On the Power of Expansion

More Efficient Constructions in the Random Probing Model

Sonia Belaïd [1], Matthieu Rivain [1]
and Abdul Rahman Taleb [1,2]

[1] CryptoExperts, France
[2] Sorbonne Université, CNRS, LIP6, F-75005 Paris, France

October 19, 2021

Side-Channel Attacks & Masking

Security against **side-channel attacks**

Side-Channel Attacks & Masking

Security against **side-channel attacks**

Masking countermeasure (sensitive variable x over field $\mathbb{K}$)

Side-Channel Attacks & Masking

Security against **side-channel attacks**

Masking countermeasure (sensitive variable x over field $\mathbb{K}$)

$$x \longrightarrow (x_1, \ldots, x_n) \in \mathbb{K}^n$$

Side-Channel Attacks & Masking

Security against **side-channel attacks**

Masking countermeasure (sensitive variable x over field $\mathbb{K}$)

$$x \longrightarrow \underbrace{(x_1, \ldots, x_n)}_{\substack{\text{shares of } x \\ x_1+\ldots+x_n=x}} \in \mathbb{K}^n$$

Side-Channel Attacks & Masking

Security against **side-channel attacks**

Masking countermeasure (sensitive variable x over field $\mathbb{K}$)

$$x \longrightarrow \underbrace{(x_1, \ldots, x_n)}_{\substack{\text{shares of } x \\ x_1+\ldots+x_n=x}} \in \mathbb{K}^n$$

$(+, \times, ||)$ operations over $\mathbb{K}$

Side-Channel Attacks & Masking

Security against **side-channel attacks**

Masking countermeasure (sensitive variable x over field $\mathbb{K}$)

$$x \longrightarrow \underbrace{(x_1, \ldots, x_n)}_{\substack{\text{shares of } x \\ x_1+\ldots+x_n=x}} \in \mathbb{K}^n$$

$(+, \times, ||)$ operations over $\mathbb{K} \longrightarrow (G_{\text{add}}, G_{\text{mult}}, G_{\text{copy}}, G_{\text{refresh}})$ n-share circuits over $\mathbb{K}$

Side-Channel Attacks & Masking

Security against **side-channel attacks**

Masking countermeasure (sensitive variable x over field $\mathbb{K}$)

$$x \longrightarrow \underbrace{(x_1, \ldots, x_n)}_{\substack{\text{shares of } x \\ x_1+\ldots+x_n=x}} \in \mathbb{K}^n$$

$(+, \times, ||)$ operations over $\mathbb{K} \longrightarrow (G_{\text{add}}, G_{\text{mult}}, G_{\text{copy}}, G_{\text{refresh}})$ n-share circuits over $\mathbb{K}$

Example $G_{\text{add}}(a, b) = c$ with $n = 2$

Side-Channel Attacks & Masking

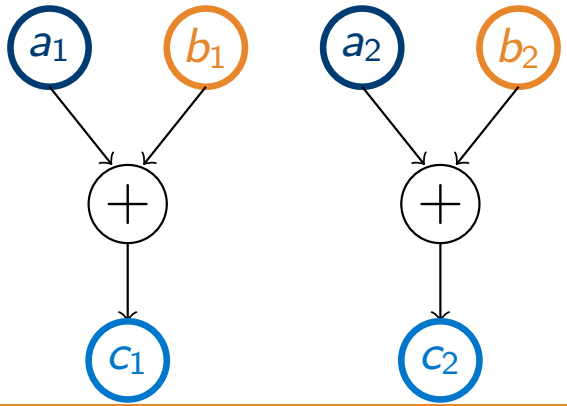
Security against **side-channel attacks**

Masking countermeasure (sensitive variable x over field $\mathbb{K}$)

$$x \longrightarrow \underbrace{(x_1, \ldots, x_n)}_{\substack{\text{shares of } x \\ x_1+\ldots+x_n=x}} \in \mathbb{K}^n$$

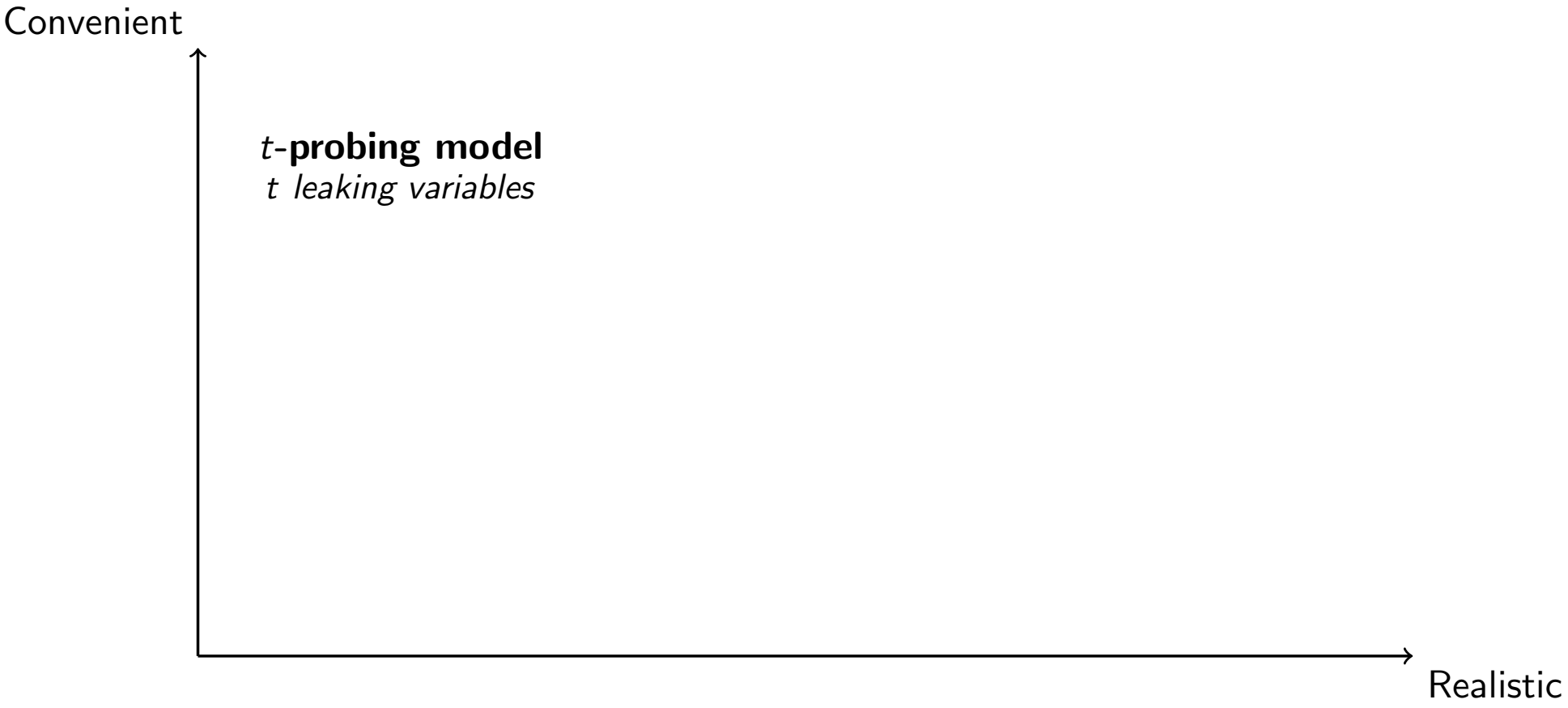
$(+, \times, ||)$ operations over $\mathbb{K} \longrightarrow (G_{\text{add}}, G_{\text{mult}}, G_{\text{copy}}, G_{\text{refresh}})$ n-share circuits over $\mathbb{K}$

Example $G_{\text{add}}(a, b) = c$ with $n = 2$

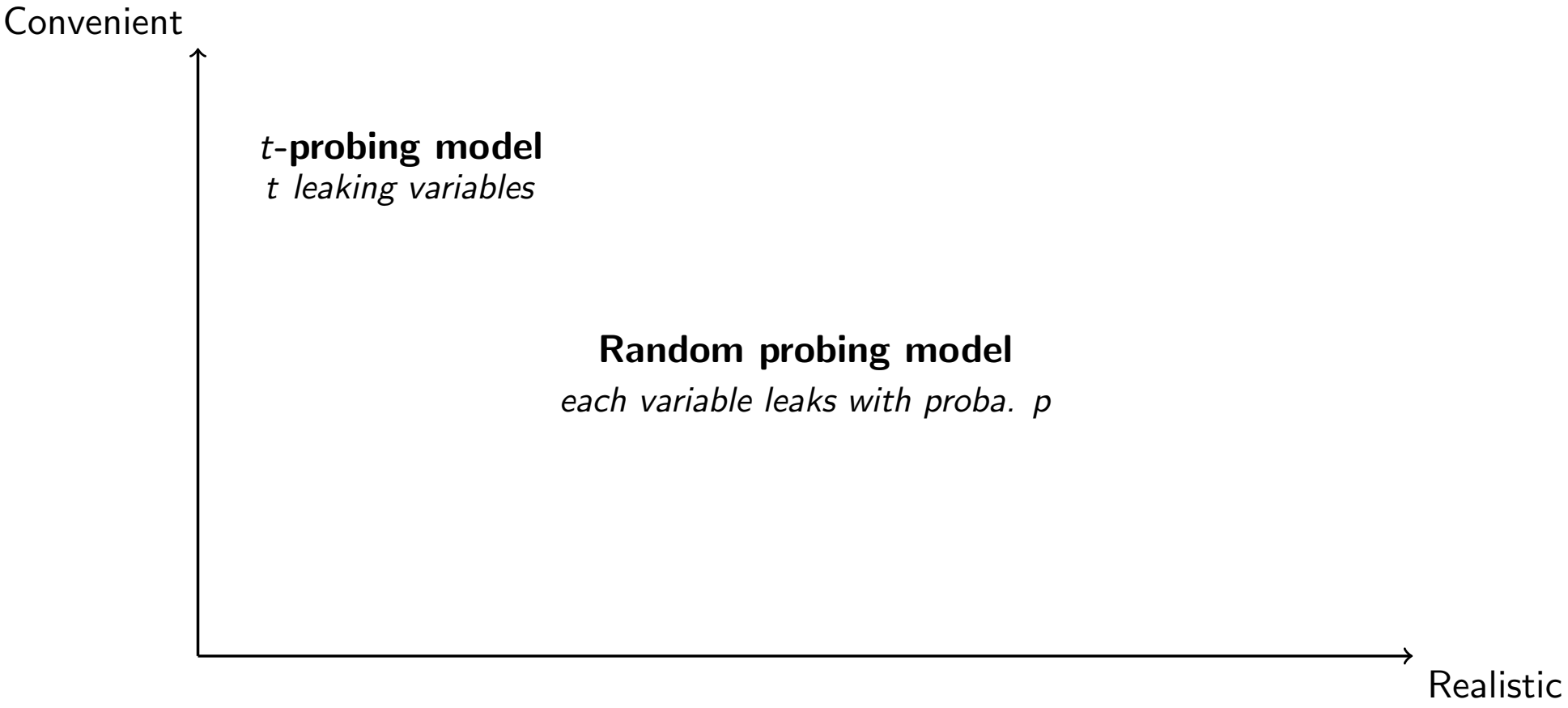


Leakage Models

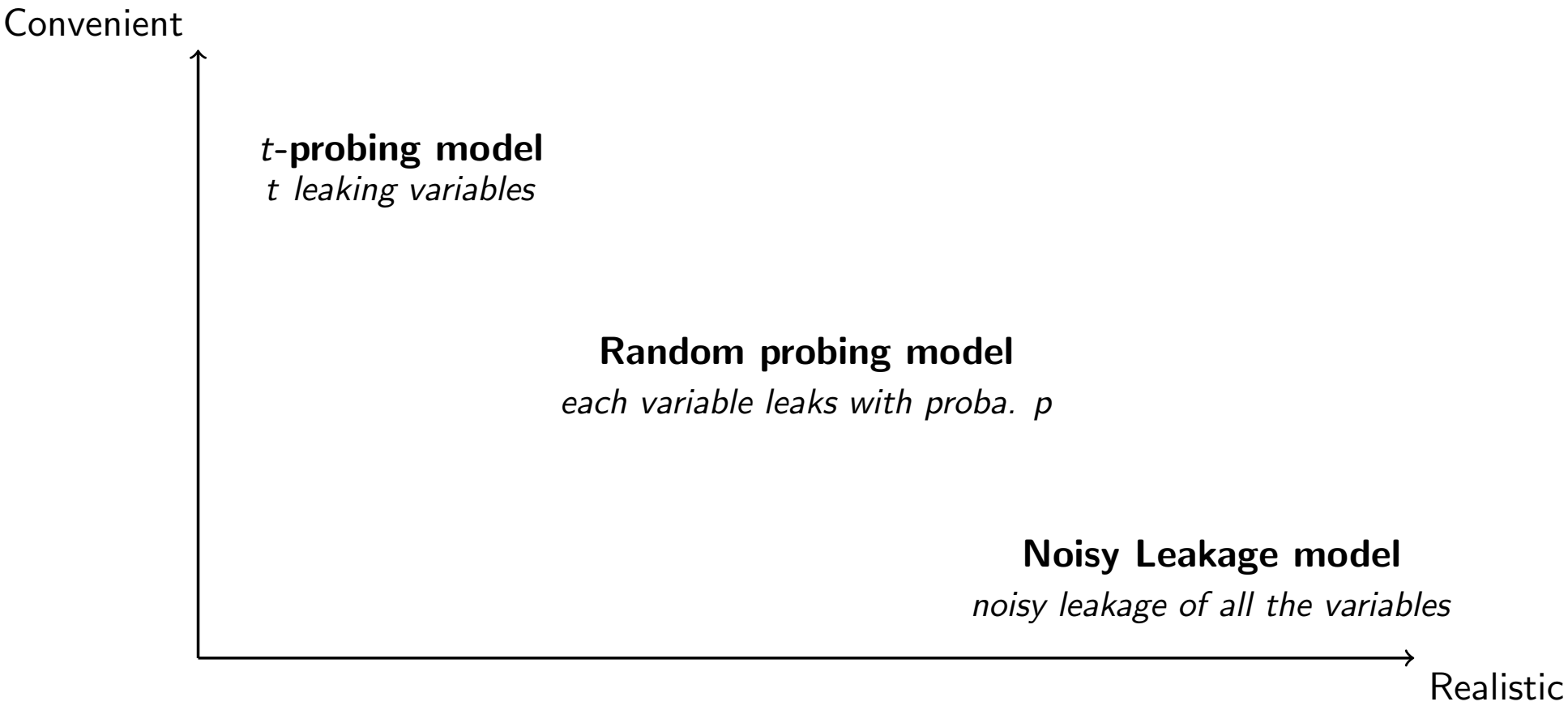
Leakage Models



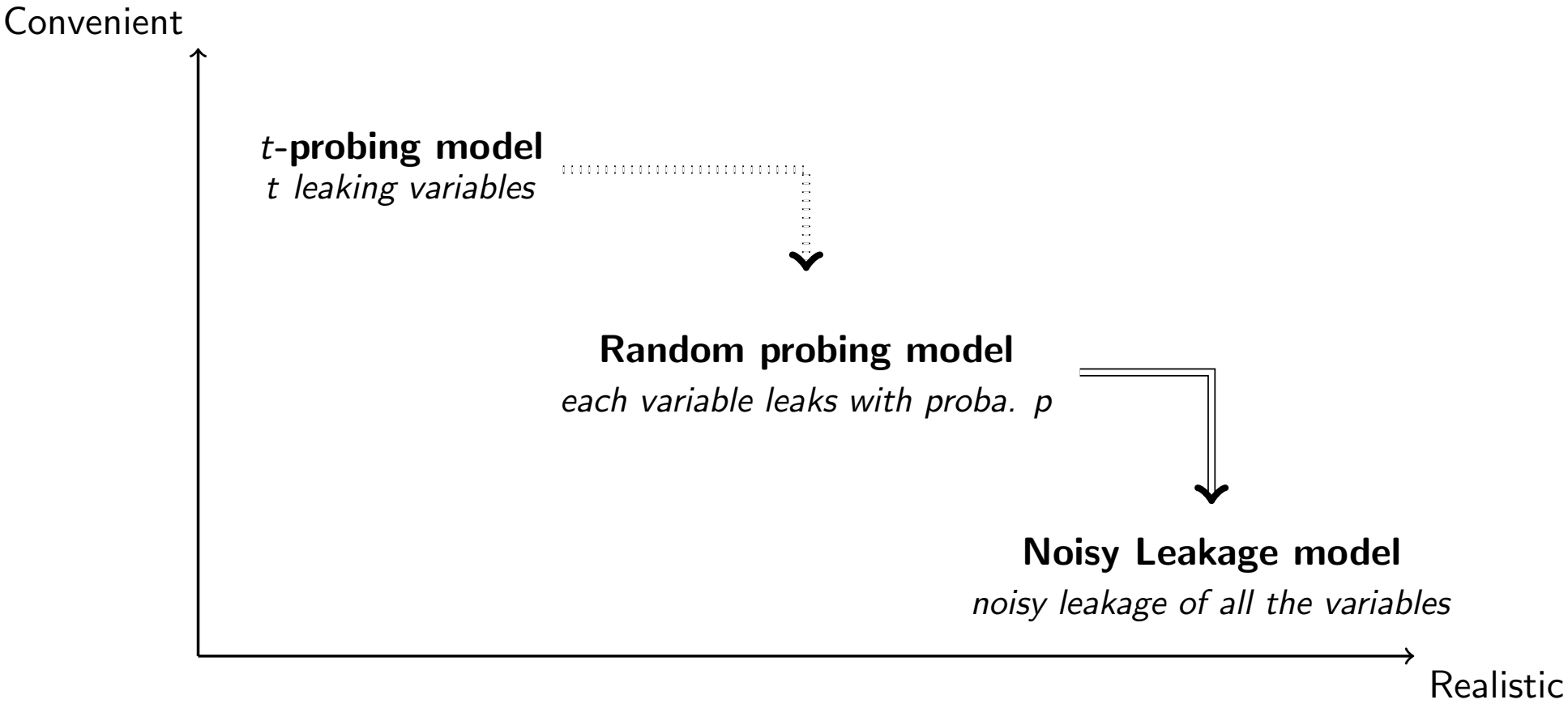
Leakage Models



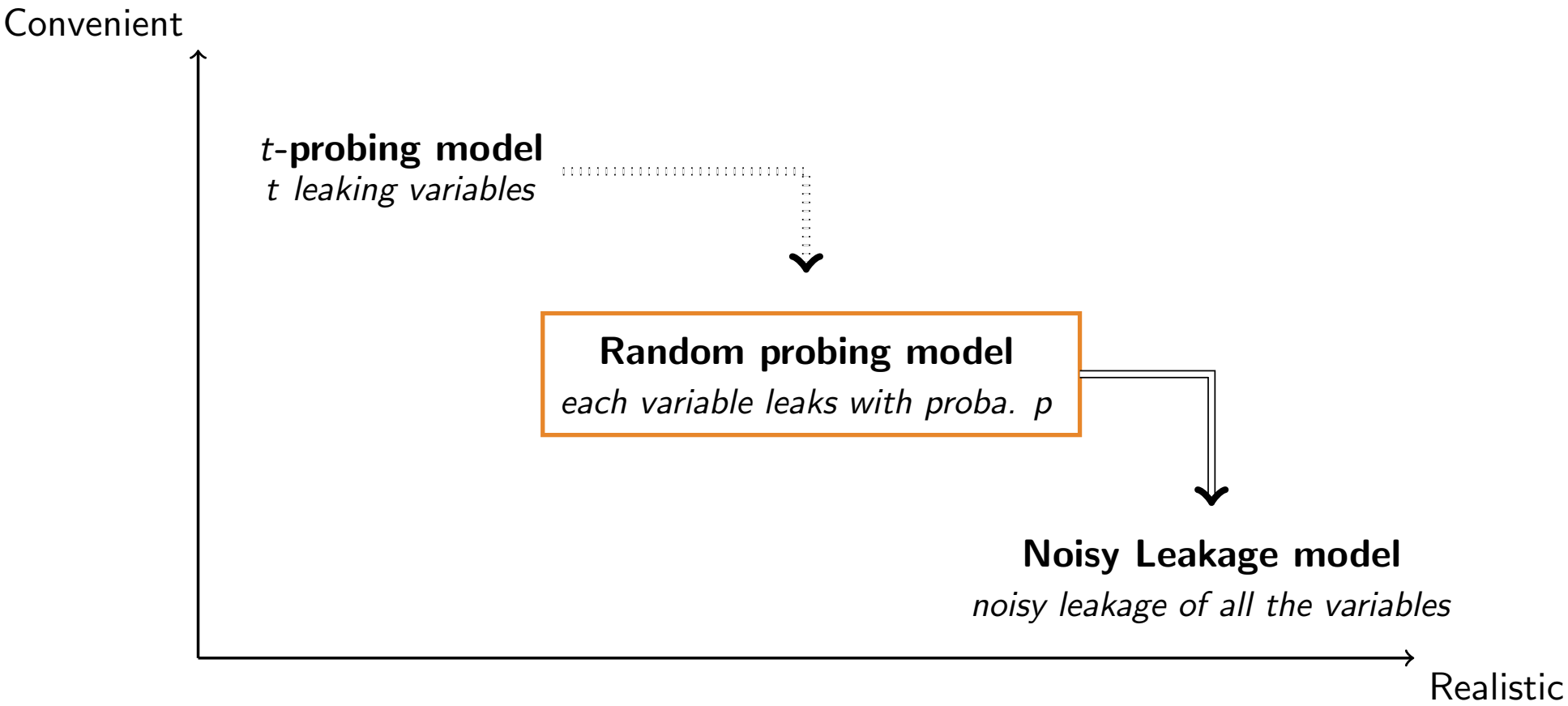
Leakage Models



Leakage Models



Leakage Models



Prior Work

[CRYPTO 2020] Random probing security: verification, composition, expansion and new constructions. *Sonia Belaïd, Jean-Sébastien Coron, Emmanuel Prouff, Matthieu Rivain, Abdul Rahman Taleb*.

Prior Work

[CRYPTO 2020] Random probing security: verification, composition, expansion and new constructions. *Sonia Belaïd, Jean-Sébastien Coron, Emmanuel Prouff, Matthieu Rivain, Abdul Rahman Taleb*.

- Security of masking in the **Random Probing (RP) Model**

Prior Work

[CRYPTO 2020] Random probing security: verification, composition, expansion and new constructions. *Sonia Belaïd, Jean-Sébastien Coron, Emmanuel Prouff, Matthieu Rivain, Abdul Rahman Taleb*.

- Security of masking in the **Random Probing (RP) Model**
- RP-secure gadgets composition (RP composition)

Prior Work

[CRYPTO 2020] Random probing security: verification, composition, expansion and new constructions. *Sonia Belaïd, Jean-Sébastien Coron, Emmanuel Prouff, Matthieu Rivain, Abdul Rahman Taleb*.

- Security of masking in the **Random Probing (RP) Model**
- RP-secure gadgets composition (RP composition)
- RP-secure security level amplification (RP expansion)

Prior Work

[CRYPTO 2020] Random probing security: verification, composition, expansion and new constructions. *Sonia Belaïd, Jean-Sébastien Coron, Emmanuel Prouff, Matthieu Rivain, Abdul Rahman Taleb*.

- Security of masking in the **Random Probing (RP) Model**
- RP-secure gadgets composition (RP composition)
- RP-secure security level amplification (RP expansion)
- **VRAPS:** (V)erifier of (RA)ndom (P)robing (S)ecurity

Contributions

- In-depth analysis of RP expansion (relations, complexity bounds, ...)

Contributions

- In-depth analysis of RP expansion (relations, complexity bounds, ...)
- Generic constructions for RP expansion with improved complexities

Contributions

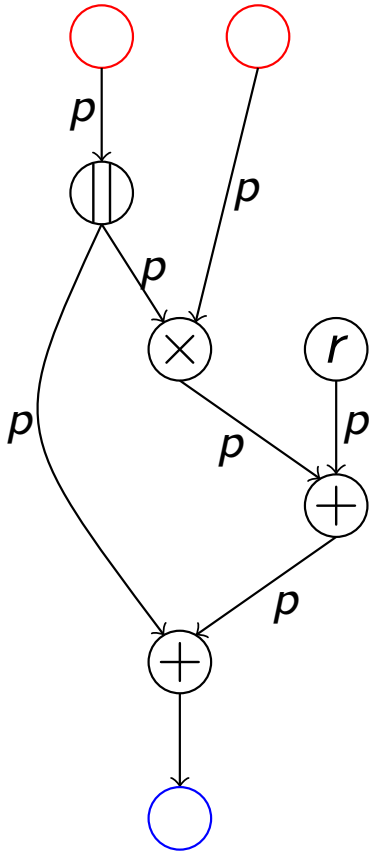
- In-depth analysis of RP expansion (relations, complexity bounds, ...)
- Generic constructions for RP expansion with improved complexities
- Concrete instantiations for RP expansion (circuit C, security parameter κ)

Contributions

- In-depth analysis of RP expansion (relations, complexity bounds, ...)
- Generic constructions for RP expansion with improved complexities
- Concrete instantiations for RP expansion (circuit C, security parameter κ)

Construction	Complexity	Tolerated Leakage rate
[AIS CRYPTO 18] MPC based	$\mathcal{O}(\lvert C\rvert \cdot \kappa^{7.87})$	$p = 2^{-25}$
[CRYPTO 20] 3-share	$\mathcal{O}(\lvert C\rvert \cdot \kappa^{7.5})$	$p = 2^{-8}$
New 3-share	$\mathcal{O}(\lvert C\rvert \cdot \kappa^{3.9})$	$p = 2^{-7.5}$
New 5-share	$\mathcal{O}(\lvert C\rvert \cdot \kappa^{3.2})$	$2^{-12} \leq p \leq 2^{-6}$

RP Security

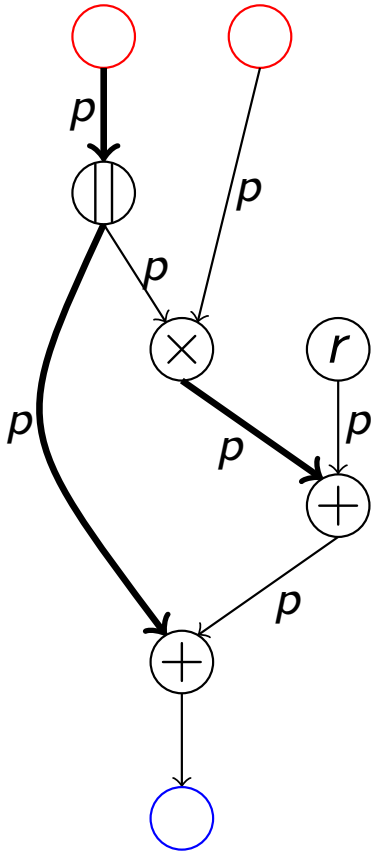


Add Mult.

Copy Random

(p, ε)-RP Security

RP Security



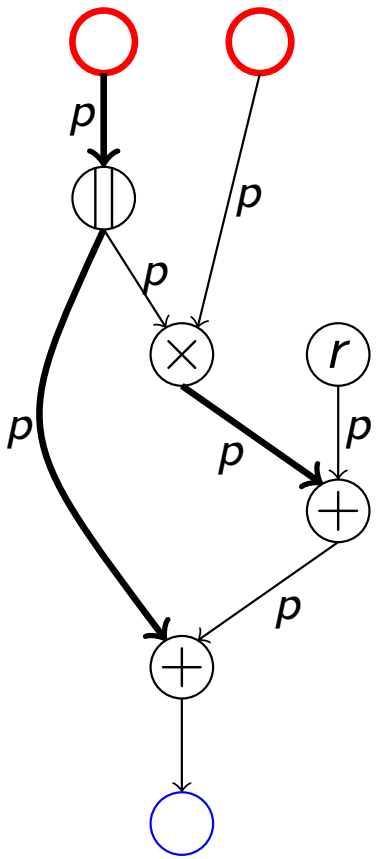
⊕ Add ⊗ Mult.

Copy r Random

(p, ε)-RP Security

W set of wires

RP Security



⊕ Add ⊗ Mult.

Copy r Random

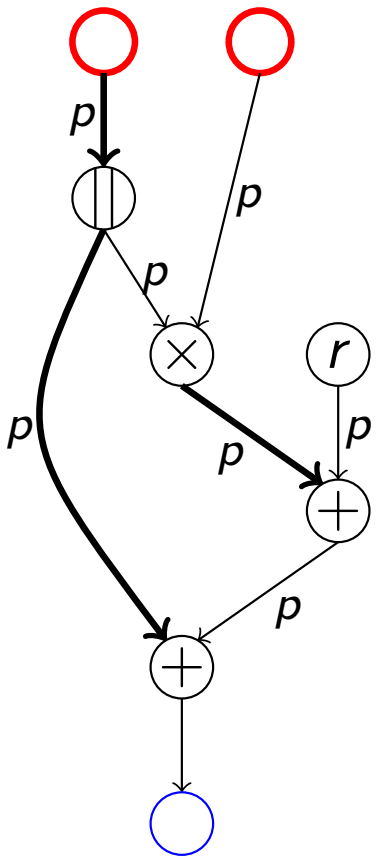
(p, ε)-RP Security

W set of wires

↓

Independent from secret inputs ?

RP Security



⊕ Add ⊗ Mult.

Copy r Random

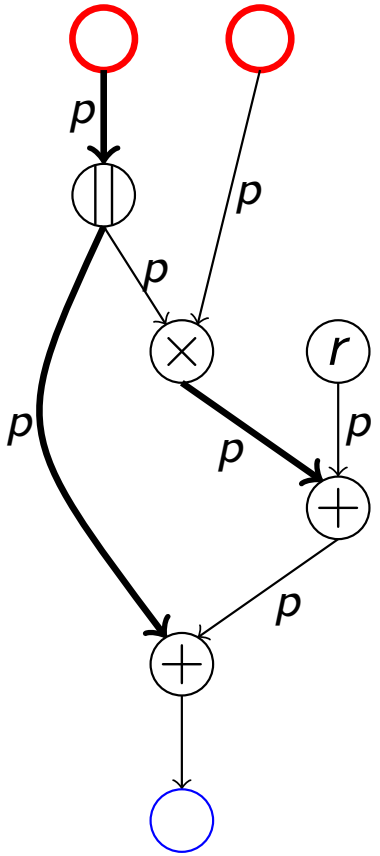
(p, ε)-RP Security

W set of wires

Independent from secret inputs ?

yes no

RP Security



⊕ Add ⊗ Mult.

Copy r Random

(p, ε)-RP Security

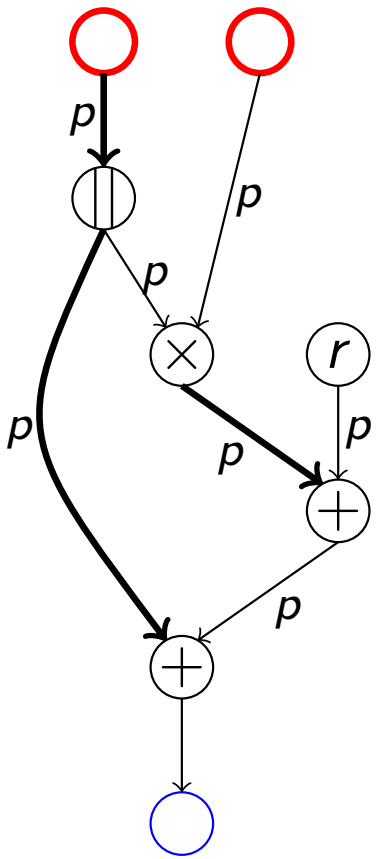
W set of wires

Independent from secret inputs ?

yes no

Simulation Success

RP Security



⊕ Add ⊗ Mult.

Copy r Random

(p, ε)-RP Security

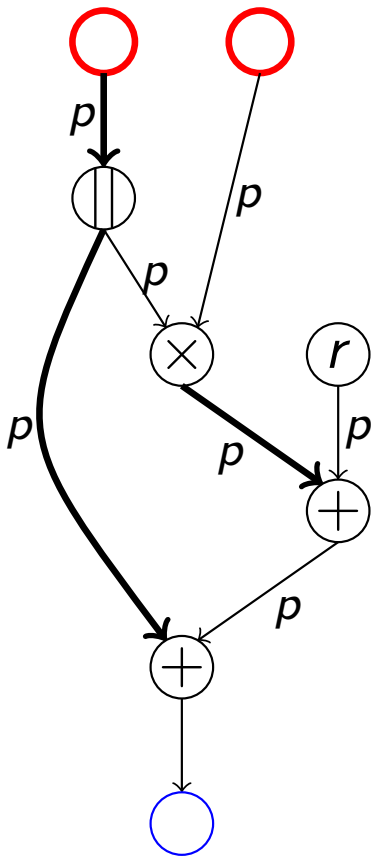
W set of wires

Independent from secret inputs ?

yes no

Simulation Success *Simulation Failure*

RP Security



⊕ Add ⊗ Mult.

Copy r Random

(p, ε)-RP Security

W set of wires

↓

Independent from secret inputs ?

yes — *Simulation Success*

no — *Simulation Failure*

↓

Failure Probability ε

RP Expansion

Illustration

Using n-share gadgets G_{add}, G_{copy}, G_{mult}

RP Expansion

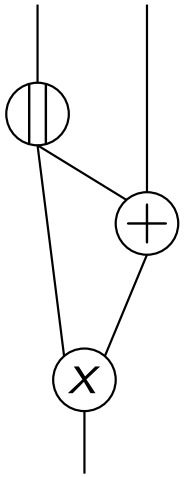
Illustration

Using n-share gadgets G_{add}, G_{copy}, G_{mult}

RP Expansion

Illustration

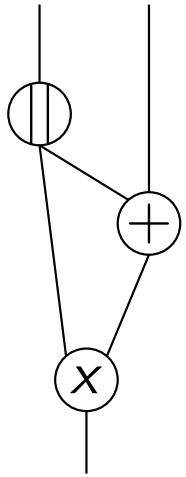
Using n-share gadgets G_{add}, G_{copy}, G_{mult}



RP Expansion

Illustration

Using n-share gadgets G_{add}, G_{copy}, G_{mult}

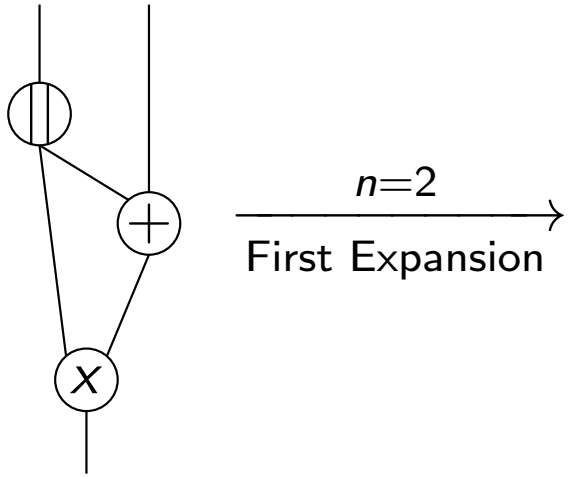


Leakage probability
p

RP Expansion

Illustration

Using n-share gadgets G_{add}, G_{copy}, G_{mult}

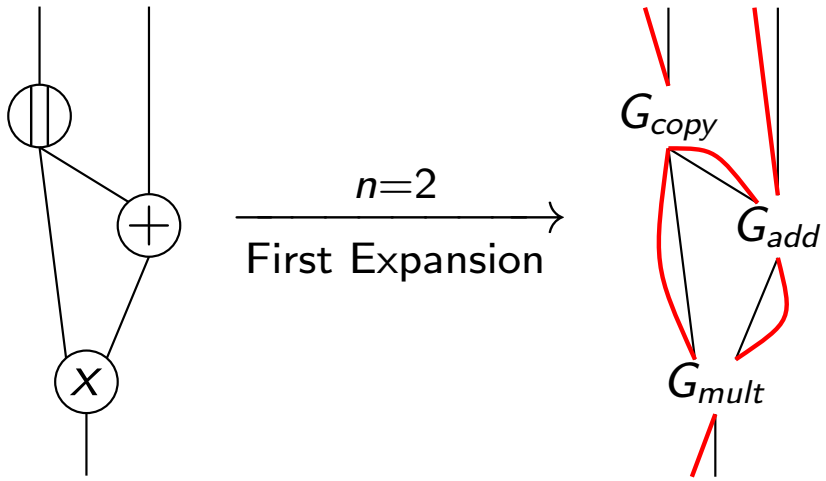


Leakage probability
p

RP Expansion

Illustration

Using n-share gadgets G_{add}, G_{copy}, G_{mult}

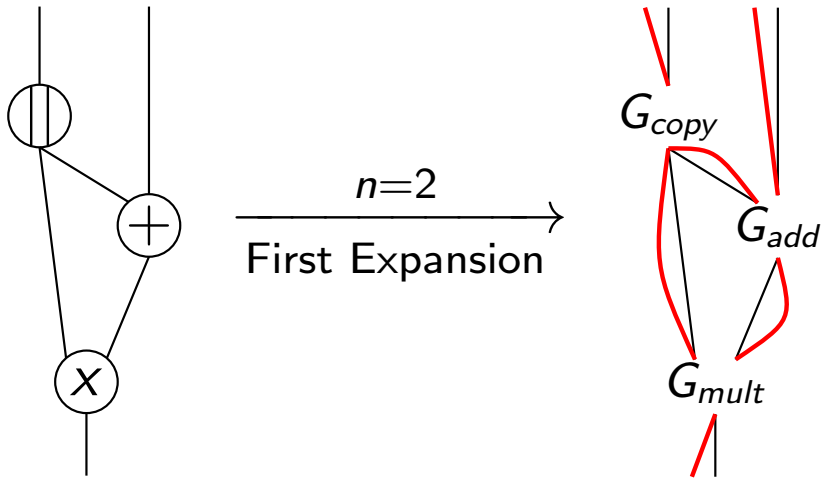


Leakage probability
p

RP Expansion

Illustration

Using n-share gadgets G_{add}, G_{copy}, G_{mult}



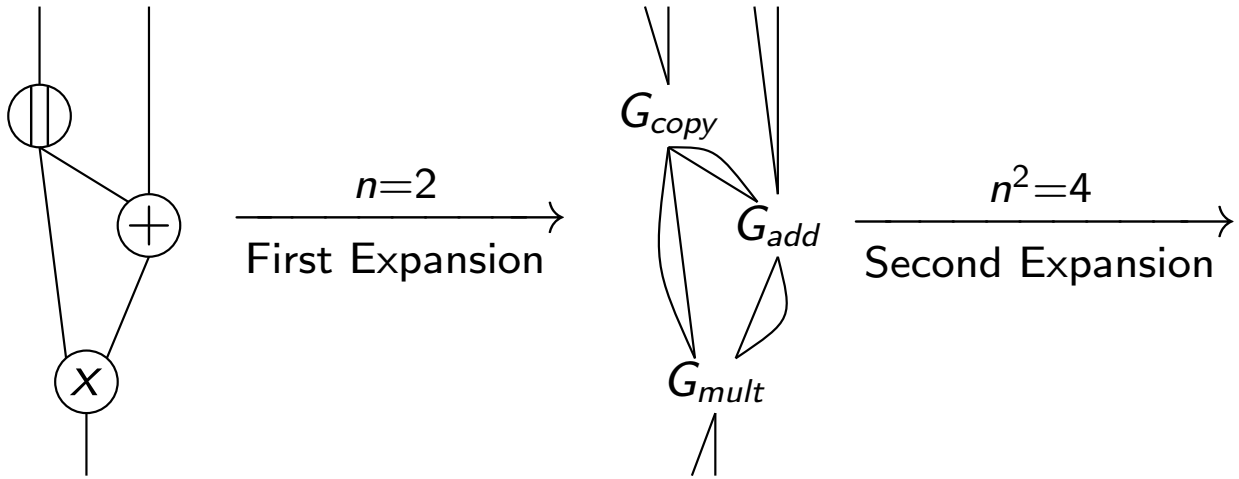
Leakage probability
p

Simulation Failure
ε

RP Expansion

Illustration

Using n-share gadgets G_{add}, G_{copy}, G_{mult}



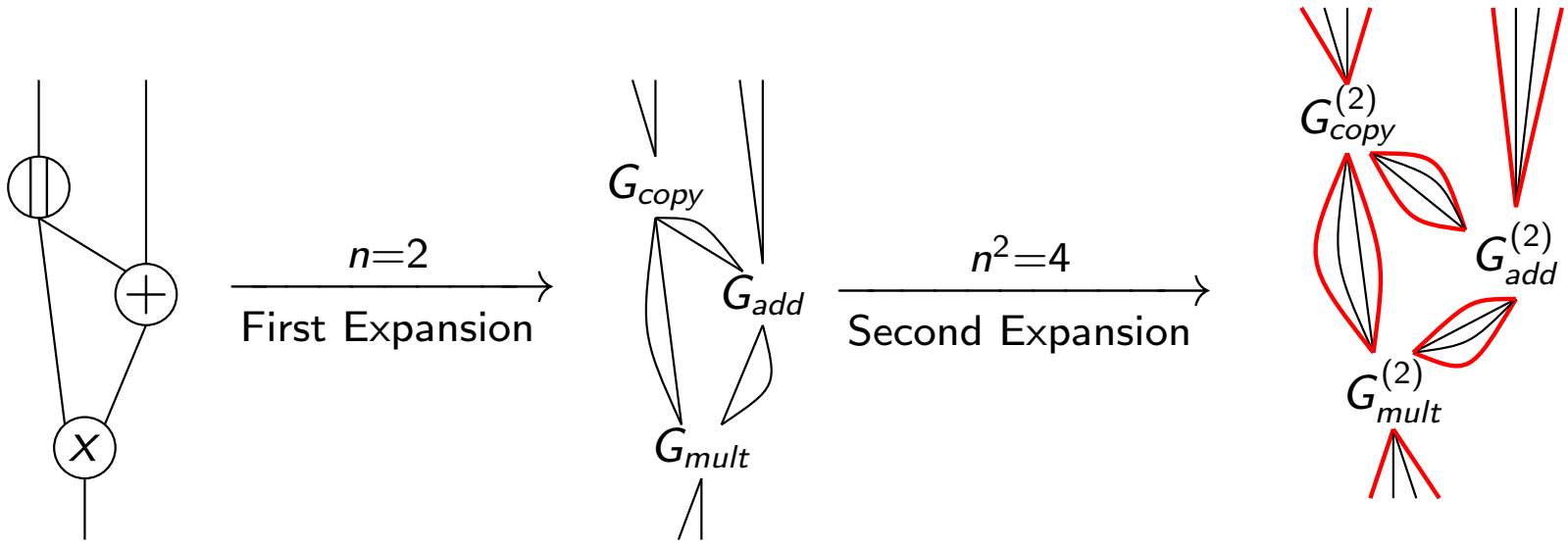
Leakage probability
p

Simulation Failure
ε

RP Expansion

Illustration

Using n-share gadgets G_{add}, G_{copy}, G_{mult}



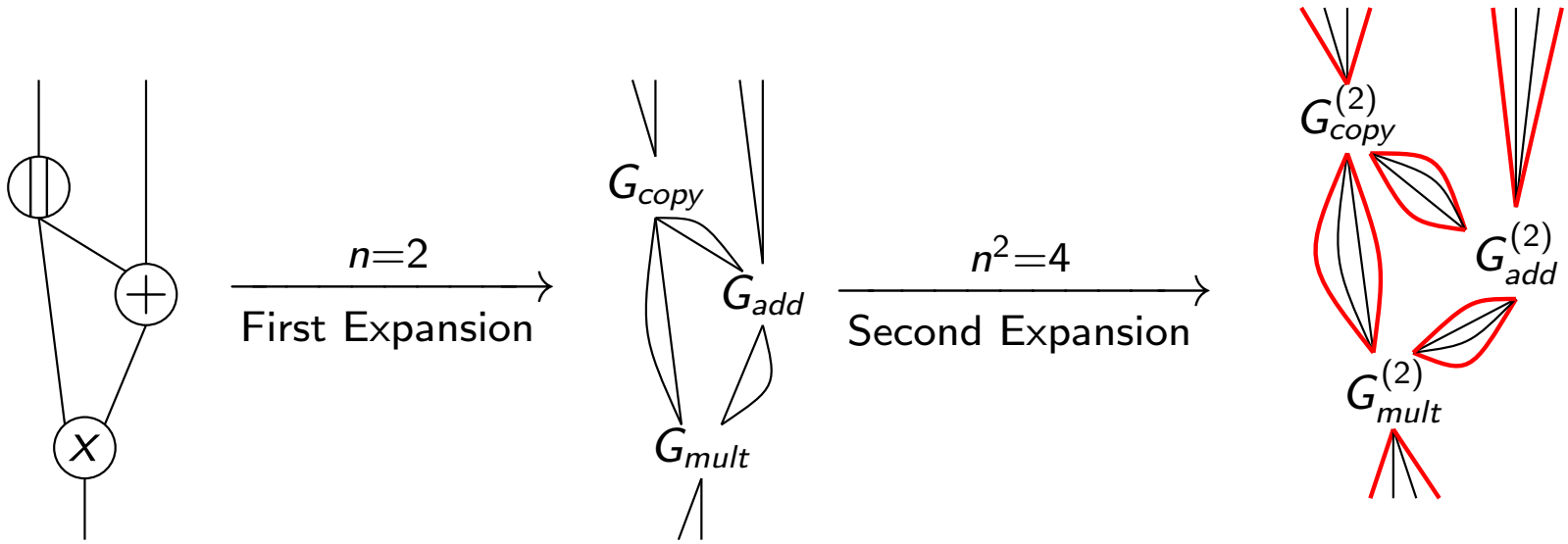
Leakage probability
p

Simulation Failure
ε

RP Expansion

Illustration

Using n-share gadgets G_{add}, G_{copy}, G_{mult}



Leakage probability
p

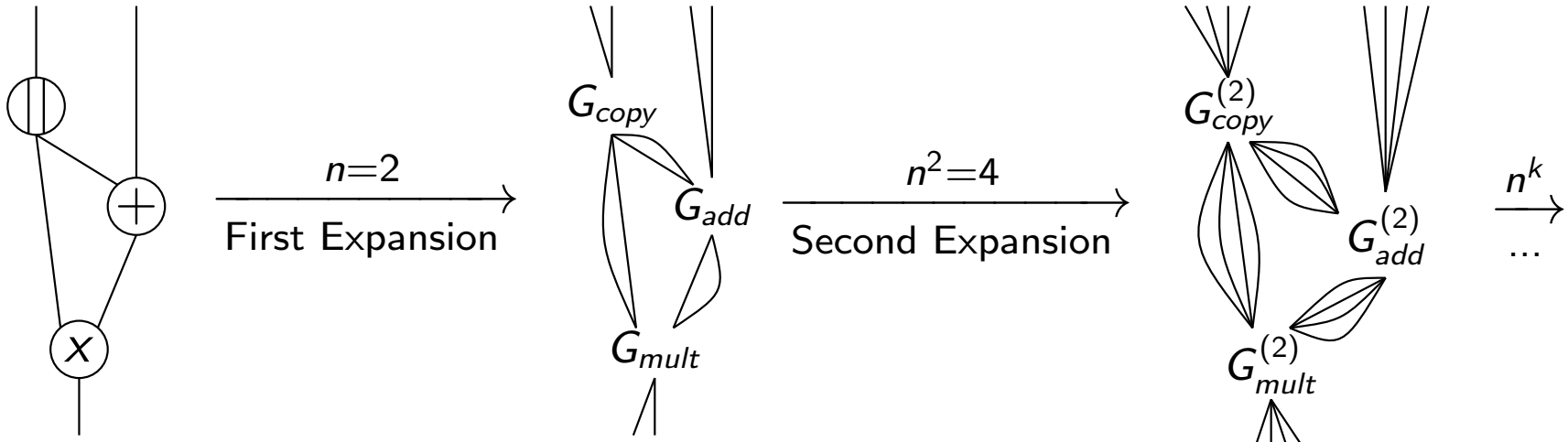
Simulation Failure
ε

ε^2

RP Expansion

Illustration

Using n-share gadgets G_{add}, G_{copy}, G_{mult}



Leakage probability
p

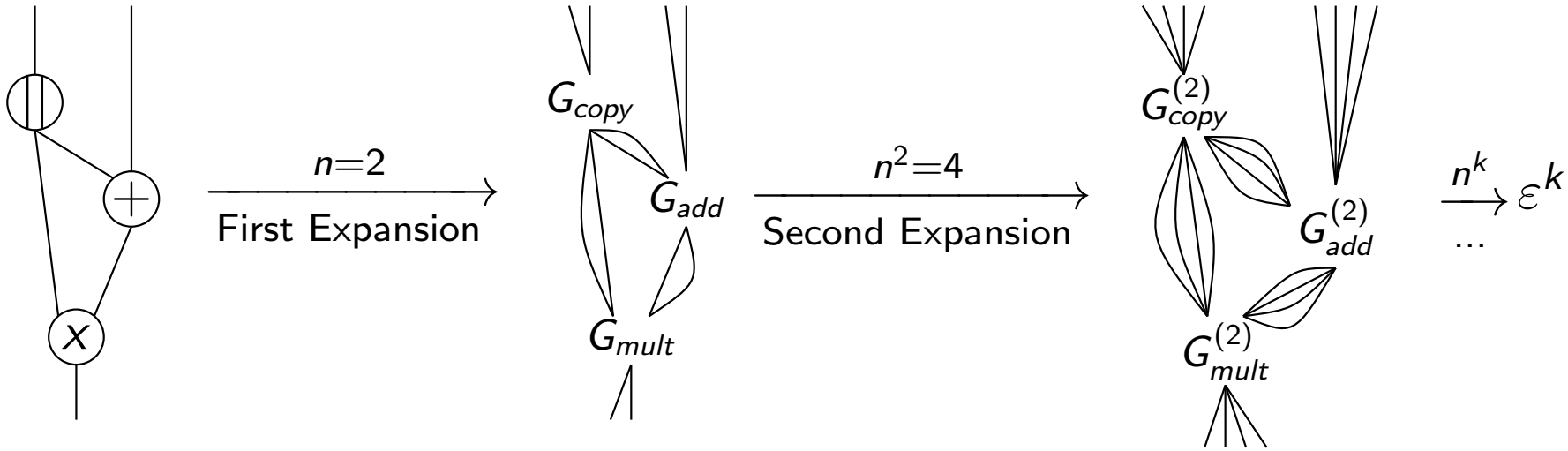
Simulation Failure
ε

ε^2

RP Expansion

Illustration

Using n-share gadgets G_{add}, G_{copy}, G_{mult}



Leakage probability
p

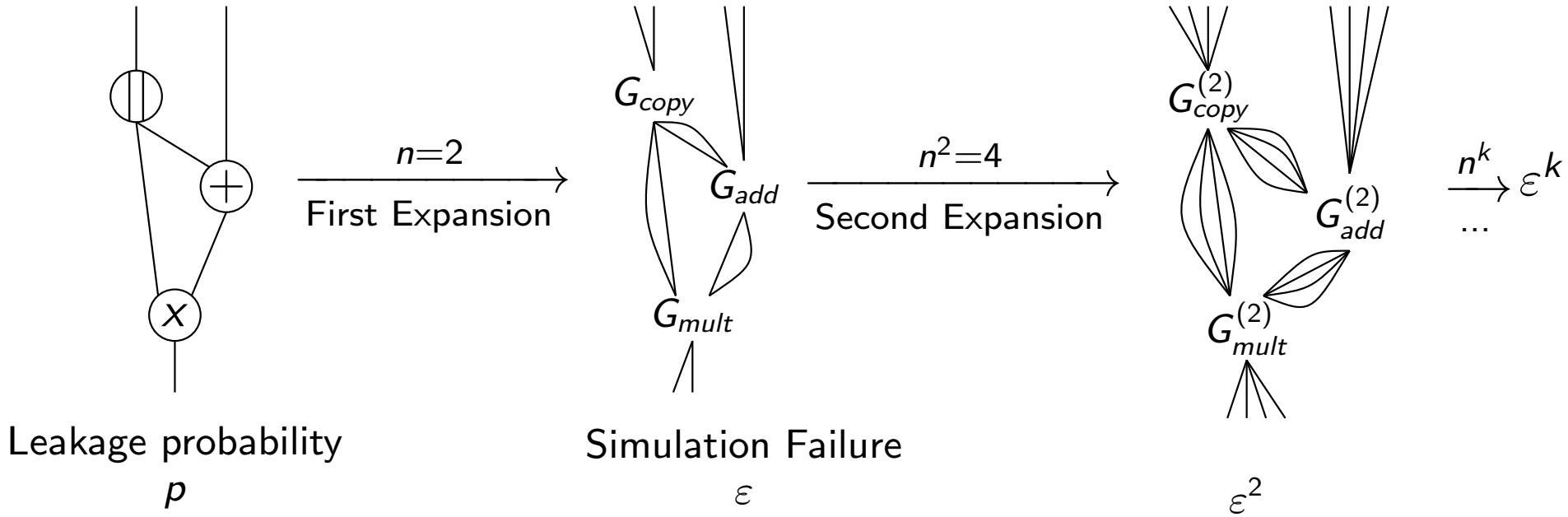
Simulation Failure
ε

ε^2

RP Expansion

Illustration

Using n-share gadgets G_{add}, G_{copy}, G_{mult}



Condition : $\varepsilon < p$ (tolerated leakage rate)

RP Expansion

Definition

$(\mathbf{t}, p, \varepsilon)$-**RP expandability** (RPE) of gadget G garantees:

RP Expansion

Definition

$(\mathbf{t}, p, \varepsilon)$-**RP expandability** (RPE) of gadget G garantees:

- (p, ε)-RP security of G (RPE is stronger than RP)

RP Expansion

Definition

$(\mathbf{t}, p, \varepsilon)$-**RP expandability** (RPE) of gadget G garantees:

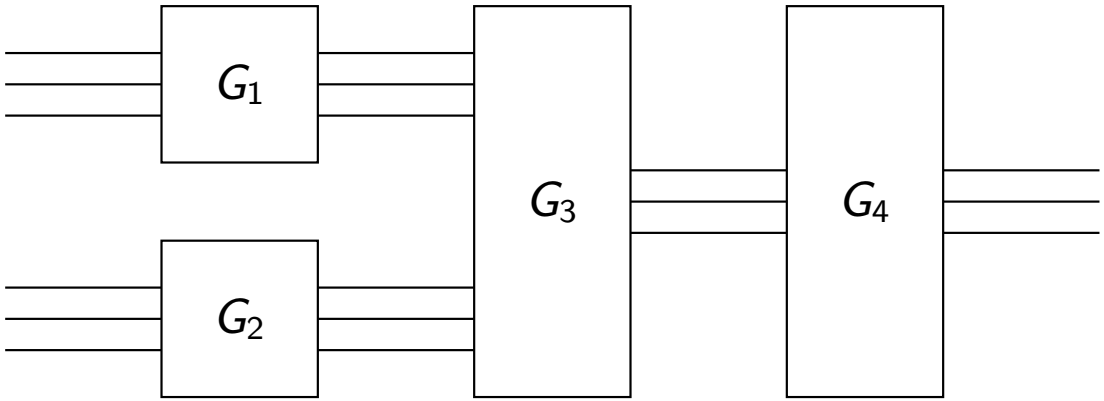
- (p, ε)-RP security of G (RPE is stronger than RP)
- **composition** of G with other RP secure gadgets: ability to simulate any set W of internal wires and t output shares using t input shares

RP Expansion

Definition

$(\mathbf{t}, p, \varepsilon)$-**RP expandability** (RPE) of gadget G garantees:

- (p, ε)-RP security of G (RPE is stronger than RP)
- **composition** of G with other RP secure gadgets: ability to simulate any set W of internal wires and t output shares using t input shares

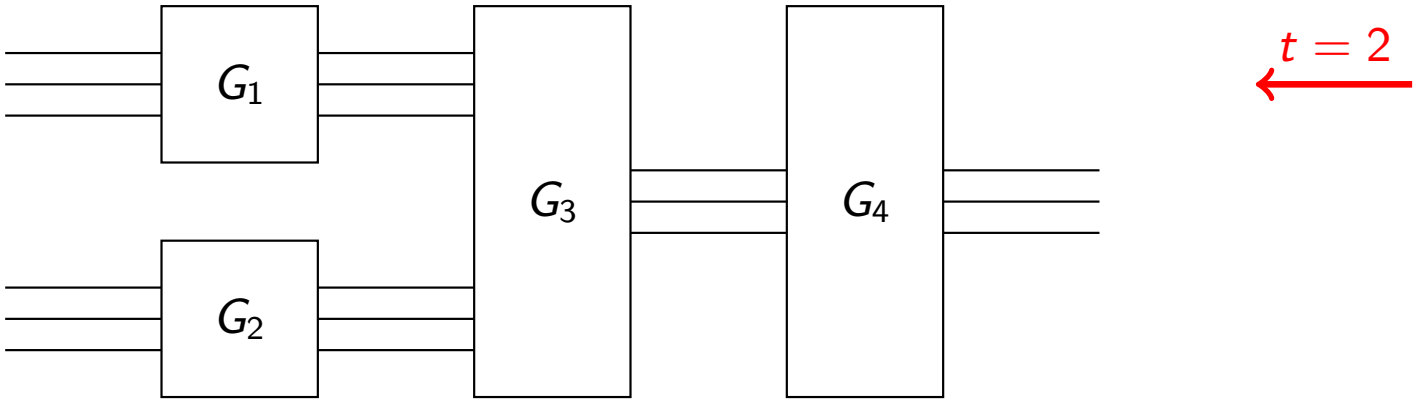


RP Expansion

Definition

$(\mathbf{t}, p, \varepsilon)$-**RP expandability** (RPE) of gadget G garantees:

- (p, ε)-RP security of G (RPE is stronger than RP)
- **composition** of G with other RP secure gadgets: ability to simulate any set W of internal wires and t output shares using t input shares

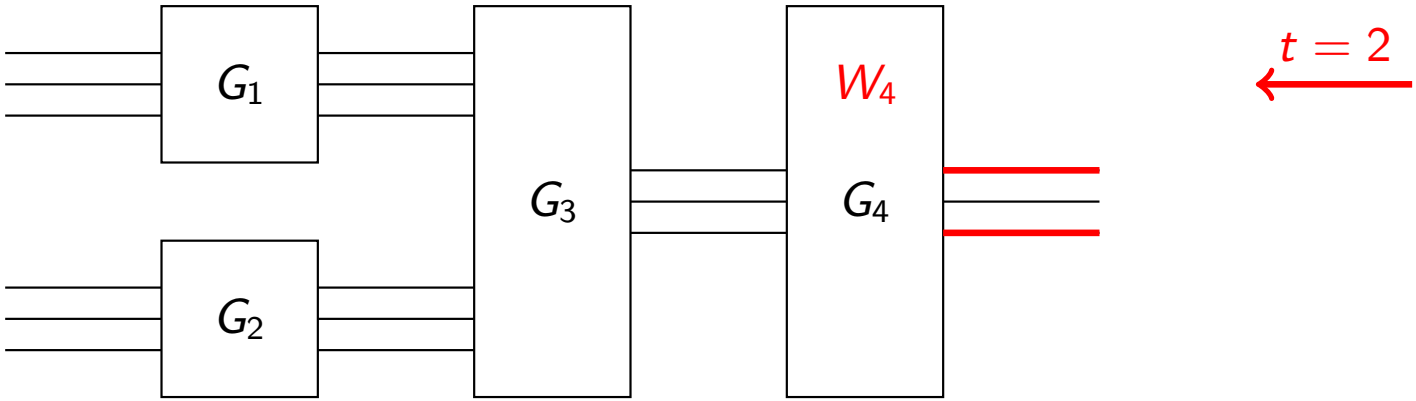


RP Expansion

Definition

$(\mathbf{t}, p, \varepsilon)$-**RP expandability** (RPE) of gadget G garantees:

- (p, ε)-RP security of G (RPE is stronger than RP)
- **composition** of G with other RP secure gadgets: ability to simulate any set W of internal wires and t output shares using t input shares

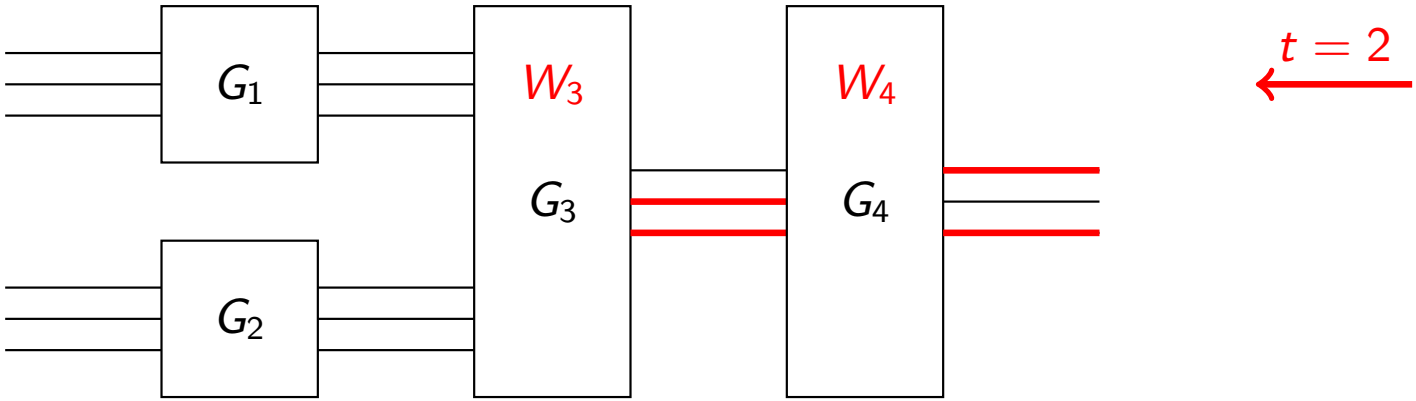


RP Expansion

Definition

$(\mathbf{t}, p, \varepsilon)$-**RP expandability** (RPE) of gadget G garantees:

- (p, ε)-RP security of G (RPE is stronger than RP)
- **composition** of G with other RP secure gadgets: ability to simulate any set W of internal wires and t output shares using t input shares

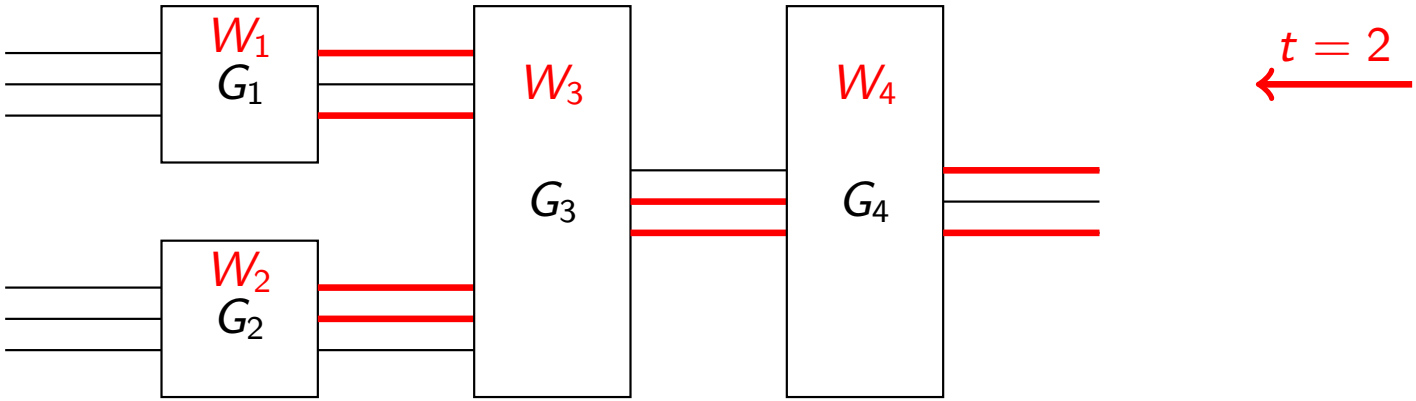


RP Expansion

Definition

$(\mathbf{t}, p, \varepsilon)$-**RP expandability** (RPE) of gadget G garantees:

- (p, ε)-RP security of G (RPE is stronger than RP)
- **composition** of G with other RP secure gadgets: ability to simulate any set W of internal wires and t output shares using t input shares

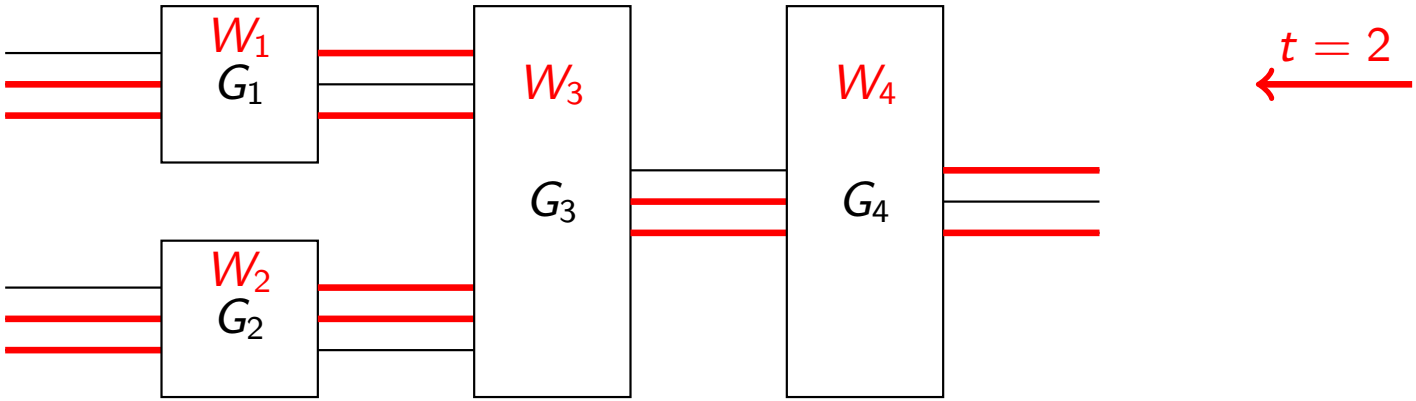


RP Expansion

Definition

$(\mathbf{t}, p, \varepsilon)$-**RP expandability** (RPE) of gadget G garantees:

- (p, ε)-RP security of G (RPE is stronger than RP)
- **composition** of G with other RP secure gadgets: ability to simulate any set W of internal wires and t output shares using t input shares

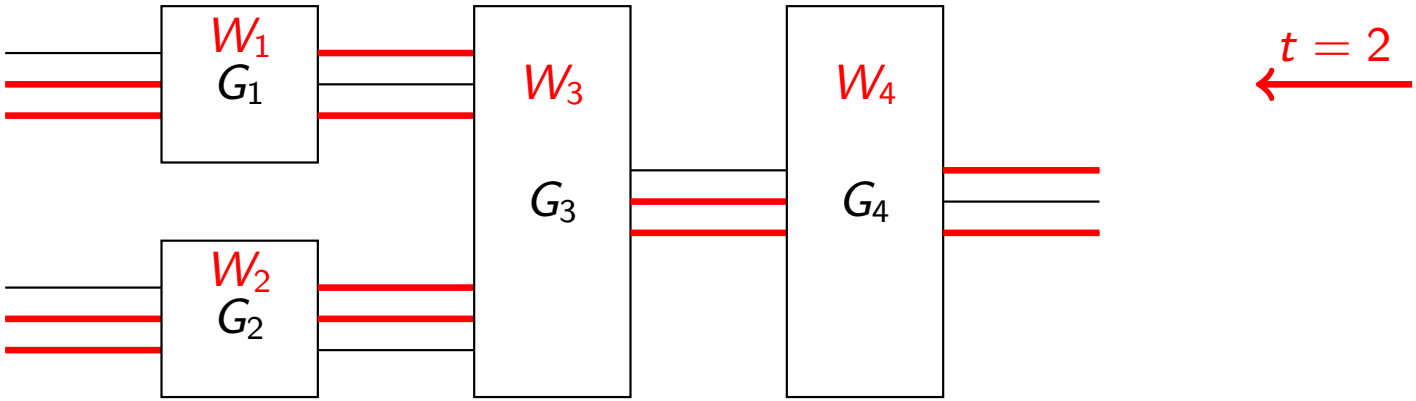


RP Expansion

Definition

$(\mathbf{t}, p, \varepsilon)$-**RP expandability** (RPE) of gadget G garantees:

- (p, ε)-RP security of G (RPE is stronger than RP)
- **composition** of G with other RP secure gadgets: ability to simulate any set W of internal wires and t output shares using t input shares



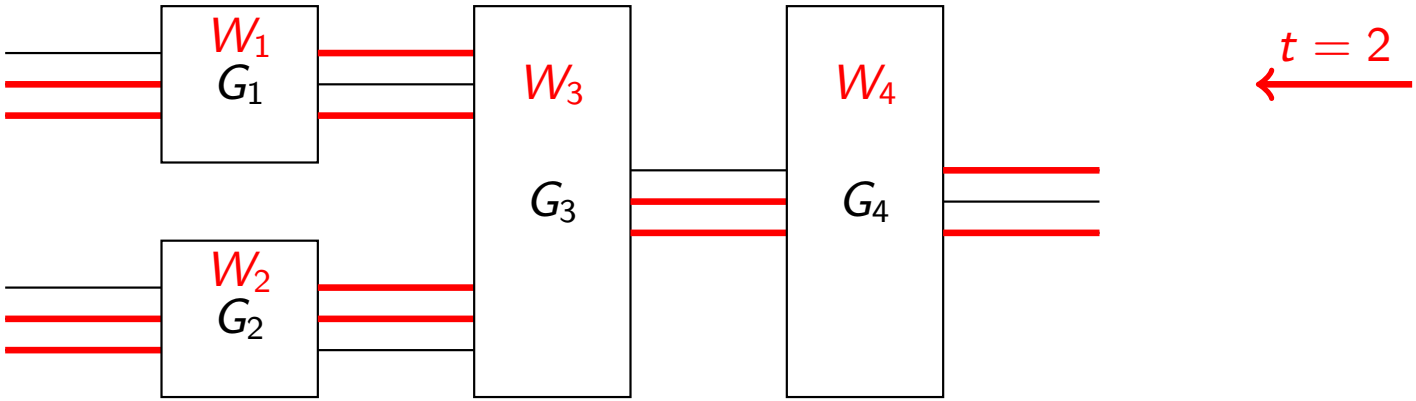
- Independent failure probability on each input sharing

RP Expansion

Definition

$(\mathbf{t}, p, \varepsilon)$-**RP expandability** (RPE) of gadget G garantees:

- (p, ε)-RP security of G (RPE is stronger than RP)
- **composition** of G with other RP secure gadgets: ability to simulate any set W of internal wires and t output shares using t input shares



- Independent failure probability on each input sharing
- expansion of G with arbitrary level k

RP Expansion

Security

For an n-share gadget G:

RP Expansion

Security

For an n-share gadget G:

$$G \text{ RP-Expandable, } \varepsilon \quad \Longrightarrow \quad G^{(k)} \text{ RP-Expandable, } \varepsilon^k$$

RP Expansion

Security

For an n-share gadget G:

$$G \text{ RP-Expandable, } \varepsilon \quad \Longrightarrow \quad G^{(k)} \text{ RP-Expandable, } \varepsilon^k$$

For a circuit C, using G_{add}, G_{copy}, G_{mult}:

$$G_{add}, G_{copy}, G_{mult} \textbf{ RP-Expandable, } \varepsilon \quad \Longrightarrow \quad \textbf{Compiled circuit } (p, 2.|C|.\varepsilon^k)\textbf{-RP Secure}$$

RP Expansion

Parameters

Security parameter κ, (t, p, ε)-RP expandable gadgets $G_{\mathsf{add}}, G_{\mathsf{copy}}, G_{\mathsf{mult}}$, circuit C to expand, complexity:

RP Expansion

Parameters

Security parameter κ, (t, p, ε)-RP expandable gadgets $G_{\text{add}}, G_{\text{copy}}, G_{\text{mult}}$, circuit C to expand, complexity:

$$\mathcal{O}(|C|.\kappa^e), \quad e = \frac{log(\mathrm{N}_{\max})}{log(\mathrm{d})}$$

RP Expansion

Parameters

Security parameter κ, (t, p, ε)-RP expandable gadgets $G_{\text{add}}, G_{\text{copy}}, G_{\text{mult}}$, circuit C to expand, complexity:

$$\mathcal{O}(|C|.\kappa^e), \quad e = \frac{log(\mathrm{N}_{\max})}{log(\mathrm{d})}$$

$\mathbf{N_{max}} \approx \max($ Nb. of $\times$ in G_{mult}, Nb. of $+, ||$ in $G_{\text{add}}, G_{\text{copy}})$

RP Expansion

Parameters

Security parameter κ, (t, p, ε)-RP expandable gadgets $G_{\text{add}}, G_{\text{copy}}, G_{\text{mult}}$, circuit C to expand, complexity:

$$\mathcal{O}(|C|.\kappa^e), \quad e = \frac{log(\mathrm{N}_{\max})}{log(\mathrm{d})}$$

$\mathbf{N_{max}} \approx \max($ Nb. of $\times$ in G_{mult}, Nb. of $+, ||$ in $G_{\text{add}}, G_{\text{copy}})$

d: amplification order (*i.e.* smallest failure set of internal wires)

RP Expansion

Parameters

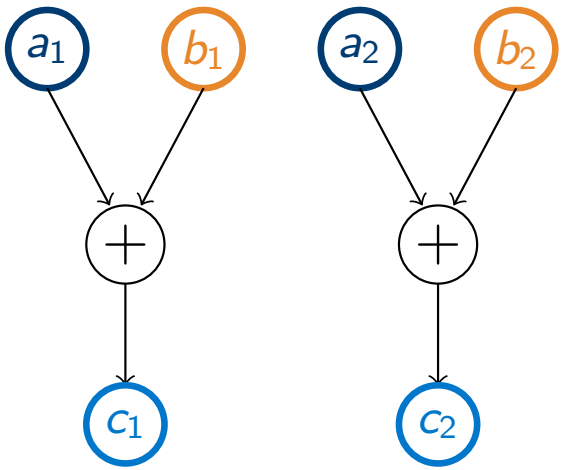
Security parameter κ, (t, p, ε)-RP expandable gadgets $G_{\text{add}}, G_{\text{copy}}, G_{\text{mult}}$, circuit C to expand, complexity:

$$\mathcal{O}(|C|.\kappa^e), \quad e = \frac{log(\mathrm{N}_{\max})}{log(\mathrm{d})}$$

$\mathbf{N_{max}} \approx \max($ Nb. of $\times$ in G_{mult}, Nb. of $+, ||$ in $G_{\text{add}}, G_{\text{copy}})$

d: amplification order (*i.e.* smallest failure set of internal wires)

Example $t = 1$, $n = 2$



RP Expansion

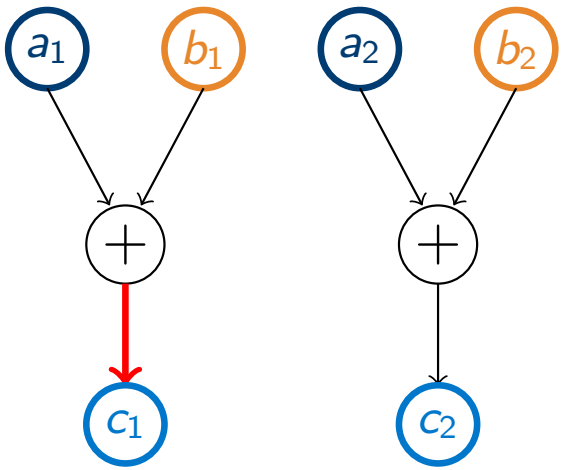
Parameters

Security parameter κ, (t, p, ε)-RP expandable gadgets $G_{\text{add}}, G_{\text{copy}}, G_{\text{mult}}$, circuit C to expand, complexity:

$$\mathcal{O}(|C|.\kappa^e), \quad e = \frac{log(\mathrm{N}_{\max})}{log(\mathrm{d})}$$

$\mathbf{N_{max}} \approx \max($ Nb. of $\times$ in G_{mult}, Nb. of $+, ||$ in $G_{\text{add}}, G_{\text{copy}})$

d: amplification order (*i.e.* smallest failure set of internal wires)



Example $t = 1$, $n = 2$

Output $c_1 = a_1 + b_1$,

RP Expansion

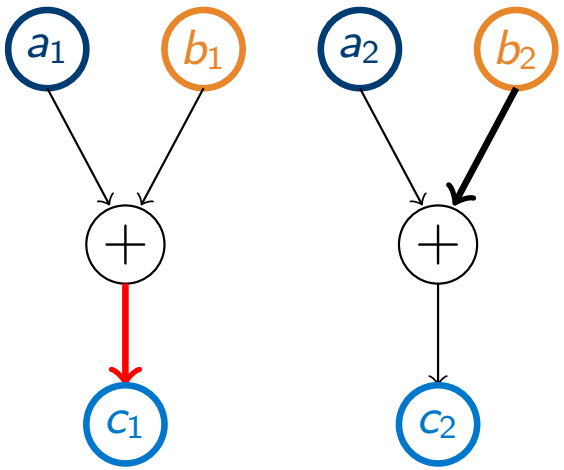
Parameters

Security parameter κ, (t, p, ε)-RP expandable gadgets $G_{\text{add}}, G_{\text{copy}}, G_{\text{mult}}$, circuit C to expand, complexity:

$$\mathcal{O}(|C|.\kappa^e), \quad e = \frac{log(\mathrm{N}_{\max})}{log(\mathrm{d})}$$

$\mathbf{N_{max}} \approx \max($ Nb. of $\times$ in G_{mult}, Nb. of $+, ||$ in $G_{\text{add}}, G_{\text{copy}})$

d: amplification order (*i.e.* smallest failure set of internal wires)



Example $t = 1$, $n = 2$

Output $c_1 = a_1 + b_1$, **set** $\mathbf{W} = \{b_2\}$

RP Expansion

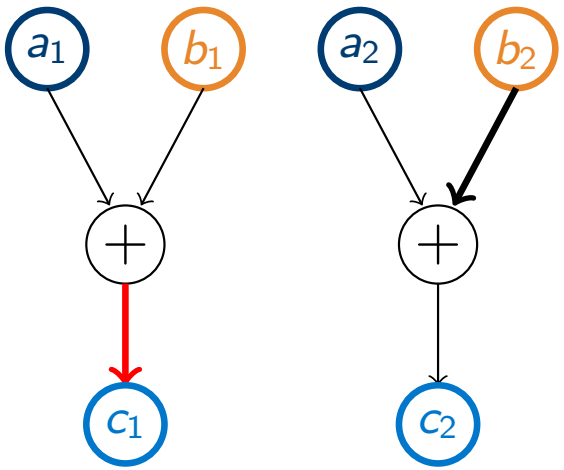
Parameters

Security parameter κ, (t, p, ε)-RP expandable gadgets $G_{\text{add}}, G_{\text{copy}}, G_{\text{mult}}$, circuit C to expand, complexity:

$$\mathcal{O}(|C|.\kappa^e), \quad e = \frac{log(\mathrm{N}_{\max})}{log(\mathrm{d})}$$

$\mathbf{N_{max}} \approx \max($ Nb. of $\times$ in G_{mult}, Nb. of $+, ||$ in $G_{\text{add}}, G_{\text{copy}})$

d: amplification order (*i.e.* smallest failure set of internal wires)



Example $t = 1$, $n = 2$

Output $c_1 = a_1 + b_1$, **set** $\mathbf{W} = \{b_2\}$

Simulation needs a_1 $(\leq t)$ and b_1, b_2 $(> t)$

RP Expansion

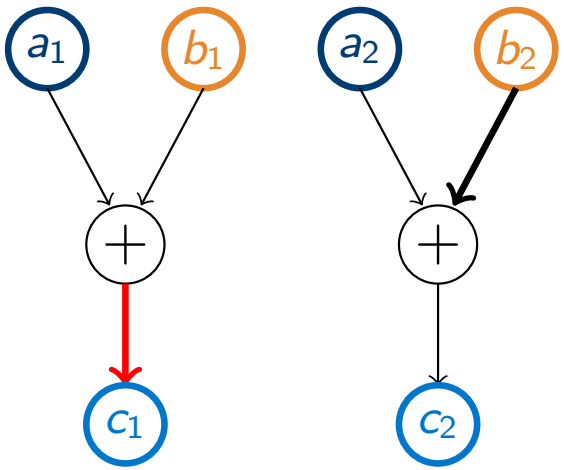
Parameters

Security parameter κ, (t, p, ε)-RP expandable gadgets $G_{\text{add}}, G_{\text{copy}}, G_{\text{mult}}$, circuit C to expand, complexity:

$$\mathcal{O}(|C|.\kappa^e), \quad e = \frac{log(\mathrm{N}_{\max})}{log(\mathrm{d})}$$

$\mathbf{N_{max}} \approx \max($ Nb. of $\times$ in G_{mult}, Nb. of $+, ||$ in $G_{\text{add}}, G_{\text{copy}})$

d: amplification order (*i.e.* smallest failure set of internal wires)



Example $t = 1$, $n = 2$

Output $c_1 = a_1 + b_1$, **set** $\mathbf{W} = \{b_2\}$

Simulation needs a_1 $(\leq t)$ and b_1, b_2 $(> t)$

Failure on b

RP Expansion

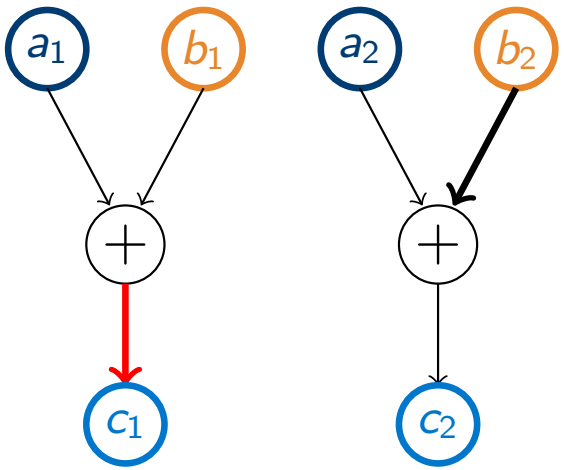
Parameters

Security parameter κ, (t, p, ε)-RP expandable gadgets $G_{\text{add}}, G_{\text{copy}}, G_{\text{mult}}$, circuit C to expand, complexity:

$$\mathcal{O}(|C|.\kappa^e), \quad e = \frac{log(\mathrm{N}_{\max})}{log(\mathrm{d})}$$

$\mathbf{N_{max}} \approx \max($ Nb. of $\times$ in G_{mult}, Nb. of $+, ||$ in $G_{\text{add}}, G_{\text{copy}})$

d: amplification order (*i.e.* smallest failure set of internal wires)



Example $t = 1$, $n = 2$

Output $c_1 = a_1 + b_1$, **set** $\mathbf{W} = \{b_2\}$

Simulation needs a_1 $(\leq t)$ and b_1, b_2 $(> t)$

Failure on $b \implies \mathbf{d} = |W| = \mathbf{1}$

RP Expansion

Parameters

Security parameter κ, (t, p, ε)-RP expandable gadgets $G_{\text{add}}, G_{\text{copy}}, G_{\text{mult}}$, circuit C to expand, complexity:

$$\mathcal{O}(|C|.\kappa^e), \quad e = \frac{log(\mathrm{N}_{\max})}{log(\mathrm{d})}$$

$\mathbf{N_{max}} \approx \max($ Nb. of $\times$ in G_{mult}, Nb. of $+, ||$ in $G_{\text{add}}, G_{\text{copy}})$

d: amplification order (*i.e.* smallest failure set of internal wires)

$$\varepsilon = f(p) = c_{\mathbf{d}} \cdot p^{\mathbf{d}} + \mathcal{O}(p^{\mathbf{d}+1})$$

RP Expansion

Parameters

Security parameter κ, (t, p, ε)-RP expandable gadgets $G_{\text{add}}, G_{\text{copy}}, G_{\text{mult}}$, circuit C to expand, complexity:

$$\mathcal{O}(|C|.\kappa^e), \quad e = \frac{log(\mathrm{N}_{\max})}{log(\mathrm{d})}$$

$\mathbf{N_{max}} \approx \max($ Nb. of $\times$ in G_{mult}, Nb. of $+, ||$ in $G_{\text{add}}, G_{\text{copy}})$

d: amplification order (*i.e.* smallest failure set of internal wires)

$$\varepsilon = f(p) = c_{\mathbf{d}} \cdot p^{\mathbf{d}} + \mathcal{O}(p^{\mathbf{d}+1})$$

- during expansion: $\varepsilon^k = f^{(k)}(p) = f(f(\ldots f(f(p))\ldots))$

RP Expansion

Parameters

Security parameter κ, (t, p, ε)-RP expandable gadgets $G_{\text{add}}, G_{\text{copy}}, G_{\text{mult}}$, circuit C to expand, complexity:

$$\mathcal{O}(|C|.\kappa^e), \quad e = \frac{log(\mathrm{N}_{\max})}{log(\mathrm{d})}$$

$\mathbf{N_{max}} \approx \max($ Nb. of $\times$ in G_{mult}, Nb. of $+, ||$ in $G_{\text{add}}, G_{\text{copy}})$

d: amplification order (*i.e.* smallest failure set of internal wires)

$$\varepsilon = f(p) = c_{\mathbf{d}} \cdot p^{\mathbf{d}} + \mathcal{O}(p^{\mathbf{d}+1})$$

- during expansion: $\varepsilon^k = f^{(k)}(p) = f(f(\ldots f(f(p))\ldots))$
- higher **d** $\implies$ faster decrease in failure probability

First Bound on d (with respect to t)

First Bound on d (with respect to t)

n-share circuit with input a

First Bound on d (with respect to t)

n-share circuit with input a

$W = \{a_1, \ldots, a_{t+1}\}$ of $t + 1$ probes

First Bound on d (with respect to t)

n-share circuit with input a

$W = \{a_1, \ldots, a_{t+1}\}$ of $t+1$ probes

Need all $t+1$ shares to simulate $W \implies$ failure

First Bound on d (with respect to t)

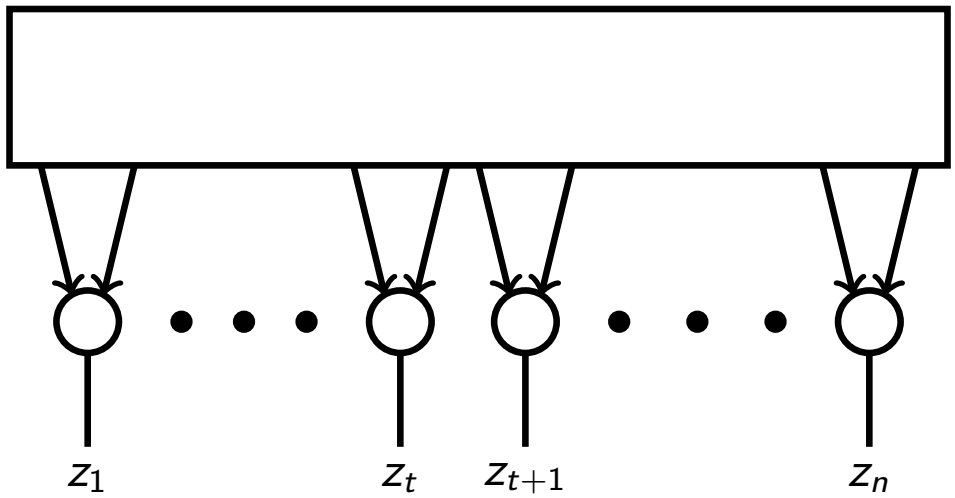
n-share circuit with input a

$W = \{a_1, \ldots, a_{t+1}\}$ of $t+1$ probes

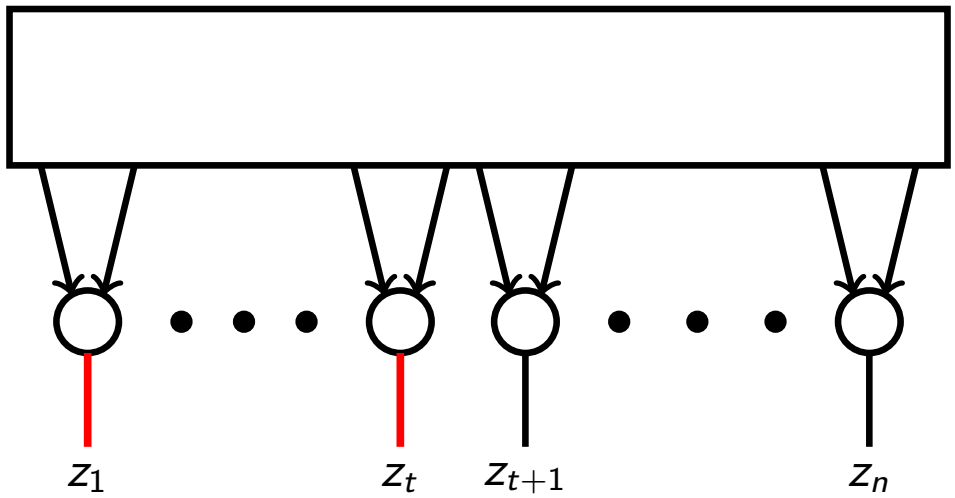
Need all $t+1$ shares to simulate $W \implies$ failure

$$\mathrm{d} \leq \mathrm{t} + 1$$

Second Bound on d (with respect to t)

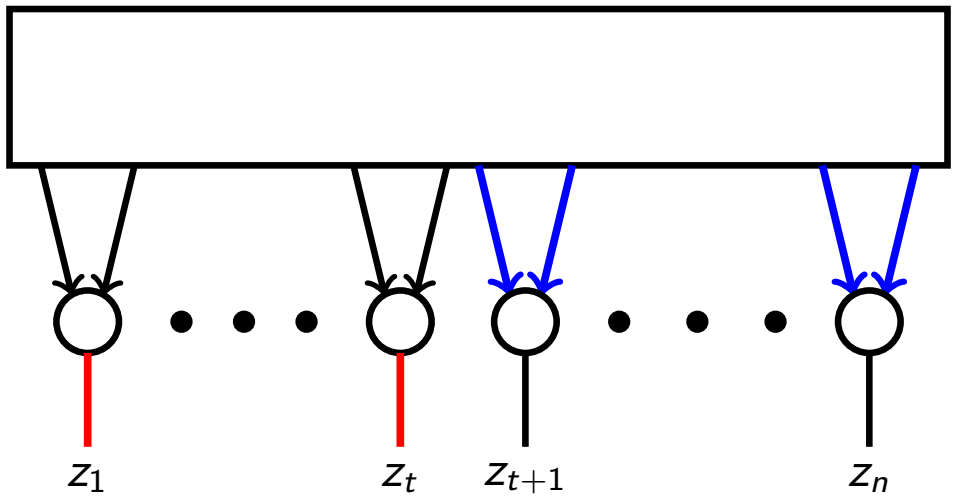


Second Bound on d (with respect to t)



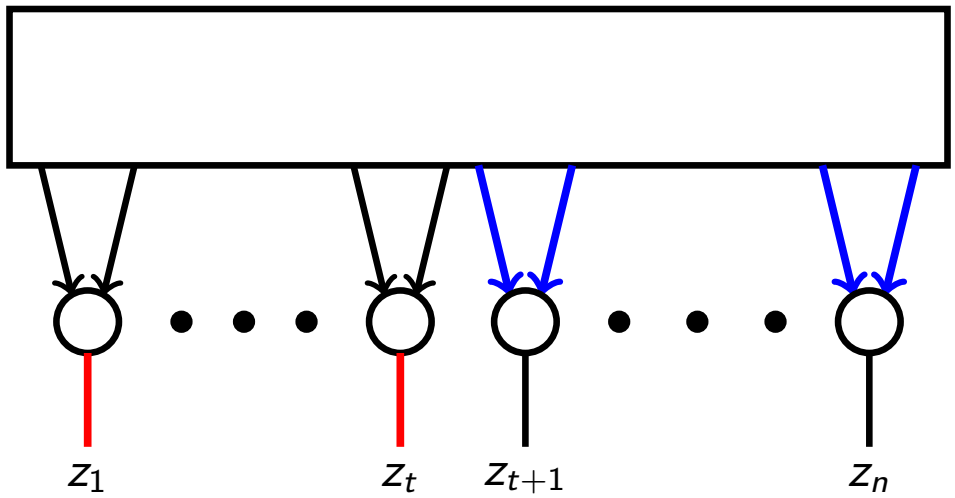
$J = \{1, \ldots, t\}$

Second Bound on d (with respect to t)



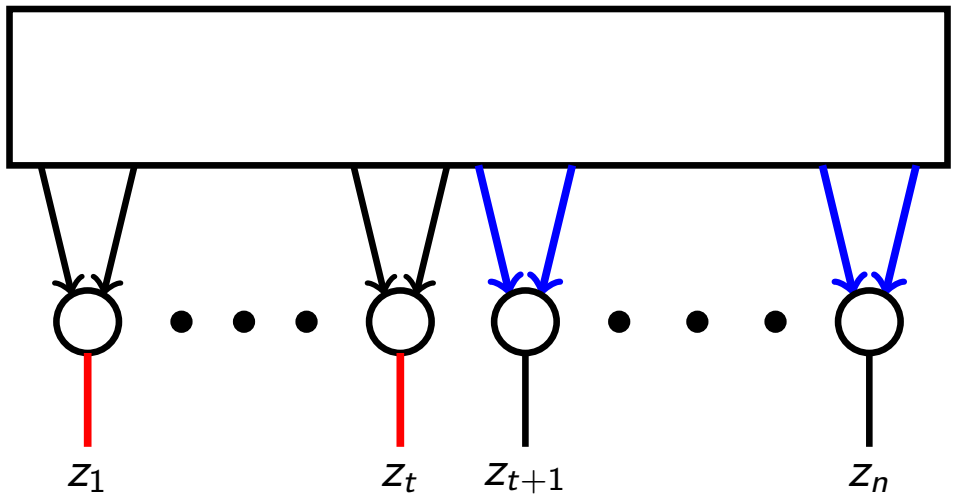
$J = \{1, \ldots, t\}$ $\quad |W| = 2(n - t)$

Second Bound on d (with respect to t)



- 1-input gadgets $\longrightarrow$ $d \leq 2(n-t)$

Second Bound on d (with respect to t)



- 1-input gadgets $\longrightarrow$ $d \leq 2(n-t)$
- 2-input gadgets $\longrightarrow$ $d' \leq \frac{d}{2} \leq (n-t)$ (Failure on both inputs with independent failure events)

RP Expansion

Bounding the Amplification Order

(t, p, ε)-RPE compiler with $G_{\mathsf{add}}, G_{\mathsf{copy}}, G_{\mathsf{mult}}$

RP Expansion

Bounding the Amplification Order

(t, p, ε)-RPE compiler with $G_{\mathsf{add}}, G_{\mathsf{copy}}, G_{\mathsf{mult}}$

- $d \leq \min(t + 1, n - t)$

RP Expansion

Bounding the Amplification Order

(t, p, ε)-RPE compiler with $G_{\mathsf{add}}, G_{\mathsf{copy}}, G_{\mathsf{mult}}$

- $d \leq \min(t+1, n-t)$
- $d_{\max} = \dfrac{n+1}{2}$

RP Expansion

Bounding the Amplification Order

(t, p, ε)-RPE compiler with $G_{\mathsf{add}}, G_{\mathsf{copy}}, G_{\mathsf{mult}}$

- $d \leq \min(t+1, n-t)$
- $d_{\max} = \dfrac{n+1}{2}$

Goal: construct **generic** gadgets achieving $d_{\max}$.

RP Expansion

Bounding the Amplification Order

(t, p, ε)-RPE compiler with $G_{\mathsf{add}}, G_{\mathsf{copy}}, G_{\mathsf{mult}}$

- $d \leq \min(t+1, n-t)$
- $d_{\max} = \dfrac{n+1}{2}$

Goal: construct **generic** gadgets achieving $d_{\max}$.

Idea:

RP Expansion

Bounding the Amplification Order

(t, p, ε)-RPE compiler with $G_{\mathsf{add}}, G_{\mathsf{copy}}, G_{\mathsf{mult}}$

- $d \leq \min(t+1, n-t)$
- $d_{\max} = \dfrac{n+1}{2}$

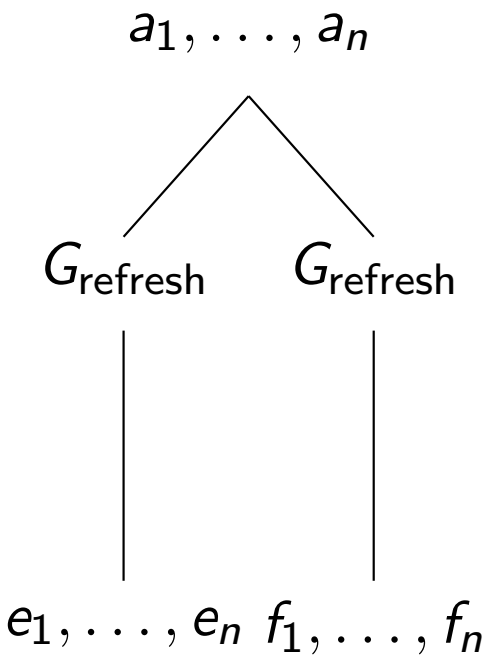
Goal: construct **generic** gadgets achieving $d_{\max}$.

Idea:

- build G_{add}, G_{copy} from single building block G_{refresh} (easier conception)
- use G_{mult} from state of the art (*e.g.* ISW, ...)

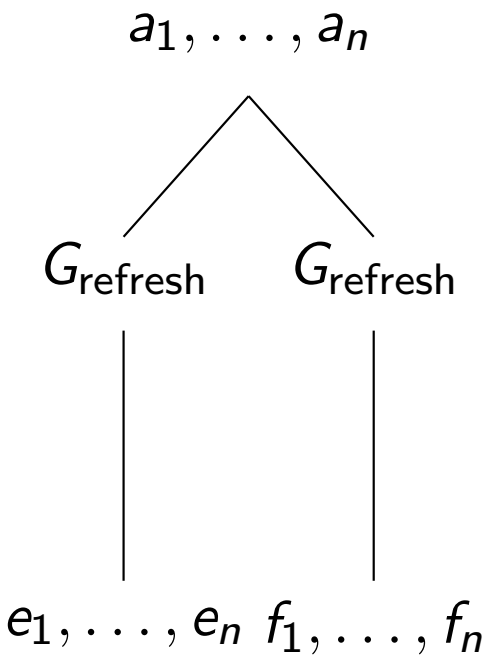
Generic Constructions

Copy Gadget



Generic Constructions

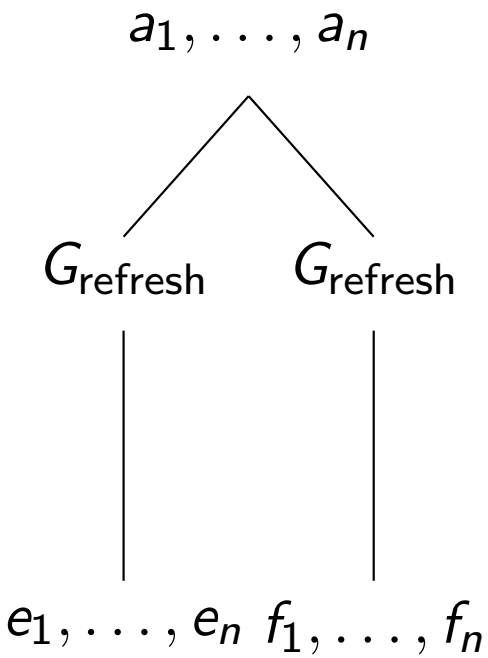
Copy Gadget



(t, p, ε)-RPE G_{refresh} achieves $d_{\max}$ $\Longrightarrow$
(t, p, ε')-RPE G_{copy} achieves $d_{\max}$

Generic Constructions

Copy Gadget

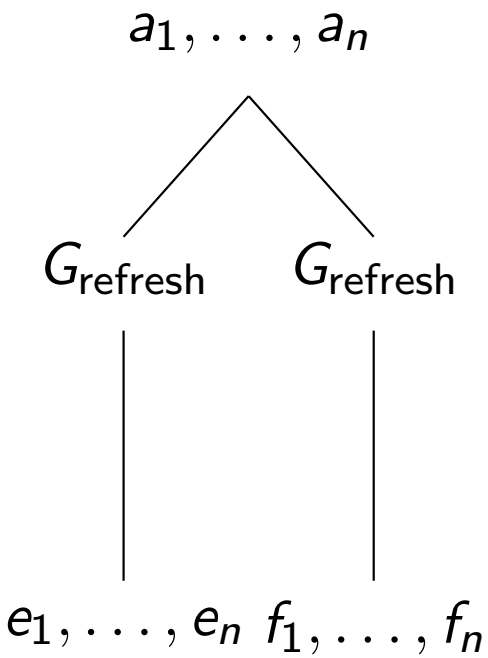


Idea:

(t, p, ε)-RPE G_{refresh} achieves $d_{\max}$ $\Longrightarrow$
(t, p, ε')-RPE G_{copy} achieves $d_{\max}$

Generic Constructions

Copy Gadget



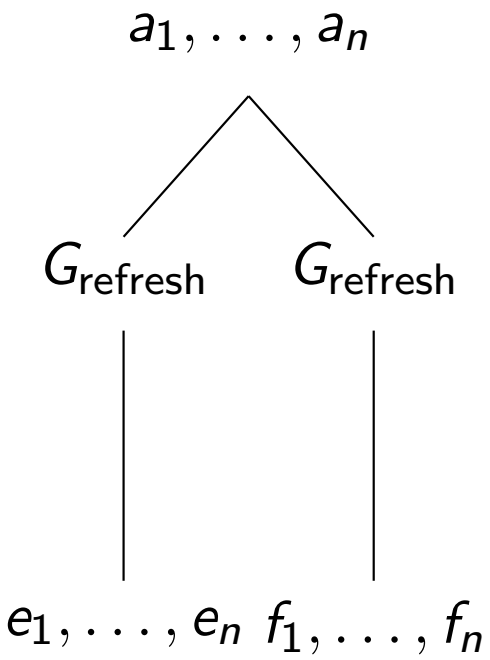
(t, p, ε)-RPE G_{refresh} achieves $d_{\max}$ $\Longrightarrow$
(t, p, ε')-RPE G_{copy} achieves $d_{\max}$

Idea:

- probes on G_{copy} = **left** probes on G_{refresh} $\cup$ **right** probes on G_{refresh} (independent)

Generic Constructions

Copy Gadget



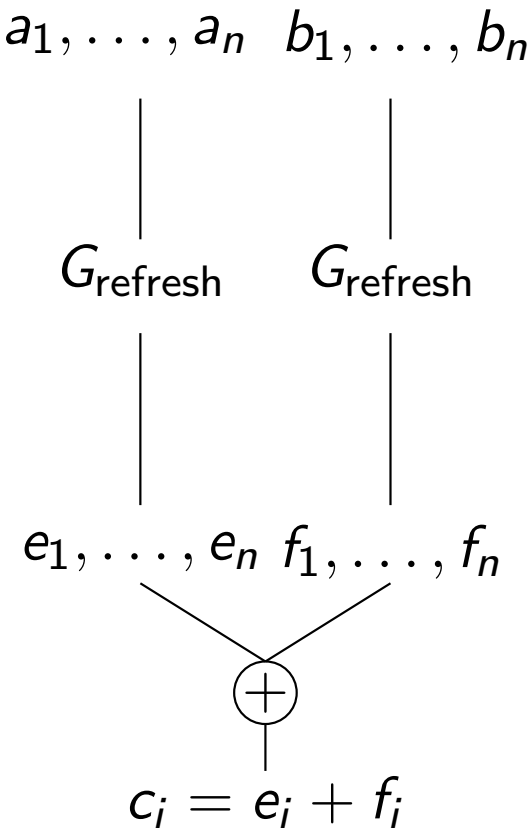
(t, p, ε)-RPE G_{refresh} achieves $d_{\max} \implies$
(t, p, ε')-RPE G_{copy} achieves $d_{\max}$

Idea:

- probes on $G_{\text{copy}} =$ **left** probes on $G_{\text{refresh}} \cup$ **right** probes on G_{refresh} (independent)
- **left** simulation success + **right** simulation success $\implies$ overall simulation success

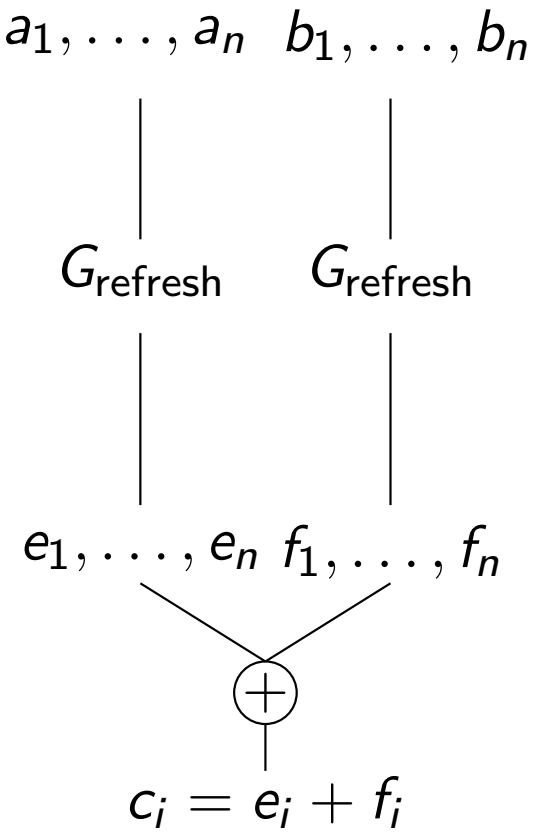
Generic Constructions

Addition Gadget



Generic Constructions

Addition Gadget

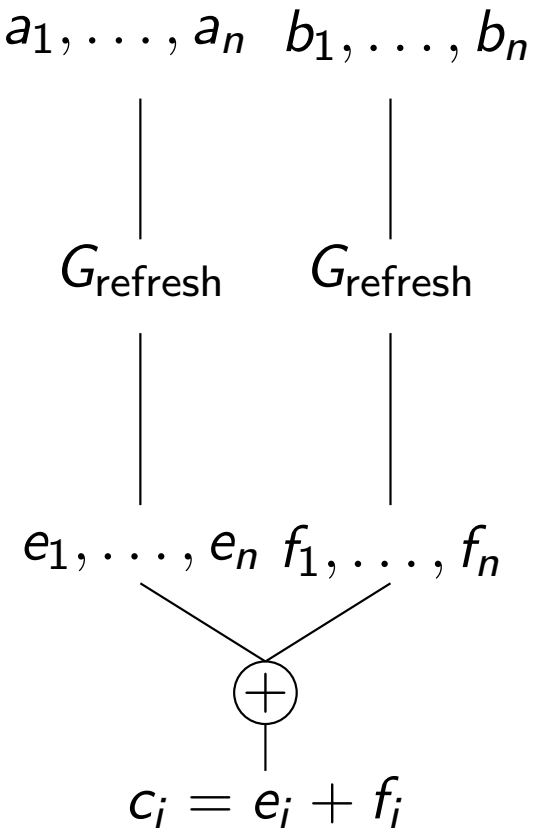


(t, p, ε)-RPE G_{refresh} achieves $d_{\max}$ $\Longrightarrow$

(t, p, ε')-RPE G_{add} achieves **at least** $\dfrac{d_{\max}}{2}$

Generic Constructions

Addition Gadget

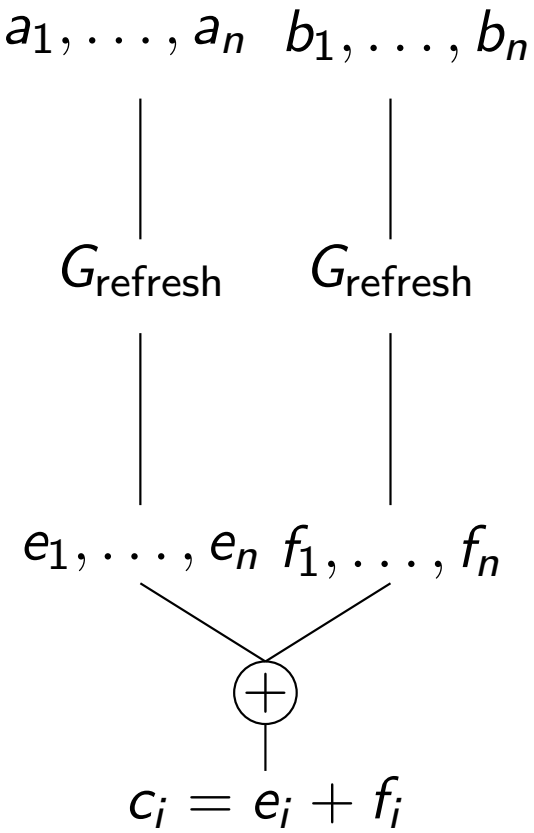


(t, p, ε)-RPE G_{refresh} achieves $d_{\max} \implies$
(t, p, ε')-RPE G_{add} achieves **at least** $\frac{d_{\max}}{2}$

Idea:

Generic Constructions

Addition Gadget



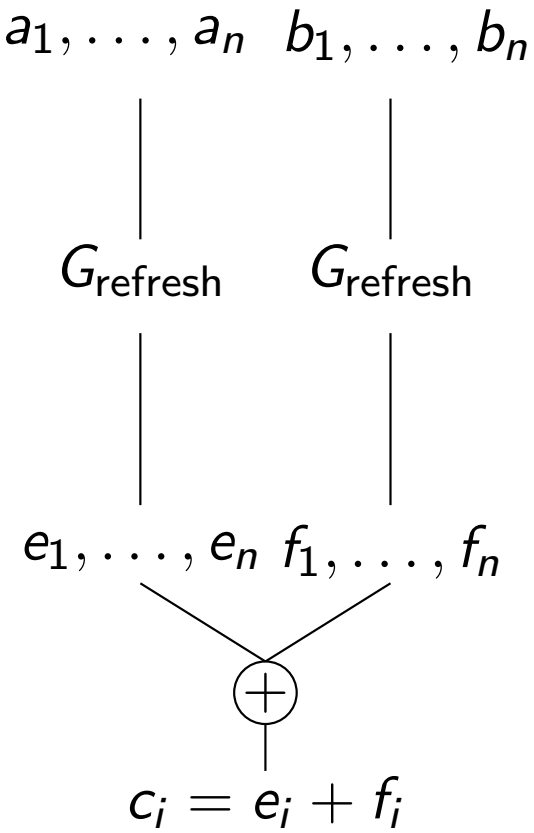
$$(t, p, \varepsilon)\text{-RPE } G_{\text{refresh}} \text{ achieves } d_{\max} \implies$$
$$(t, p, \varepsilon')\text{-RPE } G_{\text{add}} \text{ achieves } \textbf{at least } \frac{d_{\max}}{2}$$

Idea:

- similar to the case of G_{copy} (left probes + right probes)

Generic Constructions

Addition Gadget



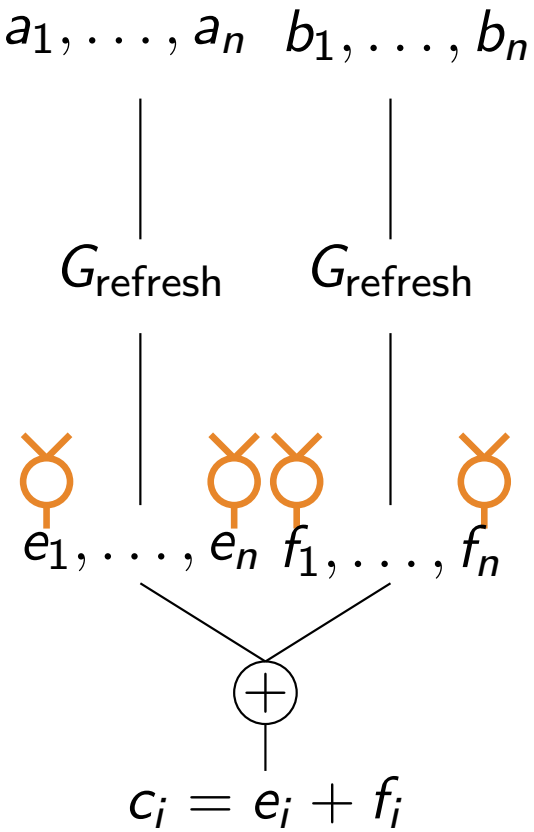
(t, p, ε)-RPE G_{refresh} achieves $d_{\max} \implies$
(t, p, ε')-RPE G_{add} achieves **at least** $\frac{d_{\max}}{2}$

Idea:

- similar to the case of G_{copy} (left probes + right probes)
- **exception:** potential internal probes on $\{e_i\}_{i \in [n]}$, $\{f_i\}_{i \in [n]}$ (output shares of G_{refresh}s)

Generic Constructions

Addition Gadget



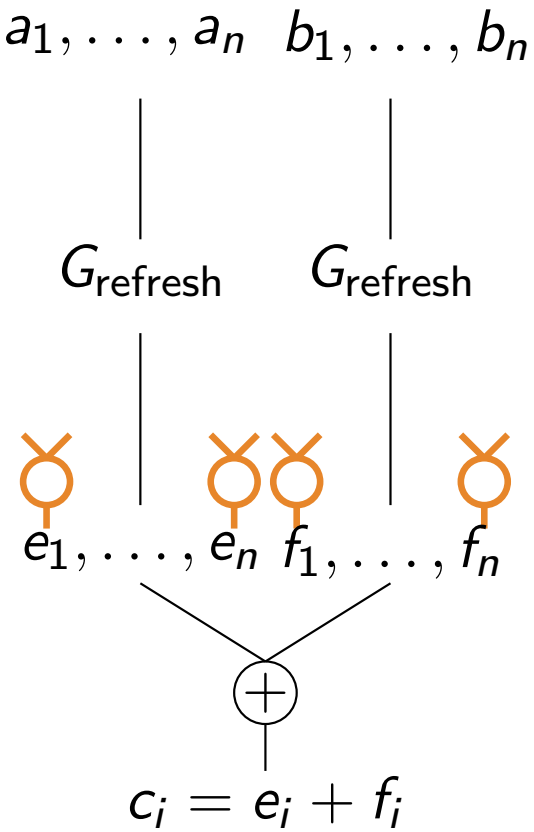
(t, p, ε)-RPE G_{refresh} achieves $d_{\max} \implies$
(t, p, ε')-RPE G_{add} achieves **at least** $\frac{d_{\max}}{2}$

Idea:

- similar to the case of G_{copy} (left probes + right probes)
- **exception:** potential internal probes on $\{e_i\}_{i\in[n]}$, $\{f_i\}_{i\in[n]}$ (output shares of G_{refresh}s)
- **solution:** replace each by 2 wires input of corresponding output gate

Generic Constructions

Addition Gadget



(t, p, ε)-RPE G_{refresh} achieves $d_{\max}$ $\Longrightarrow$
(t, p, ε')-RPE G_{add} achieves **at least** $\frac{d_{\max}}{2}$

Idea:

- similar to the case of G_{copy} (left probes + right probes)
- **exception:** potential internal probes on $\{e_i\}_{i\in[n]}$, $\{f_i\}_{i\in[n]}$ (output shares of G_{refresh}s)
- **solution:** replace each by 2 wires input of corresponding output gate
- double number of probes $\Longrightarrow$ at least $d_{\max}/2$

Generic Constructions

ISW-based construction

Generic Constructions

ISW-based construction

ISW $G_{\mathsf{refresh}} \longrightarrow$ RPE achieving $d_{\mathsf{max}} = \dfrac{n+1}{2}$

Generic Constructions

ISW-based construction

ISW $G_{\text{refresh}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$

ISW $G_{\text{copy}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$

Generic Constructions

ISW-based construction

ISW $G_{\text{refresh}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$

ISW $G_{\text{copy}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$

ISW $G_{\text{add}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$ (**Better than generic result**)

Generic Constructions

ISW-based construction

ISW $G_{\text{refresh}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$

ISW $G_{\text{copy}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$

ISW $G_{\text{add}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$ (**Better than generic result**)

ISW $G_{\text{mult}} \longrightarrow$ RPE achieving $\dfrac{d_{\max}}{2} = \dfrac{n+1}{4}$ **!!**

Generic Constructions

ISW-based construction

ISW $G_{\text{refresh}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$

ISW $G_{\text{copy}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$

ISW $G_{\text{add}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$ (**Better than generic result**)

ISW $G_{\text{mult}} \longrightarrow$ RPE achieving $\dfrac{d_{\max}}{2} = \dfrac{n+1}{4}$ **!!**

Why?

Generic Constructions

ISW-based construction

ISW $G_{\text{refresh}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$

ISW $G_{\text{copy}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$

ISW $G_{\text{add}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$ (**Better than generic result**)

ISW $G_{\text{mult}} \longrightarrow$ RPE achieving $\dfrac{d_{\max}}{2} = \dfrac{n+1}{4}$ **!!**

Why?

- direct product of input shares

Generic Constructions

ISW-based construction

ISW $G_{\text{refresh}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$

ISW $G_{\text{copy}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$

ISW $G_{\text{add}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$ (**Better than generic result**)

ISW $G_{\text{mult}} \longrightarrow$ RPE achieving $\dfrac{d_{\max}}{2} = \dfrac{n+1}{4}$ **!!**

Why?

- direct product of input shares
- $W = \{a_1 \times b_1, \ldots, a_{t+1} \times b_{t+1}\}$ simulation needs $t+1$ shares of a **and** b

Generic Constructions

ISW-based construction

ISW $G_{\text{refresh}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$

ISW $G_{\text{copy}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$

ISW $G_{\text{add}} \longrightarrow$ RPE achieving $d_{\max} = \dfrac{n+1}{2}$ (**Better than generic result**)

ISW $G_{\text{mult}} \longrightarrow$ RPE achieving $\dfrac{d_{\max}}{2} = \dfrac{n+1}{4}$ **!!**

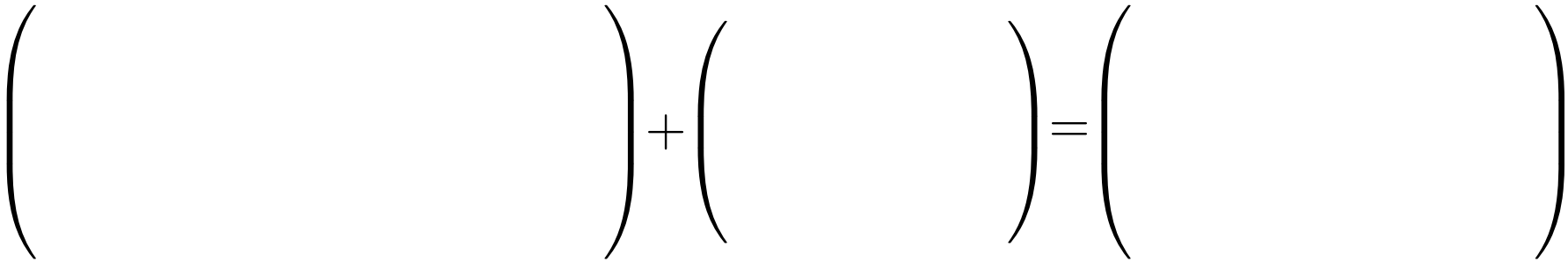
Why?

- direct product of input shares
- $W = \{a_1 \times b_1, \ldots, a_{t+1} \times b_{t+1}\}$ simulation needs $t+1$ shares of a **and** b
- Failure on both inputs with independent failure events

Generic Constructions

New Multiplication Gadget

Inputs a,b (illustration with 3 shares)



Generic Constructions

New Multiplication Gadget

Inputs a,b (illustration with 3 shares)

$$\begin{pmatrix} a_1 \cdot b_1 & a_1 \cdot b_2 & a_1 \cdot b_3 \\ a_2 \cdot b_1 & a_2 \cdot b_2 & a_2 \cdot b_3 \\ a_3 \cdot b_1 & a_3 \cdot b_2 & a_3 \cdot b_3 \end{pmatrix} + \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix} = \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix}$$

Generic Constructions

New Multiplication Gadget

Inputs a,b (illustration with 3 shares)

$$\begin{pmatrix} a_1 \cdot b_1 & a_1 \cdot b_2 & a_1 \cdot b_3 \\ a_2 \cdot b_1 & a_2 \cdot b_2 & a_2 \cdot b_3 \\ a_3 \cdot b_1 & a_3 \cdot b_2 & a_3 \cdot b_3 \end{pmatrix} + \begin{pmatrix} r_1 & r_2 & r_3 \\ r_4 & r_5 & r_6 \\ r_7 & r_8 & r_9 \end{pmatrix} = \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix}$$

Inputs a,b (illustration with 3 shares)

$$\begin{pmatrix} a_1 \cdot b_1 & a_1 \cdot b_2 & a_1 \cdot b_3 \\ a_2 \cdot b_1 & a_2 \cdot b_2 & a_2 \cdot b_3 \\ a_3 \cdot b_1 & a_3 \cdot b_2 & a_3 \cdot b_3 \end{pmatrix} + \begin{pmatrix} r_1 & r_2 & r_3 \\ r_4 & r_5 & r_6 \\ r_7 & r_8 & r_9 \end{pmatrix} = \begin{pmatrix} p_{1,1} & p_{1,2} & p_{1,3} \\ p_{2,1} & p_{2,2} & p_{2,3} \\ p_{3,1} & p_{3,2} & p_{3,3} \end{pmatrix}$$

Generic Constructions

New Multiplication Gadget

Inputs a,b (illustration with 3 shares)

$$\begin{pmatrix} a_1 \cdot b_1 & a_1 \cdot b_2 & a_1 \cdot b_3 \\ a_2 \cdot b_1 & a_2 \cdot b_2 & a_2 \cdot b_3 \\ a_3 \cdot b_1 & a_3 \cdot b_2 & a_3 \cdot b_3 \end{pmatrix} + \begin{pmatrix} r_1 & r_2 & r_3 \\ r_4 & r_5 & r_6 \\ r_7 & r_8 & r_9 \end{pmatrix} = \begin{pmatrix} p_{1,1} & p_{1,2} & p_{1,3} \\ p_{2,1} & p_{2,2} & p_{2,3} \\ p_{3,1} & p_{3,2} & p_{3,3} \end{pmatrix}$$

$$\mathbf{v} = \begin{pmatrix} p_{1,1} + p_{1,2} + p_{1,3} \\ p_{2,1} + p_{2,2} + p_{2,3} \\ p_{3,1} + p_{3,2} + p_{3,3} \end{pmatrix}$$

Inputs a, b (illustration with 3 shares)

$$\begin{pmatrix} a_1 \cdot b_1 & a_1 \cdot b_2 & a_1 \cdot b_3 \\ a_2 \cdot b_1 & a_2 \cdot b_2 & a_2 \cdot b_3 \\ a_3 \cdot b_1 & a_3 \cdot b_2 & a_3 \cdot b_3 \end{pmatrix} + \begin{pmatrix} r_1 & r_2 & r_3 \\ r_4 & r_5 & r_6 \\ r_7 & r_8 & r_9 \end{pmatrix} = \begin{pmatrix} p_{1,1} & p_{1,2} & p_{1,3} \\ p_{2,1} & p_{2,2} & p_{2,3} \\ p_{3,1} & p_{3,2} & p_{3,3} \end{pmatrix}$$

$$\mathbf{V} = \begin{pmatrix} p_{1,1} + p_{1,2} + p_{1,3} \\ p_{2,1} + p_{2,2} + p_{2,3} \\ p_{3,1} + p_{3,2} + p_{3,3} \end{pmatrix} \qquad \mathbf{X} = \begin{pmatrix} r_1 + r_4 + r_7 \\ r_2 + r_5 + r_8 \\ r_3 + r_6 + r_9 \end{pmatrix}$$

Output $C = V + X$

Generic Constructions

New Multiplication Gadget

Non-standard G_{mult}

Non-standard G_{mult}

$$\begin{pmatrix} a_1 \cdot b_1 & a_1 \cdot b_2 & a_1 \cdot b_3 \\ a_2 \cdot b_1 & a_2 \cdot b_2 & a_2 \cdot b_3 \\ a_3 \cdot b_1 & a_3 \cdot b_2 & a_3 \cdot b_3 \end{pmatrix}$$

where b, b, b are three independent fresh copies of b using G_{refresh}

Generic Constructions

New Multiplication Gadget

Non-standard G_{mult}

$$\begin{pmatrix} a_1 \cdot b_1 & a_1 \cdot b_2 & a_1 \cdot b_3 \\ a_2 \cdot b_1 & a_2 \cdot b_2 & a_2 \cdot b_3 \\ a_3 \cdot b_1 & a_3 \cdot b_2 & a_3 \cdot b_3 \end{pmatrix}$$

where b, b, b are three independent fresh copies of b using G_{refresh}

- G_{refresh} (t, p, ε)-RPE achieves d_{max} $\Longrightarrow$ G_{mult} (t, p, ε)-RPE achieves d_{max}

Non-standard G_{mult}

$$\begin{pmatrix} a_1 \cdot b_1 & a_1 \cdot b_2 & a_1 \cdot b_3 \\ a_2 \cdot b_1 & a_2 \cdot b_2 & a_2 \cdot b_3 \\ a_3 \cdot b_1 & a_3 \cdot b_2 & a_3 \cdot b_3 \end{pmatrix}$$

where b, b, b are three independent fresh copies of b using G_{refresh}

- G_{refresh} (t, p, ε)-RPE achieves d_{max} $\implies$ G_{mult} (t, p, ε)-RPE achieves d_{max}
- New G_{mult} achieves $d_{\mathsf{max}} = \dfrac{n+1}{2}$ (unlike ISW mult.)

Generic Constructions

New Multiplication Gadget

Non-standard G_{mult}

$$\begin{pmatrix} a_1 \cdot b_1 & a_1 \cdot b_2 & a_1 \cdot b_3 \\ a_2 \cdot b_1 & a_2 \cdot b_2 & a_2 \cdot b_3 \\ a_3 \cdot b_1 & a_3 \cdot b_2 & a_3 \cdot b_3 \end{pmatrix}$$

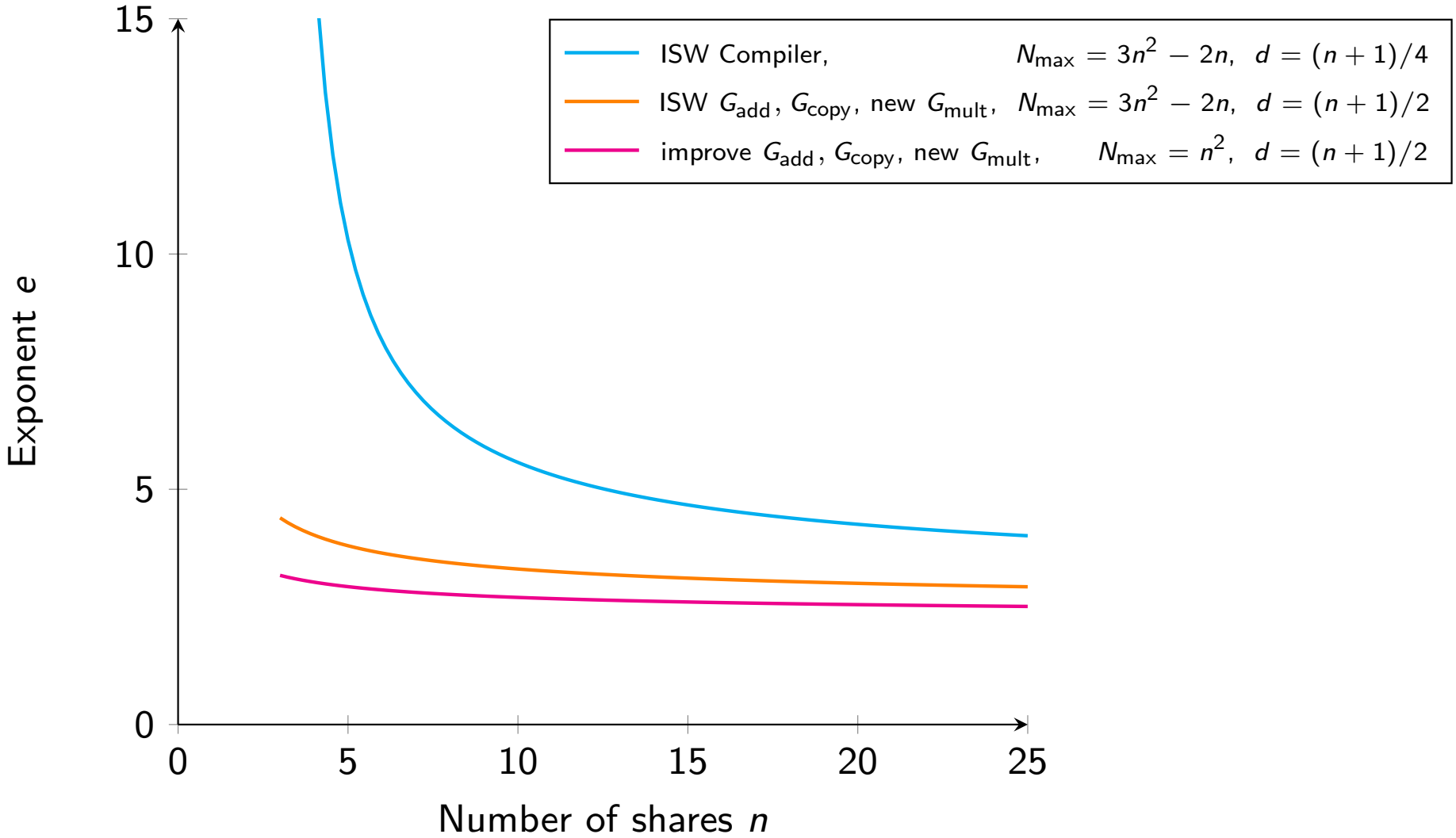
where b, b, b are three independent fresh copies of b using G_{refresh}

- G_{refresh} (t, p, ε)-RPE achieves $d_{\max}$ $\implies$ G_{mult} (t, p, ε)-RPE achieves $d_{\max}$
- New G_{mult} achieves $d_{\max} = \dfrac{n+1}{2}$ (unlike ISW mult.)
- The only multiplication gadget achieving $d_{\max}$ for any number of shares

Generic Constructions

Asymptotic Complexity

$$\mathcal{O}(|C|.\kappa^e), \quad e = \frac{log(N_{\max})}{d}$$



Concrete RPE instantiations

Concrete RPE instantiations

3-share

G_{ref} : $c_1 \leftarrow a_1 + r_1$

$c_2 \leftarrow a_2 + r_2$

$c_3 \leftarrow (r_1 + r_2) + a_3$

Concrete RPE instantiations

3-share

$$
\begin{aligned}
G_{ref} : c_1 &\leftarrow a_1 + r_1 \\
c_2 &\leftarrow a_2 + r_2 \\
c_3 &\leftarrow (r_1 + r_2) + a_3
\end{aligned}
$$

5-share

$$
\begin{aligned}
G_{ref} : c_1 &\leftarrow (r_1 + r_2) + a_1 \\
c_2 &\leftarrow (r_2 + r_3) + a_2 \\
c_3 &\leftarrow (r_3 + r_4) + a_3 \\
c_4 &\leftarrow (r_4 + r_5) + a_4 \\
c_5 &\leftarrow (r_5 + r_1) + a_5
\end{aligned}
$$

Concrete RPE instantiations

3-share

$$
\begin{aligned}
G_{ref} : c_1 &\leftarrow a_1 + r_1 \\
c_2 &\leftarrow a_2 + r_2 \\
c_3 &\leftarrow (r_1 + r_2) + a_3
\end{aligned}
$$

5-share

$$
\begin{aligned}
G_{ref} : c_1 &\leftarrow (r_1 + r_2) + a_1 \\
c_2 &\leftarrow (r_2 + r_3) + a_2 \\
c_3 &\leftarrow (r_3 + r_4) + a_3 \\
c_4 &\leftarrow (r_4 + r_5) + a_4 \\
c_5 &\leftarrow (r_5 + r_1) + a_5
\end{aligned}
$$

- G_{copy}, G_{add} based on G_{refresh}

Concrete RPE instantiations

3-share

$$
\begin{aligned}
G_{ref} : c_1 &\leftarrow a_1 + r_1 \\
c_2 &\leftarrow a_2 + r_2 \\
c_3 &\leftarrow (r_1 + r_2) + a_3
\end{aligned}
$$

5-share

$$
\begin{aligned}
G_{ref} : c_1 &\leftarrow (r_1 + r_2) + a_1 \\
c_2 &\leftarrow (r_2 + r_3) + a_2 \\
c_3 &\leftarrow (r_3 + r_4) + a_3 \\
c_4 &\leftarrow (r_4 + r_5) + a_4 \\
c_5 &\leftarrow (r_5 + r_1) + a_5
\end{aligned}
$$

- G_{copy}, G_{add} based on G_{refresh}
- G_{mult} from new generic construction using G_{refresh}

Concrete RPE instantiations

3-share

$$G_{ref}: \begin{aligned} c_1 &\leftarrow a_1 + r_1 \\ c_2 &\leftarrow a_2 + r_2 \\ c_3 &\leftarrow (r_1 + r_2) + a_3 \end{aligned}$$

5-share

$$G_{ref}: \begin{aligned} c_1 &\leftarrow (r_1 + r_2) + a_1 \\ c_2 &\leftarrow (r_2 + r_3) + a_2 \\ c_3 &\leftarrow (r_3 + r_4) + a_3 \\ c_4 &\leftarrow (r_4 + r_5) + a_4 \\ c_5 &\leftarrow (r_5 + r_1) + a_5 \end{aligned}$$

- G_{copy}, G_{add} based on G_{refresh}
- G_{mult} from new generic construction using G_{refresh}

Construction	$d_{\max}$	Complexity	Tolerated Leakage rate
[AIS 18] MPC based	-	$\mathcal{O}(\lvert C\rvert \cdot \kappa^{7.87})$	$p = 2^{-25}$
[CRYPTO 20] 3-share	3/2	$\mathcal{O}(\lvert C\rvert \cdot \kappa^{7.5})$	$p = 2^{-8}$
New 3-share	2	$\mathcal{O}(\lvert C\rvert \cdot \kappa^{3.9})$	$p = 2^{-7.5}$
New 5-share	3	$\mathcal{O}(\lvert C\rvert \cdot \kappa^{3.2})$	$2^{-12} \leq p \leq 2^{-6}$

Conclusion

- In-depth analysis of RP expansion (complexity, limitations, relation to other standard security notions)

Conclusion

- In-depth analysis of RP expansion (complexity, limitations, relation to other standard security notions)
- New generic constructions for RPE gadgets achieving *near* optimal complexity

Conclusion

- In-depth analysis of RP expansion (complexity, limitations, relation to other standard security notions)
- New generic constructions for RPE gadgets achieving *near* optimal complexity
- Concrete instantiations with 3 and 5 shares improving results of the original work from [CRYPTO 20], providing explicit tolerated leakage rate as well as improved complexities