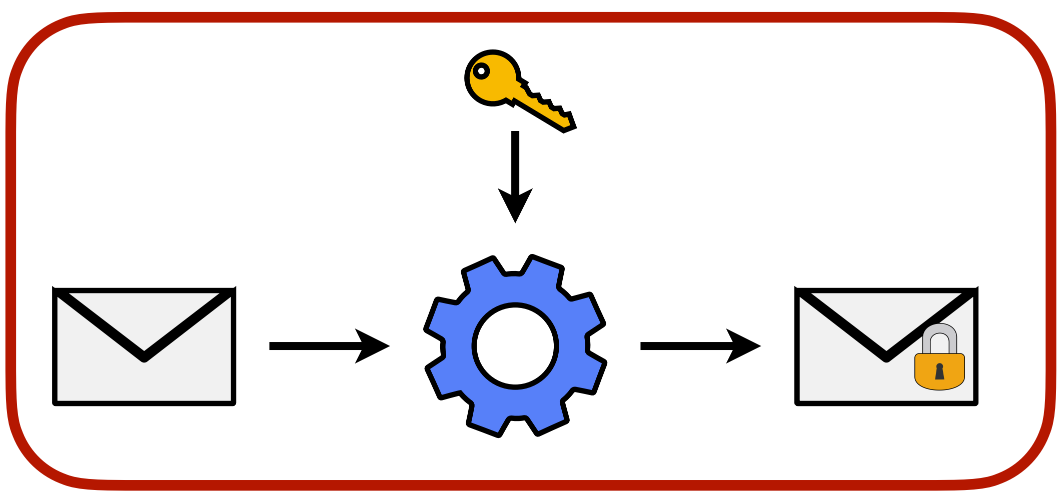
Cryptography



Cryptography

Elyes

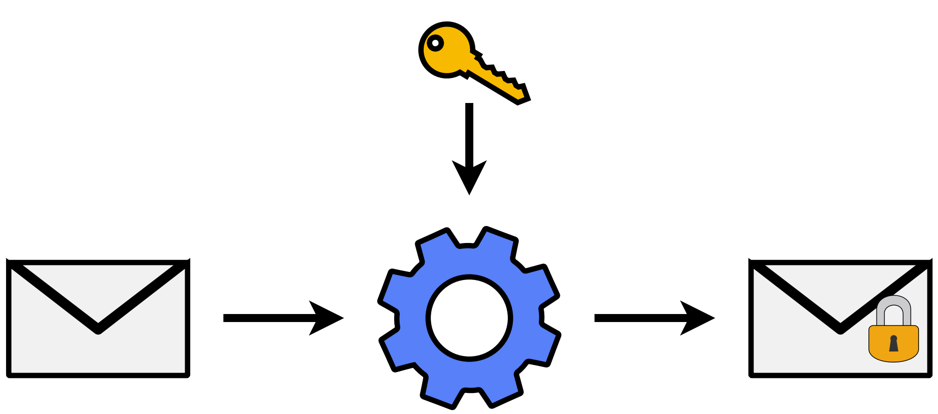
Mathis



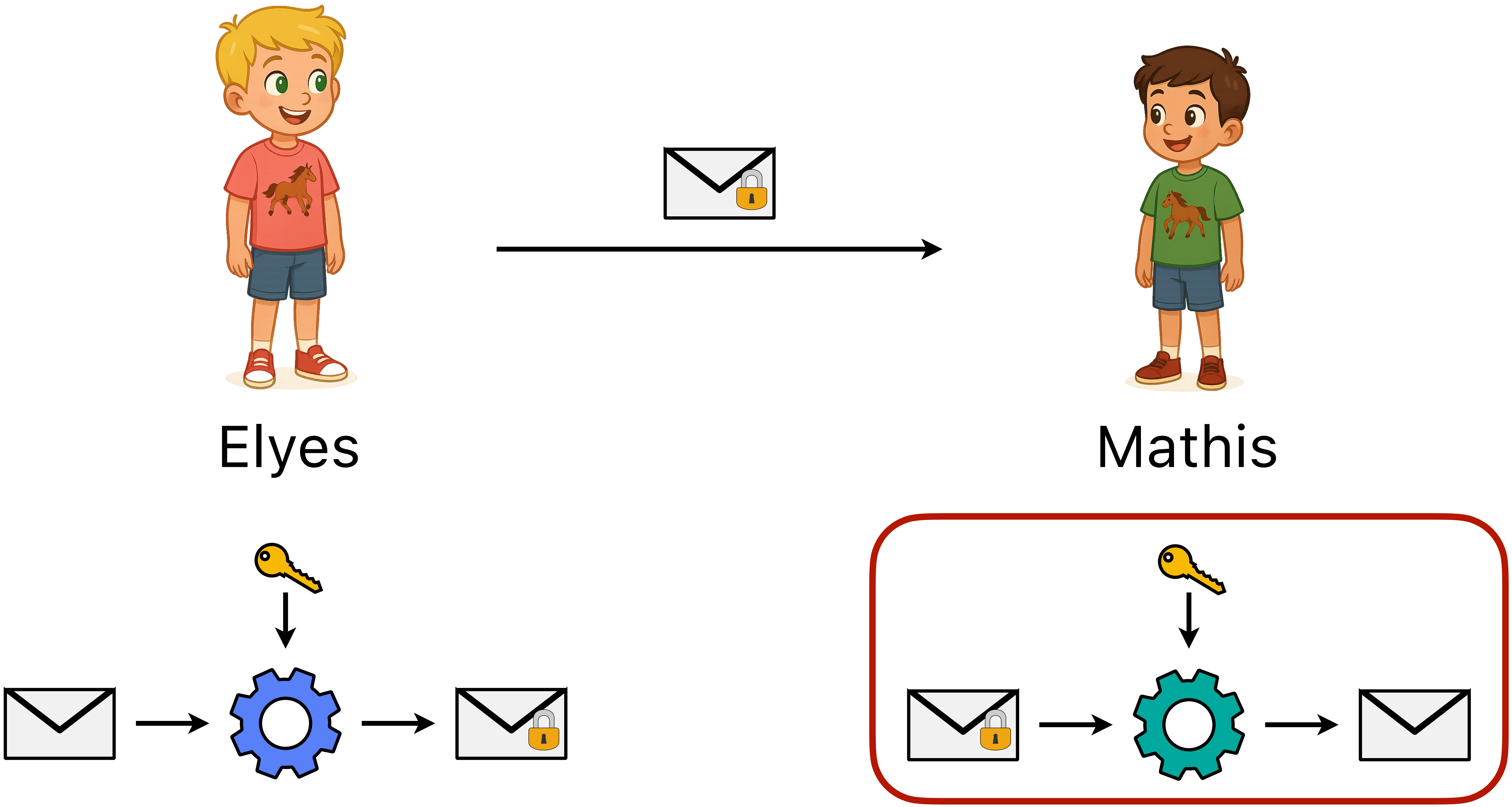
Cryptography

Elyes

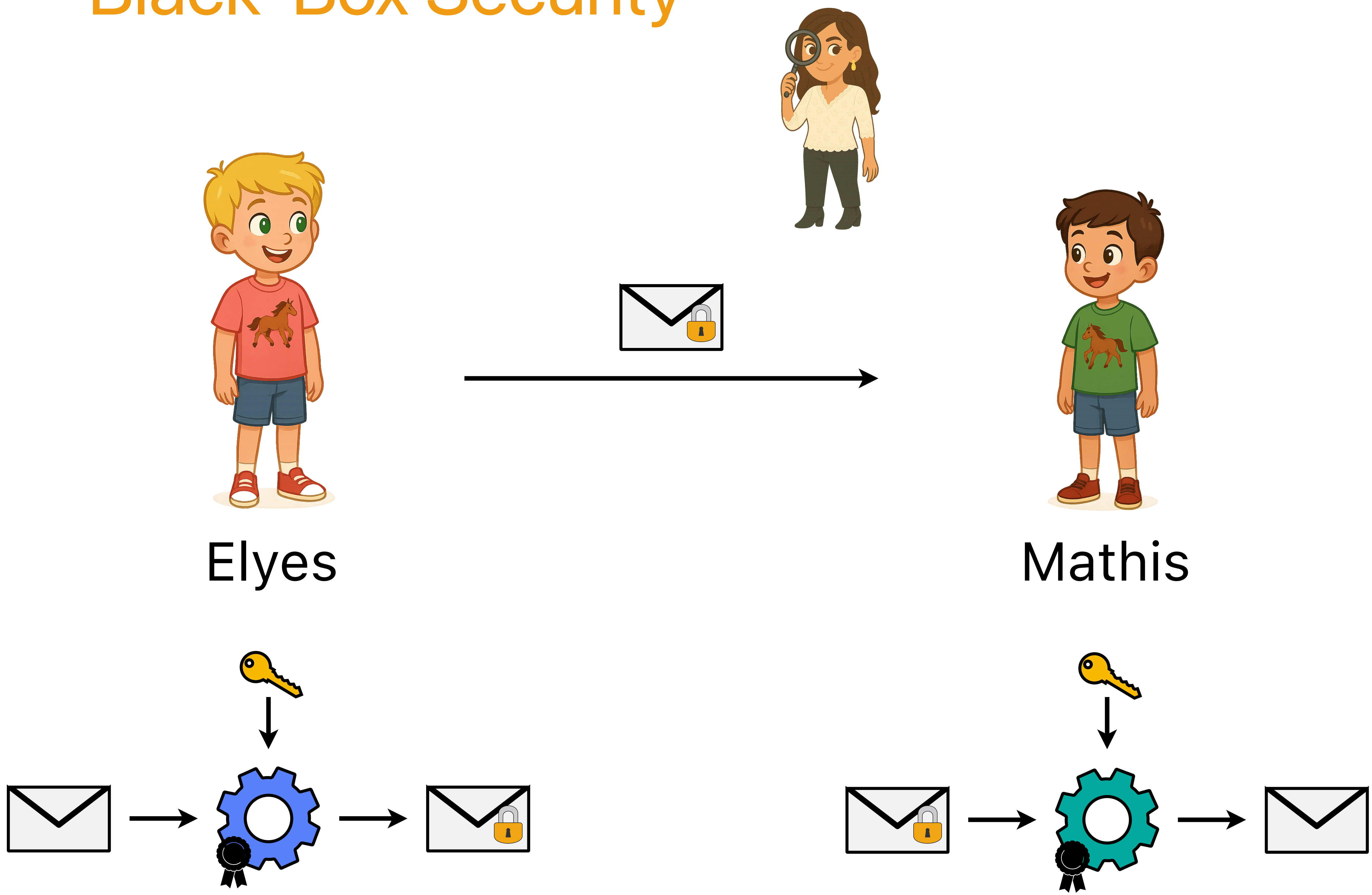
Mathis



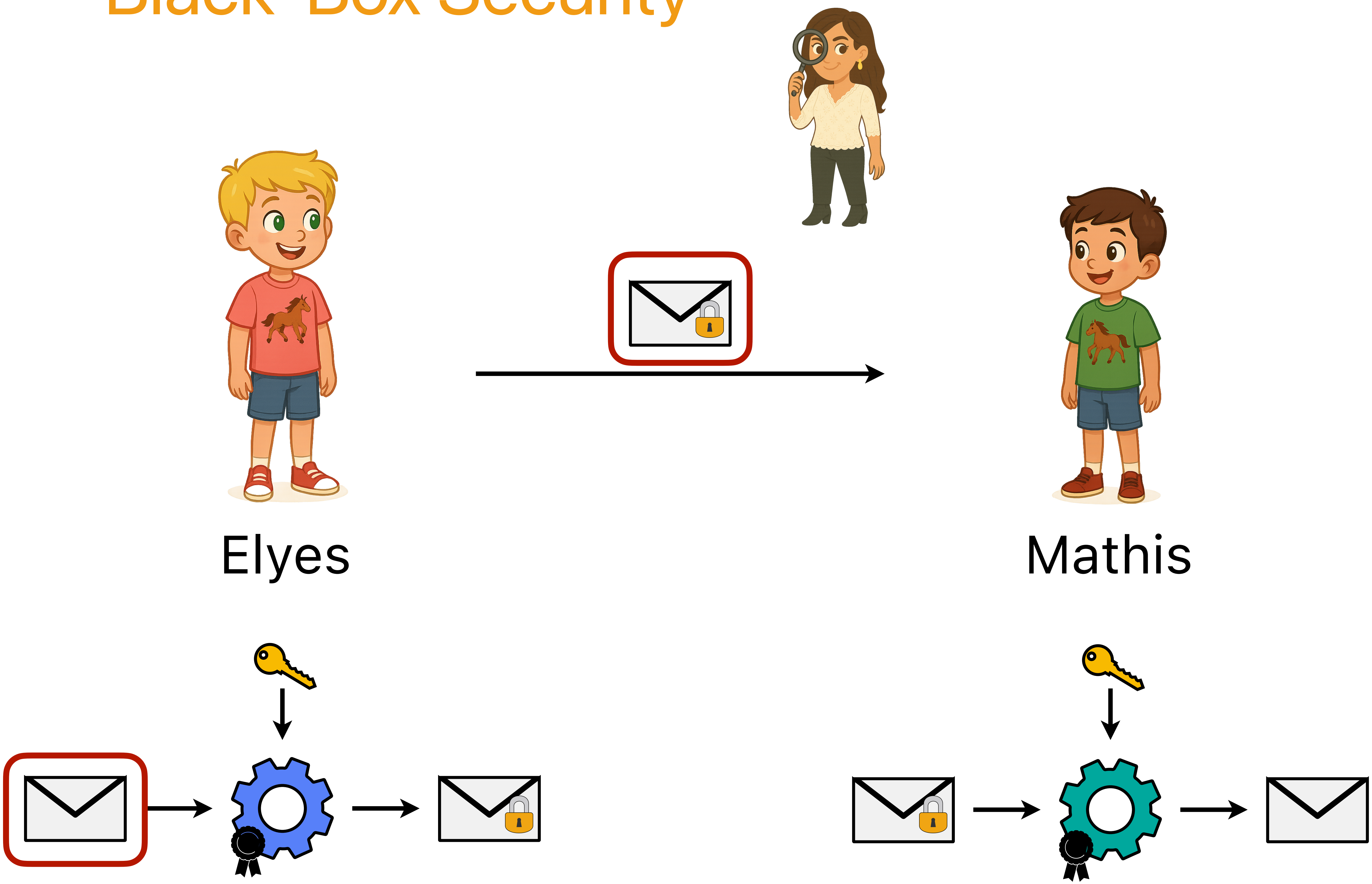
Cryptography



Black-Box Security

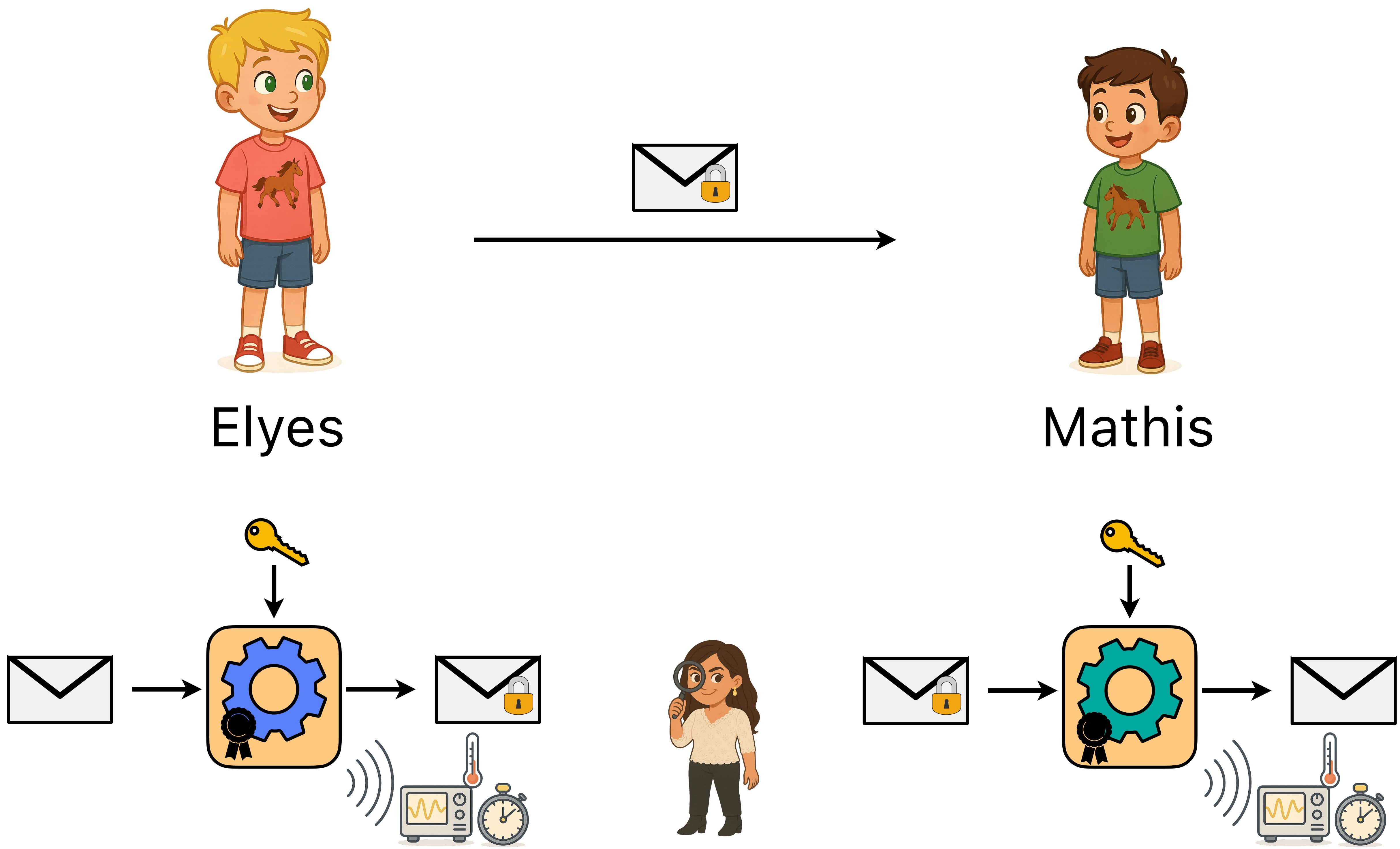


Black-Box Security



Side-Channel Attacks

Kocher • Jaffe • Jun
CRYPTO 1999



Masking

Chari • Jutla • Rao • Rohatgi

CRYPTO 1999

Goubin • Patarin

CHES, 1999

Masking

Chari • Jutla • Rao • Rohatgi

CRYPTO 1999

Goubin • Patarin

CHES, 1999

$$x \longrightarrow x_1 \quad x_2 \quad \cdots \quad x_n$$

Masking

Chari • Jutla • Rao • Rohatgi

CRYPTO 1999

Goubin • Patarin

CHES, 1999

$$x \longrightarrow \boxed{\$} \quad x_2 \quad \cdots \quad x_n$$

Masking

Chari • Jutla • Rao • Rohatgi

CRYPTO 1999

Goubin • Patarin

CHES, 1999

$$x \longrightarrow \boxed{\$} \;\; \boxed{\$} \cdots \;\; x_n$$

Masking

Chari • Jutla • Rao • Rohatgi

CRYPTO 1999

Goubin • Patarin

CHES, 1999

$$x \longrightarrow \boxed{\$}\ \boxed{\$}\ \cdots\ \boxed{x-(x_1+x_2+\ldots+x_{n-1})}$$

Masking

Chari • Jutla • Rao • Rohatgi

CRYPTO 1999

Goubin • Patarin

CHES, 1999

x $\quad\quad\quad\quad$ $x_1 \quad x_2 \quad \cdots \quad x_n$

Masking

Chari • Jutla • Rao • Rohatgi

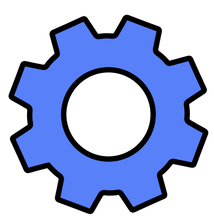
CRYPTO 1999

Goubin • Patarin

CHES, 1999

x

$\downarrow$



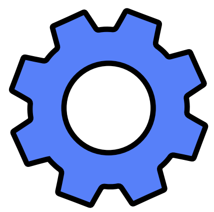
$\downarrow$

z

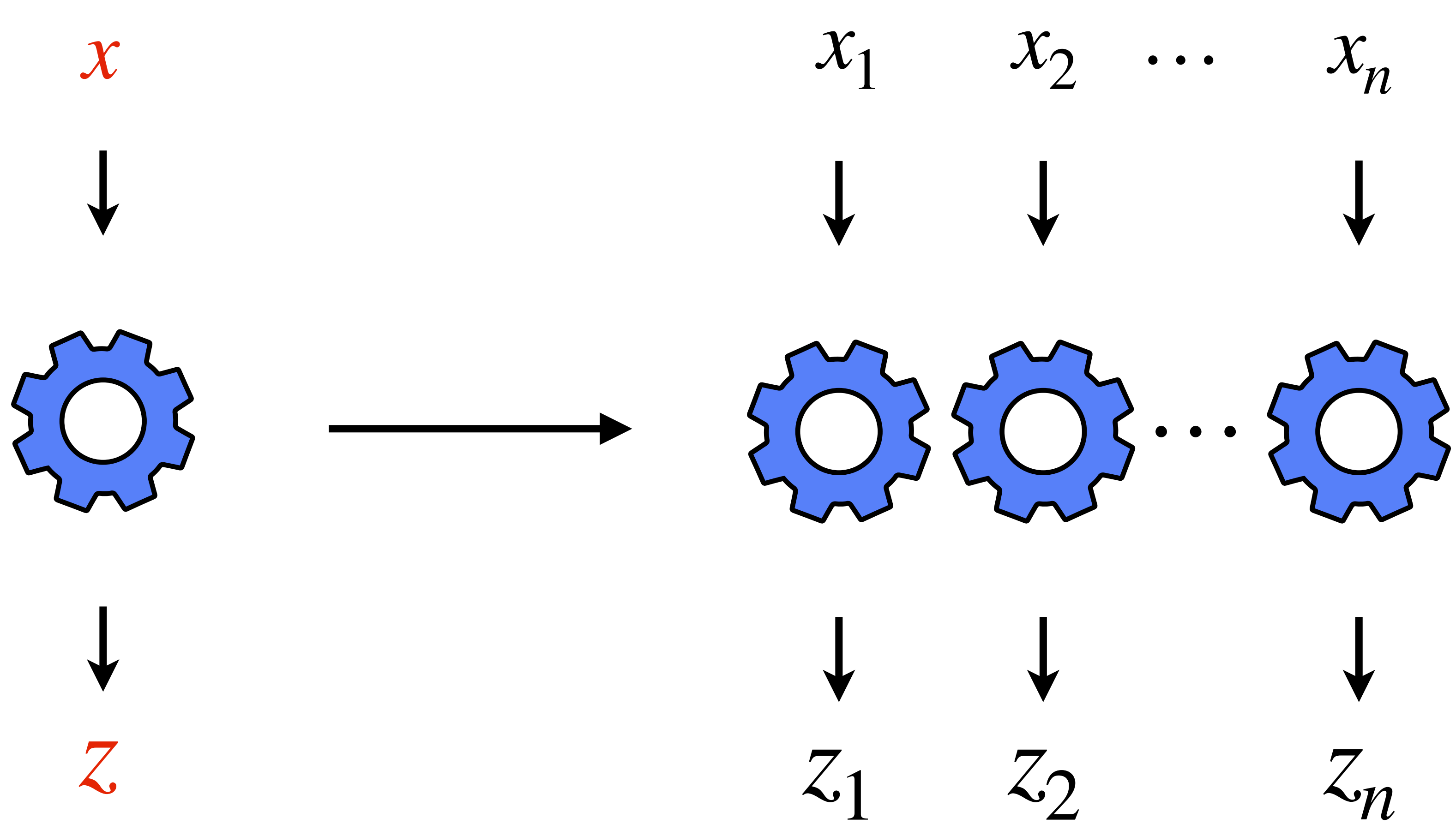
$x_1 \quad x_2 \quad \cdots \quad x_n$

Masking

Chari • Jutla • Rao • Rohatgi
CRYPTO 1999
Goubin • Patarin
CHES, 1999



linear function

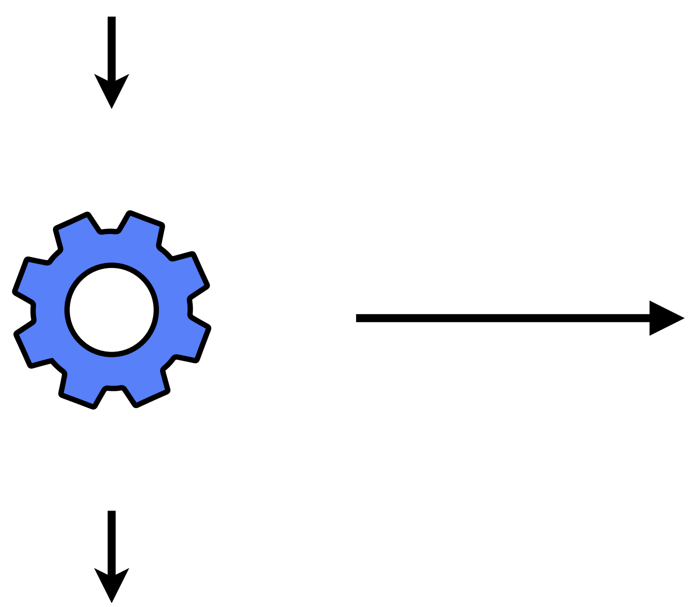


Masking

Chari • Jutla • Rao • Rohatgi
CRYPTO 1999
Goubin • Patarin
CHES, 1999

non-linear function

x

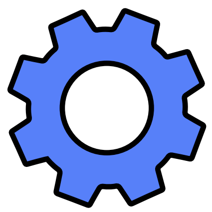


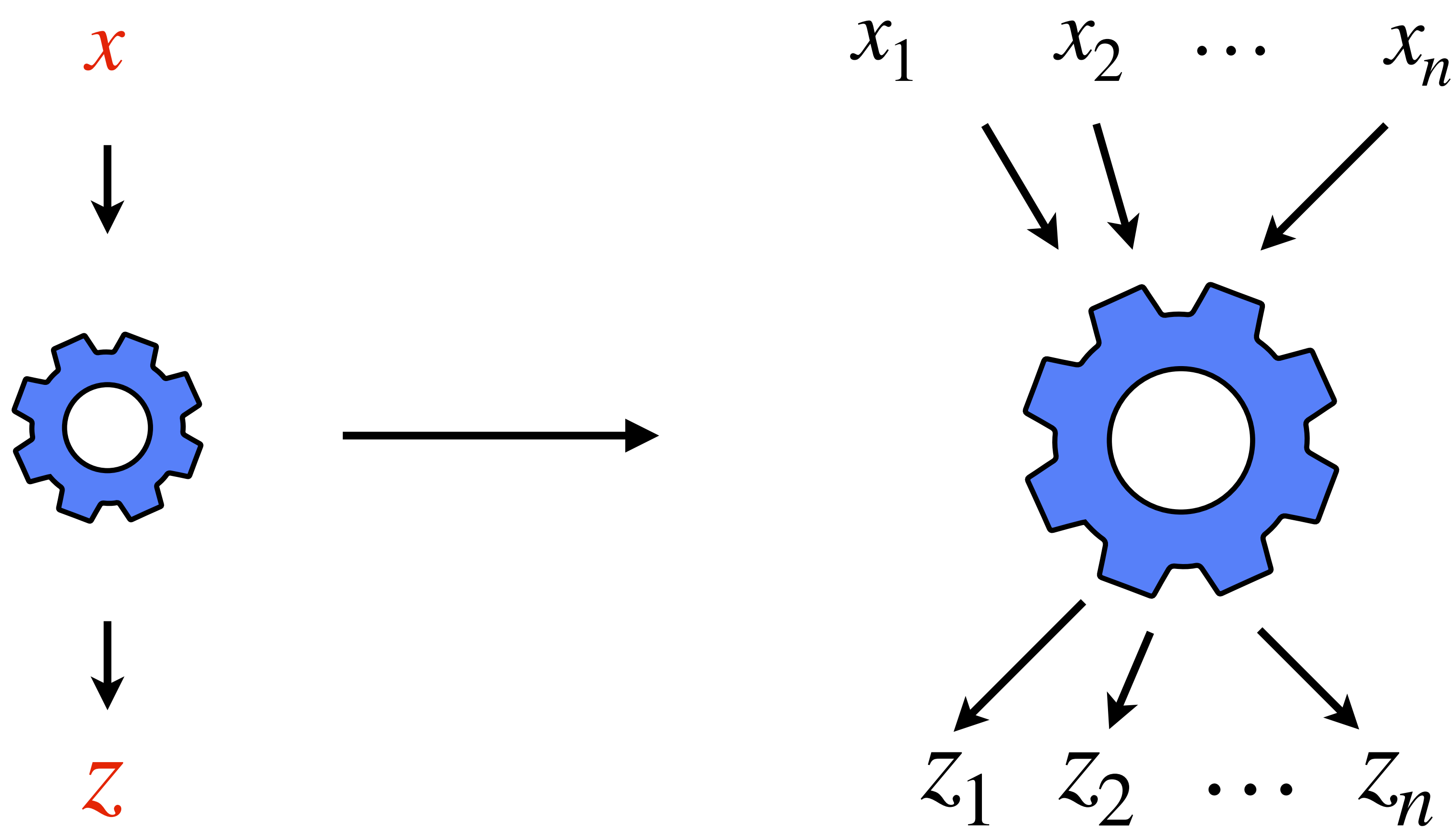
z

$x_1 \quad x_2 \quad \cdots \quad x_n$

Masking

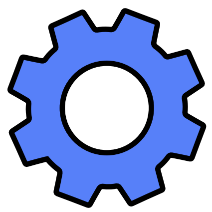
Chari • Jutla • Rao • Rohatgi
CRYPTO 1999
Goubin • Patarin
CHES, 1999


non-linear function

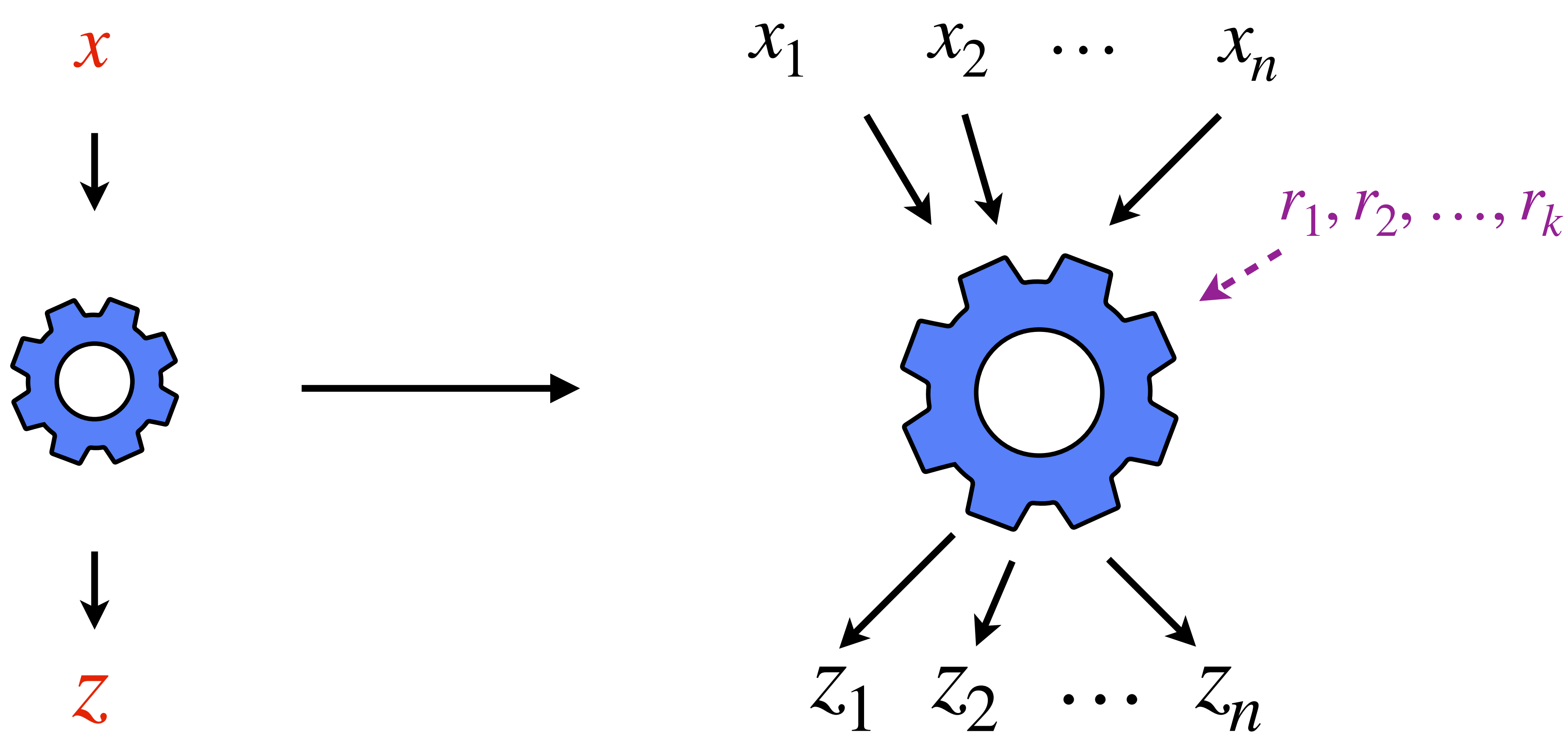


Masking

Chari • Jutla • Rao • Rohatgi
CRYPTO 1999
Goubin • Patarin
CHES, 1999



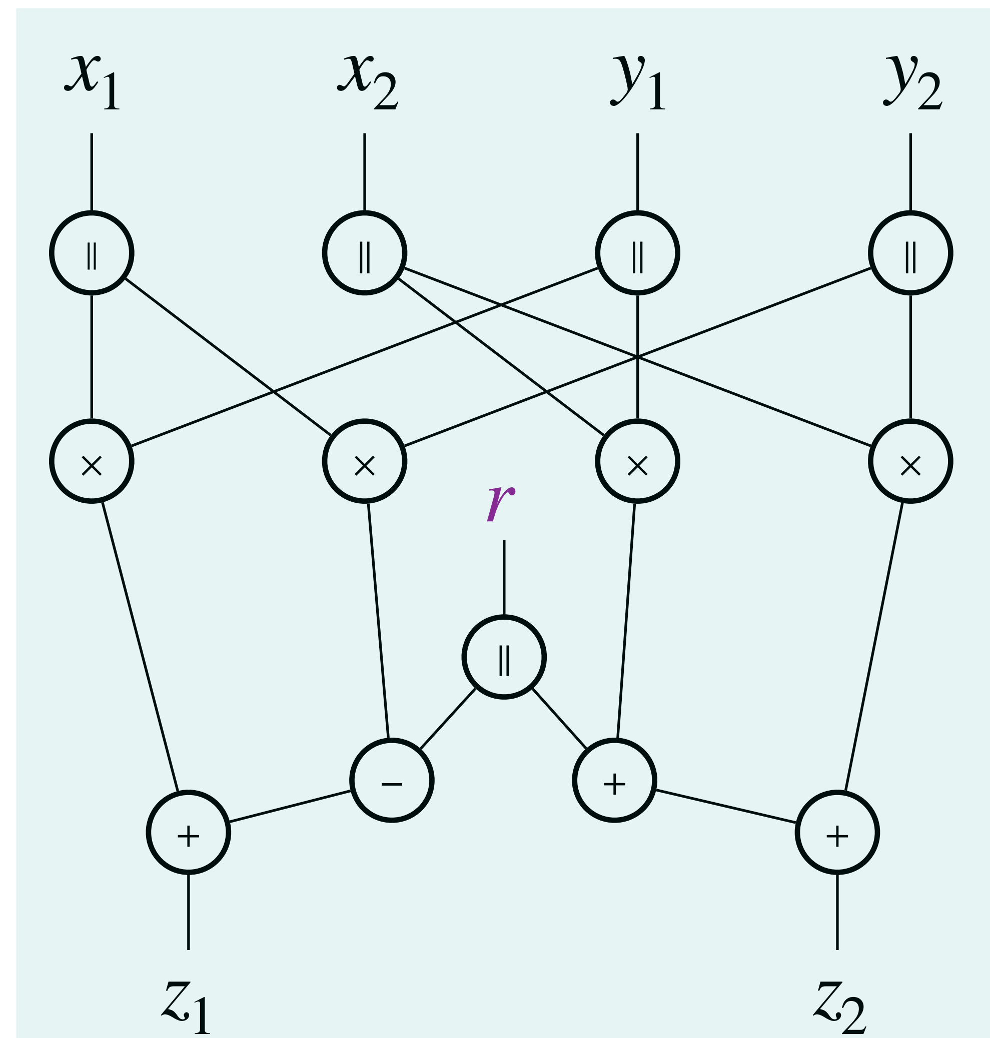
non-linear function



Masking

non-linear function

Chari • Jutla • Rao • Rohatgi
CRYPTO 1999
Goubin • Patarin
CHES, 1999



Example

Masking

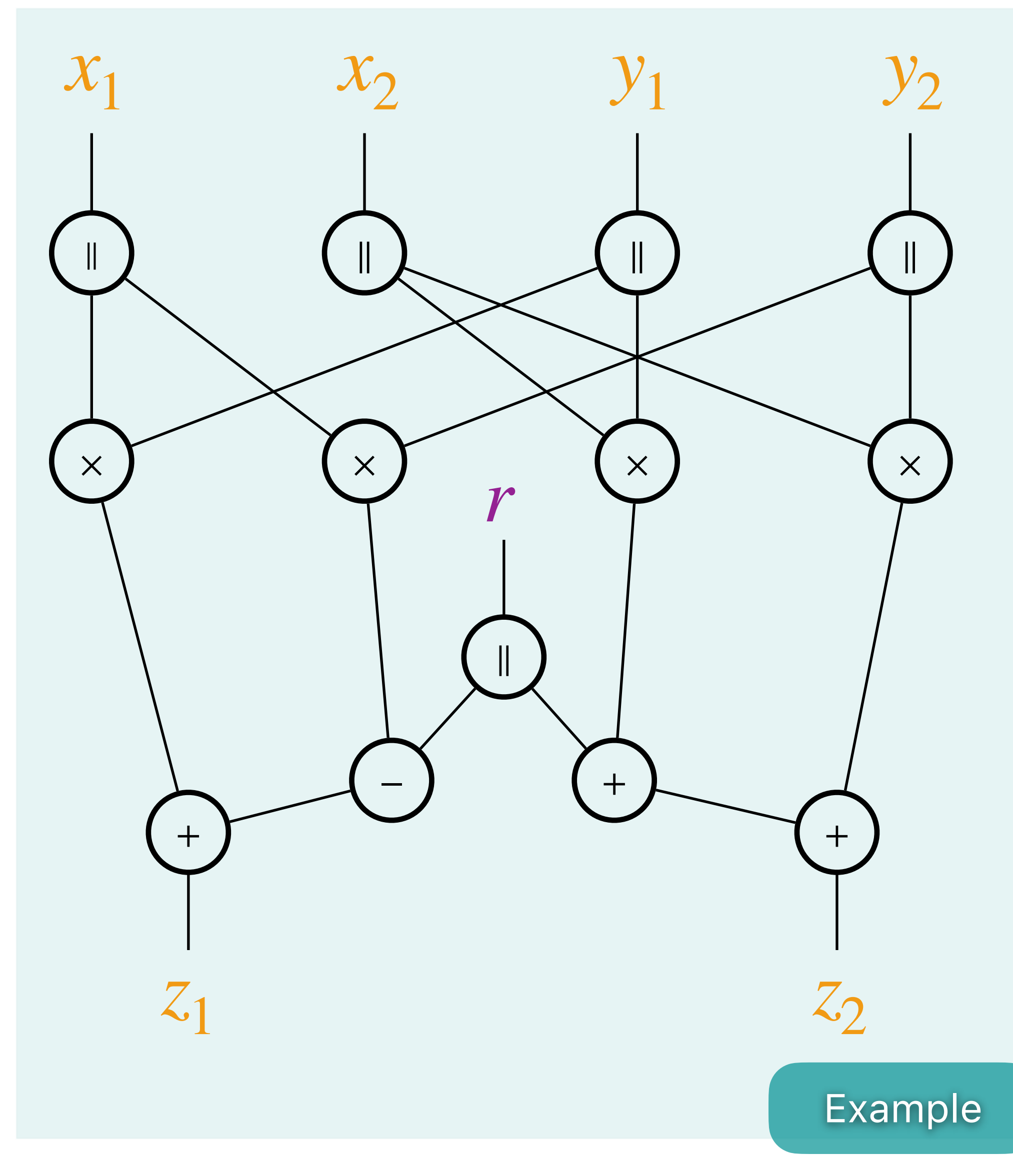
Chari • Jutla • Rao • Rohatgi

CRYPTO 1999

Goubin • Patarin

CHES, 1999

non-linear function



Inputs:

$$x = x_1 + x_2$$

$$y = y_1 + y_2$$

Output:

$$z = z_1 + z_2 = x \cdot y$$

Masking

Chari • Jutla • Rao • Rohatgi
CRYPTO 1999
Goubin • Patarin
CHES, 1999

non-linear function

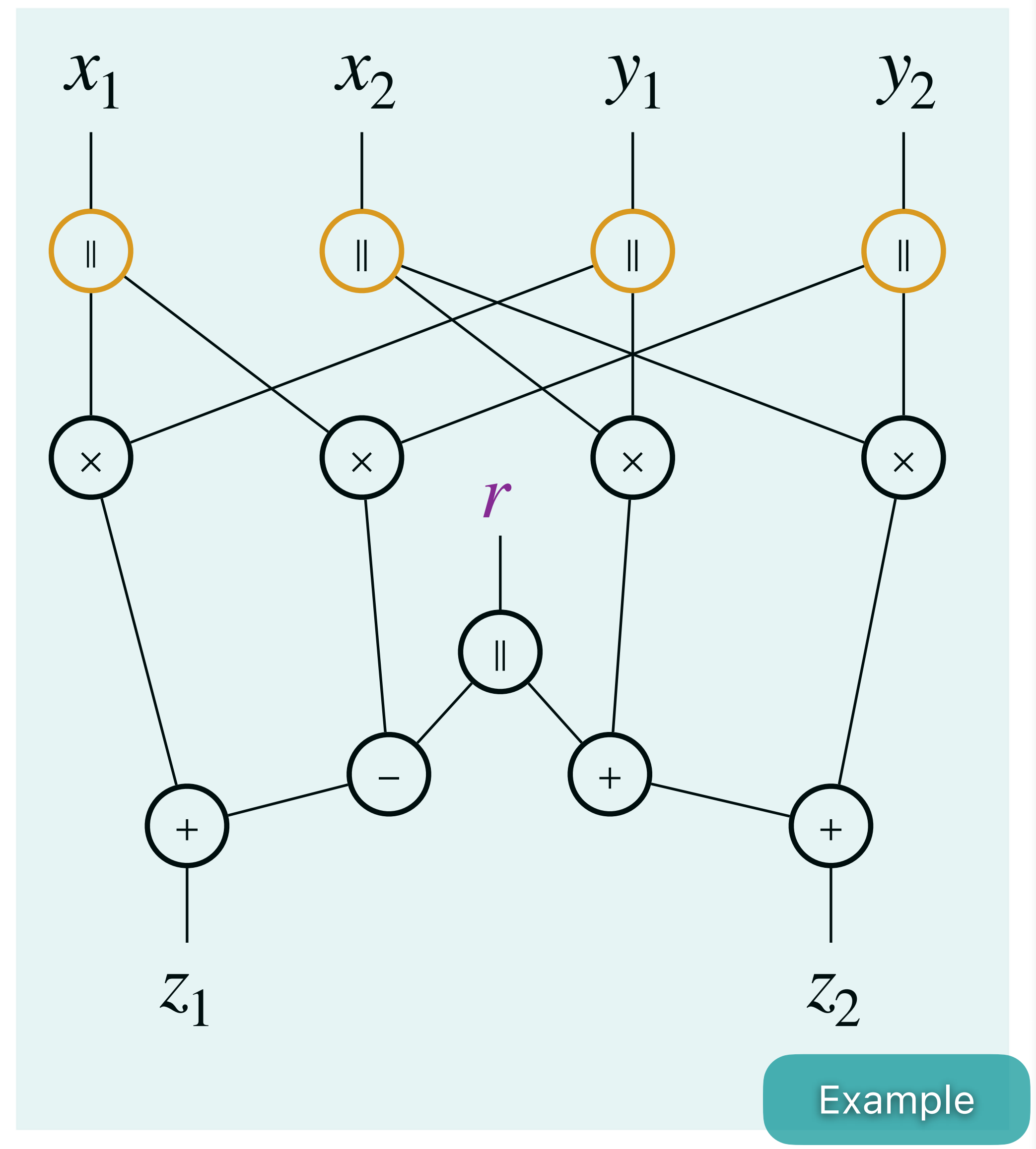
Copies:

$x_1 \rightarrow (x_1^1, x_1^2)$

$x_2 \rightarrow (x_2^1, x_2^2)$

$y_1 \rightarrow (y_1^1, y_1^2)$

$y_2 \rightarrow (y_2^1, y_2^2)$



Masking

Chari • Jutla • Rao • Rohatgi

CRYPTO 1999

Goubin • Patarin

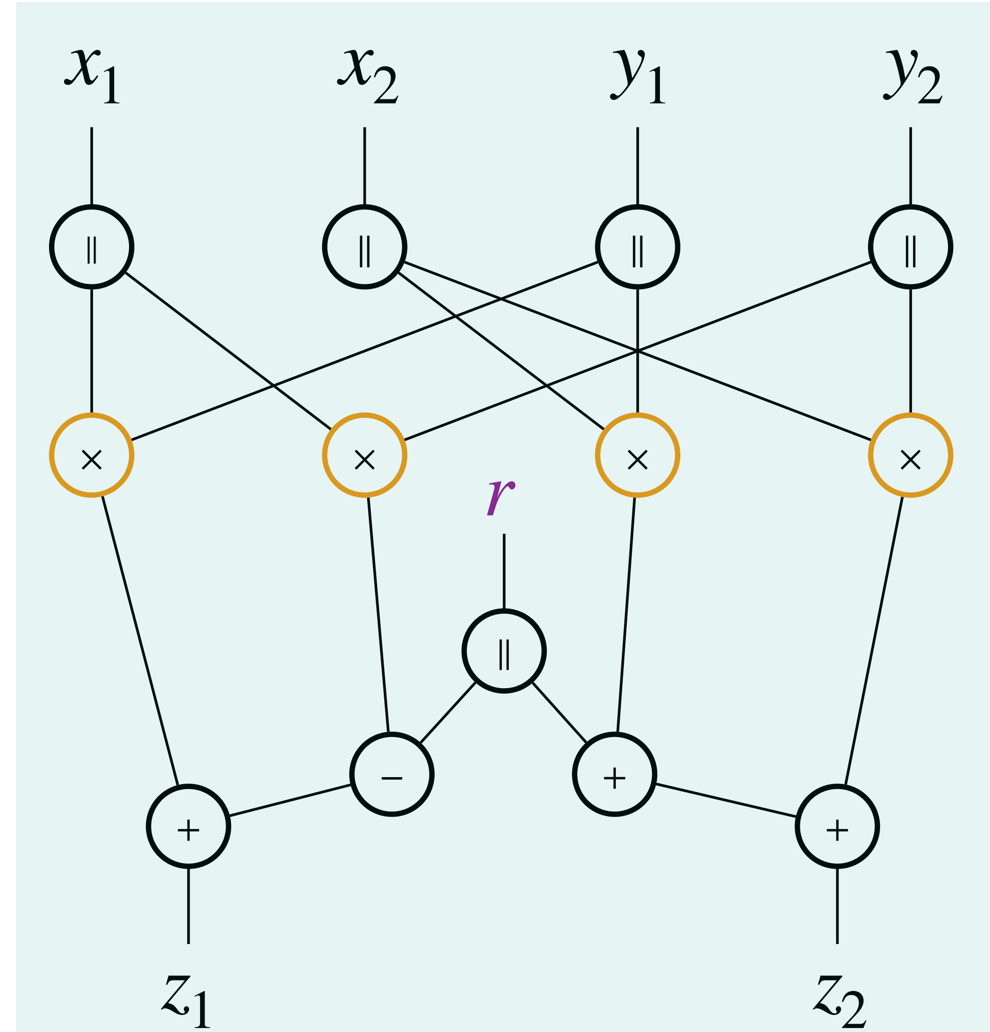
CHES, 1999

non-linear function

Cross-products:

$x_1^2 \cdot y_2^1$ $\quad$ $x_1^1 \cdot y_1^1$

$x_2^2 \cdot y_2^2$ $\quad$ $x_2^1 \cdot y_1^2$

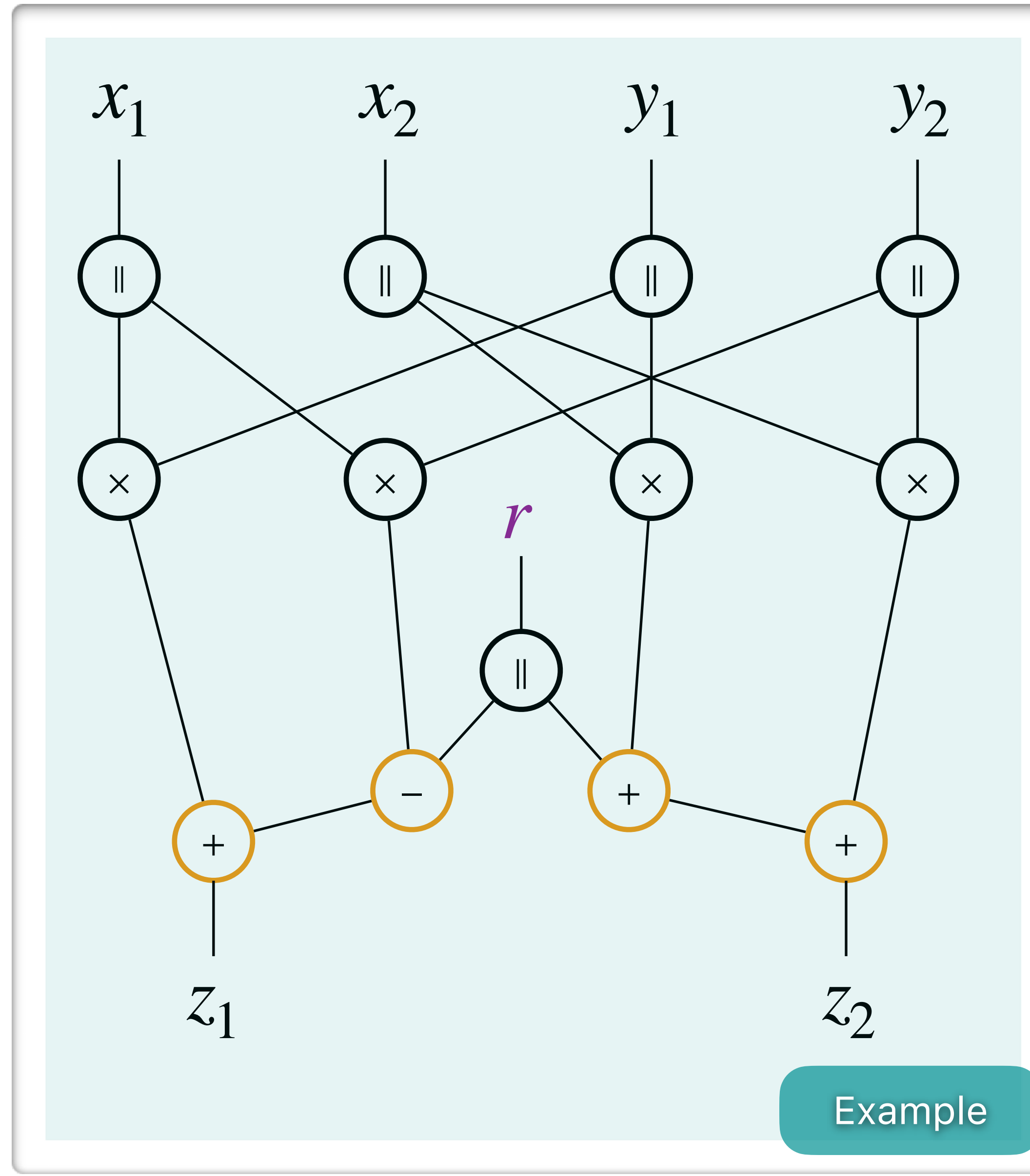


Example

Masking

Chari • Jutla • Rao • Rohatgi
CRYPTO 1999
Goubin • Patarin
CHES, 1999

non-linear function



Final sums:

$$x_1^2 \cdot y_2^1 - r + x_1^1 \cdot y_1^1$$
$$x_2^2 \cdot y_2^2 + r + x_2^1 \cdot y_1^2$$

Leakage Models

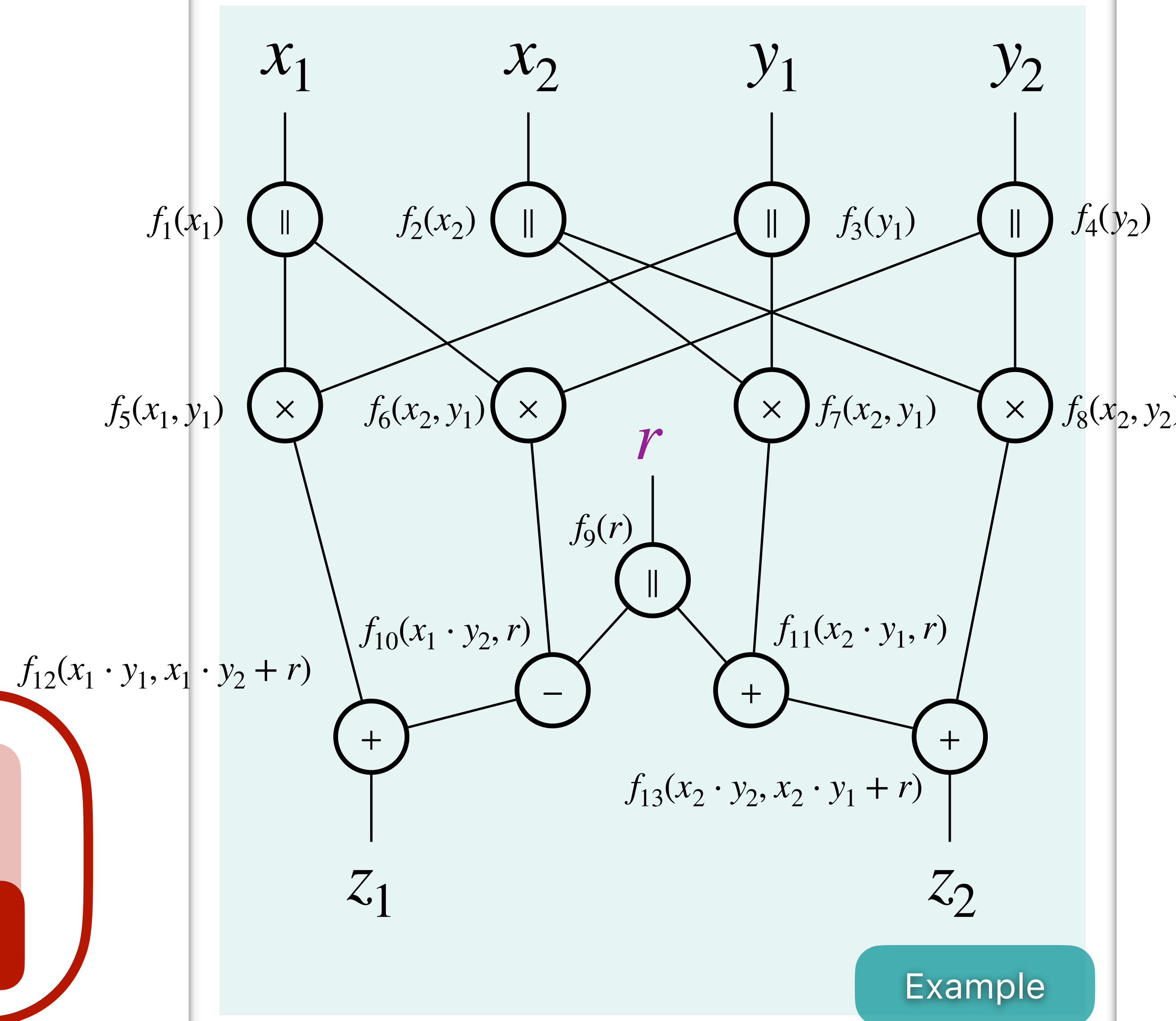
Chari • Jutla • Rao • Rohatgi
CRYPTO 1999
Prouff • Rivain
EUROCRYPT 2013

δ-noisy leakage model

Most realistic

Leakage Models

Chari • Jutla • Rao • Rohatgi
CRYPTO 1999
Prouff • Rivain
EUROCRYPT 2013

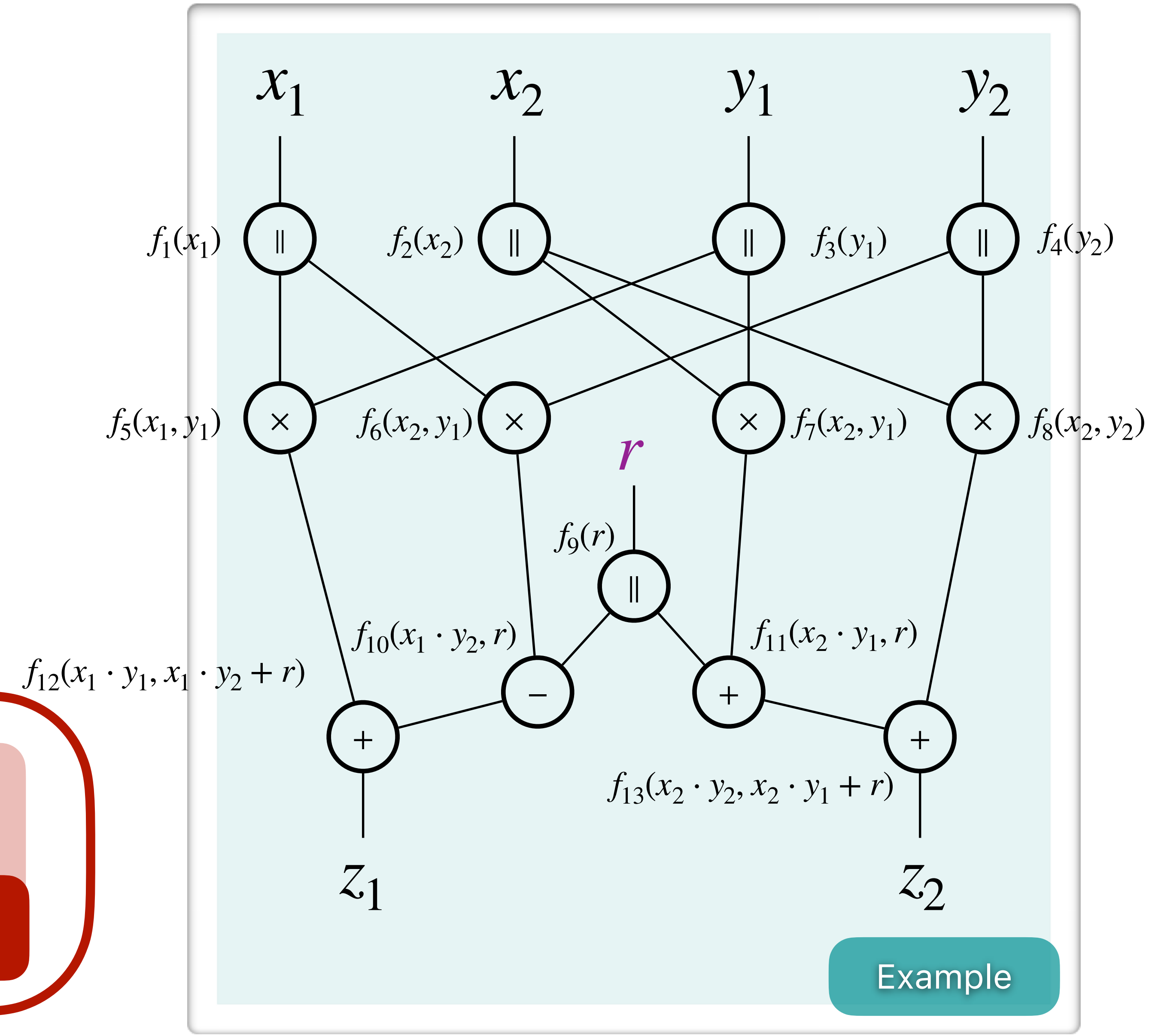


δ-noisy leakage model

Most realistic

Leakage Models

Chari • Jutla • Rao • Rohatgi
CRYPTO 1999
Prouff • Rivain
EUROCRYPT 2013



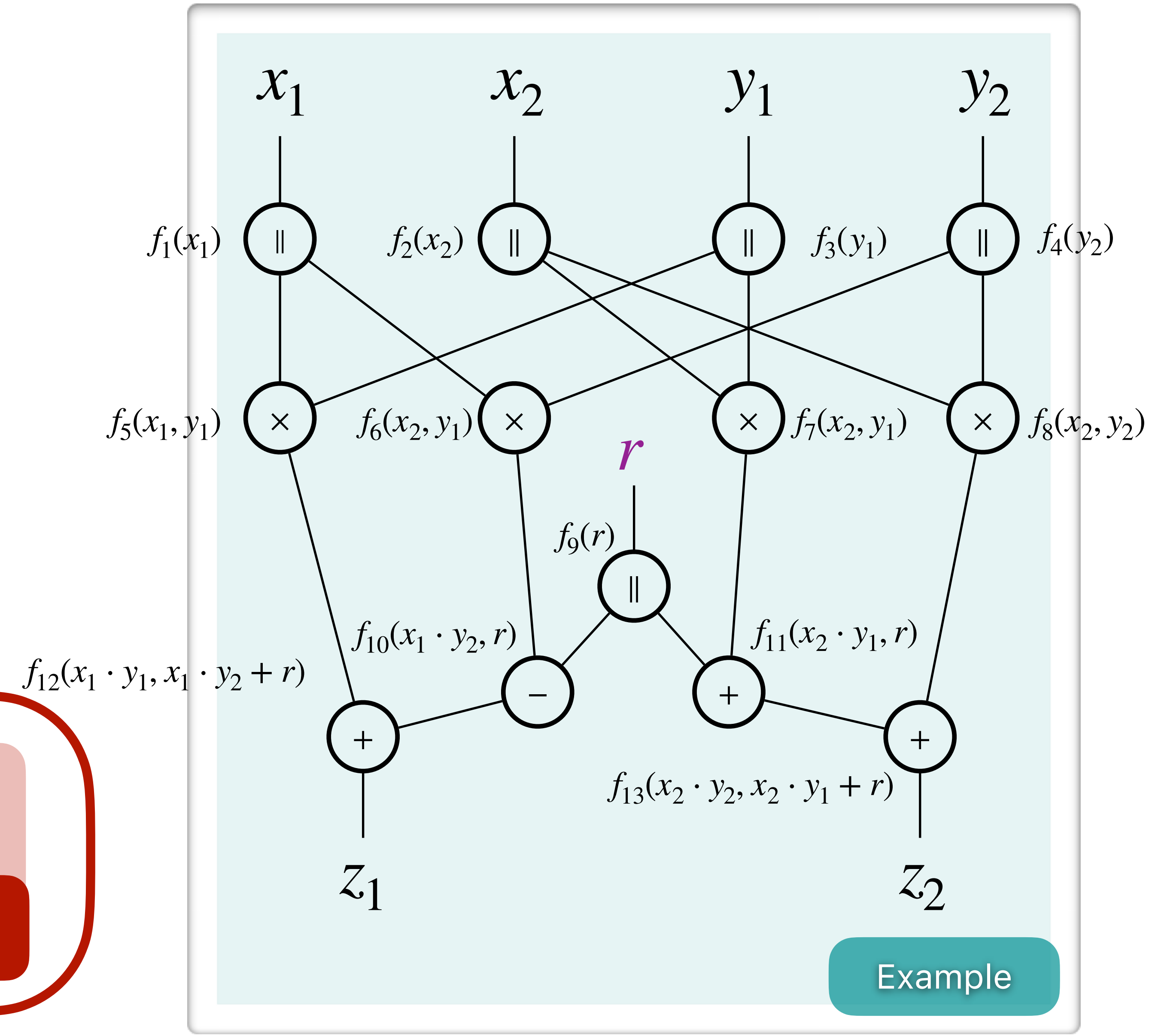
δ-noisy leakage model

Most realistic

$$\beta_\Delta(X \mid f_i(X)) = \mathbb{E}_y\left[\Delta(X; X \mid f_i(X) = y)\right] \leq \delta$$

Leakage Models

Chari • Jutla • Rao • Rohatgi
CRYPTO 1999
Prouff • Rivain
EUROCRYPT 2013



δ-noisy leakage model

Most realistic

$$\beta_\Delta(X \,|\, f_1(X), f_2(X), \ldots, f_{13}(X)) \leq \varepsilon$$

Leakage Models

Ishai • Sahai • Wagner
CRYPTO 2003

t-probing model

Most convenient

δ-noisy leakage model

Most realistic

Leakage Models

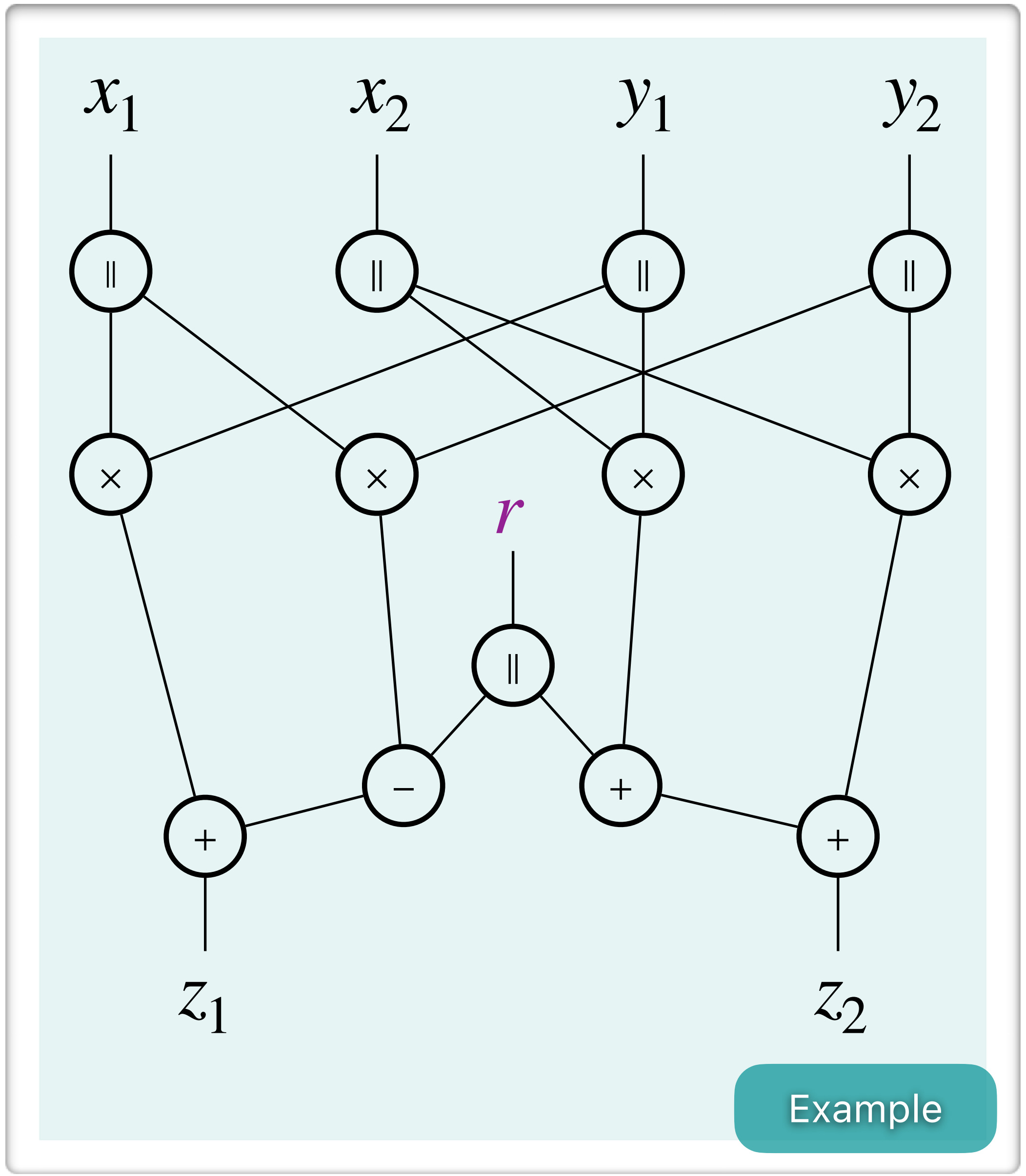
Ishai • Sahai • Wagner
CRYPTO 2003

t-probing model

Most convenient

δ-noisy leakage model

Most realistic



Leakage Models

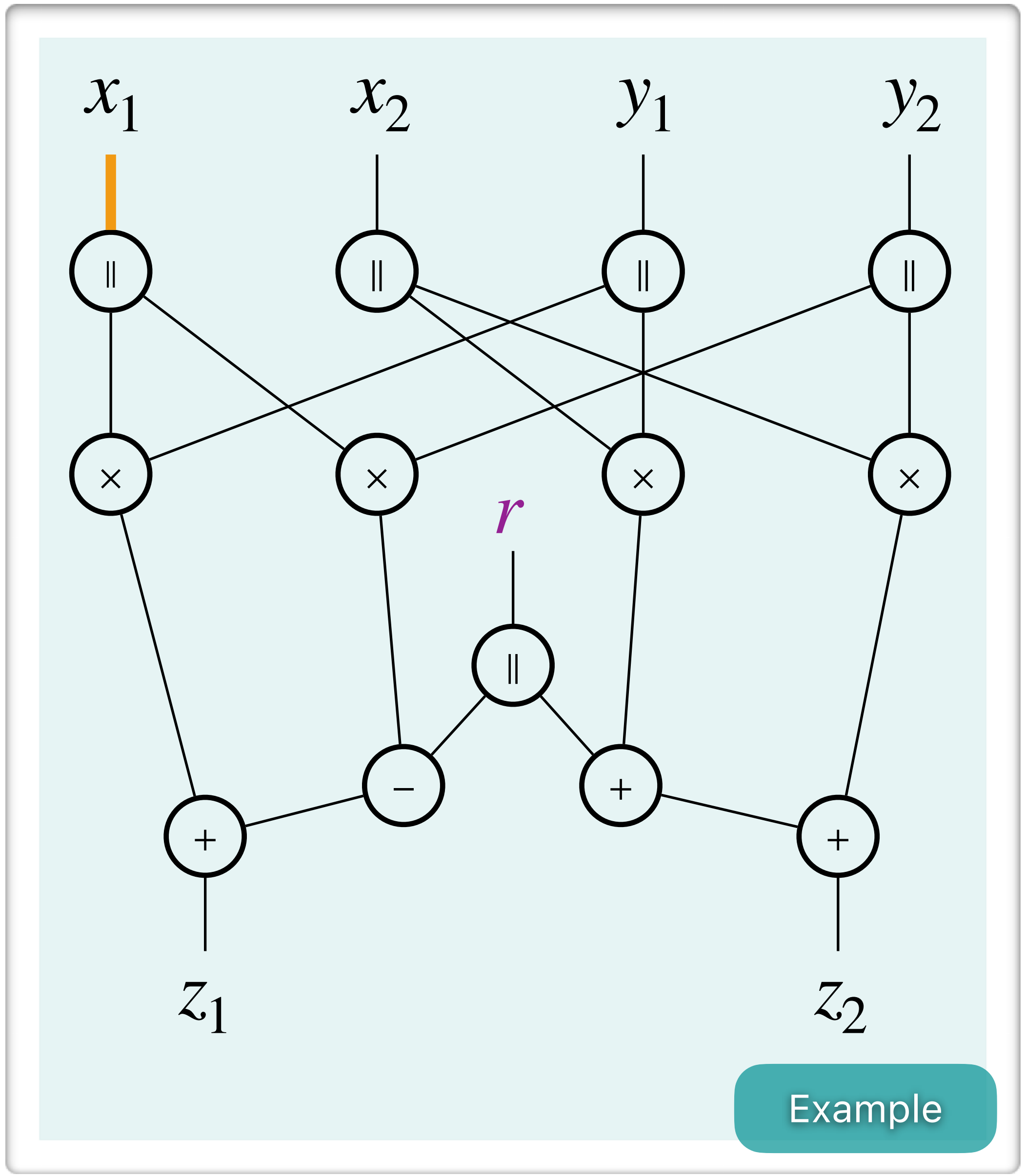
Ishai • Sahai • Wagner
CRYPTO 2003

t-probing model

Most convenient

δ-noisy leakage model

Most realistic



Leakage Models

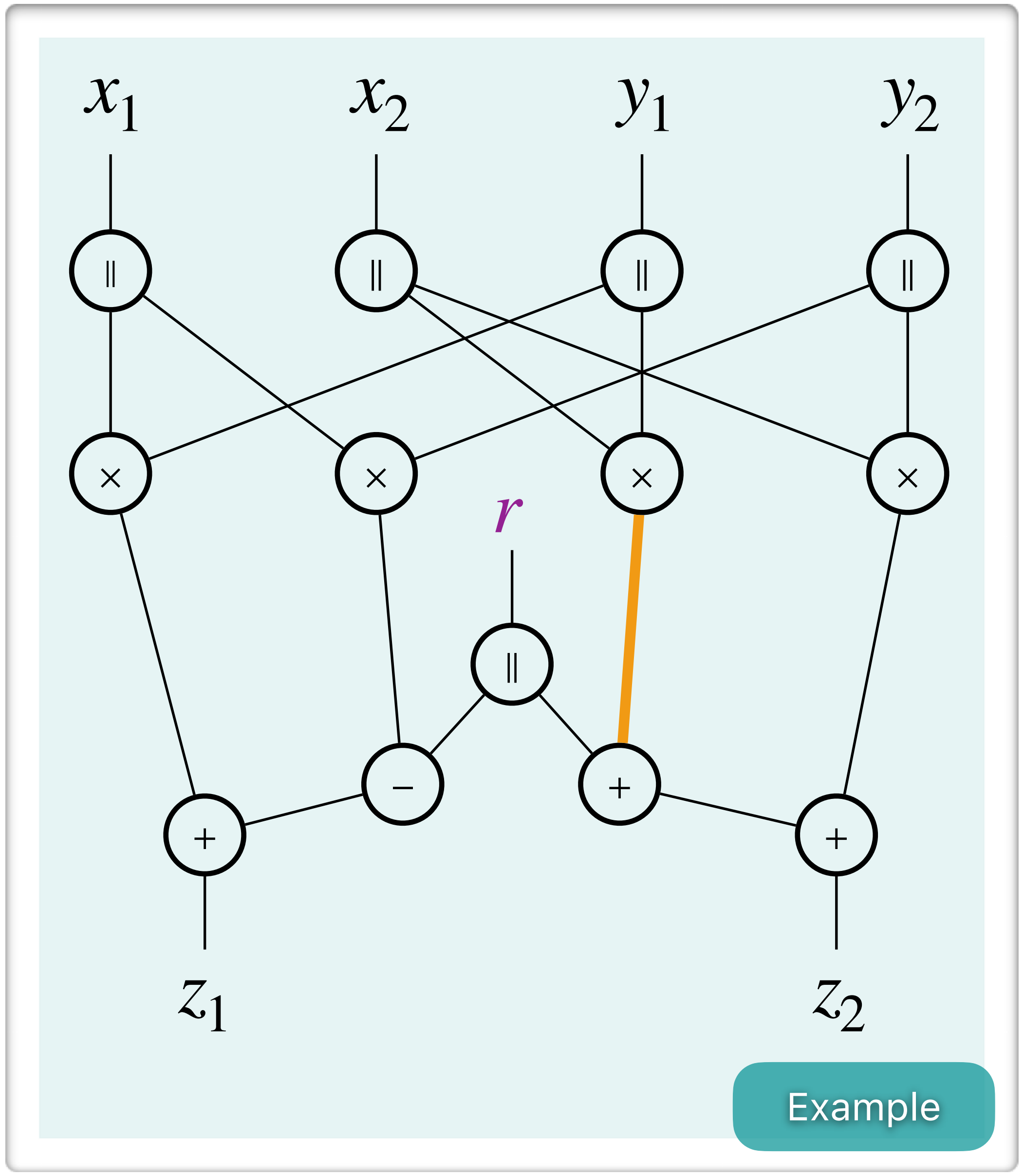
Ishai • Sahai • Wagner
CRYPTO 2003

t-probing model

Most convenient

δ-noisy leakage model

Most realistic



Leakage Models

Ishai • Sahai • Wagner
CRYPTO 2003
Duc • Dziembowski • Faust
EUROCRYPT 2014

t-probing model
Most convenient

p-random probing model
Best trade-off

δ-noisy leakage model
Most realistic

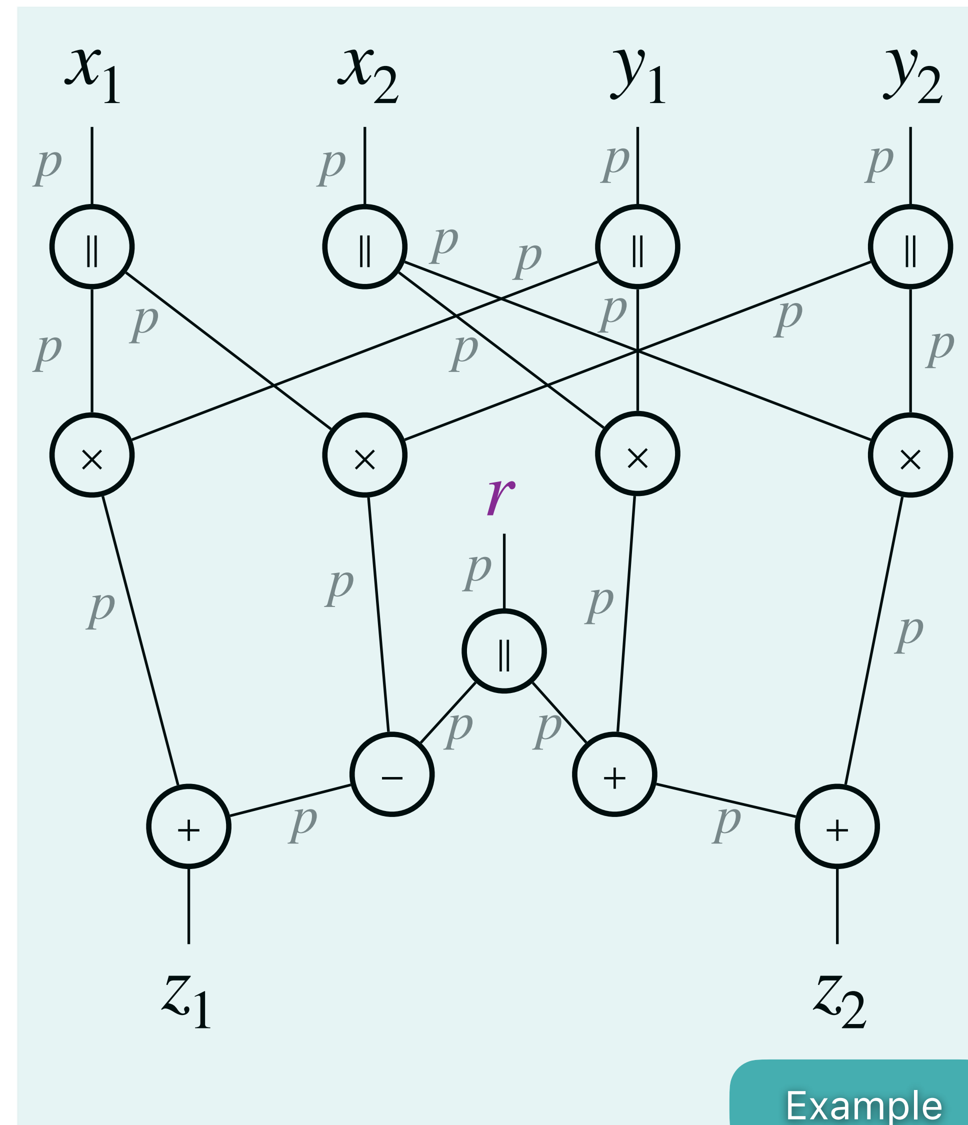
Leakage Models

Ishai • Sahai • Wagner
CRYPTO 2003
Duc • Dziembowski • Faust
EUROCRYPT 2014

t-probing model
Most convenient

p-random probing model
Best trade-off

δ-noisy leakage model
Most realistic



Leakage Models

Ishai • Sahai • Wagner
CRYPTO 2003
Duc • Dziembowski • Faust
EUROCRYPT 2014

t-probing model

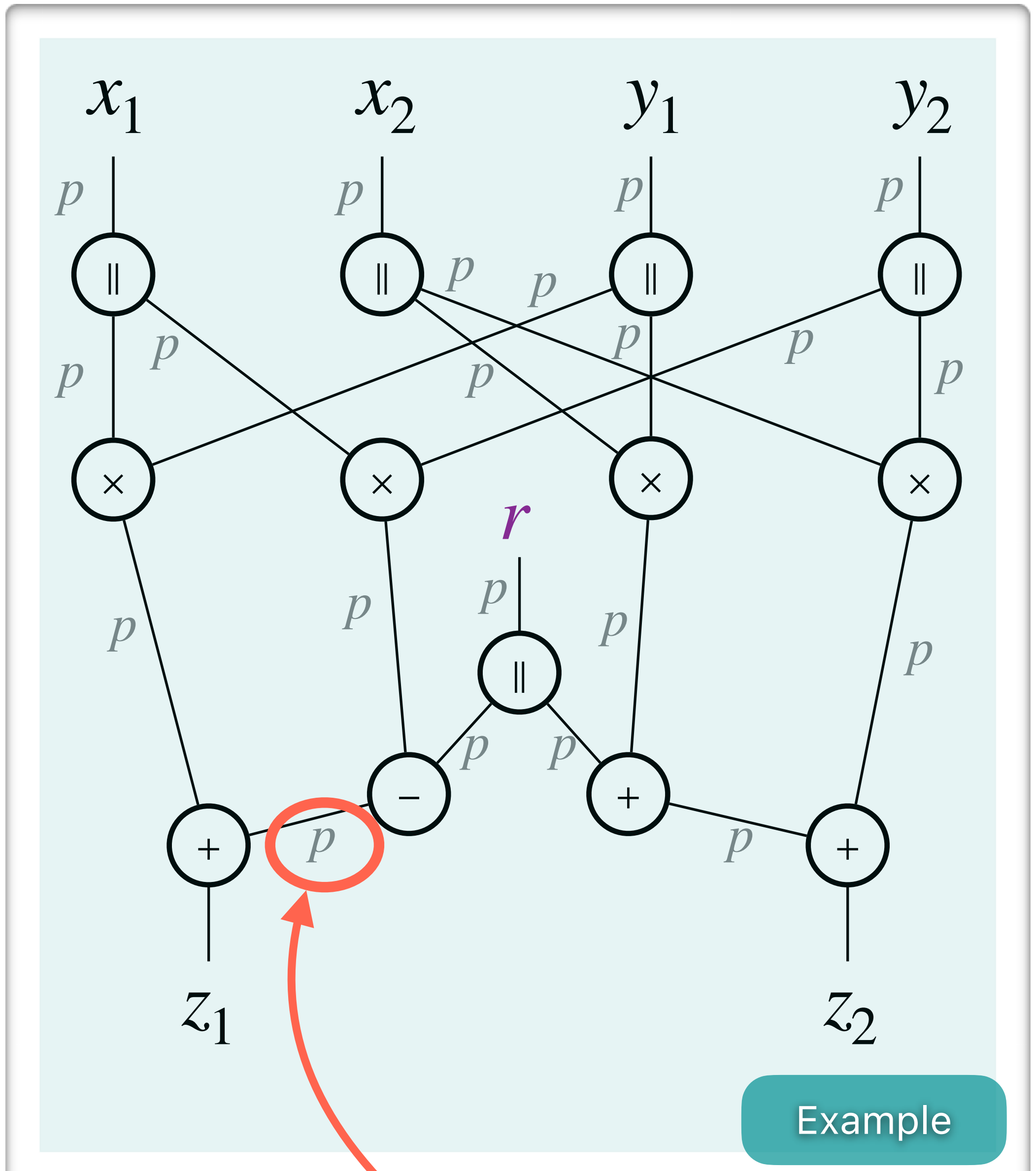
Most convenient

p-random probing model

Best trade-off

δ-noisy leakage model

Most realistic



leakage rate

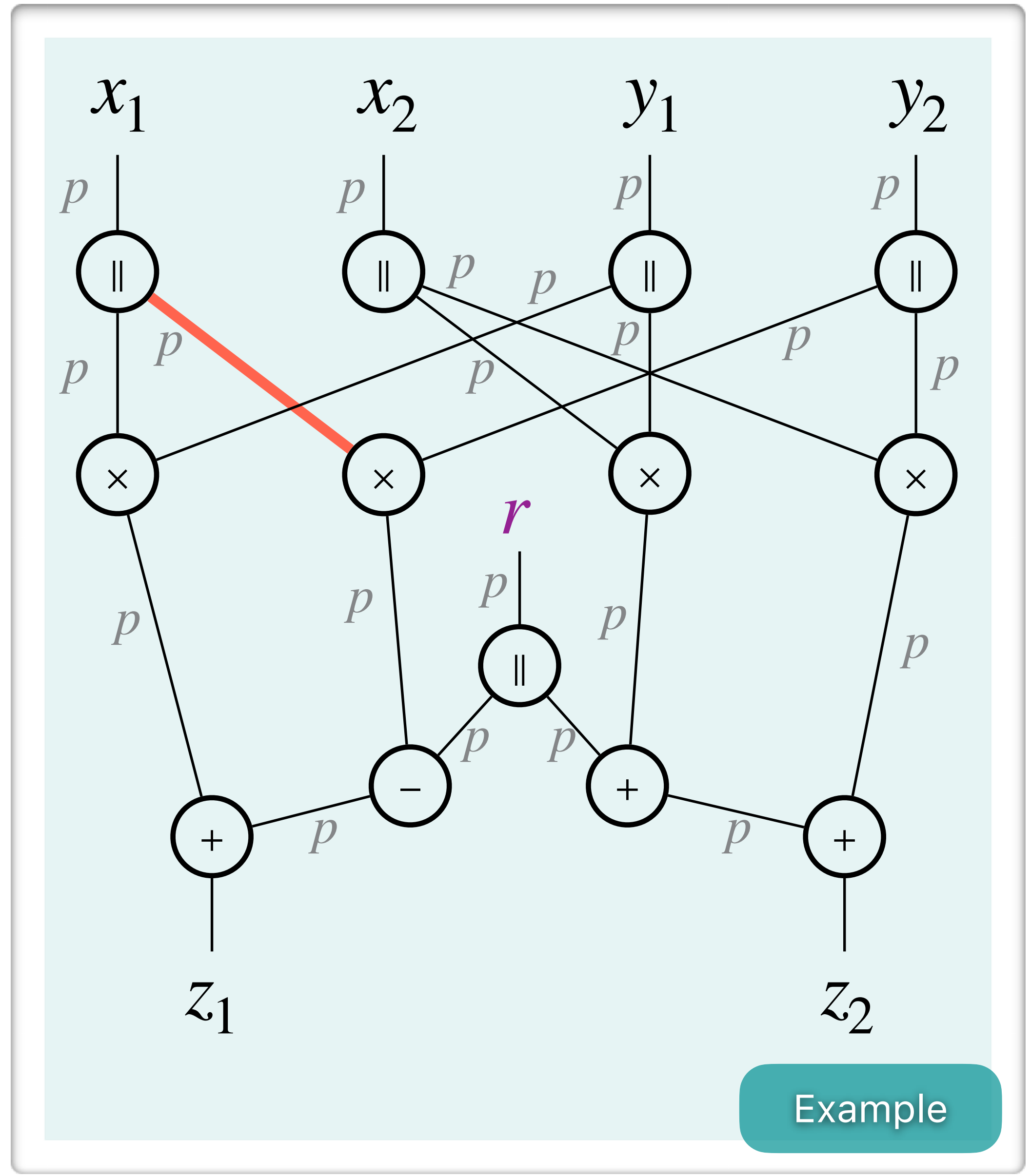
Leakage Models

Ishai • Sahai • Wagner
CRYPTO 2003
Duc • Dziembowski • Faust
EUROCRYPT 2014

t-probing model
Most convenient

p-random probing model
Best trade-off

δ-noisy leakage model
Most realistic



DDF Reduction

t-probing security

Most convenient

p-random probing security

Best trade-off

$\downarrow$

δ-noisy leakage security

Most realistic

with $\delta = \Theta(p)$

Duc • Dziembowski • Faust
EUROCRYPT 2014

DDF Reduction

t-probing security

Most convenient

p-random probing security

Best trade-off

$\downarrow$

δ-noisy leakage security

Most realistic

with $\delta = \Theta(p)$

Duc • Dziembowski • Faust

EUROCRYPT 2014

DDF Reduction

t-probing security

Most convenient

p-random probing security

Best trade-off

δ-noisy leakage security

Most realistic

with $p = \Theta\left(\frac{t}{|C|}\right)$

Duc • Dziembowski • Faust
EUROCRYPT 2014

with $\delta = \Theta(p)$

DDF Reduction

t-probing security

Most convenient

↓

p-random probing security

Best trade-off

↓

δ-noisy leakage security

Most realistic

with $p = \Theta\left(\frac{t}{|C|}\right)$

Duc • Dziembowski • Faust
EUROCRYPT 2014

with $\delta = \Theta(p)$

DDF Reduction

t-probing security

Most convenient

with $p = \Theta\left(\frac{t}{|C|}\right)$

p-random probing security

Best trade-off

δ-noisy leakage security

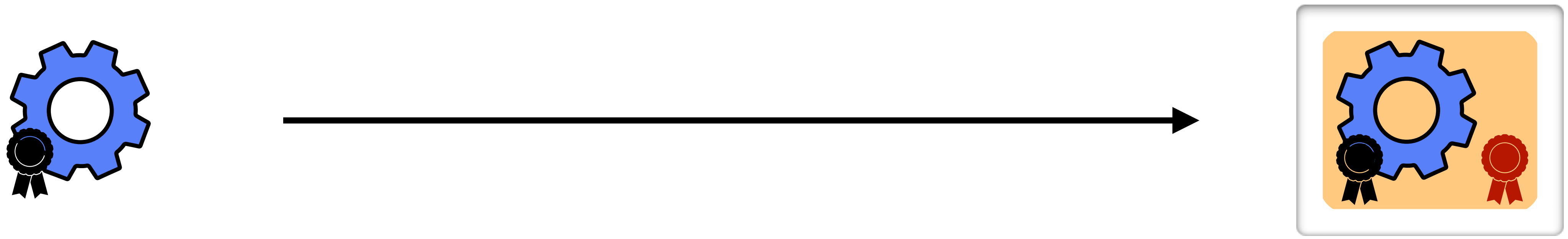
Most realistic

with $\delta = \Theta(p)$

Duc • Dziembowski • Faust
EUROCRYPT 2014

Contributions

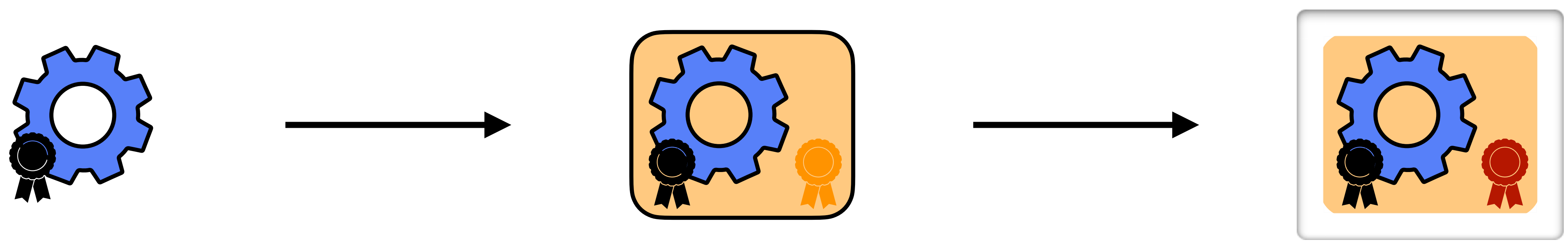
Contributions



Black-box secure

Black-box and
physically secure

Contributions



Black-box secure

Black-box and random probing secure

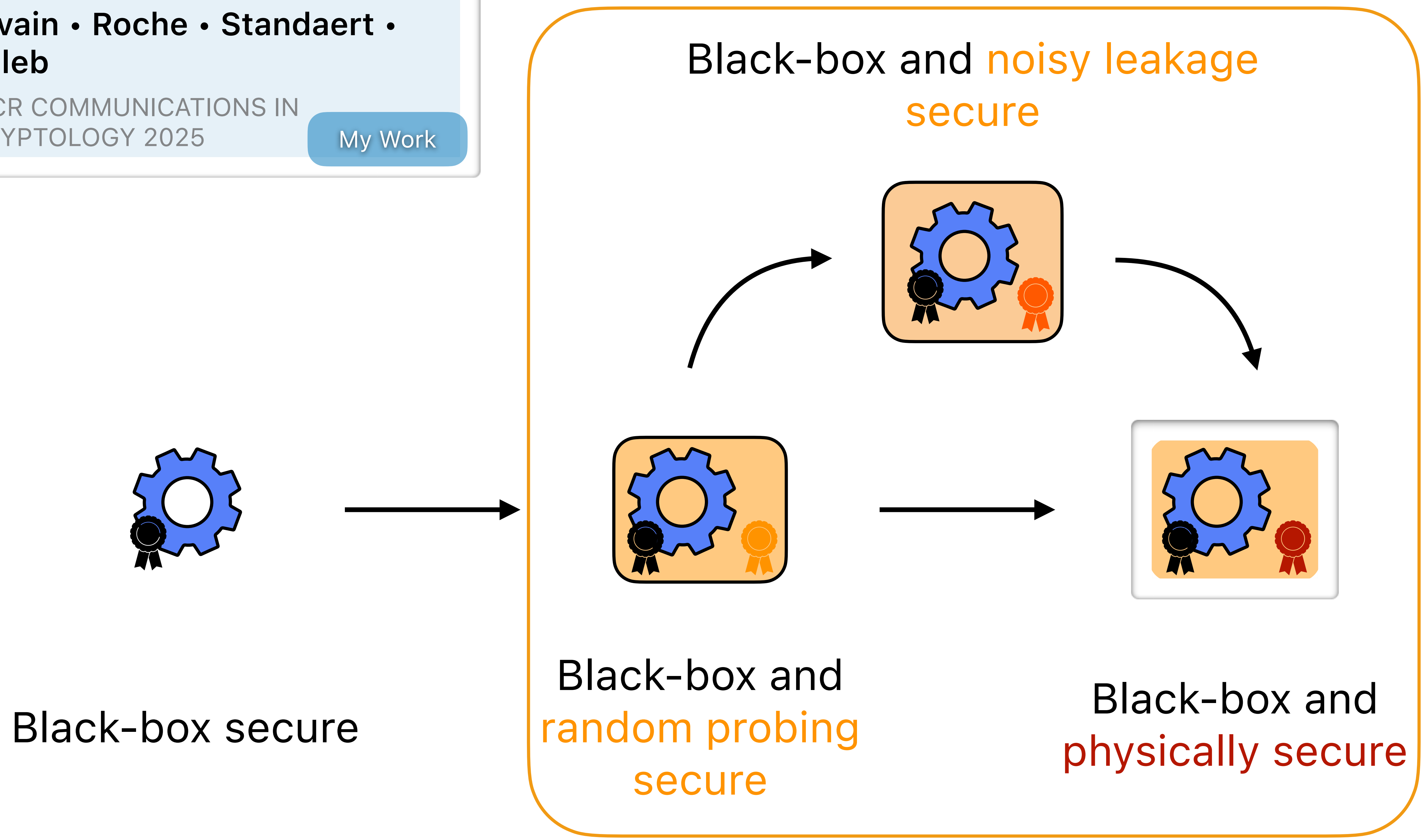
Black-box and physically secure

Contributions

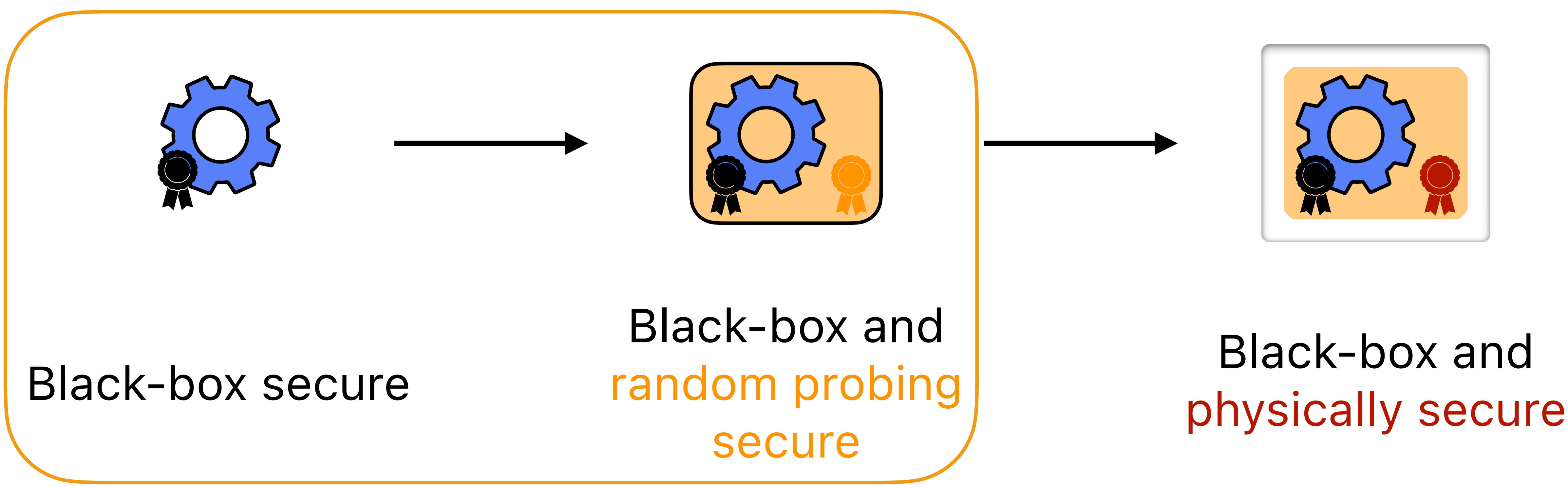
Belaïd • Cassiers • Mutschler • Rivain • Roche • Standaert • Taleb

IACR COMMUNICATIONS IN CRYPTOLOGY 2025

My Work



Contributions

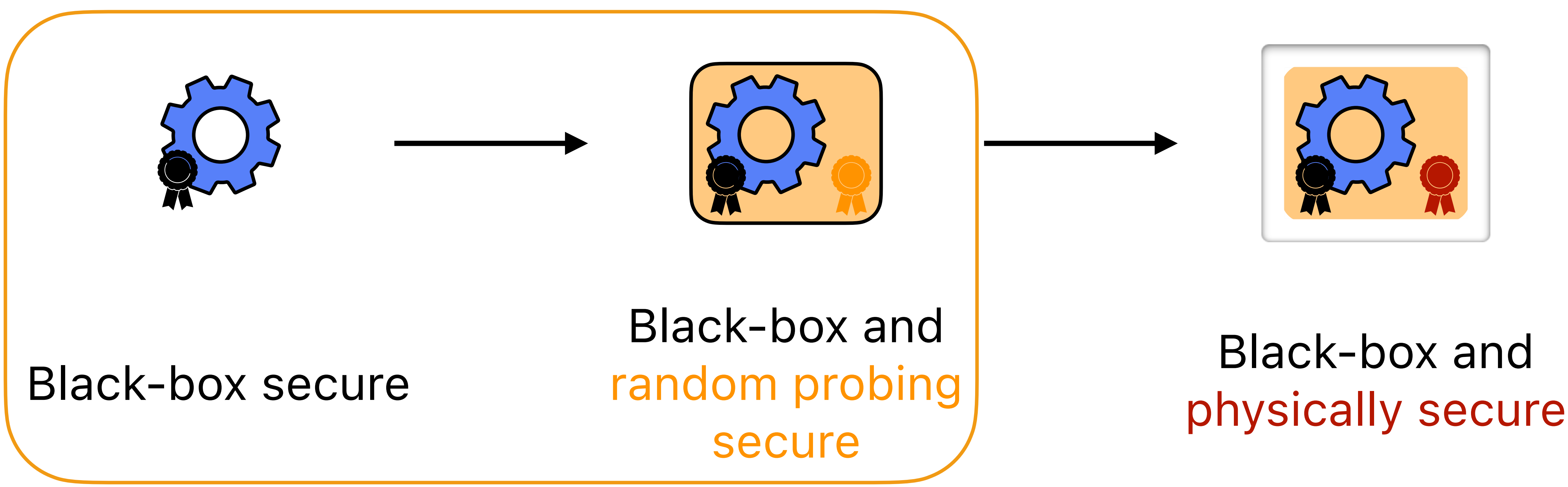


Contributions

Foundations
Random probing security & verification (small circuits)

Scaling up
Composition frameworks (larger circuits)

Building blocks
Design of efficient gadgets



Contributions

Foundations

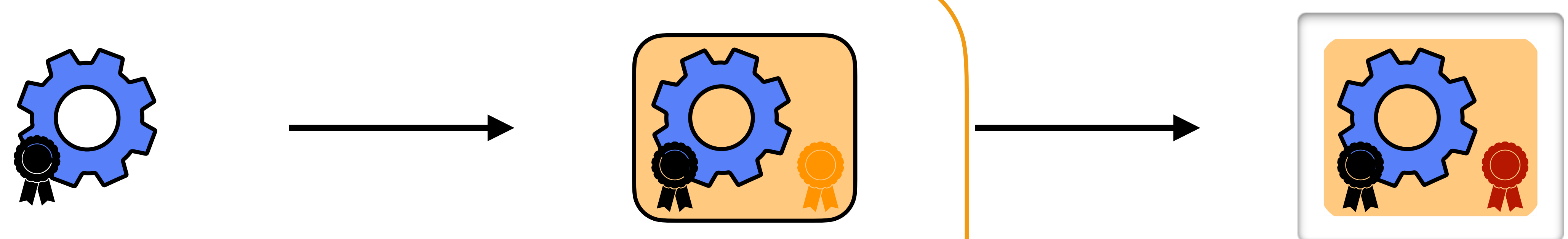
Random probing security & verification (small circuits)

Scaling up

Composition frameworks (larger circuits)

Building blocks

Design of efficient gadgets



Black-box secure

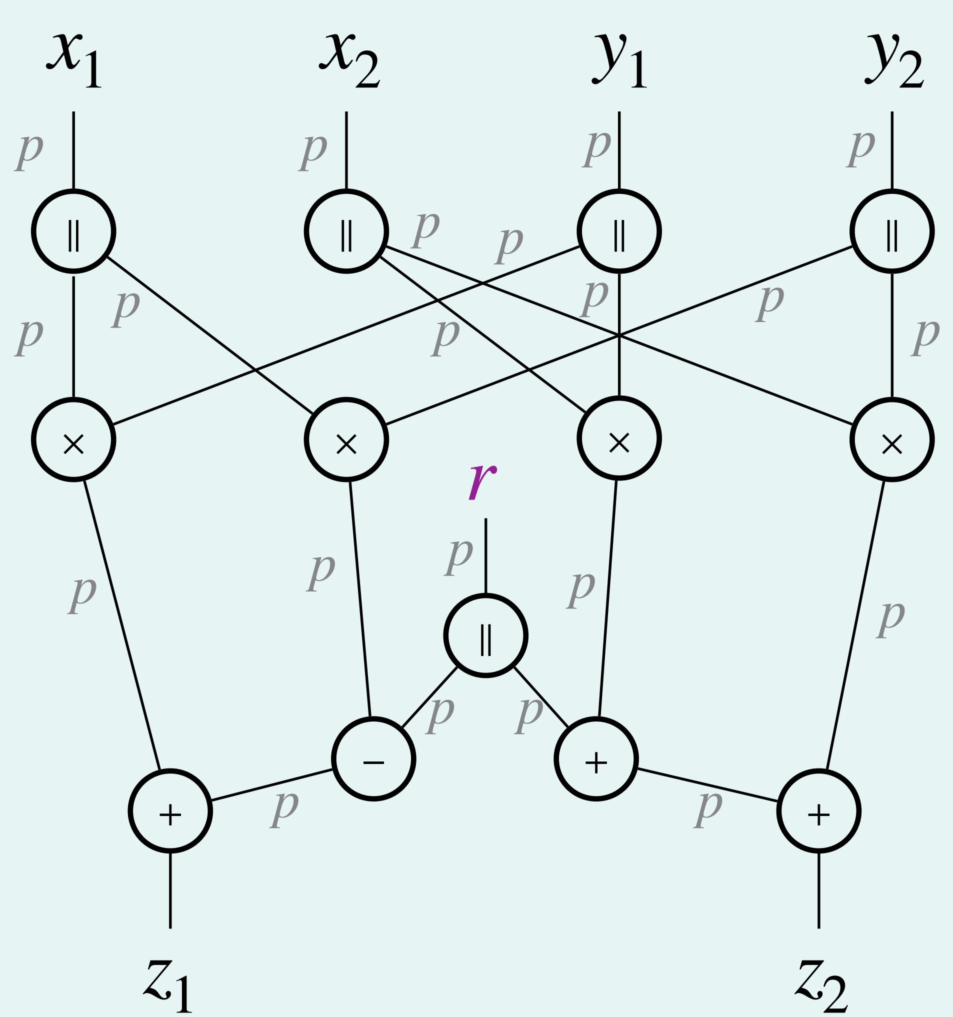
Black-box and random probing secure

Black-box and physically secure

Random Probing Security

Ananth • Ishai • Sahai
CRYPTO 2018

Adversary's view



Example

Simulator

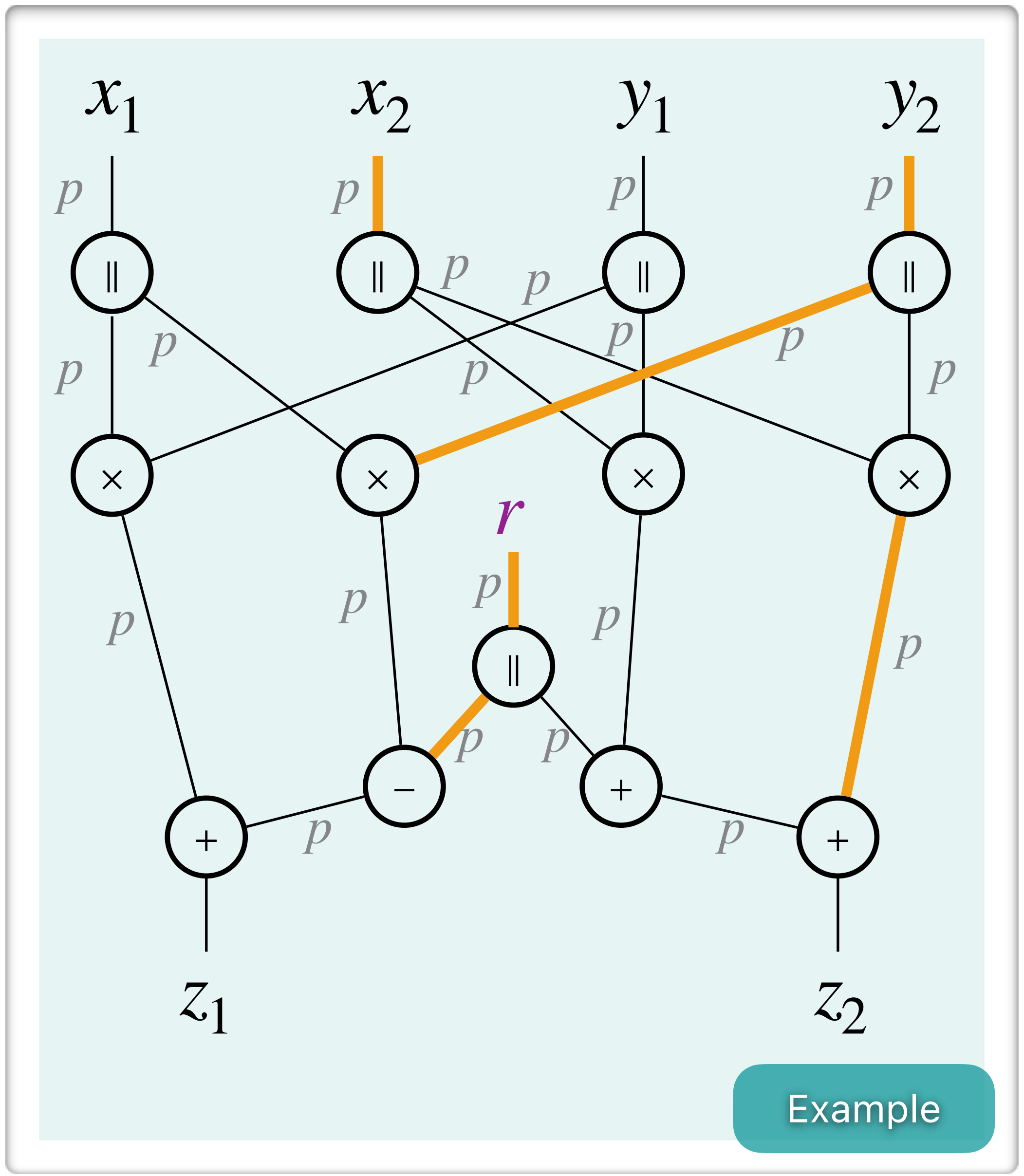
Example

A circuit is (p, ε)-random-probing secure if there exists a PPT simulator such that the distribution of the simulated leakage is ε-close to the one of the real leakage

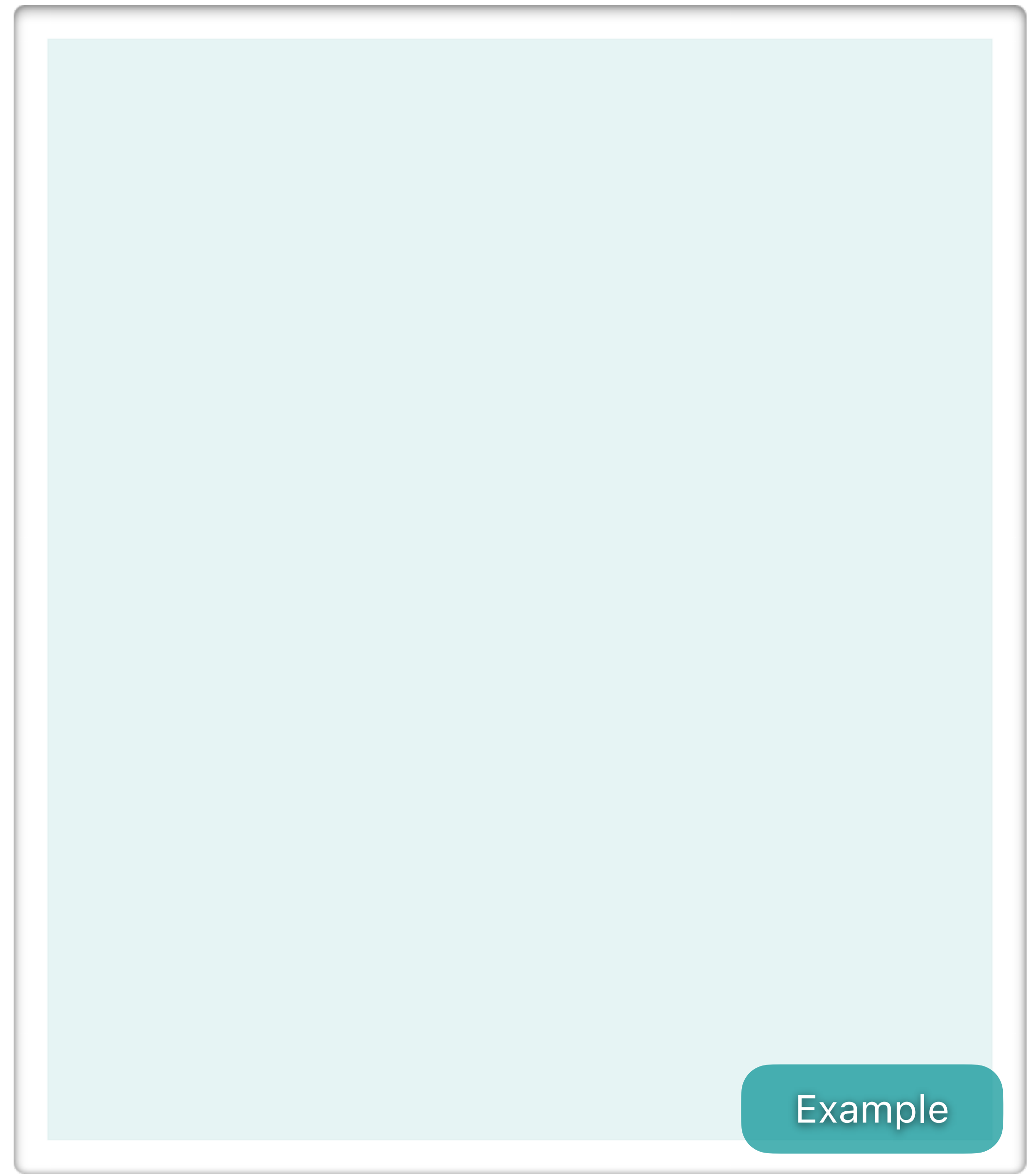
Random Probing Security

Ananth • Ishai • Sahai
CRYPTO 2018

Adversary's view



Simulator

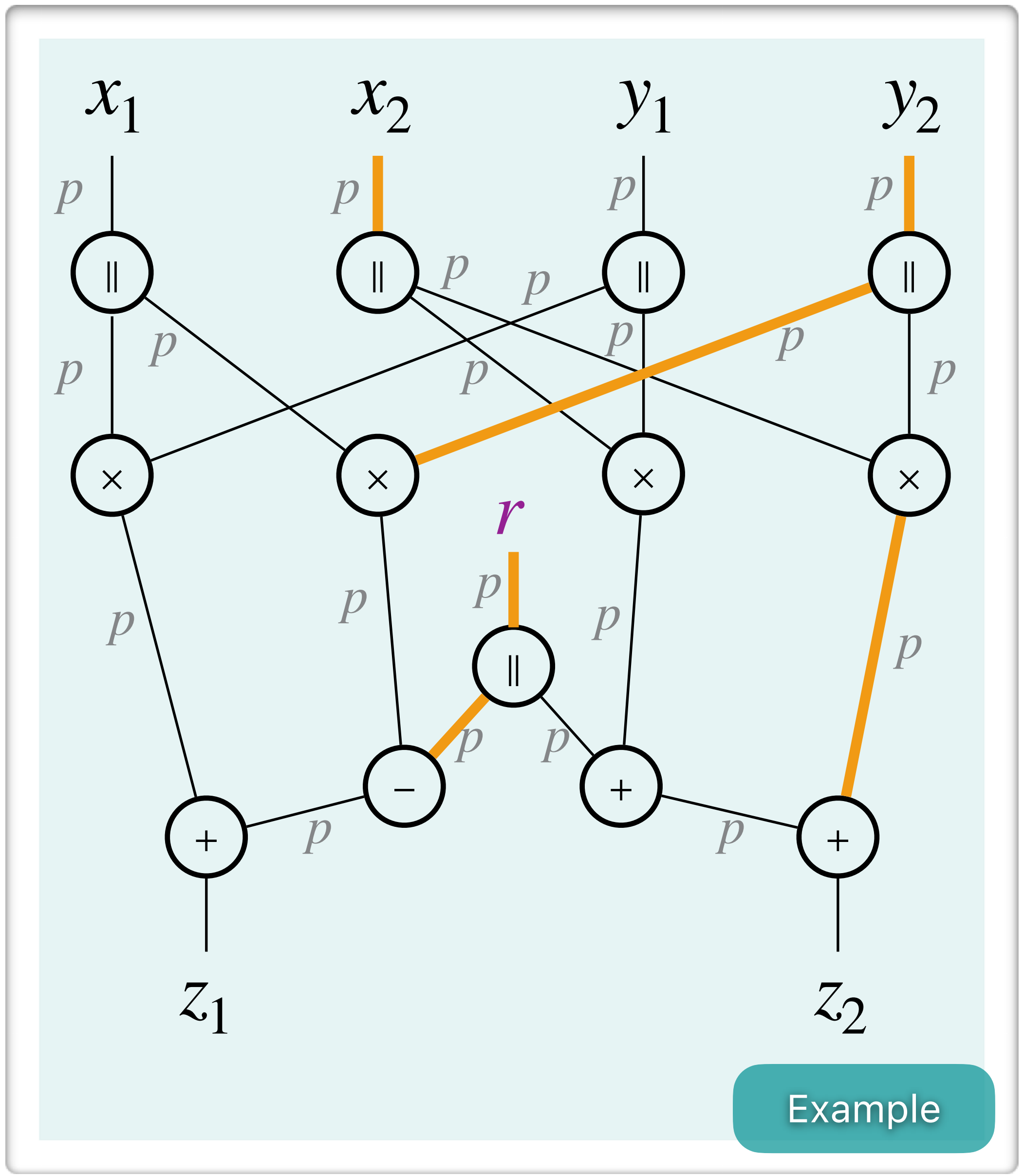


A circuit is (p, ε)-random-probing secure if there exists a PPT simulator such that the distribution of the simulated leakage is ε-close to the one of the real leakage

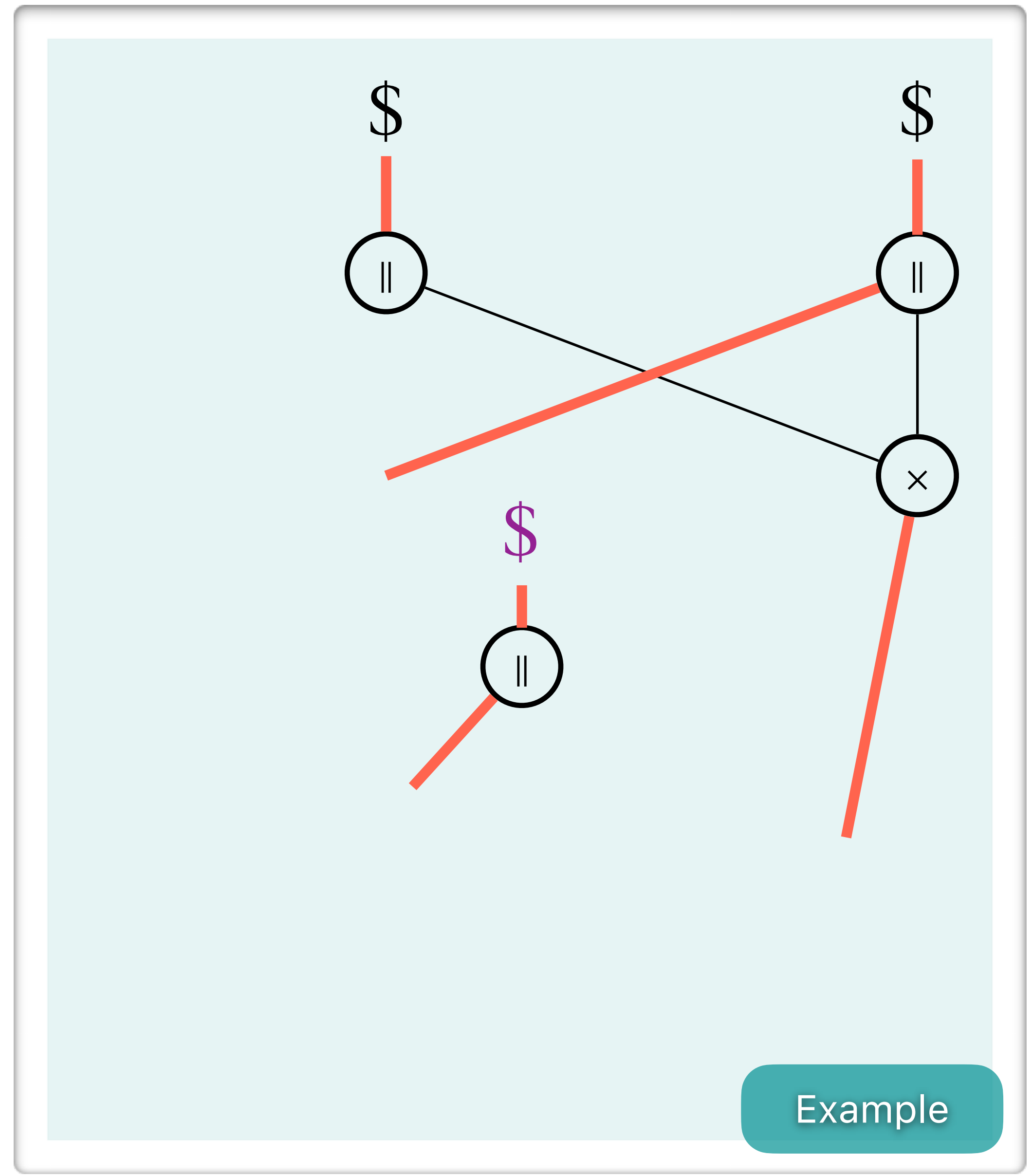
Random Probing Security

Ananth • Ishai • Sahai
CRYPTO 2018

Adversary's view



Simulator

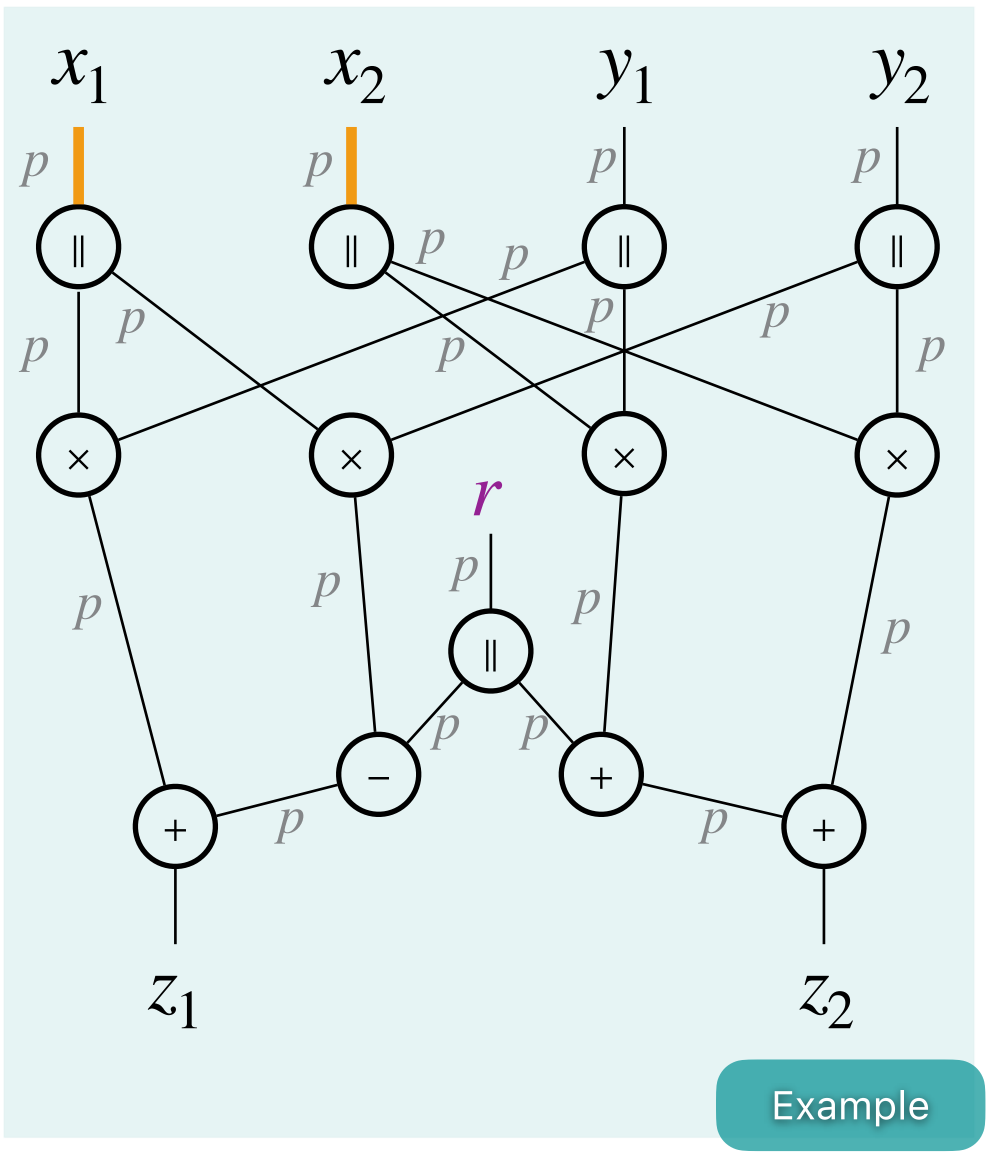


A circuit is (p, ε)-random-probing secure if there exists a PPT simulator such that the distribution of the simulated leakage is ε-close to the one of the real leakage

Random Probing Security

Ananth • Ishai • Sahai
CRYPTO 2018

Adversary's view



Simulator

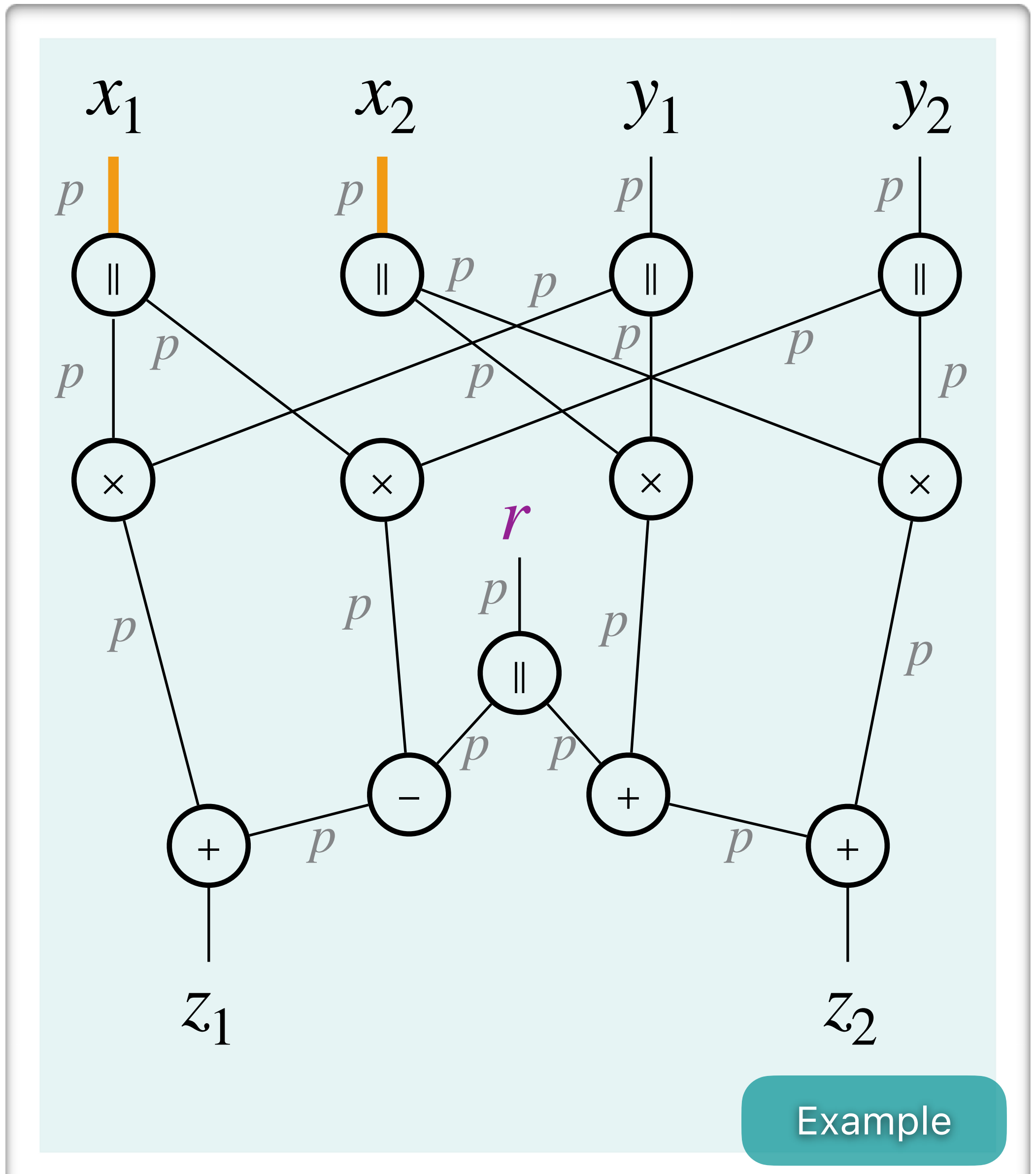
Example

A circuit is (p, ε)-random-probing secure if there exists a PPT simulator such that the distribution of the simulated leakage is ε-close to the one of the real leakage

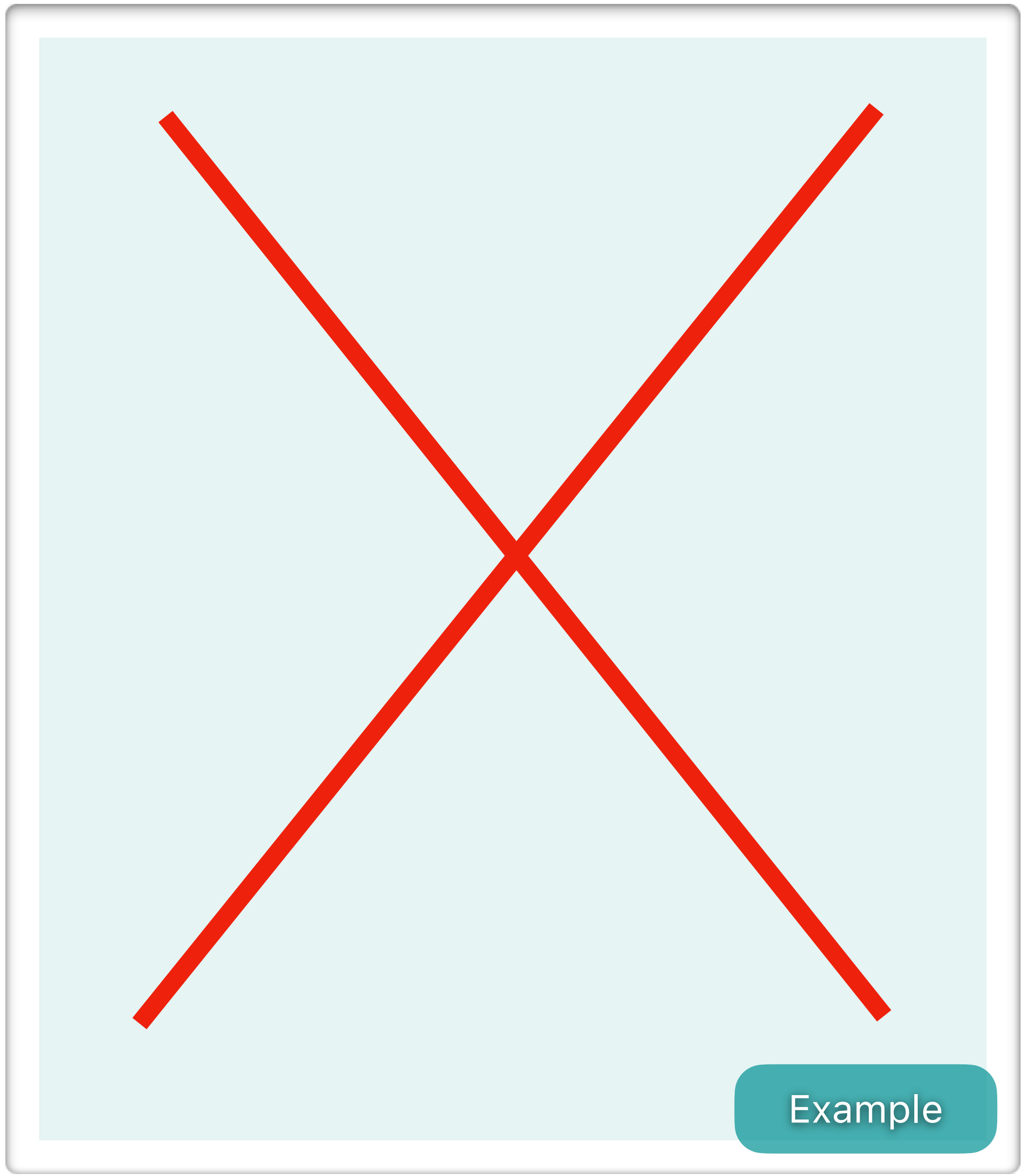
Random Probing Security

Ananth • Ishai • Sahai
CRYPTO 2018

Adversary's view



Simulator

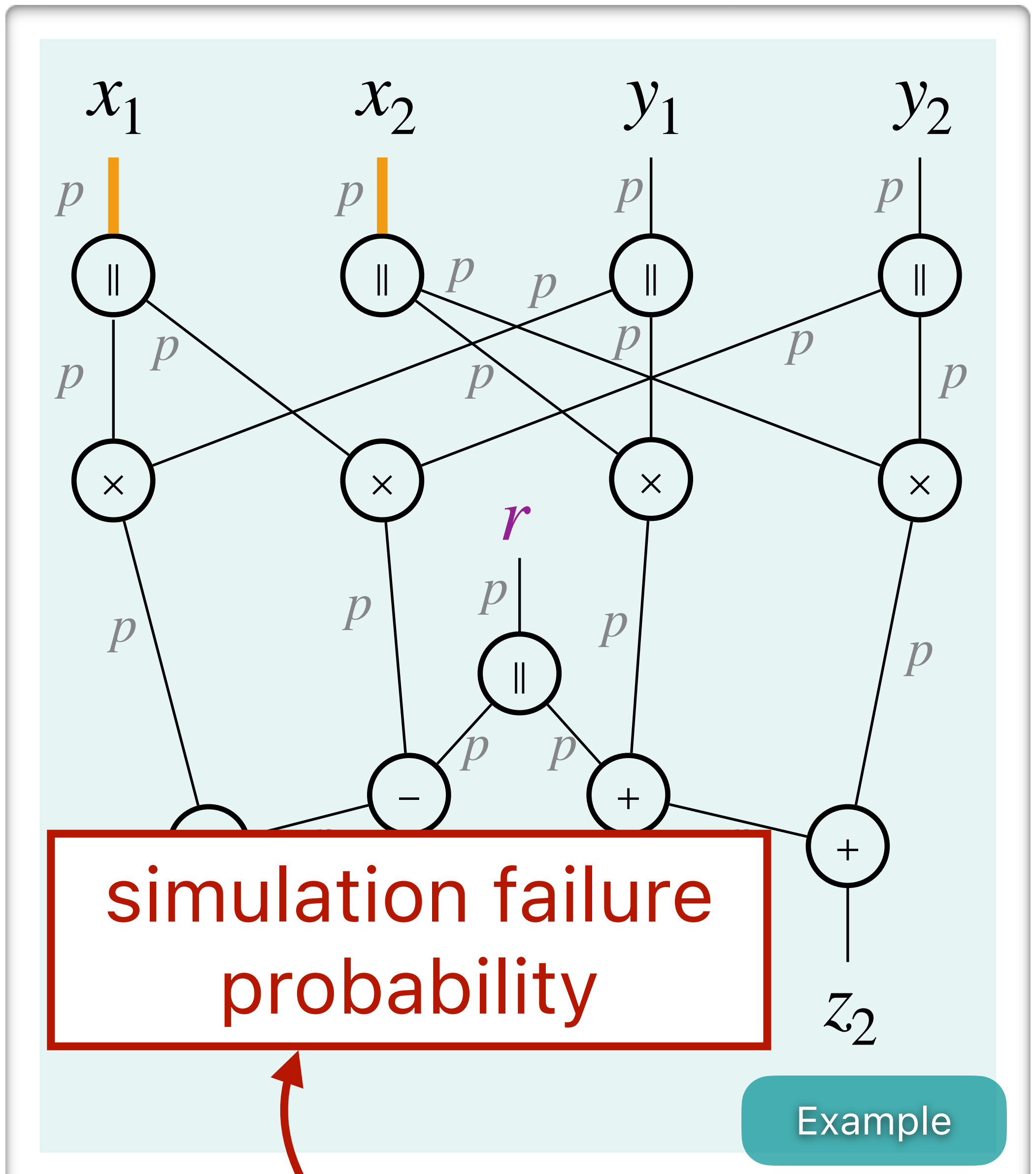


A circuit is (p, ε)-random-probing secure if there exists a PPT simulator such that the distribution of the simulated leakage is ε-close to the one of the real leakage

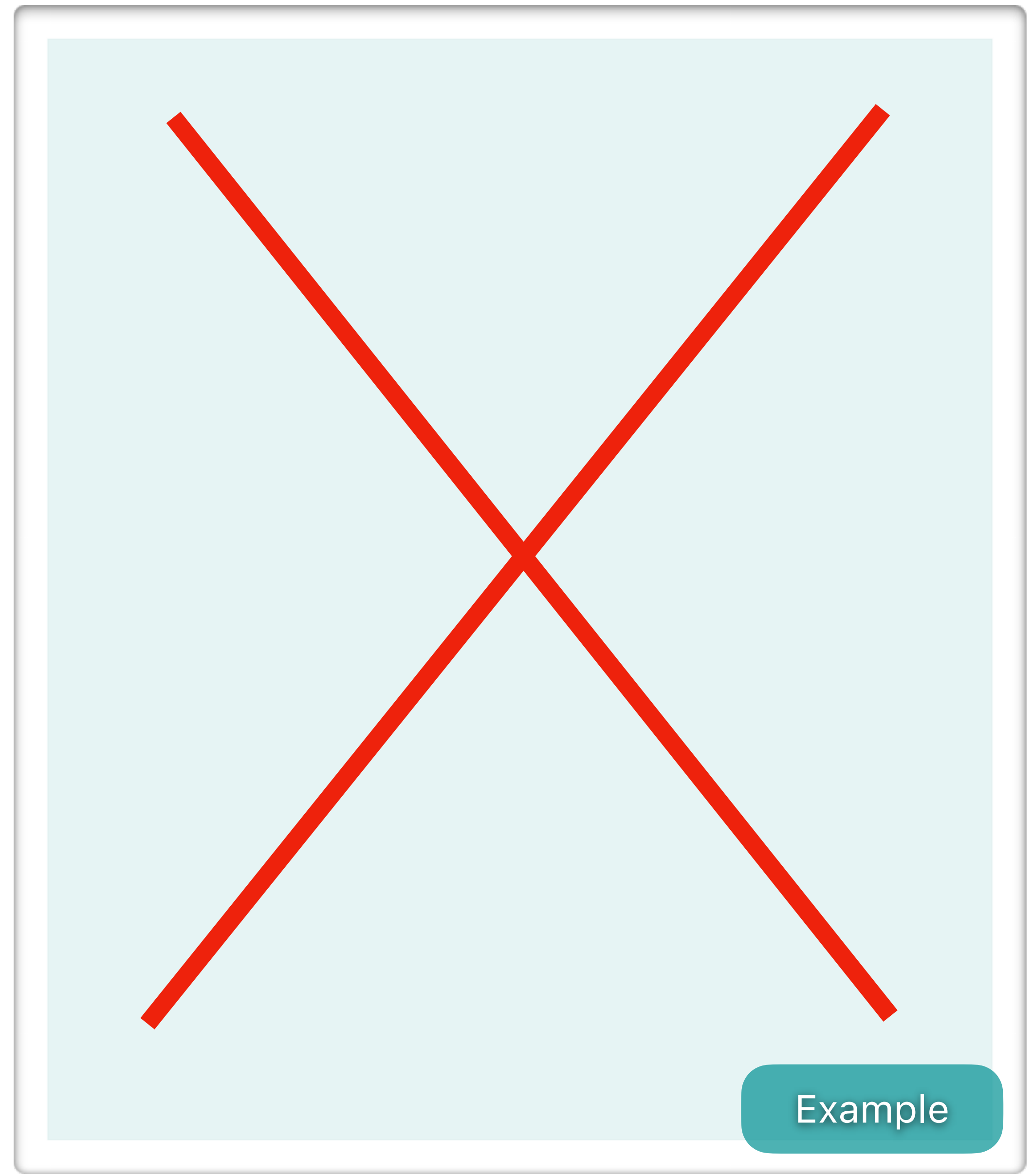
Random Probing Security

Ananth • Ishai • Sahai
CRYPTO 2018

Adversary's view



Simulator



A circuit is (p, ε)-random-probing secure if there exists a PPT simulator such that the distribution of the simulated leakage is ε-close to the one of the real leakage

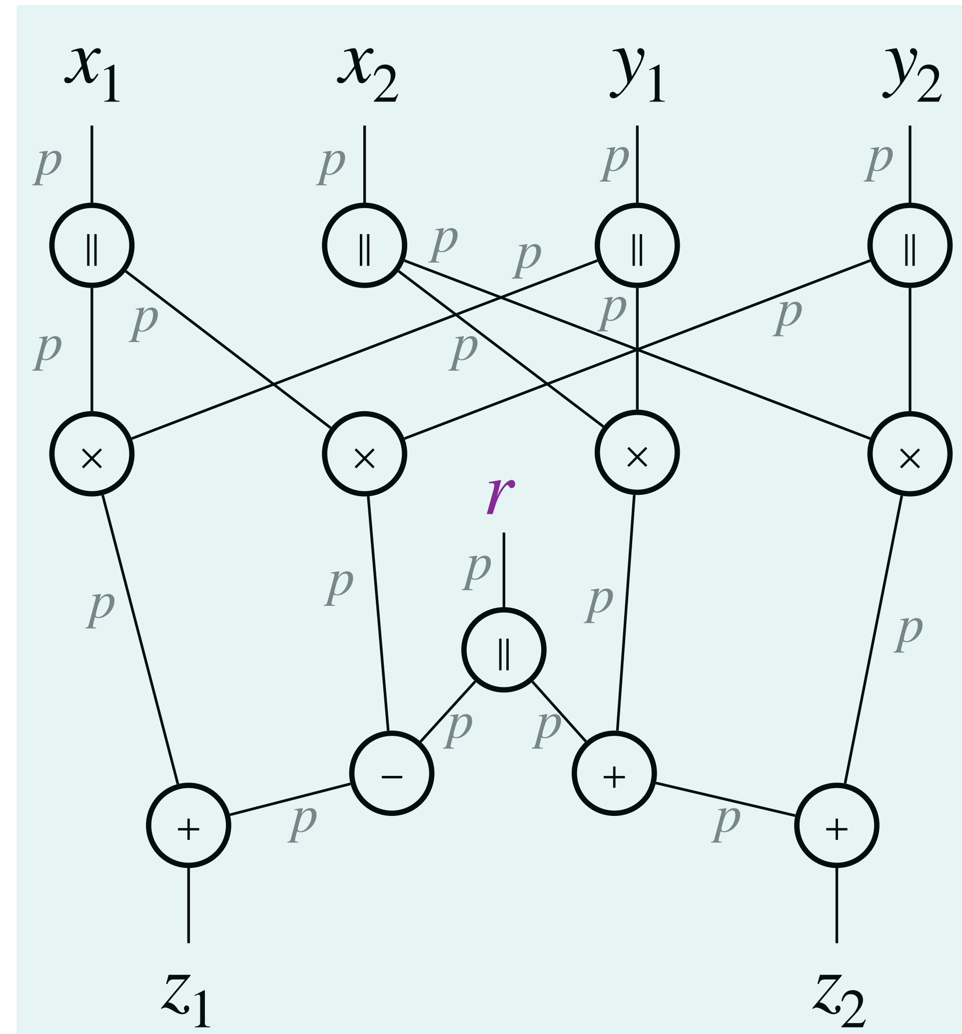
Random Probing Security

Belaïd • Coron • Prouff • Rivain • Taleb

CRYPTO 2020

My Work

$\varepsilon = \mathbb{P}(\text{failure})$



Example

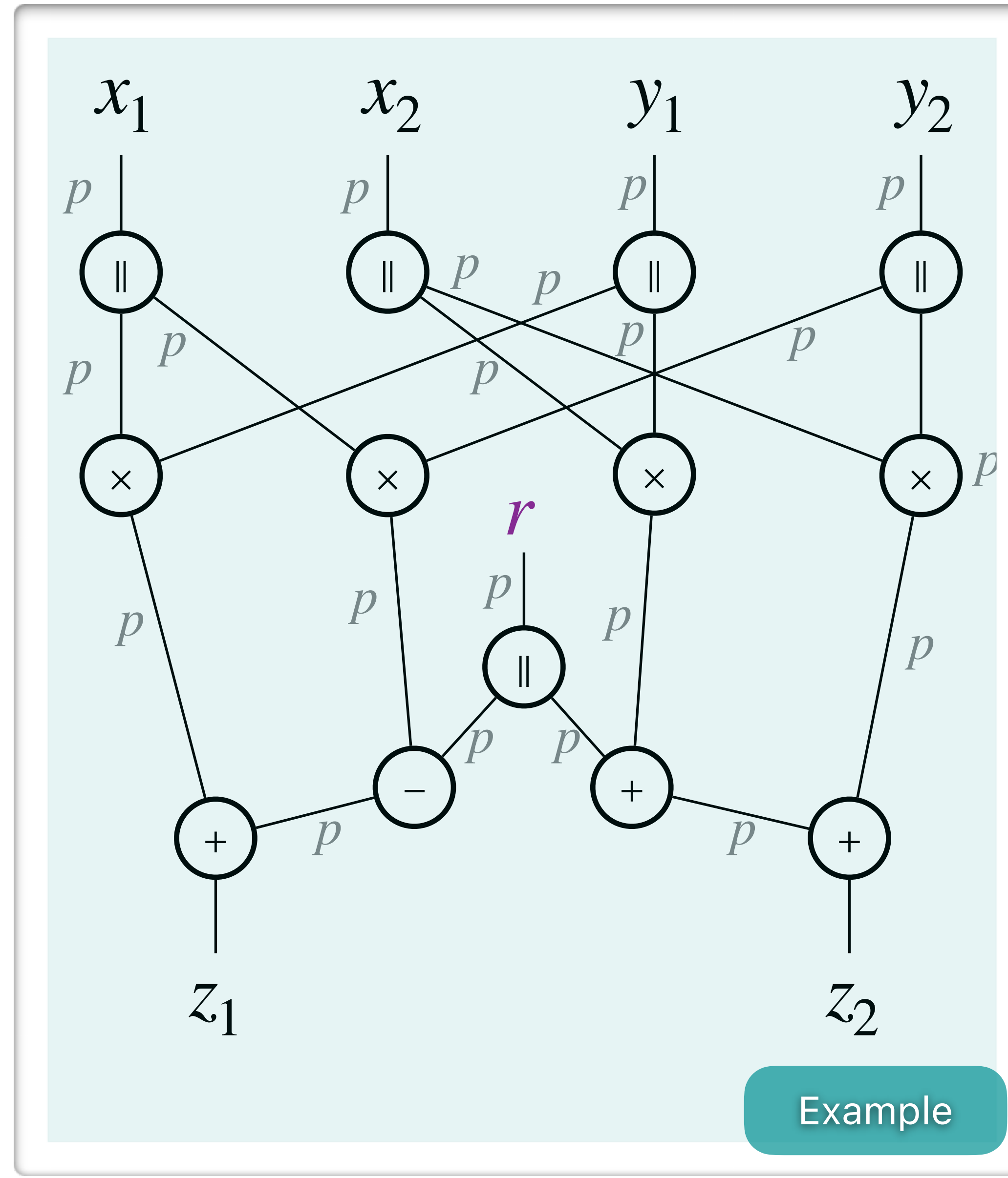
Random Probing Security

Belaïd • Coron • Prouff • Rivain • Taleb

CRYPTO 2020

My Work

$$\varepsilon = \mathbb{P}(\text{failure})$$
$$= \sum_{\mathscr{W} \in [s]} \mathbb{P}(\text{failure} \mid \mathscr{W} \text{ leaks}) \cdot \mathbb{P}(\mathscr{W} \text{ leaks})$$



Random Probing Security

Belaïd • Coron • Prouff •
Rivain • Taleb

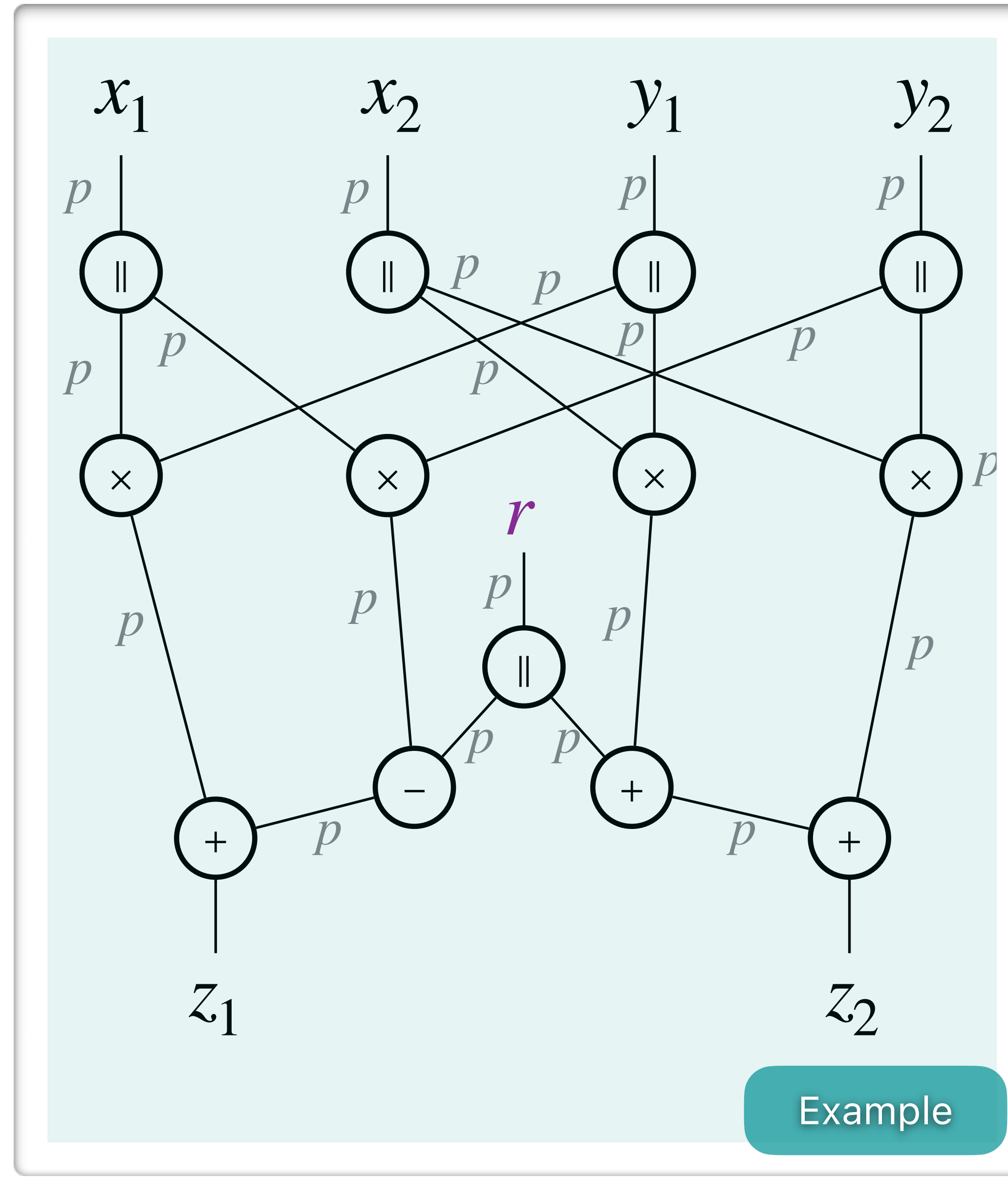
CRYPTO 2020

My Work

$$\varepsilon = \mathbb{P}(\text{failure})$$

$$= \sum_{\mathscr{W} \in [s]} \mathbb{P}(\text{failure} \mid \mathscr{W} \text{ leaks}) \cdot \mathbb{P}(\mathscr{W} \text{ leaks})$$

$$= \sum_{\mathscr{W} \in [s]} \delta_{\mathscr{W}} \cdot p^{|\mathscr{W}|} \cdot (1-p)^{s-|\mathscr{W}|}$$

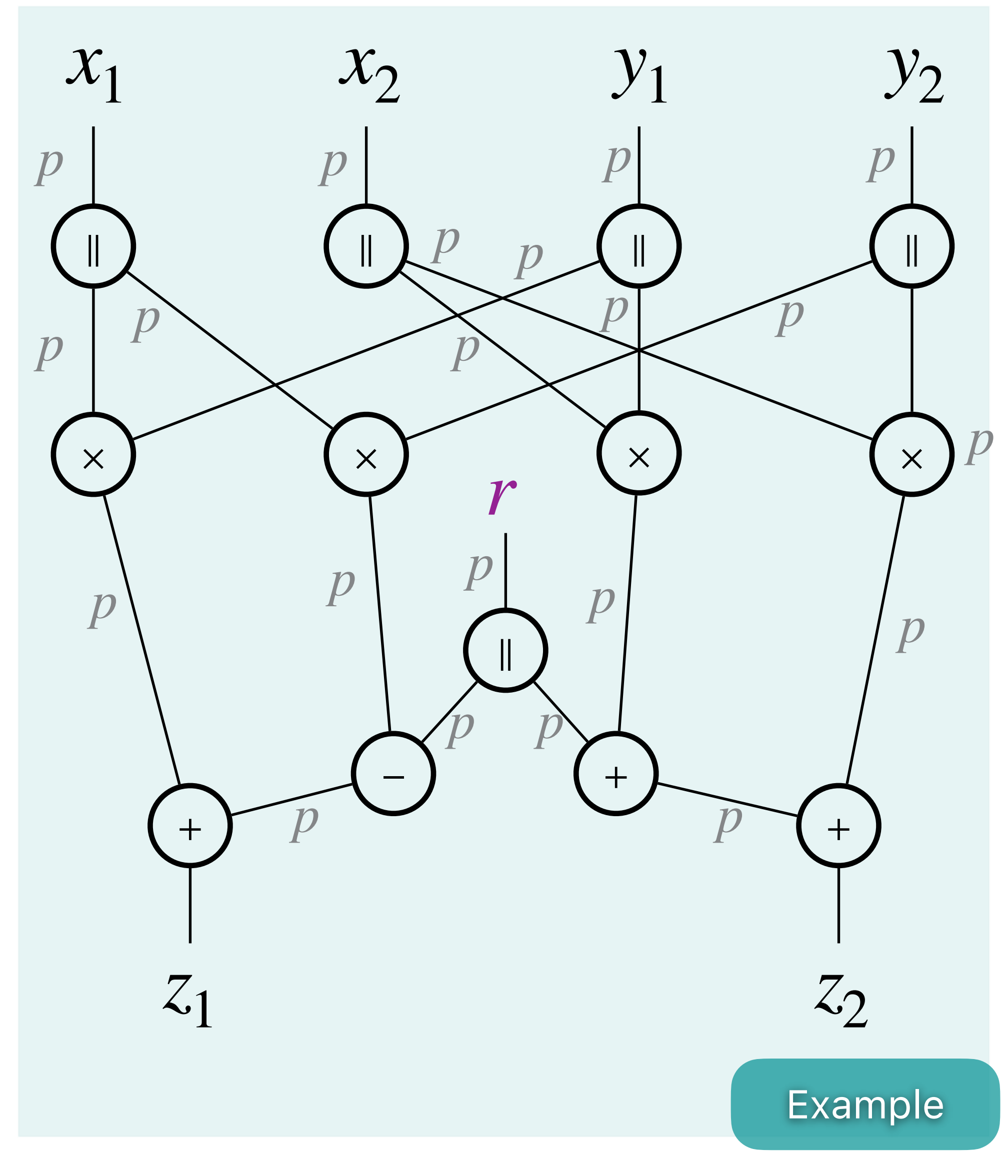


Random Probing Security

Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020
My Work

$$
\begin{aligned}
\varepsilon &= \mathbb{P}(\text{failure}) \\
&= \sum_{\mathcal{W} \in [s]} \mathbb{P}(\text{failure} \mid \mathcal{W} \text{ leaks}) \cdot \mathbb{P}(\mathcal{W} \text{ leaks}) \\
&= \sum_{\mathcal{W} \in [s]} \delta_{\mathcal{W}} \cdot p^{|\mathcal{W}|} \cdot (1-p)^{s-|\mathcal{W}|}
\end{aligned}
$$

$$
\delta_{\mathcal{W}} = \begin{cases} 0 & \text{if } \exists\ \mathrm{Sim}(C, p) \text{ for } \mathcal{W} \\ 1 & \text{otherwise.} \end{cases}
$$

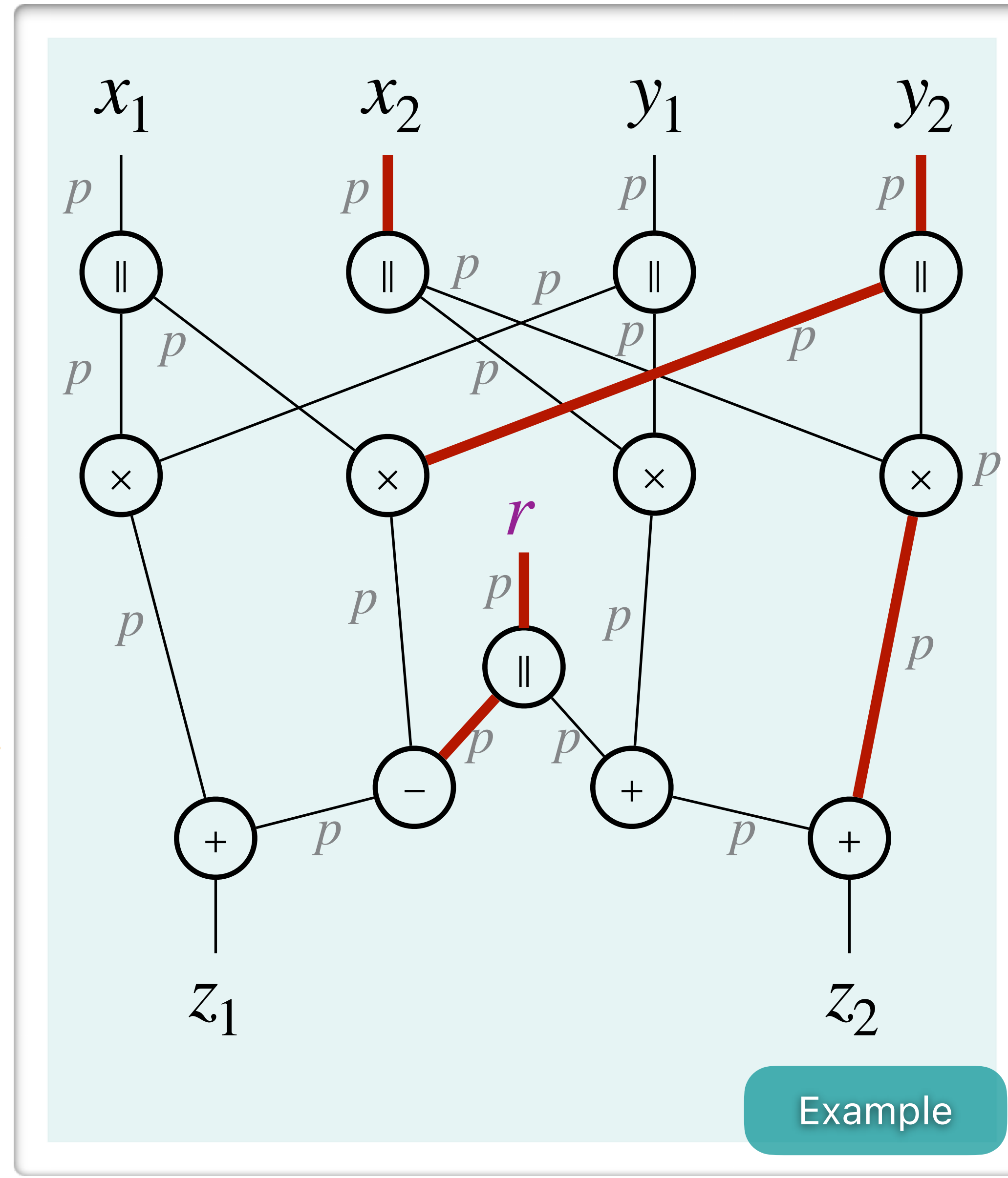


Random Probing Security

Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020
My Work

$$\varepsilon = \mathbb{P}(\text{failure})$$
$$= \sum_{\mathcal{W} \in [s]} \mathbb{P}(\text{failure} \mid \mathcal{W} \text{ leaks}) \cdot \mathbb{P}(\mathcal{W} \text{ leaks})$$
$$= \sum_{\mathcal{W} \in [s]} \delta_{\mathcal{W}} \cdot p^{|\mathcal{W}|} \cdot (1-p)^{s-|\mathcal{W}|}$$

$$\delta_{\mathcal{W}} = \begin{cases} 0 & \text{if } \exists \ \mathrm{Sim}(C,p) \text{ for } \mathcal{W} \\ 1 & \text{otherwise.} \end{cases}$$

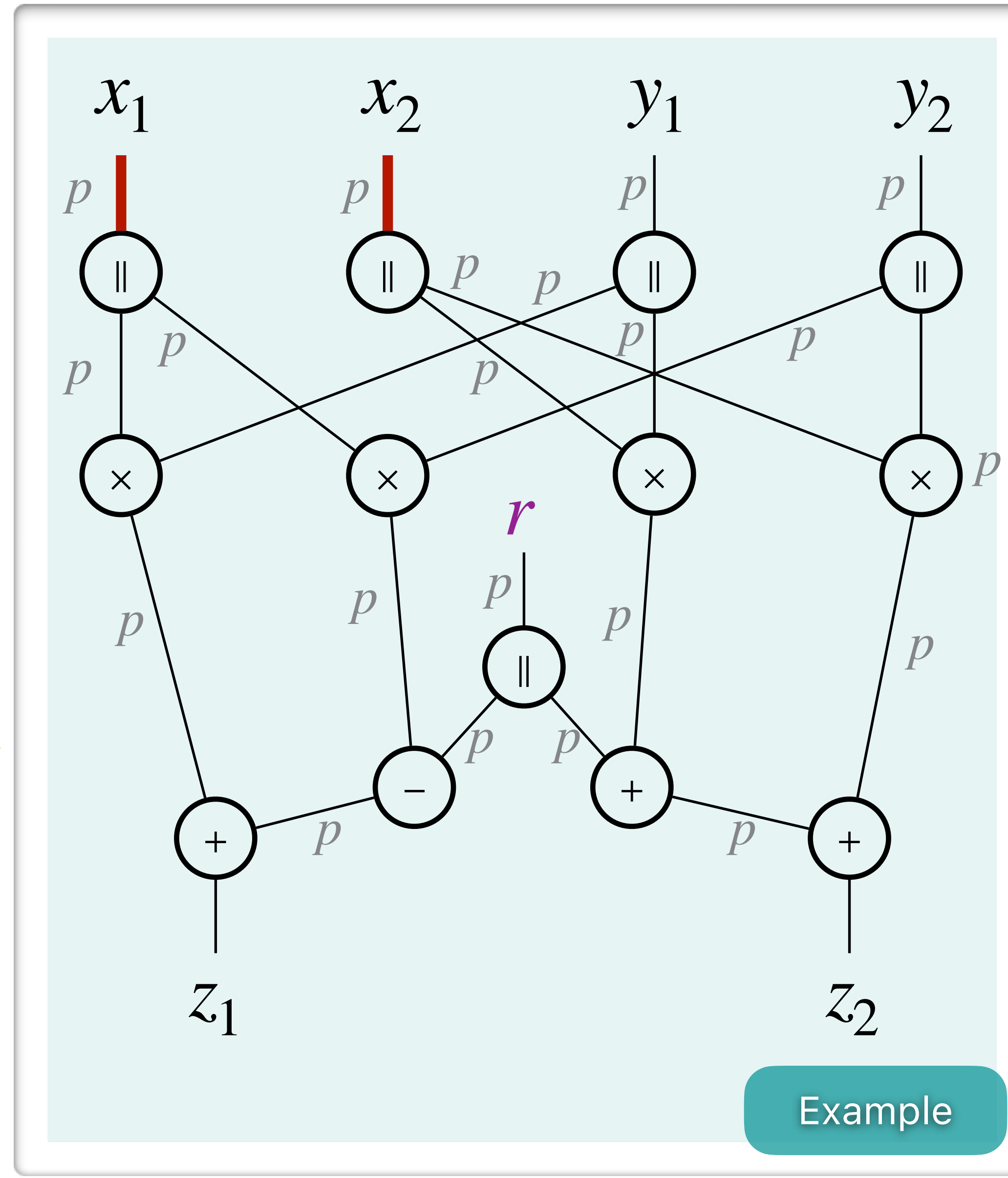


Random Probing Security

Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020
My Work

$$\begin{aligned}\varepsilon &= \mathbb{P}(\text{failure}) \\ &= \sum_{\mathscr{W} \in [s]} \mathbb{P}(\text{failure} \mid \mathscr{W} \text{ leaks}) \cdot \mathbb{P}(\mathscr{W} \text{ leaks}) \\ &= \sum_{\mathscr{W} \in [s]} \delta_{\mathscr{W}} \cdot p^{|\mathscr{W}|} \cdot (1-p)^{s-|\mathscr{W}|}\end{aligned}$$

$$\delta_{\mathscr{W}} = \begin{cases} 0 & \text{if } \exists\ \mathrm{Sim}(C, p) \text{ for } \mathscr{W} \\ 1 & \text{otherwise.} \end{cases}$$



Random Probing Security

Belaïd • Coron • Prouff • Rivain • Taleb

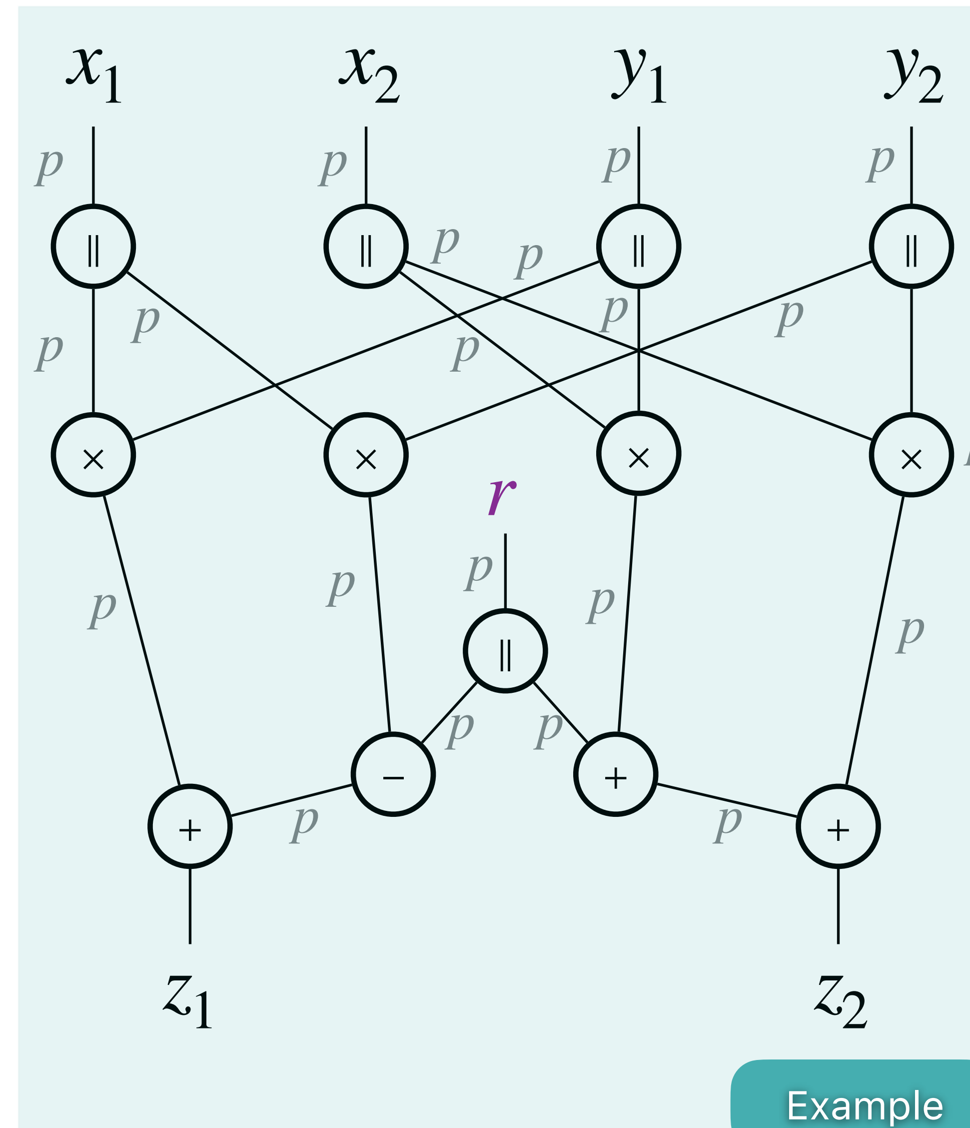
CRYPTO 2020

My Work

$$\varepsilon = \mathbb{P}(\text{failure})$$

$$= \sum_{\mathscr{W} \in [s]} \mathbb{P}(\text{failure} \mid \mathscr{W} \text{ leaks}) \cdot \mathbb{P}(\mathscr{W} \text{ leaks})$$

$$= \sum_{\mathscr{W} \in [s]} \delta_{\mathscr{W}} \cdot p^{|\mathscr{W}|} \cdot (1-p)^{s-|\mathscr{W}|}$$

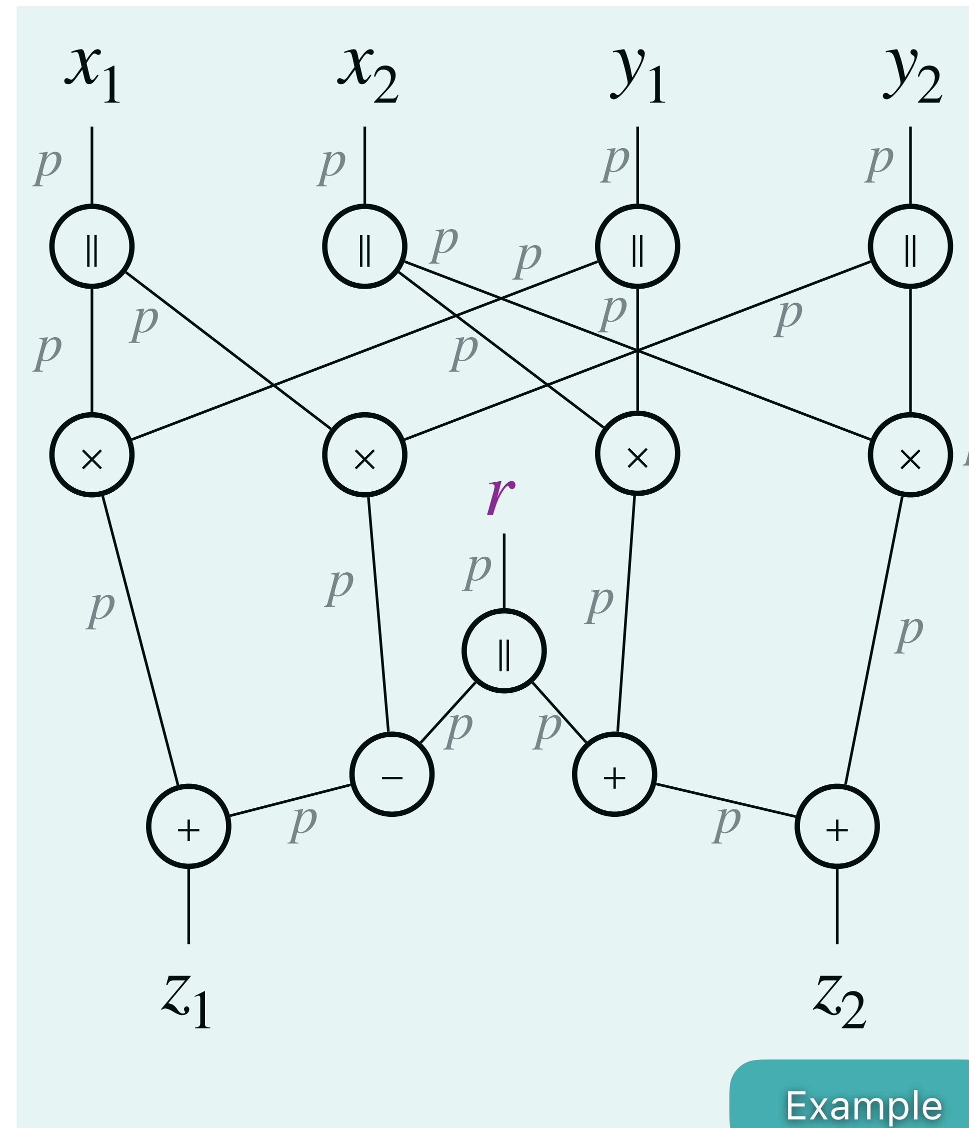


Random Probing Security

Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020
My Work

$$\varepsilon = \mathbb{P}(\text{failure})$$
$$= \sum_{\mathcal{W} \in [s]} \mathbb{P}(\text{failure} \mid \mathcal{W} \text{ leaks}) \cdot \mathbb{P}(\mathcal{W} \text{ leaks})$$
$$= \sum_{\mathcal{W} \in [s]} \delta_{\mathcal{W}} \cdot p^{|\mathcal{W}|} \cdot (1-p)^{s-|\mathcal{W}|}$$
$$= \sum_{i=1}^{s} c_i \cdot p^{i} \cdot (1-p)^{s-i}$$

where $c_i = \sum_{\mathcal{W} \subseteq [s], |\mathcal{W}| = i} \delta_{\mathcal{W}}$

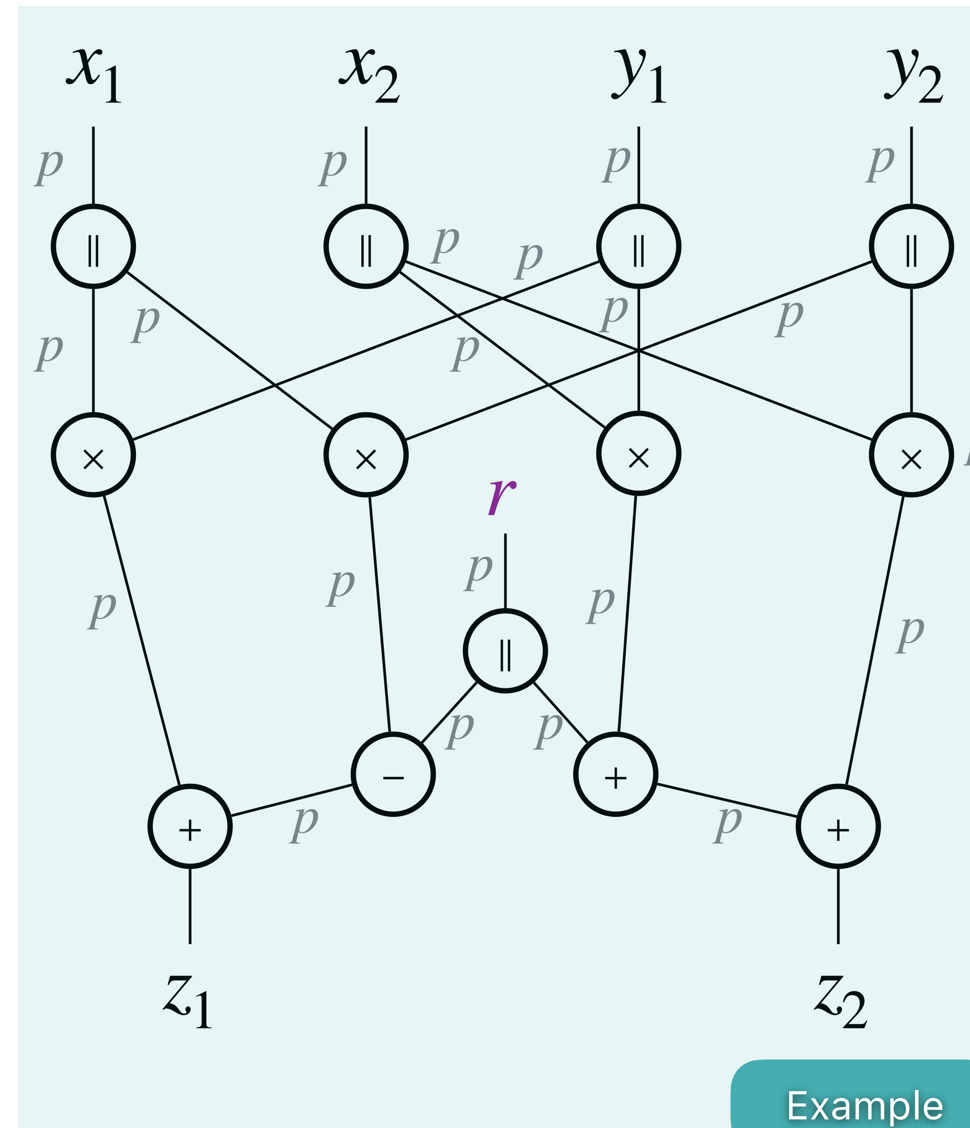


Random Probing Security

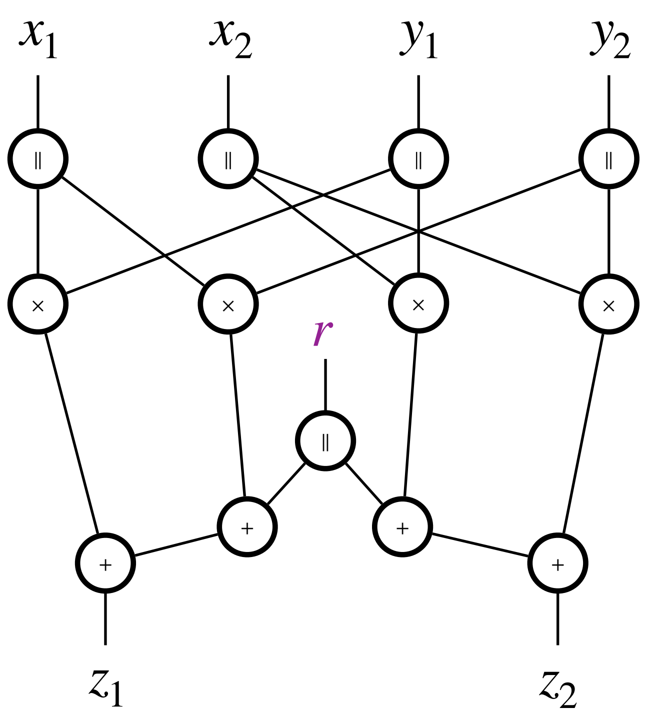
Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020
My Work

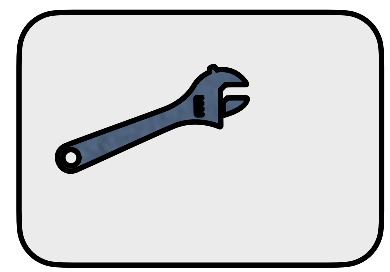
$$\varepsilon = \mathbb{P}(\text{failure})$$
$$= \sum_{\mathcal{W} \in [s]} \mathbb{P}(\text{failure} \mid \mathcal{W} \text{ leaks}) \cdot \mathbb{P}(\mathcal{W} \text{ leaks})$$
$$= \sum_{\mathcal{W} \in [s]} \delta_{\mathcal{W}} \cdot p^{|\mathcal{W}|} \cdot (1-p)^{s-|\mathcal{W}|}$$
$$= \sum_{i=1}^{s} c_i \, p^i \cdot (1-p)^{s-i}$$

where $c_i = \sum_{\mathcal{W} \subseteq [s], |\mathcal{W}| = i} \delta_{\mathcal{W}}$



Verification Tools





$(c_1, c_2, \ldots, c_s)$

$$\varepsilon = \sum_{i=1}^{s} c_i \cdot p^i \cdot (1-p)^{s-i}$$

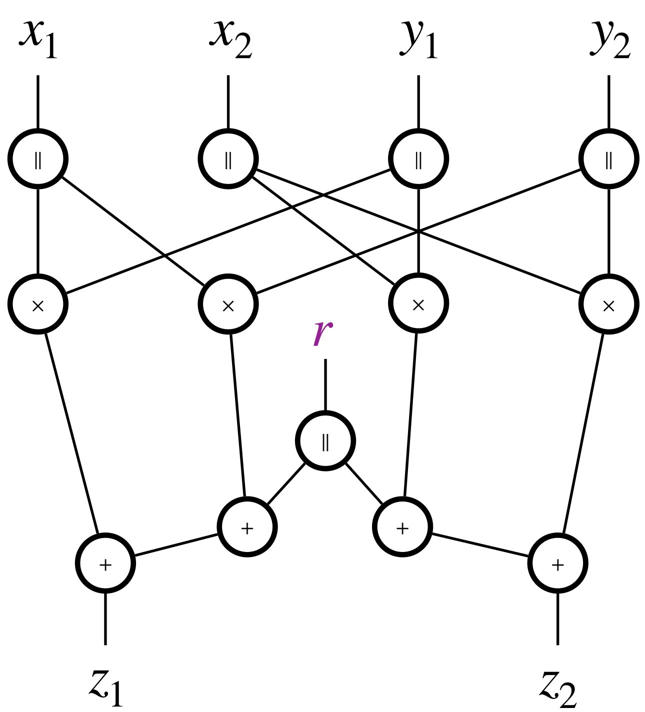
2020

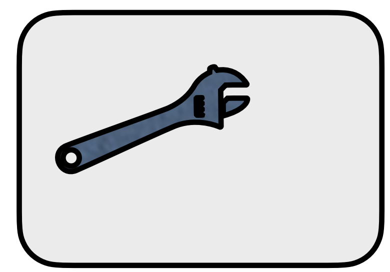
Belaïd • Coron • Prouff •
Rivain • Taleb

CRYPTO 2020 - VRAPS

My Work

Verification Tools





$(c_1, c_2, \ldots, c_s)$

$$\varepsilon = \sum_{i=1}^{s} c_i \cdot p^i \cdot (1-p)^{s-i}$$

2020 2021

Belaïd • Coron • Prouff • Rivain • Taleb

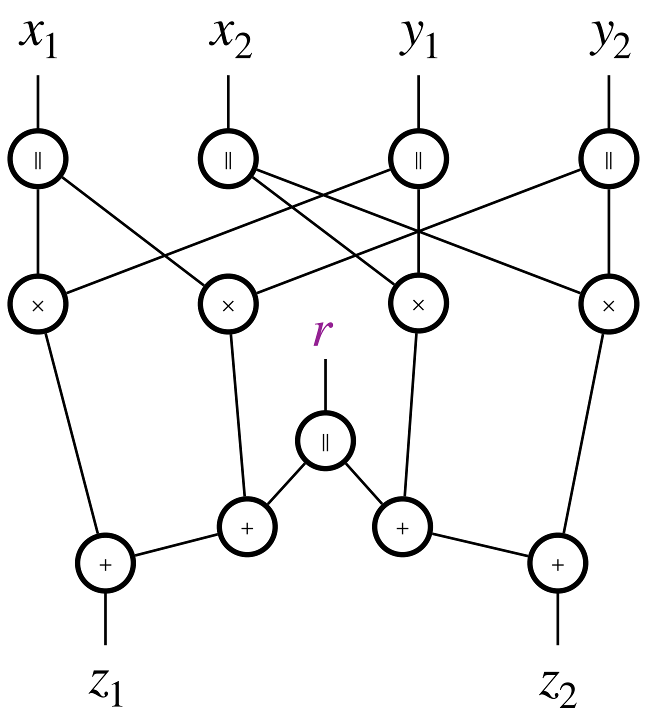
CRYPTO 2020 - VRAPS

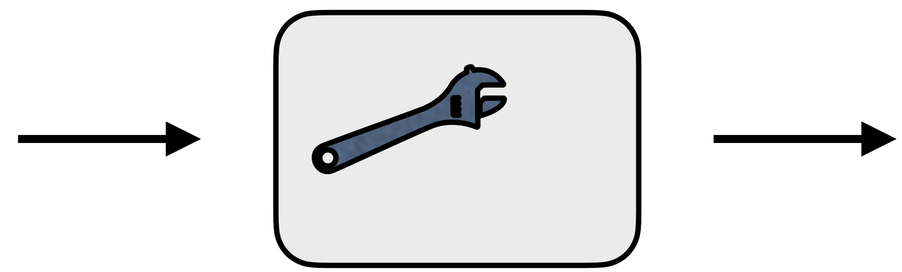
My Work

Cassiers • Faust • Orlt • Standaert

CRYPTO 2021 - STRAPS

Verification Tools





$(c_1, c_2, \ldots, c_s)$

$$\varepsilon = \sum_{i=1}^{s} c_i \cdot p^i \cdot (1-p)^{s-i}$$

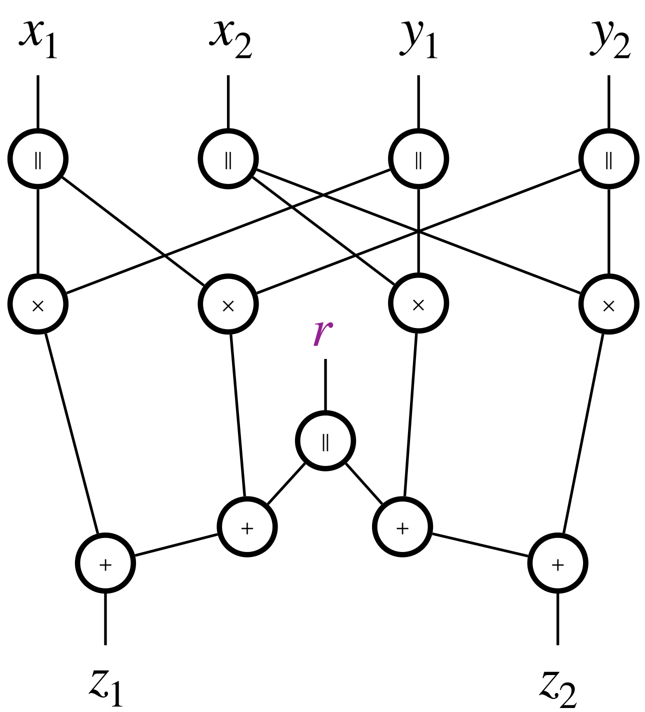
2020 2021 2022

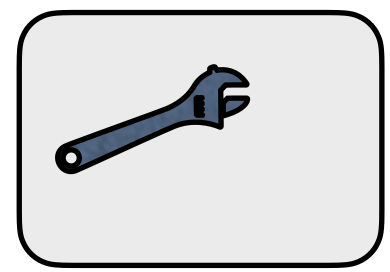
Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020 - VRAPS
My Work

Cassiers • Faust • Orlt • Standaert
CRYPTO 2021 - STRAPS

Belaïd • Mercadier • Rivain • Taleb
S&P 2022 - IronMask
My Work

Verification Tools





$(c_1, c_2, \ldots, c_s)$

$$\varepsilon = \sum_{i=1}^{s} c_i \cdot p^i \cdot (1-p)^{s-i}$$

2020 2021 2022 2024

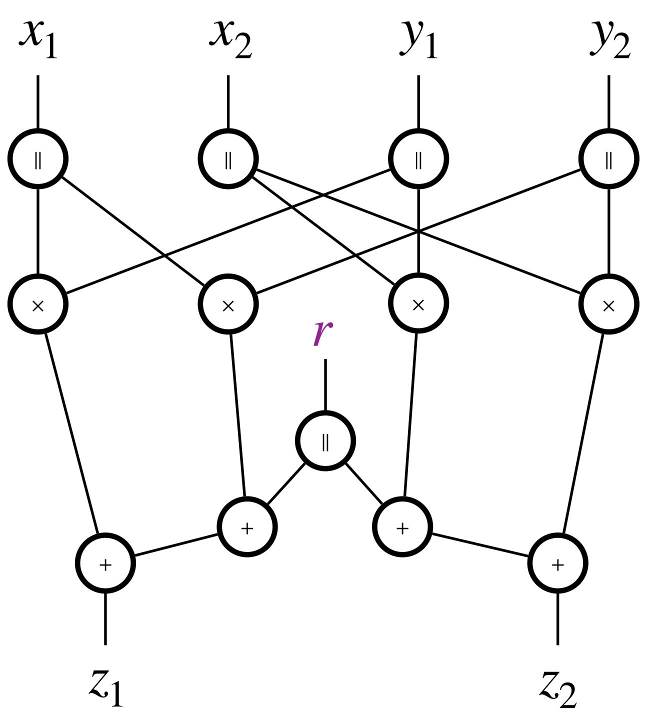
Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020 - VRAPS
My Work

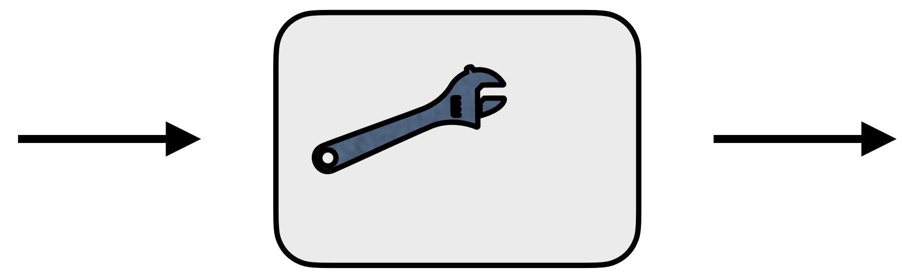
Cassiers • Faust • Orlt • Standaert
CRYPTO 2021 - STRAPS

Belaïd • Mercadier • Rivain • Taleb
S&P 2022 - IronMask
My Work

Belaïd • Feldtkeller • Güneysu • Guinet • Richter-Brockmann • Rivain • Sasdrich • Taleb
ASIACRYPT 2024 - IronMask+
My Work

Verification Tools





$(c_1, c_2, \ldots, c_s)$

$$\varepsilon = \sum_{i=1}^{s} c_i \cdot p^i \cdot (1-p)^{s-i}$$

2020 2021 2022 2024 2025

Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020 - VRAPS
My Work

Cassiers • Faust • Orlt • Standaert
CRYPTO 2021 - STRAPS

Belaïd • Mercadier • Rivain • Taleb
S&P 2022 - IronMask
My Work

Belaïd • Feldtkeller • Güneysu • Guinet • Richter-Brockmann • Rivain • Sasdrich • Taleb
ASIACRYPT 2024 - IronMask+
My Work

Beierle • Feldtkeller • Guinet • Güneysu • Leander • Richter-Brockmann • Sasdrich
EUROCRYPT 2025 - INDIANA

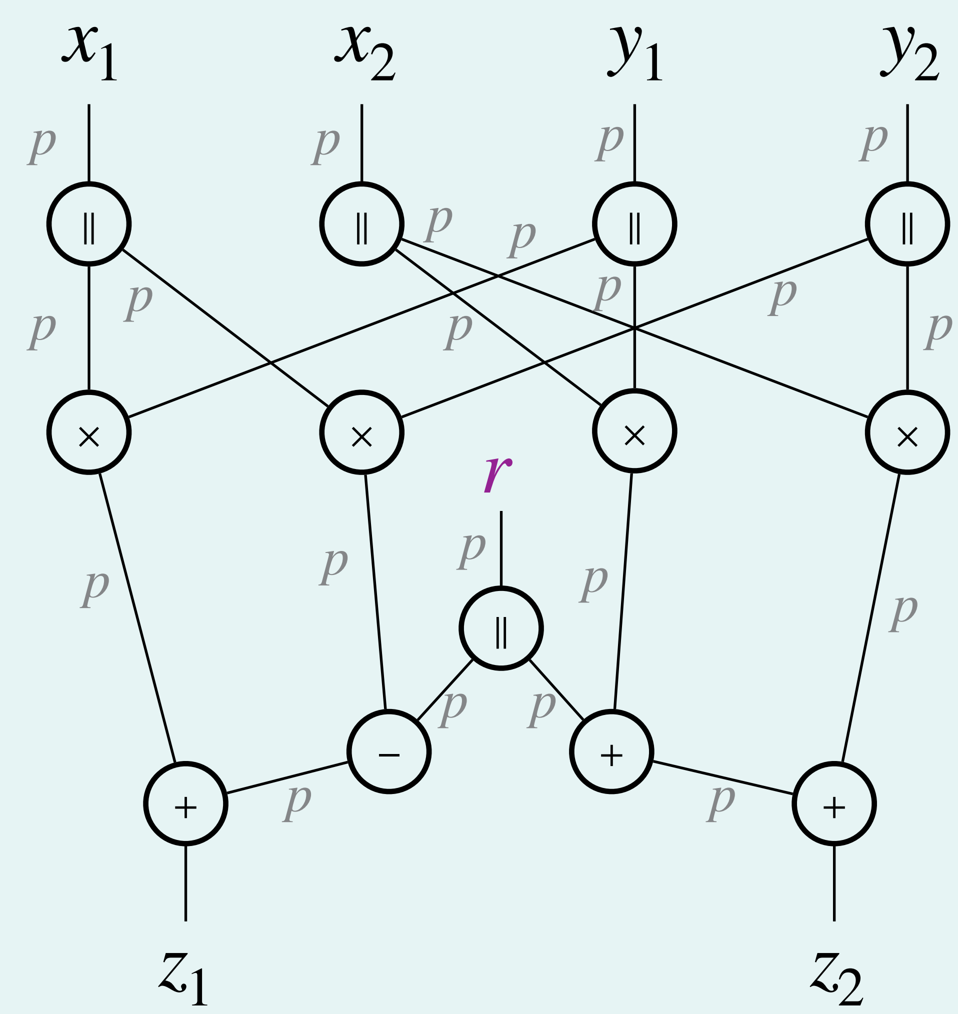
Verification of Small Circuits

$$\varepsilon = \sum_{i=1}^{s} c_i \cdot p^i \cdot (1-p)^{s-i}$$

with $s = 21$

2^{21} tuples to consider

⌛ $\leq$ 3 ms



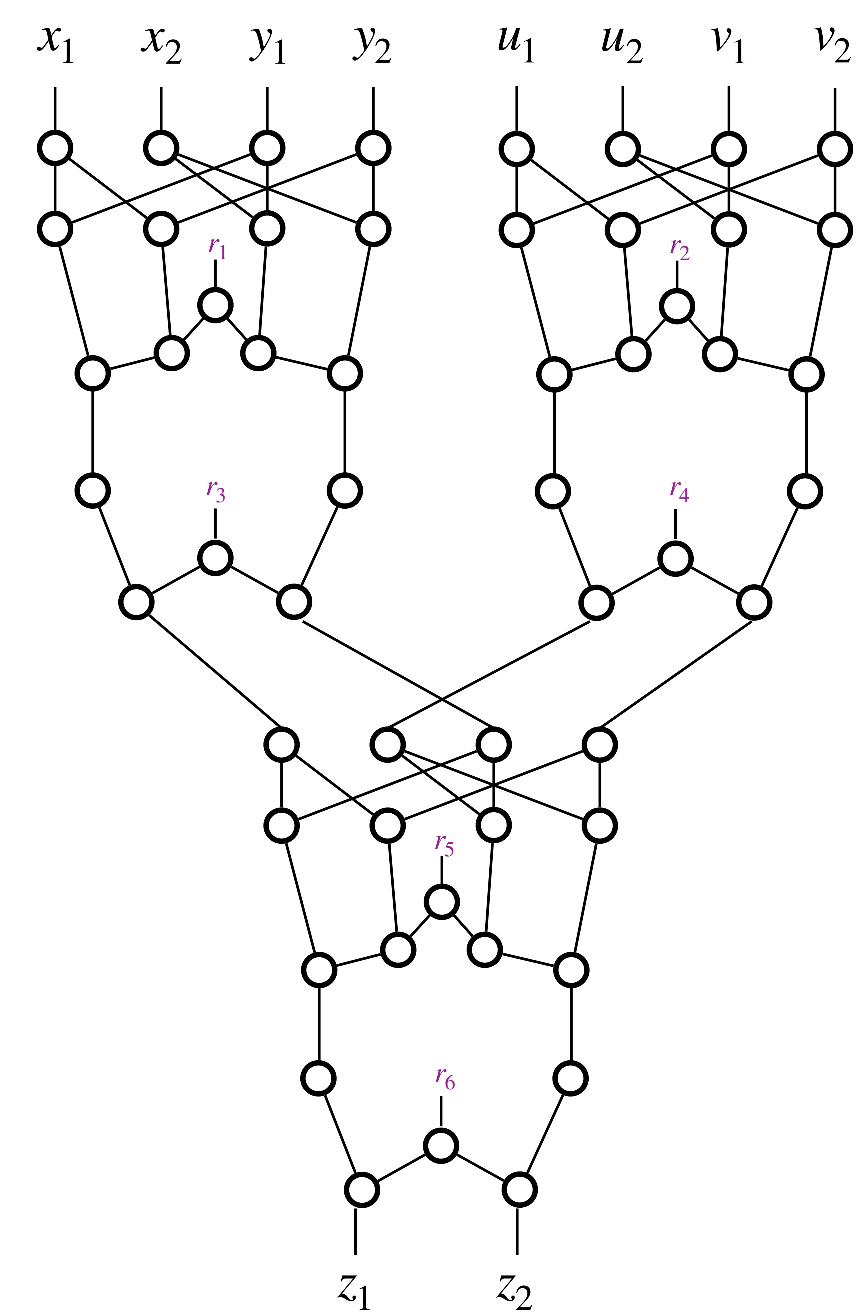
$(c_1, \cdots, c_{21}) =$
$(0,49,737,4763,18735,52798,$
$115338,203064,293800,352692,$
$352714,293930,203490,116280,$
$54264,20349,5985,1330,210,21,1)$

Example

Verification of Larger Circuits

$$\varepsilon = \sum_{i=1}^{s} c_i \cdot p^i \cdot (1-p)^{s-i}$$

⌛ impractical



Contributions

Foundations

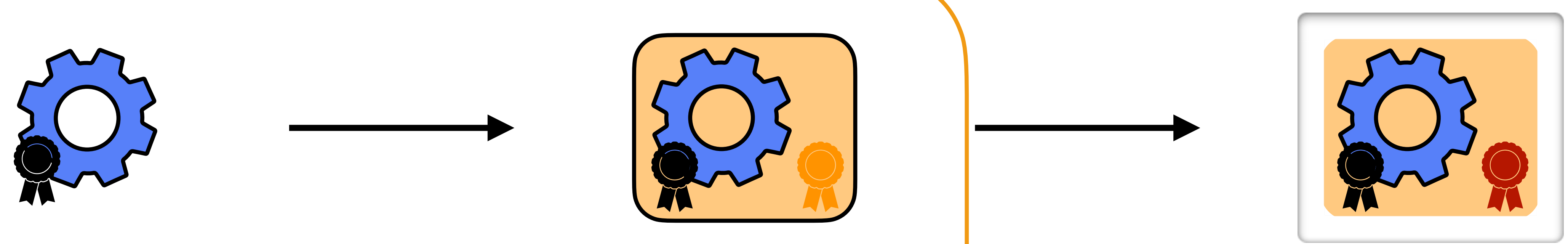
Random probing security & verification (small circuits)

Scaling up

Composition frameworks (larger circuits)

Building blocks

Design of efficient gadgets



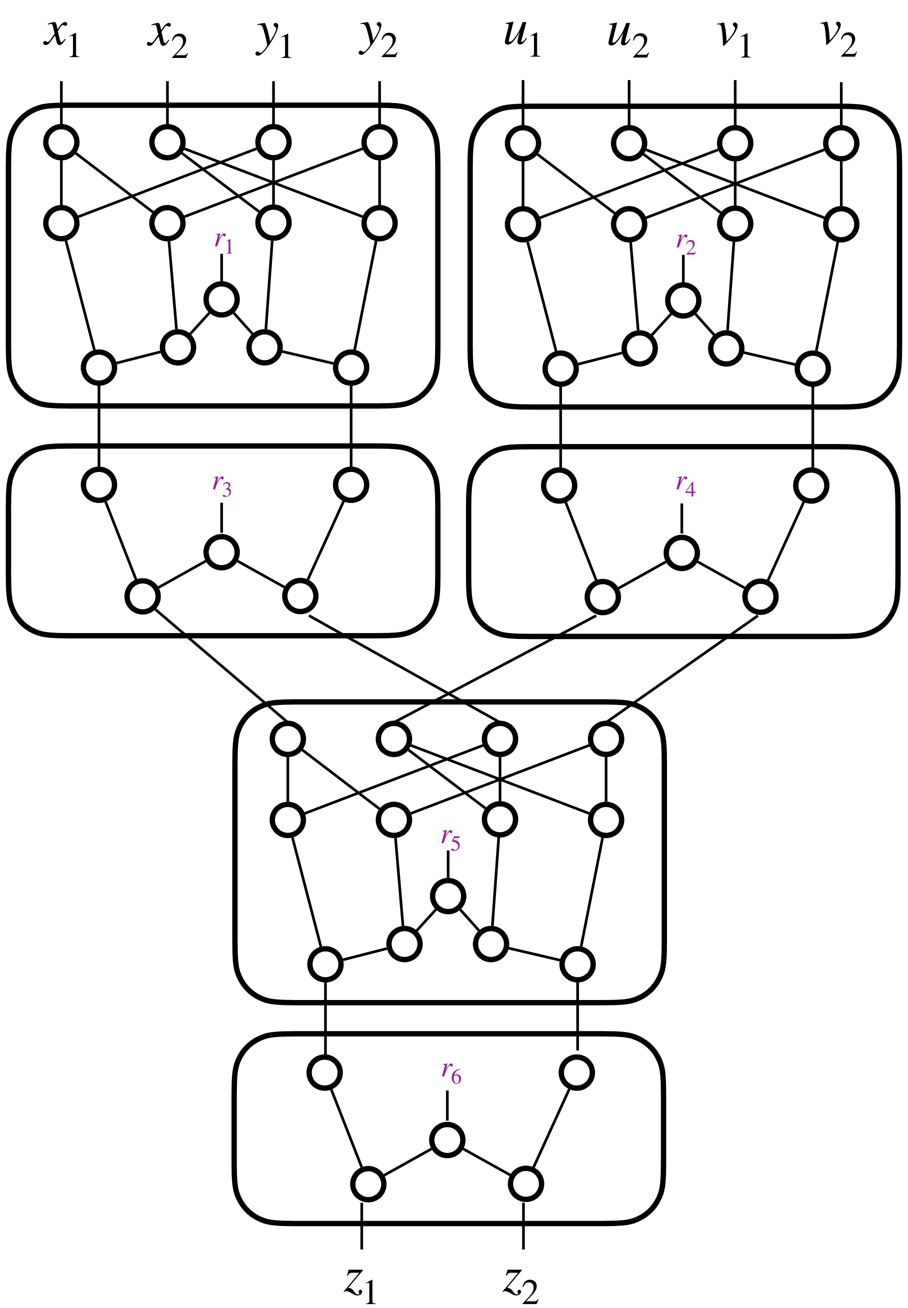
Black-box secure

Black-box and random probing secure

Black-box and physically secure

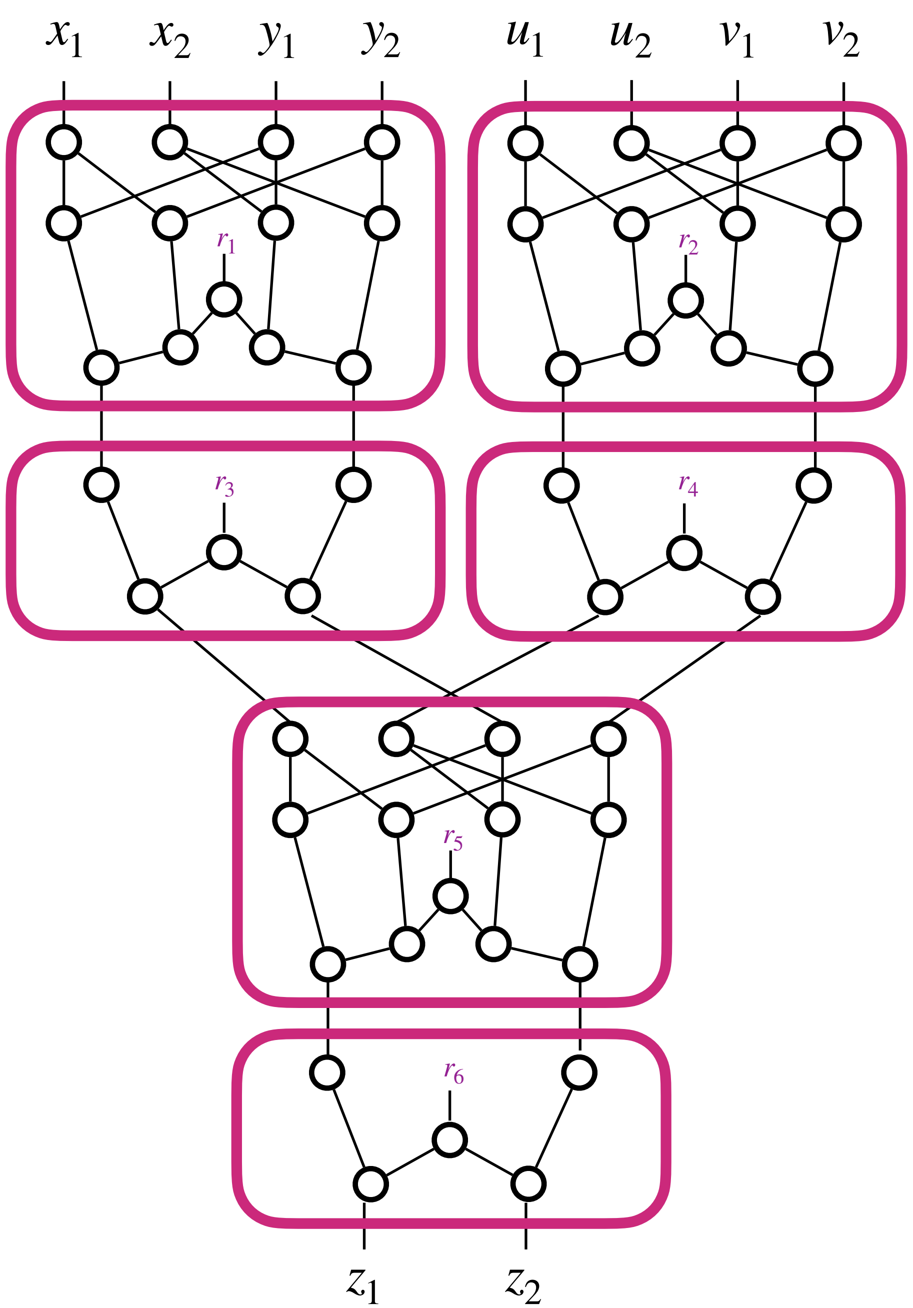
Composition

$$\varepsilon = \sum_{i=1}^{s} c_i \cdot p^i \cdot (1-p)^{s-i}$$



Composition

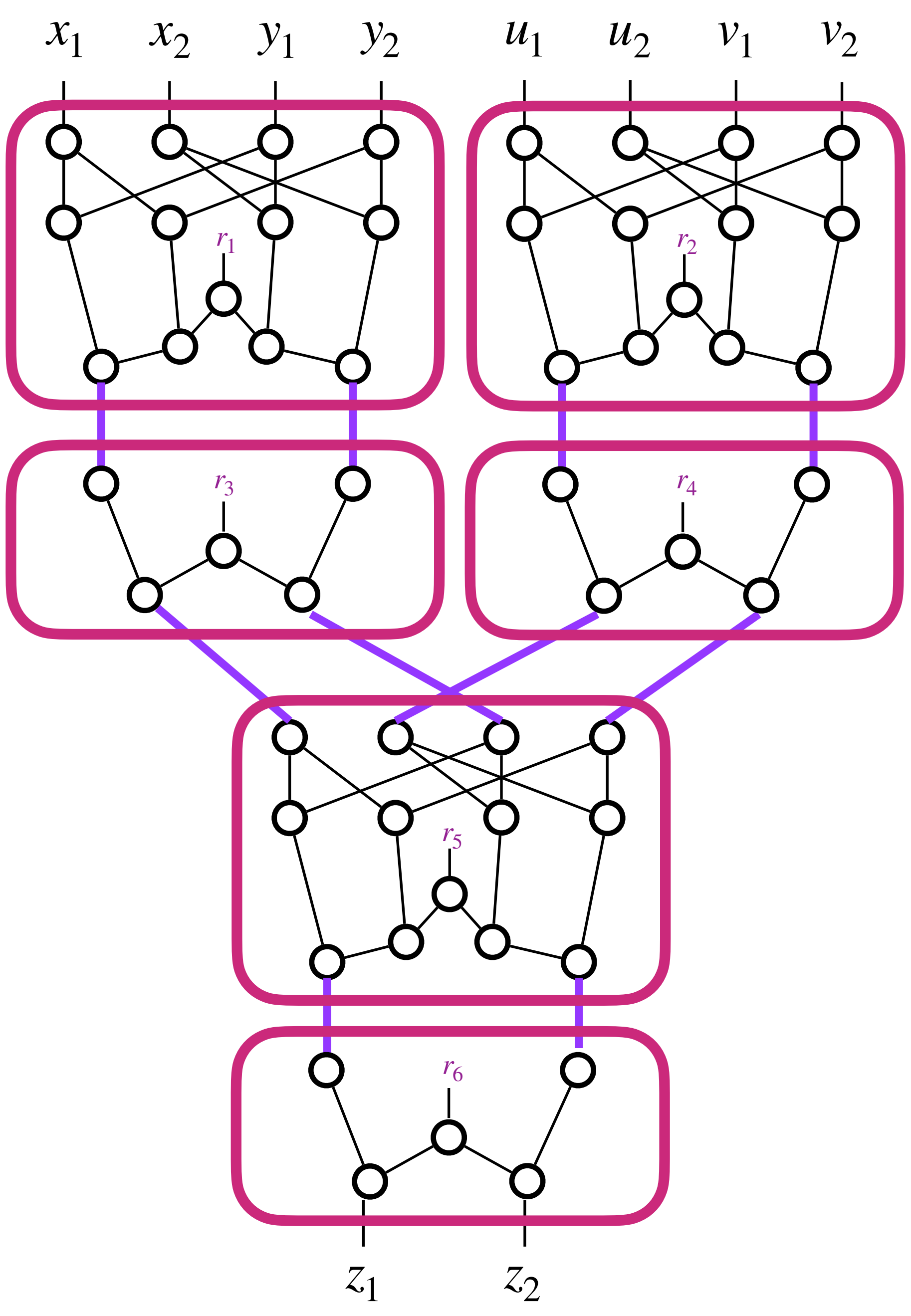
$$\varepsilon = \sum_{i=1}^{s} c_i \cdot p^i \cdot (1-p)^{s-i}$$



Local property

Composition

$$\varepsilon = \sum_{i=1}^{s} c_i \cdot p^i \cdot (1-p)^{s-i}$$

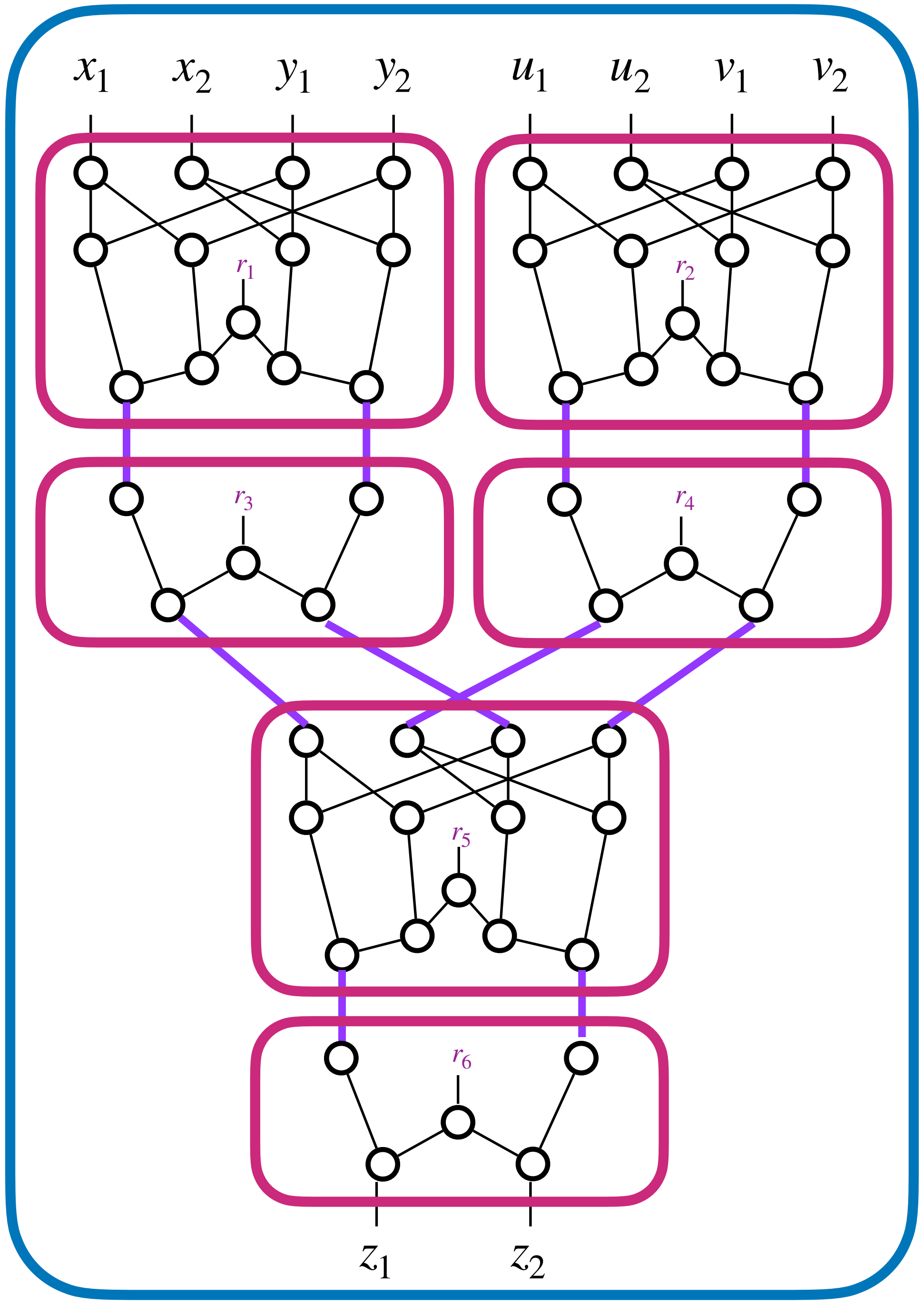


Local property

Composition

$$\varepsilon = \sum_{i=1}^{s} c_i \cdot p^i \cdot (1-p)^{s-i}$$

Global property



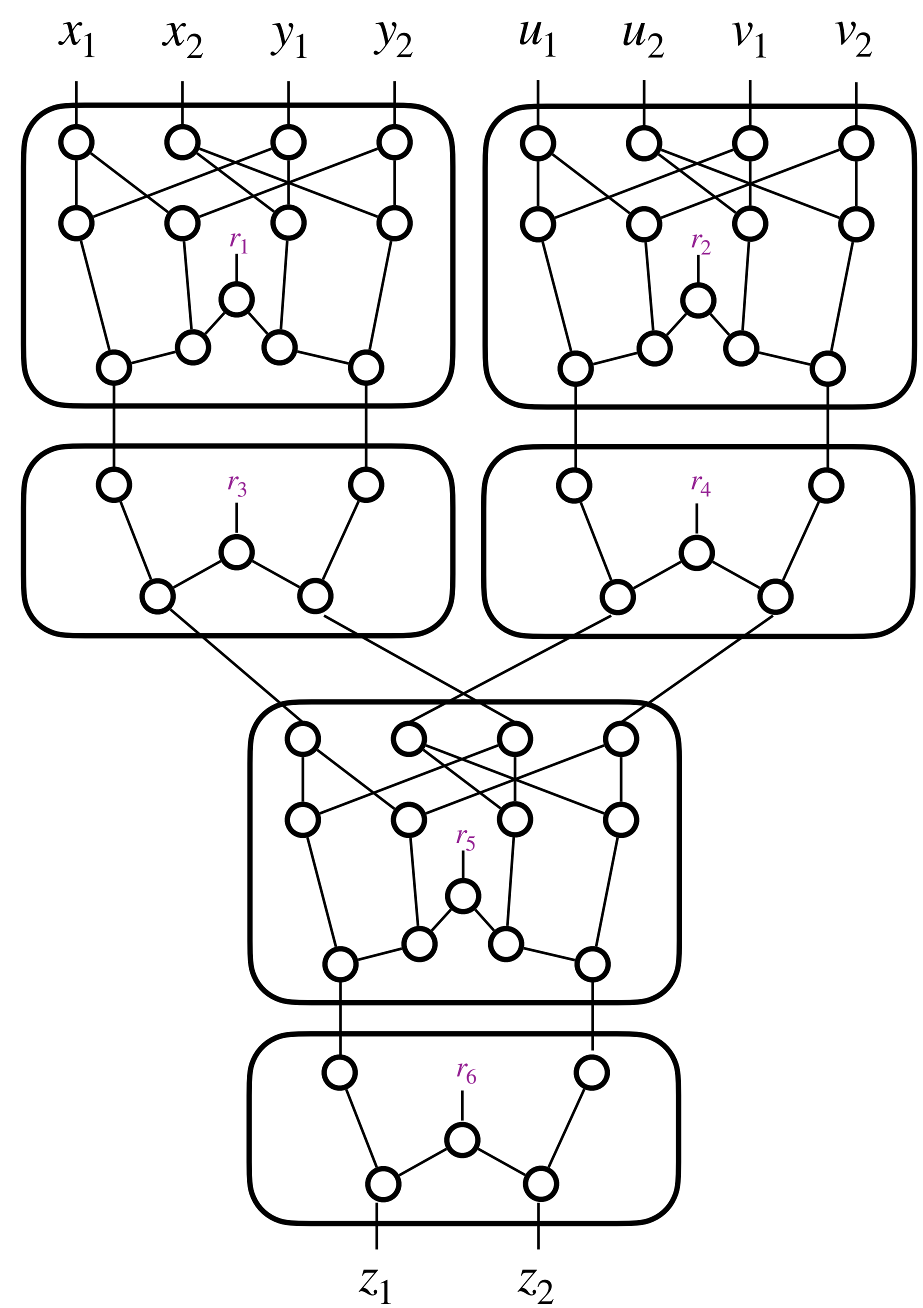
Local property

Composition

Ananth • Ishai • Sahai

CRYPTO 2018

MPC-based construction with explicit and constant leakage rate



Composition

Ananth • Ishai • Sahai

CRYPTO 2018

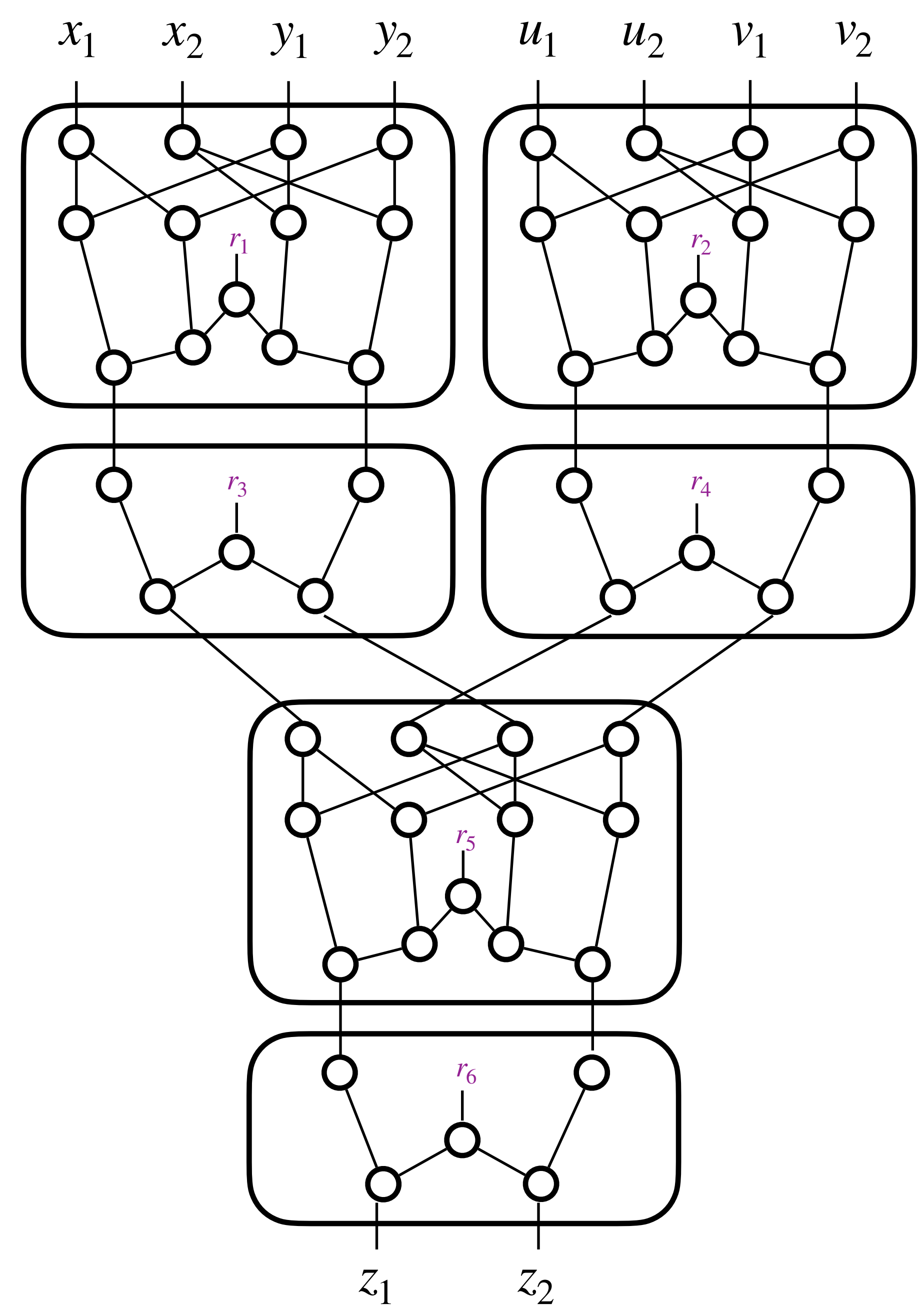
MPC-based construction with explicit and constant leakage rate

Belaïd • Coron • Prouff • Rivain • Taleb

CRYPTO 2020

Threshold RPC

My Work

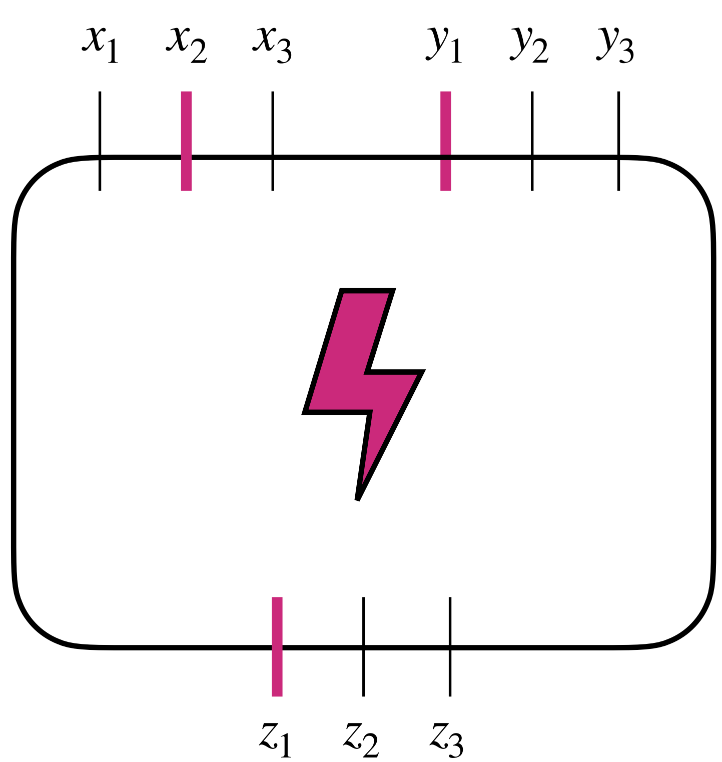


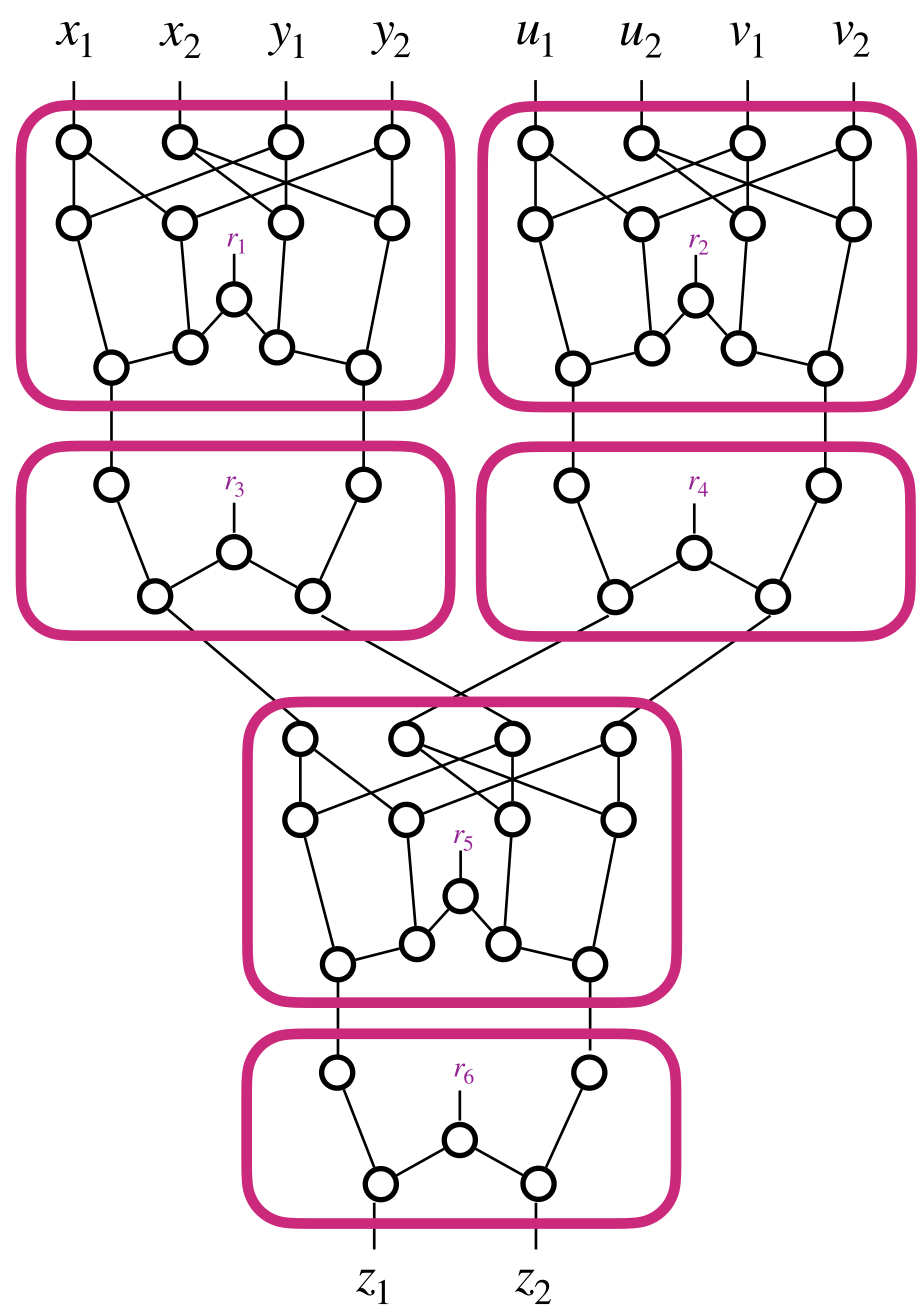
Threshold RPC

Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020
My Work

(p, t, ε)-threshold RPC:

Leakage and any t output shares can be perfectly simulated with at most t shares of each input, except with probability ε





Threshold RPC

Threshold RPC

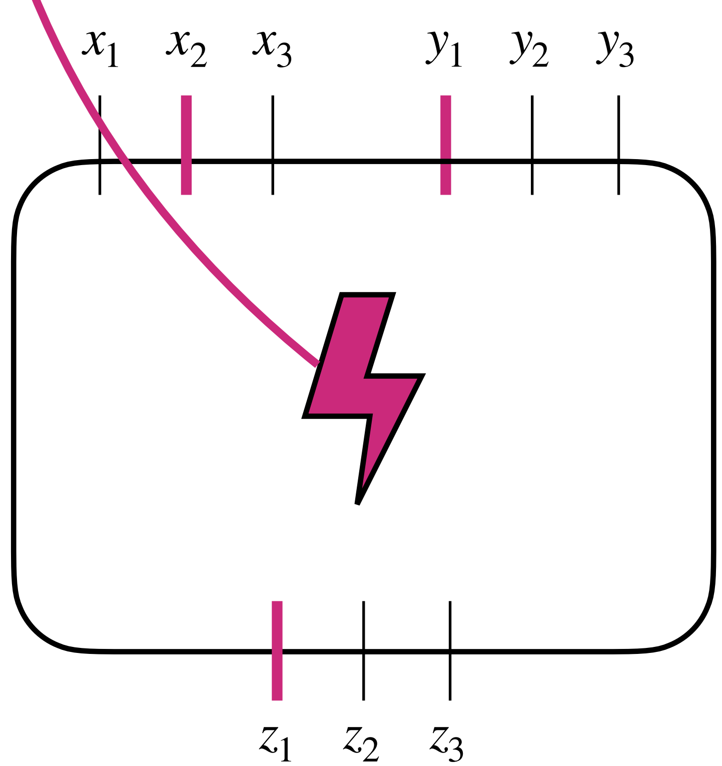
Belaïd • Coron • Prouff •
Rivain • Taleb

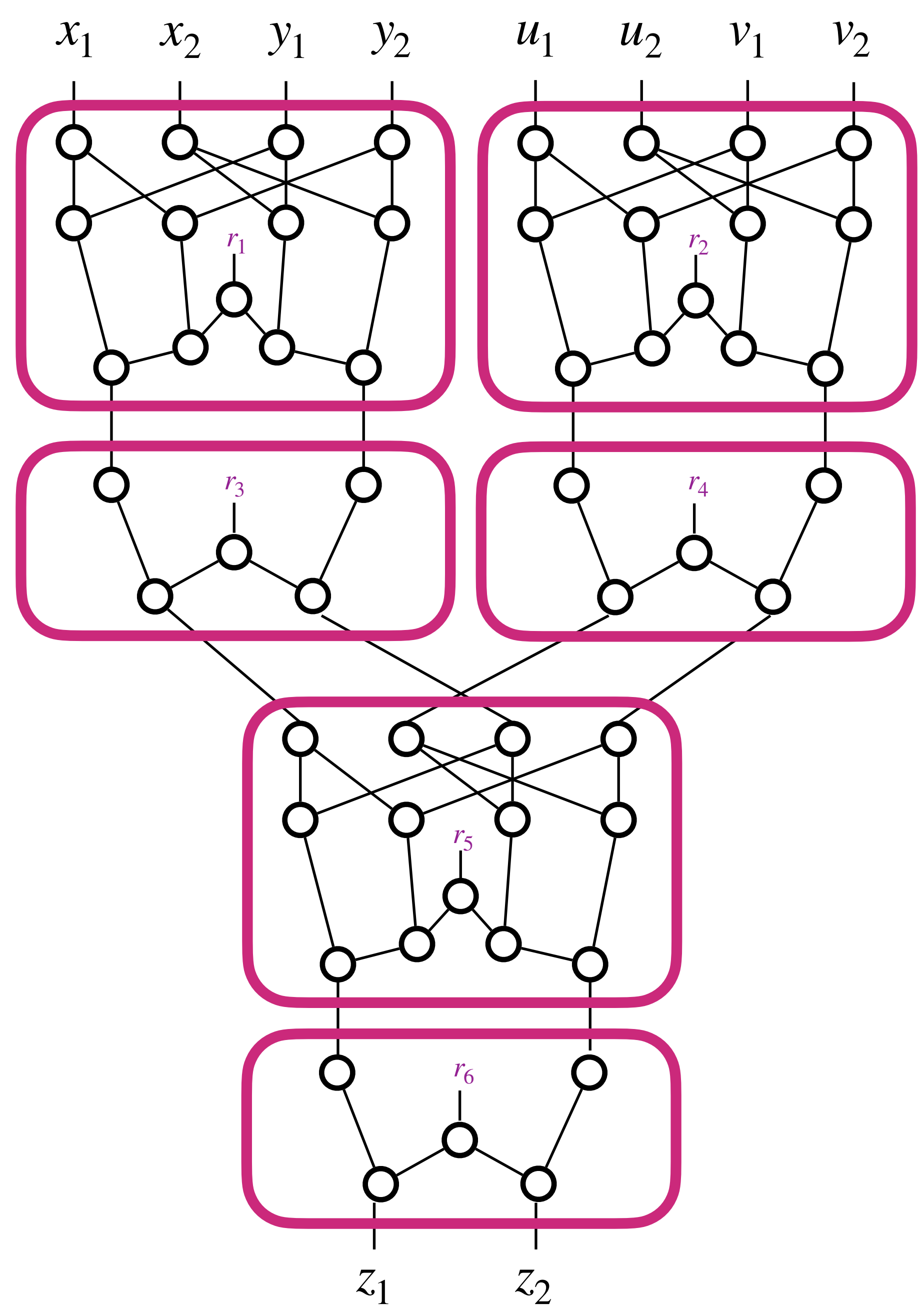
CRYPTO 2020

My Work

(p, t, ε)-threshold RPC:

Leakage and any t output shares can be perfectly simulated with at most t shares of each input, except with probability ε





Threshold RPC

Threshold RPC

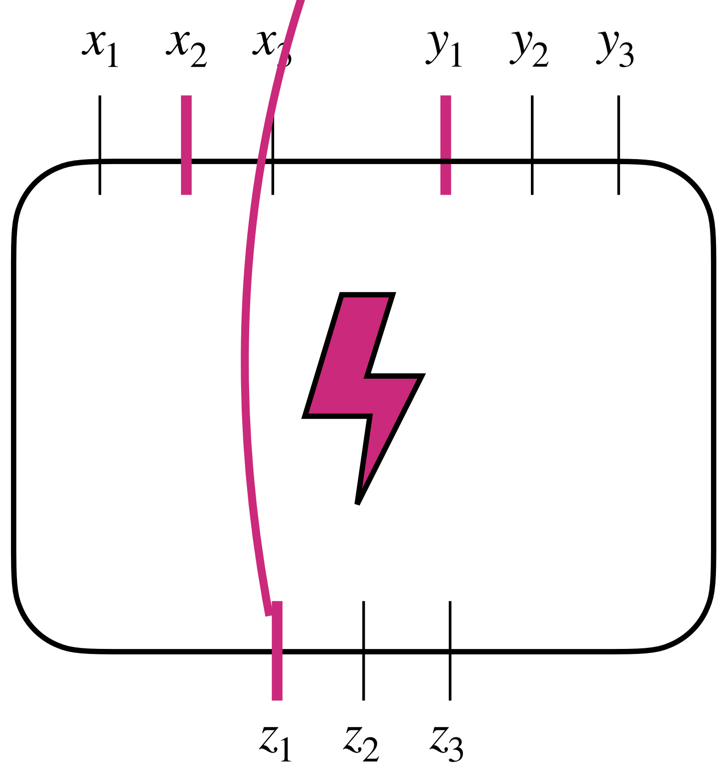
Belaïd • Coron • Prouff • Rivain • Taleb

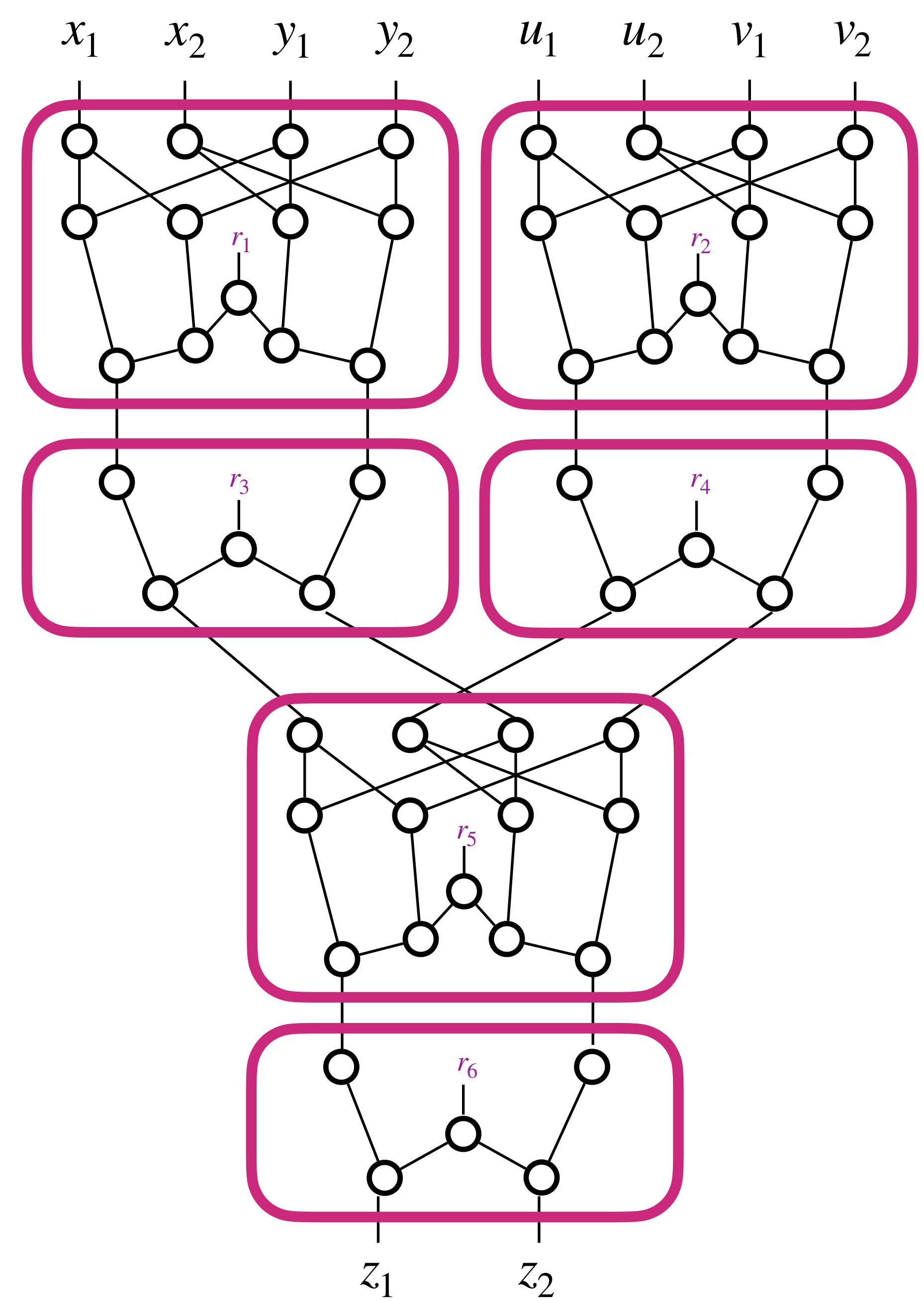
CRYPTO 2020

My Work

(p, t, ε)-threshold RPC:

Leakage and any t output shares can be perfectly simulated with at most t shares of each input, except with probability ε





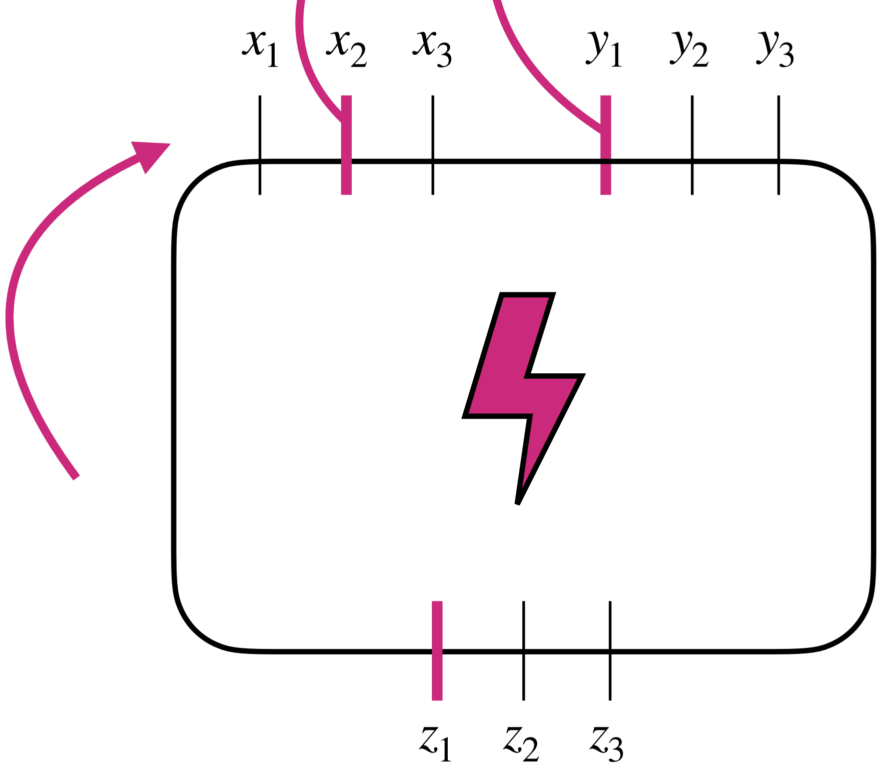
Threshold RPC

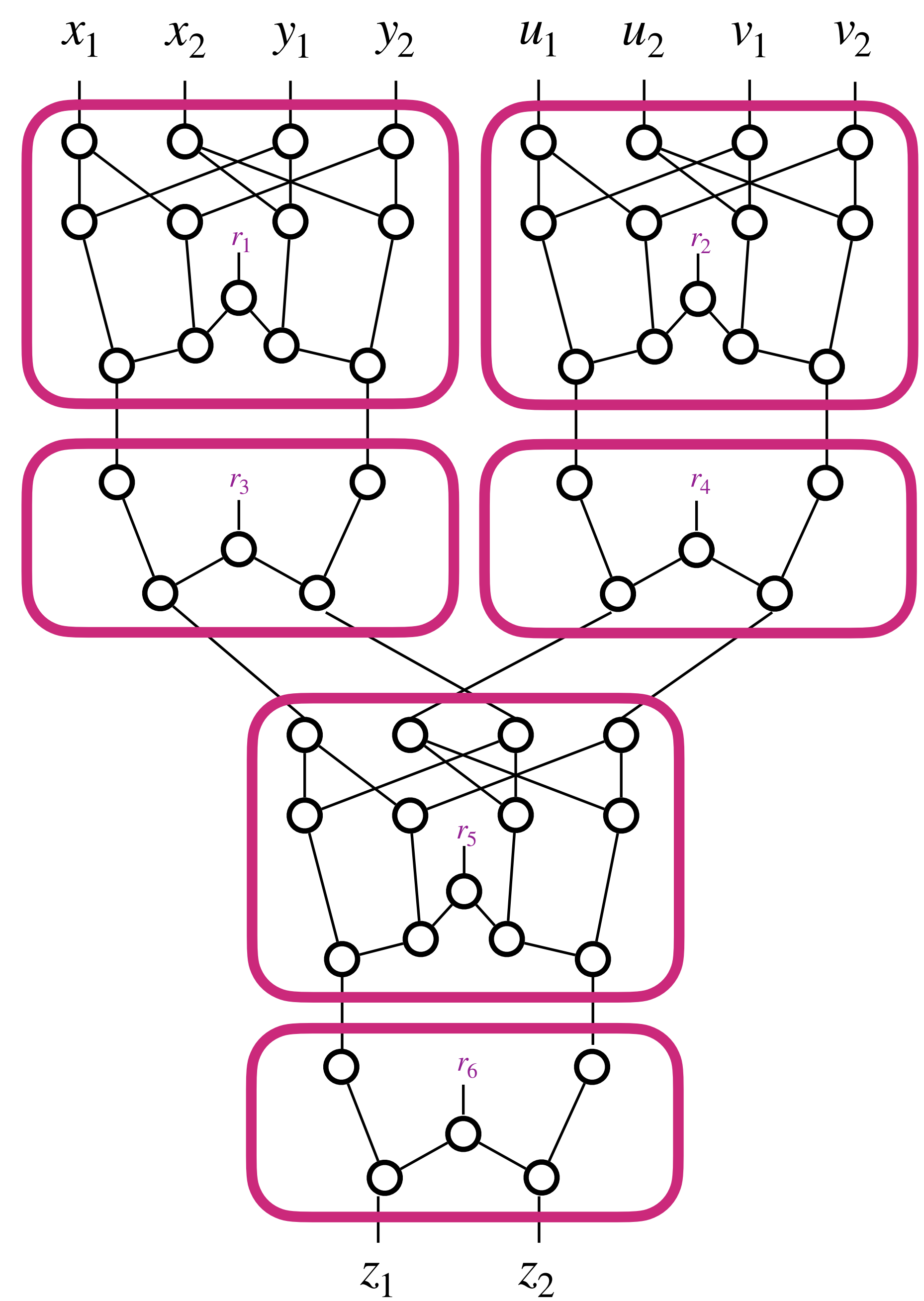
Threshold RPC

Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020
My Work

(p, t, ε)-threshold RPC:

Leakage and any t output shares can be perfectly simulated with at most t shares of each input, except with probability ε





Threshold RPC

Threshold RPC

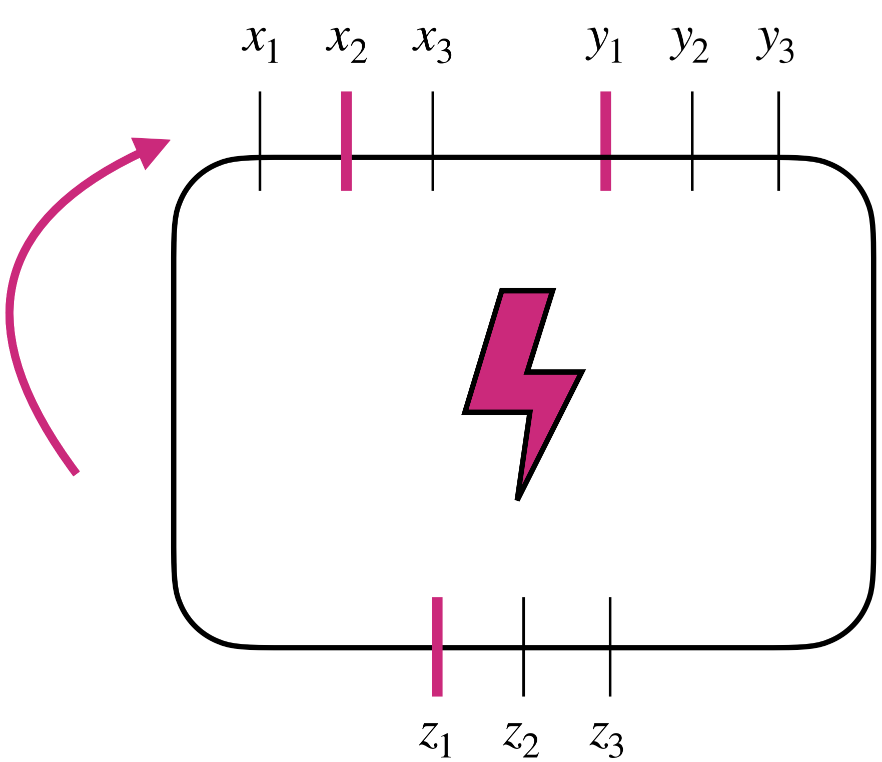
Belaïd • Coron • Prouff • Rivain • Taleb

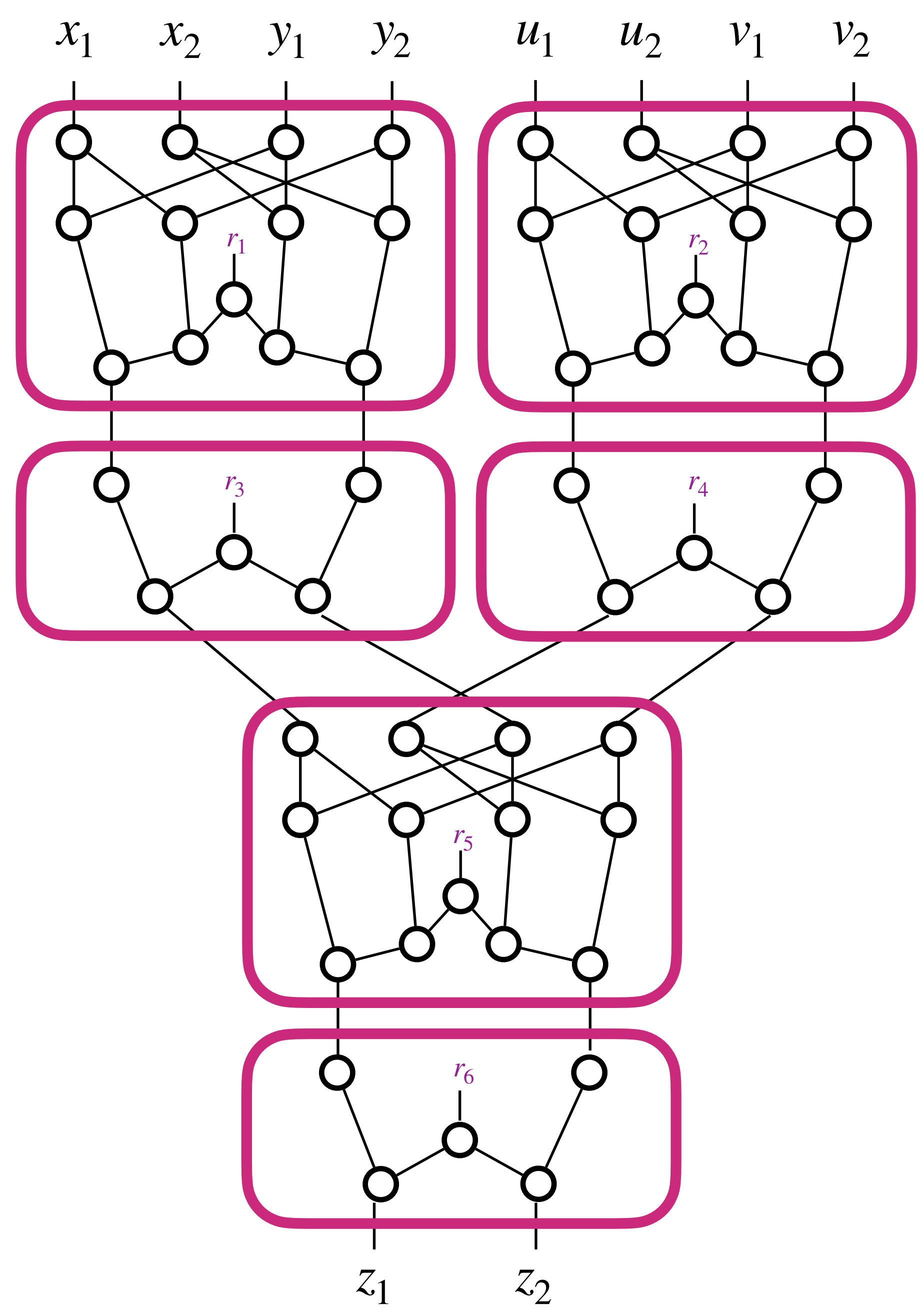
CRYPTO 2020

My Work

(p, t, ε)-threshold RPC:

Leakage and any t output shares can be perfectly simulated with at most t shares of each input, except with probability ε





Threshold RPC

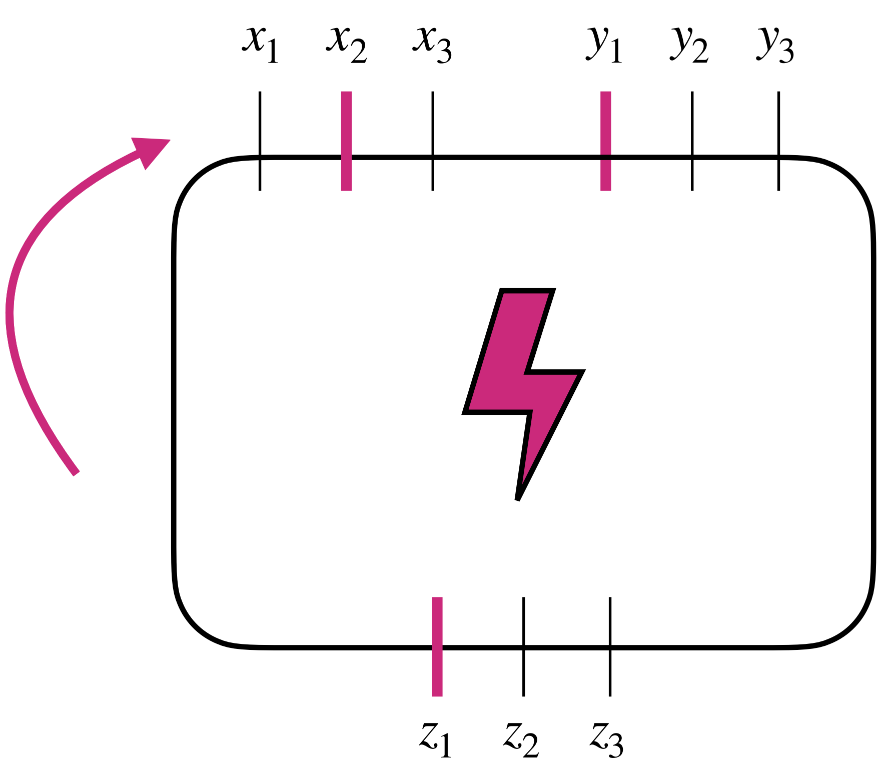
Threshold RPC

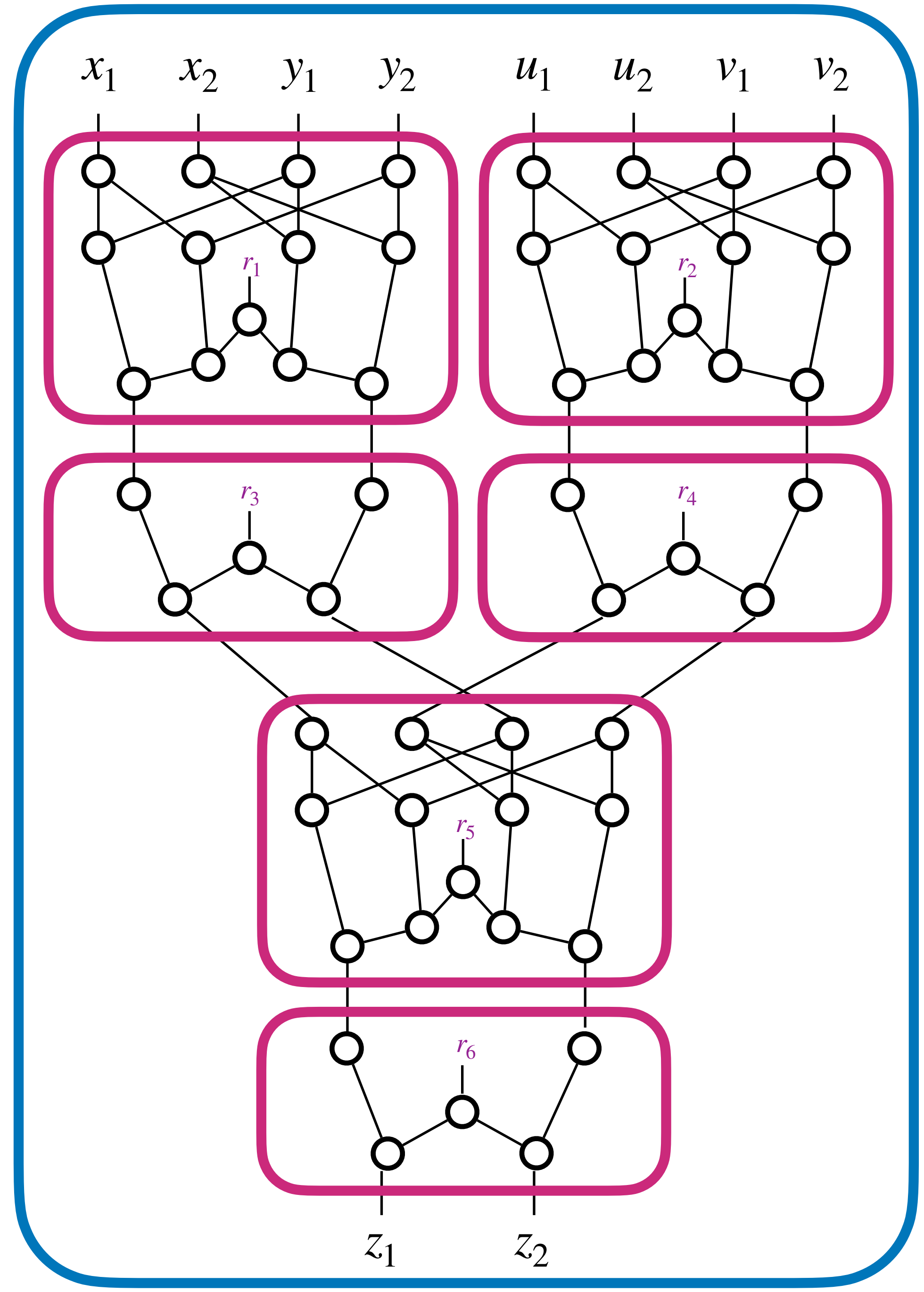
Belaïd • Coron • Prouff • Rivain • Taleb

CRYPTO 2020

My Work

Threshold RPC

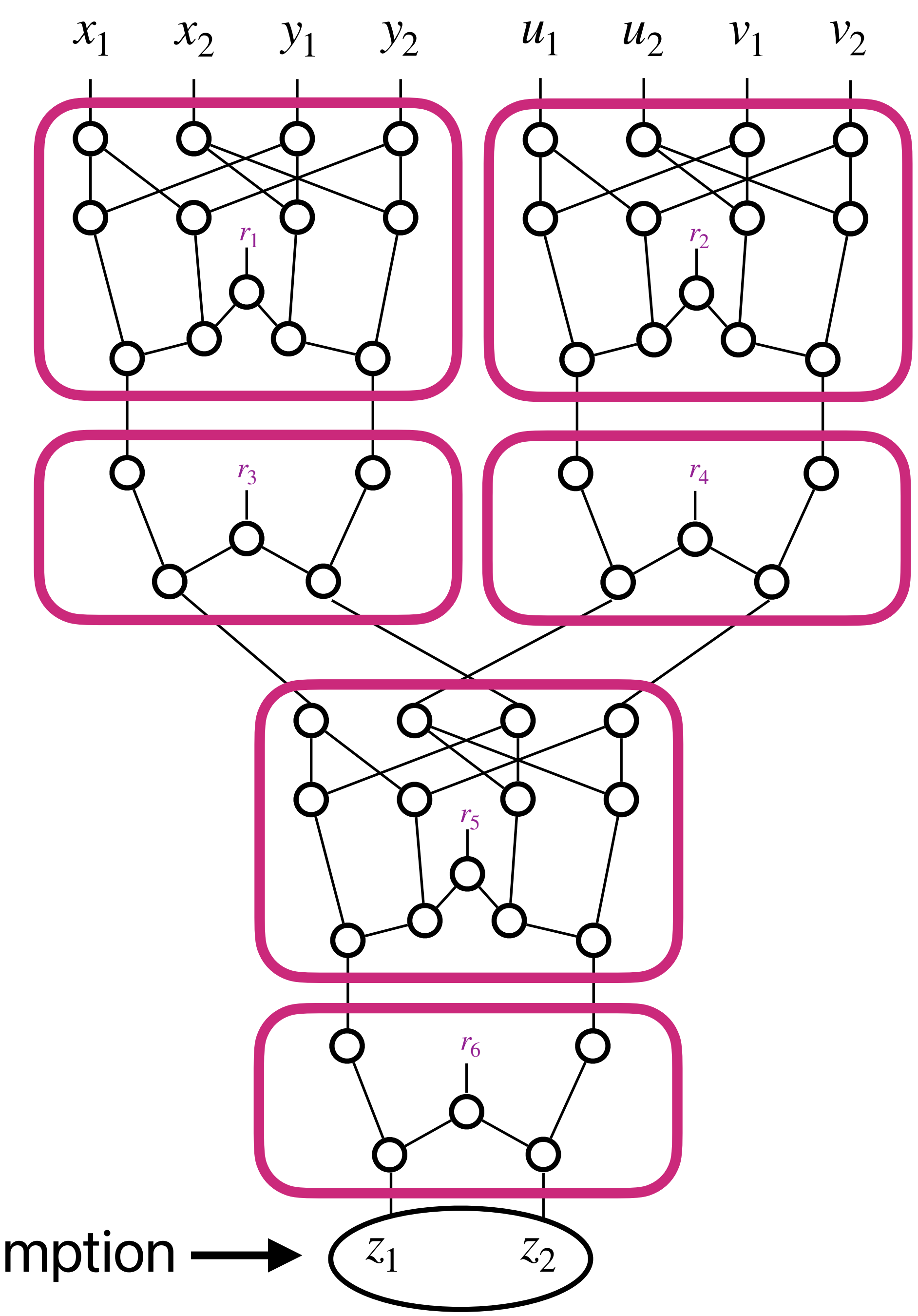




Threshold RPC

Threshold RPC

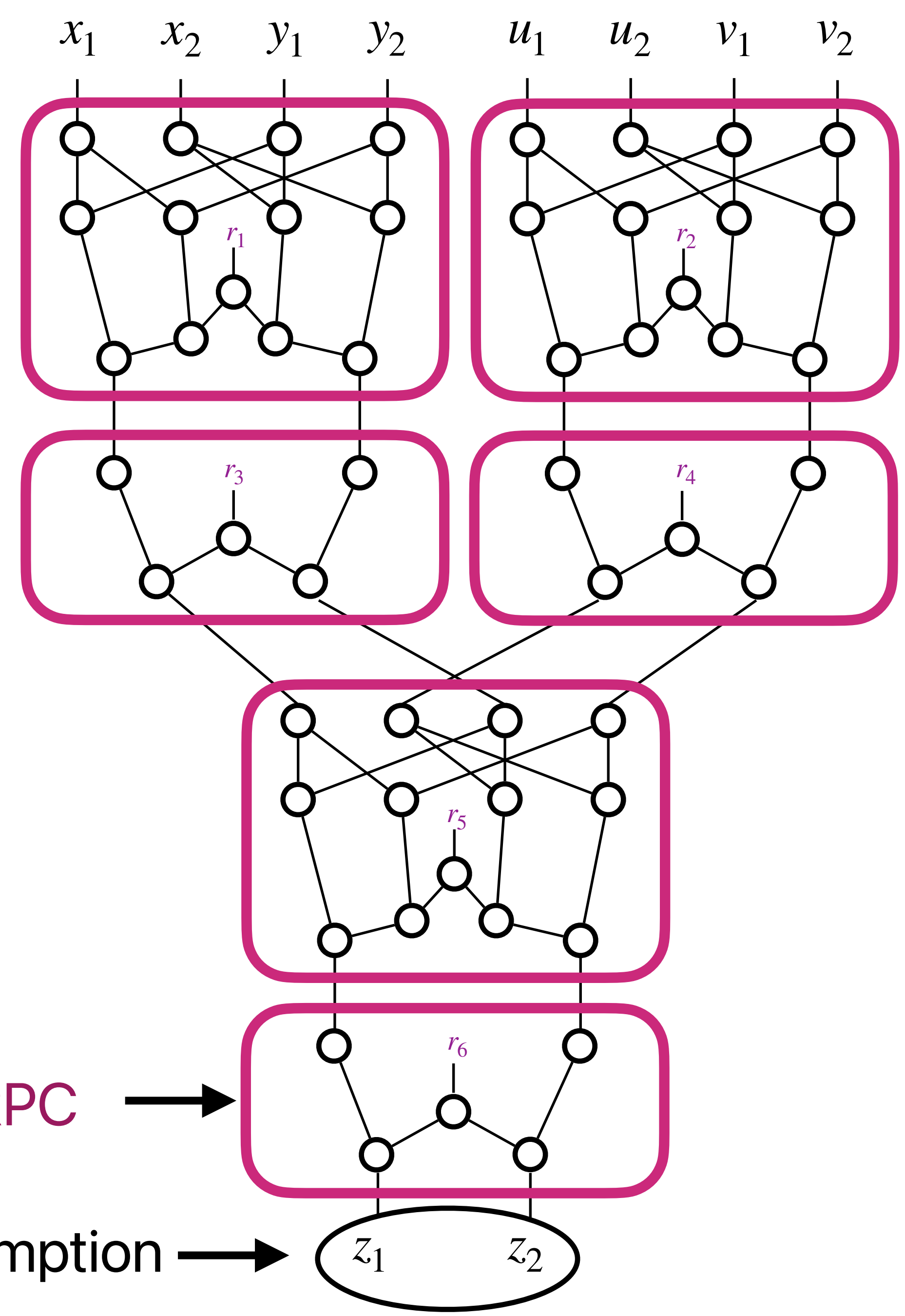
Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020
My Work



No leakage by assumption

Threshold RPC

Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020
My Work



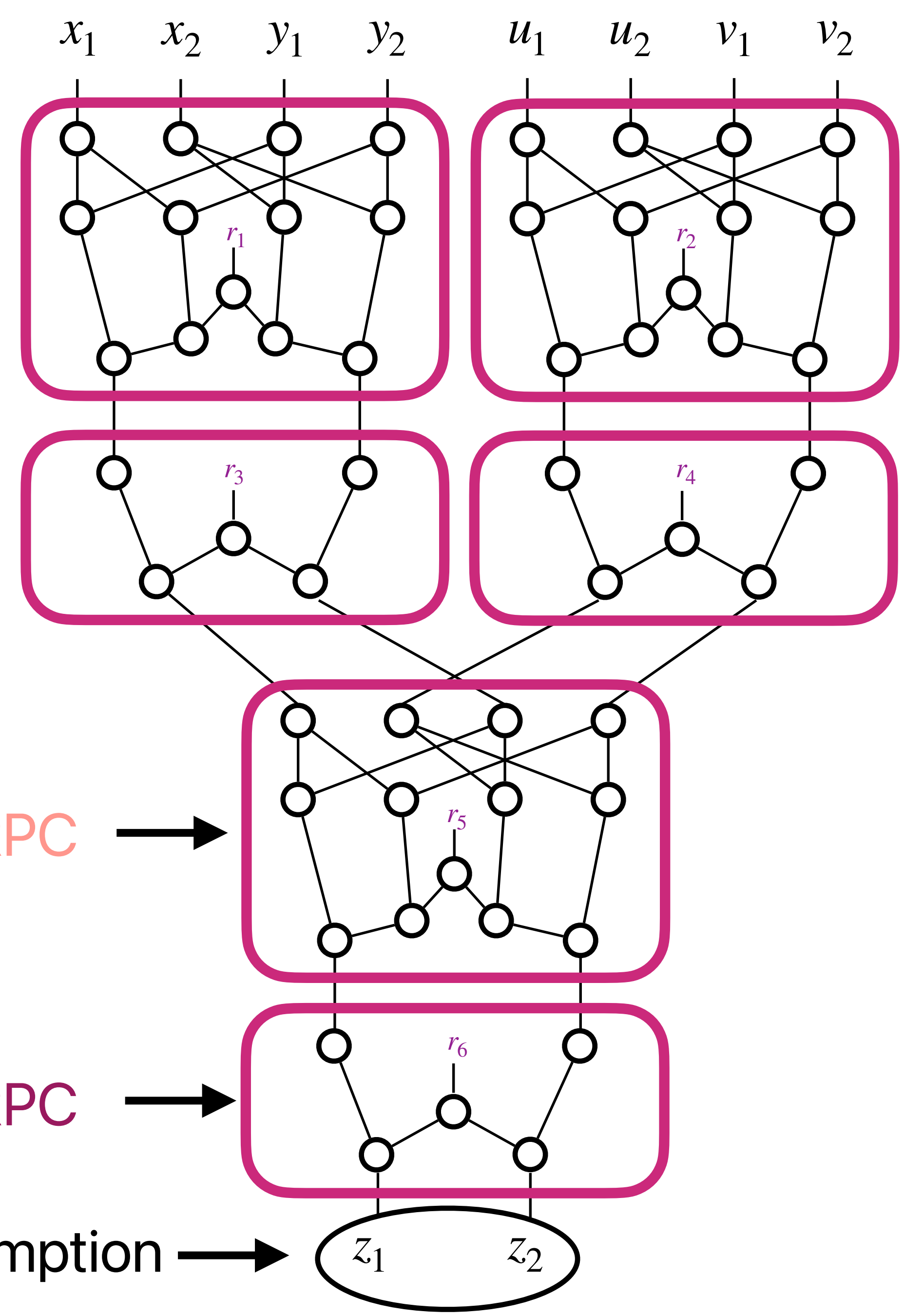
$(p, 1, \varepsilon_b)$-threshold RPC

No leakage by assumption

Simulation except with probability: $\varepsilon \leq \varepsilon_b$

Threshold RPC

Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020
My Work



$(p,1,\varepsilon_b)$-threshold RPC →

$(p,1,\varepsilon_b)$-threshold RPC →

No leakage by assumption →

Simulation except with probability: $\varepsilon \leq 1-(1-\varepsilon_b)^2$

Threshold RPC

Belaïd • Coron • Prouff • Rivain • Taleb

CRYPTO 2020

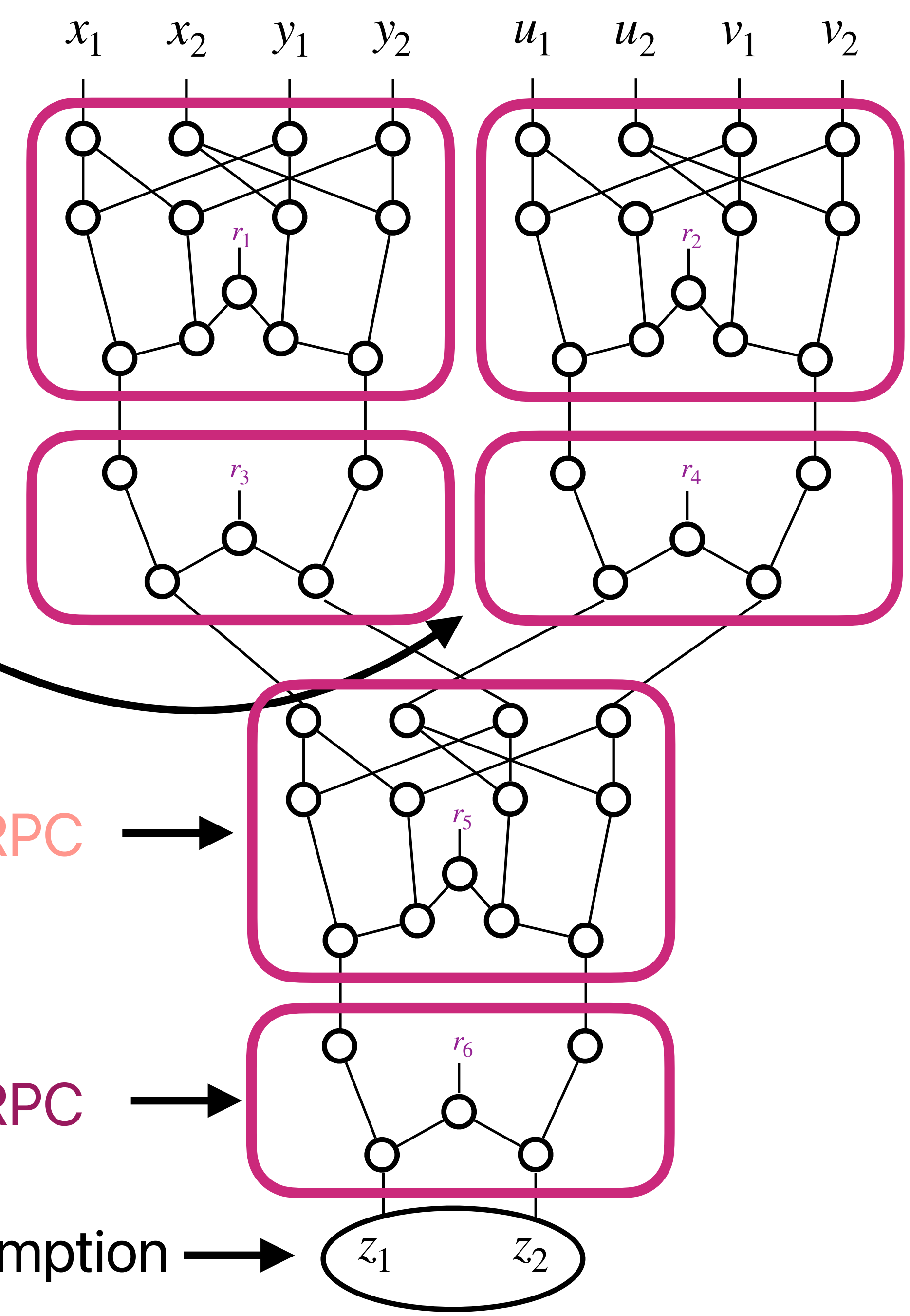
My Work

$(p,1,\varepsilon_b)$-threshold RPC

$(p,1,\varepsilon_b)$-threshold RPC

$(p,1,\varepsilon_b)$-threshold RPC

No leakage by assumption



Simulation except with probability: $\varepsilon \leq 1 - (1 - \varepsilon_b)^4$

Threshold RPC

Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020
My Work

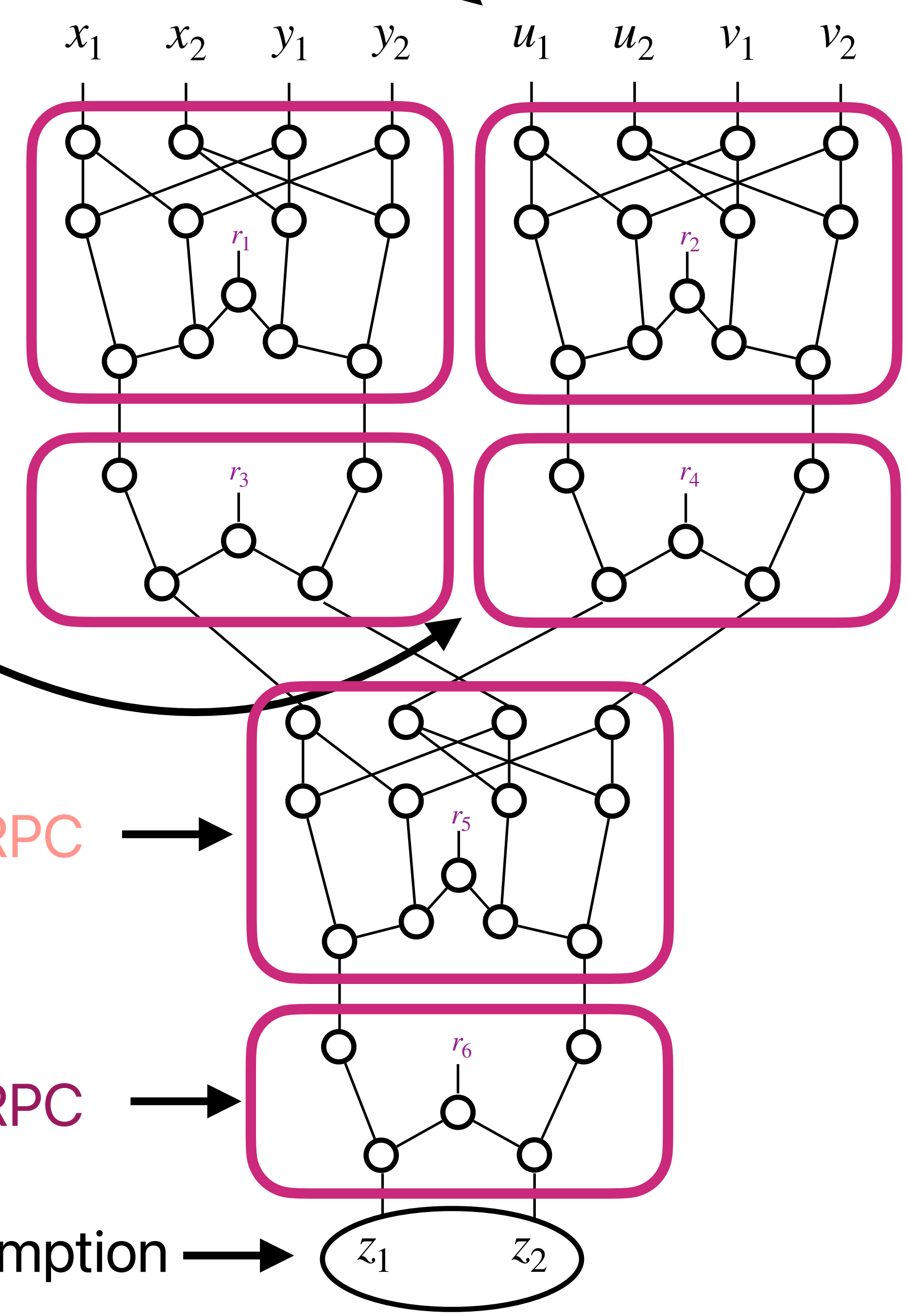
$(p,1,\varepsilon_b)$-threshold RPC

$(p,1,\varepsilon_b)$-threshold RPC

$(p,1,\varepsilon_b)$-threshold RPC

$(p,1,\varepsilon_b)$-threshold RPC

No leakage by assumption



Simulation except with probability: $\varepsilon \leq 1 - (1 - \varepsilon_b)^6$

Threshold RPC

Belaïd • Coron • Prouff • Rivain • Taleb

CRYPTO 2020

My Work

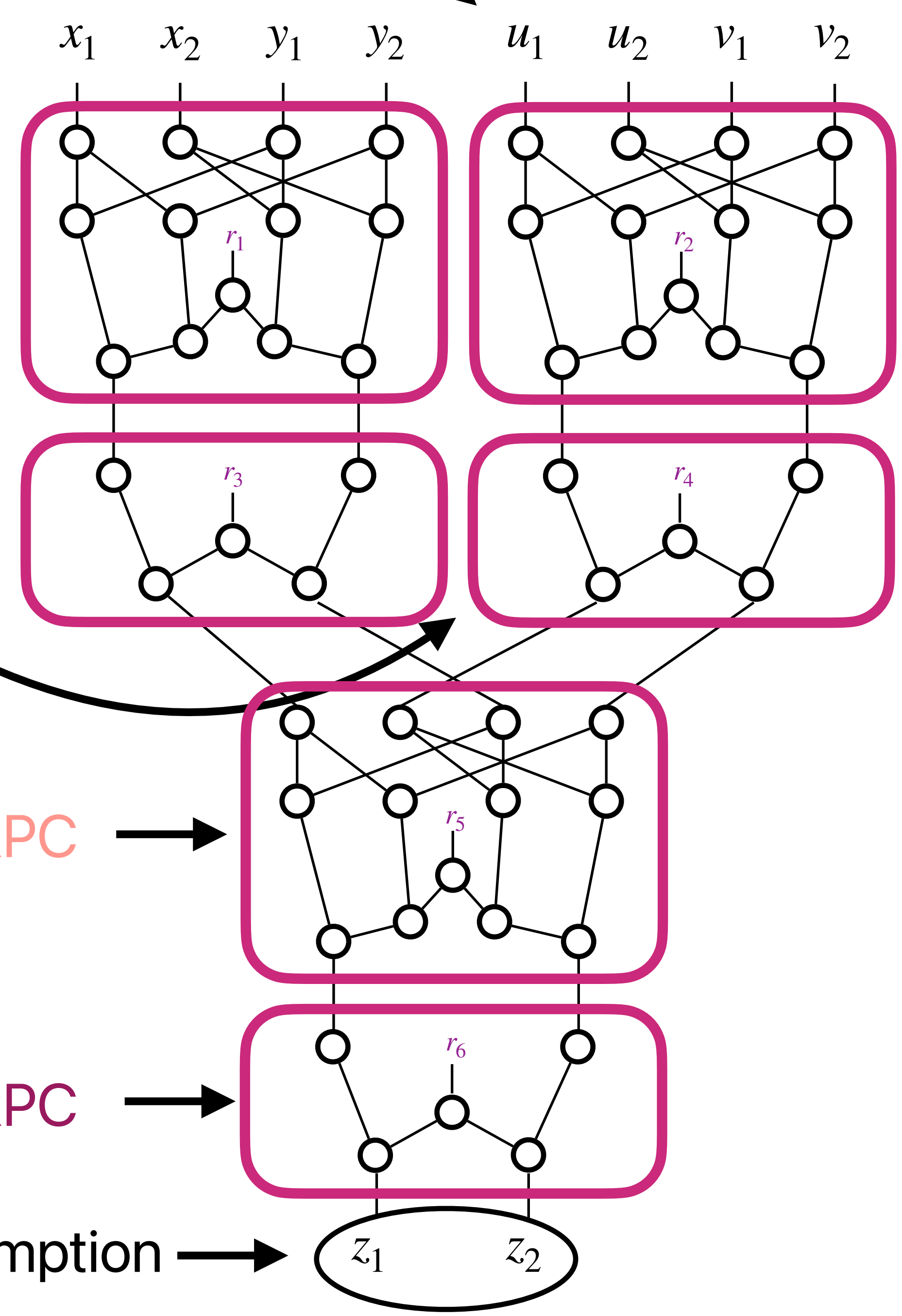
$(p,1,\varepsilon_b)$-threshold RPC

$(p,1,\varepsilon_b)$-threshold RPC

$(p,1,\varepsilon_b)$-threshold RPC

$(p,1,\varepsilon_b)$-threshold RPC

No leakage by assumption

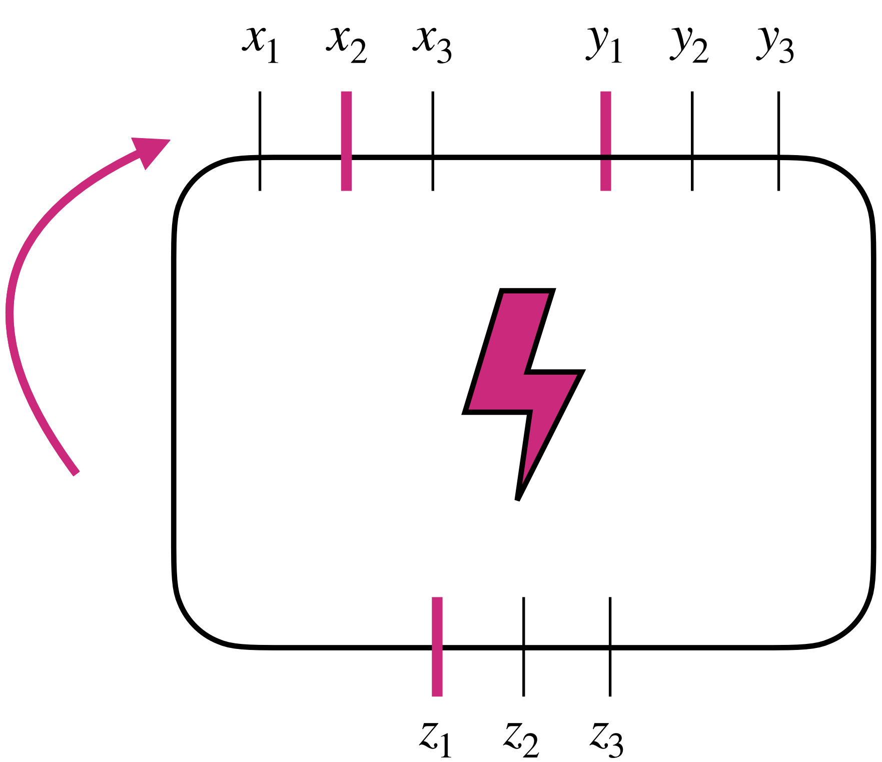


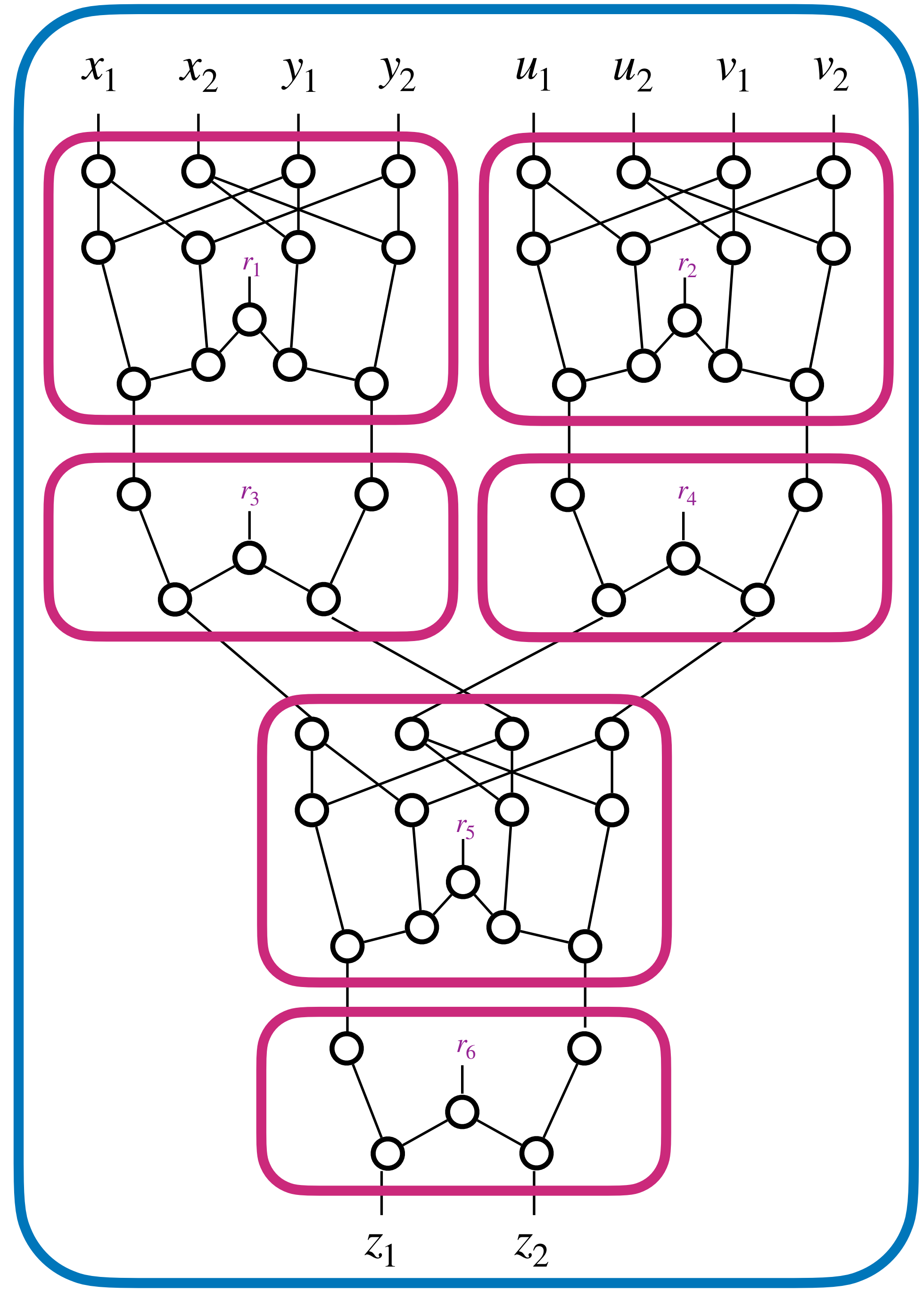
Simulation except with probability: $\varepsilon \leq 1-(1-\varepsilon_b)^6 \leq 6 \cdot \varepsilon_b$

Threshold RPC

Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020
My Work

Threshold RPC



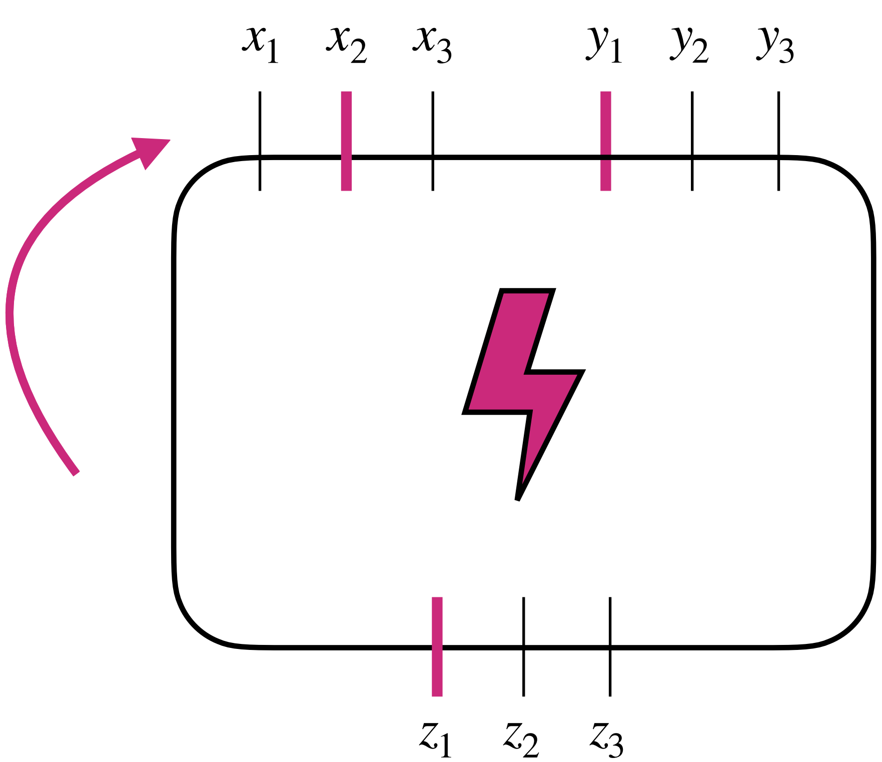


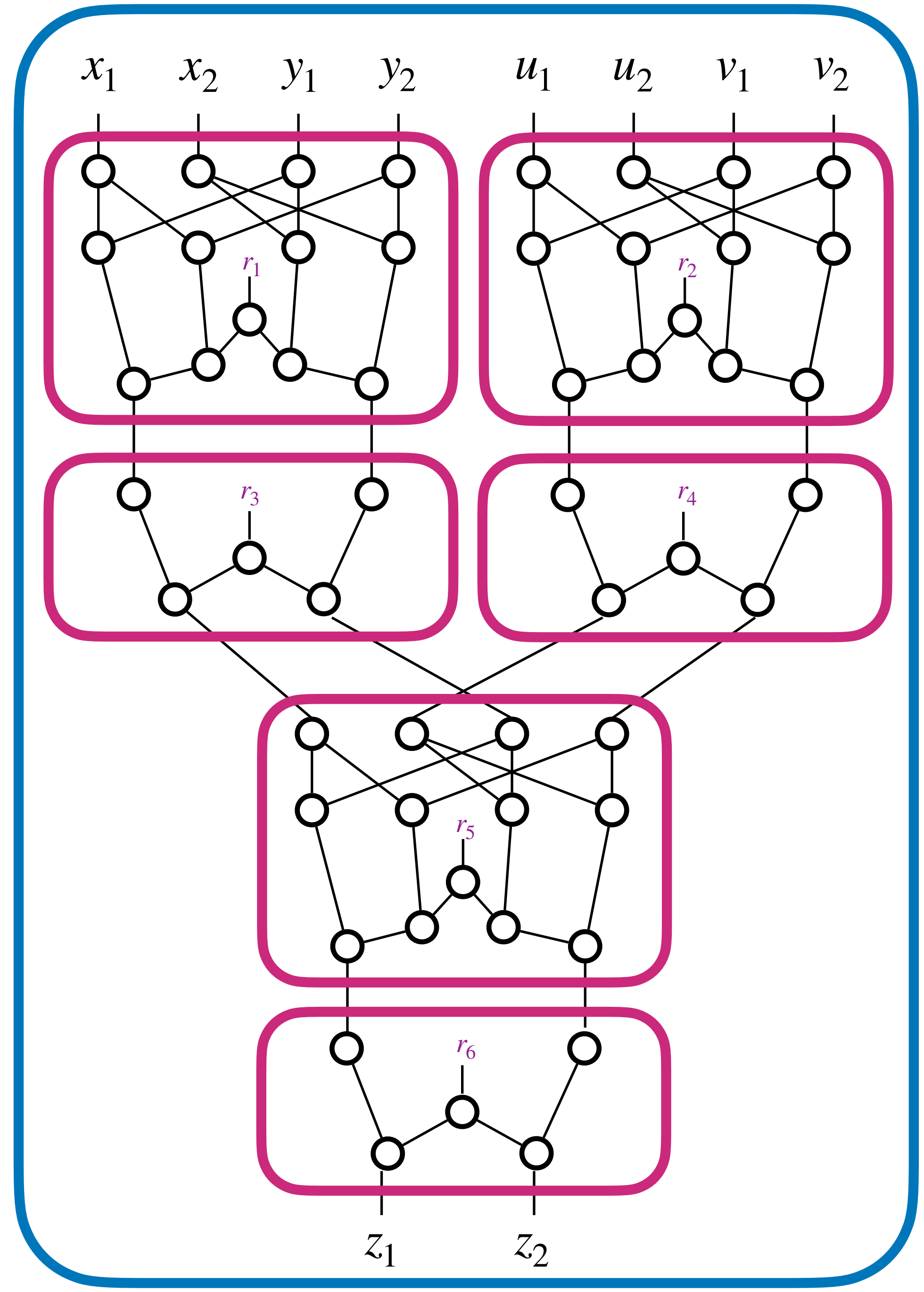
Threshold RPC

Threshold RPC

Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020
My Work

Threshold RPC
⇒ Random Probing Security

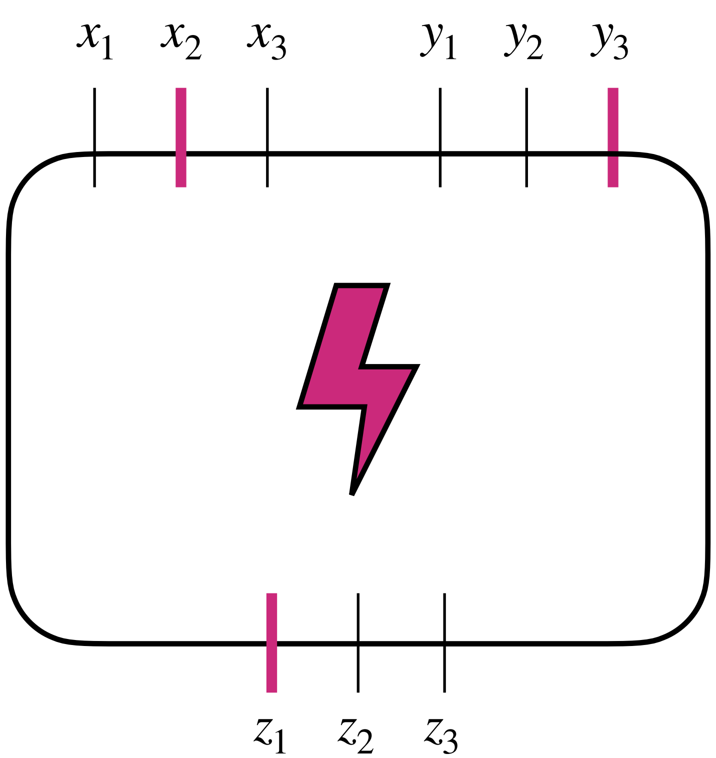




Threshold RPC

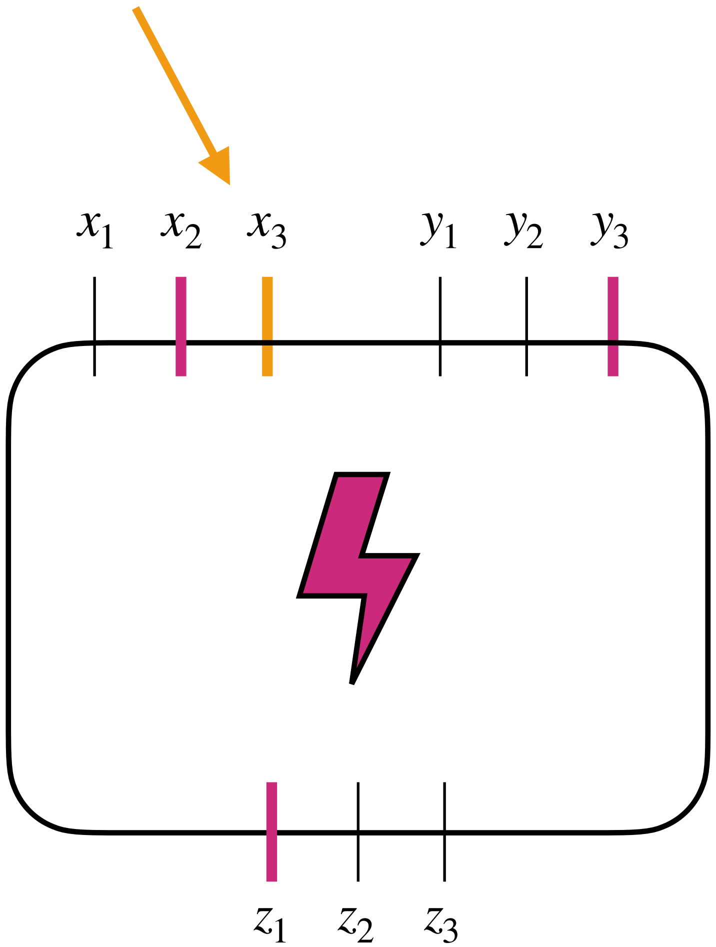
Threshold RPC

But not tight:
requiring more than t shares does not necessarily imply a failure



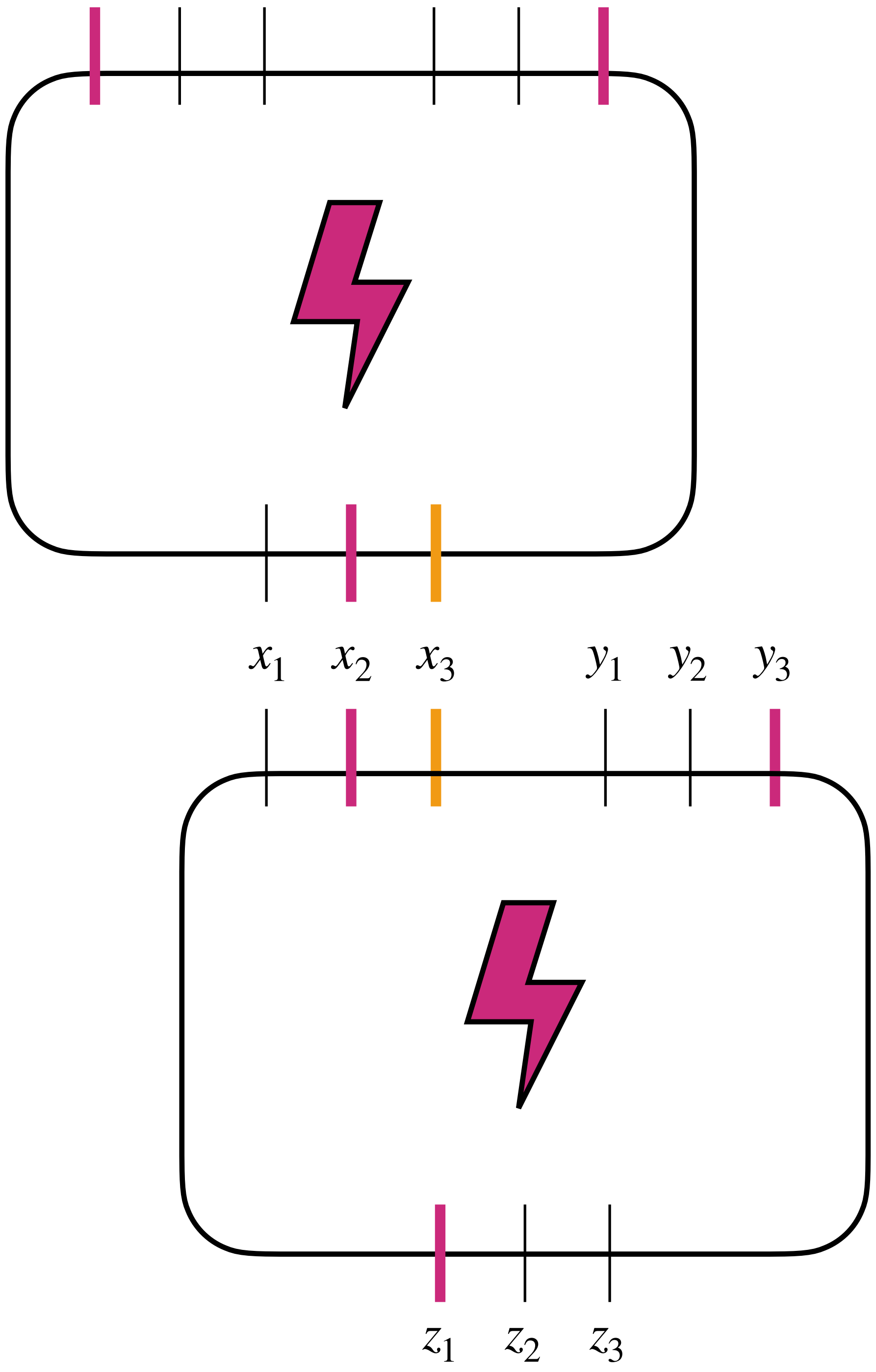
Threshold RPC

But not tight:
requiring more than t shares does not necessarily imply a failure



Threshold RPC

But not tight:
requiring more than t shares does not necessarily imply a failure

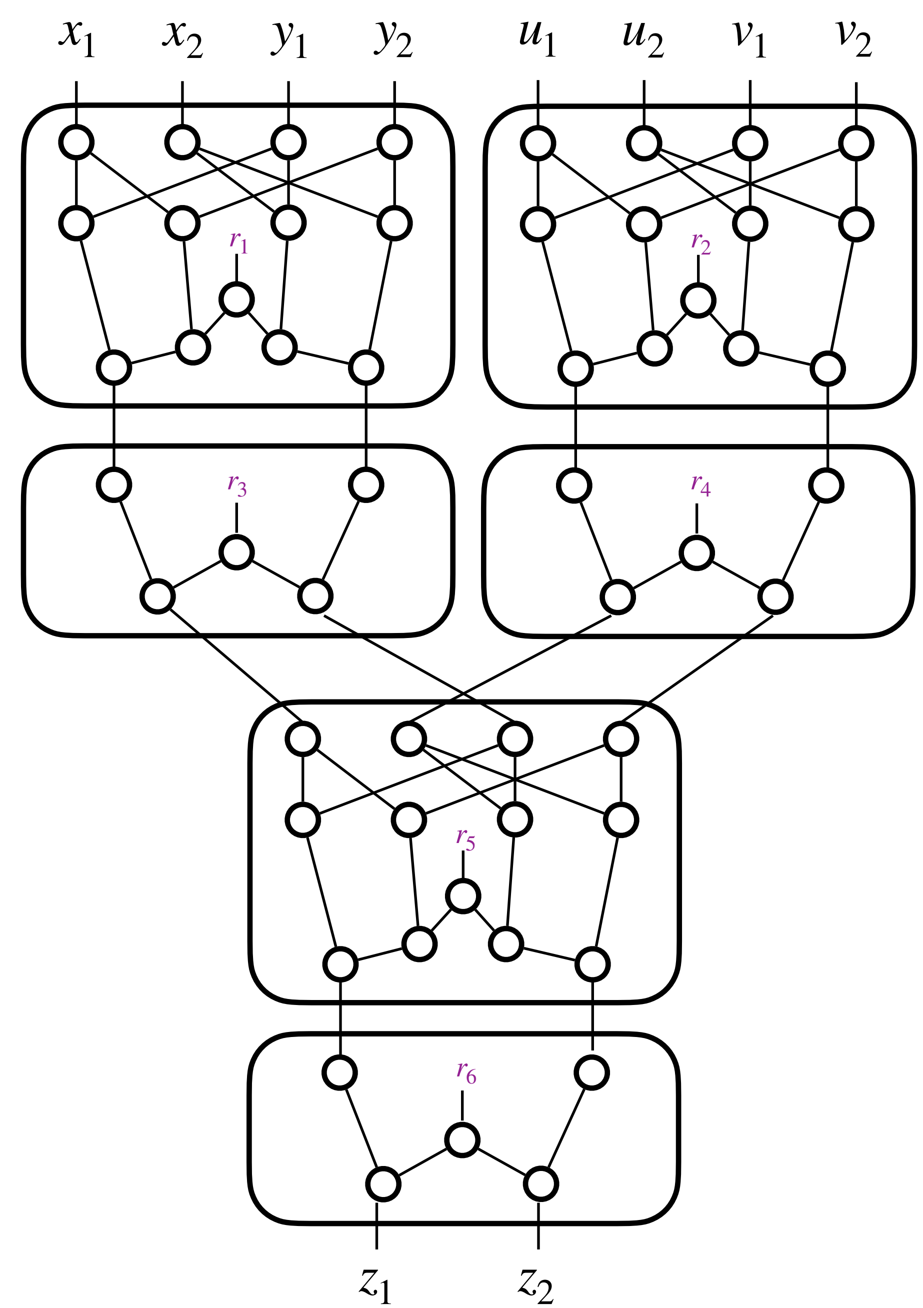


Composition

Ananth • Ishai • Sahai
CRYPTO 2018
MPC-based construction with explicit and constant leakage rate

Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020
Threshold RPC
My Work

Cassiers • Faust • Orlt • Standaert
CRYPTO 2021
General RPC (Probe Distribution Tables)

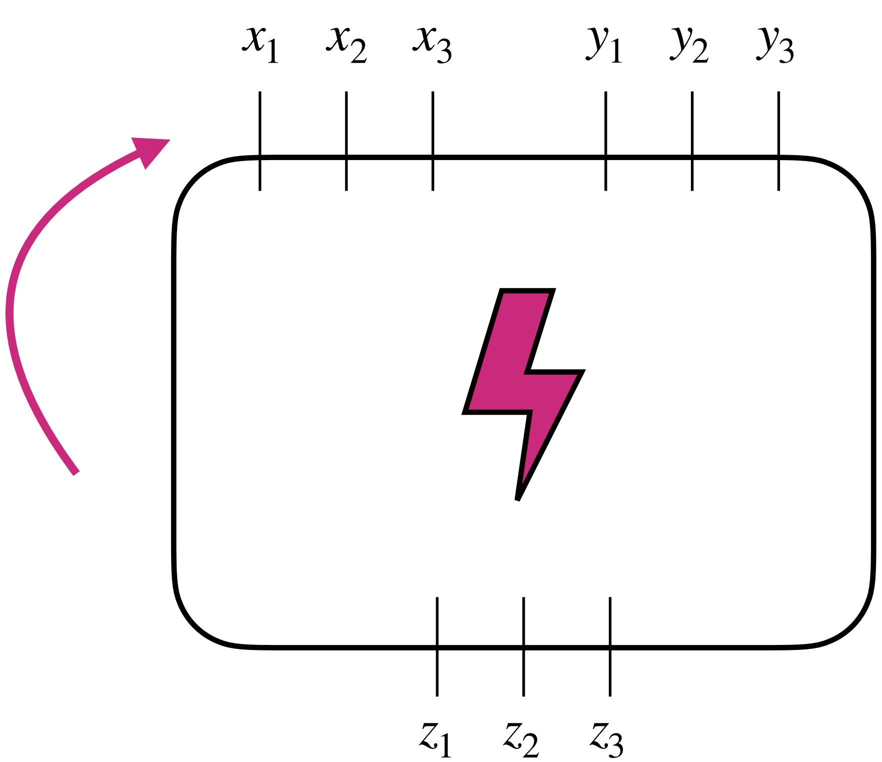


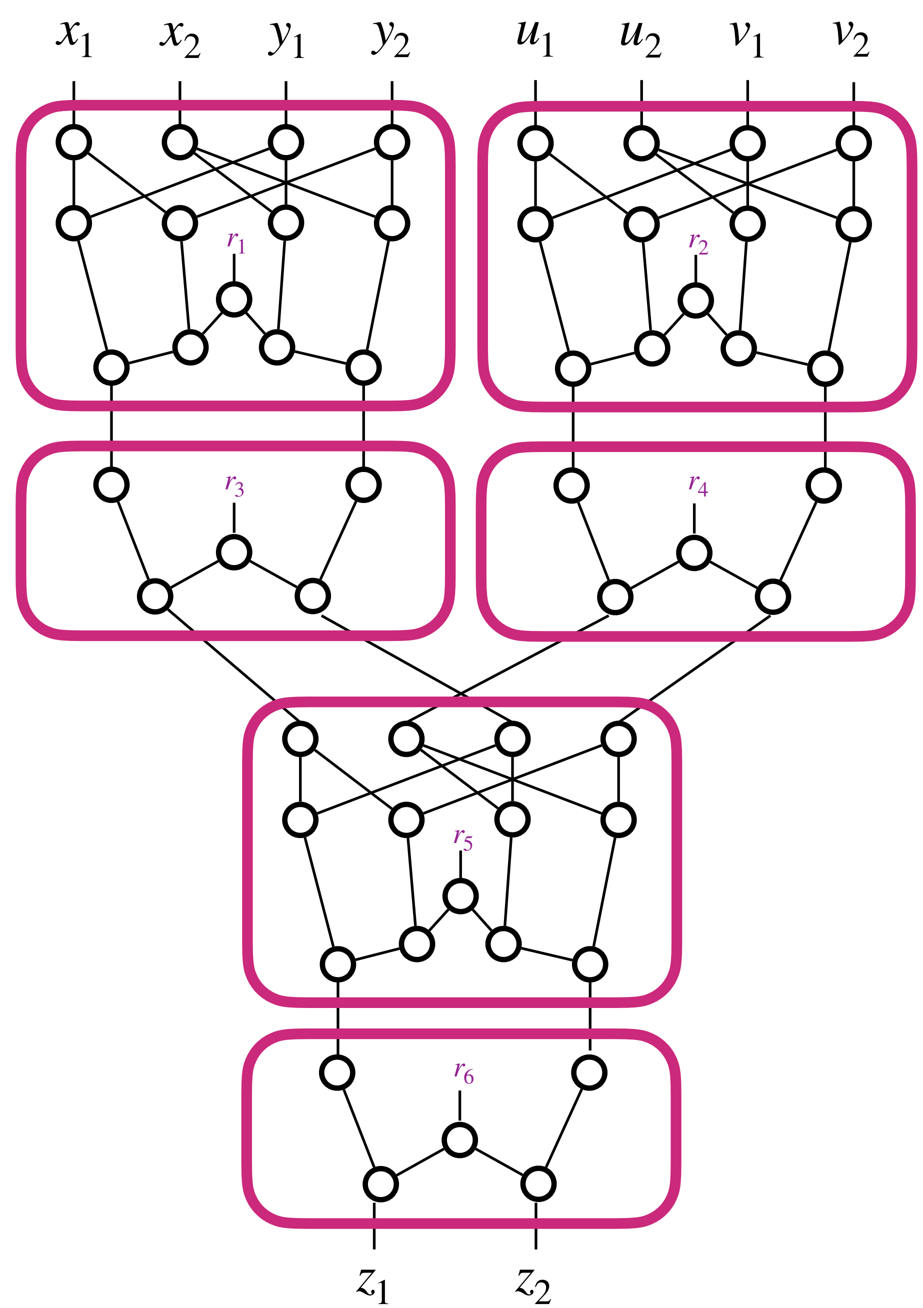
General RPC

Cassiers • Faust • Orlt • Standaert
CRYPTO 2021

$(p, \mathscr{E})$-general RPC:

For all $\mathscr{I}, \mathscr{O}$, leakage and the output shares $\mathscr{O}$ can be perfectly simulated with exactly the input shares $\mathscr{I}$ with probability $\leq \mathscr{E}_{\mathscr{O}}(\mathscr{I})$





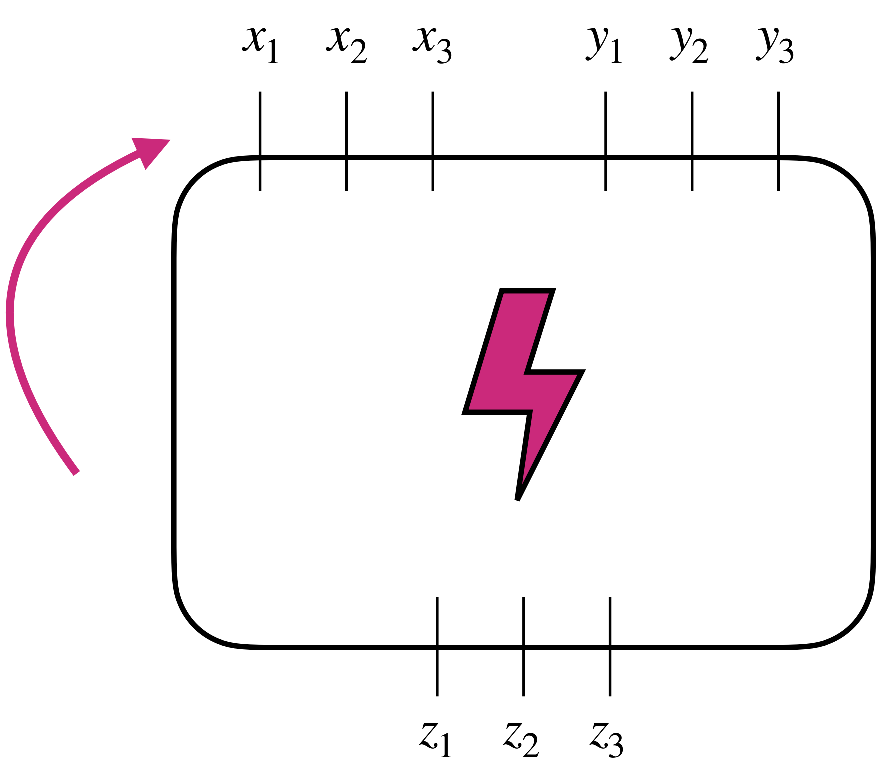
General RPC

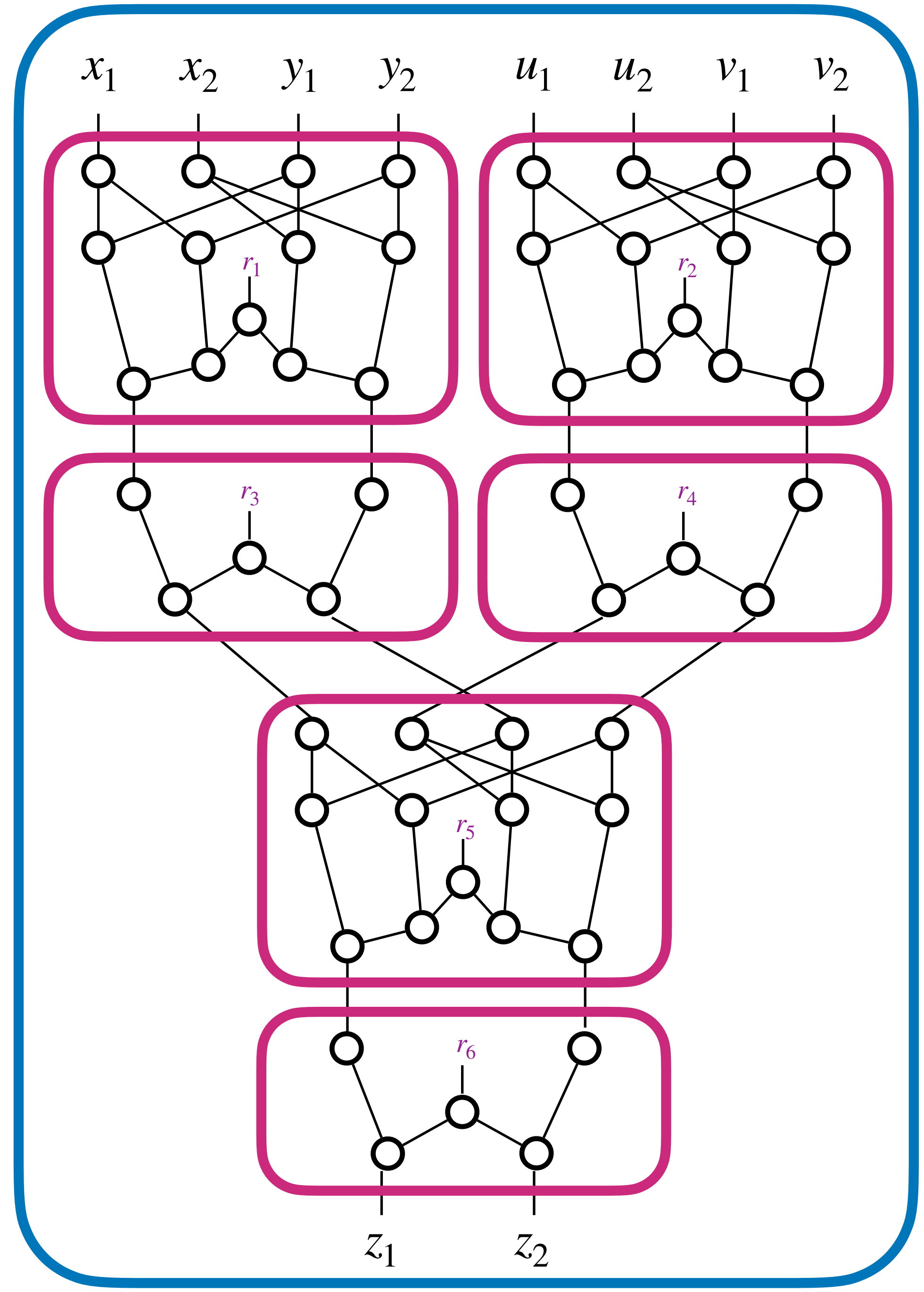
General RPC

Cassiers • Faust • Orlt • Standaert
CRYPTO 2021

General RPC

$\Rightarrow$ Random Probing Security



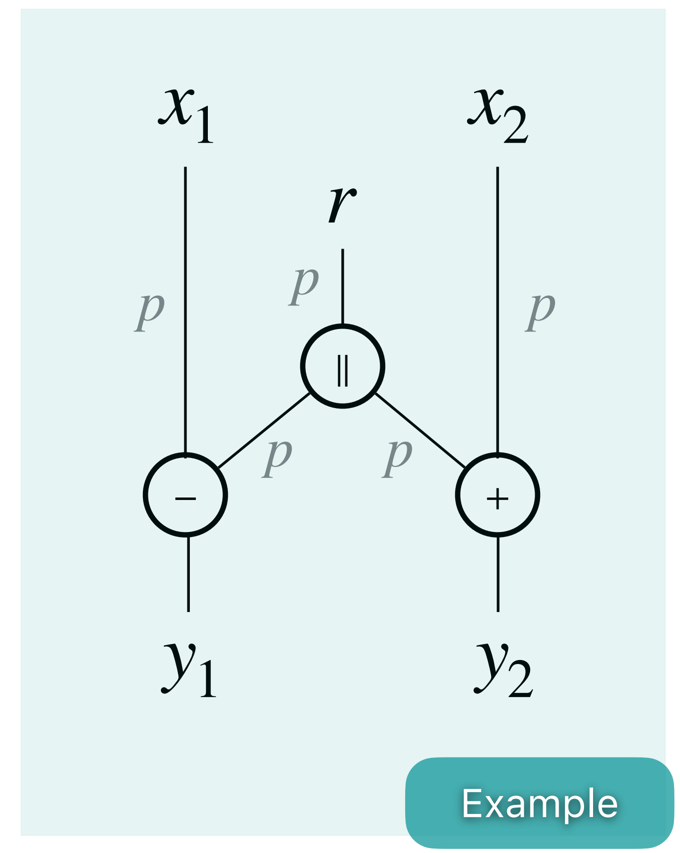


General RPC

General RPC

Cassiers • Faust • Orlt • Standaert
CRYPTO 2021

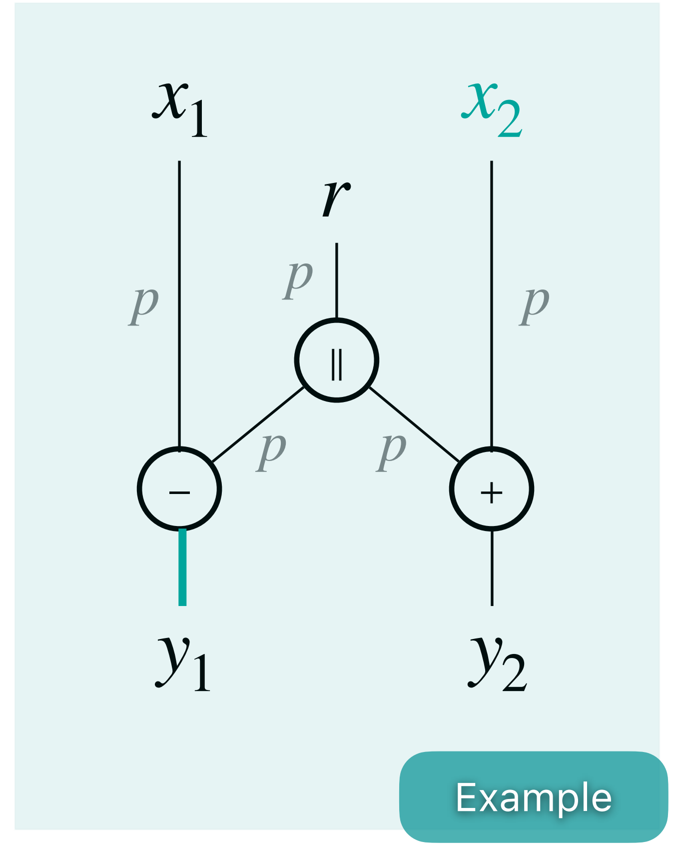
	$\varnothing$	y_1	y_2	(y_1, y_2)
$\varnothing$	$(1-p)^2$	$(1-p)^5$	$(1-p)^5$	0
x_1	$p(1-p)$	$(1-p)\cdot(1-(1-p)^4)$	$p(1-p)^4$	0
x_2	$p(1-p)$	$p(1-p)^4$	$(1-p)\cdot(1-(1-p)^4)$	0
(x_1, x_2)	p^2	$p\cdot(1-(1-p)^4)$	$p\cdot(1-(1-p)^4)$	1



General RPC

Cassiers • Faust •
Orlt • Standaert
CRYPTO 2021

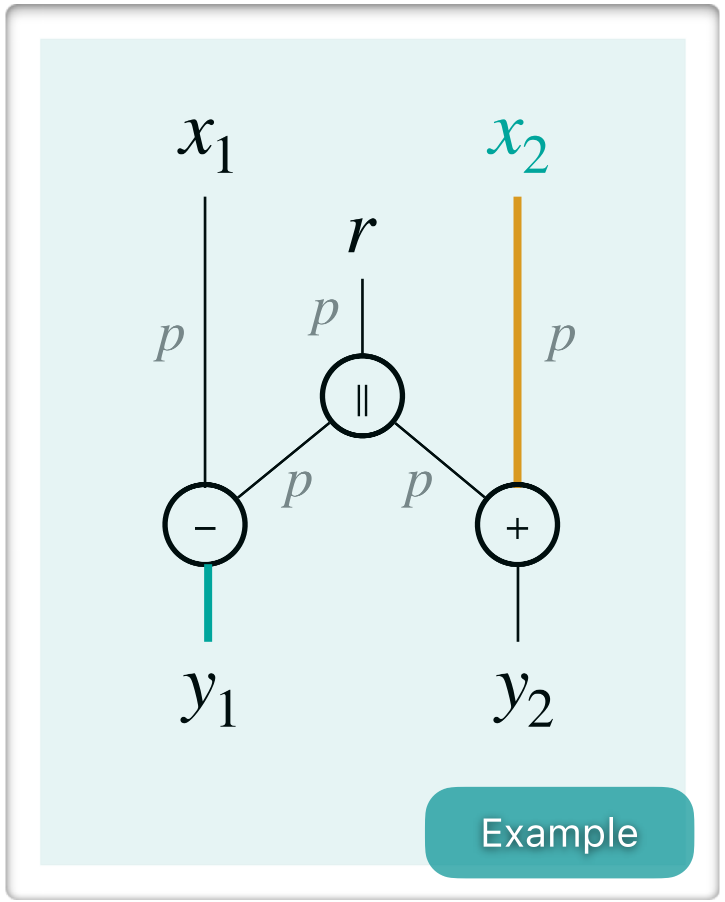
	$\varnothing$	y_1	y_2	(y_1, y_2)
$\varnothing$	$(1-p)^2$	$(1-p)^5$	$(1-p)^5$	0
x_1	$p(1-p)$	$(1-p) \cdot (1-(1-p)^4)$	$p(1-p)^4$	0
x_2	$p(1-p)$	$p(1-p)^4$	$(1-p) \cdot (1-(1-p)^4)$	0
(x_1, x_2)	p^2	$p \cdot (1-(1-p)^4)$	$p \cdot (1-(1-p)^4)$	1



General RPC

Cassiers • Faust • Orlt • Standaert
CRYPTO 2021

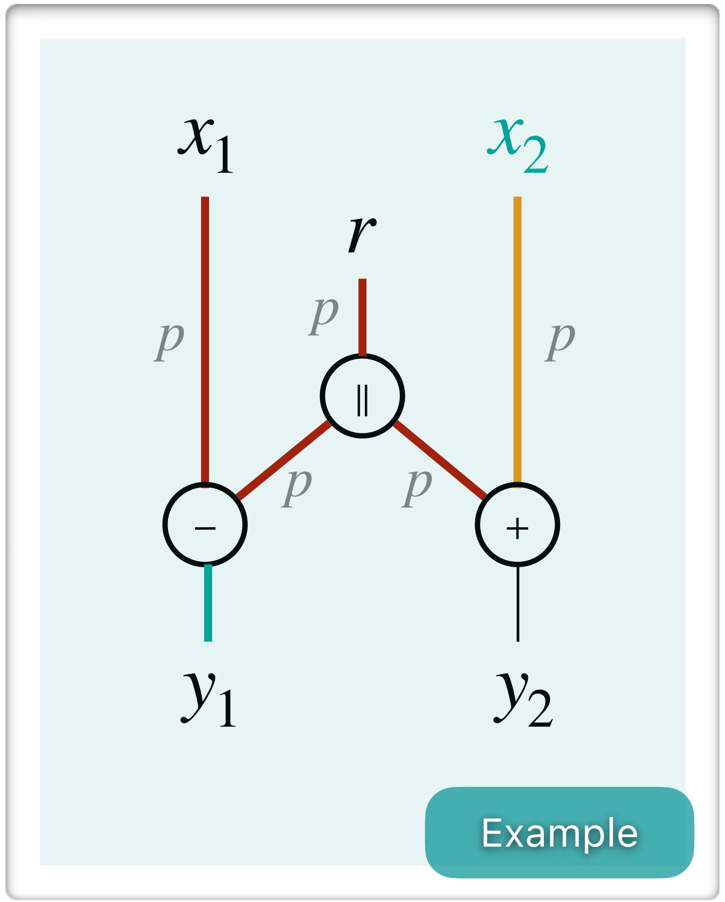
	$\varnothing$	y_1	y_2	(y_1, y_2)
$\varnothing$	$(1-p)^2$	$(1-p)^5$	$(1-p)^5$	0
x_1	$p(1-p)$	$(1-p) \cdot (1-(1-p)^4)$	$p(1-p)^4$	0
x_2	$p(1-p)$	$p(1-p)^4$	$(1-p) \cdot (1-(1-p)^4)$	0
(x_1, x_2)	p^2	$p \cdot (1-(1-p)^4)$	$p \cdot (1-(1-p)^4)$	1



General RPC

Cassiers • Faust • Orlt • Standaert
CRYPTO 2021

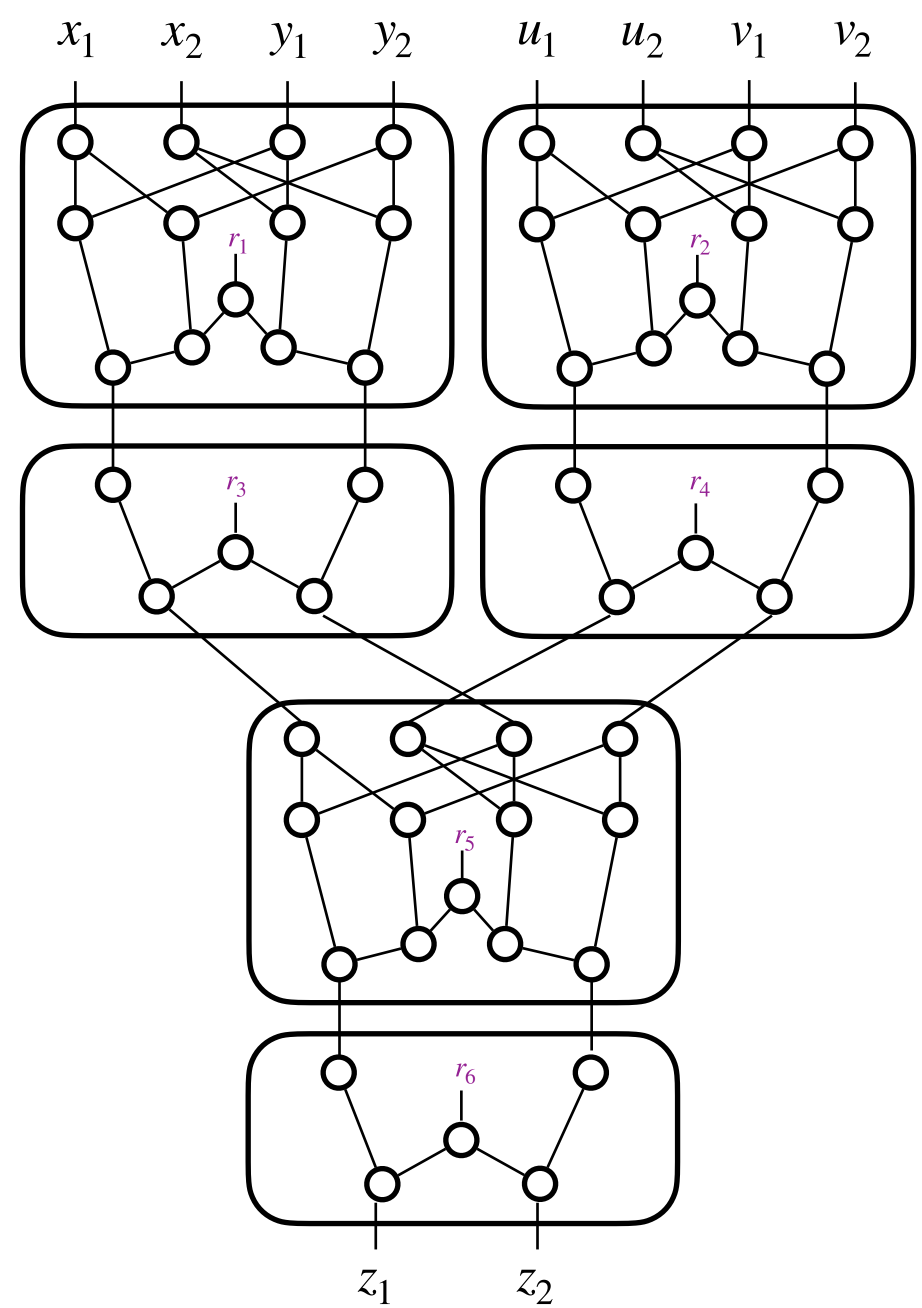
	$\varnothing$	y_1	y_2	(y_1, y_2)
$\varnothing$	$(1-p)^2$	$(1-p)^5$	$(1-p)^5$	0
x_1	$p(1-p)$	$(1-p)\cdot(1-(1-p)^4)$	$p(1-p)^4$	0
x_2	$p(1-p)$	$p(1-p)^4$	$(1-p)\cdot(1-(1-p)^4)$	0
(x_1, x_2)	p^2	$p\cdot(1-(1-p)^4)$	$p\cdot(1-(1-p)^4)$	1



General RPC

Cassiers • Faust •
Orlt • Standaert
CRYPTO 2021

	$\emptyset$	y_1	y_2	(y_1, y_2)
$\emptyset$	$(1-p)^2$	$(1-p)^5$	$(1-p)^5$	0
x_1	$p(1-p)$	$(1-p)\cdot(1-(1-p)^4)$	$p(1-p)^4$	0
x_2	$p(1-p)$	$p(1-p)^4$	$(1-p)\cdot(1-(1-p)^4)$	0
(x_1, x_2)	p^2	$p\cdot(1-(1-p)^4)$	$p\cdot(1-(1-p)^4)$	1



But to complex to evaluate large circuits > already 2^{10} cells

Composition

Ananth • Ishai • Sahai

CRYPTO 2018

MPC-based construction with explicit and constant leakage rate

Belaïd • Coron • Prouff • Rivain • Taleb

CRYPTO 2020

Threshold RPC

My Work

Cassiers • Faust • Orlt • Standaert

CRYPTO 2021

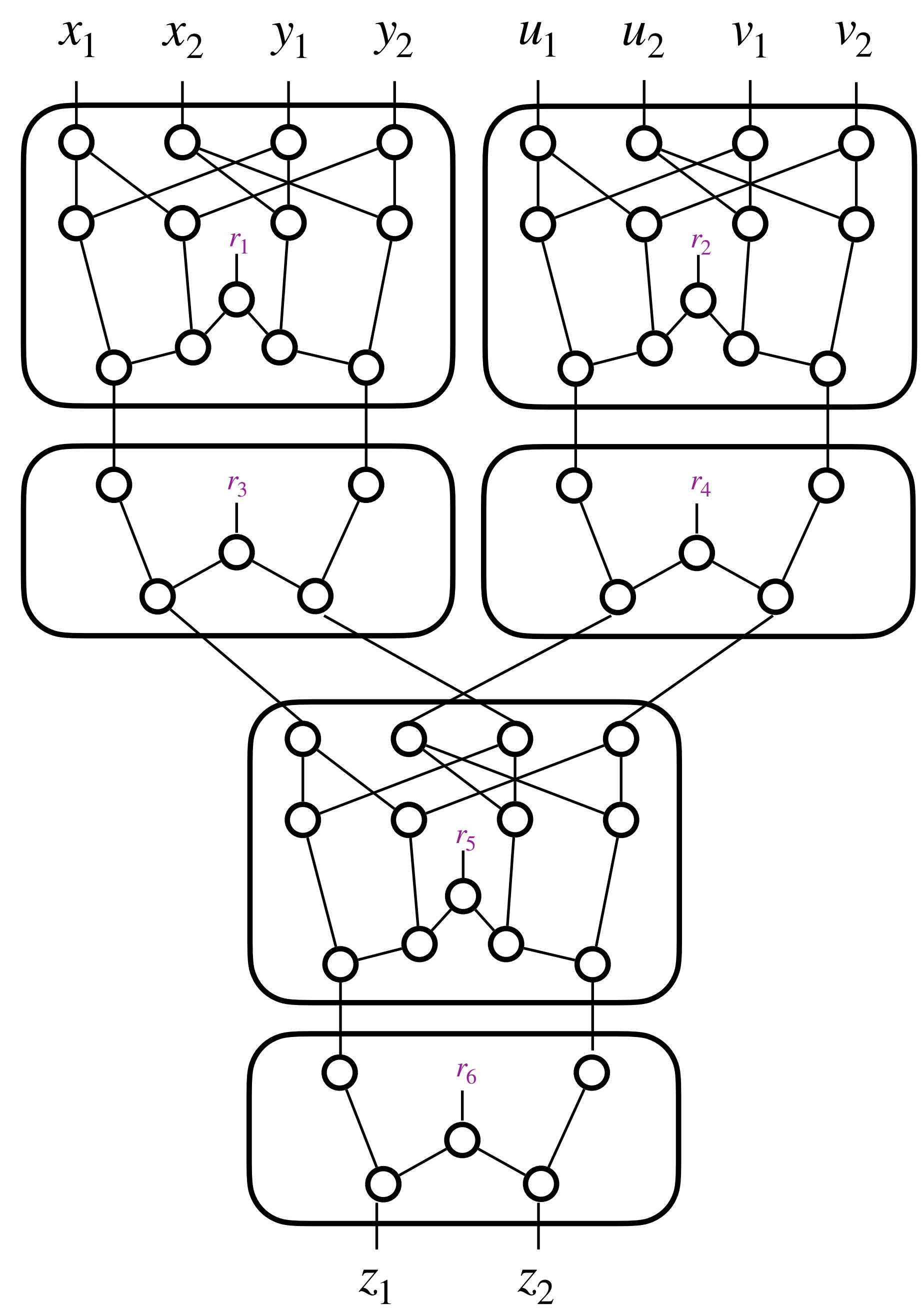
General RPC (Probe Distribution Tables)

Belaïd • Rivain • Rossi

EUROCRYPT 2025

Cardinal RPC

My Work

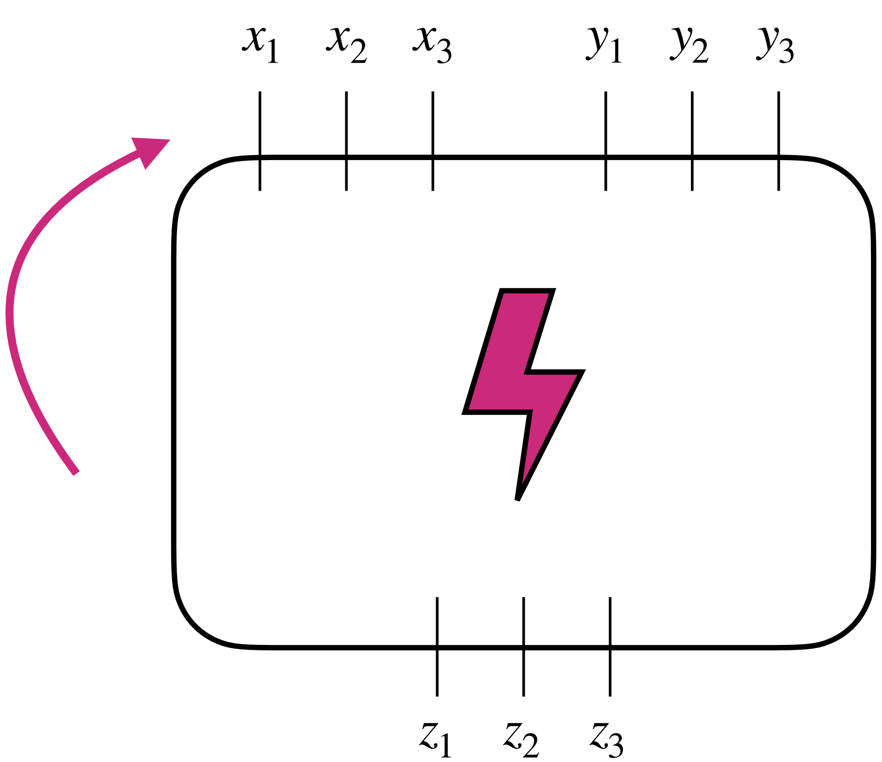


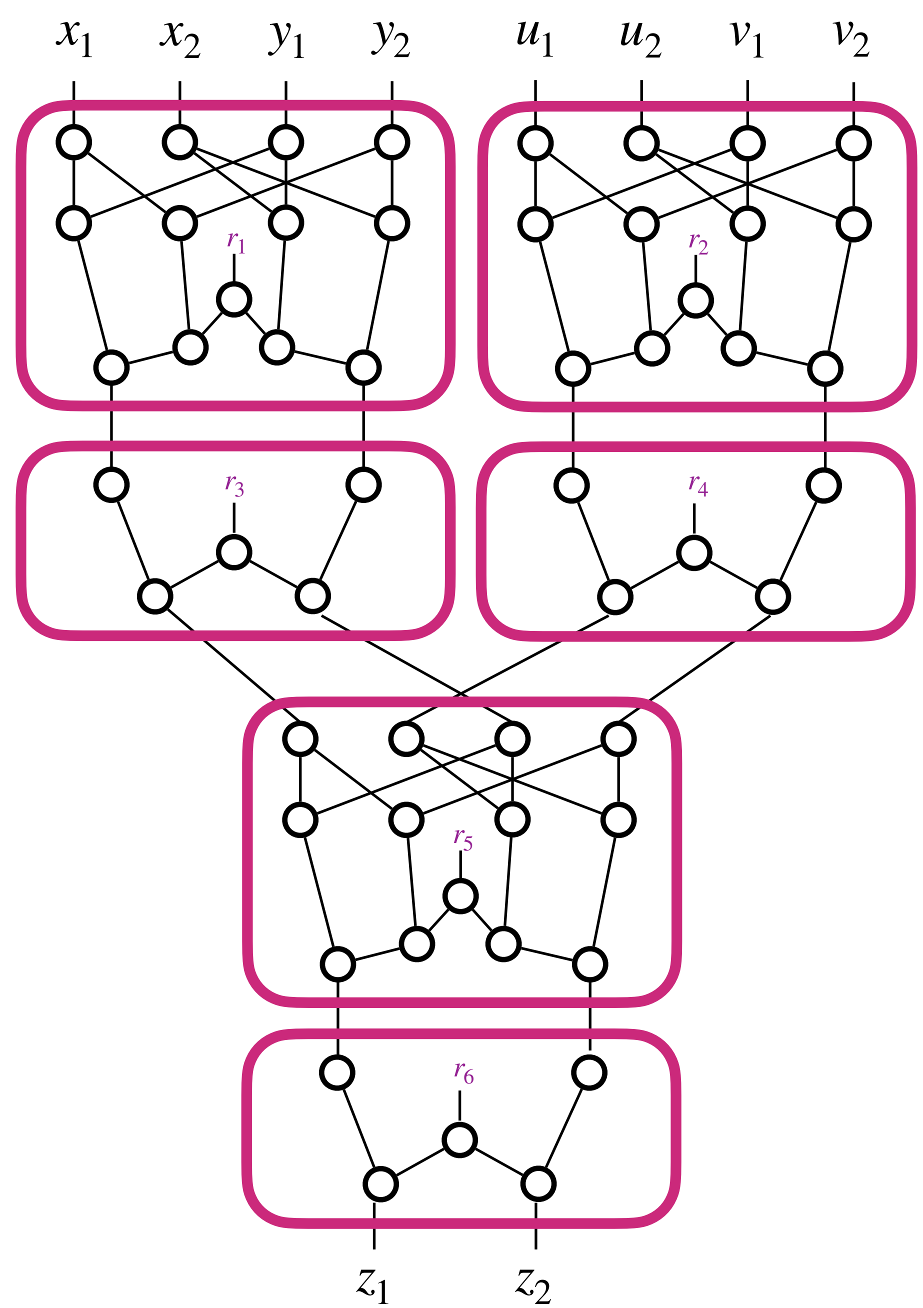
Cardinal RPC

Cassiers • Faust • Orlt • Standaert
CRYPTO 2021

$(p, \mathscr{E})$-cardinal RPC:

For all t^i, t^o, leakage and t^o output shares can be perfectly simulated with exactly t^i input shares with probability $\leq \mathscr{E}_{t^o}(t^i)$



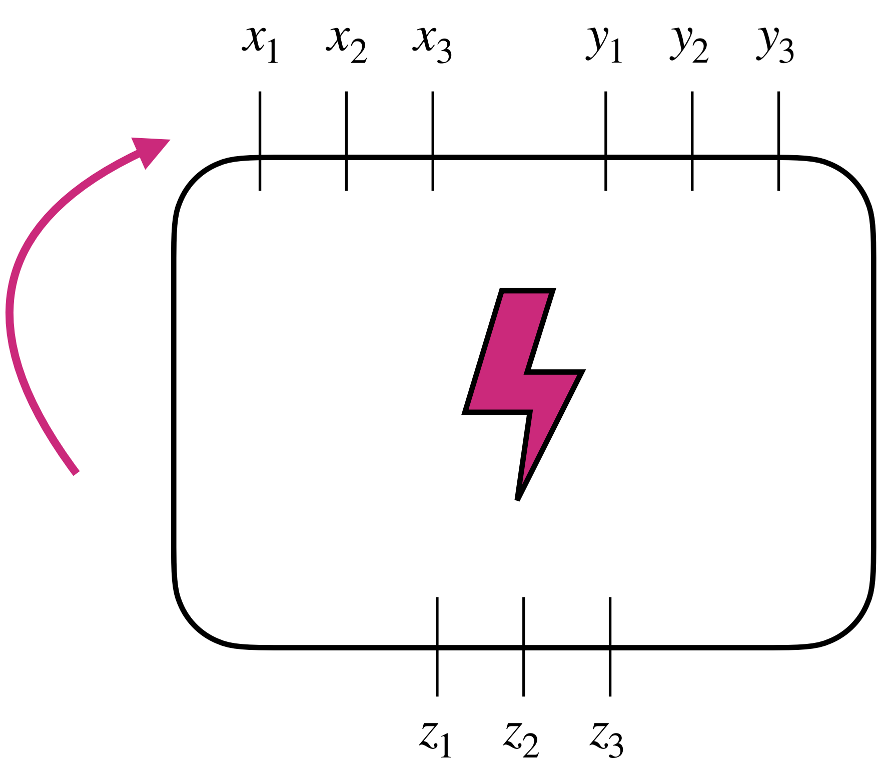


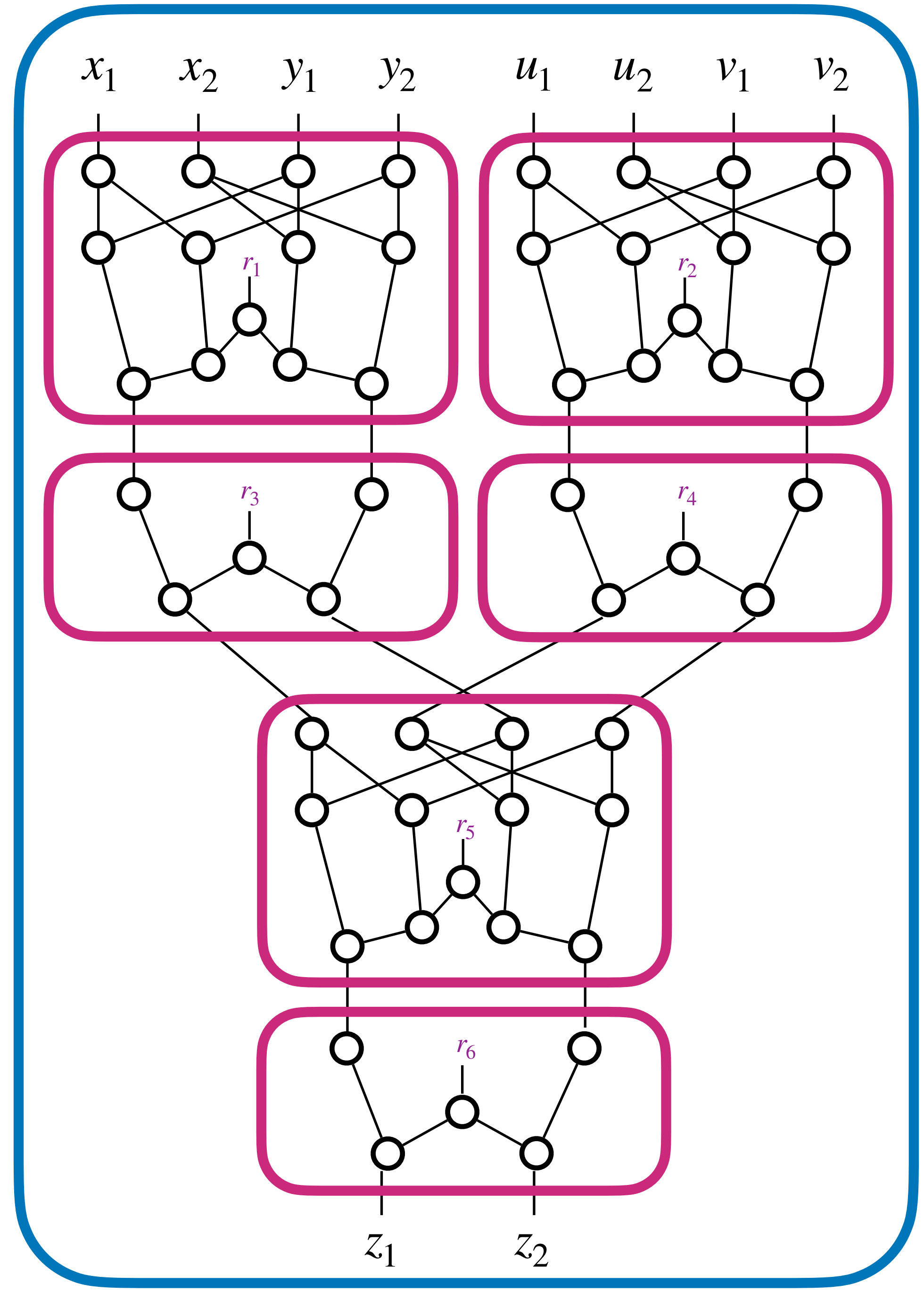
Cardinal RPC

Cardinal RPC

Cassiers • Faust • Orlt • Standaert
CRYPTO 2021

Cardinal RPC
⇒ Random Probing Security





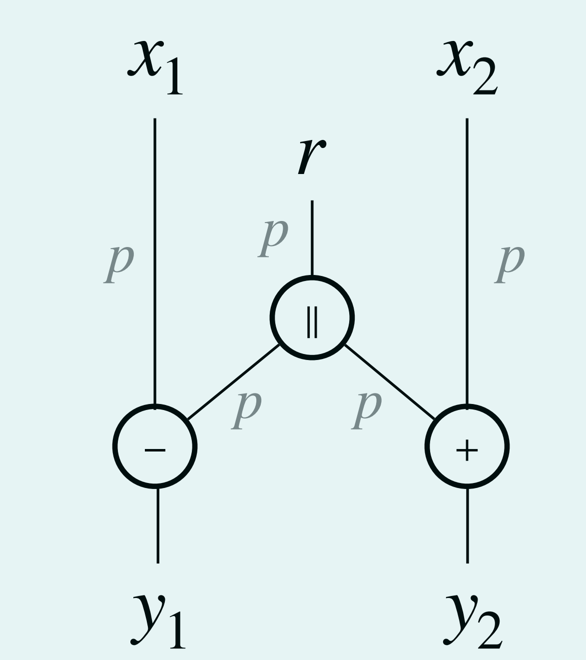
Cardinal RPC

Cardinal RPC

Belaïd • Rivain • Rossi
EUROCRYPT 2025
Cardinal RPC
My Work

	$\varnothing$	y_1	y_2	(y_1, y_2)
$\varnothing$	$(1-p)^2$	$(1-p)^5$	$(1-p)^5$	0
x_1	$p(1-p)$	$(1-p) \cdot (1-(1-p)^4)$	$p(1-p)^4$	0
x_2	$p(1-p)$	$p(1-p)^4$	$(1-p) \cdot (1-(1-p)^4)$	0
(x_1, x_2)	p^2	$p \cdot (1-(1-p)^4)$	$p \cdot (1-(1-p)^4)$	1

	0	1	2
0	$(1-p)^2$	$(1-p)^5$	0
1	$2p(1-p)$	$p(1-p)^4 + (1-p) \cdot (1-(1-p)^4)$	0
2	p^2	$p \cdot (1-(1-p)^4)$	1



Example

Uniformly Cardinal RPC

	$\varnothing$	y_1	y_2	(y_1, y_2)
$\varnothing$	$(1-p)^2$	$(1-p)^5$	$(1-p)^5$	0
x_1	$p(1-p)$	$(1-p) \cdot (1-(1-p)^4)$	$p(1-p)^4$	0
x_2	$p(1-p)$	$p(1-p)^4$	$(1-p) \cdot (1-(1-p)^4)$	0
(x_1, x_2)	p^2	$p \cdot (1-(1-p)^4)$	$p \cdot (1-(1-p)^4)$	1

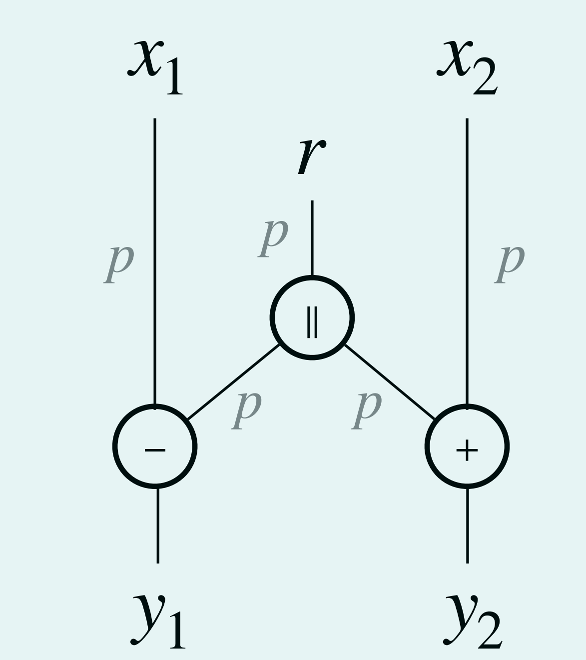
	0	1	2
0	$(1-p)^2$	$(1-p)^5$	0
1	$2p(1-p)$	$p(1-p)^4 + (1-p) \cdot (1-(1-p)^4)$	0
2	p^2	$p \cdot (1-(1-p)^4)$	1

Belaïd • Normand • Rivain

ASIACRYPT 2025

Uniformly Cardinal RPC

My Work

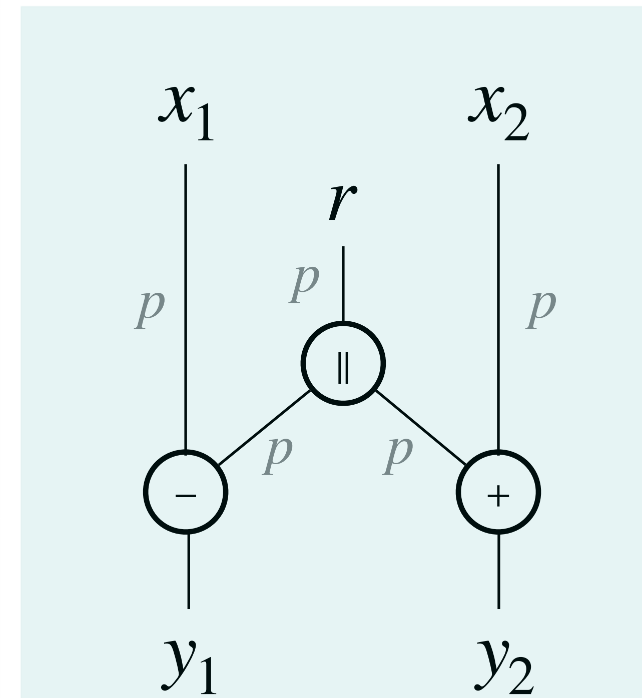


Example

Uniformly Cardinal RPC

Belaïd • Normand • Rivain
ASIACRYPT 2025
Uniformly Cardinal RPC
My Work

	$\varnothing$	y_1	y_2	(y_1, y_2)
$\varnothing$	$(1-p)^2$	$(1-p)^5$	$(1-p)^5$	0
x_1	$p(1-p)$	$(1-p)\cdot(1-(1-p)^4)$	$p(1-p)^4$	0
x_2	$p(1-p)$	$p(1-p)^4$	$(1-p)\cdot(1-(1-p)^4)$	0
(x_1, x_2)	p^2	$p\cdot(1-(1-p)^4)$	$p\cdot(1-(1-p)^4)$	1



Example

	0	1	2
0	$(1-p)^2$	$(1-p)^5$	0
1	$2p(1-p)$	$p(1-p)^4 + (1-p)\cdot(1-(1-p)^4)$	0
2	p^2	$p\cdot(1-(1-p)^4)$	1

Uniformly Cardinal RPC:

Uniformly Input RPC (UI)

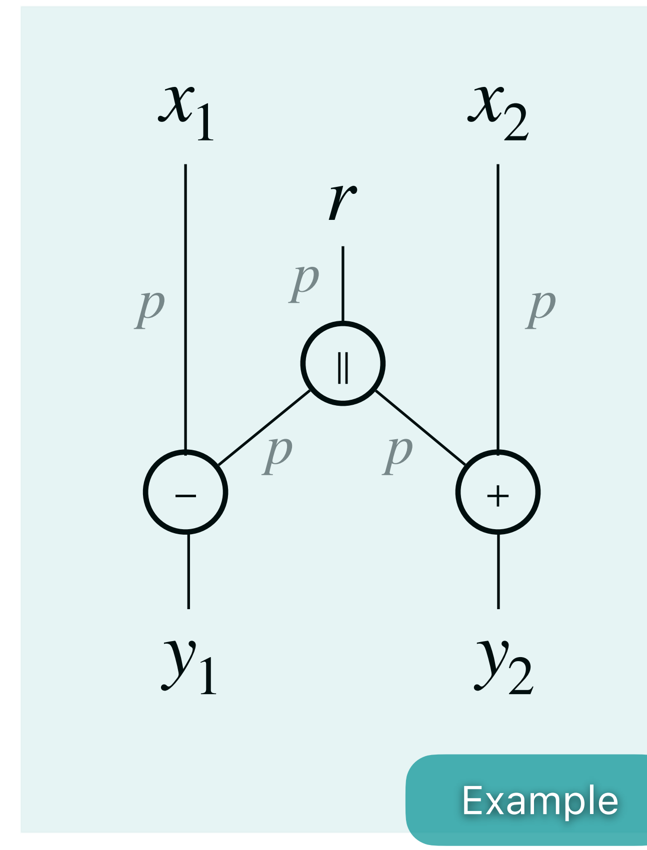
+

Uniformly Output RPC (UO)

Uniformly Cardinal RPC

Belaïd • Normand • Rivain
ASIACRYPT 2025
Uniformly Cardinal RPC
My Work

	$\varnothing$	y_1	y_2	(y_1, y_2)
$\varnothing$	$(1-p)^2$	$(1-p)^5$	$(1-p)^5$	0
x_1	$p(1-p)$	$(1-p)\cdot(1-(1-p)^4)$	$p(1-p)^4$	0
x_2	$p(1-p)$	$p(1-p)^4$	$(1-p)\cdot(1-(1-p)^4)$	0
(x_1, x_2)	p^2	$p\cdot(1-(1-p)^4)$	$p\cdot(1-(1-p)^4)$	1



	0	1	2
0	$(1-p)^2$	$(1-p)^5$	0
1	$2p(1-p)$	$p(1-p)^4+(1-p)\cdot(1-(1-p)^4)$	0
2	p^2	$p\cdot(1-(1-p)^4)$	1

Uniformly Cardinal RPC:

Uniformly Input RPC (UI)

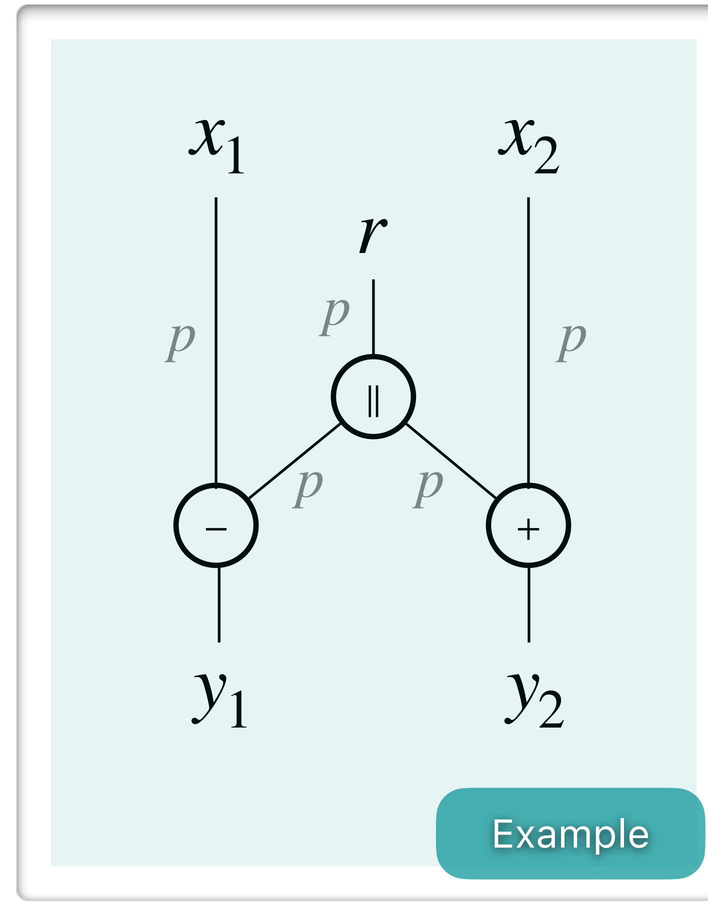
+

Uniformly Output RPC (UO)

Uniformly Cardinal RPC

Belaïd • Normand • Rivain
ASIACRYPT 2025
Uniformly Cardinal RPC
My Work

	$\emptyset$	y_1	y_2	(y_1, y_2)
$\emptyset$	$(1-p)^2$	$(1-p)^5$	$(1-p)^5$	0
x_1	$p(1-p)$	$(1-p)\cdot(1-(1-p)^4)$	$p(1-p)^4$	0
x_2	$p(1-p)$	$p(1-p)^4$	$(1-p)\cdot(1-(1-p)^4)$	0
(x_1, x_2)	p^2	$p\cdot(1-(1-p)^4)$	$p\cdot(1-(1-p)^4)$	1



	0	1	2
0	$(1-p)^2$	$(1-p)^5$	0
1	$2p(1-p)$	$p(1-p)^4 + (1-p)\cdot(1-(1-p)^4)$	0
2	p^2	$p\cdot(1-(1-p)^4)$	1

<u>Uniformly Cardinal RPC:</u>

Uniformly Input RPC (UI)

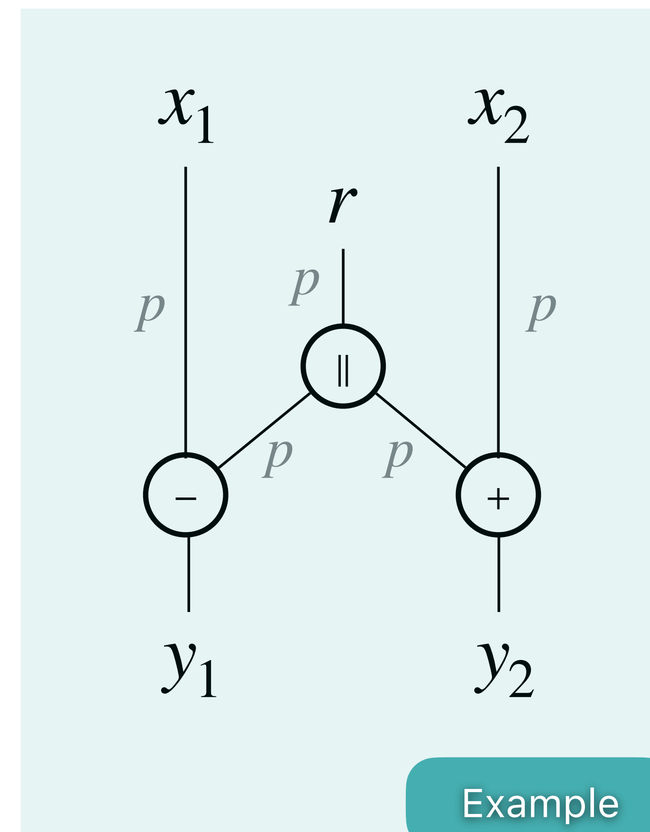
+

Uniformly Output RPC (UO)

Uniformly Cardinal RPC

Belaïd • Normand • Rivain
ASIACRYPT 2025
Uniformly Cardinal RPC
My Work

	$\varnothing$	y_1	y_2	(y_1, y_2)
$\varnothing$	$(1-p)^2$	$(1-p)^5$	$(1-p)^5$	0
x_1	$p(1-p)$	$(1-p)\cdot(1-(1-p)^4)$	$p(1-p)^4$	0
x_2	$p(1-p)$	$p(1-p)^4$	$(1-p)\cdot(1-(1-p)^4)$	0
(x_1, x_2)	p^2	$p\cdot(1-(1-p)^4)$	$p\cdot(1-(1-p)^4)$	1



	0	1	2
0	$(1-p)^2$	$(1-p)^5$	0
1	$2p(1-p)$	$p(1-p)^4 + (1-p)\cdot(1-(1-p)^4)$	0
2	p^2	$p\cdot(1-(1-p)^4)$	1

Uniformly Cardinal RPC:

Uniformly Input RPC (UI)

+

Uniformly Output RPC (UO)

Uniformly Cardinal RPC

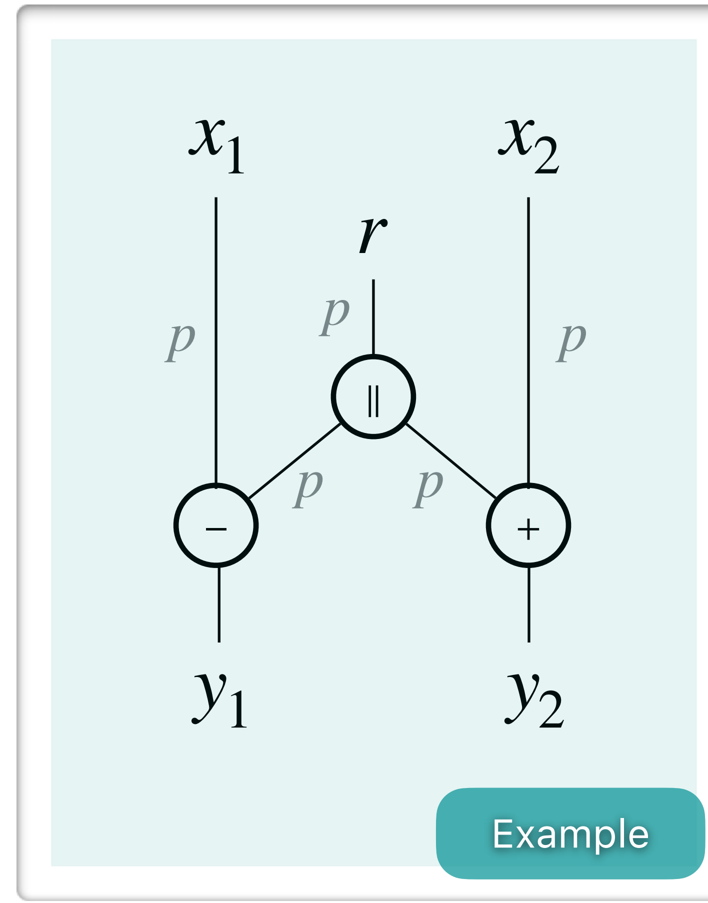
Belaïd • Normand • Rivain

ASIACRYPT 2025

Uniformly Cardinal RPC

My Work

	$\varnothing$	y_1	y_2	(y_1, y_2)
$\varnothing$	$(1-p)^2$	$(1-p)^5$	$(1-p)^5$	0
x_1	$p(1-p)$	$(1-p)\cdot(1-(1-p)^4)$	$p(1-p)^4$	0
x_2	$p(1-p)$	$p(1-p)^4$	$(1-p)\cdot(1-(1-p)^4)$	0
(x_1, x_2)	p^2	$p\cdot(1-(1-p)^4)$	$p\cdot(1-(1-p)^4)$	1



	0	1	2
0	$(1-p)^2$	$(1-p)^5$	0
1	$2p(1-p)$	$p(1-p)^4+(1-p)\cdot(1-(1-p)^4)$	0
2	p^2	$p\cdot(1-(1-p)^4)$	1

Uniformly Cardinal RPC:

Uniformly Input RPC (UI)

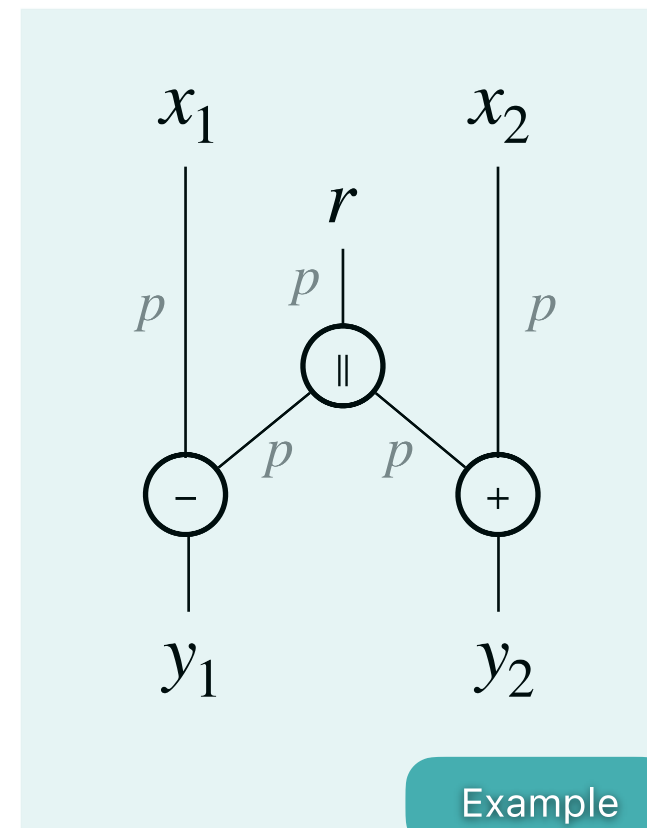
+

Uniformly Output RPC (UO)

Uniformly Cardinal RPC

Belaïd • Normand • Rivain
ASIACRYPT 2025
Uniformly Cardinal RPC
My Work

	$\varnothing$	y_1	y_2	(y_1, y_2)
$\varnothing$	$(1-p)^2$	$(1-p)^5$	$(1-p)^5$	0
x_1	$p(1-p)$	$(1-p)\cdot(1-(1-p)^4)$	$p(1-p)^4$	0
x_2	$p(1-p)$	$p(1-p)^4$	$(1-p)\cdot(1-(1-p)^4)$	0
(x_1, x_2)	p^2	$p\cdot(1-(1-p)^4)$	$p\cdot(1-(1-p)^4)$	1



	0	1	2
0	$(1-p)^2$	$(1-p)^5$	0
1	$2p(1-p)$	$p(1-p)^4+(1-p)\cdot(1-(1-p)^4)$	0
2	p^2	$p\cdot(1-(1-p)^4)$	1

Uniformly Cardinal RPC:

Uniformly Input RPC (UI)

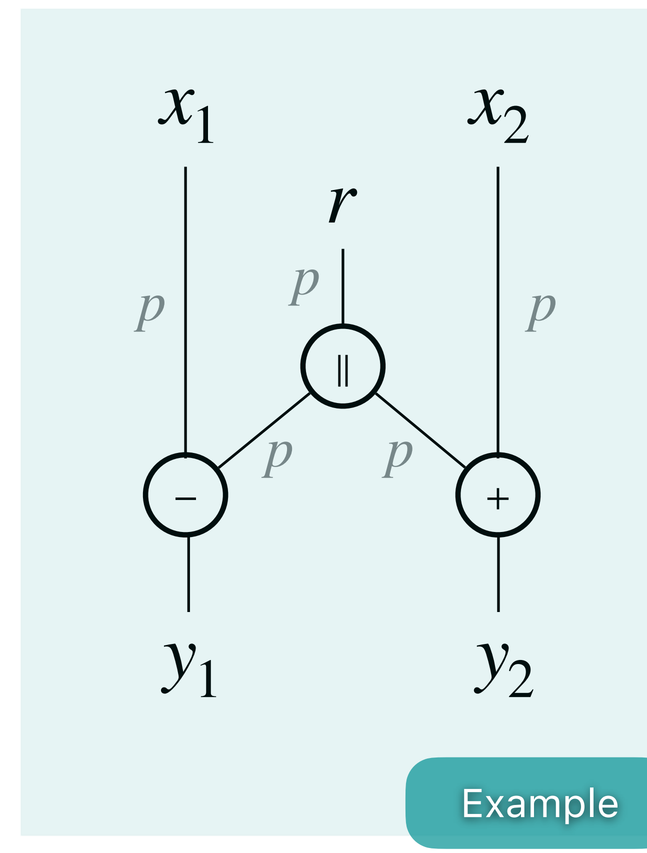
+

Uniformly Output RPC (UO)

Uniformly Cardinal RPC

Belaïd • Normand • Rivain
ASIACRYPT 2025
Uniformly Cardinal RPC
My Work

	$\varnothing$	y_1	y_2	(y_1, y_2)
$\varnothing$	$(1-p)^2$	$(1-p)^5$	$(1-p)^5$	0
x_1	$p(1-p)$	$(1-p)\cdot(1-(1-p)^4)$	$p(1-p)^4$	0
x_2	$p(1-p)$	$p(1-p)^4$	$(1-p)\cdot(1-(1-p)^4)$	0
(x_1, x_2)	p^2	$p\cdot(1-(1-p)^4)$	$p\cdot(1-(1-p)^4)$	1



	0	1	2
0	$(1-p)^2$	$(1-p)^5$	0
1	$2p(1-p)$	$p(1-p)^4+(1-p)\cdot(1-(1-p)^4)$	0
2	p^2	$p\cdot(1-(1-p)^4)$	1

Uniformly Cardinal RPC:

Uniformly Input RPC (UI)

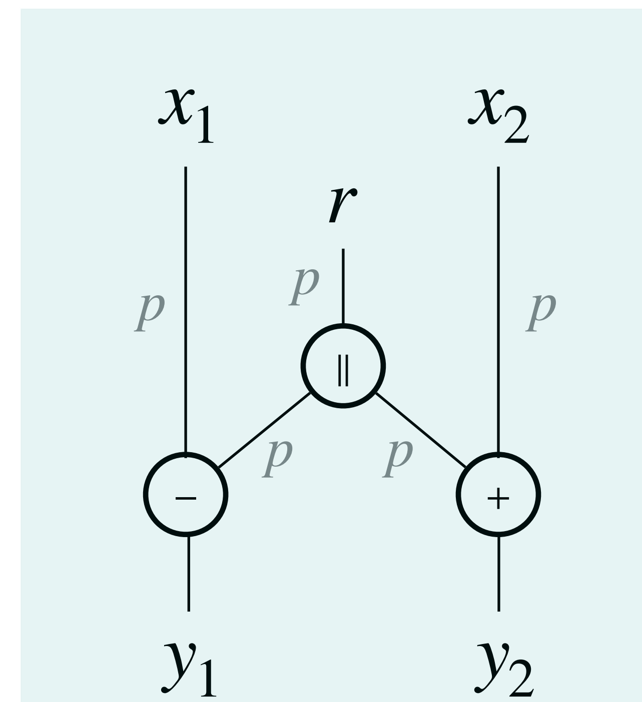
+

Uniformly Output RPC (UO)

Uniformly Cardinal RPC

Belaïd • Normand • Rivain
ASIACRYPT 2025
Uniformly Cardinal RPC
My Work

	$\varnothing$	y_1	y_2	(y_1, y_2)
$\varnothing$	$(1-p)^2$	$(1-p)^5$	$(1-p)^5$	0
x_1	$p(1-p)$	$(1-p)\cdot(1-(1-p)^4)$	$p(1-p)^4$	0
x_2	$p(1-p)$	$p(1-p)^4$	$(1-p)\cdot(1-(1-p)^4)$	0
(x_1, x_2)	p^2	$p\cdot(1-(1-p)^4)$	$p\cdot(1-(1-p)^4)$	1



Example

	0	1	2
0	$(1-p)^2$	$(1-p)^5$	0
1	$2p(1-p)$	$p(1-p)^4+(1-p)\cdot(1-(1-p)^4)$	0
2	p^2	$p\cdot(1-(1-p)^4)$	1

Uniformly Cardinal RPC:

Uniformly Input RPC (UI)

+

Uniformly Output RPC (UO)

Uniformly Cardinal RPC

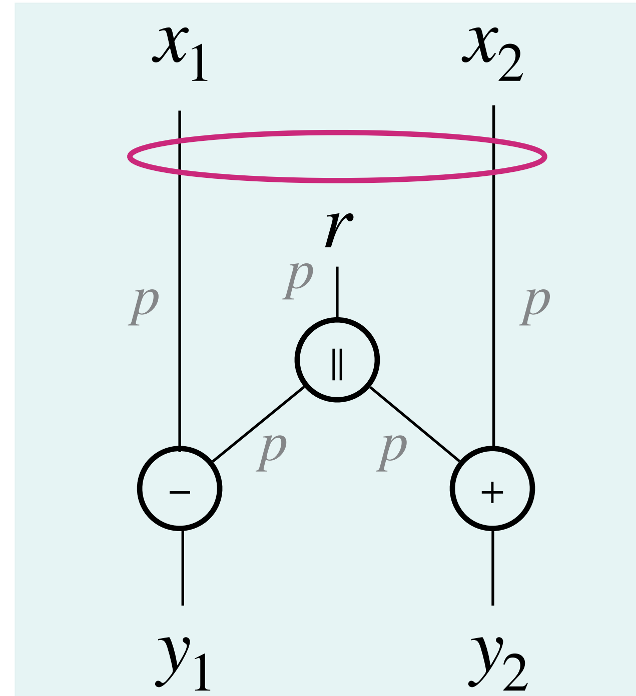
Belaïd • Normand • Rivain

ASIACRYPT 2025

Uniformly Cardinal RPC

My Work

	$\varnothing$	y_1	y_2	(y_1, y_2)
$\varnothing$	$(1-p)^2$	$(1-p)^5$	$(1-p)^5$	0
x_1	$p(1-p)$	p'	p'	0
x_2	$p(1-p)$	p'	p'	0
(x_1, x_2)	p^2	$p \cdot (1-(1-p)^4)$	$p \cdot (1-(1-p)^4)$	1



Example

	0	1	2
0	$(1-p)^2$	$(1-p)^5$	0
1	$2p(1-p)$	$2 \cdot p'$	0
2	p^2	$p \cdot (1-(1-p)^4)$	1

$$p' = \frac{(1-p)\cdot(1-(1-p)^4) + p(1-p)^4}{2}$$

Uniformly Cardinal RPC:

Uniformly Input RPC (UI)

+

Uniformly Output RPC (UO)

Contributions

Foundations

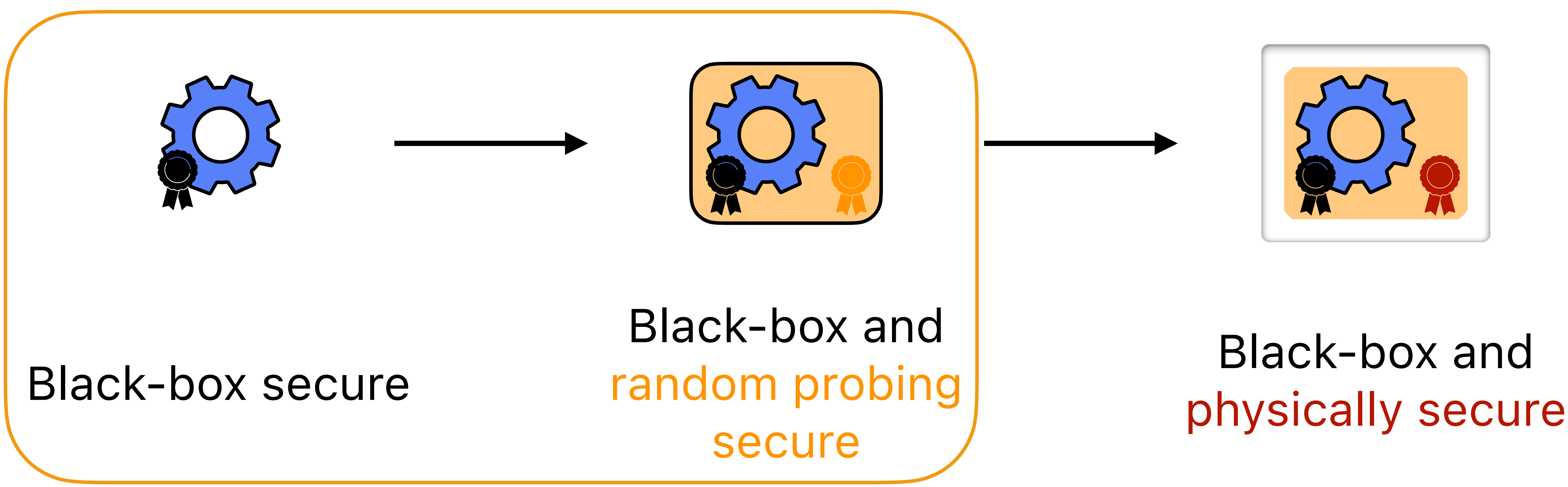
Random probing security & verification (small circuits)

Scaling up

Composition frameworks (larger circuits)

Building blocks

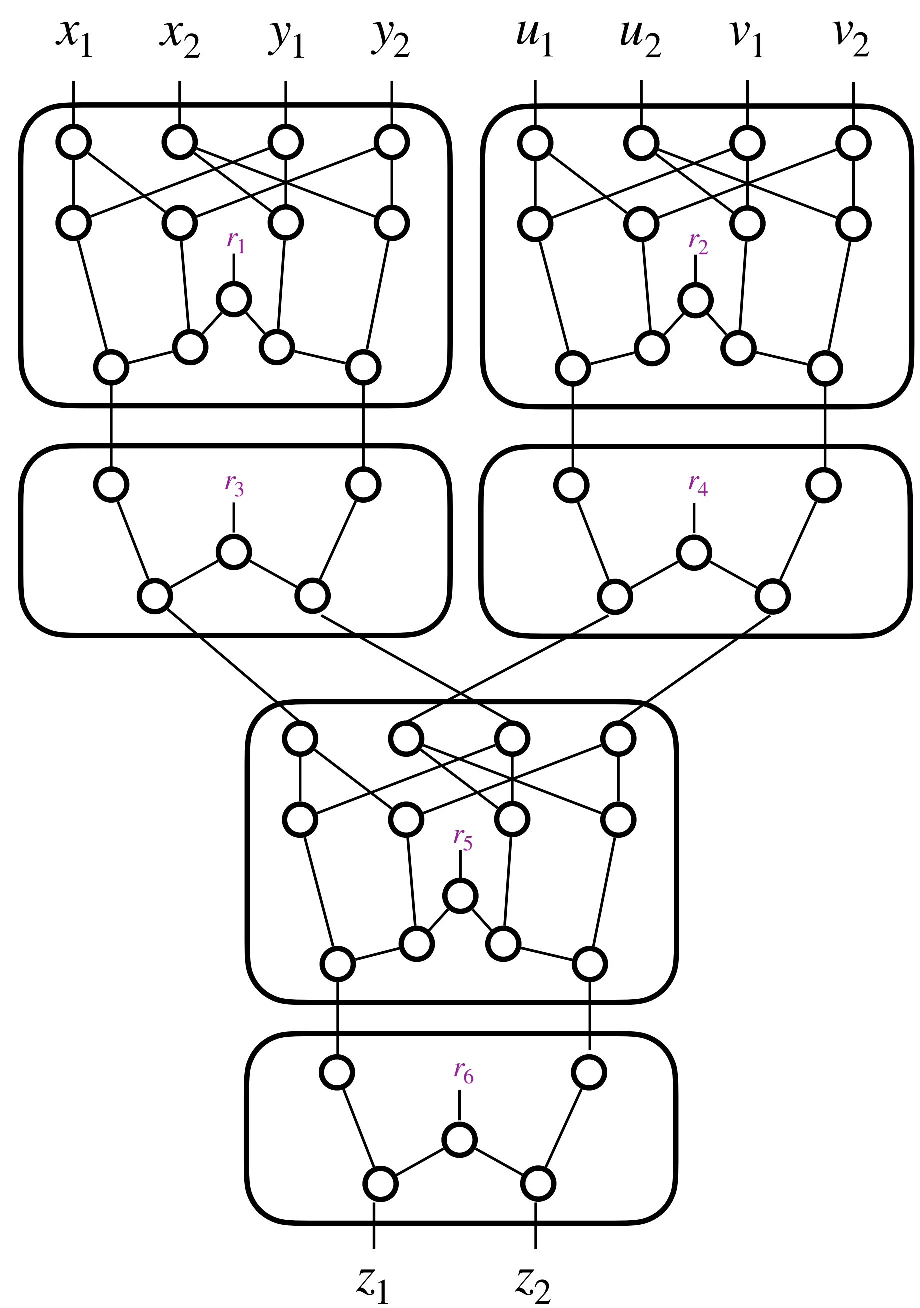
Design of efficient gadgets



Composition

Belaïd • Rivain • Rossi
EUROCRYPT 2025
Belaïd • Normand • Rivain
ASIACRYPT 2025
(Uniformly) cardinal RPC
framework + gadgets
My Work

Toolbox:
- Linear gadgets
- Non-linear gadgets
- Refresh gadgets

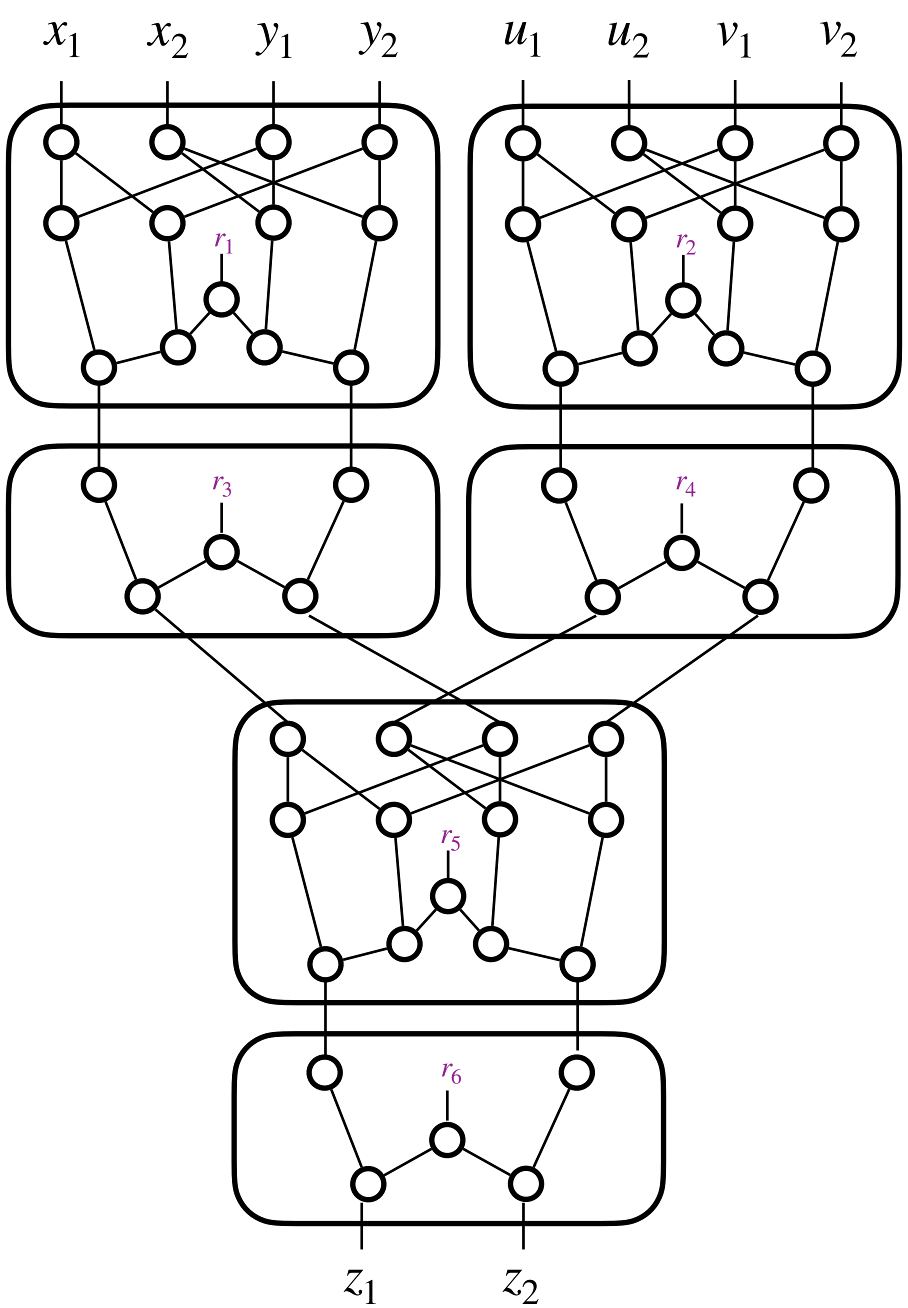


Composition

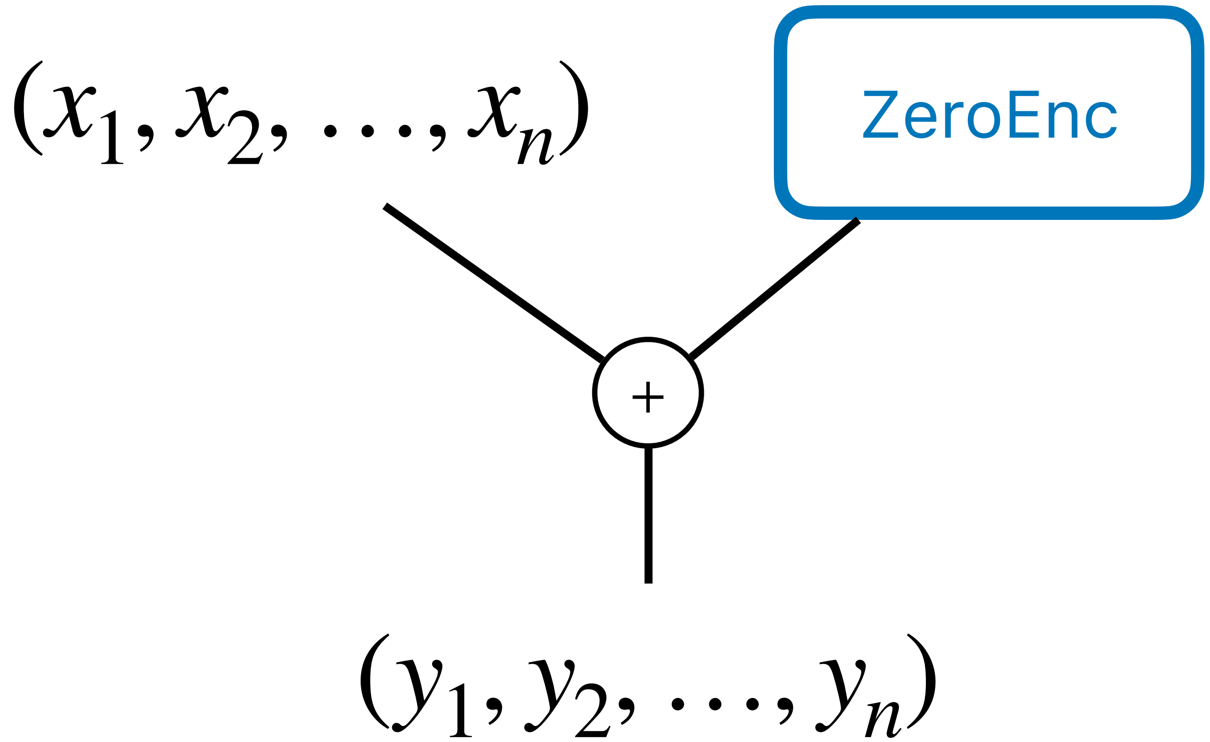
Belaïd • Rivain • Rossi
EUROCRYPT 2025
Belaïd • Normand • Rivain
ASIACRYPT 2025
(Uniformly) cardinal RPC
framework + gadgets
My Work

Toolbox:

- Linear gadgets
- Non-linear gadgets
- Refresh gadgets



Refresh Gadget



$$y_1 + y_2 + \ldots + y_n = x_1 + x_2 + \ldots + x_n$$

RPZeroEnc

1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0

RPZeroEnc

Belaïd • Rivain • Rossi
EUROCRYPT 2025
My Work

1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0

1st iteration: $r_1 \leftarrow \$, \quad (i_1, j_1) \leftarrow \$$ (example : $i_1 = 3,\ j_1 = 7$)

RPZeroEnc

1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0

1st iteration: $r_1 \leftarrow \$, \quad (i_1, j_1) \leftarrow \$ \qquad (\text{example}: i_1 = 3,\ j_1 = 7)$

1	2	3	4	5	6	7	8
0	0	r_1	0	0	0	$-r_1$	0

RPZeroEnc

Belaïd • Rivain • Rossi
EUROCRYPT 2025
My Work

1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0

1st iteration: $r_1 \leftarrow \$, \quad (i_1, j_1) \leftarrow \$ \qquad (\text{example} : i_1 = 3,\ j_1 = 7)$

1	2	3	4	5	6	7	8
0	0	r_1	0	0	0	$-r_1$	0

2nd iteration: $r_2 \leftarrow \$, \quad (i_2, j_2) \leftarrow \$ \qquad (\text{example} : i_2 = 1,\ j_2 = 8)$

1	2	3	4	5	6	7	8
r_2	0	r_1	0	0	0	$-r_1$	$-r_2$

RPZeroEnc

1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0

1st iteration: $r_1 \leftarrow \$, \quad (i_1, j_1) \leftarrow \$$ (example : $i_1 = 3,\ j_1 = 7$)

1	2	3	4	5	6	7	8
0	0	r_1	0	0	0	$-r_1$	0

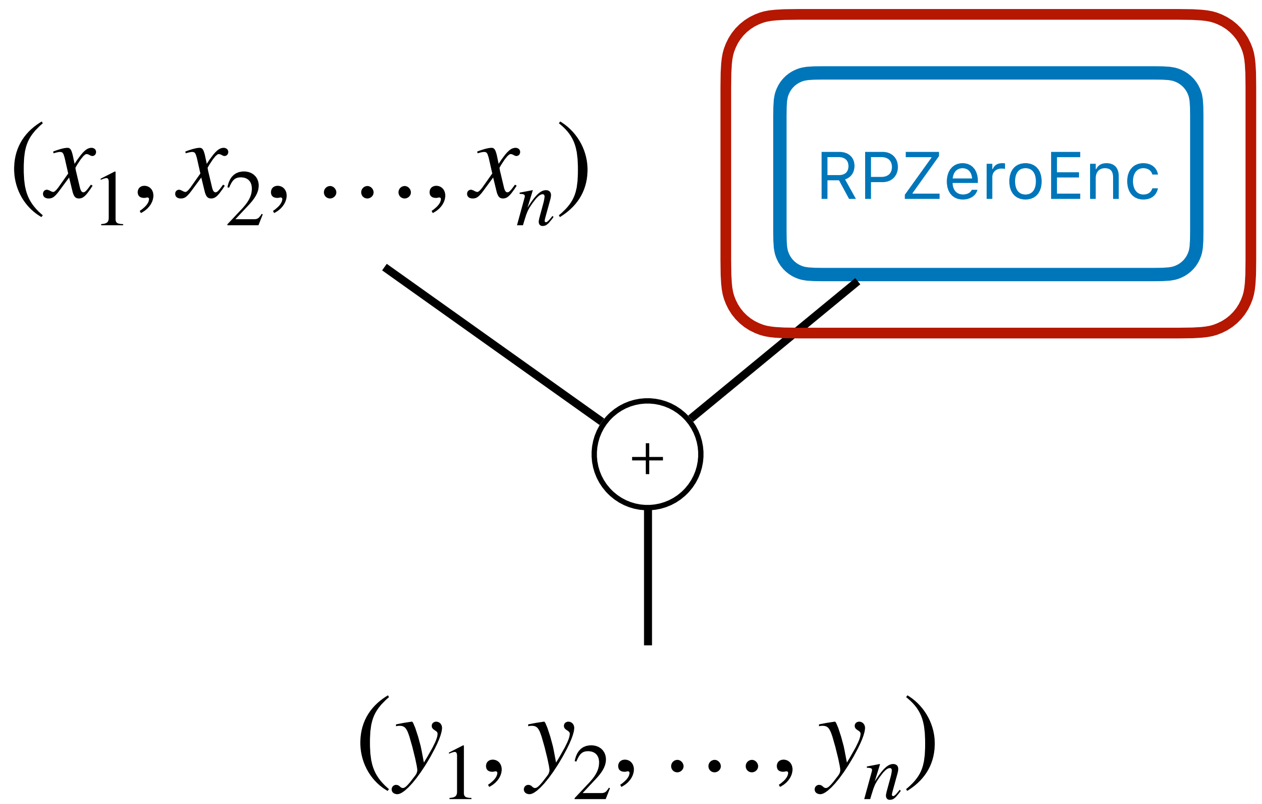
2nd iteration: $r_2 \leftarrow \$, \quad (i_2, j_2) \leftarrow \$$ (example : $i_2 = 1,\ j_2 = 8$)

1	2	3	4	5	6	7	8
r_2	0	r_1	0	0	0	$-r_1$	$-r_2$

3rd iteration: $r_3 \leftarrow \$, \quad (i_3, j_3) \leftarrow \$$ (example : $i_3 = 2,\ j_3 = 3$)

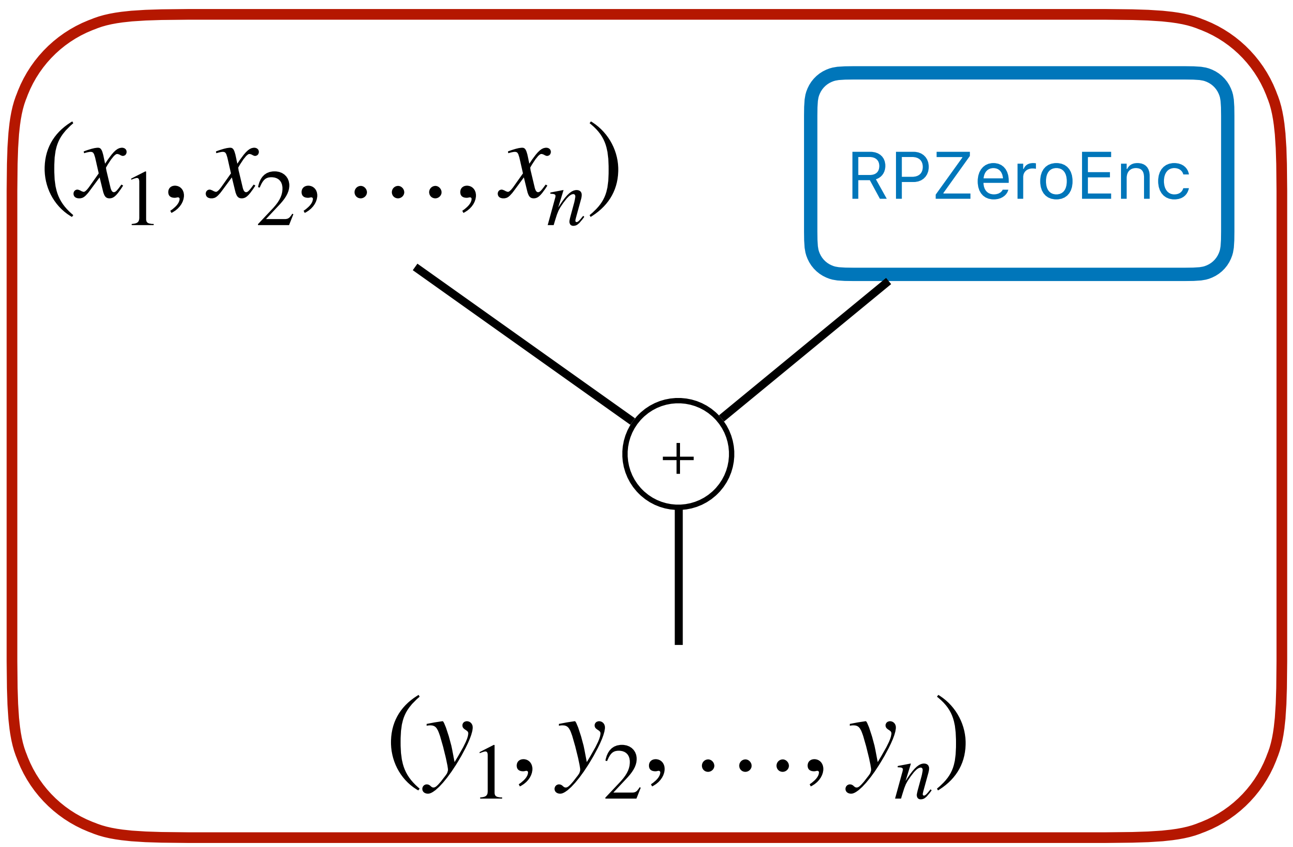
1	2	3	4	5	6	7	8
r_2	r_3	$r_1 - r_3$	0	0	0	$-r_1$	$-r_2$

Refresh Gadget



RPRefresh is cardinal RPC

Refresh Gadget

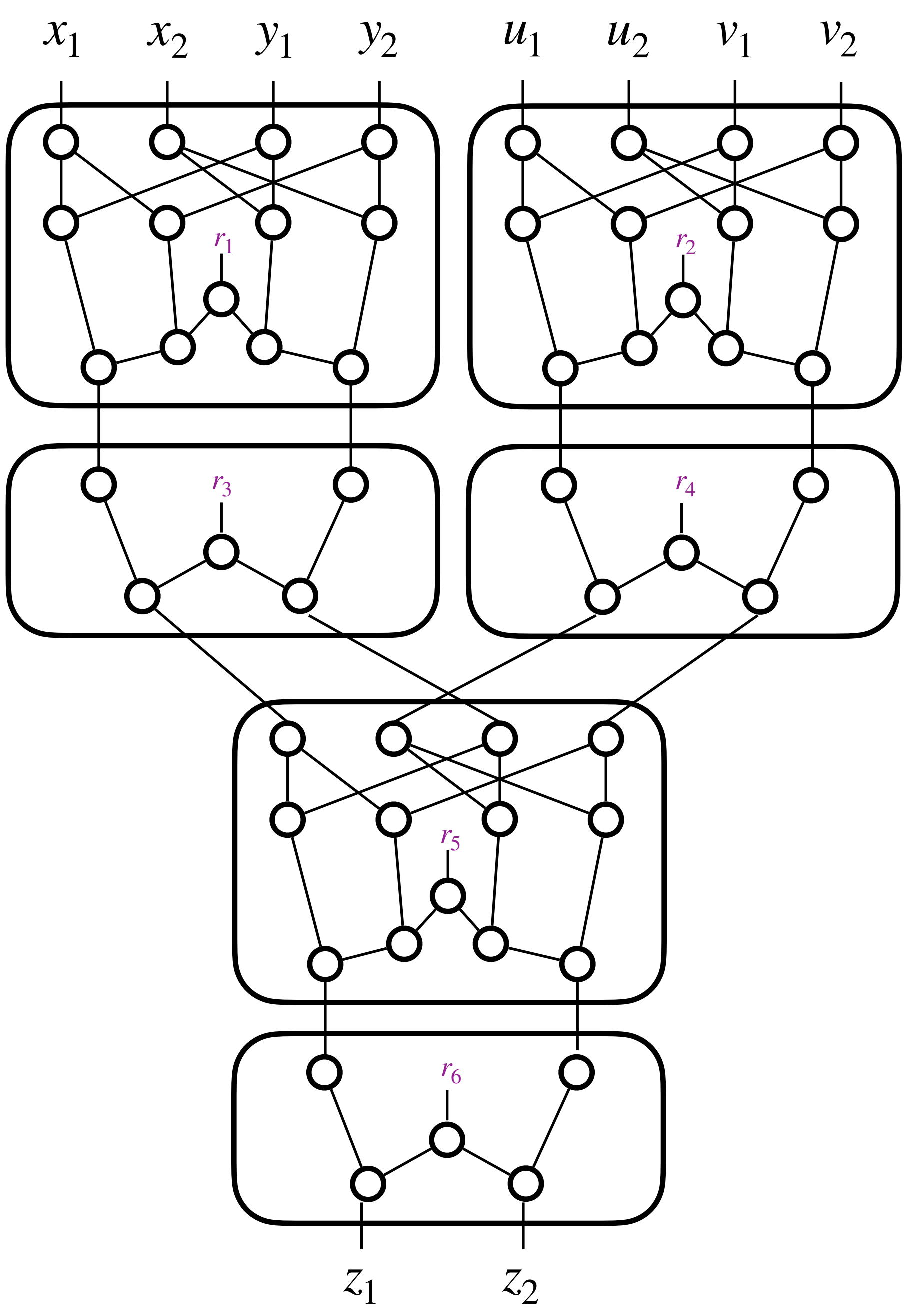


RPRefresh is cardinal RPC

Composition

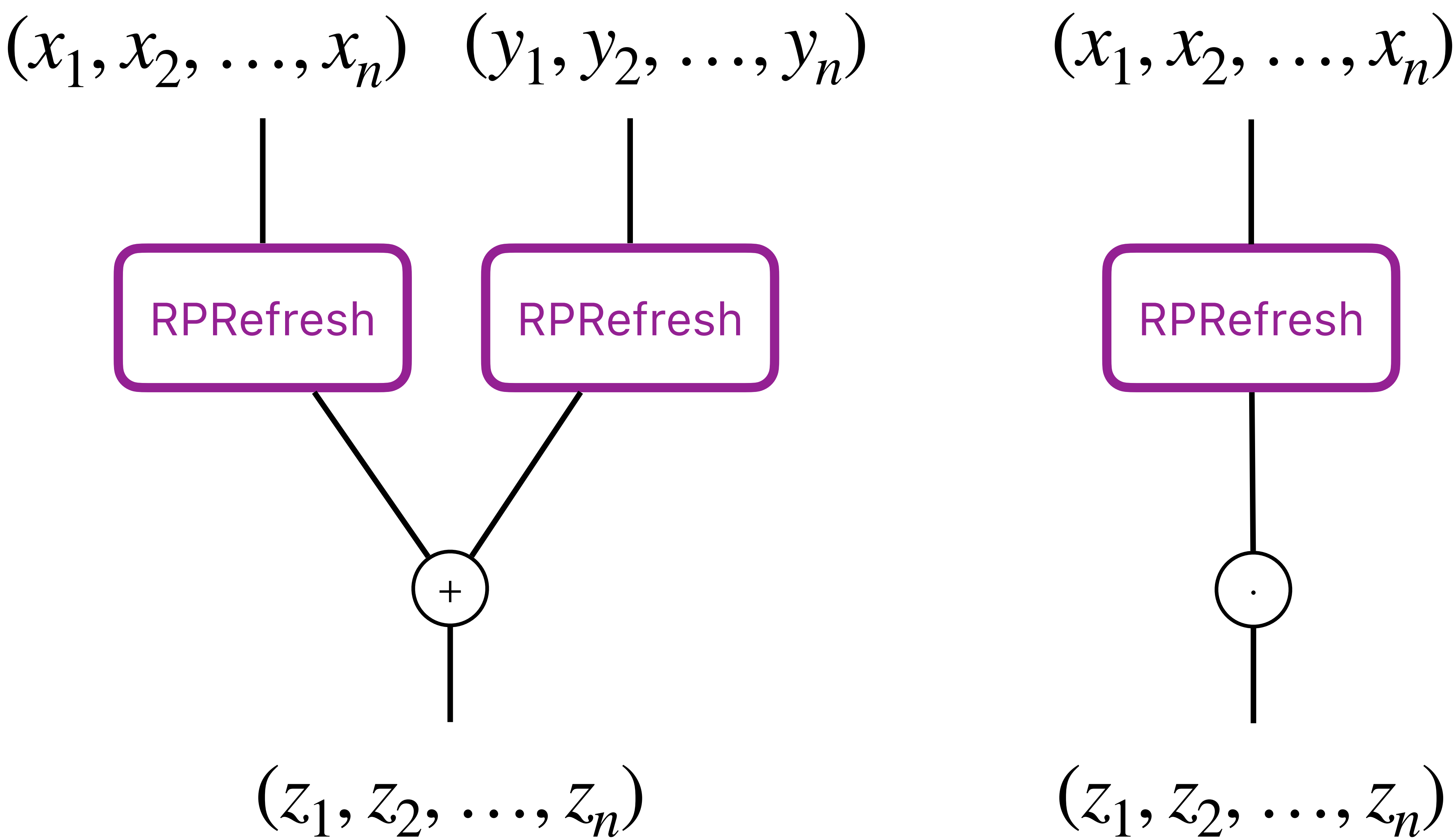
Belaïd • Rivain • Rossi
EUROCRYPT 2025
Belaïd • Normand • Rivain
ASIACRYPT 2025
(Uniformly) cardinal RPC
framework + gadgets
My Work

Toolbox:
- Linear gadgets
- Non-linear gadgets
- Refresh gadgets



Linear Gadgets

Belaïd • Rivain • Rossi
EUROCRYPT 2025
My Work



Composition

Belaïd • Rivain • Rossi

EUROCRYPT 2025

Belaïd • Normand • Rivain

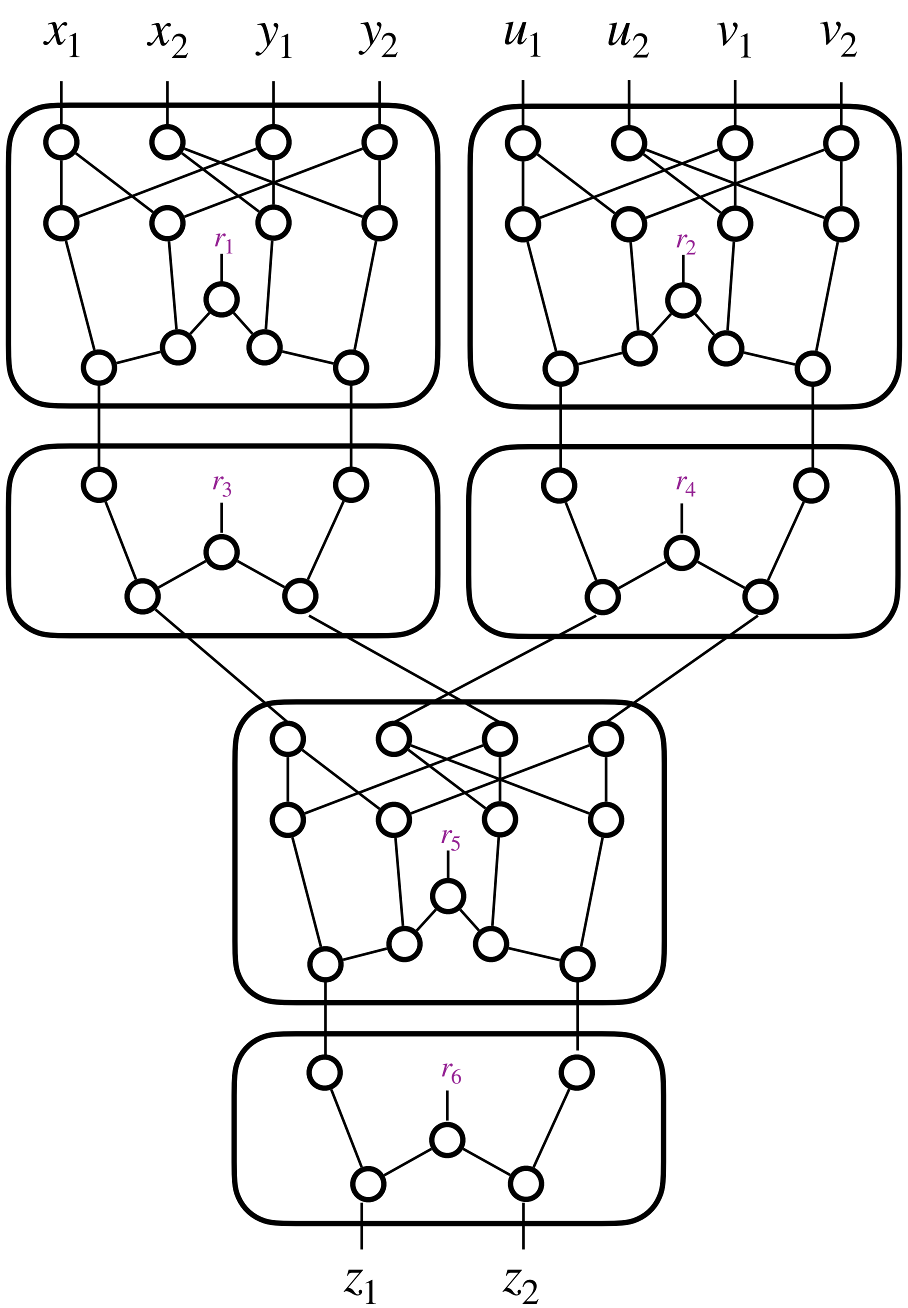
ASIACRYPT 2025

(Uniformly) cardinal RPC
framework + gadgets

My Work

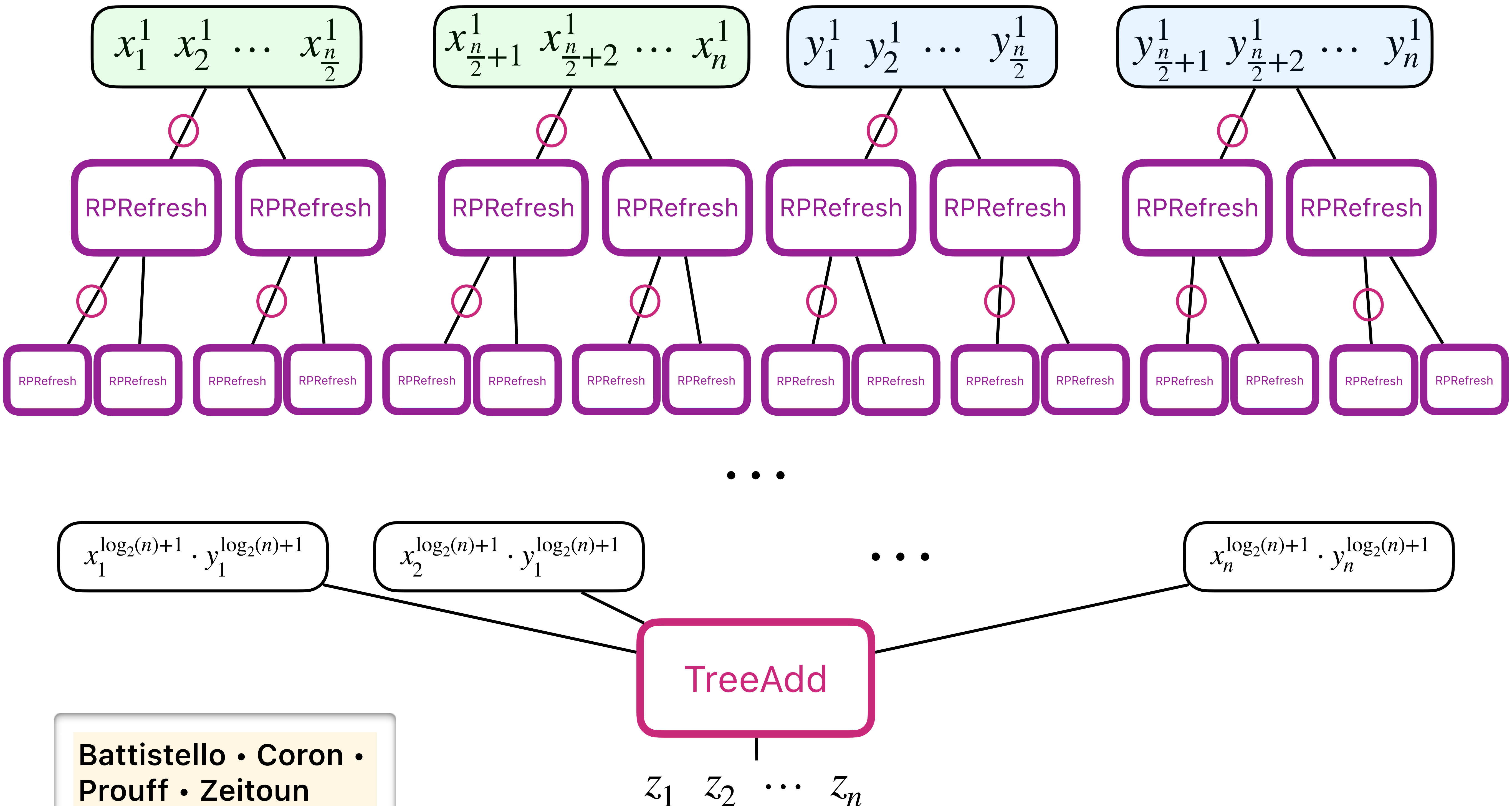
Toolbox:

- Linear gadgets ✓
- Non-linear gadgets
- Refresh gadgets ✓



Multiplication Gadget

Belaïd • Normand • Rivain
ASIACRYPT 2025
My Work



Battistello • Coron • Prouff • Zeitoun
CHES 2016

Composition

Belaïd • Rivain • Rossi

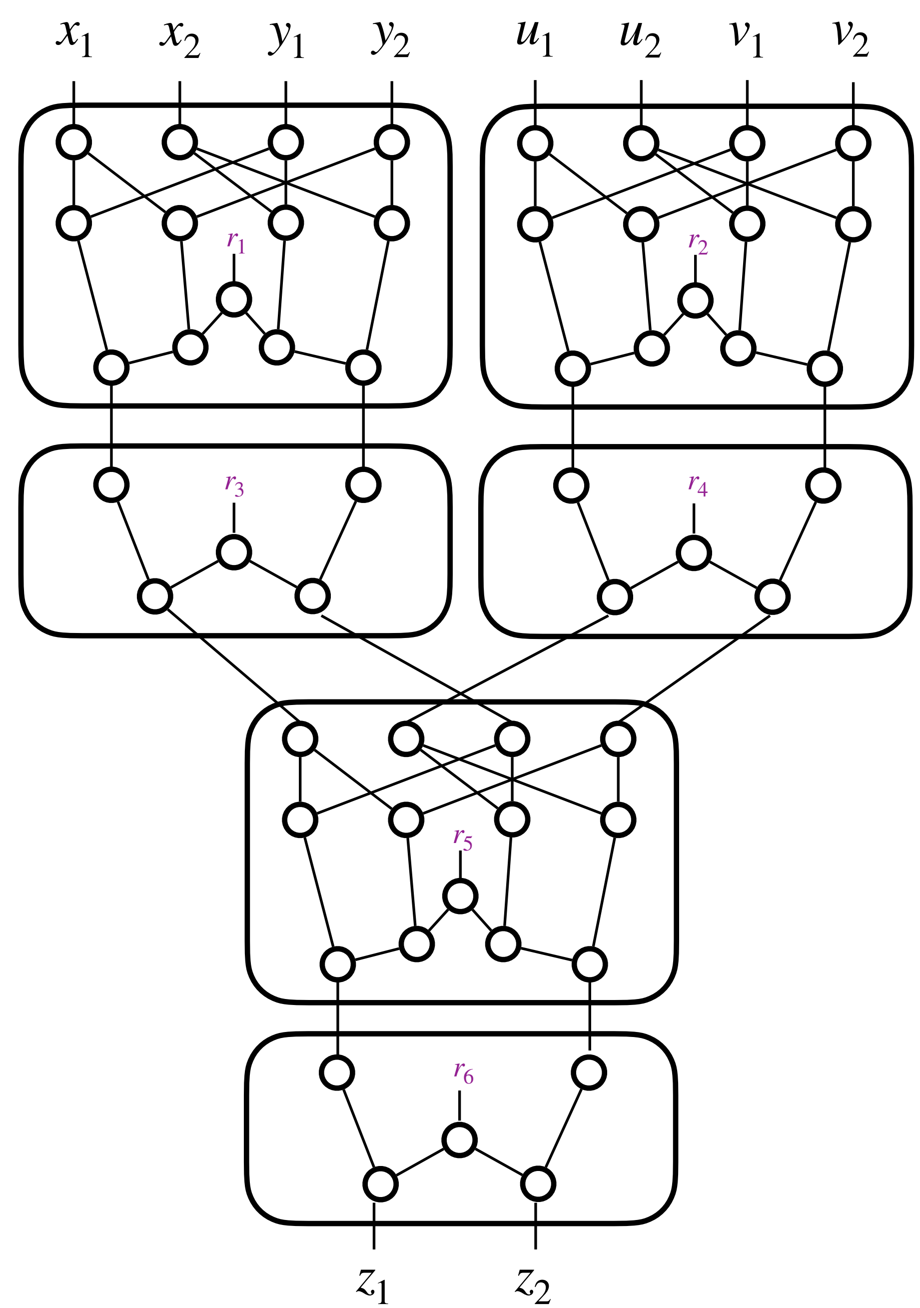
EUROCRYPT 2025

Belaïd • Normand • Rivain

ASIACRYPT 2025

(Uniformly) cardinal RPC
framework + gadgets

My Work



Toolbox:

- Linear gadgets ✓
- Non-linear gadgets ✓
- Refresh gadgets ✓

Composition

Ananth • Ishai • Sahai
CRYPTO 2018
Composition framework with explicit and constant leakage rate

Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020
Threshold RPC
My Work

Cassiers • Faust • Orlt • Standaert
CRYPTO 2021
General RPC (Probe Distribution Tables)

Belaïd • Rivain • Rossi
EUROCRYPT 2025
Cardinal RPC
My Work

Belaïd • Normand • Rivain
ASIACRYPT 2025
Uniformly CRPC
My Work

Composition

Ananth • Ishai • Sahai
CRYPTO 2018
Composition framework with explicit and constant leakage rate

Belaïd • Coron • Prouff • Rivain • Taleb
CRYPTO 2020
Threshold RPC
My Work

Cassiers • Faust • Orlt • Standaert
CRYPTO 2021
General RPC (Probe Distribution Tables)

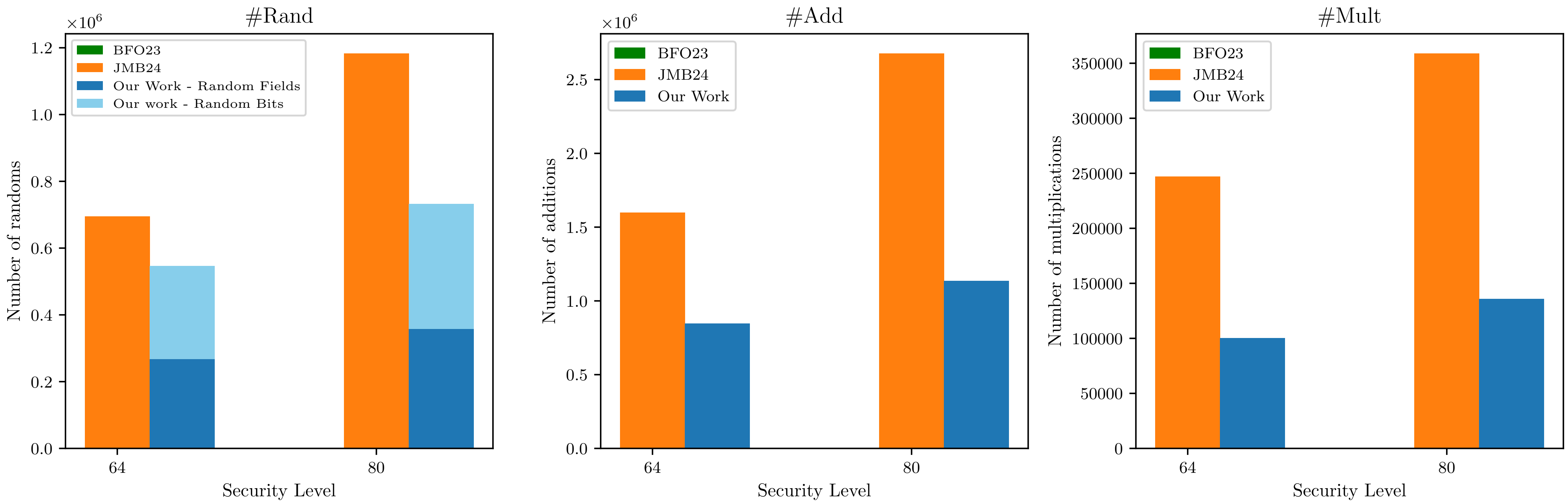
Berti • Faust • Orlt
TCHES 2023
Leakage diagrams
BFO23

Jahandideh • Mennink • Batina
TCHES 2024
Mutual information
JMB24

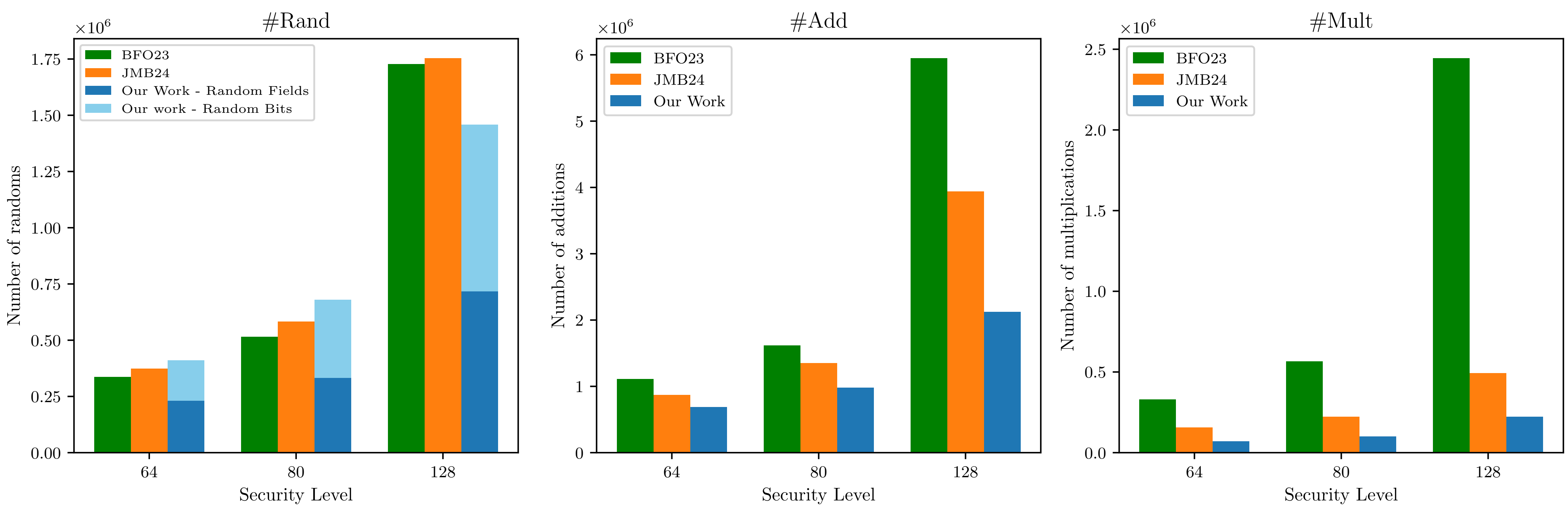
Belaïd • Rivain • Rossi
EUROCRYPT 2025
Cardinal RPC
My Work

Belaïd • Normand • Rivain
ASIACRYPT 2025
Uniformly CRPC
My Work

Application on AES

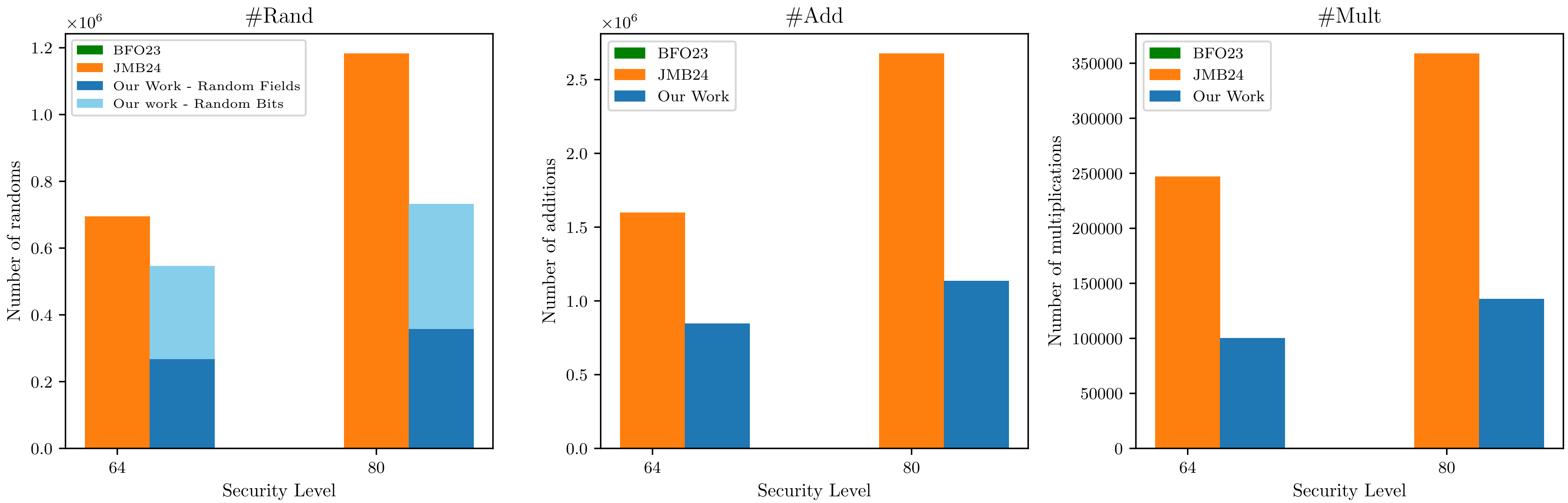


$p = 2^{-16}$

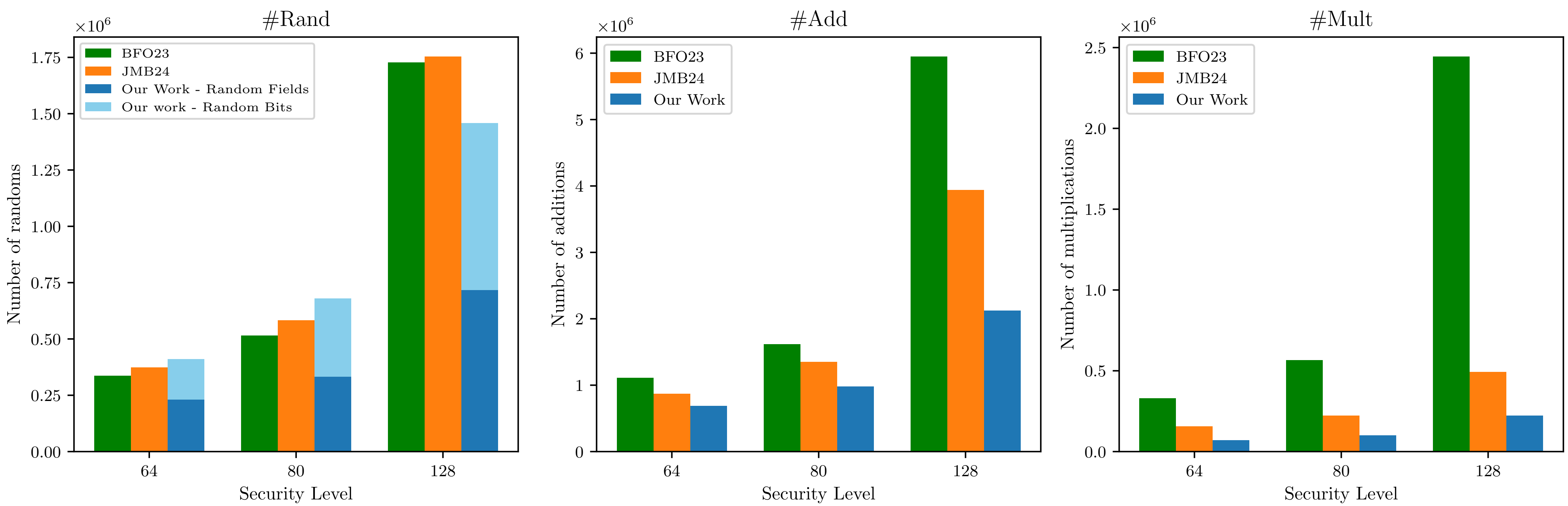


$p = 2^{-20}$

Application on AES

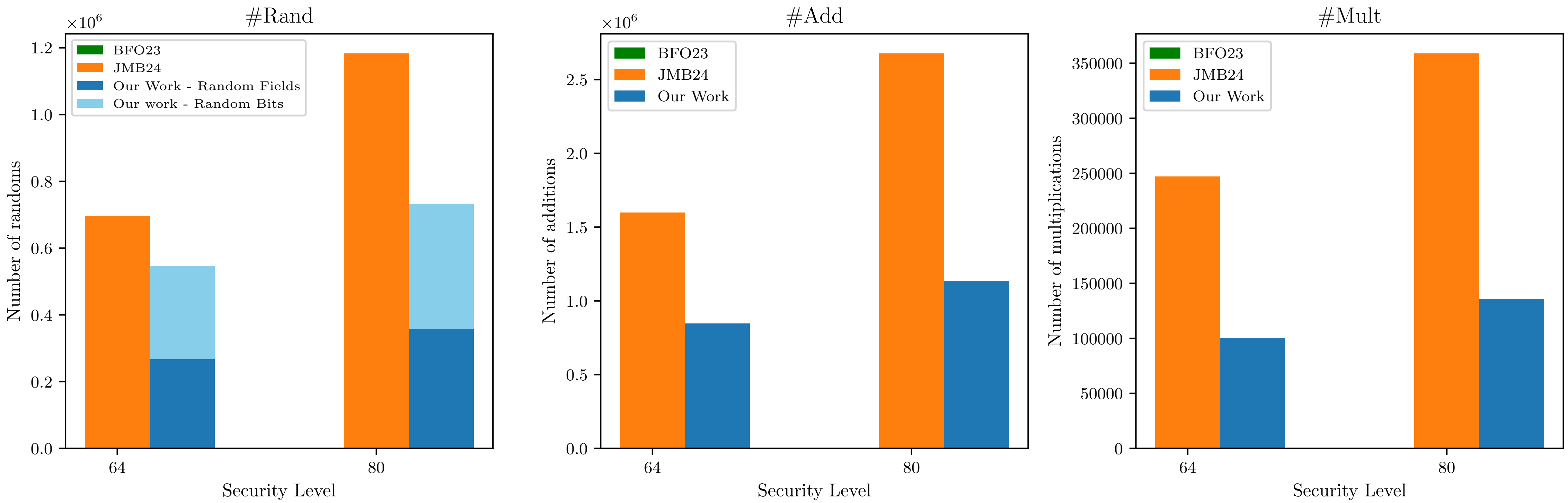


$p = 2^{-16}$

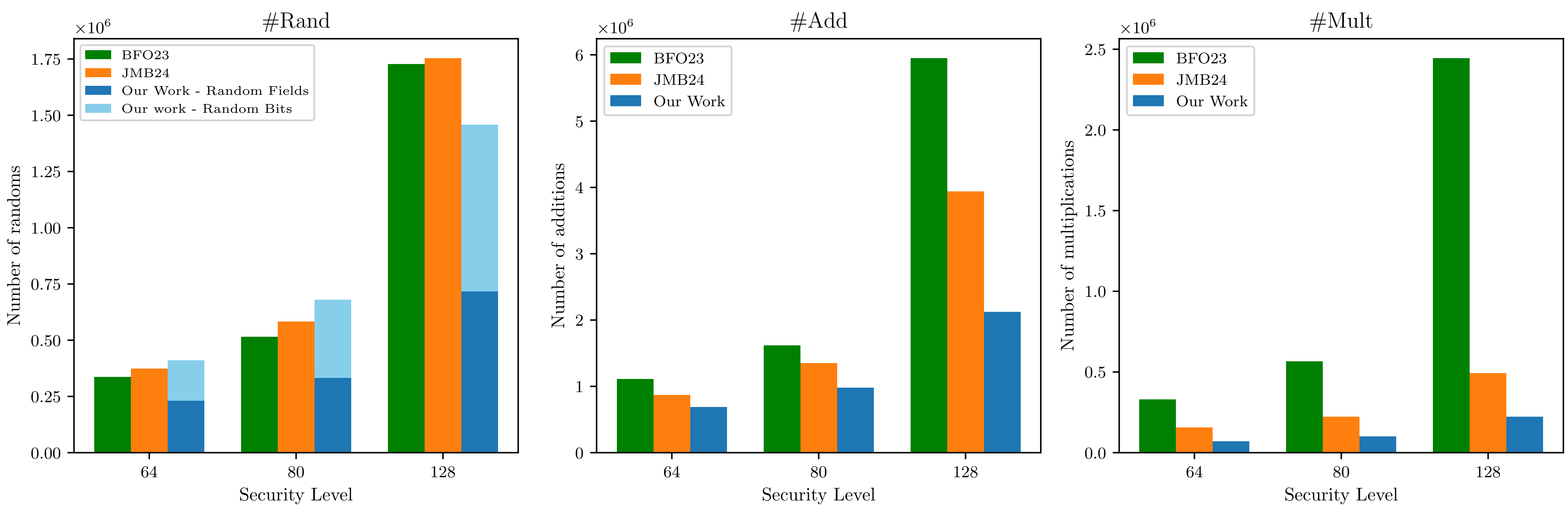


$p = 2^{-20}$

Application on AES



$p = 2^{-16}$



$p = 2^{-20}$

Conclusion

Foundations

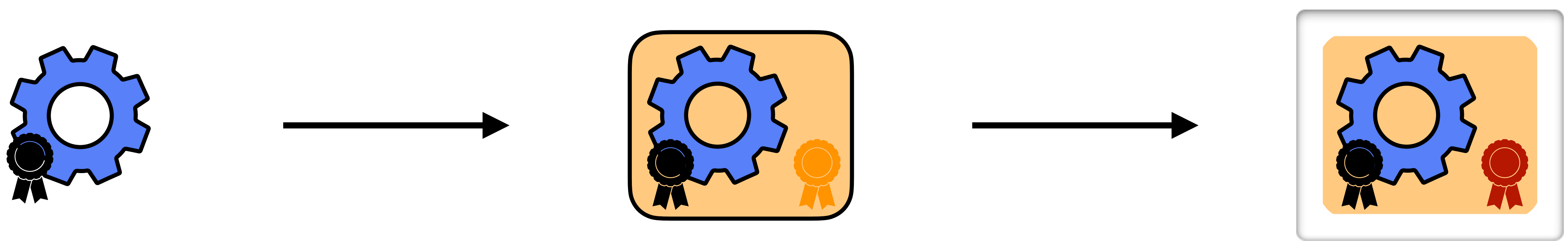
Random probing security & verification (small circuits)

Scaling up

Composition frameworks (larger circuits)

Building blocks

Design of efficient gadgets



Black-box secure

Black-box and random probing secure

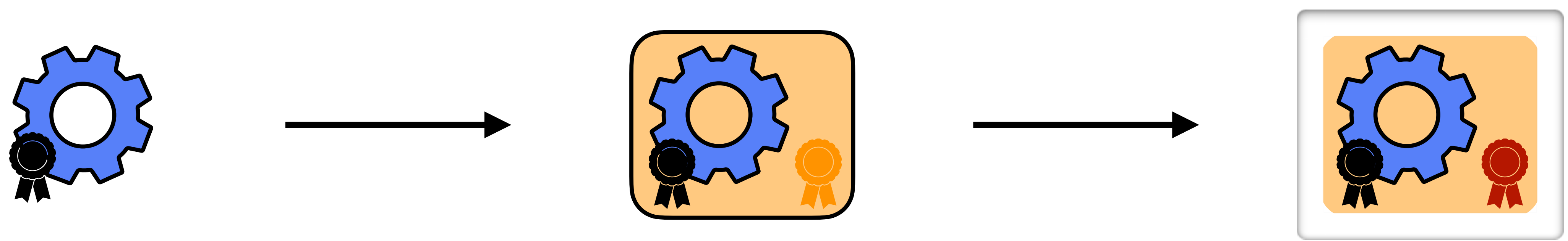
Black-box and physically secure

Conclusion

Foundations
Random probing security & verification (small circuits)

Scaling up
Composition frameworks (larger circuits)

Building blocks
Design of efficient gadgets



Black-box secure

Black-box and random probing secure

Black-box and physically secure

Conclusion

Foundations

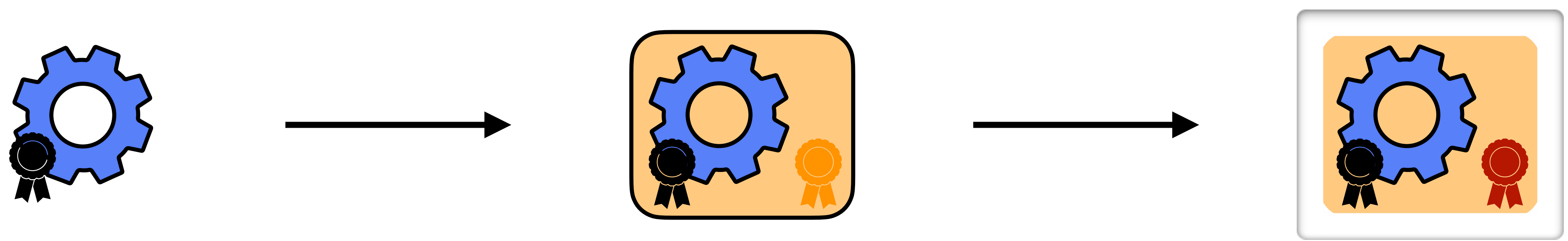
Random probing security & verification (small circuits)

Scaling up

Composition frameworks (larger circuits)

Building blocks

Design of efficient gadgets



Black-box secure

Black-box and random probing secure

Black-box and physically secure

Conclusion

Foundations

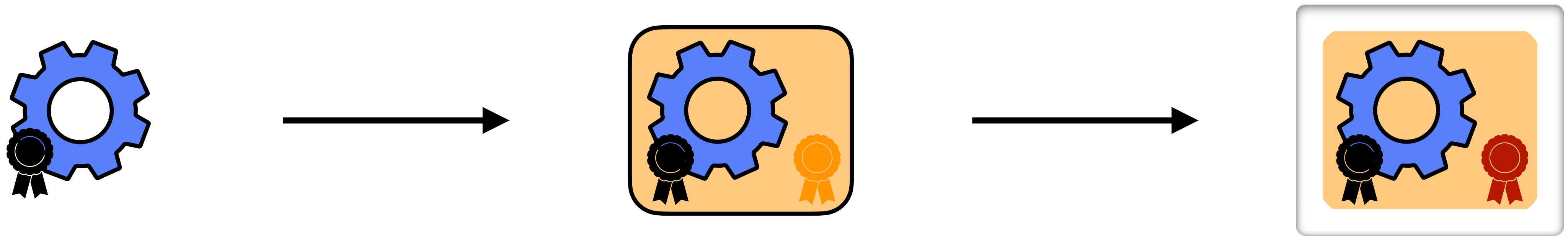
Random probing security & verification (small circuits)

Scaling up

Composition frameworks (larger circuits)

Building blocks

Design of efficient gadgets



Black-box secure

Black-box and random probing secure

Black-box and physically secure

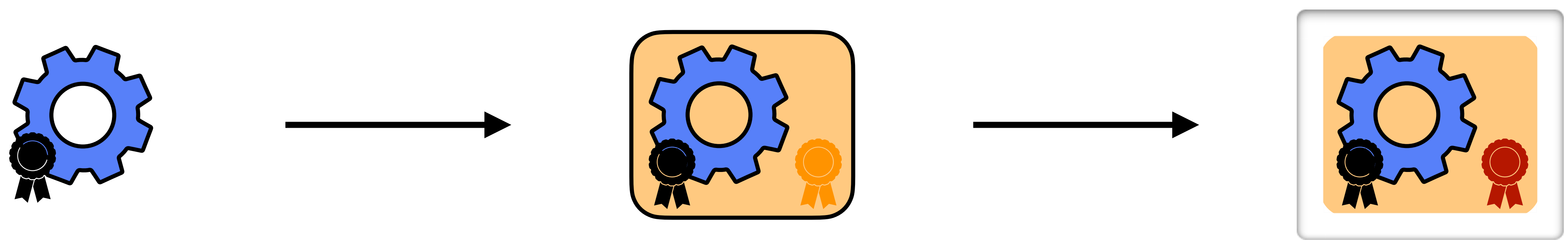
Perspectives

Design of more efficient gadgets
Better trade-off complexity/security

Design of masking friendly schemes
Better trade-off complexity/security

Evaluation in the gate model
Tighter reduction from physical security

Development of advanced security tools
Verification of customized implementations



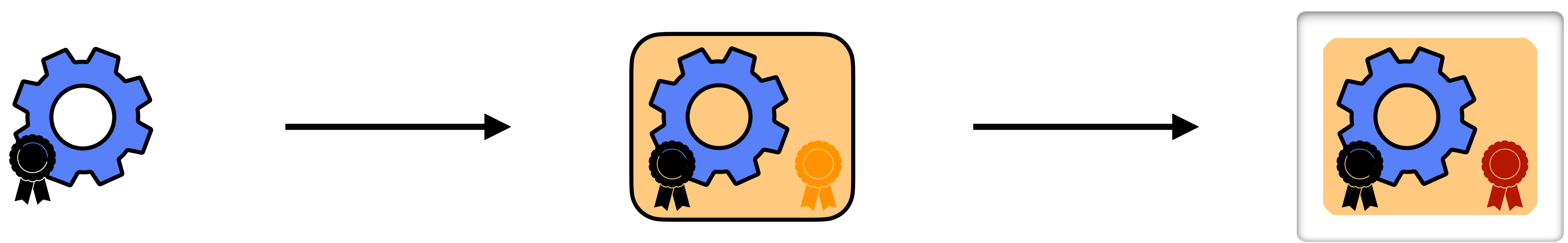
Perspectives

Design of more efficient gadgets
Better trade-off complexity/security

Design of masking friendly schemes
Better trade-off complexity/security

Evaluation in the gate model
Tighter reduction from physical security

Development of advanced security tools
Verification of customized implementations



Black-box secure

Black-box and random probing secure

Black-box and physically secure

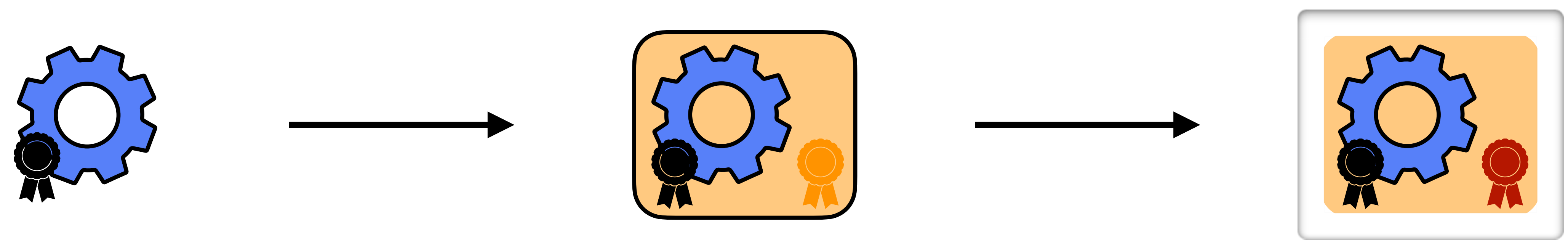
Perspectives

Design of more efficient gadgets
Better trade-off complexity/security

Design of masking friendly schemes
Better trade-off complexity/security

⊗ **Evaluation in the gate model**
Tighter reduction from physical security

Development of advanced security tools
Verification of customized implementations



Black-box secure

Black-box and random probing secure

Black-box and physically secure

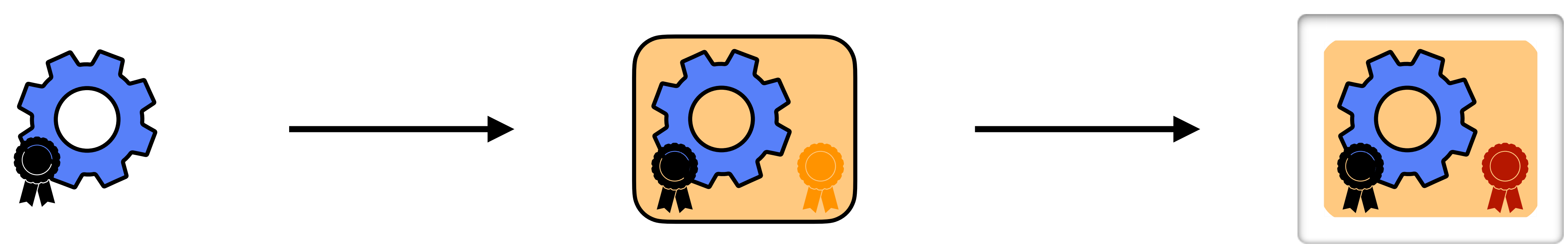
Perspectives

Design of more efficient gadgets
Better trade-off complexity/security

Design of masking friendly schemes
Better trade-off complexity/security

Evaluation in the gate model
Tighter reduction from physical security

Development of advanced security tools
Verification of customized implementations



Black-box secure

Black-box and random probing secure

Black-box and physically secure

Perspectives

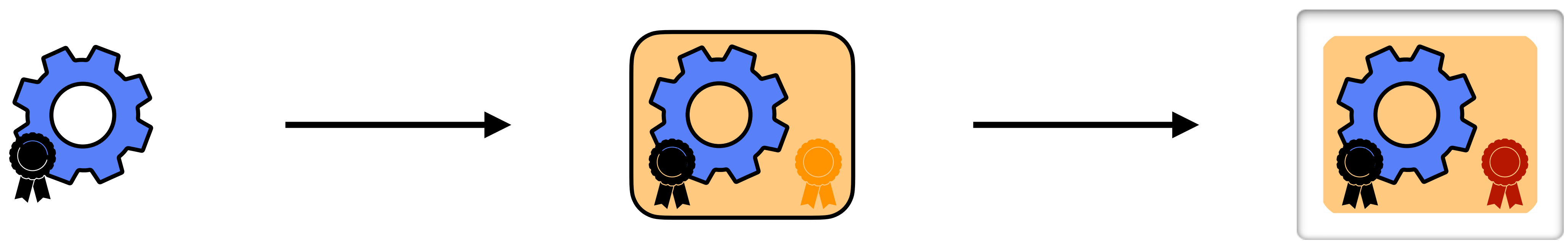
Design of more efficient gadgets
Better trade-off complexity/security

Design of masking friendly schemes
Better trade-off complexity/security

⊗ **Evaluation in the gate model**
Tighter reduction from physical security

Development of advanced security tools
Verification of customized implementations

Questions?



Black-box secure

Black-box and random probing secure

Black-box and physically secure