

Random Probing Security

Verification, Composition, Expansion and New Constructions

Sonia Belaïd ¹, Jean-Sébastien Coron ²
Emmanuel Prouff ³, Matthieu Rivain ¹
and Abdul Rahman Taleb ¹

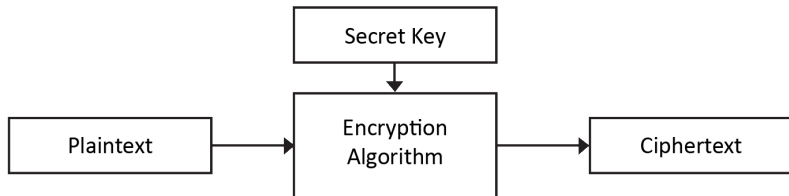
¹ CryptoExperts, France

² University of Luxembourg

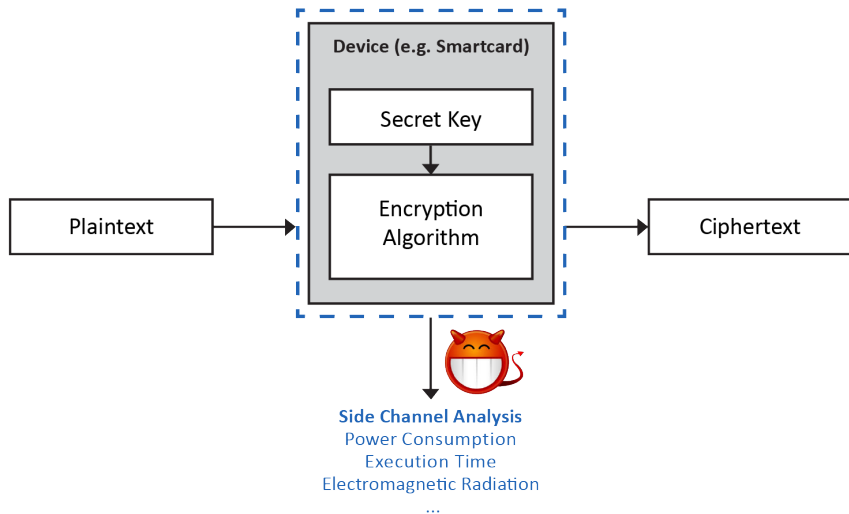
³ ANSSI, France

August 7, 2020

Side-Channel Attacks



Side-Channel Attacks



Countermeasure

Higher-order Masking

Sensitive variable x , group (G, \star) :

Countermeasure

Higher-order Masking

Sensitive variable x , group (G, \star) :

$$x = \underbrace{x_0 \star \dots \star x_{n-2}} \star \underbrace{x_{n-1}}$$

Countermeasure

Higher-order Masking

Sensitive variable x , group (G, \star) :

$$x = \underbrace{x_0 \star \dots \star x_{n-2}}_{\text{uniformly at random from } G} \star \underbrace{x_{n-1}}$$

Countermeasure

Higher-order Masking

Sensitive variable x , group (G, \star) :

$$x = \underbrace{x_0 \star \dots \star x_{n-2}}_{\text{uniformly at random from } G} \star \underbrace{x_{n-1}}_{x \star x_0 \dots \star x_{n-2}}$$

Countermeasure

Higher-order Masking

Sensitive variable x , group (G, \star) :

$$x = \underbrace{x_0 \star \dots \star x_{n-2}}_{\text{uniformly at random from } G} \star \underbrace{x_{n-1}}_{x \star x_0 \dots \star x_{n-2}}$$

Security of masking schemes?

Leakage Models

Definitions

Convenient



Realistic

Leakage Models

Definitions

Convenient

t -probing model
 t leaking variables

Realistic



Leakage Models

Definitions

Convenient

t -probing model
 t leaking variables

Random probing model
each variable leaks with proba. p

Realistic

Leakage Models

Definitions

Convenient

t -probing model
 t leaking variables

Random probing model
each variable leaks with proba. p

Noisy Leakage model
noisy leakage of all the variables

Realistic

Leakage Models

Existing Works

Leakage Models

Existing Works

- Reduction property [Duc et al., 2014]



Leakage Models

Existing Works

- Reduction property [Duc et al., 2014]



Random Probing Constructions:

Leakage Models

Existing Works

- Reduction property [Duc et al., 2014]



Random Probing Constructions:

- [Ajtai, 2011, Andrychowicz et al., 2016] based on expander graphs

Leakage Models

Existing Works

- Reduction property [Duc et al., 2014]



Random Probing Constructions:

- [Ajtai, 2011, Andrychowicz et al., 2016] based on expander graphs
- [Ananth et al., 2018] based on secure multi-party computations ($\mathcal{O}(|C|.poly(\kappa))$ for a circuit C , tolerated leakage proba. $\approx 2^{-25}$).

Random Probing Model

Contributions

Random Probing Model

Contributions

- **VRAPS Tool:** (V)erifier of (RA)ndom (P)robing (S)ecurity.

Random Probing Model

Contributions

- **VRAPS Tool:** (V)erifier of (RA)ndom (P)robing (S)ecurity.
- **Random probing composability / expandability** for global security level amplification (inspired from [Ananth et al., 2018]).

Random Probing Model

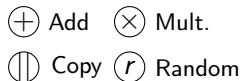
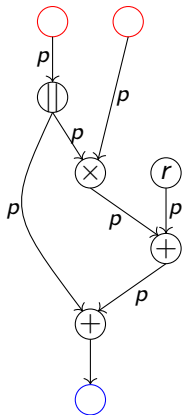
Contributions

- **VRAPS Tool:** (V)erifier of (RA)ndom (P)robing (S)ecurity.
- **Random probing composability / expandability** for global security level amplification (inspired from [Ananth et al., 2018]).
- Efficient instantiation from base gadgets in $\mathcal{O}(|C| \cdot \kappa^{7.5})$ tolerating leakage probability $\approx 2^{-8}$.

Random Probing Security

Definition

(p, ϵ) -Random Probing Security

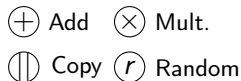
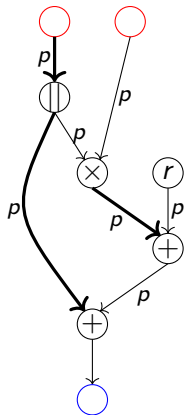


Random Probing Security

Definition

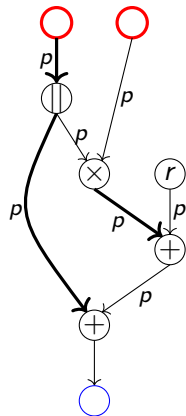
(p, ϵ) -Random Probing Security

W set of wires



Random Probing Security

Definition



(p, ϵ) -Random Probing Security

W set of wires



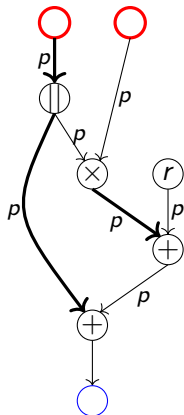
Independent from secret inputs ?

\oplus Add \otimes Mult.

\parallel Copy r Random

Random Probing Security

Definition

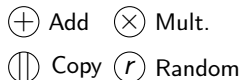
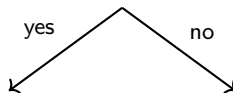


(p, ϵ) -Random Probing Security

W set of wires

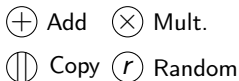
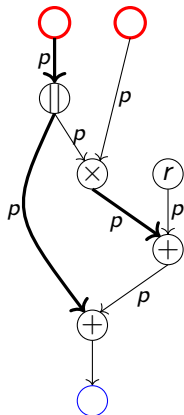


Independent from secret inputs ?



Random Probing Security

Definition



(p, ϵ) -Random Probing Security

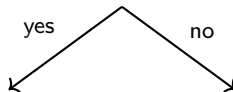
W set of wires



Independent from secret inputs ?

yes

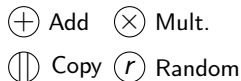
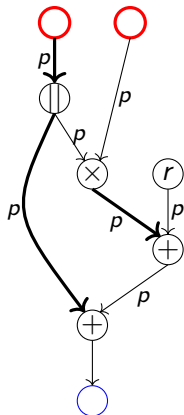
no



Simulation Success

Random Probing Security

Definition

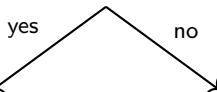


(p, ϵ) -Random Probing Security

W set of wires



Independent from secret inputs ?

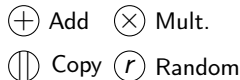
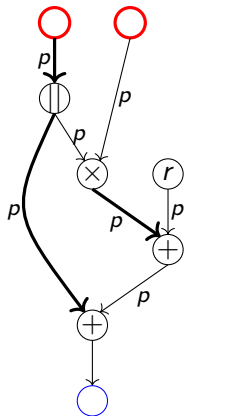


Simulation Success

Simulation Failure

Random Probing Security

Definition



(p, ϵ) -Random Probing Security

W set of wires

Independent from secret inputs ?

yes

no

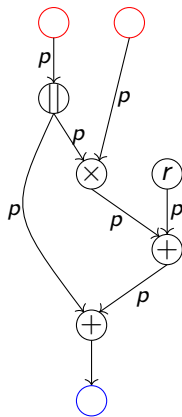
Simulation Success

Simulation Failure

↓
Failure Probability ϵ

Random Probing Security

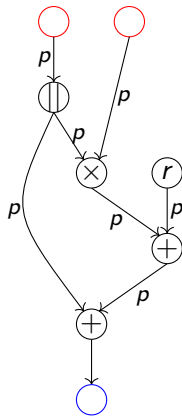
Formal Verification : Method



s: number of wires

Random Probing Security

Formal Verification : Method



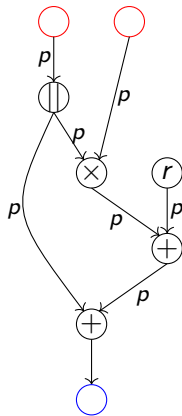
W set of wires

$$Pr(W) = p^{|W|}(1 - p)^{s-|W|}$$

s : number of wires

Random Probing Security

Formal Verification : Method



s: number of wires

W set of wires

$$Pr(W) = p^{|W|}(1 - p)^{s - |W|}$$

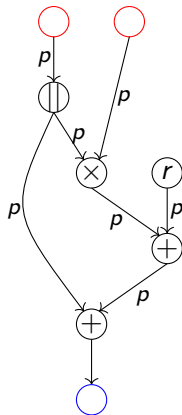
Failure probability ϵ

$$\epsilon = f(p) = \sum_{W} p^{|W|}(1 - p)^{s - |W|}$$

Failure on W

Random Probing Security

Formal Verification : Method



s : number of wires

W set of wires

$$Pr(W) = p^{|W|}(1-p)^{s-|W|}$$

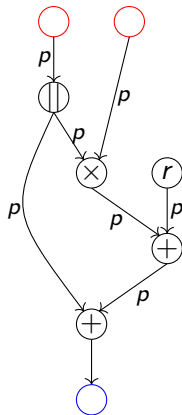
Failure probability ϵ

$$\epsilon = f(p) = \sum_{\substack{W \\ \text{Failure on } W}} p^{|W|}(1-p)^{s-|W|}$$

c_i : number of W of size i with *Simulation Failure*

Random Probing Security

Formal Verification : Method



s : number of wires

W set of wires

$$Pr(W) = p^{|W|}(1-p)^{s-|W|}$$

Failure probability ϵ

$$\epsilon = f(p) = \sum_{\substack{W \\ \text{Failure on } W}} p^{|W|}(1-p)^{s-|W|}$$

c_i : number of W of size i with *Simulation Failure*

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

Random Probing Security

Formal Verification : Algorithm (VRAPS Tool)

Input: circuit with s wires

Output: coefficients c_1, \dots, c_s

1: $c \leftarrow (0, \dots, 0)$

7: **return** c

Random Probing Security

Formal Verification : Algorithm (VRAPS Tool)

Input: circuit with s wires

Output: coefficients c_1, \dots, c_s

1: $c \leftarrow (0, \dots, 0)$

2: **for** $i = 1$ to s **do**

6: **end for**

7: **return** c

Random Probing Security

Formal Verification : Algorithm (VRAPS Tool)

Input: circuit with s wires

Output: coefficients c_1, \dots, c_s

1: $c \leftarrow (0, \dots, 0)$

2: **for** $i = 1$ to s **do**

3: $L \leftarrow \{\text{all } W \text{ of size } i\}$

6: **end for**

7: **return** c

Random Probing Security

Formal Verification : Algorithm (VRAPS Tool)

Input: circuit with s wires

Output: coefficients c_1, \dots, c_s

1: $c \leftarrow (0, \dots, 0)$

2: **for** $i = 1$ to s **do**

3: $L \leftarrow \{\text{all } W \text{ of size } i\}$

4: Apply rules inspired from **maskVerif** on L [Barthe et al., 2015]

6: **end for**

7: **return** c

Random Probing Security

Formal Verification : Algorithm (VRAPS Tool)

Input: circuit with s wires

Output: coefficients c_1, \dots, c_s

1: $c \leftarrow (0, \dots, 0)$

2: **for** $i = 1$ to s **do**

3: $L \leftarrow \{\text{all } W \text{ of size } i\}$

4: Apply rules inspired from **maskVerif** on L [Barthe et al., 2015]

5: $c_i \leftarrow \text{Nb. of failures in } L$

6: **end for**

7: **return** c

Random Probing Composability

Definition

Goal: Achieve global random probing security

Random Probing Composability

Definition

Goal: Achieve global random probing security

(t, p, ϵ) -Random probing
composable n -share
gadgets

G_{add}

G_{copy}

G_{mult}

Random Probing Composability

Definition

Goal: Achieve global random probing security

(t, p, ϵ) -Random probing
composable n -share
gadgets

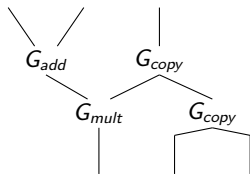
G_{add}

G_{copy}

G_{mult}



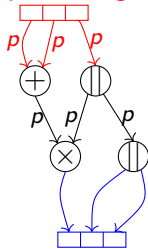
$(p, |C|, \epsilon)$ -Random
probing secure circuit C



Random Probing Composability

Definition

Input Sharing



Output Sharing

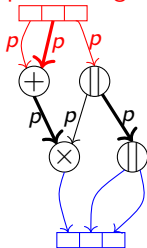
1-to-1 3-share gadget

s : number of wires

Random Probing Composability

Definition

Input Sharing

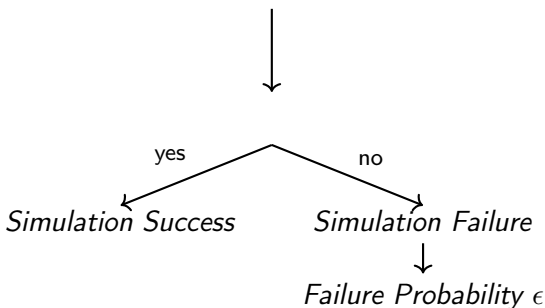


Output Sharing

1-to-1 3-share gadget
 s : number of wires

(t, p, ϵ) -Random Probing Composability

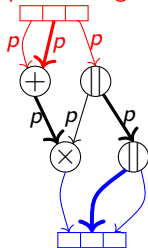
W set of wires



Random Probing Composability

Definition

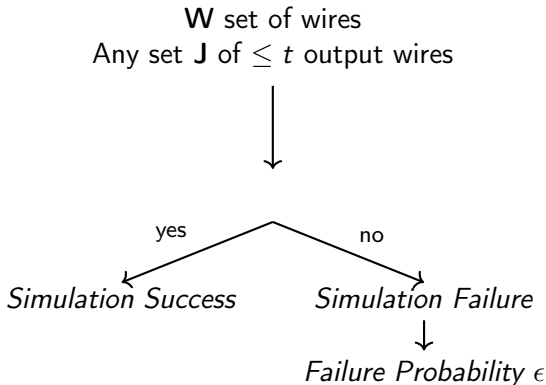
Input Sharing



Output Sharing

1-to-1 3-share gadget
 s : number of wires

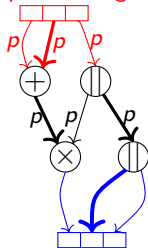
(t, p, ϵ) -Random Probing Composability



Random Probing Composability

Definition

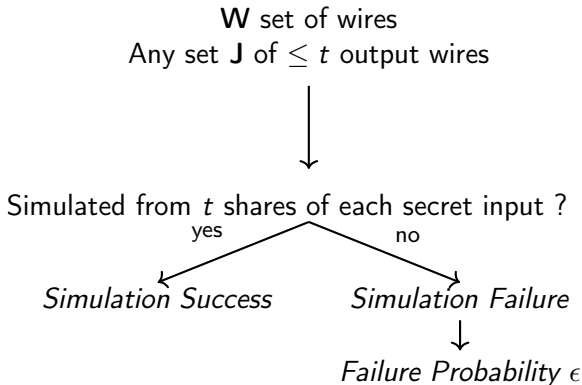
Input Sharing



Output Sharing

1-to-1 3-share gadget
 s : number of wires

(t, p, ϵ) -Random Probing Composability



Random Probing Expandability

Expansion Strategy (Revisited approach from [Ananth et al., 2018])

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

Random Probing Expandability

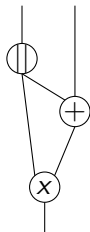
Expansion Strategy (Revisited approach from [Ananth et al., 2018])

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

Random Probing Expandability

Expansion Strategy (Revisited approach from [Ananth et al., 2018])

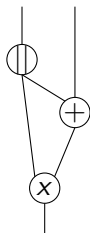
Using n -share gadgets G_{add} , G_{copy} , G_{mult}



Random Probing Expandability

Expansion Strategy (Revisited approach from [Ananth et al., 2018])

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

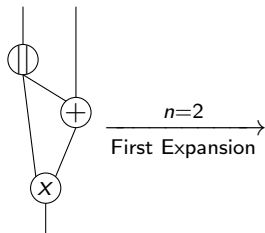


Leakage probability
 p

Random Probing Expandability

Expansion Strategy (Revisited approach from [Ananth et al., 2018])

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

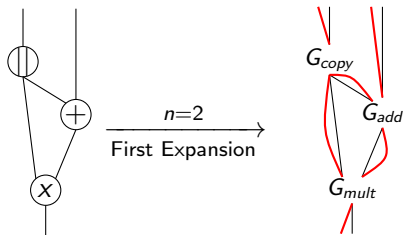


Leakage probability
 p

Random Probing Expandability

Expansion Strategy (Revisited approach from [Ananth et al., 2018])

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

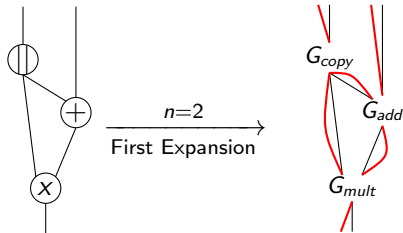


Leakage probability
 p

Random Probing Expandability

Expansion Strategy (Revisited approach from [Ananth et al., 2018])

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



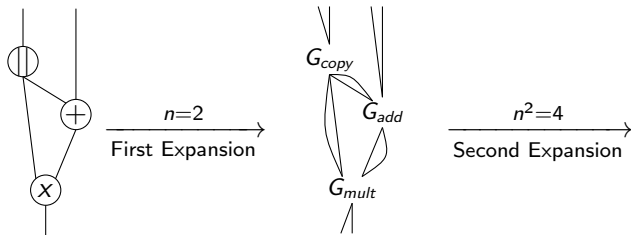
Leakage probability
 p

Simulation Failure
 $\epsilon = f(p)$

Random Probing Expandability

Expansion Strategy (Revisited approach from [Ananth et al., 2018])

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



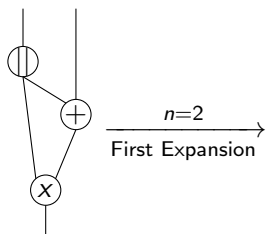
Leakage probability
 p

Simulation Failure
 $\epsilon = f(p)$

Random Probing Expandability

Expansion Strategy (Revisited approach from [Ananth et al., 2018])

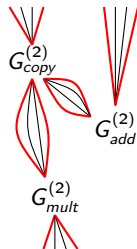
Using n -share gadgets G_{add} , G_{copy} , G_{mult}



Leakage probability
 p



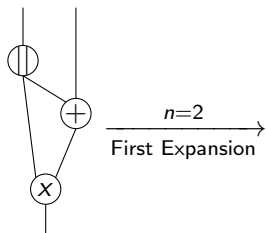
Simulation Failure
 $\epsilon = f(p)$



Random Probing Expandability

Expansion Strategy (Revisited approach from [Ananth et al., 2018])

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

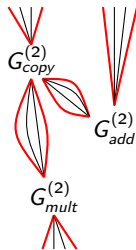


Leakage probability
 p



Simulation Failure
 $\epsilon = f(p)$

$n^2=4$
 Second Expansion

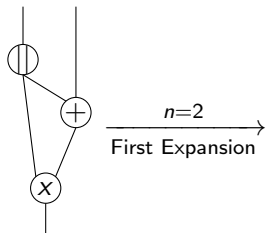


$\epsilon^2 = f^2(p)$

Random Probing Expandability

Expansion Strategy (Revisited approach from [Ananth et al., 2018])

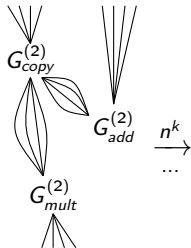
Using n -share gadgets G_{add} , G_{copy} , G_{mult}



$n=2$
 First Expansion



$n^2=4$
 Second Expansion



n^k
 ...

$$\epsilon^2 = f^2(p)$$

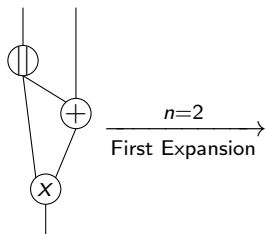
Leakage probability
 p

Simulation Failure
 $\epsilon = f(p)$

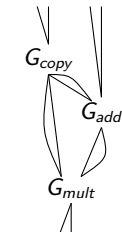
Random Probing Expandability

Expansion Strategy (Revisited approach from [Ananth et al., 2018])

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

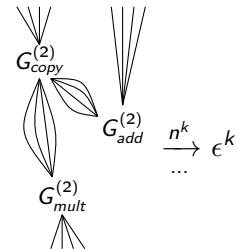


$n=2$
 First Expansion



Simulation Failure
 $\epsilon = f(p)$

$n^2=4$
 Second Expansion



$\epsilon^2 = f^2(p)$

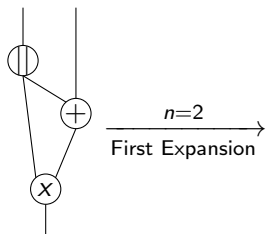
$n^k \rightarrow \epsilon^k$
 ...

Leakage probability
 p

Random Probing Expandability

Expansion Strategy (Revisited approach from [Ananth et al., 2018])

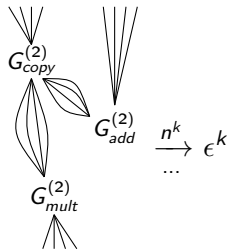
Using n -share gadgets G_{add} , G_{copy} , G_{mult}



Leakage probability
 p



Simulation Failure
 $\epsilon = f(p)$

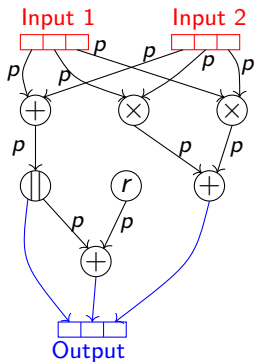


$\epsilon^2 = f^2(p)$

Condition : $f(p) < p$

Random Probing Expandability

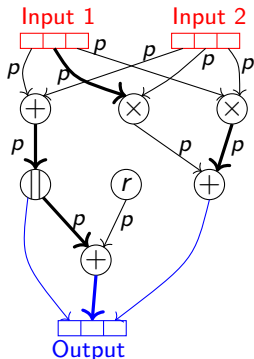
Expansion Security



2-to-1 3-share gadget

Random Probing Expandability

Expansion Security

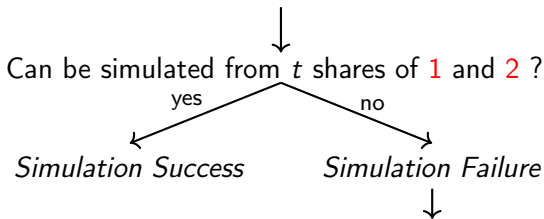


2-to-1 3-share gadget

(t, ϵ) -Random Probing Expandability

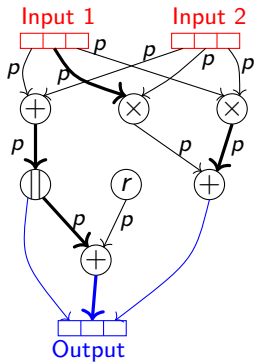
W set of wires

Any set J of $\leq t$ output wires



Random Probing Expandability

Expansion Security



2-to-1 3-share gadget

(t, ϵ) -Random Probing Expandability

\mathbf{W} set of wires

Any set \mathbf{J} of $\leq t$ output wires

Can be simulated from t shares of **1** and **2** ?

yes

no

Simulation Success

Simulation Failure

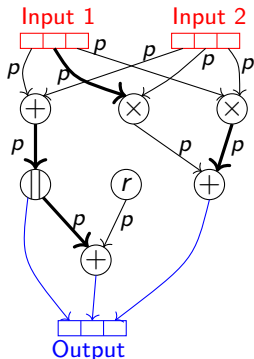
Failure Proba. on 1 = ϵ

Failure Proba. on 2 = ϵ

Failure Proba. on $1 \wedge 2$ = ϵ^2

Random Probing Expandability

Expansion Security



2-to-1 3-share gadget

(t, ϵ) -Random Probing Expandability

W set of wires

Any set J of $\leq t$ output wires

and for a **chosen set J'** of $n - 1$ output wires

Can be simulated from t shares of **1** and **2** ?

yes

no

Simulation Success

Simulation Failure

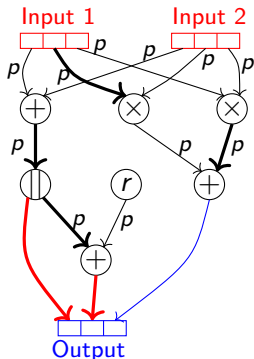
Failure Proba. on 1 = ϵ

Failure Proba. on 2 = ϵ

Failure Proba. on $1 \wedge 2$ = ϵ^2

Random Probing Expandability

Expansion Security



2-to-1 3-share gadget

(t, ϵ) -Random Probing Expandability

\mathbf{W} set of wires

Any set \mathbf{J} of $\leq t$ output wires

and for a **chosen set \mathbf{J}'** of $n - 1$ output wires

Can be simulated from t shares of **1** and **2** ?

yes

no

Simulation Success

Simulation Failure

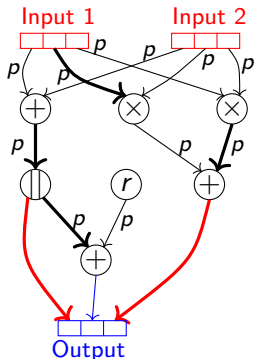
Failure Proba. on 1 = ϵ

Failure Proba. on 2 = ϵ

Failure Proba. on $1 \wedge 2$ = ϵ^2

Random Probing Expandability

Expansion Security



2-to-1 3-share gadget

(t, ϵ) -Random Probing Expandability

\mathbf{W} set of wires

Any set \mathbf{J} of $\leq t$ output wires

and for a **chosen set \mathbf{J}'** of $n - 1$ output wires

Can be simulated from t shares of **1** and **2** ?

yes

no

Simulation Success

Simulation Failure

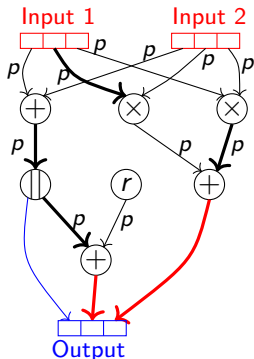
Failure Proba. on 1 = ϵ

Failure Proba. on 2 = ϵ

Failure Proba. on $1 \wedge 2$ = ϵ^2

Random Probing Expandability

Expansion Security



2-to-1 3-share gadget

(t, ϵ) -Random Probing Expandability

\mathbf{W} set of wires

Any set \mathbf{J} of $\leq t$ output wires

and for a **chosen set \mathbf{J}'** of $n - 1$ output wires

Can be simulated from t shares of **1** and **2** ?

yes

no

Simulation Success

Simulation Failure

Failure Proba. on 1 = ϵ

Failure Proba. on 2 = ϵ

Failure Proba. on $1 \wedge 2$ = ϵ^2

Random Probing Expandability

Expansion Security

Random Probing Expandability

Expansion Security

For an n -share gadget G :

Random Probing Expandability

Expansion Security

For an n -share gadget G :

G Random Probing
Expandable, $\epsilon = f(p)$



$G^{(k)}$ Random Probing
Expandable, $\epsilon' = f^k(p)$

Random Probing Expandability

Expansion Security

For an n -share gadget G :

G Random Probing
Expandable, $\epsilon = f(p)$ \implies $G^{(k)}$ Random Probing
Expandable, $\epsilon' = f^k(p)$

G Random Probing
Expandable, $\epsilon = f(p)$ \implies G Random Probing
Composable, $\epsilon' = 2f(p)$

Random Probing Expandability

Expansion Security

For an n -share gadget G :

G Random Probing
Expandable, $\epsilon = f(p)$ \implies $G^{(k)}$ Random Probing
Expandable, $\epsilon' = f^k(p)$

G Random Probing
Expandable, $\epsilon = f(p)$ \implies G Random Probing
Composable, $\epsilon' = 2f(p)$

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

Random Probing Expandability

Expansion Security

For an n -share gadget G :

G Random Probing Expandable, $\epsilon = f(p)$ \implies $G^{(k)}$ Random Probing Expandable, $\epsilon' = f^k(p)$

G Random Probing Expandable, $\epsilon = f(p)$ \implies G Random Probing Composable, $\epsilon' = 2f(p)$

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

G_{add} , G_{copy} , G_{mult} Random Probing Expandable, $\epsilon = f(p)$ \implies Compiled circuit $(p, 2 \cdot f^{(k)})$ -Random Probing Secure

Random Probing Expandability

3-share gadgets Construction

Random Probing Expandability

3-share gadgets Construction

$$G_{copy} : v_0 \leftarrow \mathbf{x}_0 + r_0 + r_1; w_0 \leftarrow \mathbf{x}_0 + r_3 + r_4$$
$$v_1 \leftarrow \mathbf{x}_1 + r_1 + r_2; w_1 \leftarrow \mathbf{x}_1 + r_4 + r_5$$
$$v_2 \leftarrow \mathbf{x}_2 + r_2 + r_0; w_2 \leftarrow \mathbf{x}_2 + r_5 + r_3$$

Random Probing Expandability

3-share gadgets Construction

$$\begin{aligned}G_{copy} : v_0 &\leftarrow \mathbf{x}_0 + r_0 + r_1; w_0 \leftarrow \mathbf{x}_0 + r_3 + r_4 \\v_1 &\leftarrow \mathbf{x}_1 + r_1 + r_2; w_1 \leftarrow \mathbf{x}_1 + r_4 + r_5 \\v_2 &\leftarrow \mathbf{x}_2 + r_2 + r_0; w_2 \leftarrow \mathbf{x}_2 + r_5 + r_3\end{aligned}$$

$$\begin{aligned}G_{add} : z_0 &\leftarrow \mathbf{x}_0 + r_0 + r_4 + \mathbf{y}_0 + r_1 + r_3 \\z_1 &\leftarrow \mathbf{x}_1 + r_1 + r_5 + \mathbf{y}_1 + r_2 + r_4 \\z_2 &\leftarrow \mathbf{x}_2 + r_2 + r_3 + \mathbf{y}_2 + r_0 + r_5\end{aligned}$$

Random Probing Expandability

3-share gadgets Construction

$$\begin{array}{ll} G_{copy} : v_0 \leftarrow \mathbf{x}_0 + r_0 + r_1; & w_0 \leftarrow \mathbf{x}_0 + r_3 + r_4 \\ v_1 \leftarrow \mathbf{x}_1 + r_1 + r_2; & w_1 \leftarrow \mathbf{x}_1 + r_4 + r_5 \\ v_2 \leftarrow \mathbf{x}_2 + r_2 + r_0; & w_2 \leftarrow \mathbf{x}_2 + r_5 + r_3 \end{array} \quad \begin{array}{l} G_{add} : z_0 \leftarrow \mathbf{x}_0 + r_0 + r_4 + \mathbf{y}_0 + r_1 + r_3 \\ z_1 \leftarrow \mathbf{x}_1 + r_1 + r_5 + \mathbf{y}_1 + r_2 + r_4 \\ z_2 \leftarrow \mathbf{x}_2 + r_2 + r_3 + \mathbf{y}_2 + r_0 + r_5 \end{array}$$

$$\begin{array}{lll} G_{mult} : u_0 \leftarrow \mathbf{x}_0 + r_5 + r_6; & u_1 \leftarrow \mathbf{x}_1 + r_6 + r_7; & u_2 \leftarrow \mathbf{x}_2 + r_7 + r_5 \\ v_0 \leftarrow \mathbf{y}_0 + r_8 + r_9; & v_1 \leftarrow \mathbf{y}_1 + r_9 + r_{10}; & v_2 \leftarrow \mathbf{y}_2 + r_{10} + r_8 \end{array}$$

Random Probing Expandability

3-share gadgets Construction

$$\begin{array}{ll}
 G_{copy} : v_0 \leftarrow \mathbf{x}_0 + r_0 + r_1; & w_0 \leftarrow \mathbf{x}_0 + r_3 + r_4 \\
 v_1 \leftarrow \mathbf{x}_1 + r_1 + r_2; & w_1 \leftarrow \mathbf{x}_1 + r_4 + r_5 \\
 v_2 \leftarrow \mathbf{x}_2 + r_2 + r_0; & w_2 \leftarrow \mathbf{x}_2 + r_5 + r_3
 \end{array}
 \quad
 \begin{array}{l}
 G_{add} : z_0 \leftarrow \mathbf{x}_0 + r_0 + r_4 + \mathbf{y}_0 + r_1 + r_3 \\
 z_1 \leftarrow \mathbf{x}_1 + r_1 + r_5 + \mathbf{y}_1 + r_2 + r_4 \\
 z_2 \leftarrow \mathbf{x}_2 + r_2 + r_3 + \mathbf{y}_2 + r_0 + r_5
 \end{array}$$

$$\begin{array}{lll}
 G_{mult} : u_0 \leftarrow \mathbf{x}_0 + r_5 + r_6; & u_1 \leftarrow \mathbf{x}_1 + r_6 + r_7; & u_2 \leftarrow \mathbf{x}_2 + r_7 + r_5 \\
 v_0 \leftarrow \mathbf{y}_0 + r_8 + r_9; & v_1 \leftarrow \mathbf{y}_1 + r_9 + r_{10}; & v_2 \leftarrow \mathbf{y}_2 + r_{10} + r_8
 \end{array}$$

$$\begin{array}{l}
 z_0 \leftarrow (u_0 \cdot v_0 + r_0) + (u_0 \cdot v_1 + r_1) + (u_0 \cdot v_2 + r_2) \\
 z_1 \leftarrow (u_1 \cdot v_0 + r_1) + (u_1 \cdot v_1 + r_4) + (u_1 \cdot v_2 + r_3) \\
 z_2 \leftarrow (u_2 \cdot v_0 + r_2) + (u_2 \cdot v_1 + r_3) + (u_2 \cdot v_2 + r_0) + r_4
 \end{array}$$

Random Probing Expandability

3-share gadgets Construction

$$\begin{array}{ll}
 G_{copy} : v_0 \leftarrow \mathbf{x}_0 + r_0 + r_1; & w_0 \leftarrow \mathbf{x}_0 + r_3 + r_4 \\
 v_1 \leftarrow \mathbf{x}_1 + r_1 + r_2; & w_1 \leftarrow \mathbf{x}_1 + r_4 + r_5 \\
 v_2 \leftarrow \mathbf{x}_2 + r_2 + r_0; & w_2 \leftarrow \mathbf{x}_2 + r_5 + r_3
 \end{array}
 \qquad
 \begin{array}{ll}
 G_{add} : z_0 \leftarrow \mathbf{x}_0 + r_0 + r_4 + \mathbf{y}_0 + r_1 + r_3 \\
 z_1 \leftarrow \mathbf{x}_1 + r_1 + r_5 + \mathbf{y}_1 + r_2 + r_4 \\
 z_2 \leftarrow \mathbf{x}_2 + r_2 + r_3 + \mathbf{y}_2 + r_0 + r_5
 \end{array}$$

$$\begin{array}{lll}
 G_{mult} : u_0 \leftarrow \mathbf{x}_0 + r_5 + r_6; & u_1 \leftarrow \mathbf{x}_1 + r_6 + r_7; & u_2 \leftarrow \mathbf{x}_2 + r_7 + r_5 \\
 v_0 \leftarrow \mathbf{y}_0 + r_8 + r_9; & v_1 \leftarrow \mathbf{y}_1 + r_9 + r_{10}; & v_2 \leftarrow \mathbf{y}_2 + r_{10} + r_8
 \end{array}$$

$$\begin{array}{l}
 z_0 \leftarrow (u_0 \cdot v_0 + r_0) + (u_0 \cdot v_1 + r_1) + (u_0 \cdot v_2 + r_2) \\
 z_1 \leftarrow (u_1 \cdot v_0 + r_1) + (u_1 \cdot v_1 + r_4) + (u_1 \cdot v_2 + r_3) \\
 z_2 \leftarrow (u_2 \cdot v_0 + r_2) + (u_2 \cdot v_1 + r_3) + (u_2 \cdot v_2 + r_0) + r_4
 \end{array}$$

$$t = 1, \quad f(p) \leq \sqrt{83}p^{3/2} + \mathcal{O}(p^2), \quad p_{max} \approx 2^{-8}$$

Random Probing Expandability

Asymptotic Complexity

$$N = (N_{add}, N_{copy}, N_{mult}, N_{rand})$$

Random Probing Expandability

Asymptotic Complexity

$$N = (N_{add}, N_{copy}, N_{mult}, N_{rand})$$

On previous 3-share gadgets:

Random Probing Expandability

Asymptotic Complexity

$$N = (N_{add}, N_{copy}, N_{mult}, N_{rand})$$

On previous 3-share gadgets:

$$M = \begin{pmatrix} N_{G_{add}}^T & N_{G_{copy}}^T & N_{G_{mult}}^T & N_{rand}^T \\ 15 & 12 & 28 & 0 \\ 6 & 9 & 23 & 0 \\ 0 & 0 & 9 & 0 \\ 6 & 6 & 11 & 3 \end{pmatrix}$$

Random Probing Expandability

Asymptotic Complexity

$$N = (N_{add}, N_{copy}, N_{mult}, N_{rand})$$

On previous 3-share gadgets:

$$M = \begin{pmatrix} N_{G_{add}}^T & N_{G_{copy}}^T & N_{G_{mult}}^T & N_{rand}^T \\ 15 & 12 & 28 & 0 \\ 6 & 9 & 23 & 0 \\ 0 & 0 & 9 & 0 \\ 6 & 6 & 11 & 3 \end{pmatrix} = Q \cdot \Lambda \cdot Q^{-1}$$

Random Probing Expandability

Asymptotic Complexity

$$N = (N_{add}, N_{copy}, N_{mult}, N_{rand})$$

On previous 3-share gadgets:

$$M = \begin{pmatrix} N_{G_{add}}^T & N_{G_{copy}}^T & N_{G_{mult}}^T & N_{rand}^T \\ 15 & 12 & 28 & 0 \\ 6 & 9 & 23 & 0 \\ 0 & 0 & 9 & 0 \\ 6 & 6 & 11 & 3 \end{pmatrix} = Q.\Lambda.Q^{-1}$$

Compiling a circuit C : $N_{\hat{C}} = M^k N_C = Q.\Lambda^k.Q^{-1}.N_C$

Random Probing Expandability

Asymptotic Complexity

$$N = (N_{add}, N_{copy}, N_{mult}, N_{rand})$$

On previous 3-share gadgets:

$$M = \begin{pmatrix} N_{G_{add}}^T & N_{G_{copy}}^T & N_{G_{mult}}^T & N_{rand}^T \\ & M_{ac} & 28 & 0 \\ 0 & 0 & 23 & 0 \\ 6 & 6 & N_m & 0 \\ & & 1 & 3 \end{pmatrix} = Q.\Lambda.Q^{-1}$$

Compiling a circuit C : $N_C = M^k N_C = Q.\Lambda^k.Q^{-1}.N_C$

Random Probing Expandability

Asymptotic Complexity

$$N = (N_{add}, N_{copy}, N_{mult}, N_{rand})$$

On previous 3-share gadgets:

$$M = \begin{pmatrix} N_{G_{add}}^T & N_{G_{copy}}^T & N_{G_{mult}}^T & N_{rand}^T \\ & M_{ac} & 28 & 0 \\ 0 & 0 & 23 & 0 \\ 6 & 6 & N_m & 0 \\ & & 1 & 3 \end{pmatrix} = Q \cdot \Lambda \cdot Q^{-1}$$

Compiling a circuit C : $N_{\hat{C}} = M^k N_C = Q \cdot \Lambda^k \cdot Q^{-1} \cdot N_C$

$$|\hat{C}| = \mathcal{O}(|C| \cdot N_{\max}^k), \quad N_{\max} = \max(\text{eigenvalues}(M_{ac}), N_{mult})$$

Random Probing Expandability

Asymptotic Complexity

For a security parameter κ , and $f(p) = c_d p^d + \mathcal{O}(p^{d+1})$ of *amplification order* d ,

Random Probing Expandability

Asymptotic Complexity

For a security parameter κ , and $f(p) = c_d p^d + \mathcal{O}(p^{d+1})$ of *amplification order* d , we need $f^{(k)}(p) \leq 2^{-\kappa}$:

Random Probing Expandability

Asymptotic Complexity

For a security parameter κ , and $f(p) = c_d p^d + \mathcal{O}(p^{d+1})$ of *amplification order* d , we need $f^{(k)}(p) \leq 2^{-\kappa}$:

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

Random Probing Expandability

Asymptotic Complexity

For a security parameter κ , and $f(p) = \sqrt{83}p^{3/2} + \mathcal{O}(p^2)$ of *amplification order* $3/2$, we need $f^{(k)}(p) \leq 2^{-\kappa}$:

$$|\hat{C}| = \mathcal{O}(|C| \cdot \kappa^{7.5}), \quad e = \frac{\log(21)}{\log(3/2)}$$

Random Probing Expandability

Comparison with [Ananth et al., 2018]

Our Expansion Strategy

[Ananth et al., 2018] Strategy

Random Probing Expandability

Comparison with [Ananth et al., 2018]

Our Expansion Strategy

(t, f) -RPE Security

[Ananth et al., 2018] Strategy

(p, ϵ) -Composable Security

Random Probing Expandability

Comparison with [Ananth et al., 2018]

Our Expansion Strategy

(t, f) -RPE Security

Secure (t, f) -RPE gadgets

[Ananth et al., 2018] Strategy

(p, ϵ) -Composable Security

(m, c) -MPC protocols

Random Probing Expandability

Comparison with [Ananth et al., 2018]

Our Expansion Strategy

(t, f) -RPE Security

Secure (t, f) -RPE gadgets

Instantiation with $(1, f)$ -RPE
3-share G_{add} , G_{copy} , G_{mult}

[Ananth et al., 2018] Strategy

(p, ϵ) -Composable Security

(m, c) -MPC protocols

Instantiation with [Maurer, 2006]
 $(m = 5, c = 2)$ -MPC protocol

Random Probing Expandability

Comparison with [Ananth et al., 2018]

Our Expansion Strategy

(t, f) -RPE Security

Secure (t, f) -RPE gadgets

Instantiation with $(1, f)$ -RPE
3-share G_{add} , G_{copy} , G_{mult}

$$\mathcal{O}(|C| \cdot \kappa^{7.5})$$

[Ananth et al., 2018] Strategy

(p, ϵ) -Composable Security

(m, c) -MPC protocols

Instantiation with [Maurer, 2006]
 $(m = 5, c = 2)$ -MPC protocol

$$\mathcal{O}(|C| \cdot \kappa^{7.87})$$

Random Probing Expandability

Comparison with [Ananth et al., 2018]

Our Expansion Strategy

(t, f) -RPE Security

Secure (t, f) -RPE gadgets

Instantiation with $(1, f)$ -RPE
3-share G_{add} , G_{copy} , G_{mult}

$$\mathcal{O}(|C| \cdot \kappa^{7.5})$$

$$p_{max} \approx 2^{-8}$$

[Ananth et al., 2018] Strategy

(p, ϵ) -Composable Security

(m, c) -MPC protocols

Instantiation with [Maurer, 2006]
 $(m = 5, c = 2)$ -MPC protocol

$$\mathcal{O}(|C| \cdot \kappa^{7.87})$$

$$p_{max} \approx 2^{-25}$$

Conclusion

- **VRAPS** tool for verification of Random Probing Security:
<https://github.com/CryptoExperts/VRAPS>

Conclusion

- **VRAPS** tool for verification of Random Probing Security:
<https://github.com/CryptoExperts/VRAPS>
- New gadget composition / expansion properties for random probing security

Conclusion

- **VRAPS** tool for verification of Random Probing Security:
<https://github.com/CryptoExperts/VRAPS>
- New gadget composition / expansion properties for random probing security
- New 3-share construction achieving random probing security with tolerated leakage proba. $\approx 2^{-8}$, and a complexity of $\mathcal{O}(|C| \cdot \kappa^{7.5})$

Conclusion

- **VRAPS** tool for verification of Random Probing Security: <https://github.com/CryptoExperts/VRAPS>
- New gadget composition / expansion properties for random probing security
- New 3-share construction achieving random probing security with tolerated leakage proba. $\approx 2^{-8}$, and a complexity of $\mathcal{O}(|C| \cdot \kappa^{7.5})$
- Implementation of the expansion strategy, and an implementation of a secure n^k -share AES128: <https://github.com/CryptoExperts/poc-expanding-compiler>

References

- Miklós Ajtai. Secure computation with information leaking to an adversary. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 715–724, 2011.
- Prabhanjan Ananth, Yuval Ishai, and Amit Sahai. Private circuits: A modular approach. In *Annual International Cryptology Conference*, pages 427–455. Springer, 2018.
- Marcin Andrychowicz, Stefan Dziembowski, and Sebastian Faust. Circuit compilers with $o(1/\log(n))$ leakage rate. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 586–615. Springer, 2016.
- Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, and Pierre-Yves Strub. Verified proofs of higher-order masking. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 457–485. Springer, 2015.
- Alexandre Duc, Stefan Dziembowski, and Sebastian Faust. Unifying leakage models: From probing attacks to noisy leakage. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 423–440. Springer, 2014.
- Ueli Maurer. Secure multi-party computation made simple. *Discrete Applied Mathematics*, 154(2): 370–381, 2006.