Random Probing Security

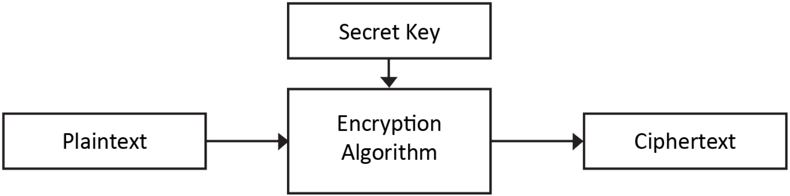
Verification, Composition, Expansion and New Constructions

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

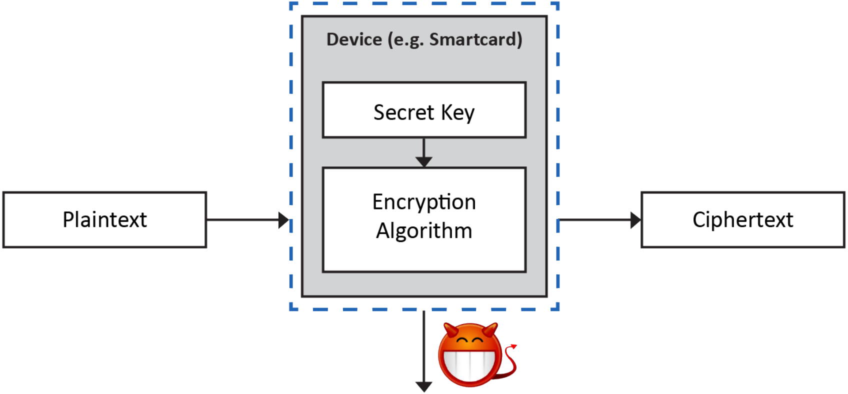
[1] CryptoExperts, France
[2] University of Luxembourg
[3] ANSSI, France

August 7, 2020

Side-Channel Attacks



Side-Channel Attacks



Side Channel Analysis
Power Consumption
Execution Time
Electromagnetic Radiation
...

Countermeasure

Higher-order Masking

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

Countermeasure

Higher-order Masking

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

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

Countermeasure

Higher-order Masking

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

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

Countermeasure

Higher-order Masking

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

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

Countermeasure
Higher-order Masking

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

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

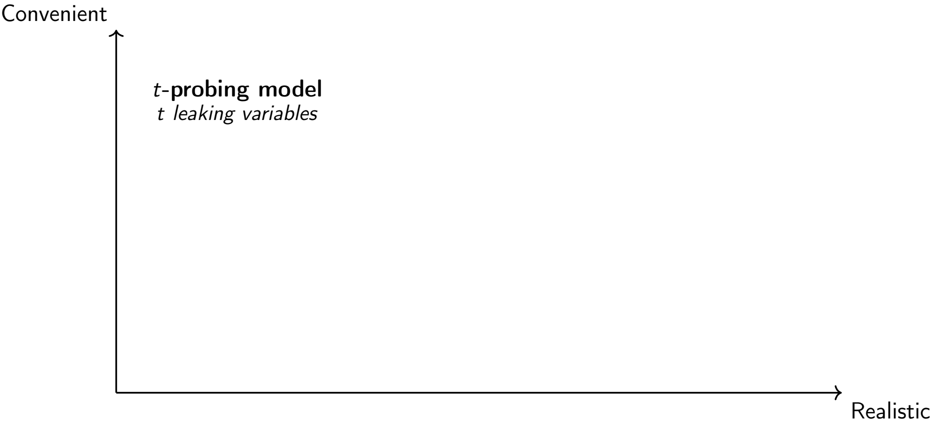
Security of masking schemes?

Leakage Models

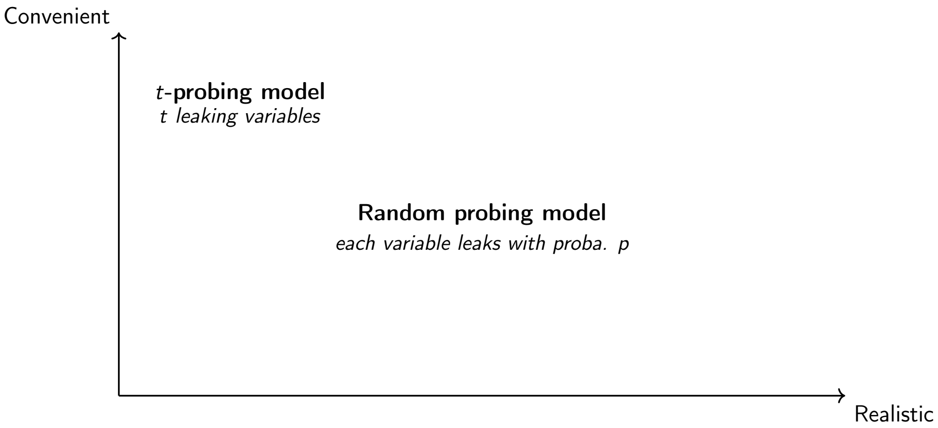
Definitions

Leakage Models

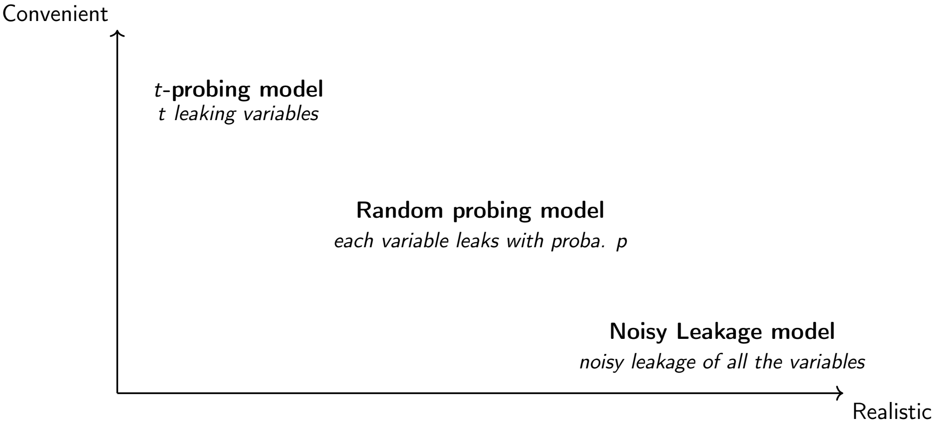
Definitions



Leakage Models
Definitions



Leakage Models
Definitions



Leakage Models

Existing Works

Leakage Models

Existing Works

- Reduction property [Duc et al., 2014]

Probing Security $\Longrightarrow$ Random Probing Security $\Longrightarrow$ Noisy Leakage Security

Leakage Models
Existing Works

- Reduction property [Duc et al., 2014]

Probing Security $\Longrightarrow$ Random Probing Security $\Longrightarrow$ Noisy Leakage Security

Random Probing Constructions:

Leakage Models

Existing Works

- Reduction property [Duc et al., 2014]

Probing Security $\Longrightarrow$ Random Probing Security $\Longrightarrow$ Noisy Leakage Security

Random Probing Constructions:

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

Leakage Models
Existing Works

- Reduction property [Duc et al., 2014]

Probing Security $\Longrightarrow$ Random Probing Security $\Longrightarrow$ Noisy Leakage Security

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

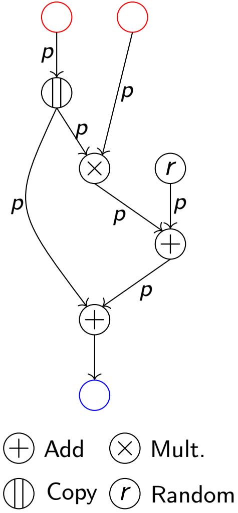
Contributions

- **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]).

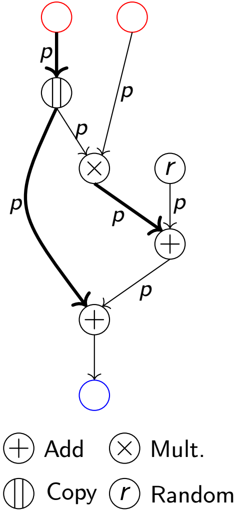
- Efficient instantiation from base gadgets in $\mathcal{O}(|C|.\kappa^{7.5})$ tolerating leakage probability $\approx 2^{-8}$.

Random Probing Security
Definition



(p, ϵ)-Random Probing Security

Random Probing Security
Definition

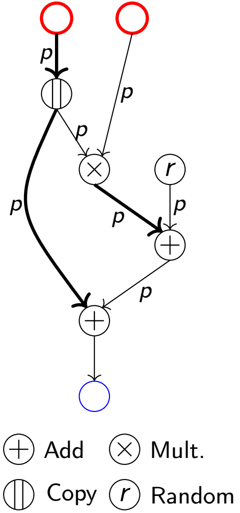


(p, ϵ)-Random Probing Security

W set of wires

Random Probing Security

Definition



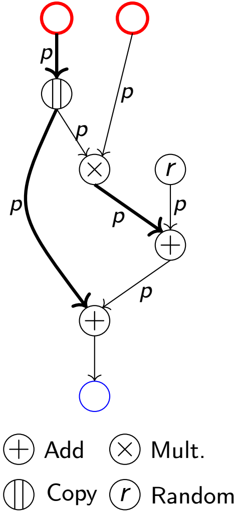
(p, ϵ)-Random Probing Security

W set of wires

$\downarrow$

Independent from secret inputs ?

Random Probing Security
Definition



(p, ϵ)-Random Probing Security

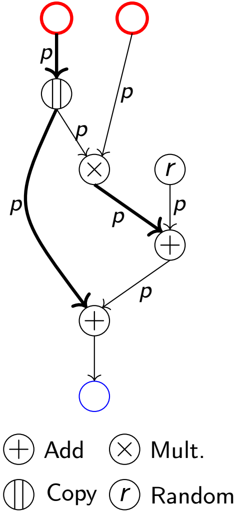
W set of wires

Independent from secret inputs ?

yes

no

Random Probing Security
Definition



(p, ϵ)-Random Probing Security

W set of wires

$\downarrow$

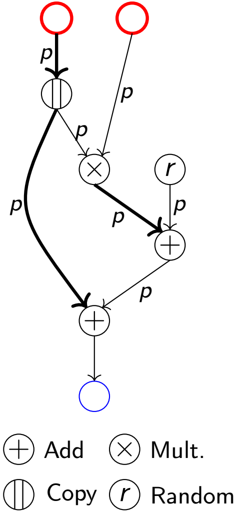
Independent from secret inputs ?

yes — *Simulation Success*

no

Random Probing Security

Definition



(p, ϵ)-Random Probing Security

W set of wires

↓

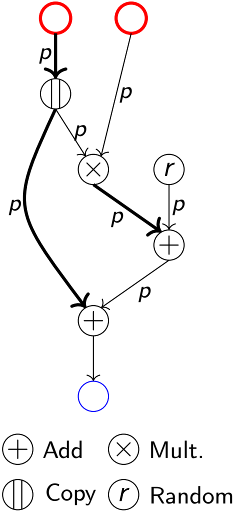
Independent from secret inputs ?

yes → *Simulation Success*

no → *Simulation Failure*

Random Probing Security

Definition



(p, ϵ)-Random Probing Security

W set of wires

↓

Independent from secret inputs ?

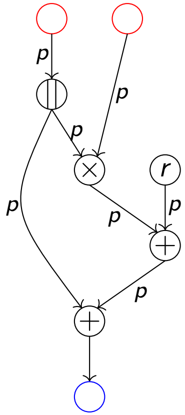
yes → *Simulation Success*

no → *Simulation Failure*

↓

Failure Probability ϵ

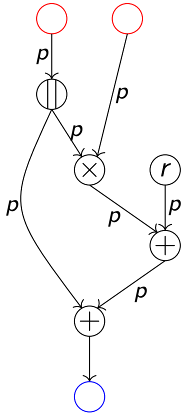
Random Probing Security
Formal Verification : Method



s: number of wires

Random Probing Security

Formal Verification : Method



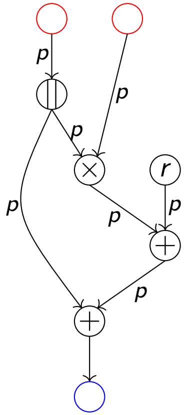
s: number of wires

W set of wires

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

Random Probing Security

Formal Verification : Method



s: number of wires

W set of wires

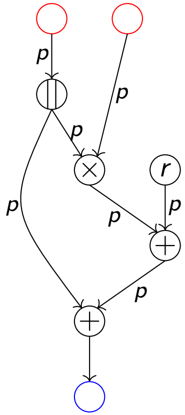
$$Pr(W) = p^{|W|}(1-p)^{s-|W|}$$

Failure probability ϵ

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

Random Probing Security

Formal Verification : Method



s: number of wires

W set of wires

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

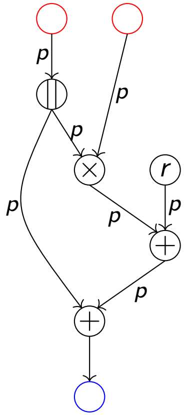
Failure probability ϵ

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

$\mathbf{c_i}$: 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

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

$\mathbf{c_i}$: 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 $c_1, \ldots, c_s$

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

7: **return** c

Random Probing Security

Formal Verification : Algorithm (VRAPS Tool)

Input: circuit with s wires
Output: coefficients $c_1, \ldots, c_s$

$c \leftarrow (0, \ldots, 0)$
for $i = 1$ to s **do**

end for
return c

Random Probing Security

Formal Verification : Algorithm (VRAPS Tool)

Input: circuit with s wires
Output: coefficients $c_1, \ldots, c_s$

```
c ← (0, . . . , 0)
for i = 1 to s do
    L ← {all W of size i}
end for
return c
```

Random Probing Security

Formal Verification : Algorithm (VRAPS Tool)

Input: circuit with s wires
Output: coefficients $c_1, \ldots, c_s$

$c \leftarrow (0, \ldots, 0)$
for $i = 1$ to s **do**
  $L \leftarrow \{\text{all } W \text{ of size } i\}$
  Apply rules inspired from **maskVerif** on L [Barthe et al., 2015]

end for
return c

Random Probing Security

Formal Verification : Algorithm (VRAPS Tool)

Input: circuit with s wires
Output: coefficients $c_1, \ldots, c_s$

```
c ← (0, ..., 0)
for i = 1 to s do
    L ← {all W of size i}
    Apply rules inspired from maskVerif on L [Barthe et al., 2015]
    c_i ← Nb. of failures in L
end for
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

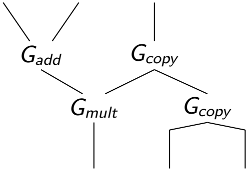
(t, p, ϵ)-**Random probing composable** n-share gadgets

G_{add} G_{copy}

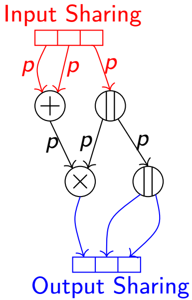
G_{mult}

$\Longrightarrow$

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



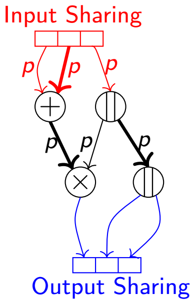
Random Probing Composability
Definition



1-to-1 3-share gadget

s: number of wires

Random Probing Composability
Definition



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

(t,p,ϵ)-Random Probing Composability

W set of wires

$\downarrow$

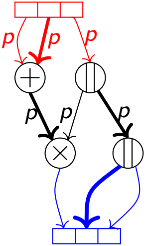
yes → *Simulation Success*

no → *Simulation Failure* $\rightarrow$ *Failure Probability* ϵ

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

Any set **J** of $\leq t$ output wires

$\downarrow$

yes — *Simulation Success*

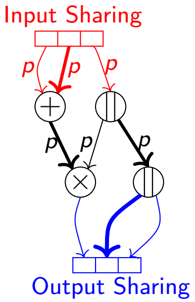
no — *Simulation Failure*

$\downarrow$

Failure Probability ϵ

Random Probing Composability

Definition



1-to-1 3-share gadget

s: number of wires

(t,p,ϵ)-Random Probing Composability

W set of wires

Any set **J** of $\leq t$ output wires

↓

Simulated from t shares of each secret input ?

yes → *Simulation Success*

no → *Simulation Failure* → *Failure Probability* ϵ

Random Probing Expandability

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

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

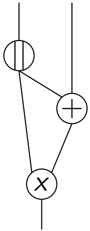
Random Probing Expandability

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])

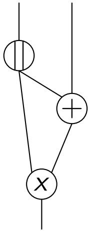
Using n-share gadgets G_{add}, G_{copy}, G_{mult}



Random Probing Expandability

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

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

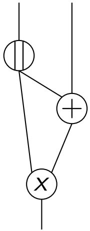


Leakage probability
p

Random Probing Expandability

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

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



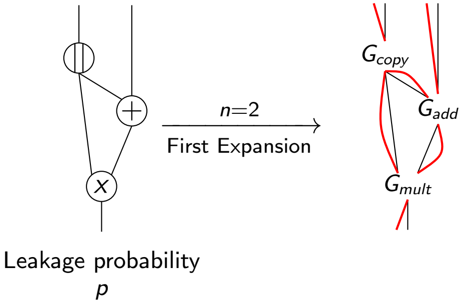
$\xrightarrow[\text{First Expansion}]{n=2}$

Leakage probability
p

Random Probing Expandability

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

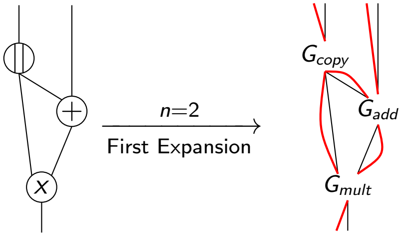
Using n-share gadgets G_{add}, G_{copy}, G_{mult}



Random Probing Expandability

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

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



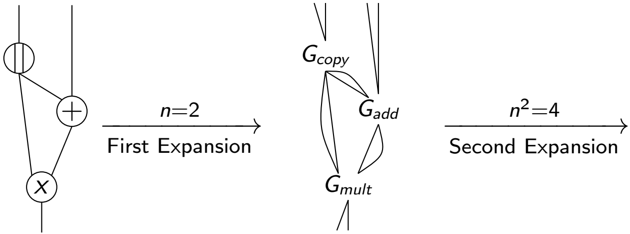
Leakage probability
p

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}



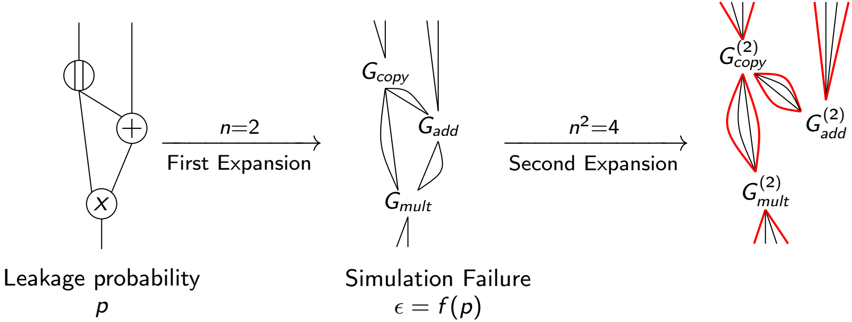
Leakage probability
p

Simulation Failure
$\epsilon = f(p)$

Random Probing Expandability

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

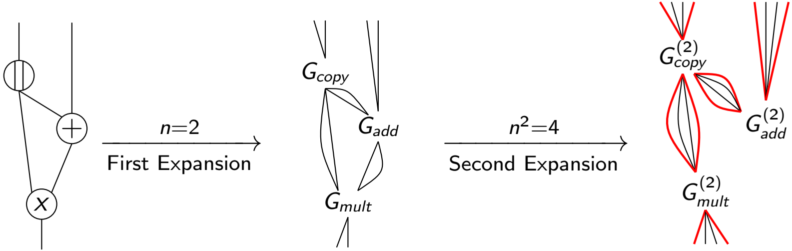
Using n-share gadgets G_{add}, G_{copy}, G_{mult}



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

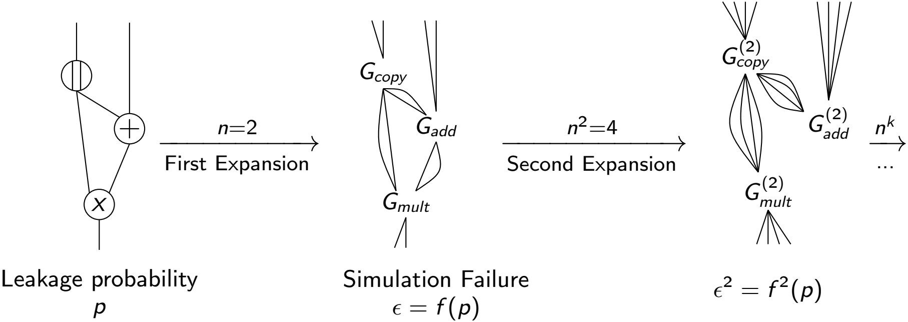
Simulation Failure
$\epsilon = f(p)$

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

Random Probing Expandability

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

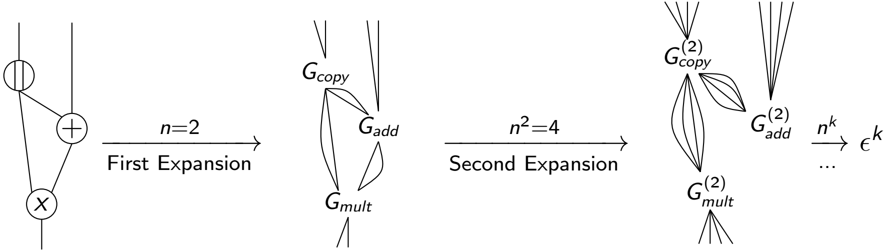
Using n-share gadgets G_{add}, G_{copy}, G_{mult}



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

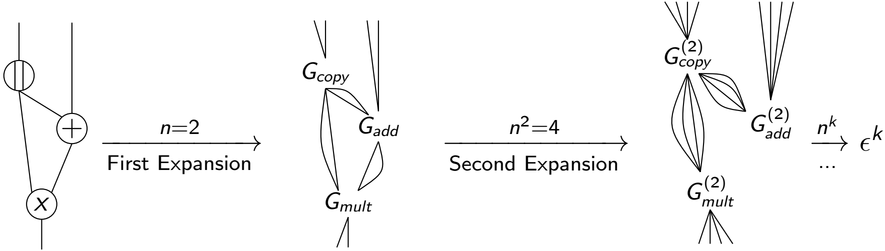
Simulation Failure
$\epsilon = f(p)$

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

Random Probing Expandability

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

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



Leakage probability
p

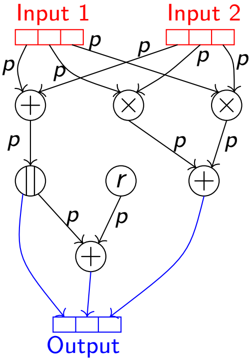
Simulation Failure
$\epsilon = f(p)$

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

Condition : $f(p) < p$

Random Probing Expandability

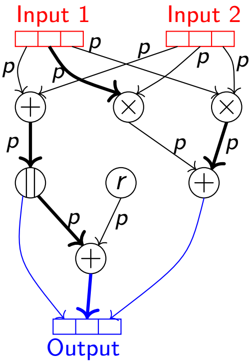
Expansion Security



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

↓

Can be simulated from t shares of 1 and 2 ?

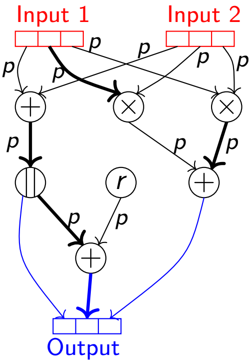
yes → *Simulation Success*

no → *Simulation Failure*

↓

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

Can be simulated from t shares of 1 and 2 ?

yes → *Simulation Success*

no → *Simulation Failure*

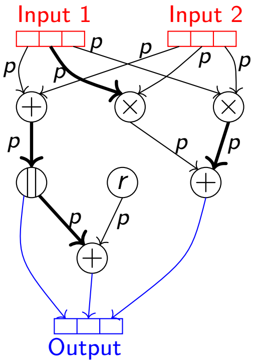
Failure Proba. on 1 $= \epsilon$

Failure Proba. on 2 $= \epsilon$

Failure Proba. on 1 $\wedge$ *2* $= \epsilon^2$

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 → *Simulation Success*

no → *Simulation Failure*

↓

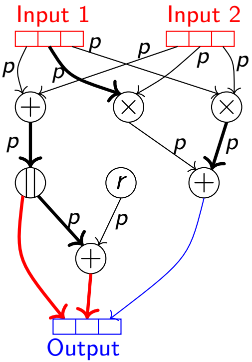
Failure Proba. on 1 $= \epsilon$

Failure Proba. on 2 $= \epsilon$

Failure Proba. on 1 $\wedge$ *2* $= \epsilon^2$

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 $\mathbf{n-1}$ output wires

↓

Can be simulated from t shares of 1 and 2 ?

yes → *Simulation Success*

no → *Simulation Failure*

↓

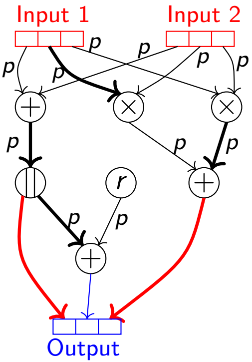
Failure Proba. on 1 $= \epsilon$

Failure Proba. on 2 $= \epsilon$

Failure Proba. on 1 $\wedge$ *2* $= \epsilon^2$

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 $\mathbf{n-1}$ output wires

$\downarrow$

Can be simulated from t shares of 1 and 2 ?

yes → *Simulation Success*

no → *Simulation Failure*

$\downarrow$

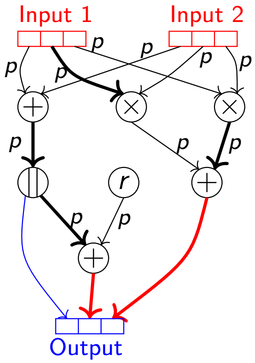
Failure Proba. on 1 $= \epsilon$

Failure Proba. on 2 $= \epsilon$

Failure Proba. on 1 $\wedge$ *2* $= \epsilon^2$

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 → *Simulation Success*

no → *Simulation Failure*

↓

Failure Proba. on 1 $= \epsilon$

Failure Proba. on 2 $= \epsilon$

Failure Proba. on 1 $\wedge$ *2* $= \epsilon^2$

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

Random Probing Expandability

Expansion Security

For an n-share gadget G:

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

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

Random Probing Expandability

Expansion Security

For an n-share gadget G:

G Random Probing Expandable, $\epsilon = f(p)$	$\Longrightarrow$	$G^{(k)}$ Random Probing Expandable, $\epsilon' = f^k(p)$
G Random Probing Expandable, $\epsilon = f(p)$	$\Longrightarrow$	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, $\epsilon = f(p)$	$\Longrightarrow$	$G^{(k)}$ Random Probing Expandable, $\epsilon' = f^k(p)$
G Random Probing Expandable, $\epsilon = f(p)$	$\Longrightarrow$	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,** $\epsilon = f(p)$	$\Longrightarrow$	**Compiled circuit** $(p, 2.f^{(k)})$**-Random Probing Secure**

Random Probing Expandability

3-share gadgets Construction

Random Probing Expandability

3-share gadgets Construction

$$
\begin{aligned}
G_{copy}: \; & v_0 \leftarrow \mathbf{x_0} + r_0 + r_1; \;\; w_0 \leftarrow \mathbf{x_0} + r_3 + r_4 \\
& v_1 \leftarrow \mathbf{x_1} + r_1 + r_2; \;\; w_1 \leftarrow \mathbf{x_1} + r_4 + r_5 \\
& v_2 \leftarrow \mathbf{x_2} + r_2 + r_0; \;\; w_2 \leftarrow \mathbf{x_2} + r_5 + r_3
\end{aligned}
$$

Random Probing Expandability

3-share gadgets Construction

$$G_{copy} : \begin{array}{ll} v_0 \leftarrow \mathbf{x_0} + r_0 + r_1; & w_0 \leftarrow \mathbf{x_0} + r_3 + r_4 \\ v_1 \leftarrow \mathbf{x_1} + r_1 + r_2; & w_1 \leftarrow \mathbf{x_1} + r_4 + r_5 \\ v_2 \leftarrow \mathbf{x_2} + r_2 + r_0; & w_2 \leftarrow \mathbf{x_2} + r_5 + r_3 \end{array}$$

$$G_{add} : \begin{array}{l} z_0 \leftarrow \mathbf{x_0} + r_0 + r_4 + \mathbf{y_0} + r_1 + r_3 \\ z_1 \leftarrow \mathbf{x_1} + r_1 + r_5 + \mathbf{y_1} + r_2 + r_4 \\ z_2 \leftarrow \mathbf{x_2} + r_2 + r_3 + \mathbf{y_2} + r_0 + r_5 \end{array}$$

Random Probing Expandability

3-share gadgets Construction

$$G_{copy}: \begin{array}{ll} v_0 \leftarrow \mathbf{x_0} + r_0 + r_1; & w_0 \leftarrow \mathbf{x_0} + r_3 + r_4 \\ v_1 \leftarrow \mathbf{x_1} + r_1 + r_2; & w_1 \leftarrow \mathbf{x_1} + r_4 + r_5 \\ v_2 \leftarrow \mathbf{x_2} + r_2 + r_0; & w_2 \leftarrow \mathbf{x_2} + r_5 + r_3 \end{array}$$

$$G_{add}: \begin{array}{l} z_0 \leftarrow \mathbf{x_0} + r_0 + r_4 + \mathbf{y_0} + r_1 + r_3 \\ z_1 \leftarrow \mathbf{x_1} + r_1 + r_5 + \mathbf{y_1} + r_2 + r_4 \\ z_2 \leftarrow \mathbf{x_2} + r_2 + r_3 + \mathbf{y_2} + r_0 + r_5 \end{array}$$

$$G_{mult}: \begin{array}{lll} u_0 \leftarrow \mathbf{x_0} + r_5 + r_6; & u_1 \leftarrow \mathbf{x_1} + r_6 + r_7; & u_2 \leftarrow \mathbf{x_2} + r_7 + r_5 \\ v_0 \leftarrow \mathbf{y_0} + r_8 + r_9; & v_1 \leftarrow \mathbf{y_1} + r_9 + r_{10}; & v_2 \leftarrow \mathbf{y_2} + r_{10} + r_8 \end{array}$$

Random Probing Expandability

3-share gadgets Construction

$$G_{copy}: \begin{aligned} v_0 &\leftarrow \mathbf{x_0} + r_0 + r_1; & w_0 &\leftarrow \mathbf{x_0} + r_3 + r_4 \\ v_1 &\leftarrow \mathbf{x_1} + r_1 + r_2; & w_1 &\leftarrow \mathbf{x_1} + r_4 + r_5 \\ v_2 &\leftarrow \mathbf{x_2} + r_2 + r_0; & w_2 &\leftarrow \mathbf{x_2} + r_5 + r_3 \end{aligned}$$

$$G_{add}: \begin{aligned} z_0 &\leftarrow \mathbf{x_0} + r_0 + r_4 + \mathbf{y_0} + r_1 + r_3 \\ z_1 &\leftarrow \mathbf{x_1} + r_1 + r_5 + \mathbf{y_1} + r_2 + r_4 \\ z_2 &\leftarrow \mathbf{x_2} + r_2 + r_3 + \mathbf{y_2} + r_0 + r_5 \end{aligned}$$

$$G_{mult}: \begin{aligned} u_0 &\leftarrow \mathbf{x_0} + r_5 + r_6; & u_1 &\leftarrow \mathbf{x_1} + r_6 + r_7; & u_2 &\leftarrow \mathbf{x_2} + r_7 + r_5 \\ v_0 &\leftarrow \mathbf{y_0} + r_8 + r_9; & v_1 &\leftarrow \mathbf{y_1} + r_9 + r_{10}; & v_2 &\leftarrow \mathbf{y_2} + r_{10} + r_8 \end{aligned}$$

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

Random Probing Expandability

3-share gadgets Construction

$$G_{copy} : v_0 \leftarrow \mathbf{x_0} + r_0 + r_1;\ w_0 \leftarrow \mathbf{x_0} + r_3 + r_4$$
$$v_1 \leftarrow \mathbf{x_1} + r_1 + r_2;\ w_1 \leftarrow \mathbf{x_1} + r_4 + r_5$$
$$v_2 \leftarrow \mathbf{x_2} + r_2 + r_0;\ w_2 \leftarrow \mathbf{x_2} + r_5 + r_3$$

$$G_{add} : z_0 \leftarrow \mathbf{x_0} + r_0 + r_4 + \mathbf{y_0} + r_1 + r_3$$
$$z_1 \leftarrow \mathbf{x_1} + r_1 + r_5 + \mathbf{y_1} + r_2 + r_4$$
$$z_2 \leftarrow \mathbf{x_2} + r_2 + r_3 + \mathbf{y_2} + r_0 + r_5$$

$$G_{mult} : u_0 \leftarrow \mathbf{x_0} + r_5 + r_6; \quad u_1 \leftarrow \mathbf{x_1} + r_6 + r_7; \quad u_2 \leftarrow \mathbf{x_2} + r_7 + r_5$$
$$v_0 \leftarrow \mathbf{y_0} + r_8 + r_9; \quad v_1 \leftarrow \mathbf{y_1} + r_9 + r_{10}; \quad v_2 \leftarrow \mathbf{y_2} + r_{10} + r_8$$

$$z_0 \leftarrow \big(u_0 \cdot v_0 + r_0\big) + \big(u_0 \cdot v_1 + r_1\big) + \big(u_0 \cdot v_2 + r_2\big)$$
$$z_1 \leftarrow \big(u_1 \cdot v_0 + r_1\big) + \big(u_1 \cdot v_1 + r_4\big) + \big(u_1 \cdot v_2 + r_3\big)$$
$$z_2 \leftarrow \big(u_2 \cdot v_0 + r_2\big) + \big(u_2 \cdot v_1 + r_3\big) + \big(u_2 \cdot v_2 + r_0\big) + r_4$$

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

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:

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

Random Probing Expandability
Asymptotic Complexity

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

On previous 3-share gadgets:

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

Random Probing Expandability

Asymptotic Complexity

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

On previous 3-share gadgets:

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

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:

$$M = \begin{array}{c} \begin{array}{cccc} N_{G_{add}}^T & N_{G_{copy}}^T & N_{G_{mult}}^T & N_{rand}^T \end{array} \\ \begin{pmatrix} \multicolumn{2}{c}{\multirow{2}{*}{\mathrm{M}_{ac}}} & 28 & 0 \\ & & 23 & 0 \\ 0 & 0 & N_m & 0 \\ 6 & 6 & 1 & 3 \end{pmatrix} \end{array} = Q.\Lambda.Q^{-1}$$

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:

$$M = \begin{array}{c} \begin{array}{cccc} N^T_{G_{add}} & N^T_{G_{copy}} & N^T_{G_{mult}} & N^T_{rand} \end{array} \\ \begin{pmatrix} \multicolumn{2}{c}{\multirow{2}{*}{M_{ac}}} & 28 & 0 \\ & & 23 & 0 \\ 0 & 0 & N_m & 0 \\ 6 & 6 & 1 & 3 \end{pmatrix} \end{array} = Q.\Lambda.Q^{-1}$$

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

$|\hat{C}| = \mathcal{O}(|C|.N^k_{\max}), \qquad N_{\max} = \max\left(eigenvalues(M_{ac}), N_{mult}\right)$

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 $f^{(k)}(p) \leq 2^{-\kappa}$:

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

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 $f^{(k)}(p) \leq 2^{-\kappa}$:

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

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	**[Ananth et al., 2018] Strategy**
(t, f)-RPE Security	(p, ϵ)-Composable Security
Secure (t, f)-RPE gadgets	(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}

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

[Ananth et al., 2018] Strategy

(p, ϵ)-Composable Security

(m, c)-MPC protocols

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

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

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}

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

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

[Ananth et al., 2018] Strategy

(p, ϵ)-Composable Security

(m, c)-MPC protocols

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

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

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

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

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