On the provable security of cryptographic implementations

Matthieu Rivain

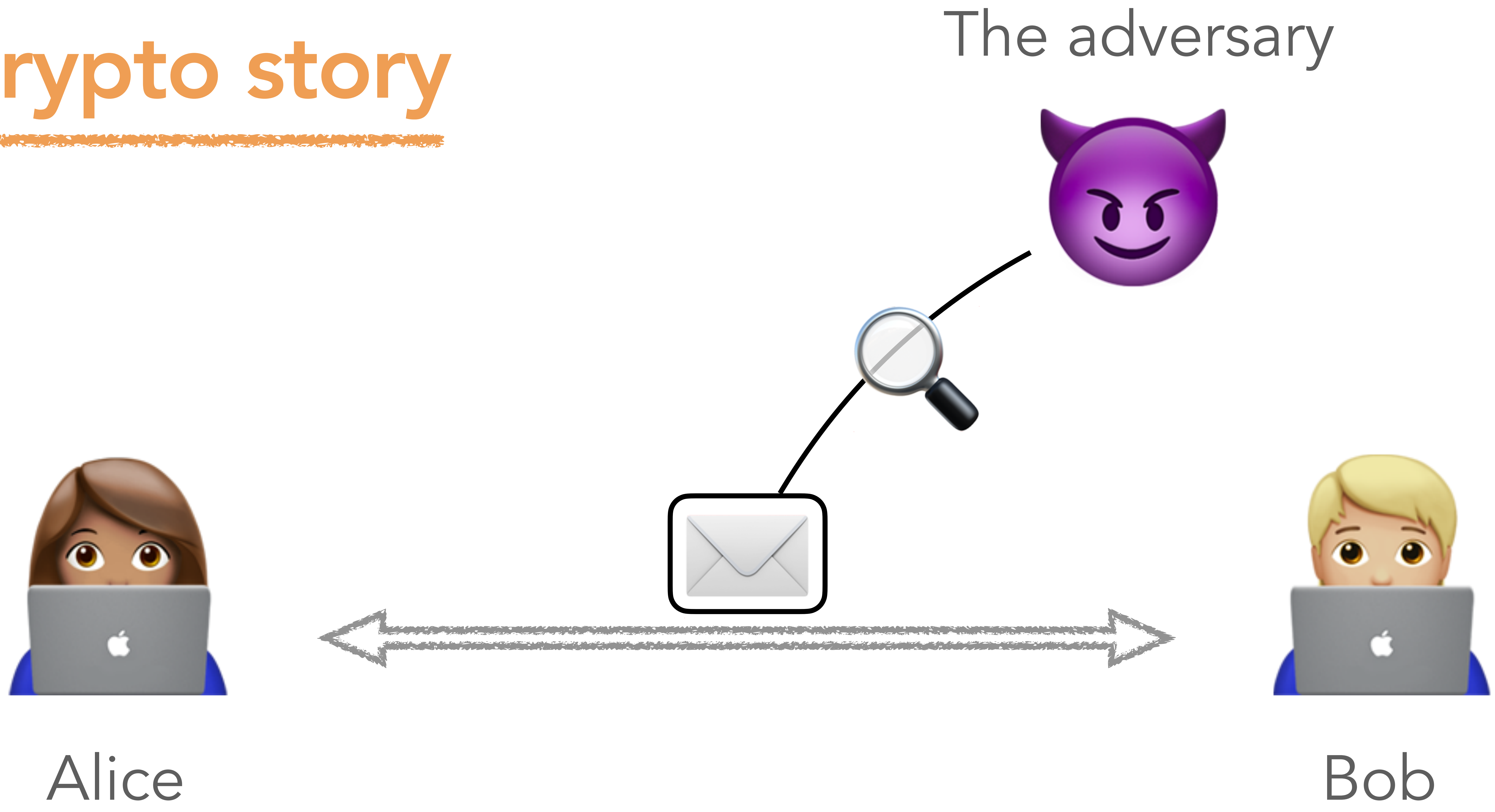
Habilitation defense

June 21, 2022, École normale supérieure

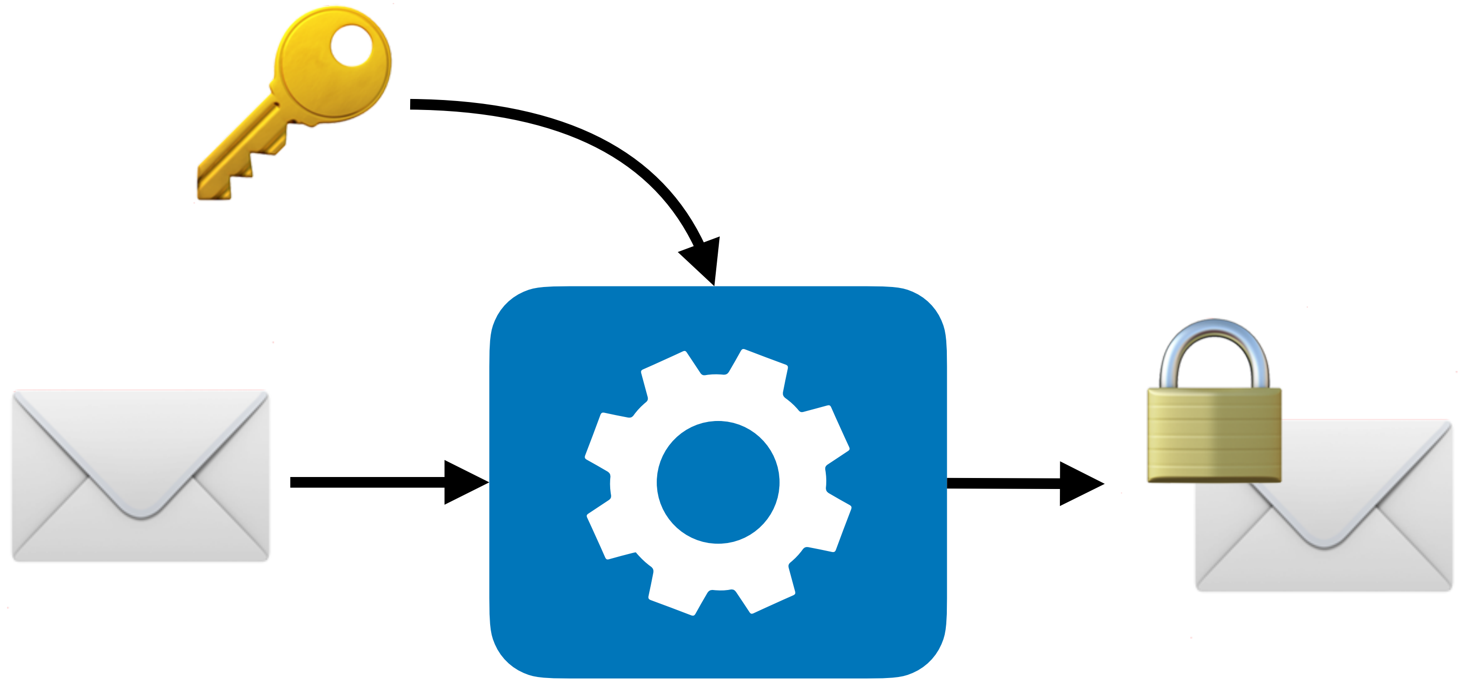
1. Introduction

A crypto story

A crypto story

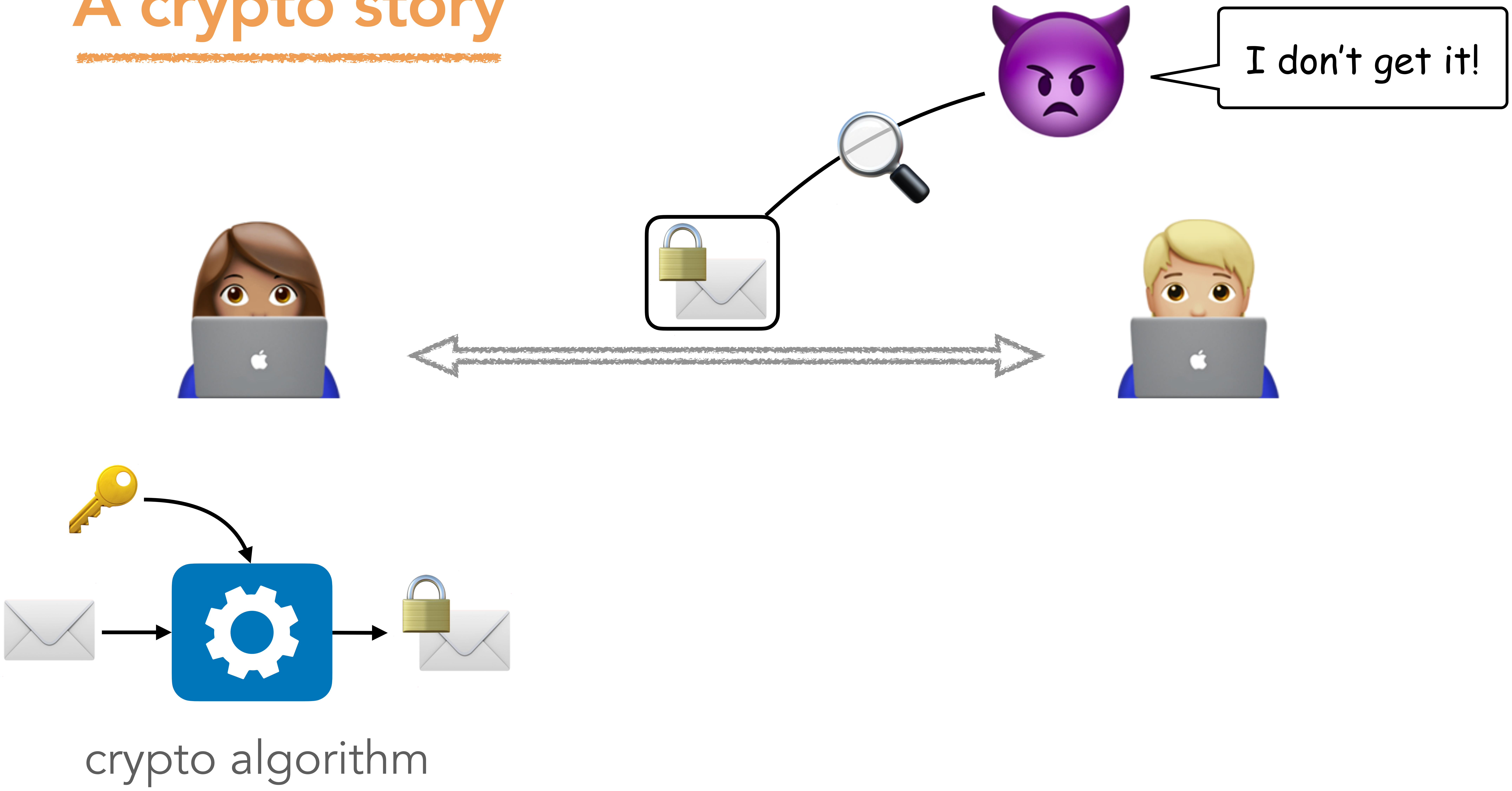


A crypto story

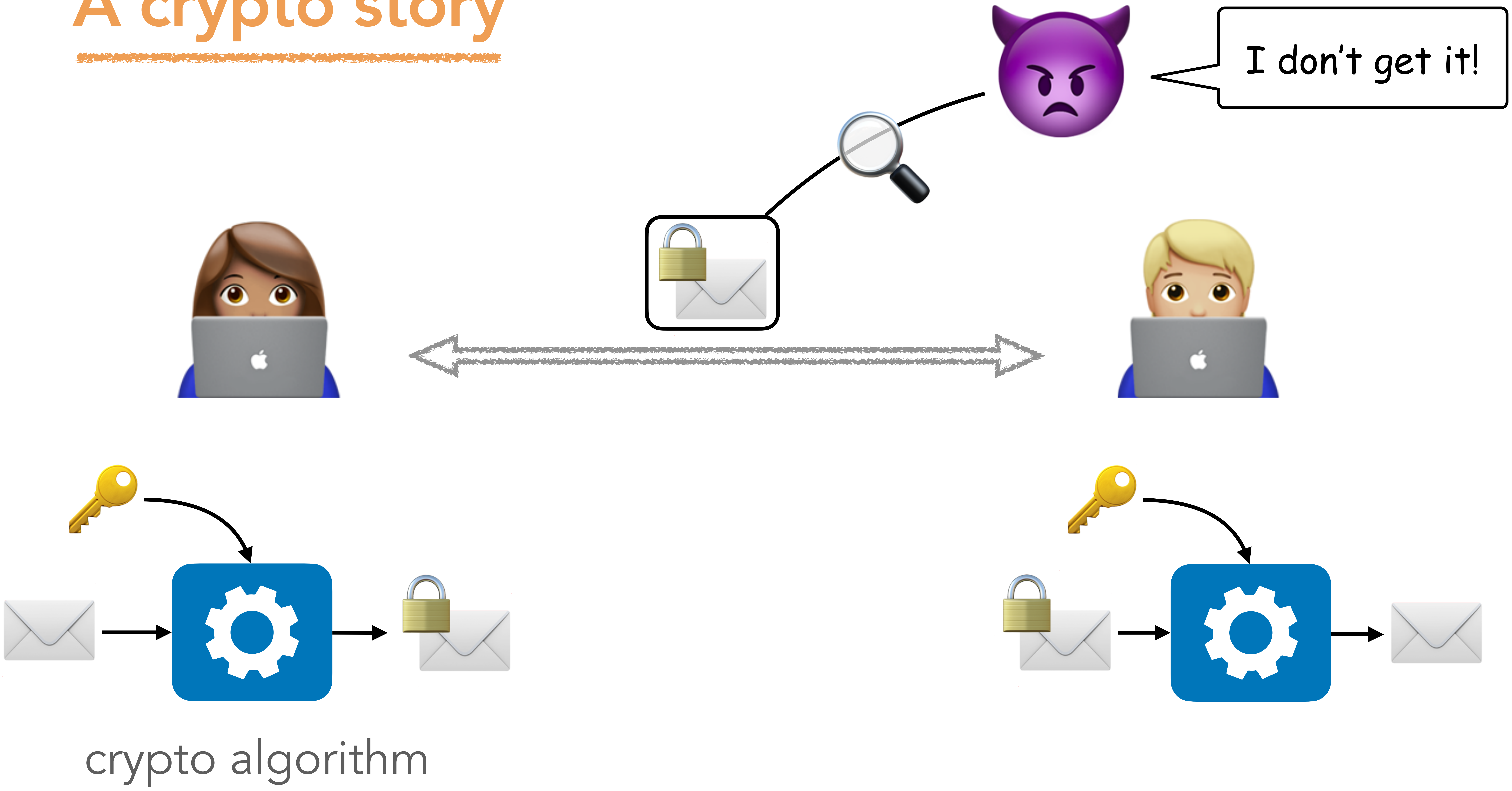


crypto algorithm

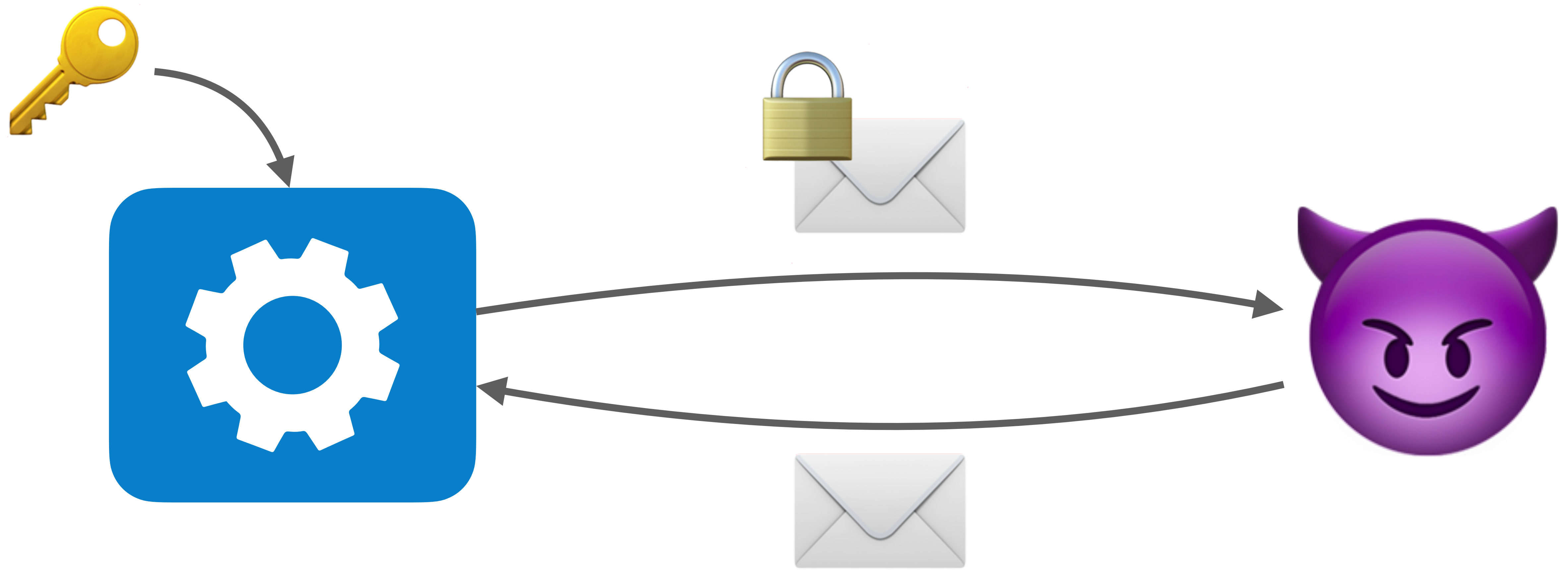
A crypto story



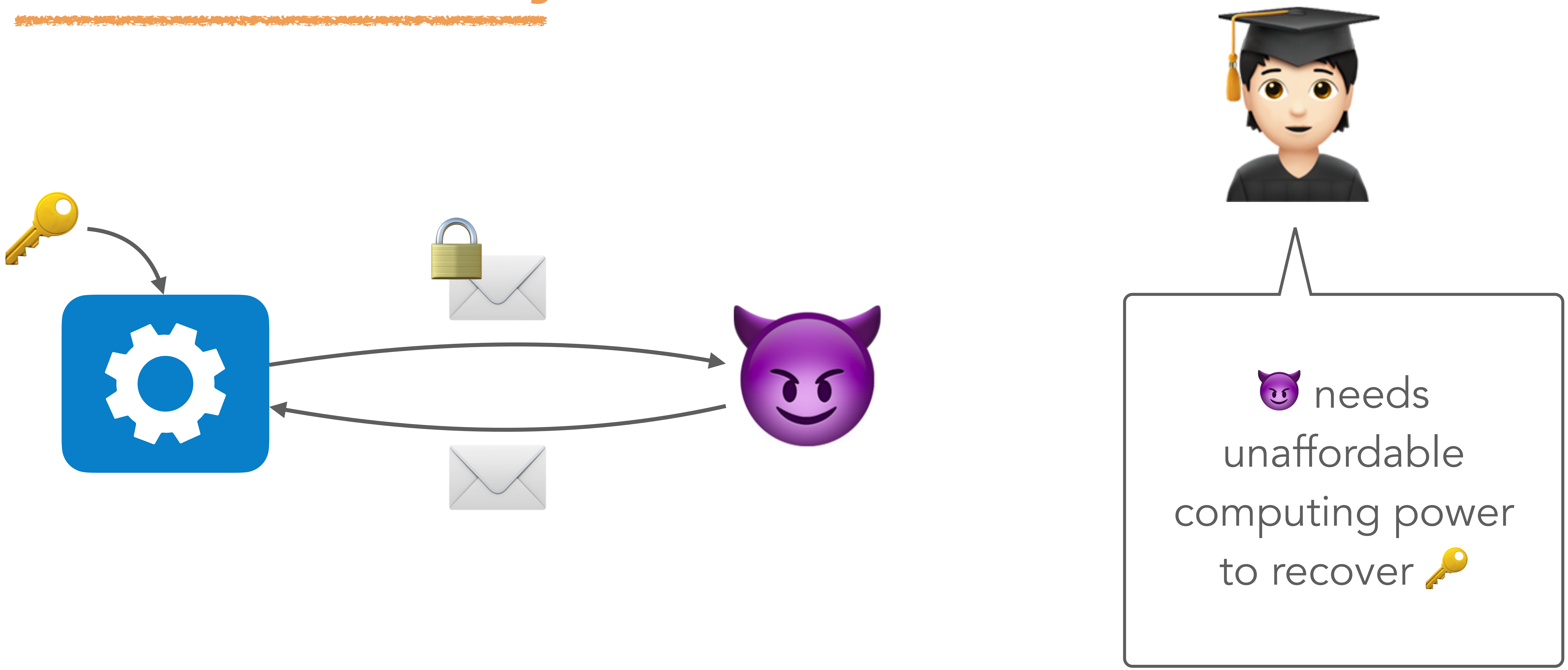
A crypto story



Provable security

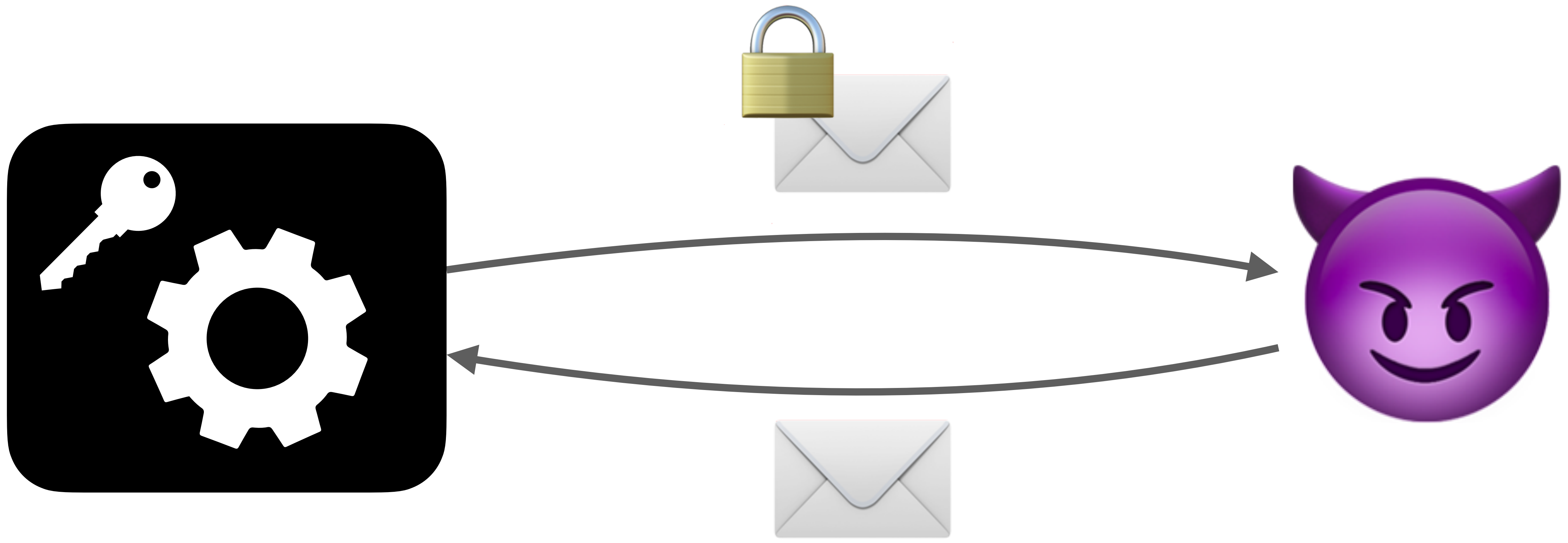


Provable security



security proof

Provable security

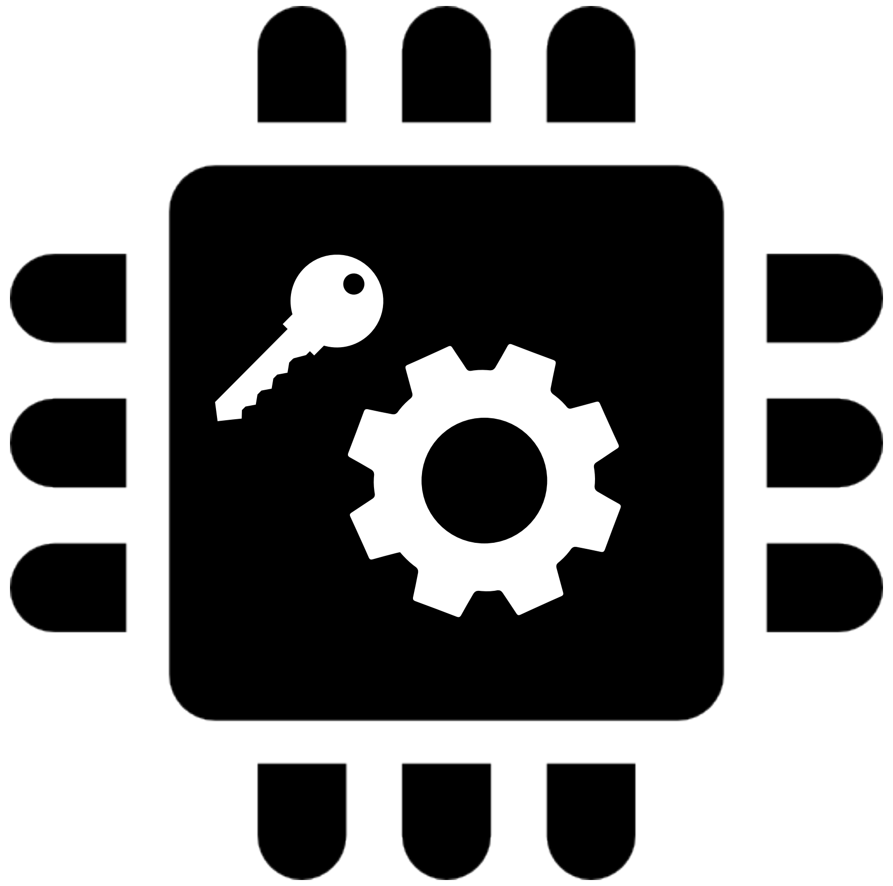


The "black-box model"

needs unaffordable computing power to recover

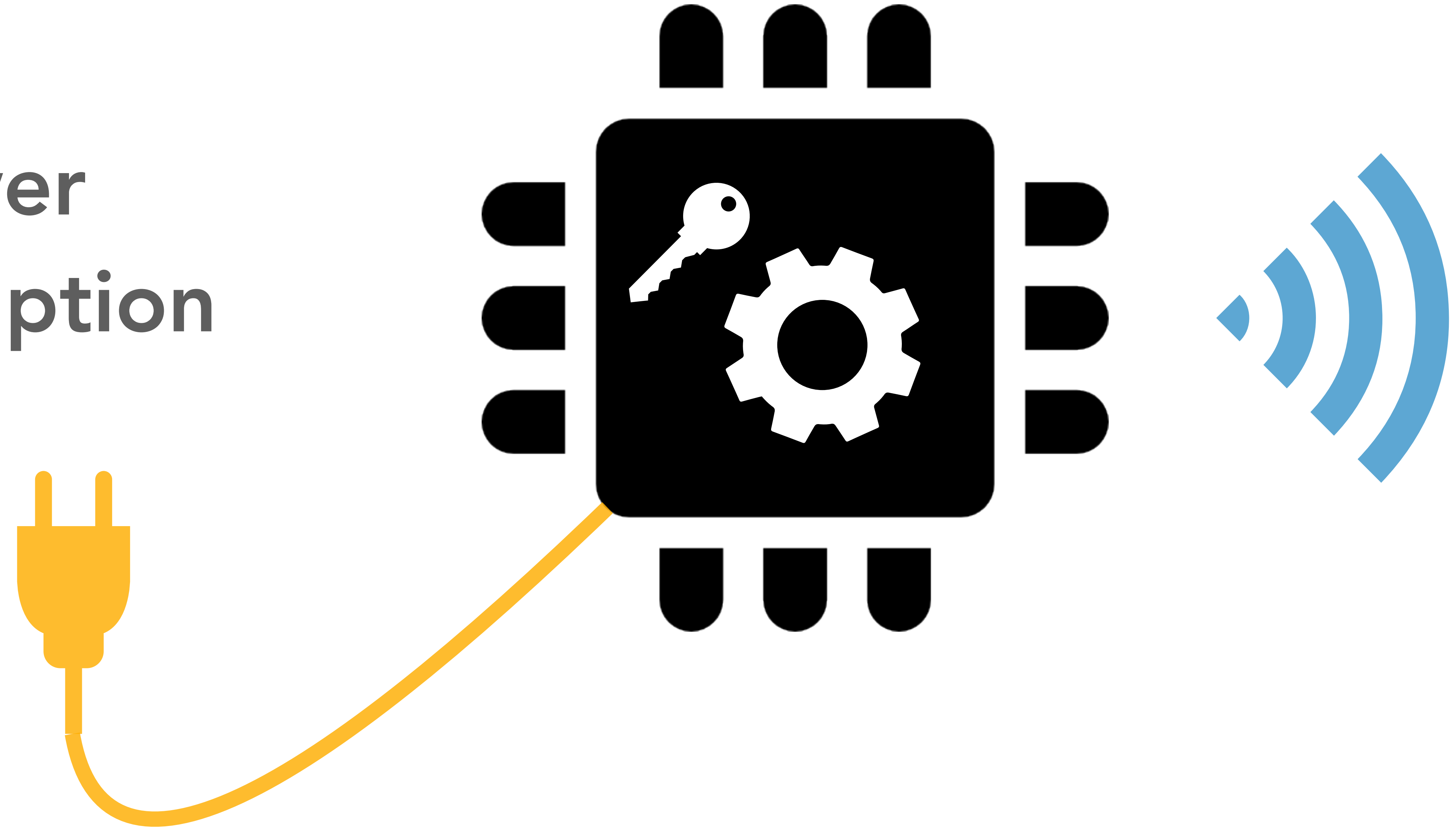
security proof

Side-channel attacks



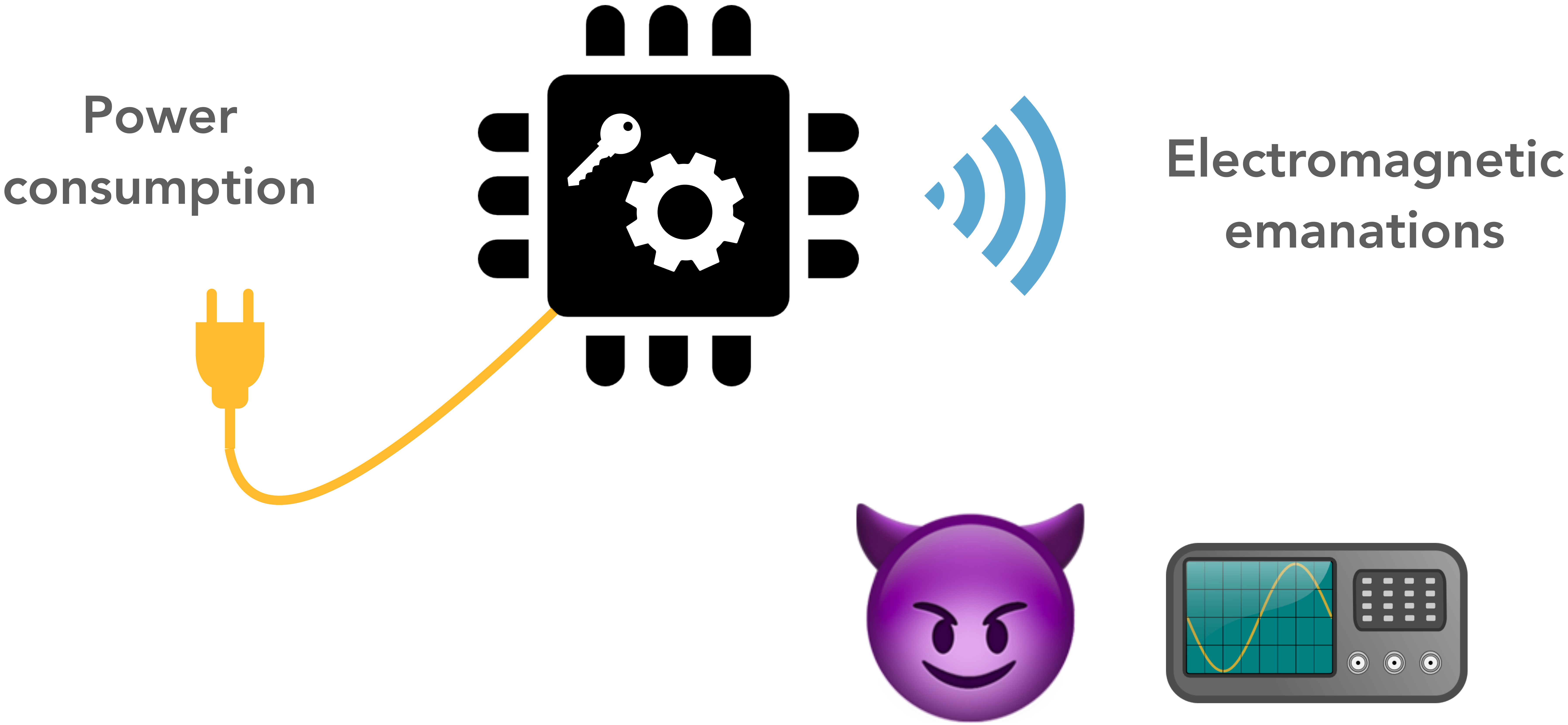
Side-channel attacks

Power consumption



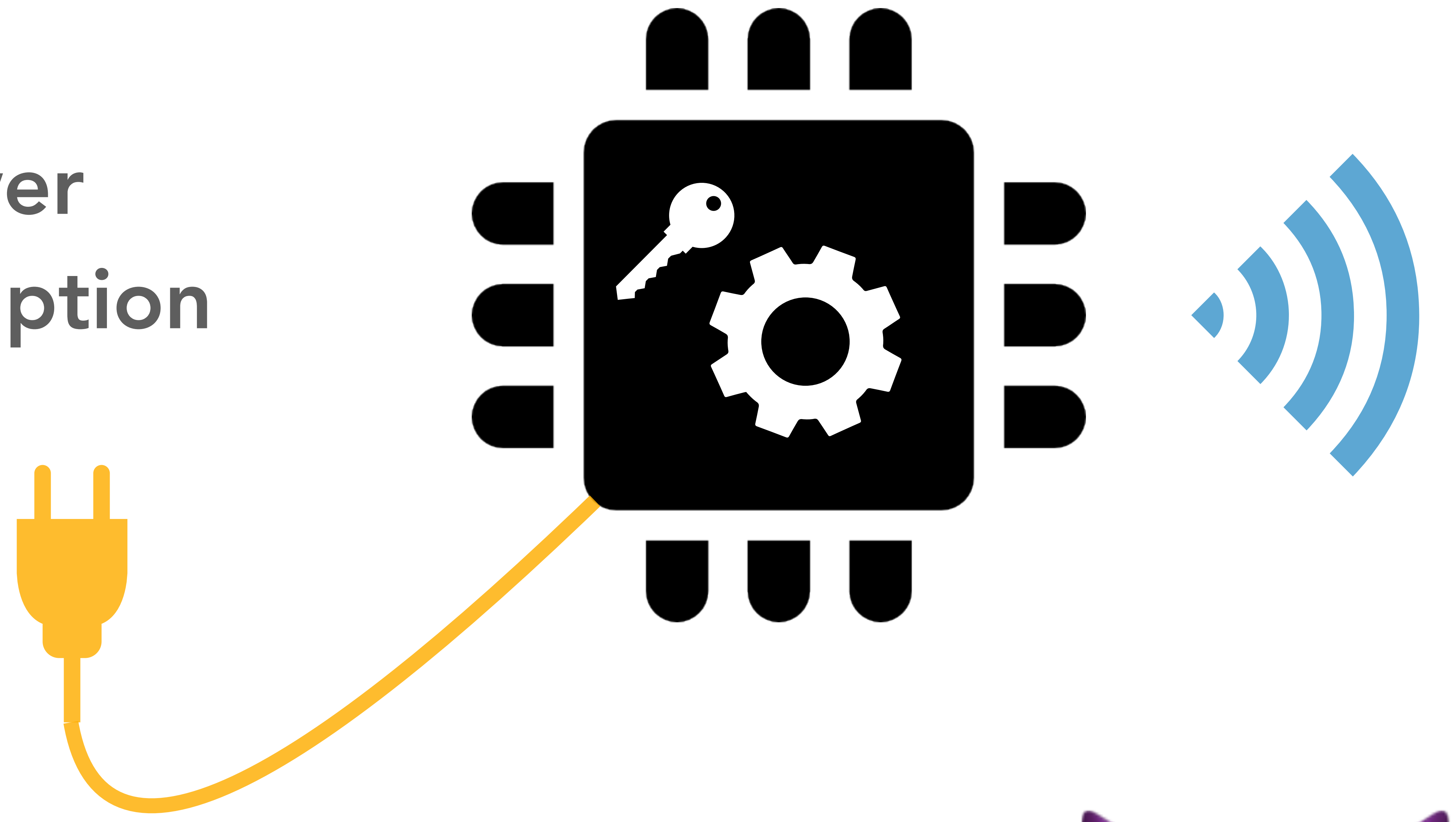
Electromagnetic emanations

Side-channel attacks



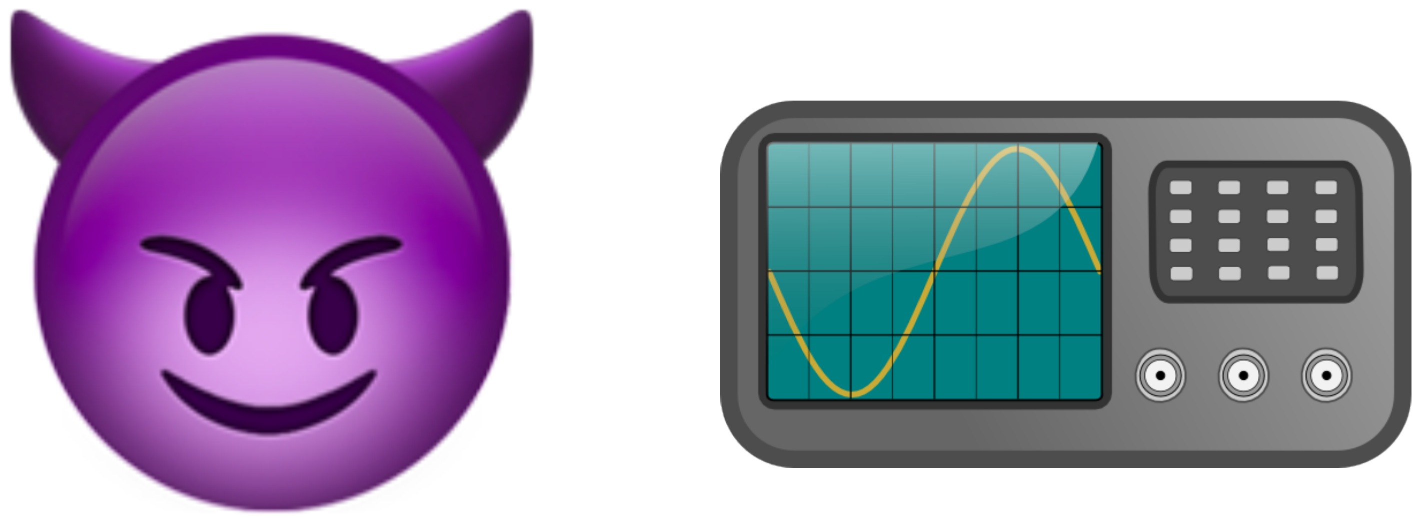
Side-channel attacks

Power consumption

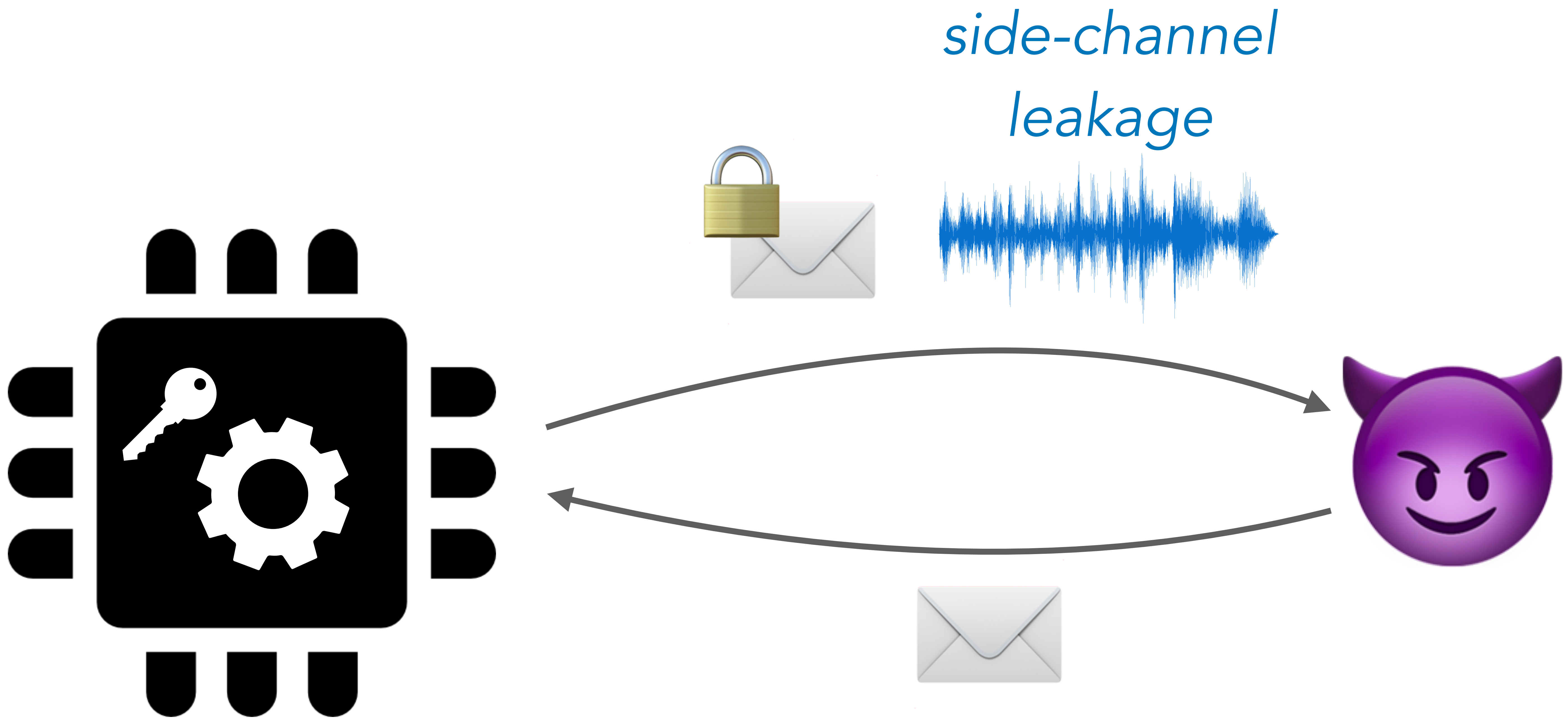


Electromagnetic emanations

Kocher, Jaffe, Jun - CRYPTO'99



Provable security in the presence of leakage



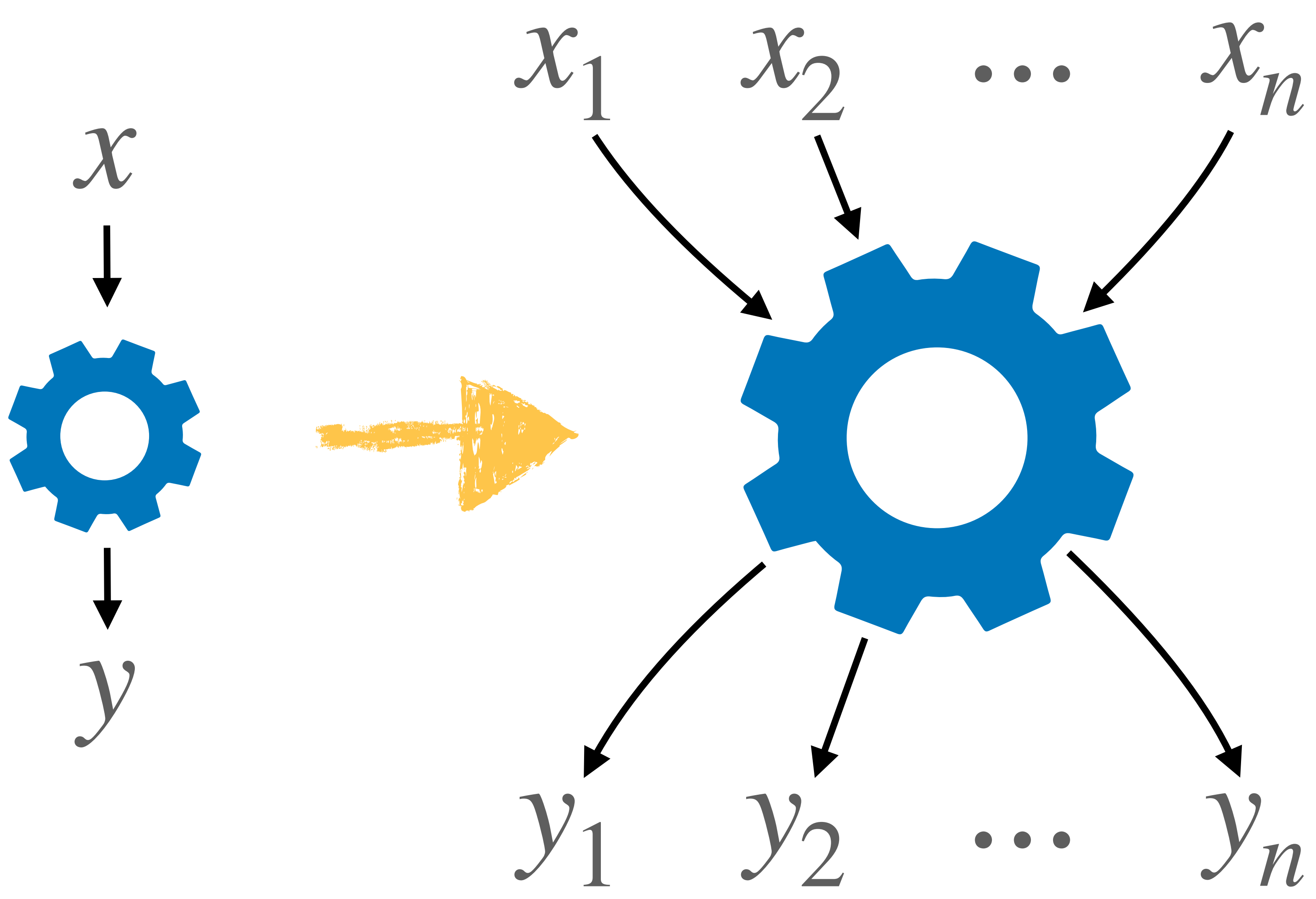
security proof

2. A tell of masks

Masking

Apply secret sharing at the computation level

$$x = x_1 + \cdots + x_n$$



Chari, Jutla, Rao, Rohatgi - CRYPTO’99

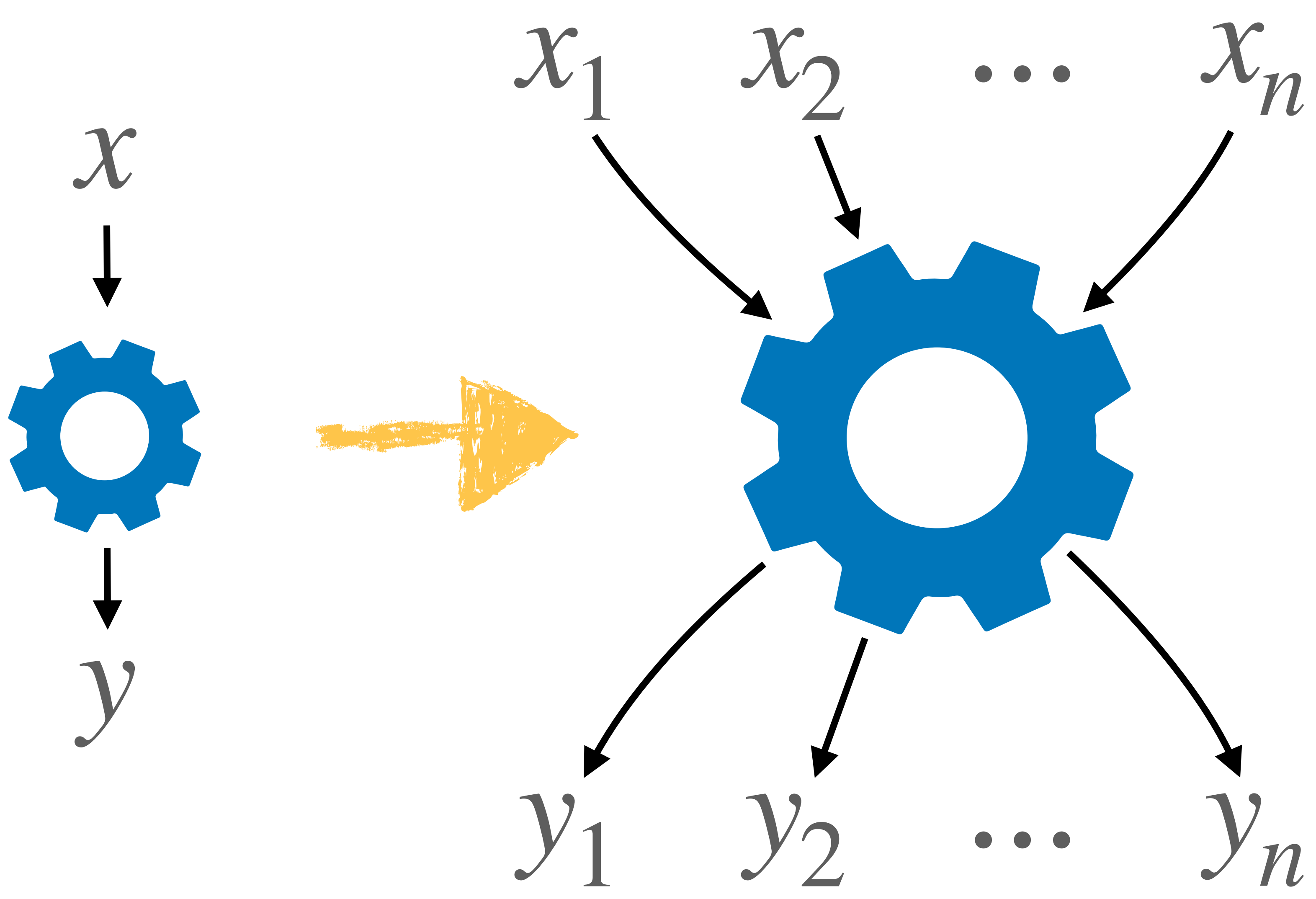
Goubin, Patarin - CHES’99

Patents by Kocher, Jaffe, Jun (1998)

Masking

Apply secret sharing at the computation level

$$x = x_1 + \cdots + x_n$$



Chari, Jutla, Rao, Rohatgi - CRYPTO'99

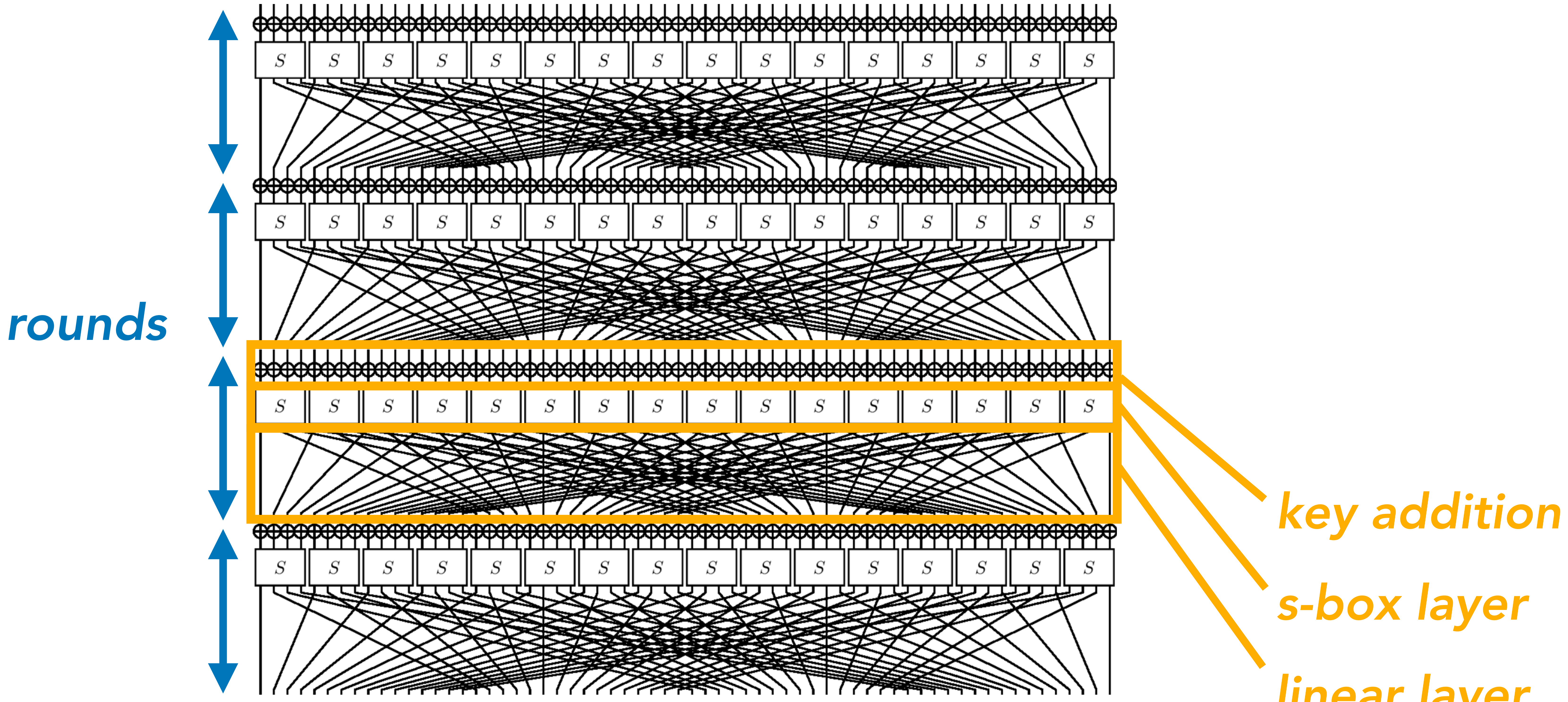
Goubin, Patarin - CHES'99

Patents by Kocher, Jaffe, Jun (1998)

<u>n-order side-channel security:</u>

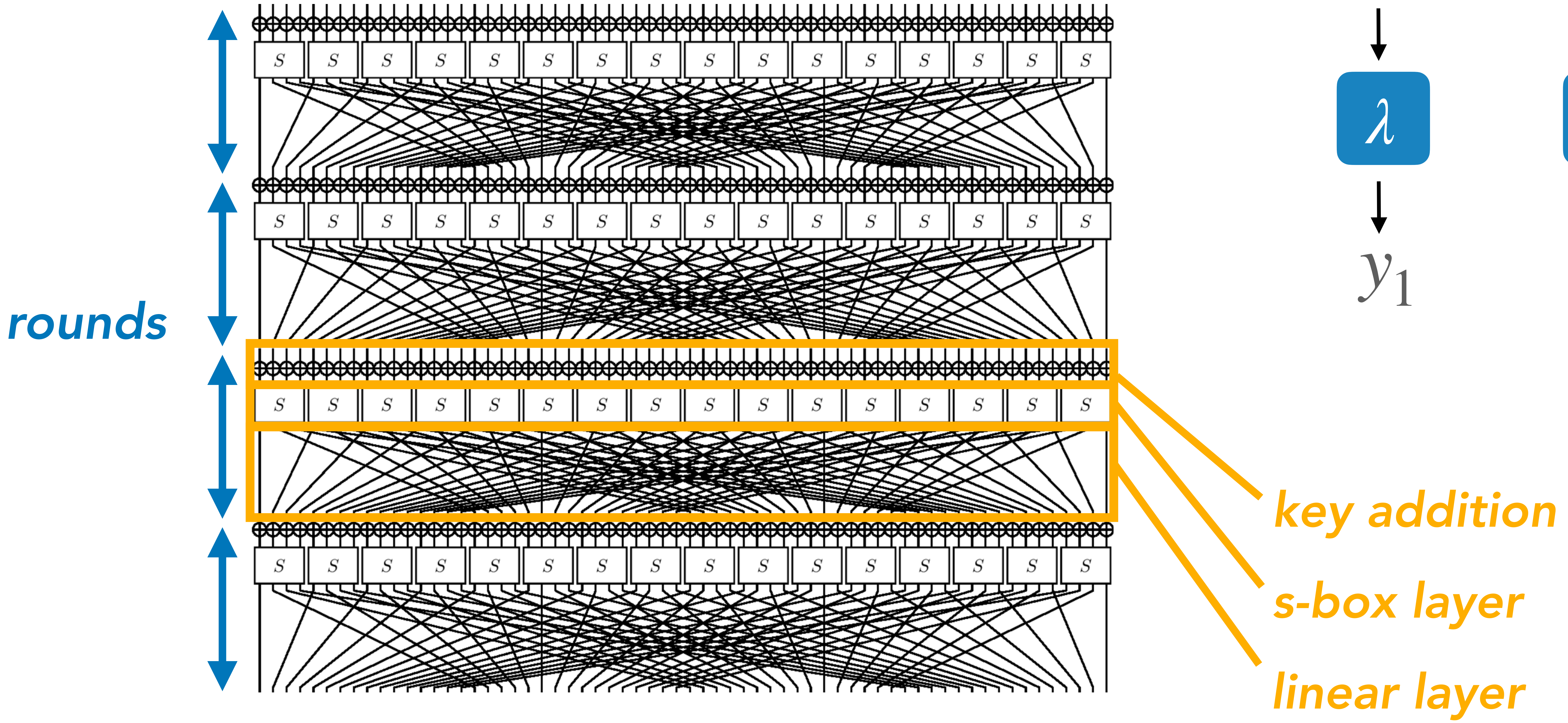
Any tuple of size $< n$ is independent of the secrets

Masking of block ciphers



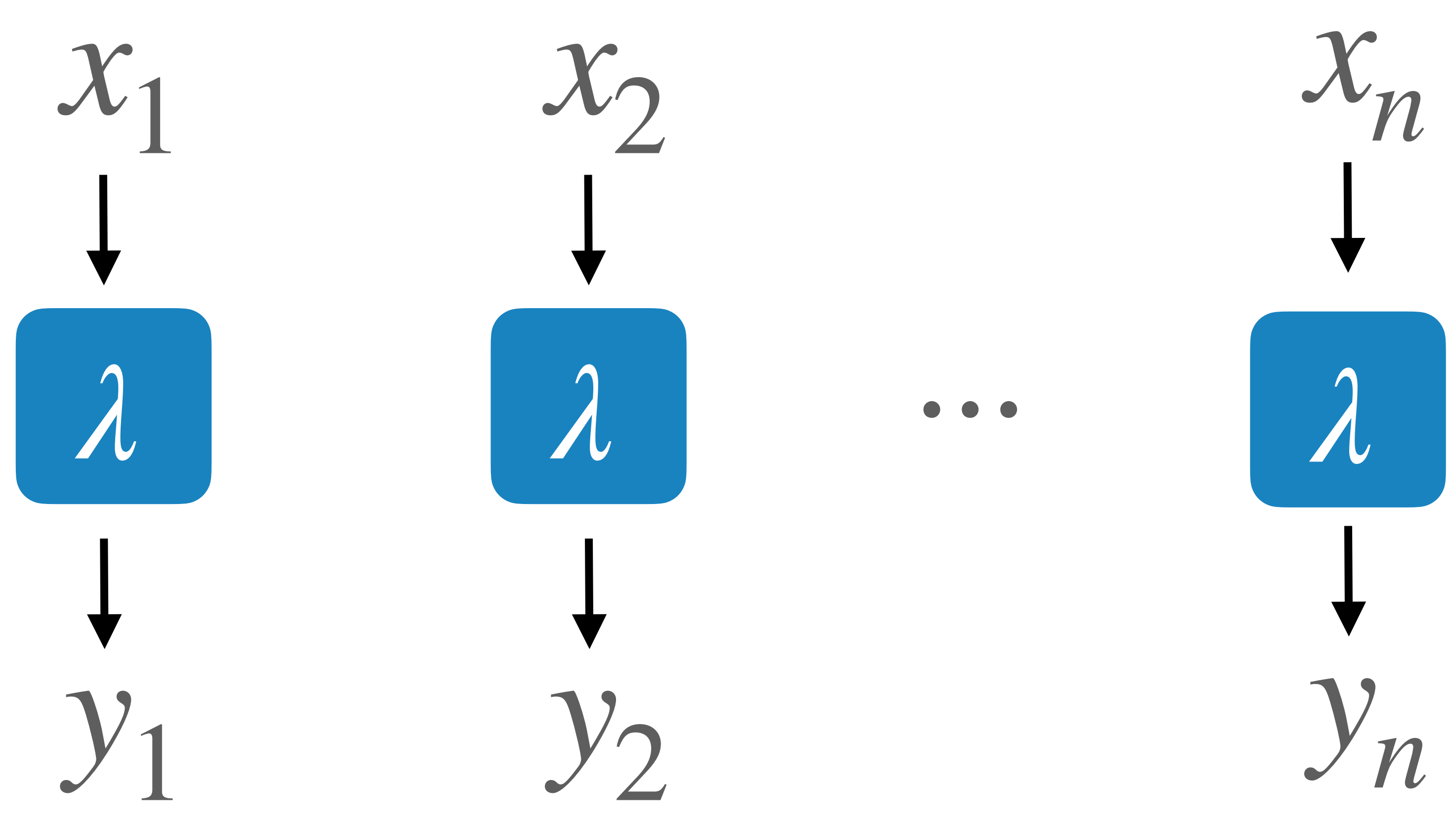
Source: https://www.iacr.org/authors/tikz/
Jérémy Jean

Masking of block ciphers

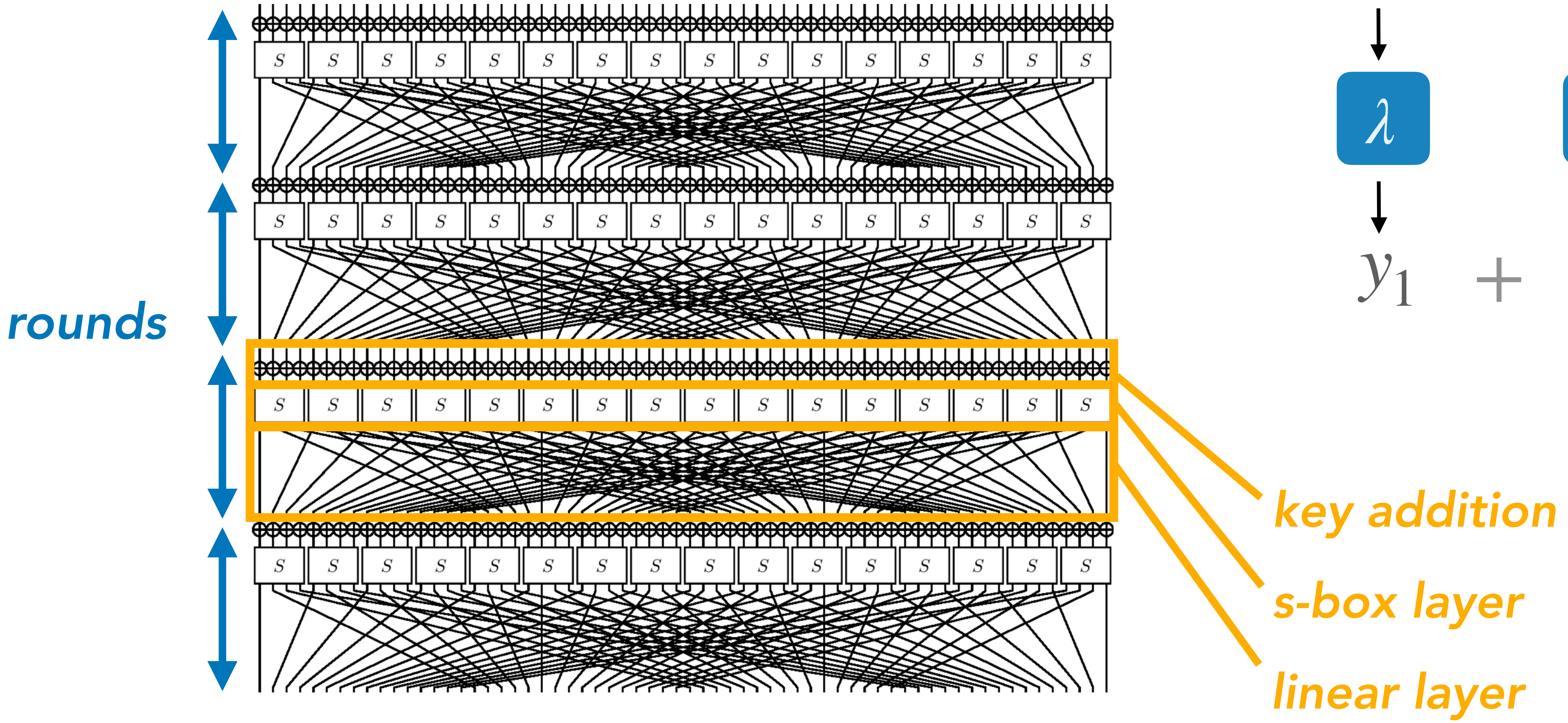


Source: https://www.iacr.org/authors/tikz/
Jérémy Jean

Linear operations:



Masking of block ciphers



Source: https://www.iacr.org/authors/tikz/
Jérémy Jean

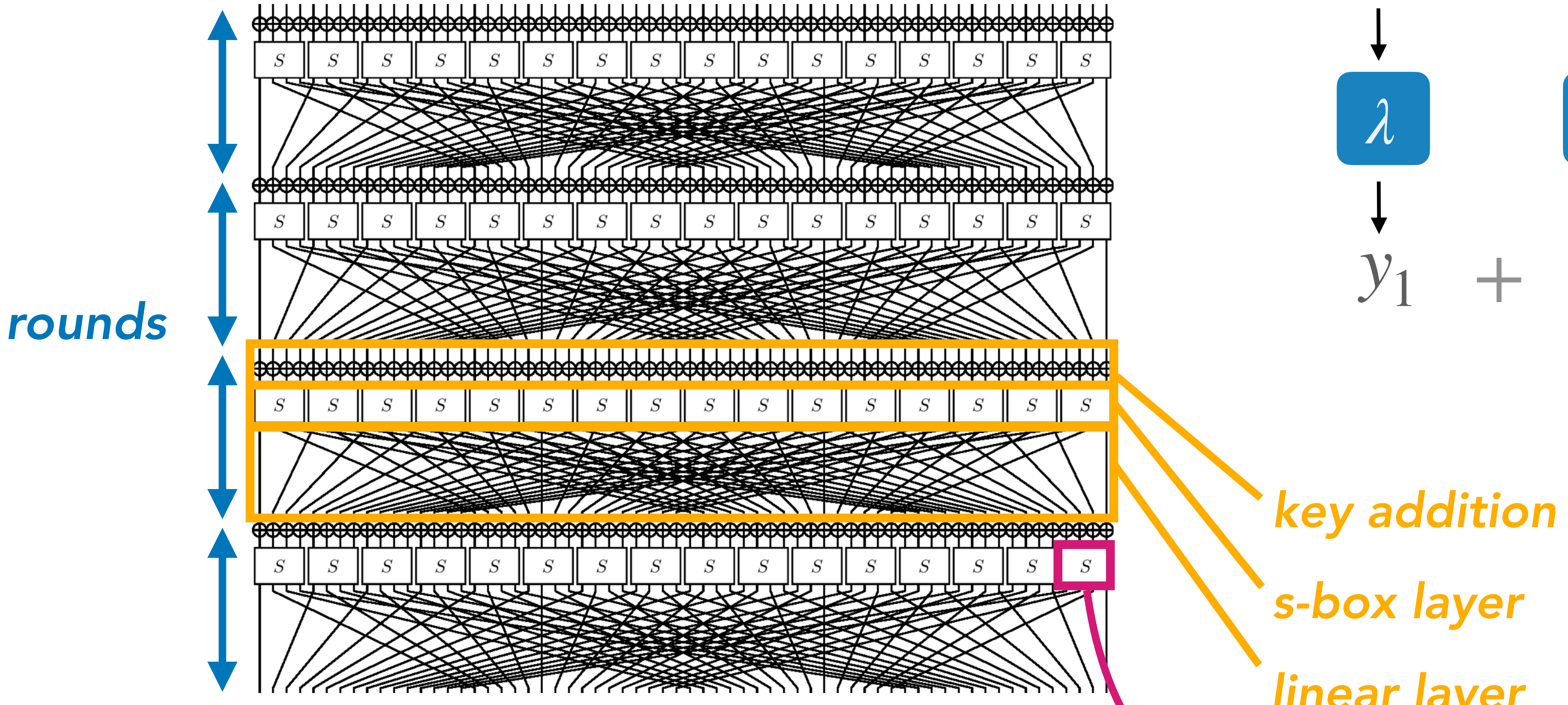
Linear operations:

$$x_1 + x_2 + \cdots + x_n = x$$

$$\lambda \qquad \lambda \qquad \cdots \qquad \lambda$$

$$y_1 + y_2 + \cdots + y_n = \lambda(x)$$

Masking of block ciphers



Source: https://www.iacr.org/authors/tikz/
Jérémy Jean

Linear operations:

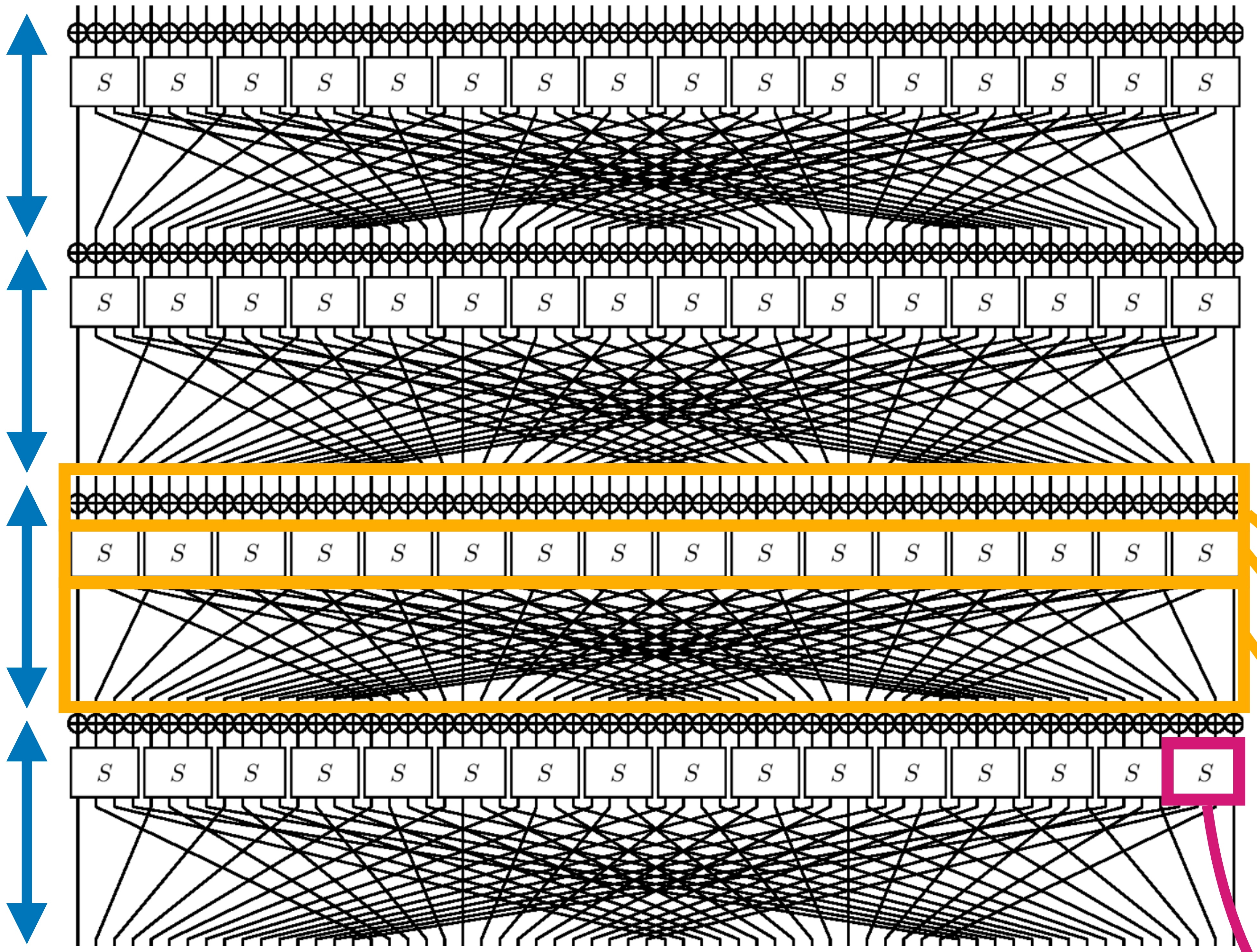
$$x_1 + x_2 + \cdots + x_n = x$$

$$\downarrow \lambda \qquad \downarrow \lambda \qquad \cdots \qquad \downarrow \lambda$$

$$y_1 + y_2 + \cdots + y_n = \lambda(x)$$

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	[illegible]	[illegible]
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	[illegible]	[illegible]
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	[illegible]	[illegible]
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	[illegible]	[illegible]	[illegible]
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	[illegible]	[illegible]
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	[illegible]	[illegible]
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

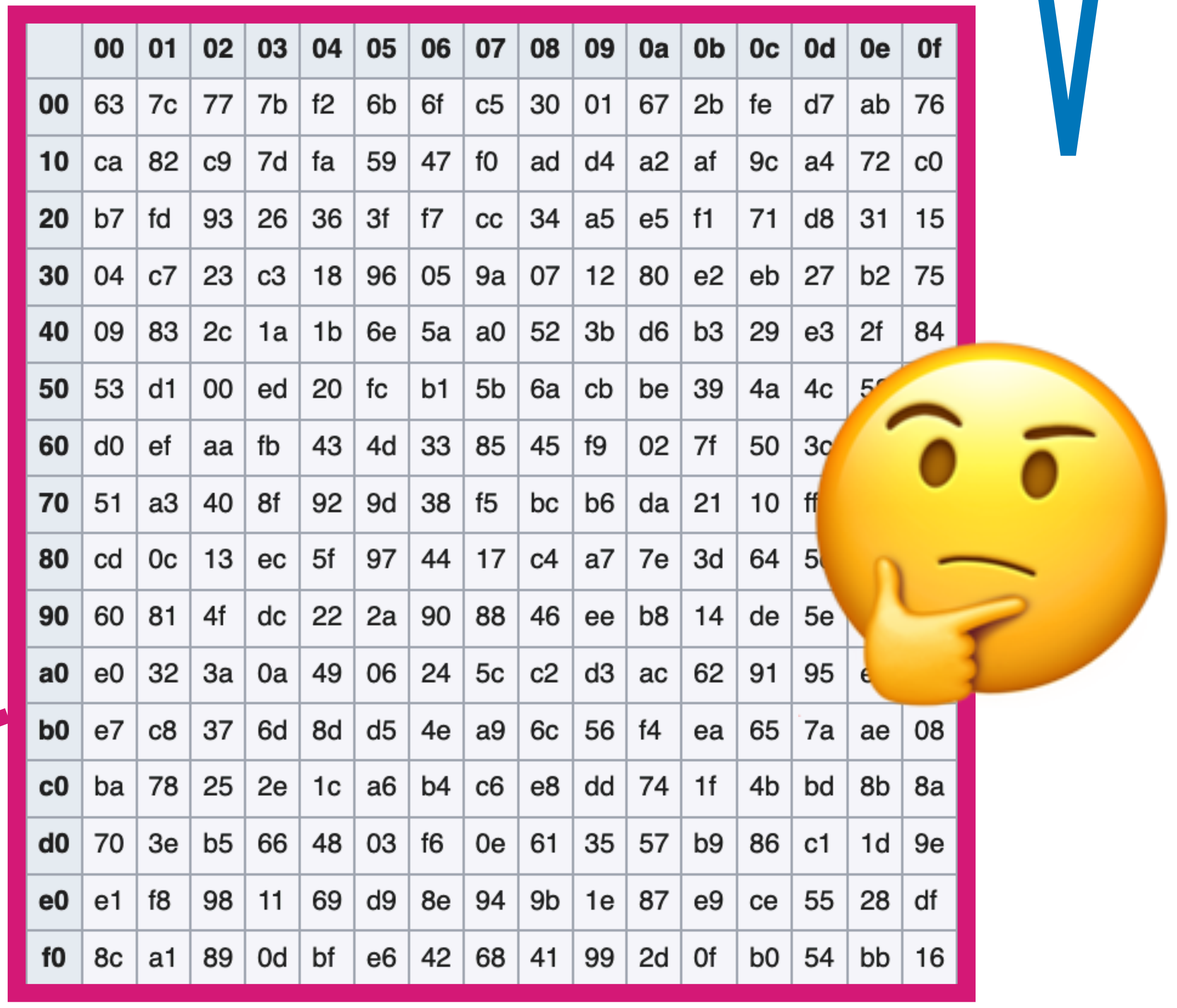
Masking of block ciphers



Source: https://www.iacr.org/authors/tikz/
Jérémy Jean

Back before 2010:

- Solutions based on table randomisation
- First (or second) order masking only
- Any masking order: open problem?

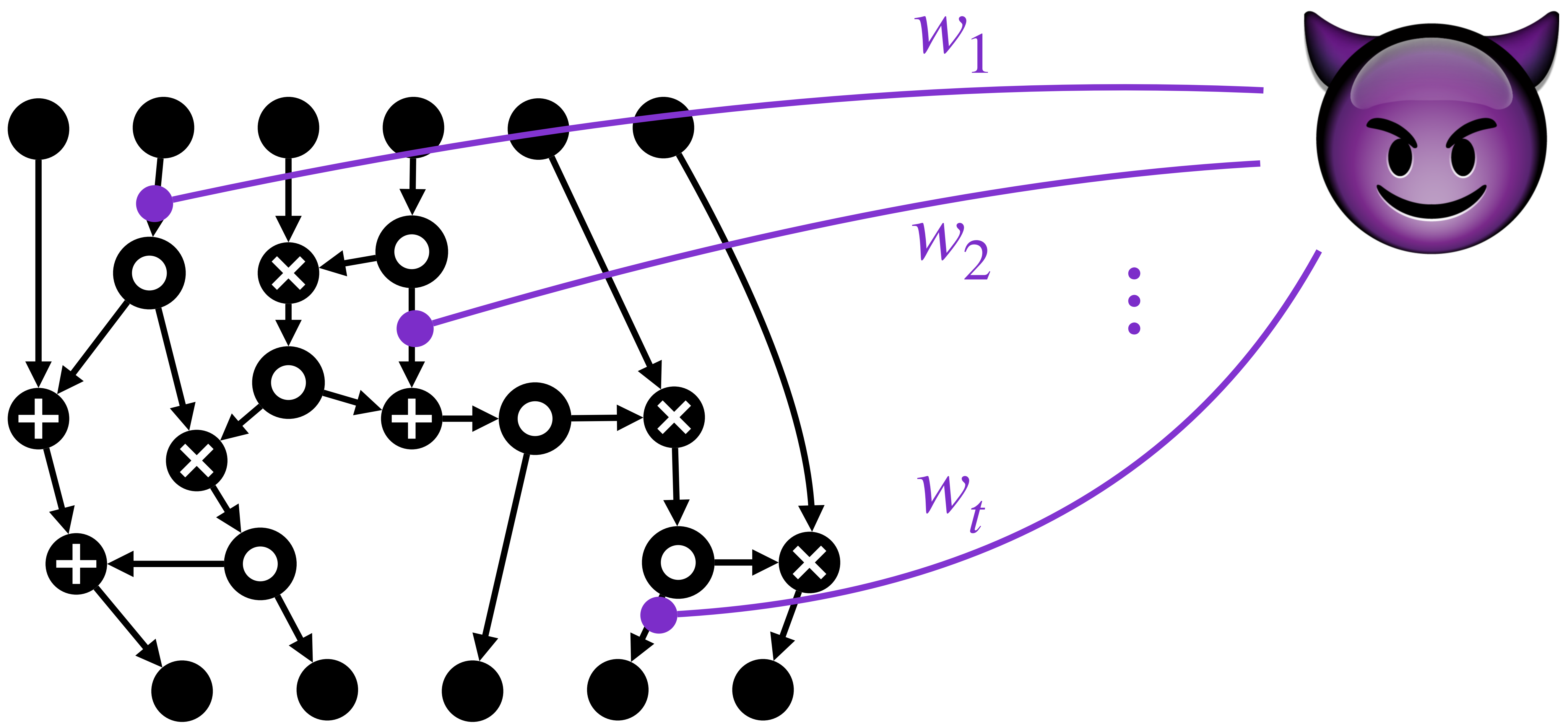


	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	[illegible]	[illegible]
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	[illegible]	[illegible]
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	[illegible]	[illegible]
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	[illegible]	[illegible]	[illegible]
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	[illegible]	[illegible]
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	[illegible]	[illegible]
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

The ISW scheme

Ishai, Sahai, Wagner - CRYPTO 2003

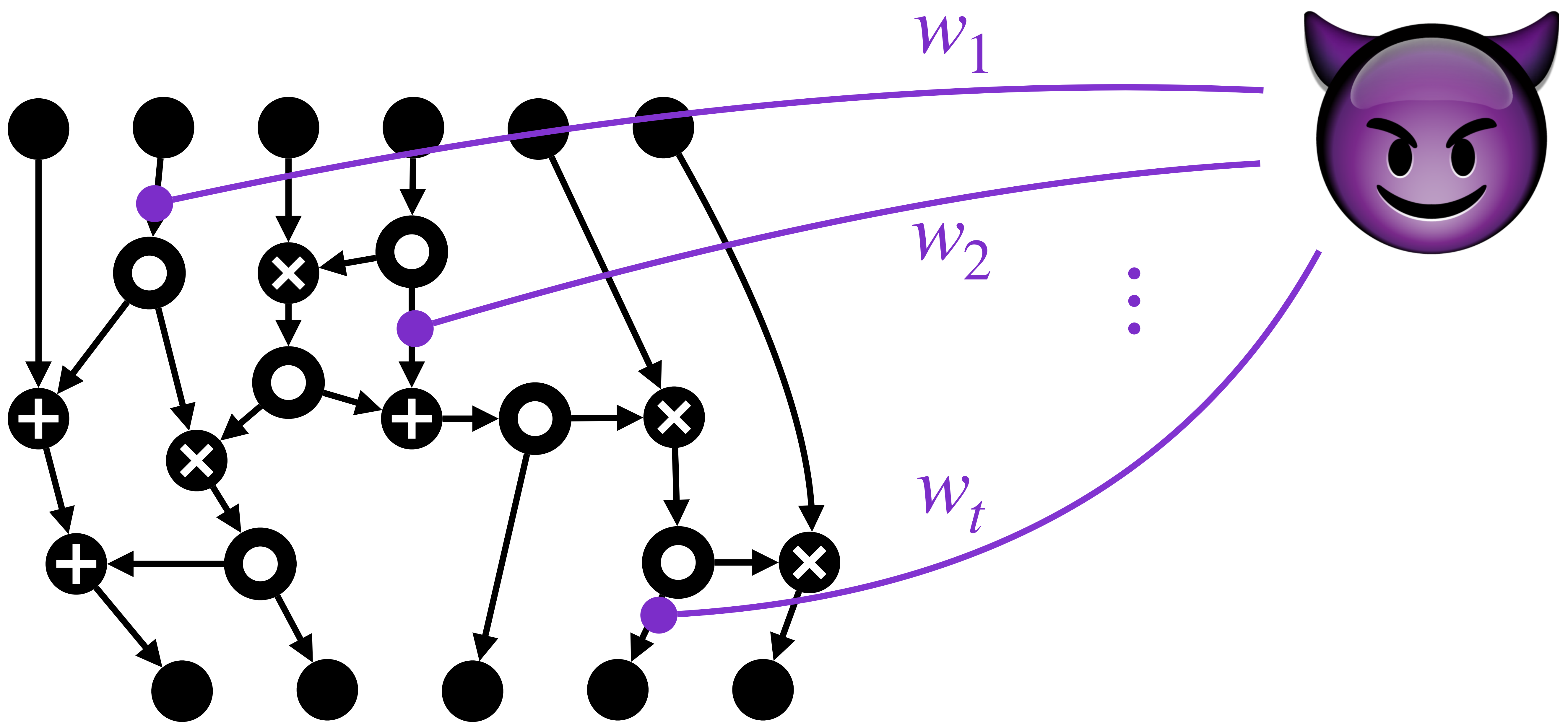
Probing model



The ISW scheme

Ishai, Sahai, Wagner - CRYPTO 2003

Probing model



t-probing security

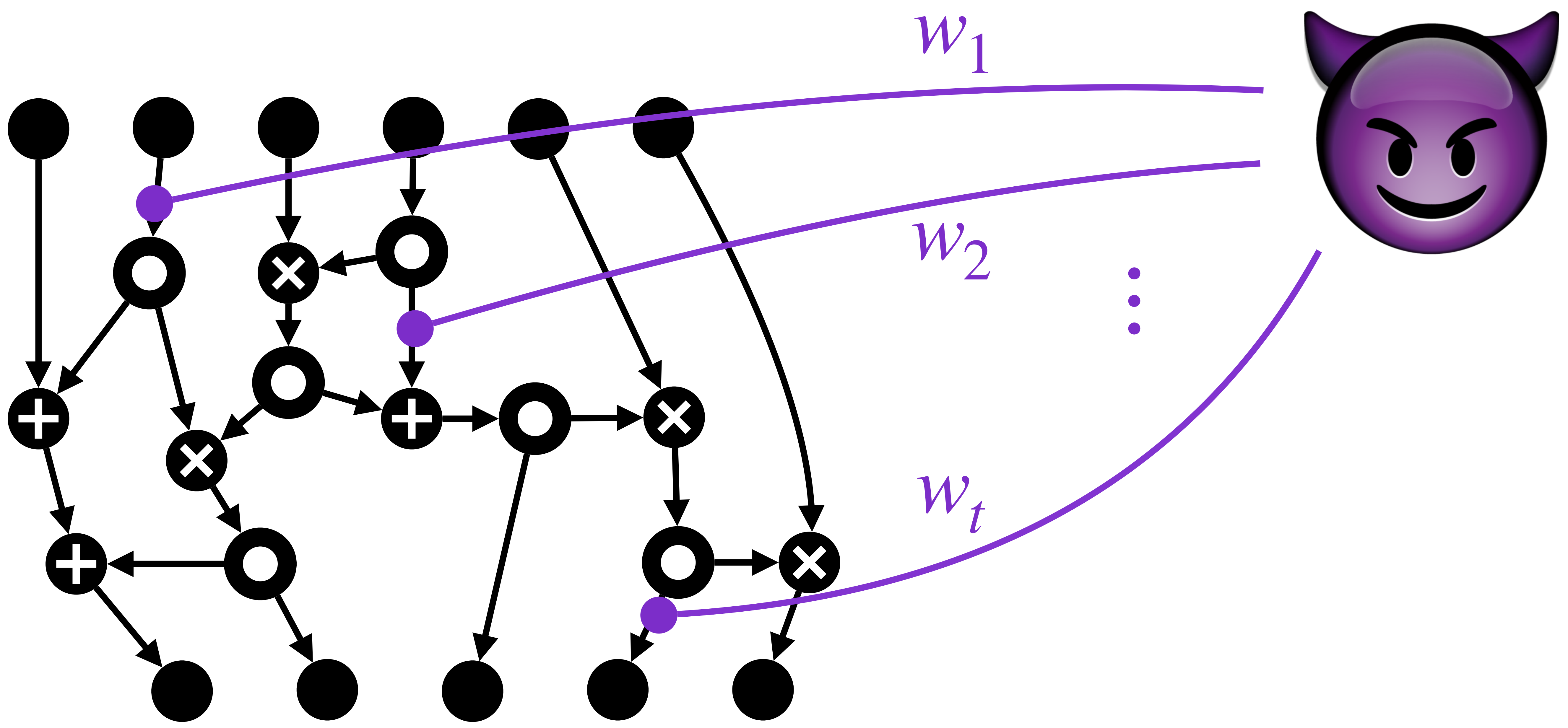
$\simeq$

t-order SCA security

The ISW scheme

Ishai, Sahai, Wagner - CRYPTO 2003

Probing model



t-probing security

$\simeq$

t-order SCA security

Masking an AND gate

$$\left(\sum_i a_i\right)\left(\sum_i b_i\right) = \sum_{i,j} a_i b_j$$

split into n shares

$$\begin{matrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{matrix} \quad + \begin{pmatrix} 0 & r_{1,2} & r_{1,3} \\ r_{1,2} & 0 & r_{2,3} \\ r_{1,3} & r_{2,3} & 0 \end{pmatrix}$$

add fresh randomness

Efficient application to block ciphers

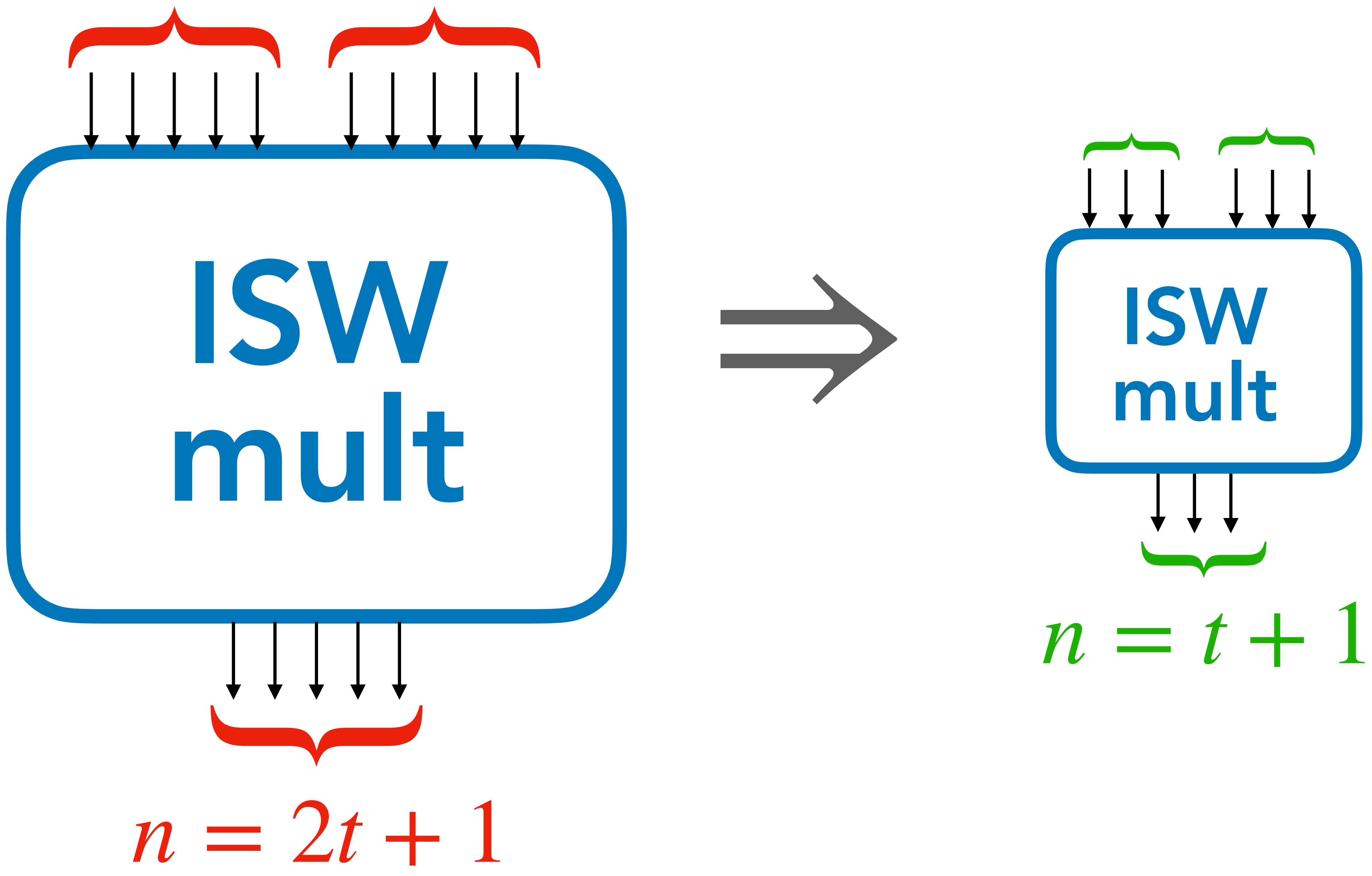
Rivain, Prouff - CHES 2010

Carlet, Goubin, Prouff, Quisquater, Rivain - FSE 2012

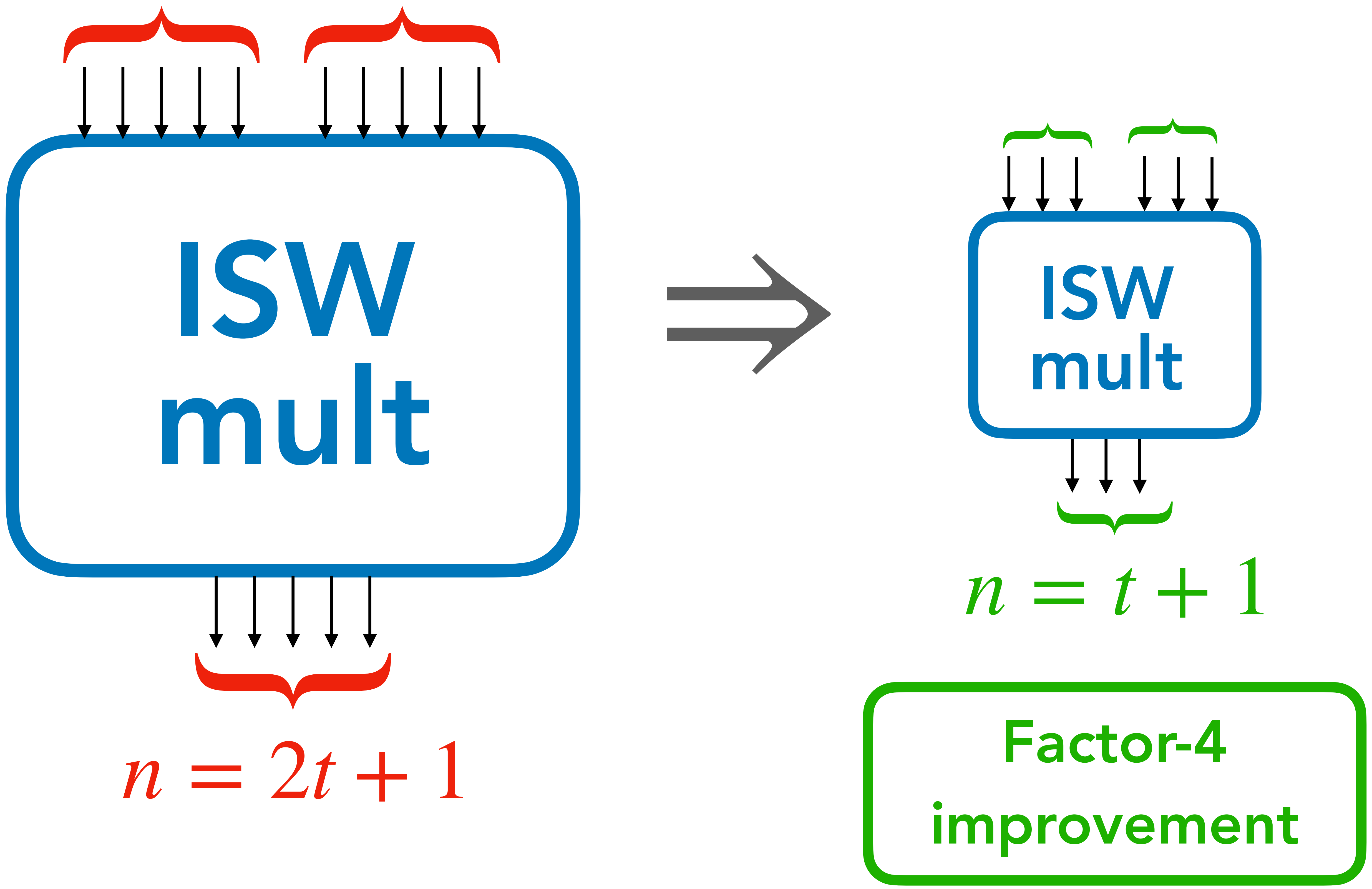
- Represent an m-bit s-box as an algebraic circuit on GF(2^m)
- Use ISW scheme for GF(2^m) multiplications
- Observation:
  - Linear operation $\Rightarrow \mathcal{O}(n)$ complexity
  - Multiplication $\Rightarrow \mathcal{O}(n^2)$ complexity
- S-box representations with the minimum number of multiplications

  $\Rightarrow$ optimal circuit for AES / efficient heuristics for general s-boxes

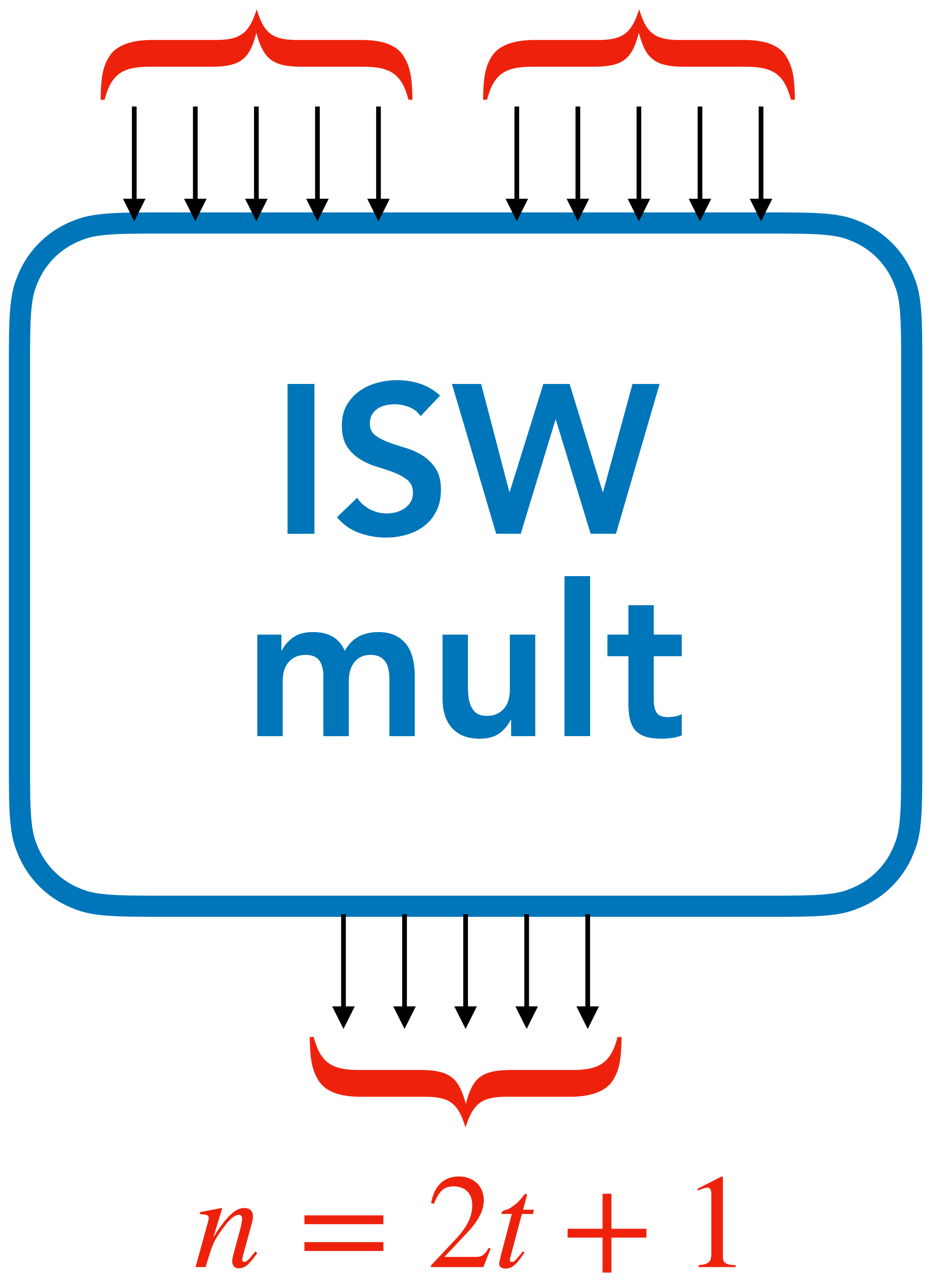
Tight probing security

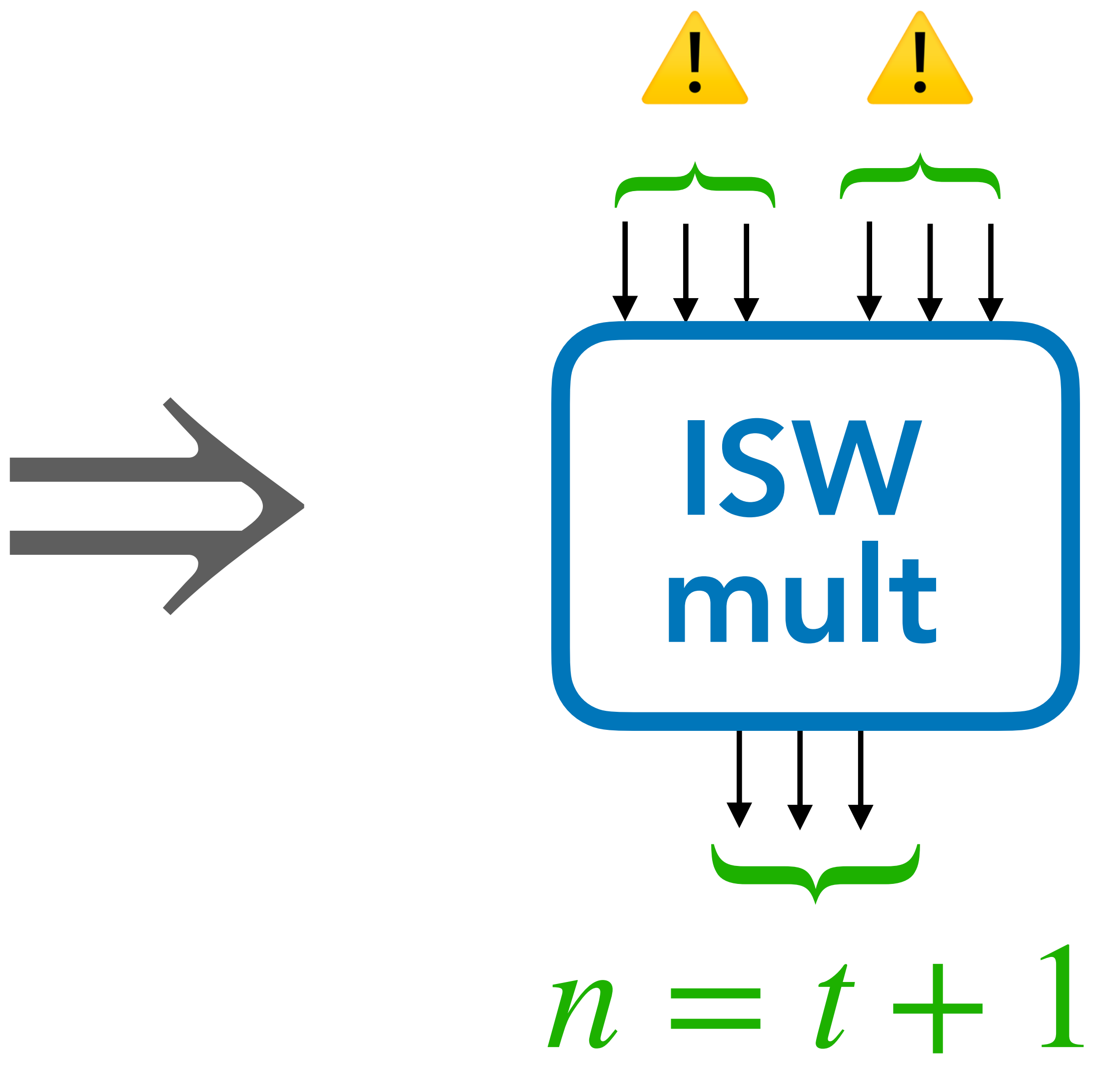


Tight probing security



Tight probing security

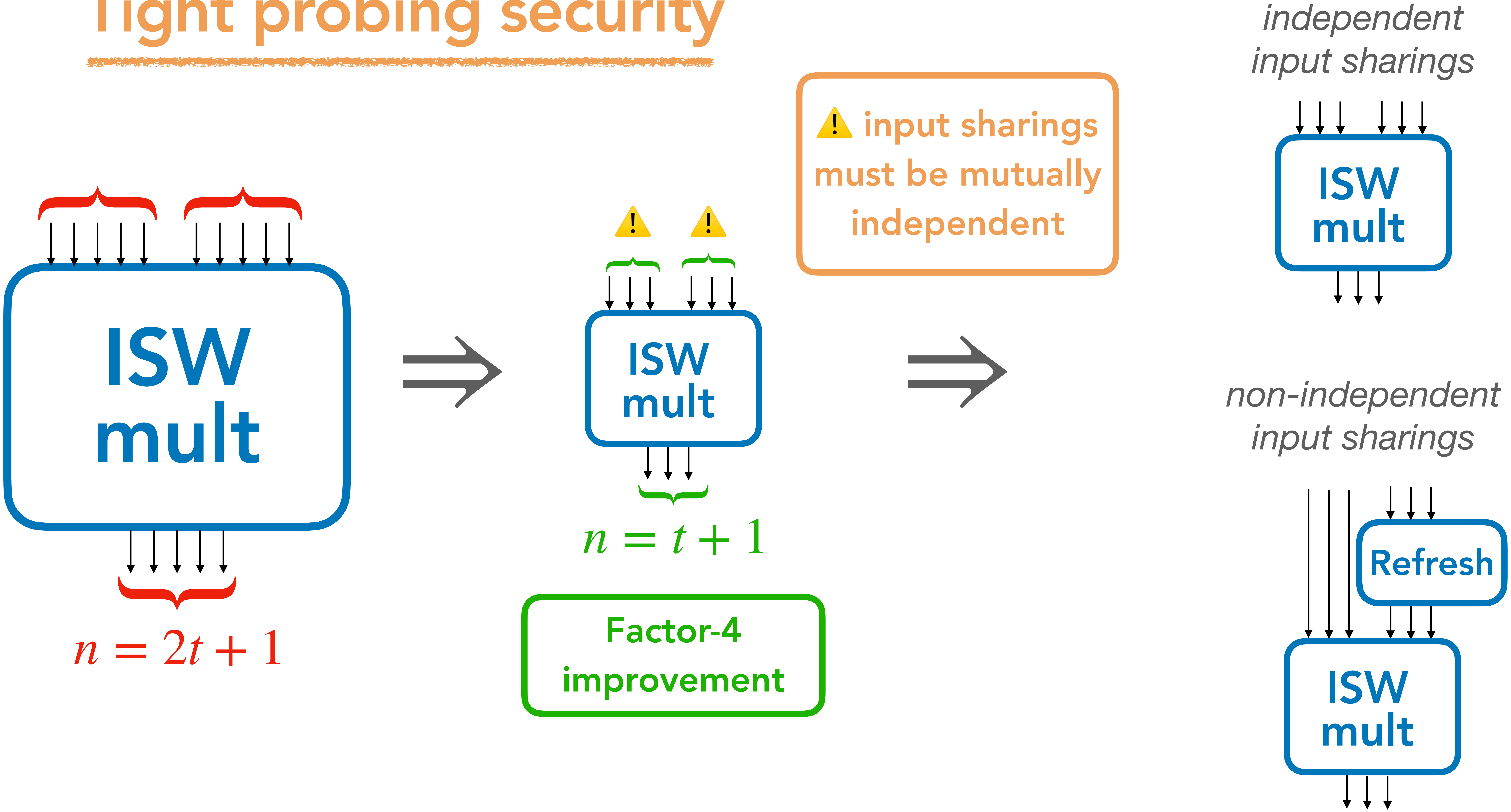




⚠️ input sharings must be mutually independent

Factor-4 improvement

Tight probing security



Many follow-up works

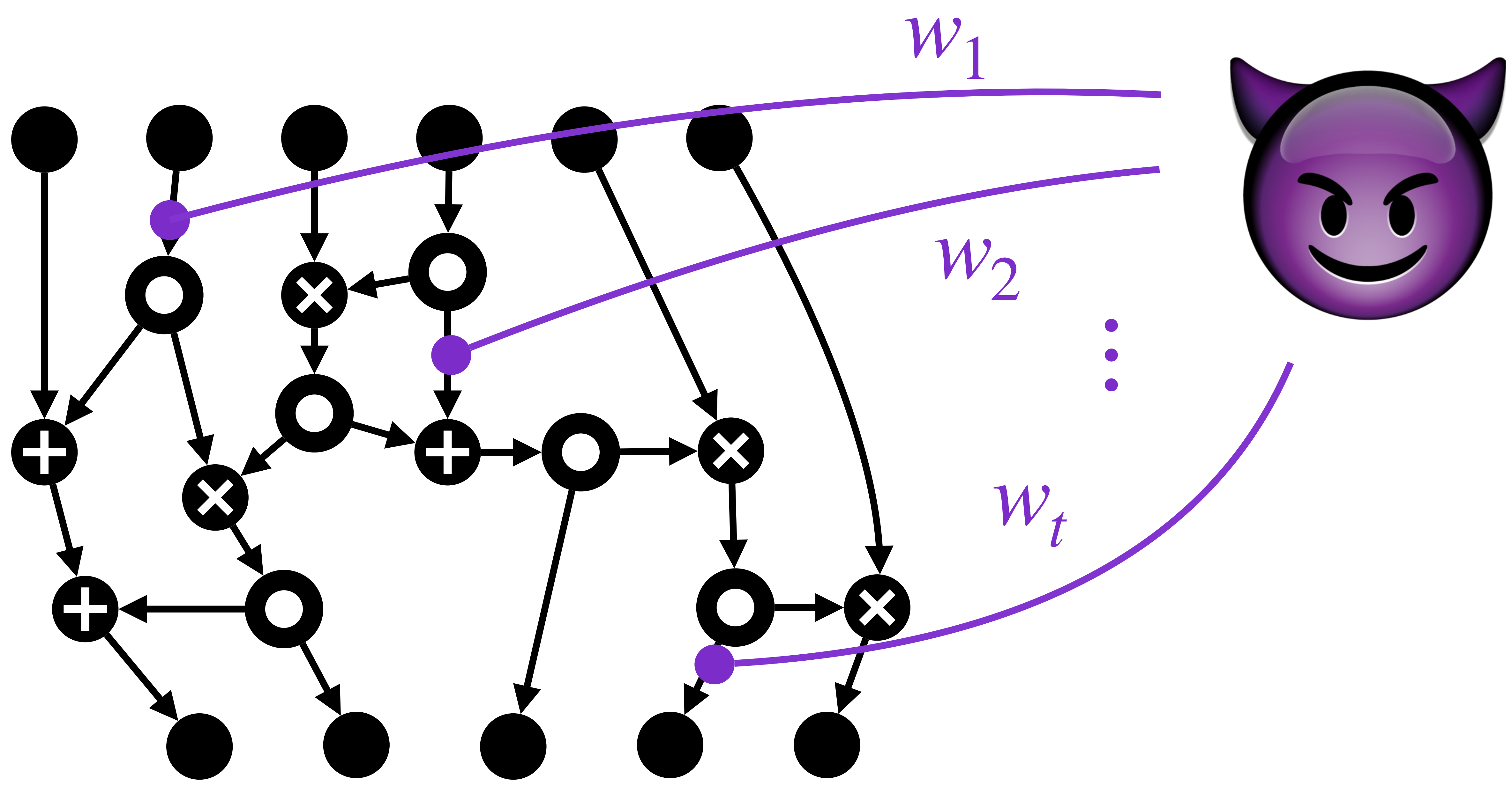
- Formal composition security notions
- Secure refresh gadgets
- Methods for placing refresh gadgets
- Efficient heuristics to minimise non-linear operations

Many follow-up works

- Formal composition security notions
- Secure refresh gadgets
- Methods for placing refresh gadgets
- Efficient heuristics to minimise non-linear operations

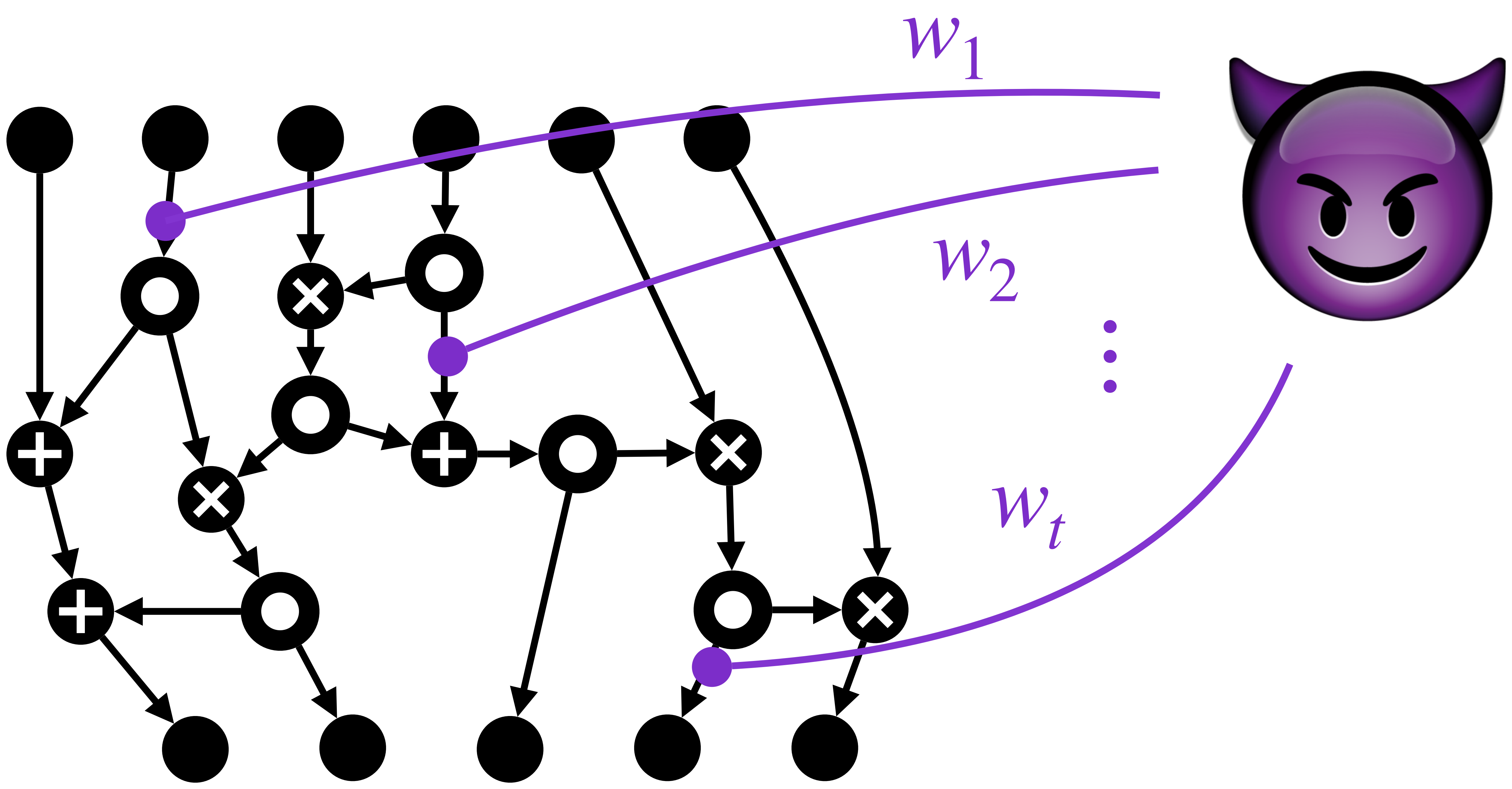
End of the story?

Limitation of probing security

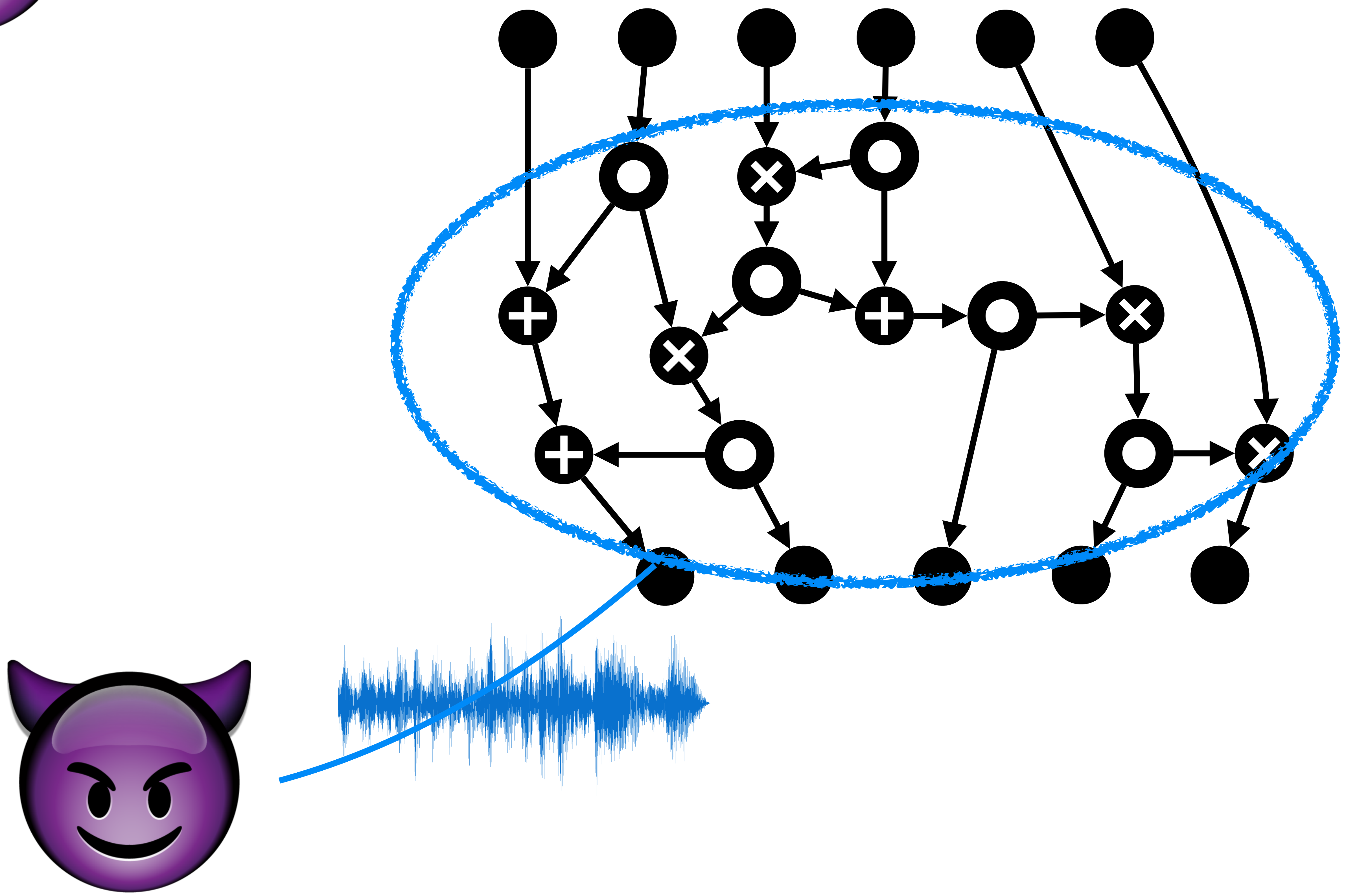


Why would 😈 limit to leakage on t variables ?!

Limitation of probing security



In practice, it's more like:



Why would 😈 limit to leakage on t variables ?!

3. Provable security vs. noisy leakage

The noisy leakage model

Micali, Reyzin - TCC 2004

Prouff, Rivain - EUROCRYPT 2013

"Only computation leaks" assumption

Noisy leakage functions

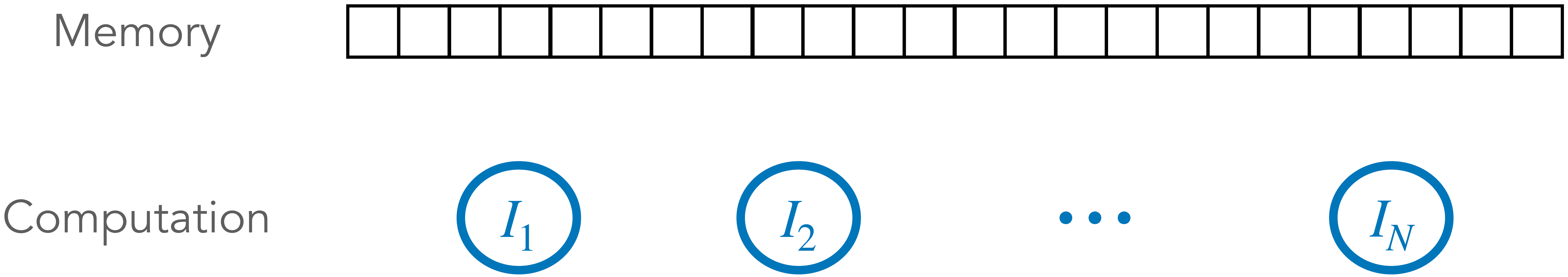
The noisy leakage model

Micali, Reyzin - TCC 2004

"Only computation leaks" assumption

Prouff, Rivain - EUROCRYPT 2013

Noisy leakage functions



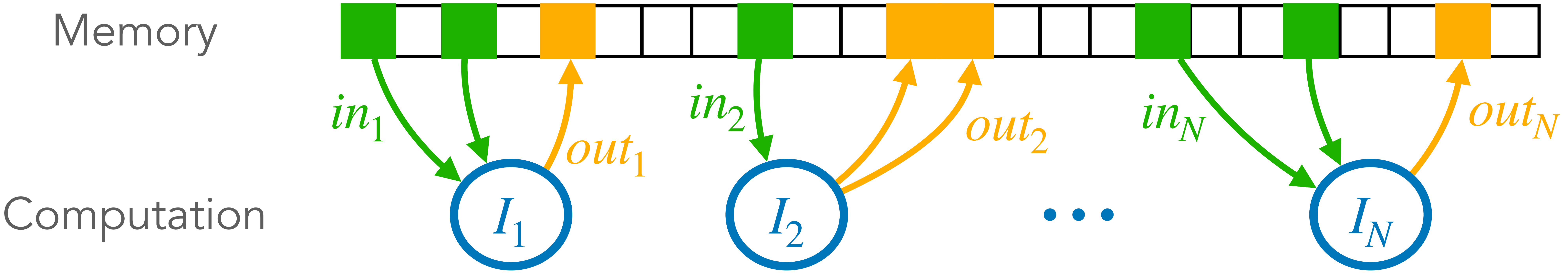
The noisy leakage model

Micali, Reyzin - TCC 2004

Prouff, Rivain - EUROCRYPT 2013

"Only computation leaks" assumption

Noisy leakage functions



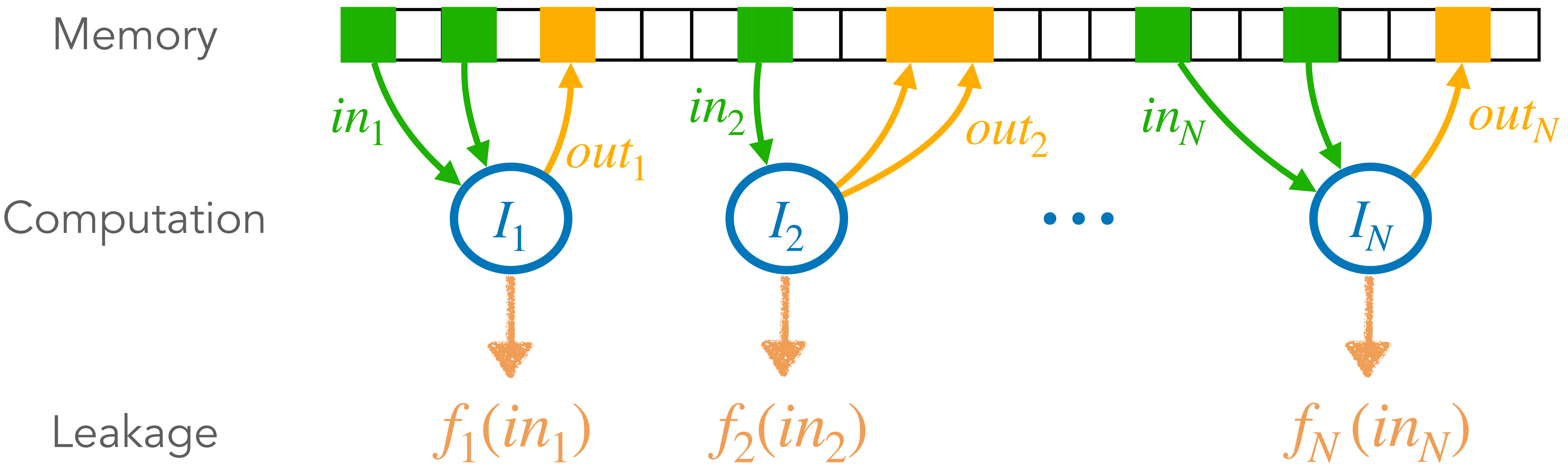
The noisy leakage model

Micali, Reyzin - TCC 2004

"Only computation leaks" assumption

Prouff, Rivain - EUROCRYPT 2013

Noisy leakage functions



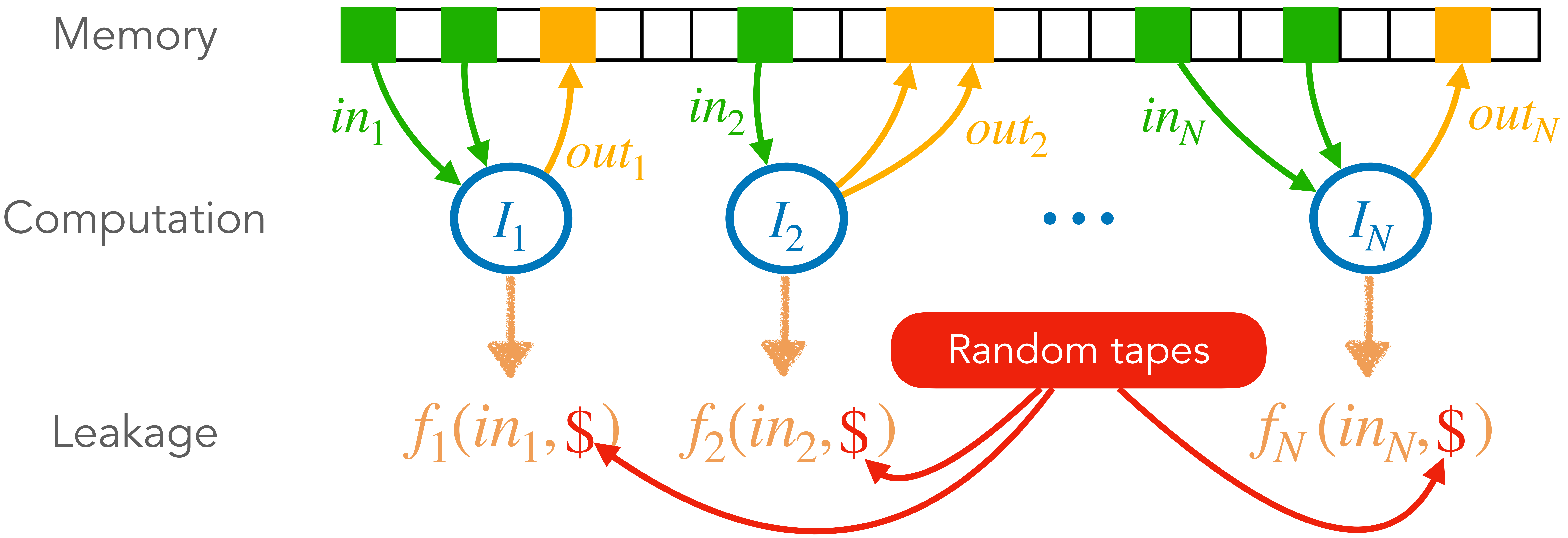
The noisy leakage model

Micali, Reyzin - TCC 2004

"Only computation leaks" assumption

Prouff, Rivain - EUROCRYPT 2013

Noisy leakage functions



Noisy leakage functions

A function is δ-**noisy** if (for $X \sim \mathcal{U}$):

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

Noisy leakage functions

A function is δ-**noisy** if (for $X \sim \mathcal{U}$):

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

statistical distance between X and X and given $f(X) = y$

Noisy leakage functions

A function is δ-**noisy** if (for $X \sim \mathcal{U}$):

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

expectation on the possible leakage values

statistical distance between X and X and given $f(X) = y$

Noisy leakage functions

more noise

$\Rightarrow$ smaller δ

A function is **δ-noisy** if (for $X \sim \mathcal{U}$):

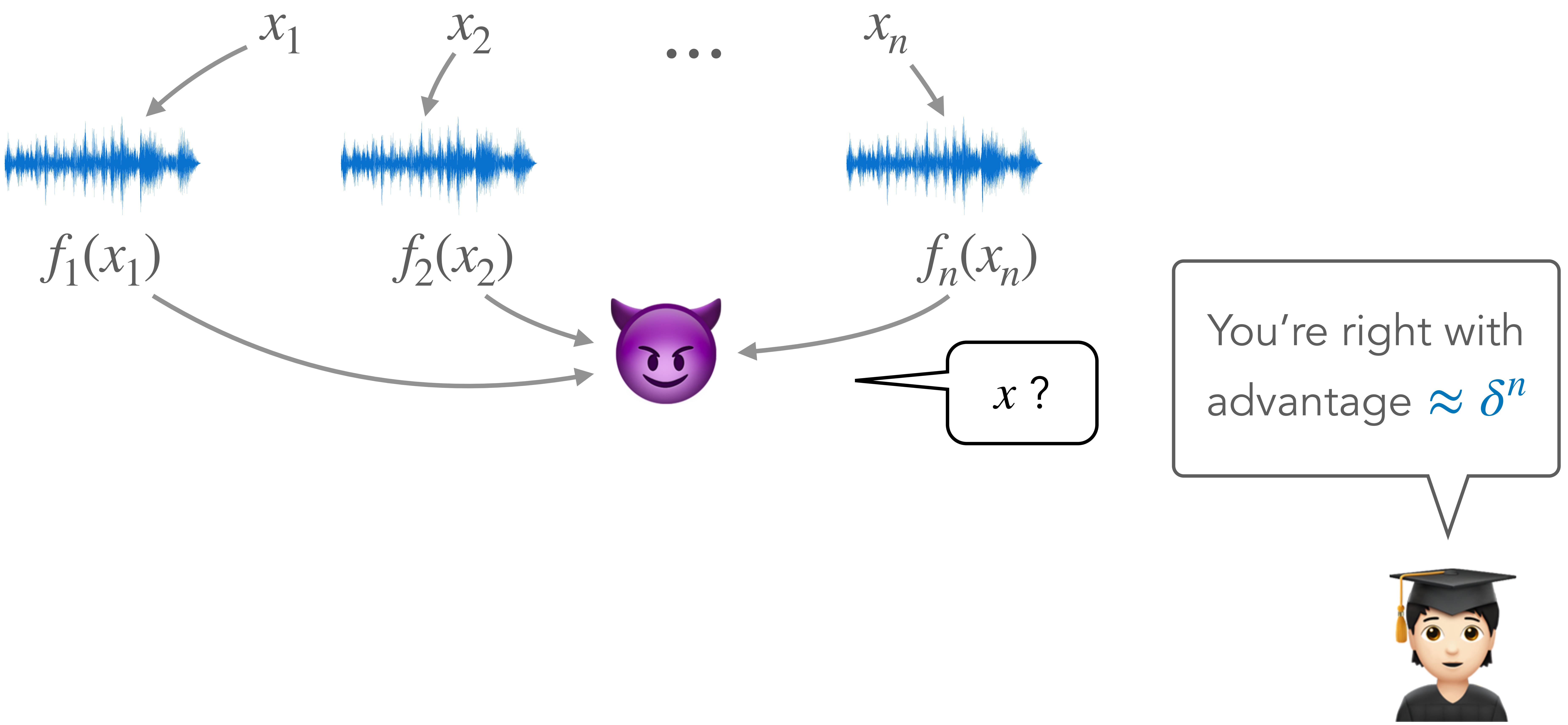
$$\mathbb{E}_y\left[\Delta\big(X;\ (X \mid f(X) = y)\big)\right] \leq \delta$$

expectation on the possible leakage values

statistical distance between X and X and given $f(X) = y$

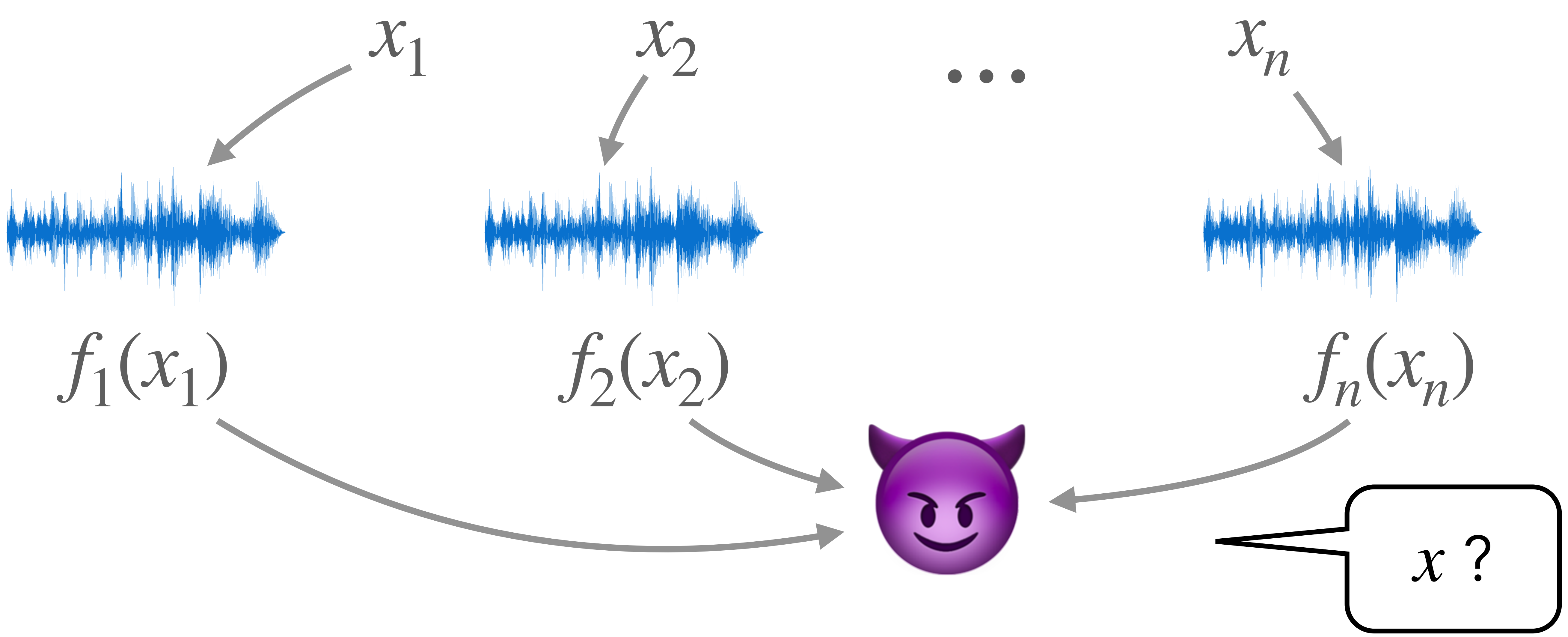
Masking security in the noisy leakage model

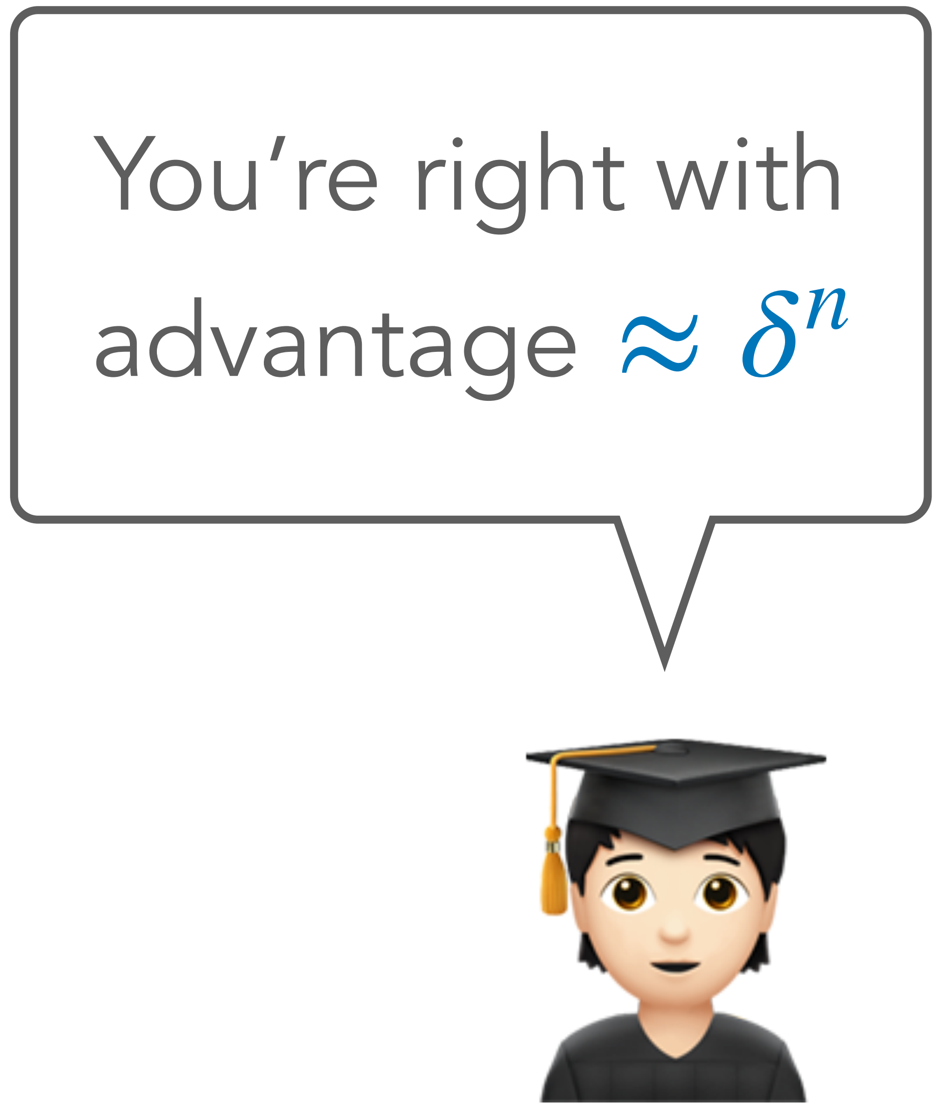
- Generalised soundness of masking



Masking security in the noisy leakage model

- Generalised soundness of masking



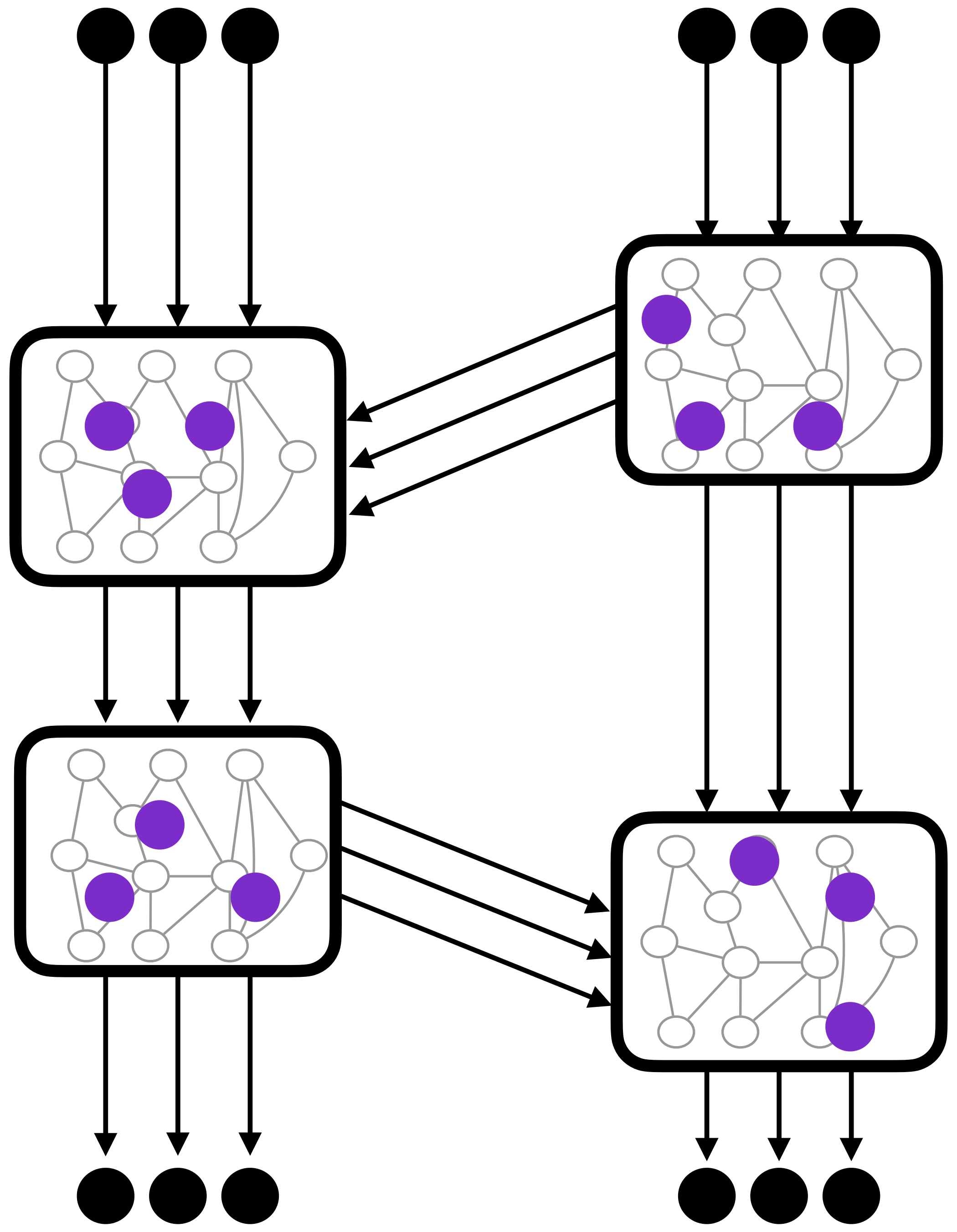


- Formal proof for masked block cipher
  - leak-free refresh gadget ⚠️

The DDF reduction

Duc, Dziembowski, Faust - EUROCRYPT 2014

Region probing model



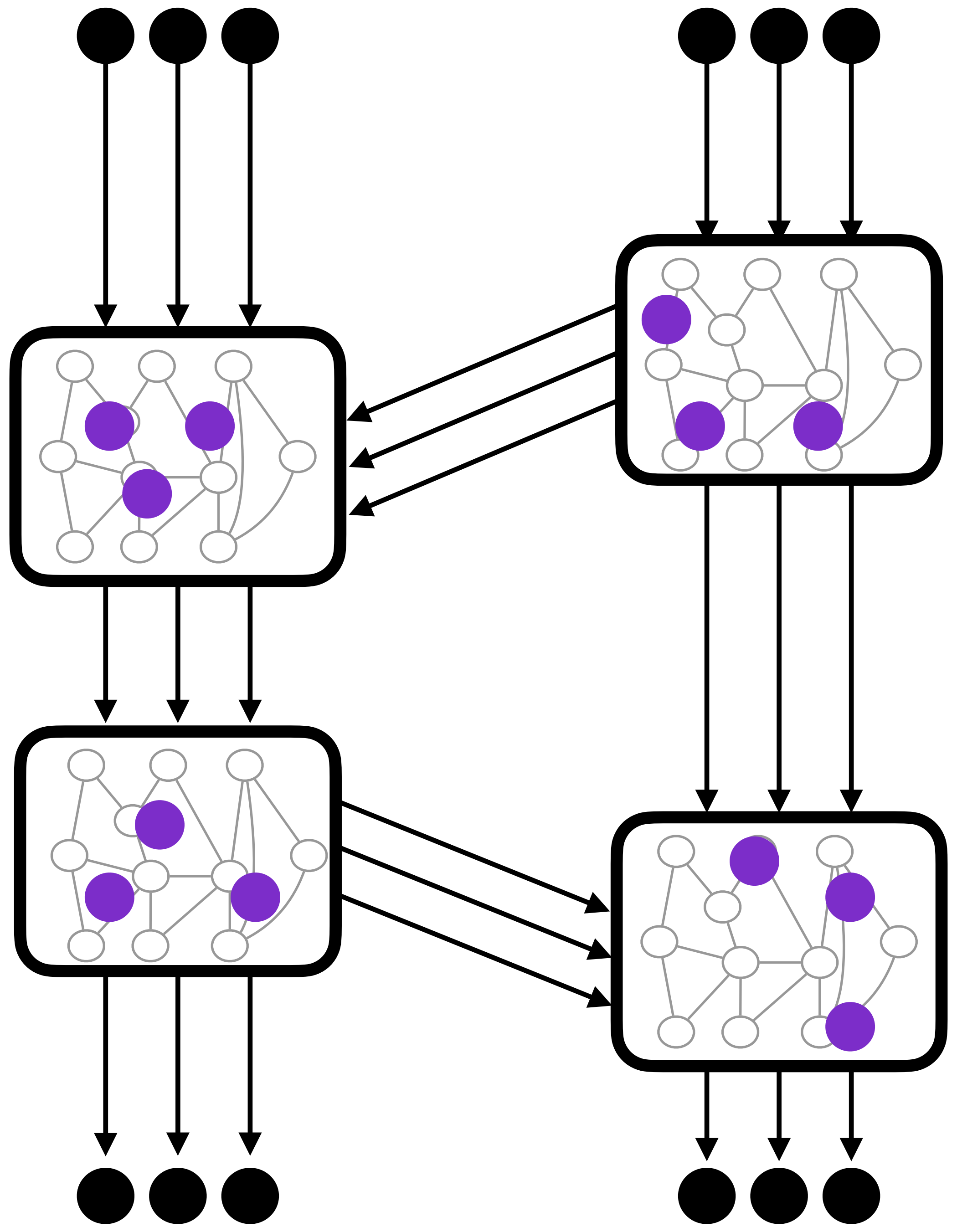
gets t probes per *region*

with $t = r \cdot |C_i|$

The DDF reduction

Duc, Dziembowski, Faust - EUROCRYPT 2014

Region probing model



probing rate

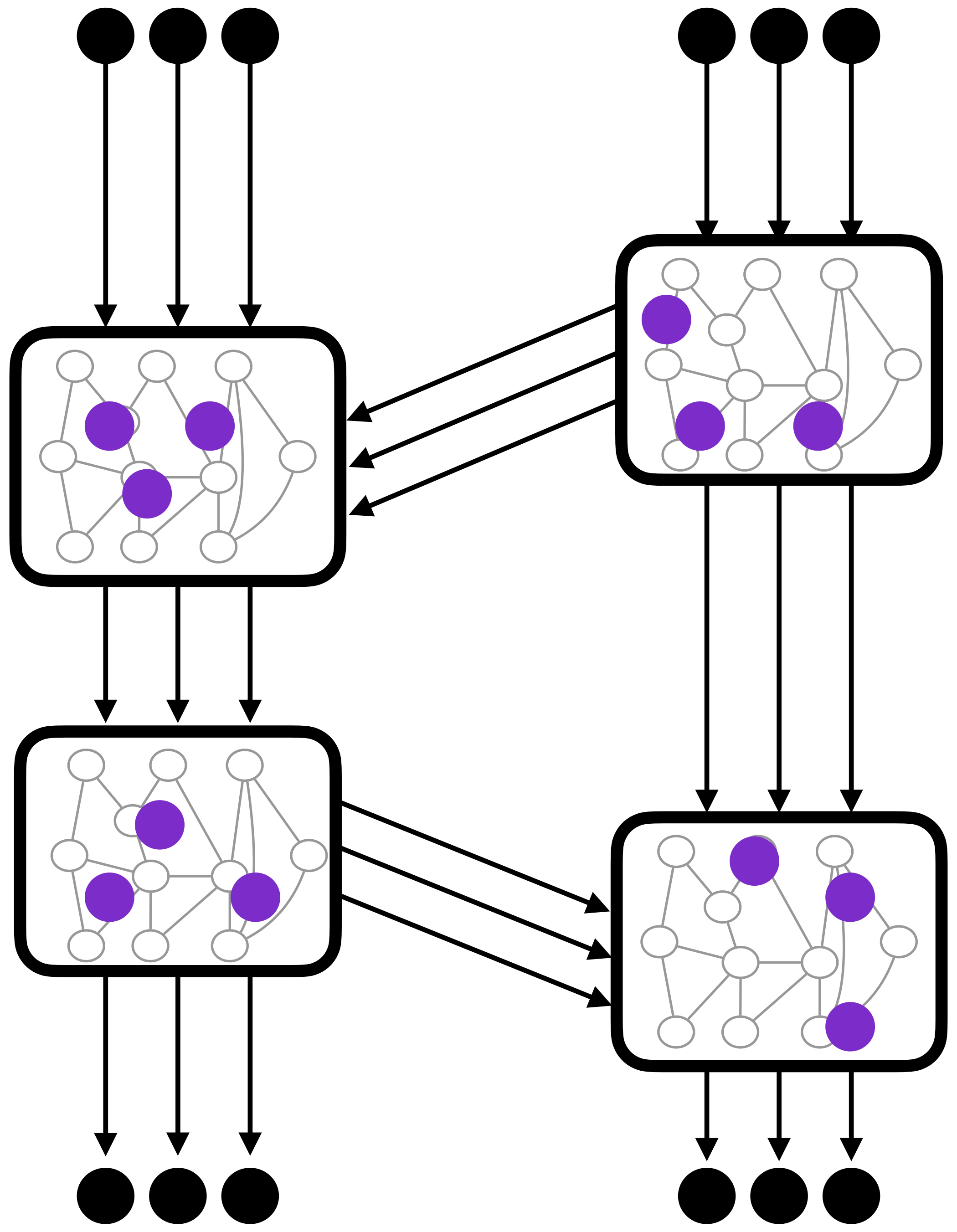
gets t probes per *region*

with $t = r\ |C_i|$

The DDF reduction

Duc, Dziembowski, Faust - EUROCRYPT 2014

Region probing model



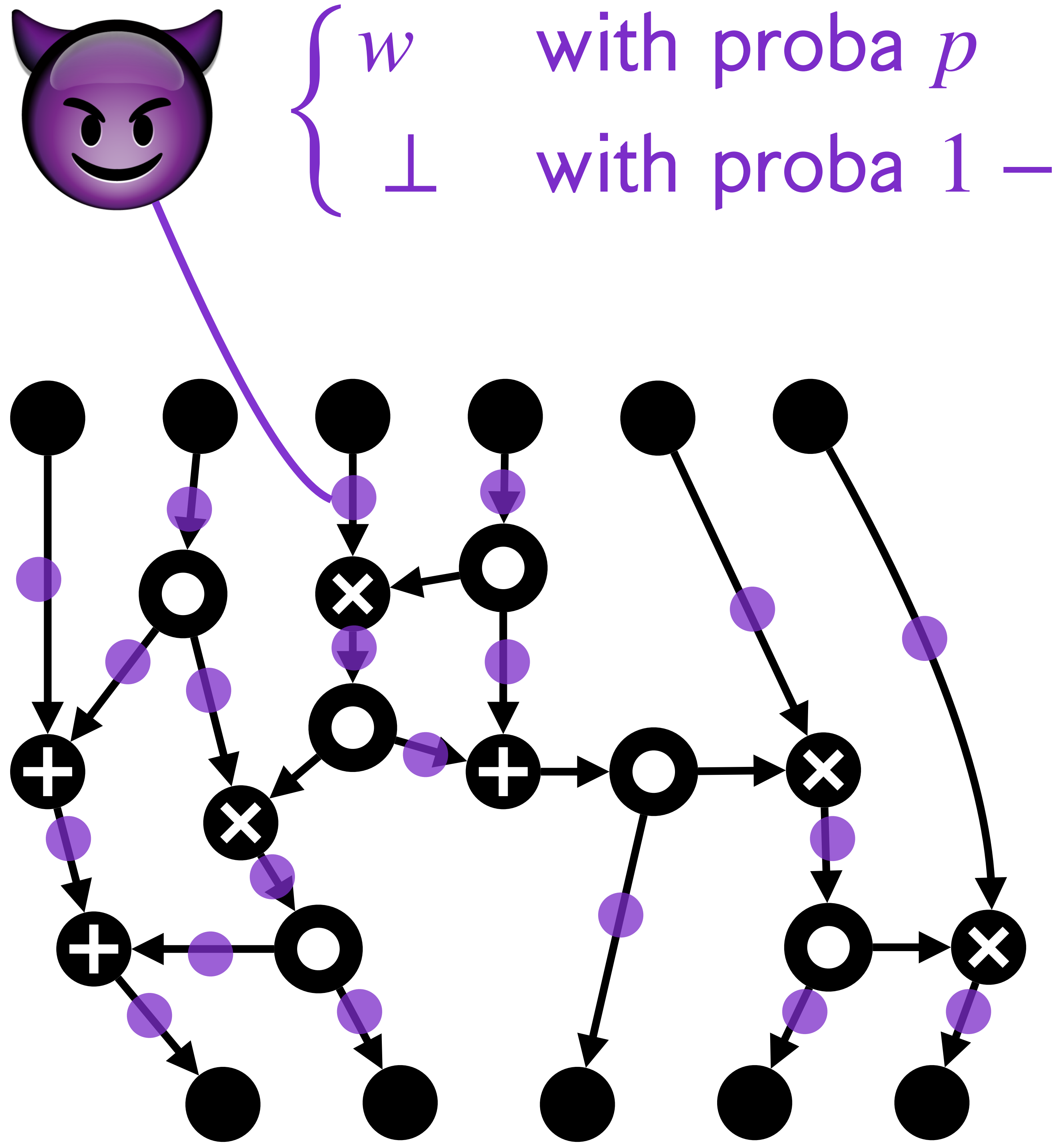
probing rate

gets t probes per *region*

with $t = r \cdot |C_i|$

Random probing model

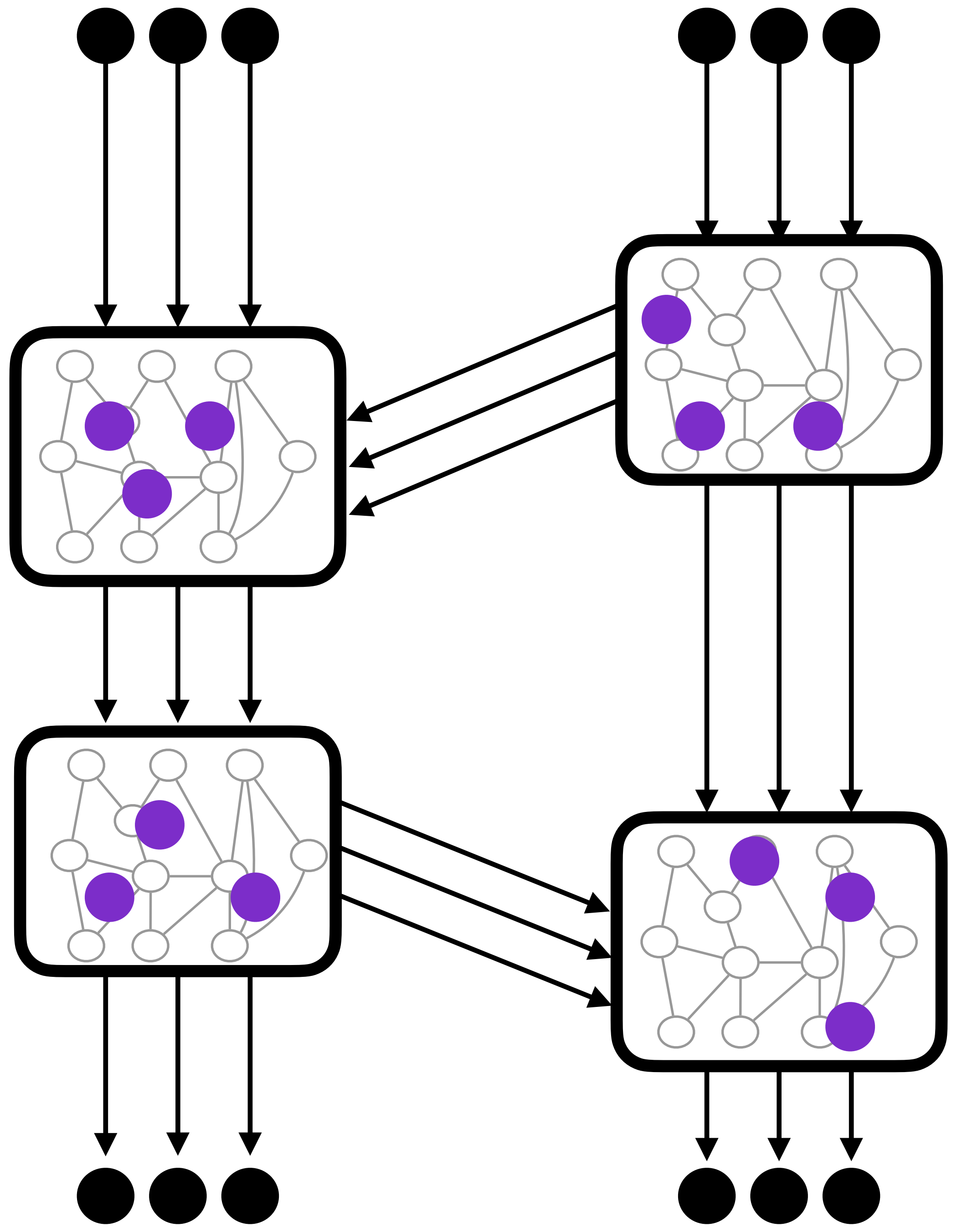
$\begin{cases} w & \text{with proba } p \\ \perp & \text{with proba } 1-p \end{cases}$



The DDF reduction

Duc, Dziembowski, Faust - EUROCRYPT 2014

Region probing model



probing rate

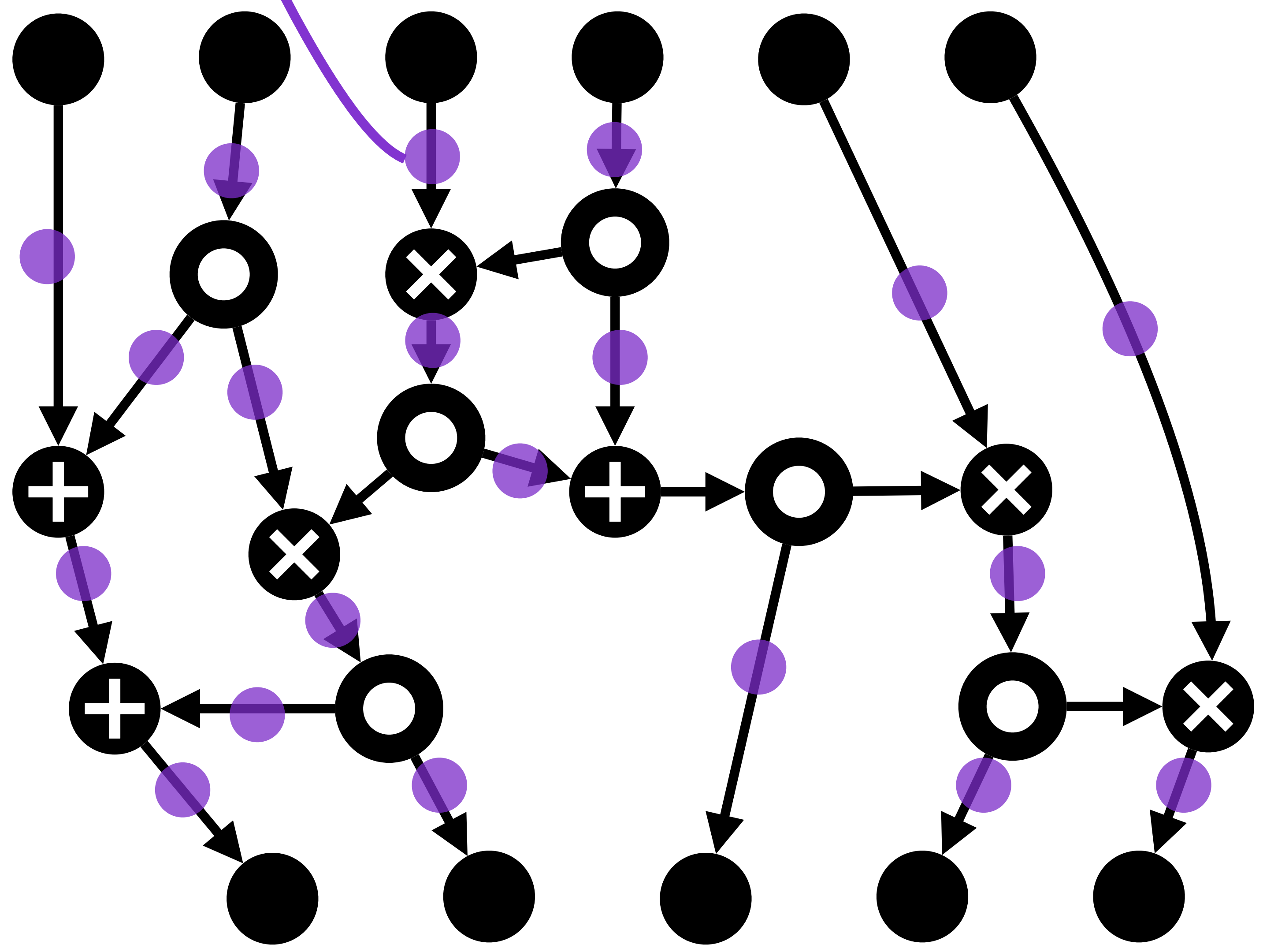
gets t probes per *region*

with $t = r \, |C_i|$

Random probing model

$\begin{cases} w & \text{with proba } p \\ \perp & \text{with proba } 1-p \end{cases}$

leakage probability



The DDF reduction

Duc, Dziembowski, Faust - EUROCRYPT 2014

DDF reduction:

r-region probing security

$\Rightarrow$

p-random probing security

with $p = \Theta(r)$

$\Rightarrow$

δ-noisy leakage security

with $\delta = \Theta(p)$

The DDF reduction

Duc, Dziembowski, Faust - EUROCRYPT 2014

DDF reduction:

r-region probing security

$\Rightarrow$

p-random probing security

with $p = \Theta(r)$

$\Rightarrow$

δ-noisy leakage security

with $\delta = \Theta(p)$

Chernoff bound

The DDF reduction

Duc, Dziembowski, Faust - EUROCRYPT 2014

DDF reduction:

r-region probing security

$\Rightarrow$

p-random probing security with $p = \Theta(r)$

$\Rightarrow$

δ-noisy leakage security with $\delta = \Theta(p)$

Chernoff bound

Key lemma of DDF

The DDF reduction

Duc, Dziembowski, Faust - EUROCRYPT 2014

DDF reduction:

r-region probing security

$\Rightarrow$

p-random probing security
with $p = \Theta(r)$

$\Rightarrow$

δ-noisy leakage security
with $\delta = \Theta(p)$

Chernoff bound

Key lemma of DDF

leakage rate

State of the art

- State-of-the-art noisy-leakage-secure schemes
  - most schemes with **at least $\mathcal{O}(n^2)$ complexity**
  - a few schemes with $\mathcal{O}(1)$ leakage rate, but **constant not explicit**

State of the art

- State-of-the-art noisy-leakage-secure schemes
  - most schemes with **at least $\mathcal{O}(n^2)$ complexity**
  - a few schemes with $\mathcal{O}(1)$ leakage rate, but **constant not explicit**
- In what follows
  - region probing security in **quasilinear complexity**
  - random probing security with **explicit constant leakage rate**

4. Security in quasilinear complexity

Quasilinear masking

Goudarzi, Joux, Rivain - ASIACRYPT 2018

Goudarzi, Prest, Rivain, Vergnaud - TCHES 2021

A $\vec{v}$-sharing of x

$$\vec{x} = (x_0, x_1, \ldots, x_{n-1}) \quad \text{s.t.} \quad \langle \vec{v}, \vec{x} \rangle = x$$

Quasilinear masking

Goudarzi, Joux, Rivain - ASIACRYPT 2018

Goudarzi, Prest, Rivain, Vergnaud - TCHES 2021

A $\overrightarrow{v}$-sharing of x

$$\overrightarrow{x} = (x_0, x_1, \ldots, x_{n-1}) \quad \text{s.t.} \quad \langle \overrightarrow{v}, \overrightarrow{x} \rangle = x$$

$$\overrightarrow{v} = (1, \omega, \omega^2, \ldots, \omega^{n-1}) \quad \text{for} \quad \omega \xleftarrow{\$} \mathbb{F}$$

Quasilinear masking

Goudarzi, Joux, Rivain - ASIACRYPT 2018

Goudarzi, Prest, Rivain, Vergnaud - TCHES 2021

Polynomial $P_{\vec{x}}(\omega)$

(shares = coefficients)

A $\vec{v}$-sharing of x

$$\vec{x} = (x_0, x_1, \ldots, x_{n-1}) \quad \text{s.t.} \quad \langle \vec{v}, \vec{x} \rangle = x = \sum_{i=0}^{n-1} x_i \cdot \omega^i$$

$$\vec{v} = (1, \omega, \omega^2, \ldots, \omega^{n-1}) \quad \text{for} \quad \omega \xleftarrow{\$} \mathbb{F}$$

Efficient multiplication

- Let $\vec{t}$ such that

$$P_{\vec{t}} = P_{\vec{x}} \cdot P_{\vec{y}}$$

- We get

$$P_{\vec{t}}(\omega) = \sum_{i=0}^{2n-1} t_i \omega^i = x \cdot y$$

Efficient multiplication

- Let $\vec{t}$ such that

$$P_{\vec{t}} = P_{\vec{x}} \cdot P_{\vec{y}}$$

- We get

$$P_{\vec{t}}(\omega) = \sum_{i=0}^{2n-1} t_i \omega^i = x \cdot y$$

Efficient multiplication

- Let $\vec{t}$ such that

$$P_{\vec{t}} = P_{\vec{x}} \cdot P_{\vec{y}}$$

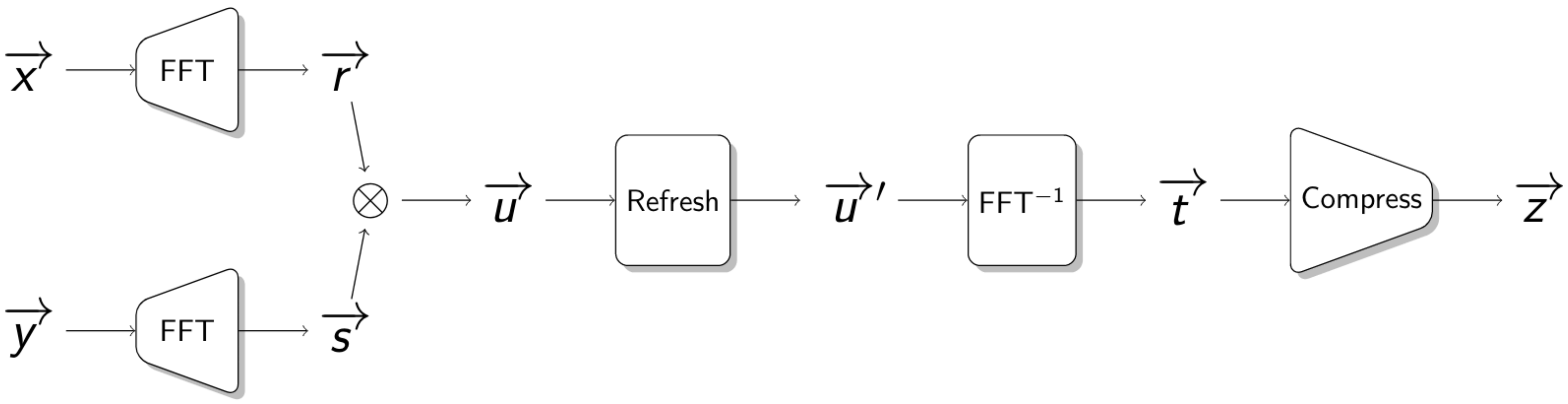
- We get

$$P_{\vec{t}}(\omega) = \sum_{i=0}^{2n-1} t_i \omega^i = x \cdot y$$

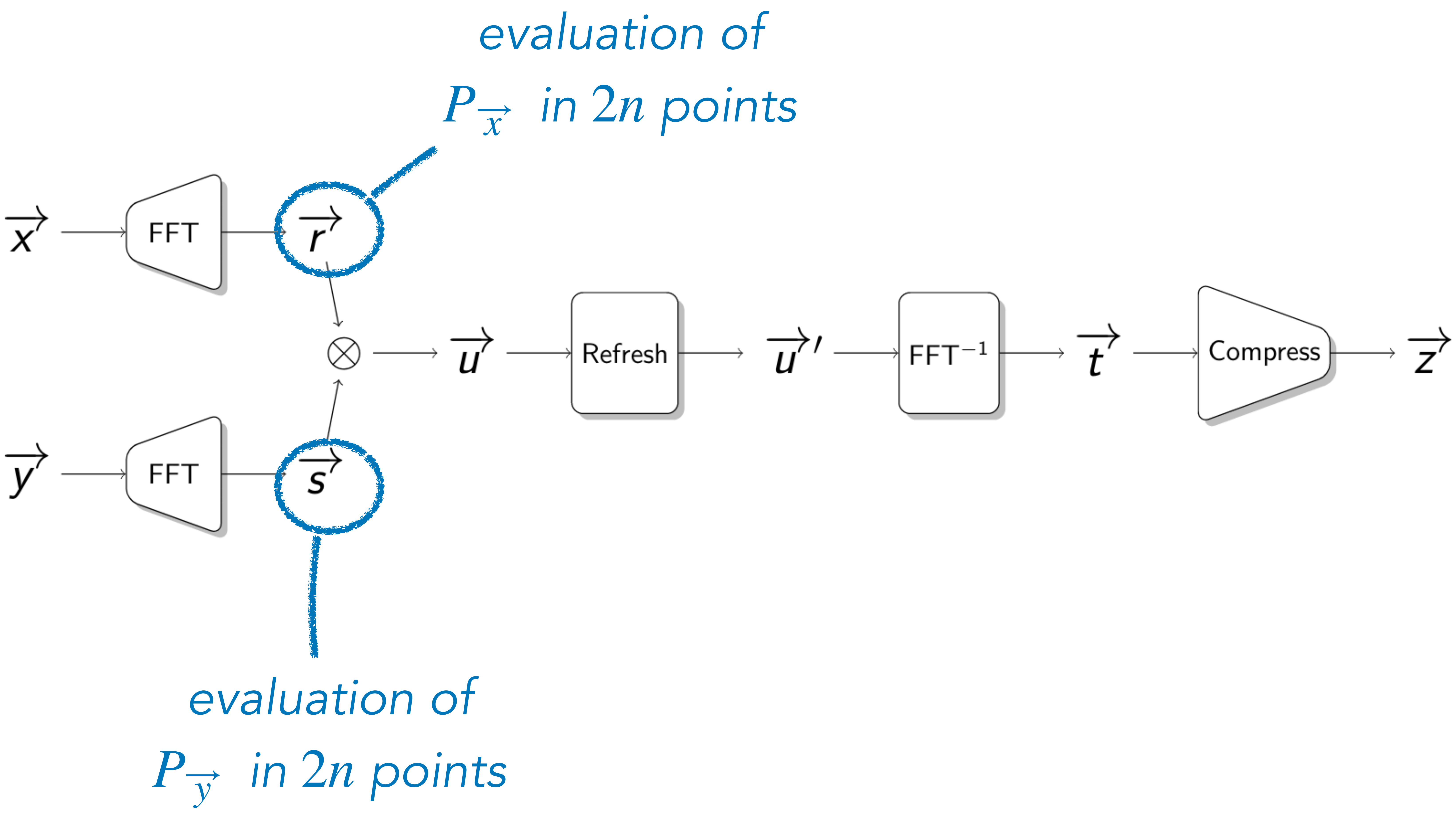
- Compression:

$$\vec{z} = (t_0, \ldots, t_{n-1}) + \omega^n \cdot (t_n, \ldots, t_{2n-1})$$

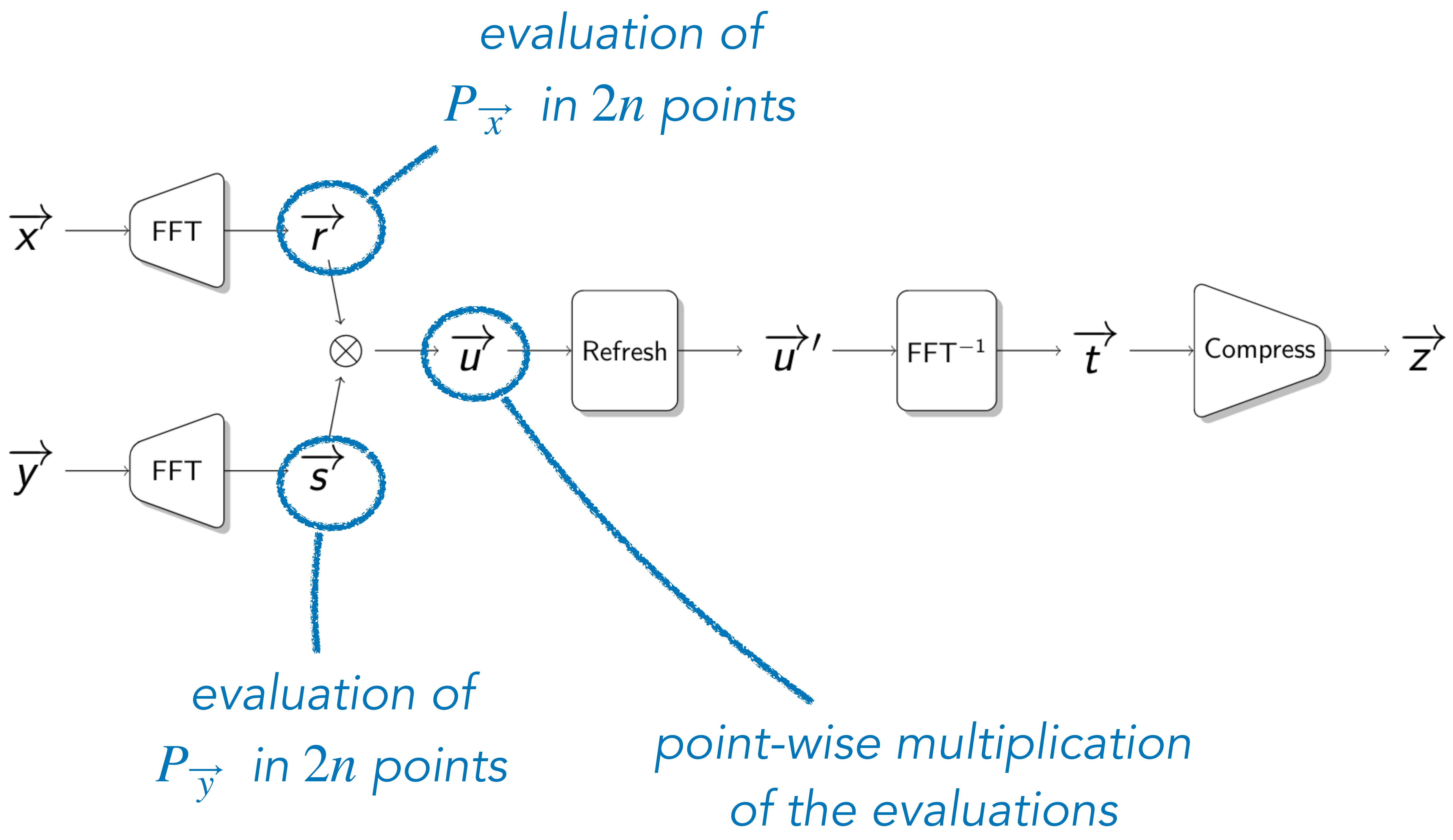
Multiplication gadget



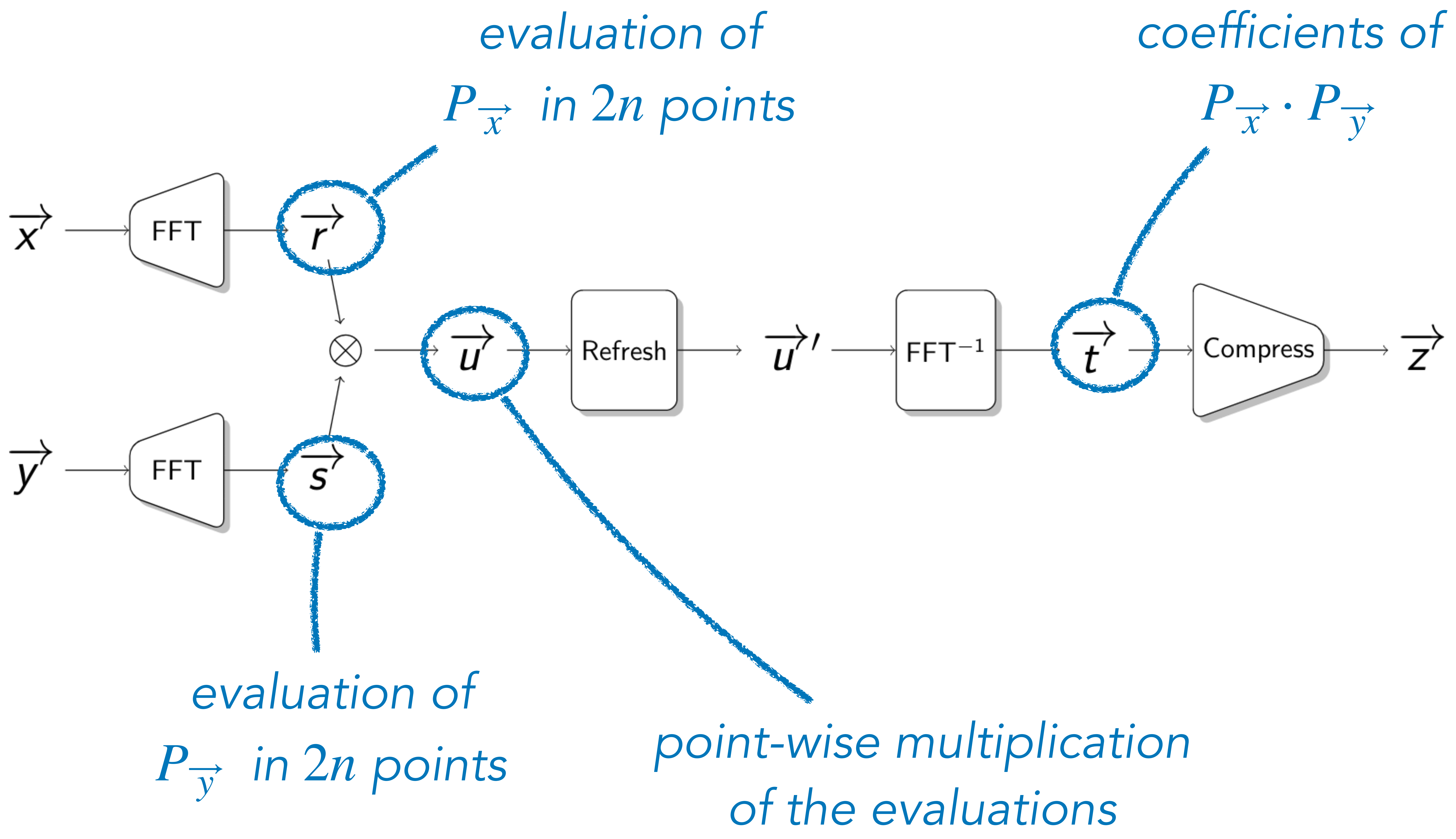
Multiplication gadget



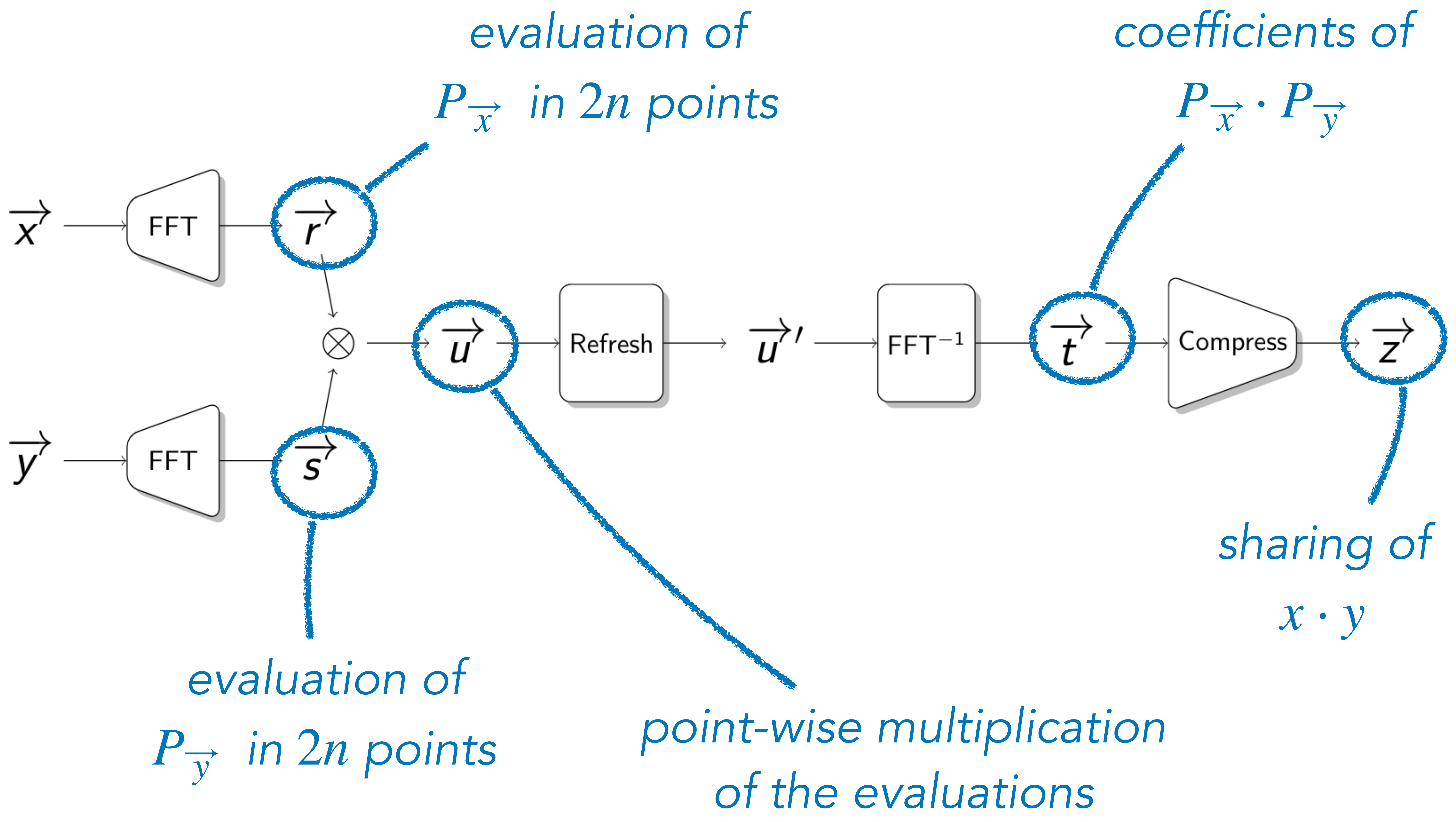
Multiplication gadget



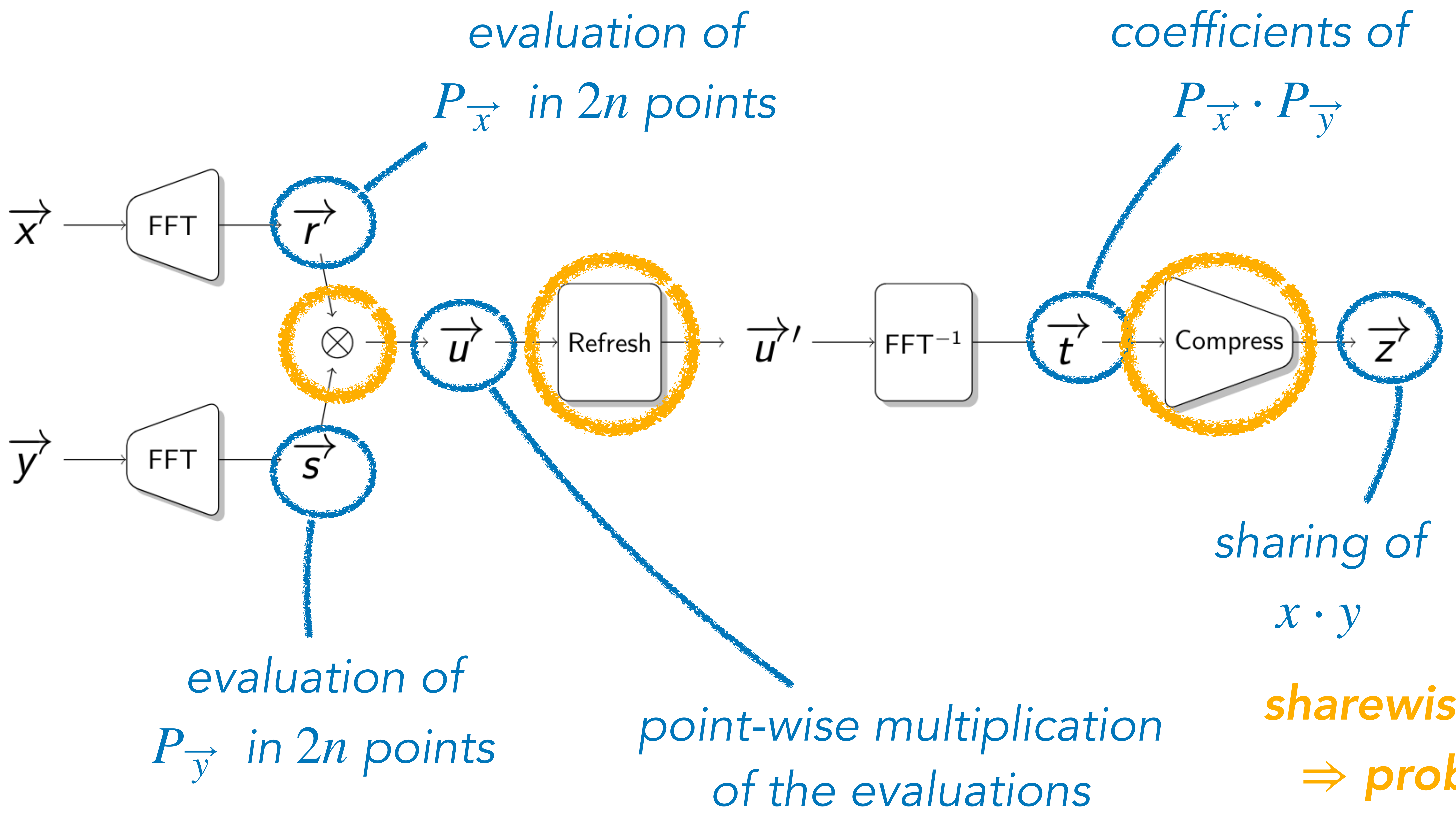
Multiplication gadget



Multiplication gadget



Multiplication gadget



sharewise operations
$\Rightarrow$ probing secure

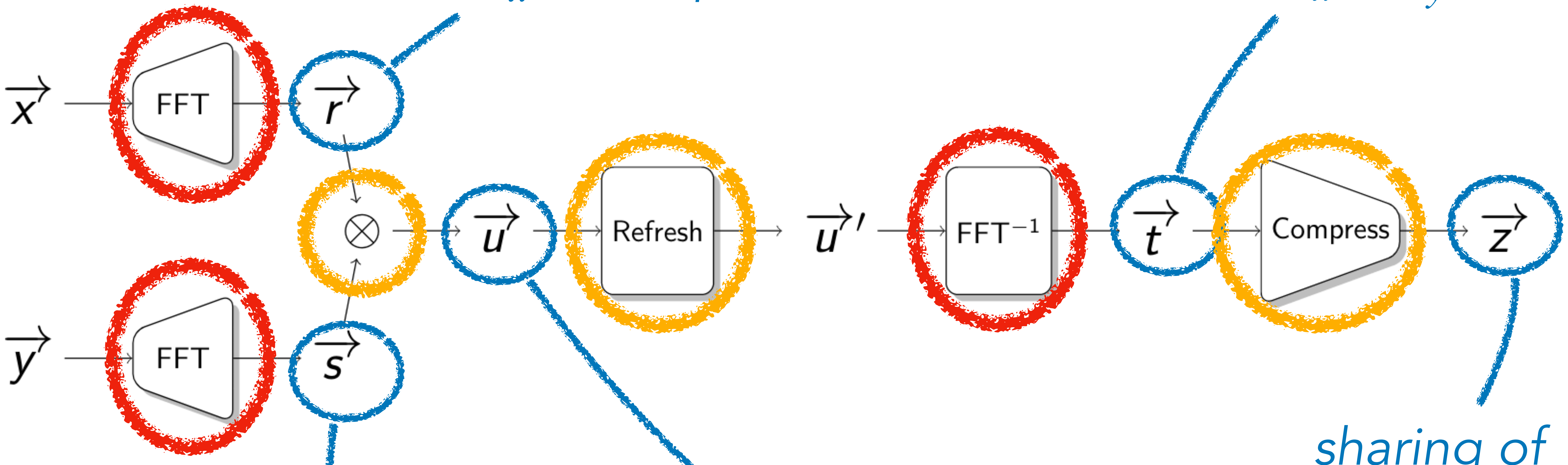
Multiplication gadget

evaluation of

$P_{\vec{x}}$ in $2n$ points

coefficients of

$P_{\vec{x}} \cdot P_{\vec{y}}$



sharing of

$x \cdot y$

what about the FFT?

evaluation of

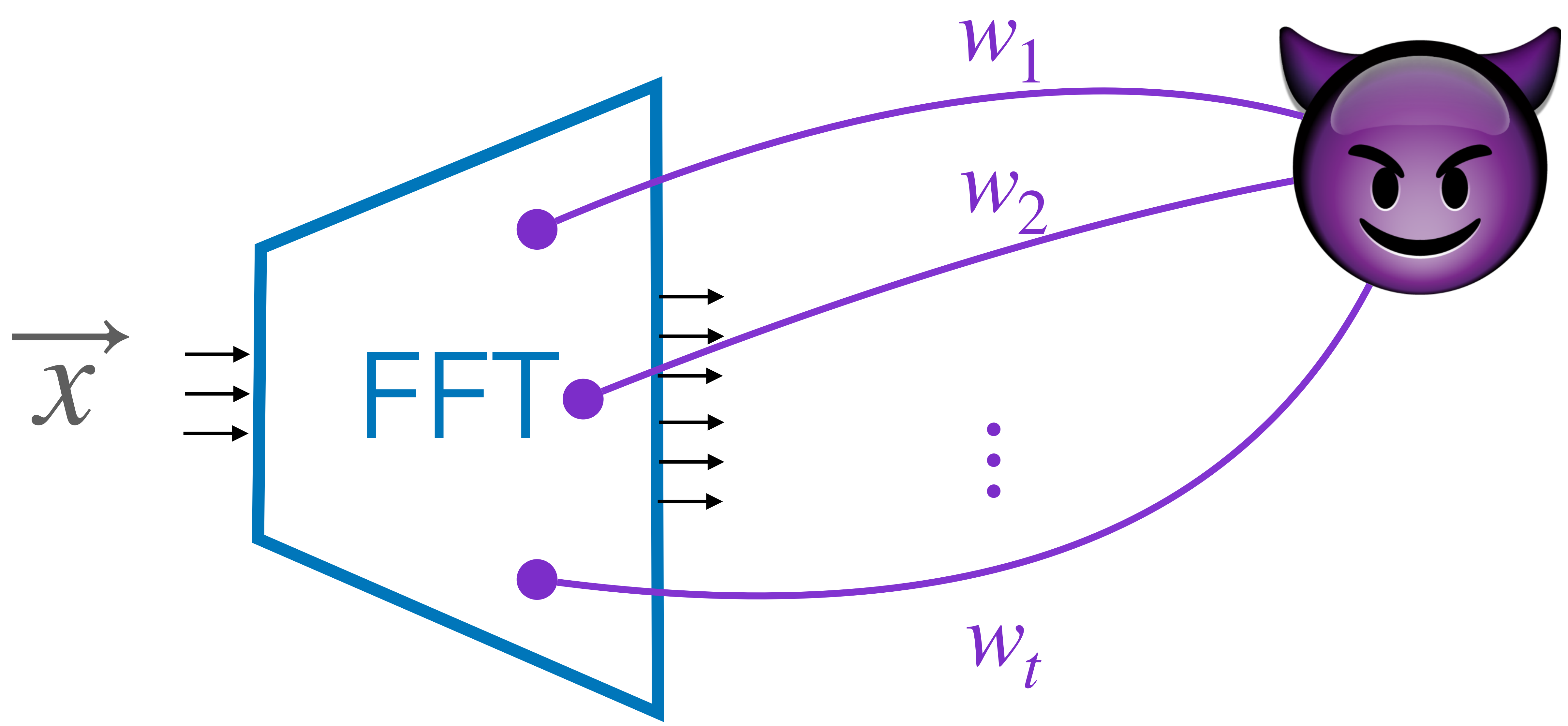
$P_{\vec{y}}$ in $2n$ points

point-wise multiplication of the evaluations

sharewise operations

$\Rightarrow$ probing secure

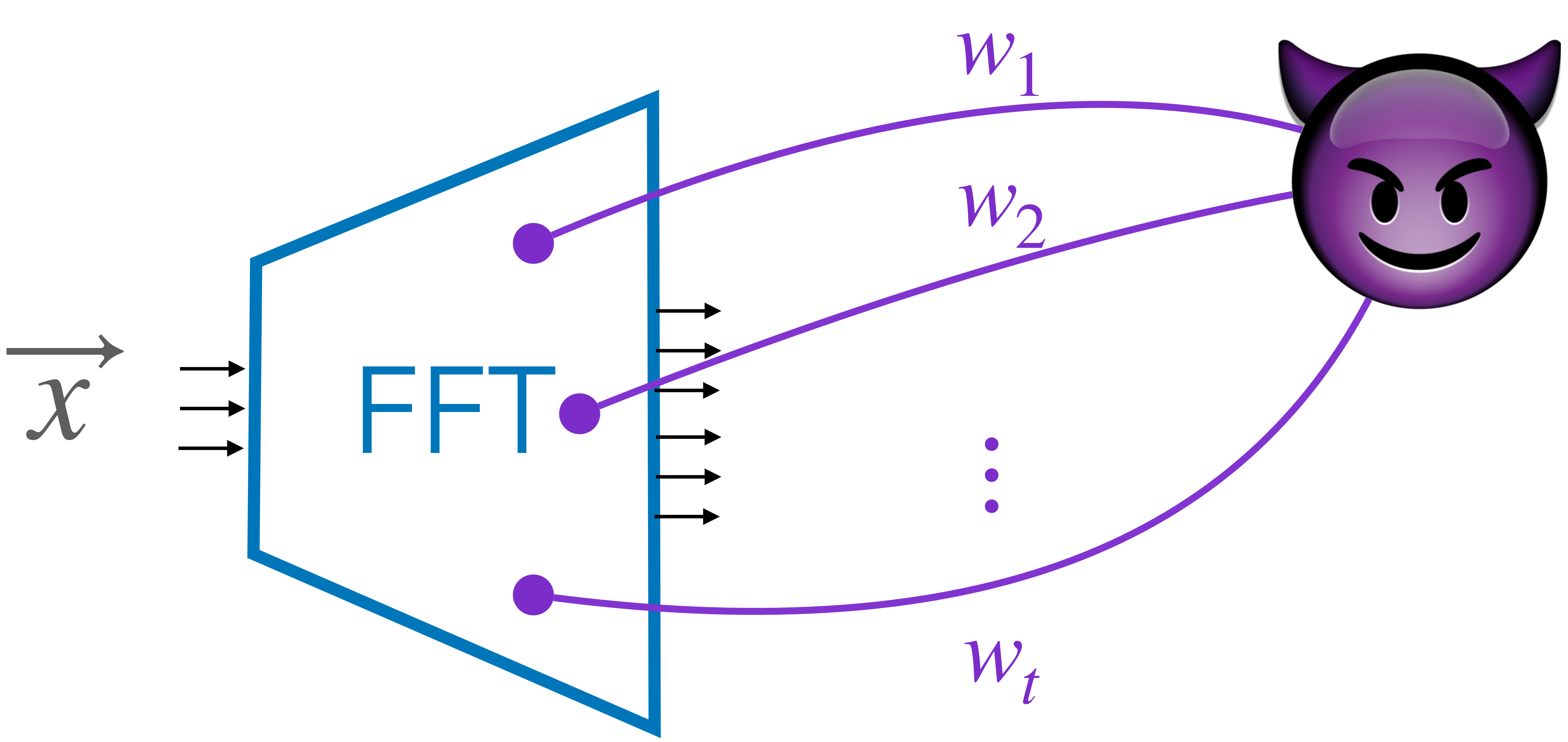
Probing security



💡 *FFT computes linear combinations of the x_i's*

$$\begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_t \end{pmatrix} = \begin{bmatrix} \ A \ \end{bmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_t \end{pmatrix}$$

Probing security



FFT computes linear combinations of the x_i's

$$\begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_t \end{pmatrix} = \begin{bmatrix} & A & \end{bmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_t \end{pmatrix}$$

Lemma 1

If $\vec{v} = \begin{pmatrix} \omega^0 \\ \omega^1 \\ \vdots \\ \omega^{n-1} \end{pmatrix} \notin \langle \begin{bmatrix} & A & \end{bmatrix} \rangle$ then $\begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_t \end{pmatrix} \sim \mathcal{U}(\mathbb{F}^t)$ *(assuming A full rank wlog)*

Probing security

Lemma 2

$\exists$ at most t values of $\omega \in \mathbb{F}$ s.t. $\overrightarrow{v} = \begin{pmatrix} \omega^0 \\ \omega^1 \\ \vdots \\ \omega^{n-1} \end{pmatrix} \in \left\langle \left[\; A \; \right] \right\rangle$

Probing security

Lemma 2

$$\exists \text{ at most } t \text{ values of } \omega \in \mathbb{F} \text{ s.t. } \vec{v} = \begin{pmatrix} \omega^0 \\ \omega^1 \\ \vdots \\ \omega^{n-1} \end{pmatrix} \in \left\langle \begin{bmatrix} A \end{bmatrix} \right\rangle$$

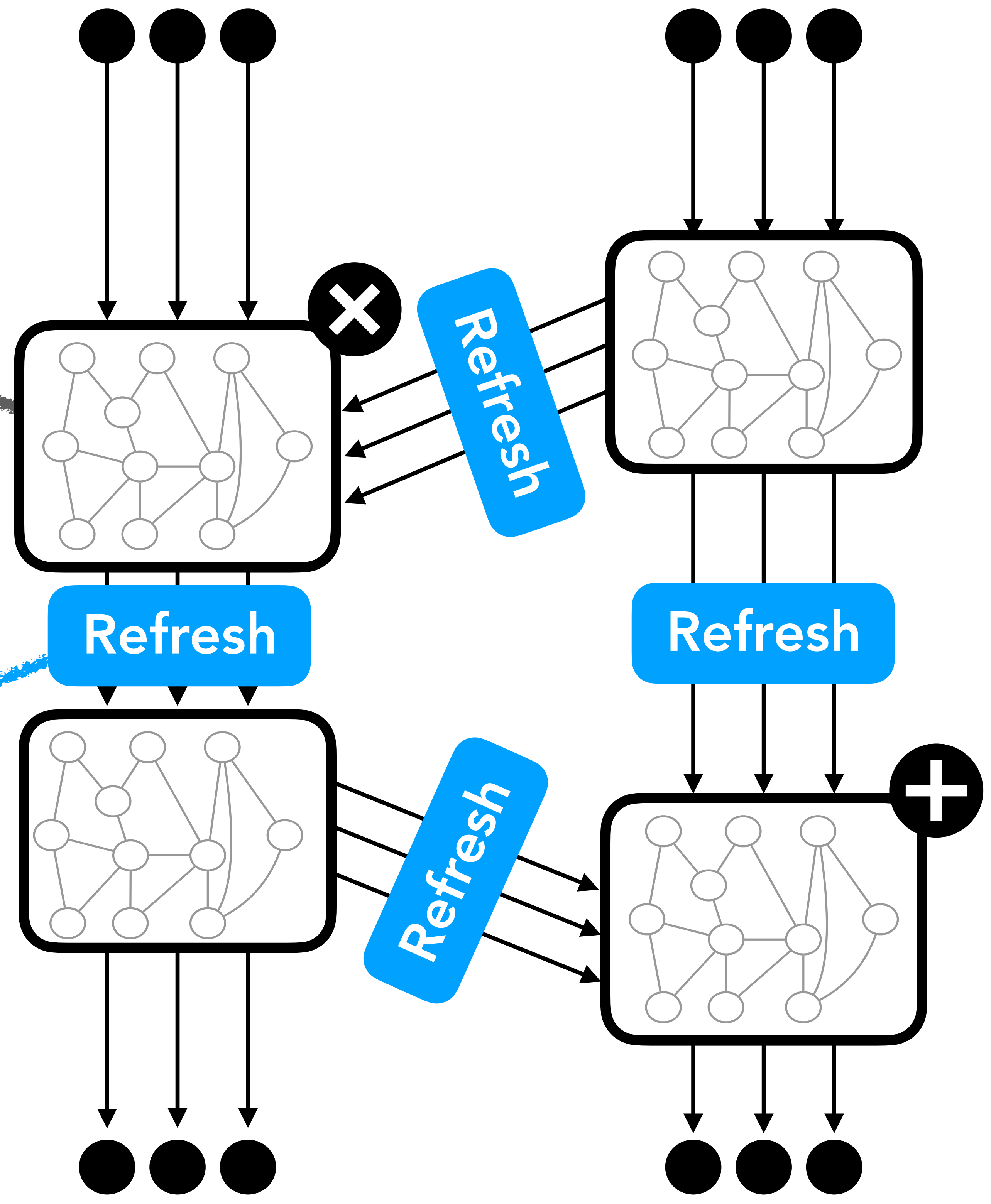
Lemma 1 + Lemma 2

$$P\left[(w_1, \ldots, w_t) \text{ cannot be simulated} \right] \leq \frac{t}{|\mathbb{F}|} < \frac{n}{|\mathbb{F}|}$$

Composition security

probing security

input-output separation (IOS) property



⇒ region probing security

5. Security with constant leakage rate

The expansion strategy

Ananth, Ishai, Sahai - CRYPTO 2018

- Idea: bootstrap constant-size gadgets
- Amplification of random probing security

$$p \longrightarrow f(p)$$

The expansion strategy

Ananth, Ishai, Sahai - CRYPTO 2018

- Idea: bootstrap constant-size gadgets
- Amplification of random probing security

$$p \longrightarrow f(p) \longrightarrow f(f(p))$$

The expansion strategy

Ananth, Ishai, Sahai - CRYPTO 2018

- Idea: bootstrap constant-size gadgets
- Amplification of random probing security

$$p \longrightarrow f(p) \longrightarrow f(f(p)) \longrightarrow \cdots \longrightarrow f^{(k)}(p)$$

The expansion strategy

Ananth, Ishai, Sahai - CRYPTO 2018

- Idea: bootstrap constant-size gadgets
- Amplification of random probing security

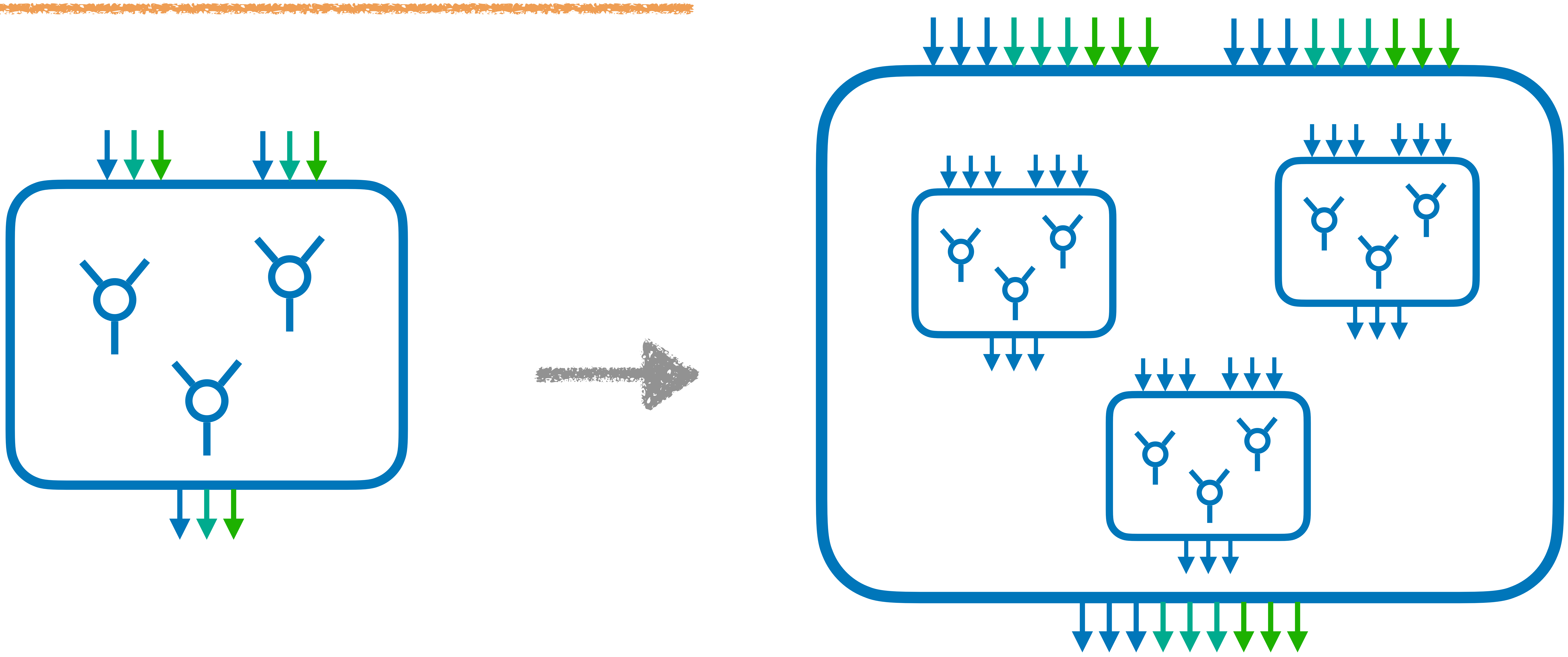
$$p \longrightarrow f(p) \longrightarrow f(f(p)) \longrightarrow \cdots \longrightarrow f^{(k)}(p)$$

Belaïd, Coron, Prouff, Rivain, Taleb - CRYPTO 2020

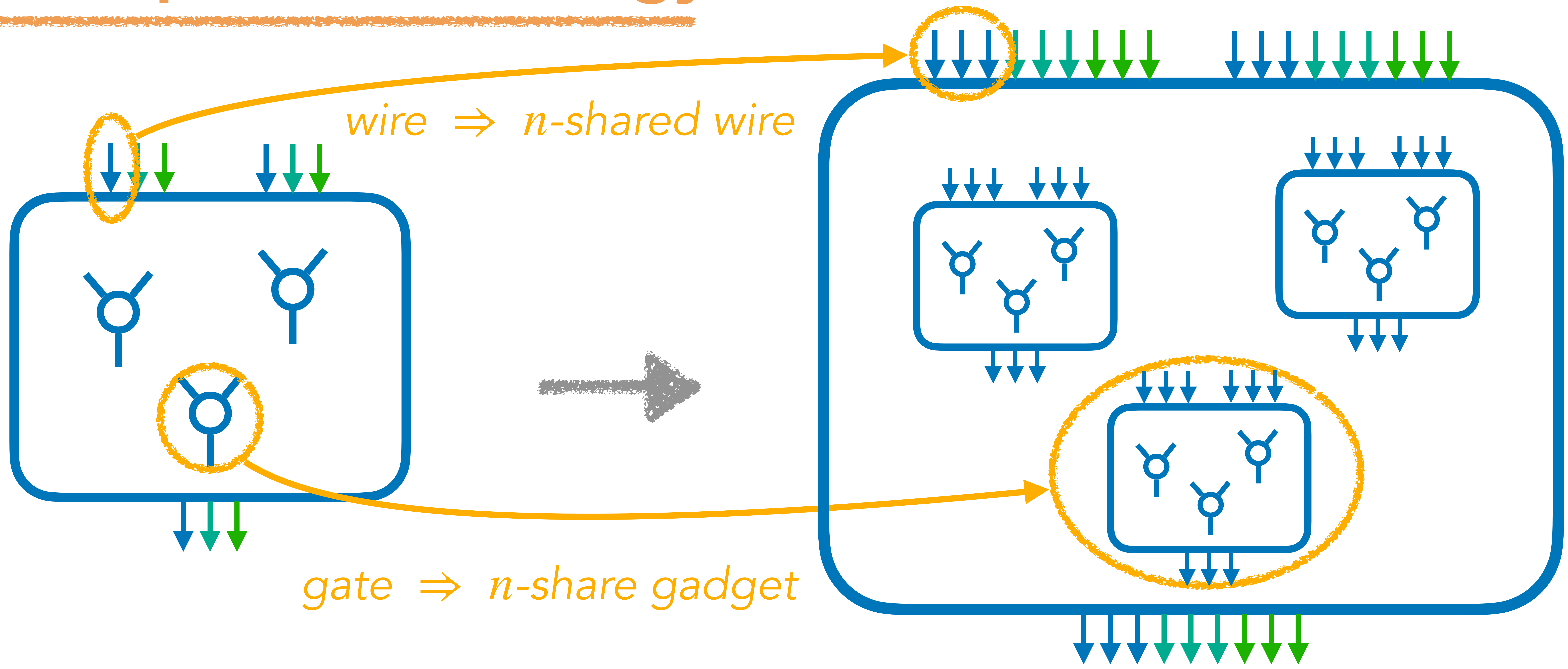
Belaïd, Rivain, Taleb - EUROCRYPT 2021

- Formalise new composition / expansion notions
- Obtain lower complexity / tolerate higher leakage rate

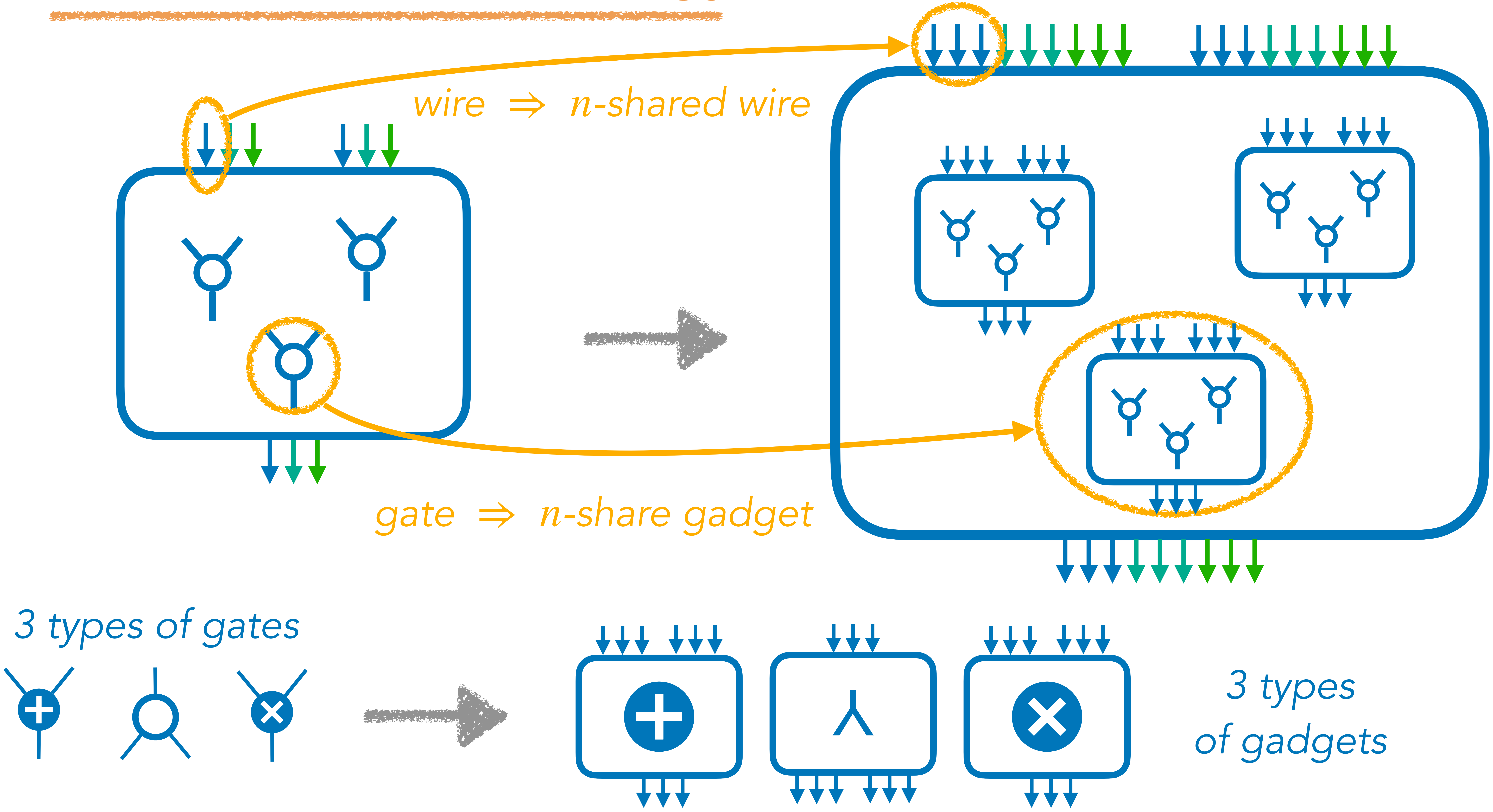
The expansion strategy



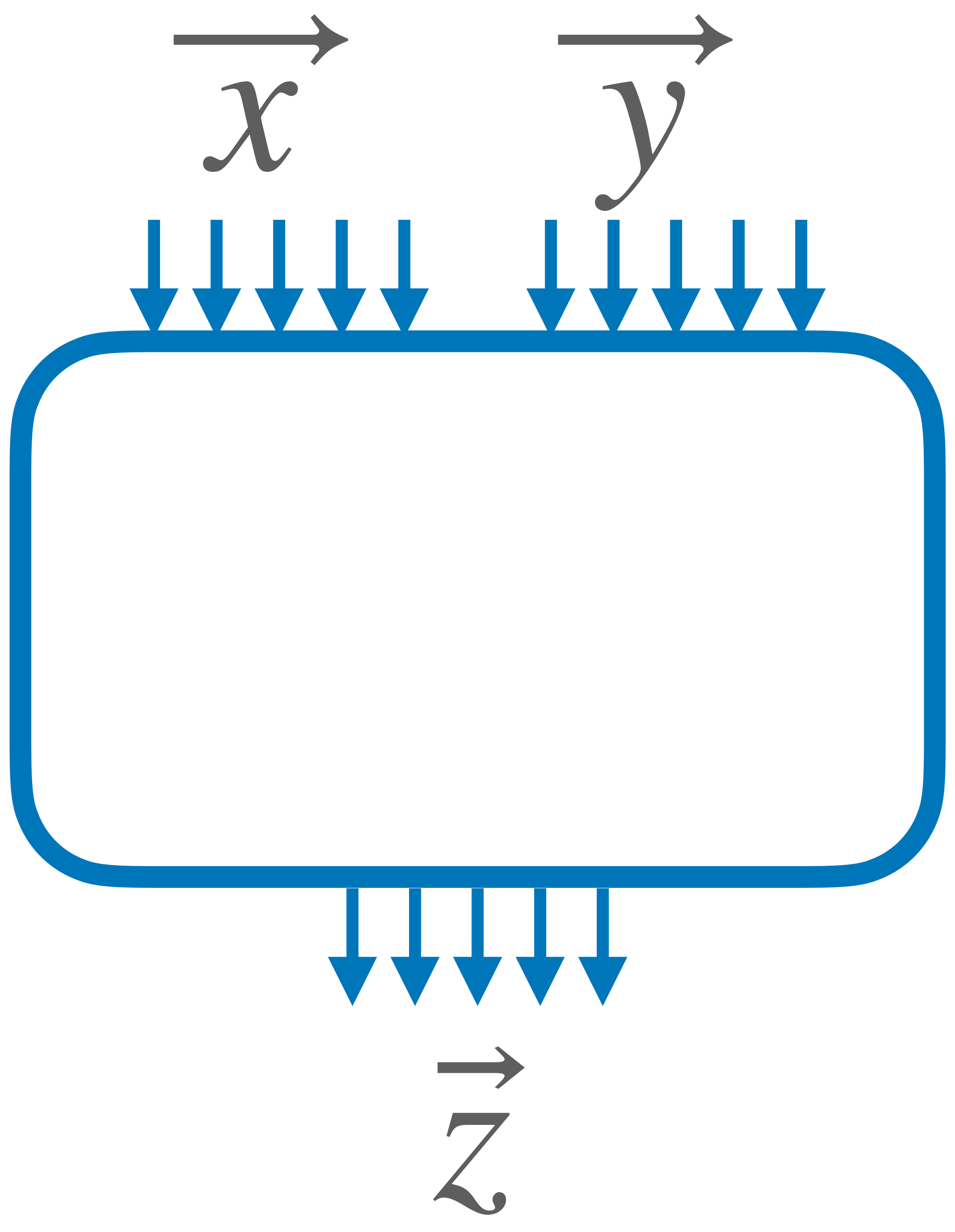
The expansion strategy



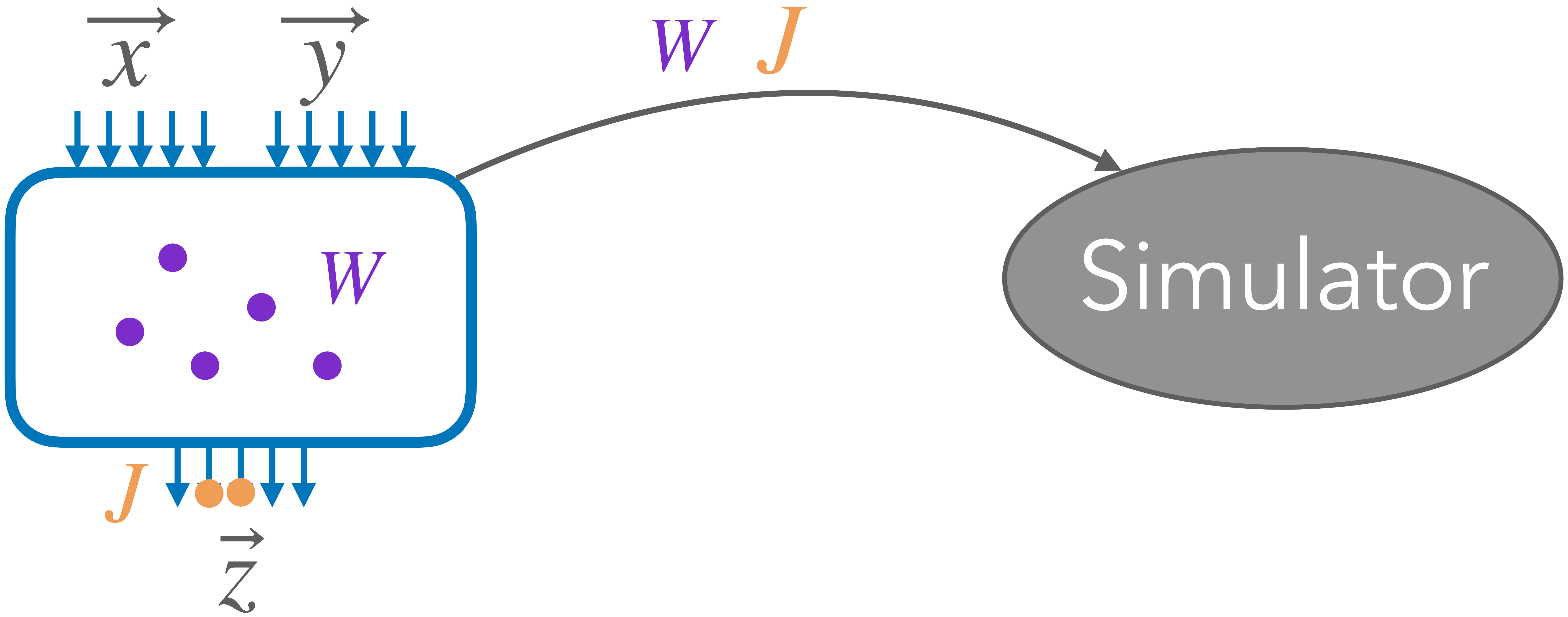
The expansion strategy



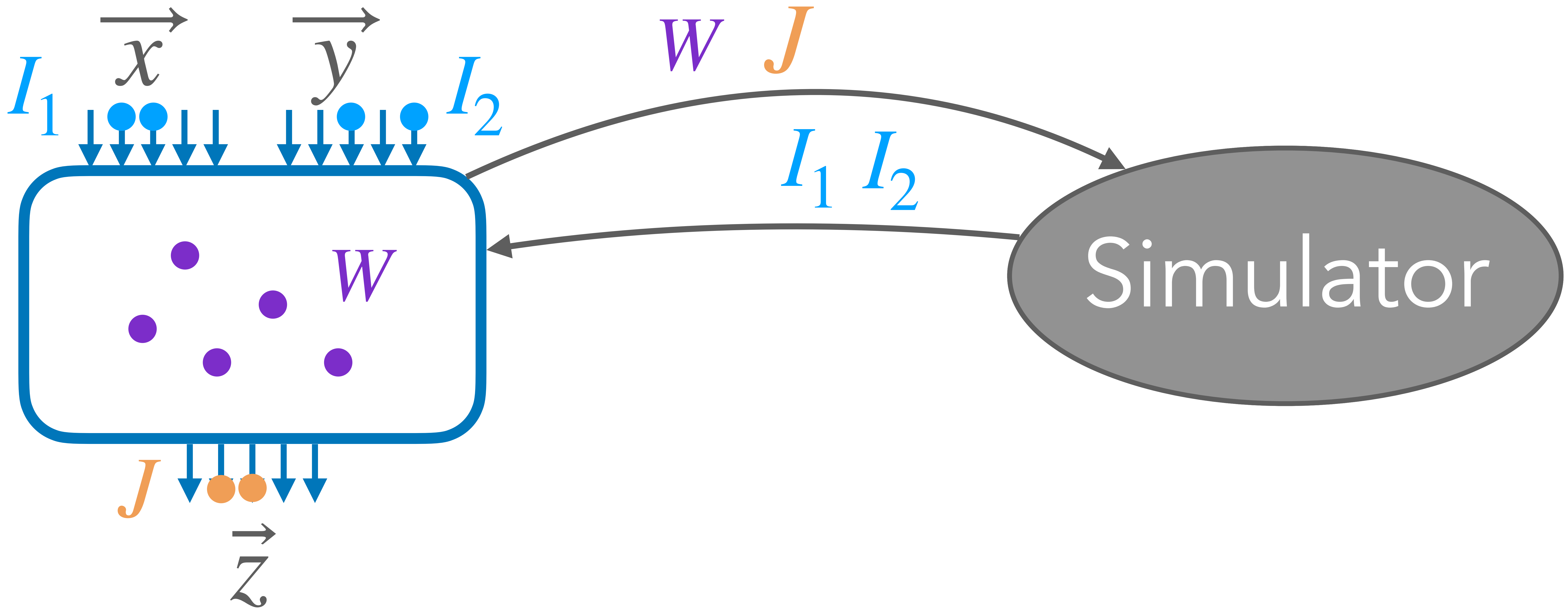
Random probing expandability (RPE)



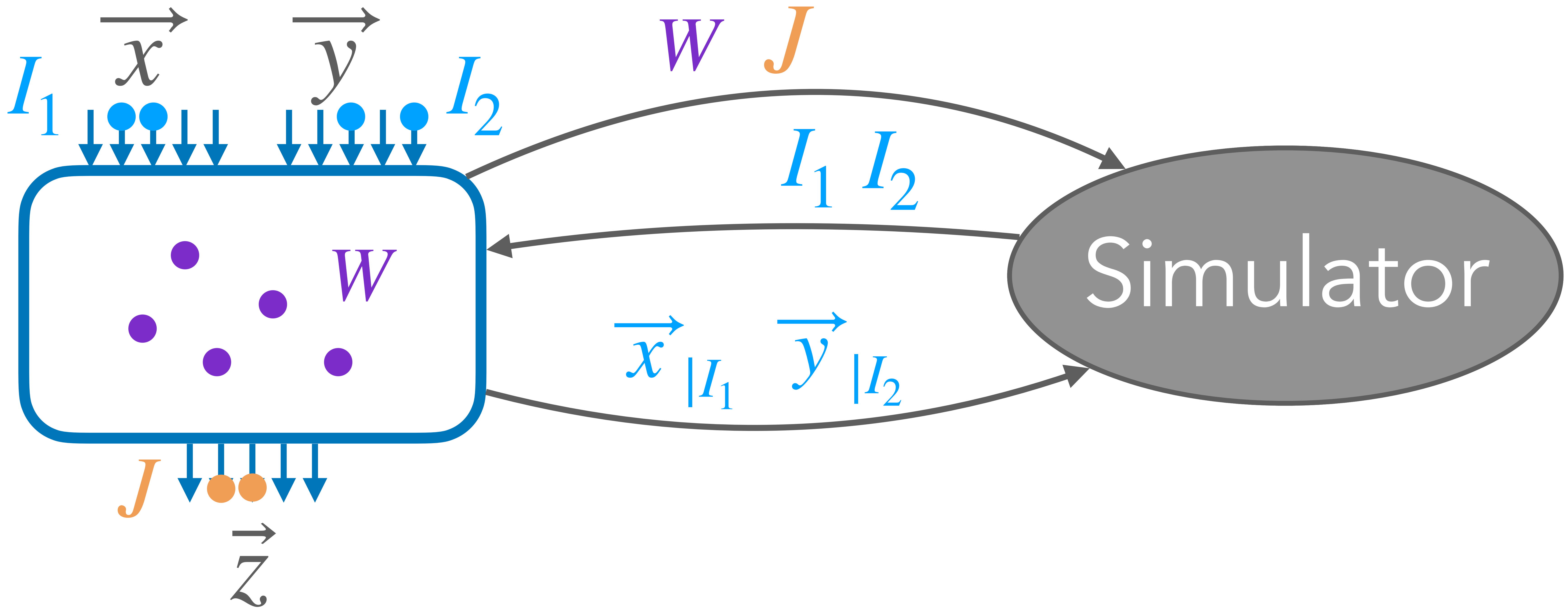
Random probing expandability (RPE)



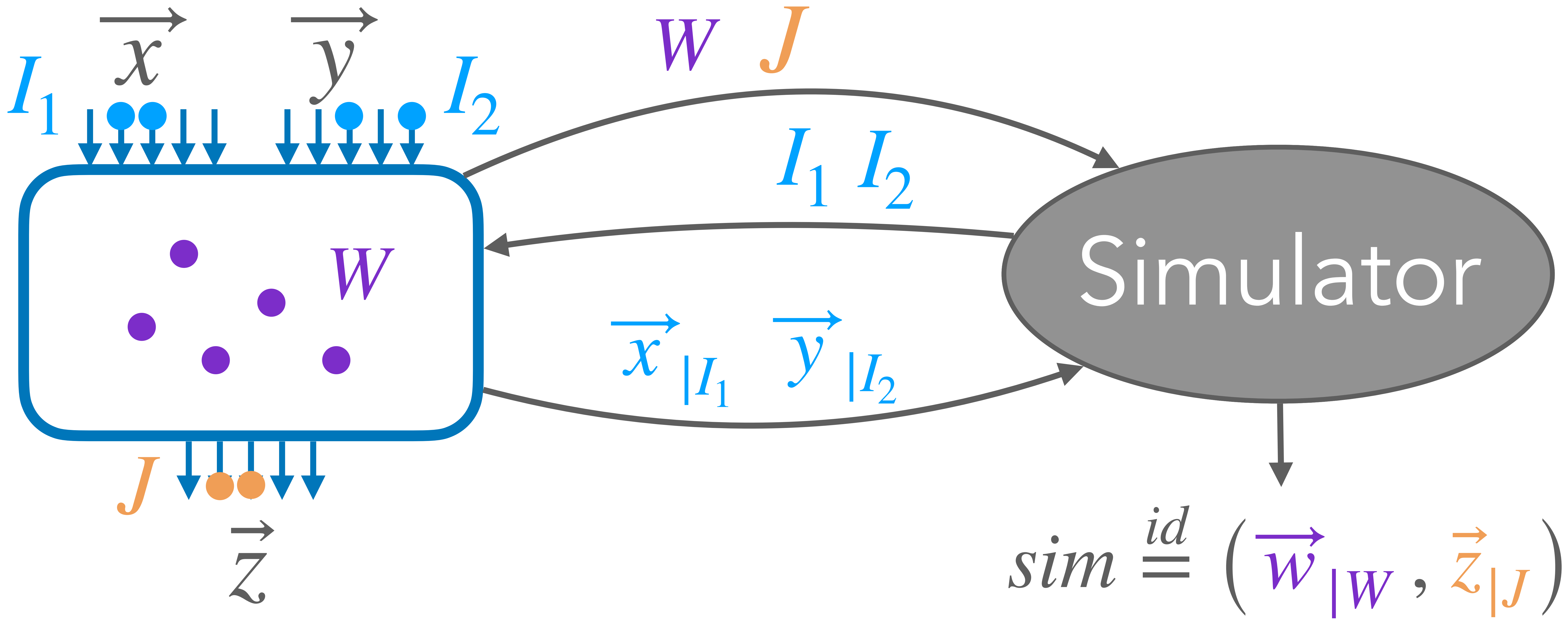
Random probing expandability (RPE)



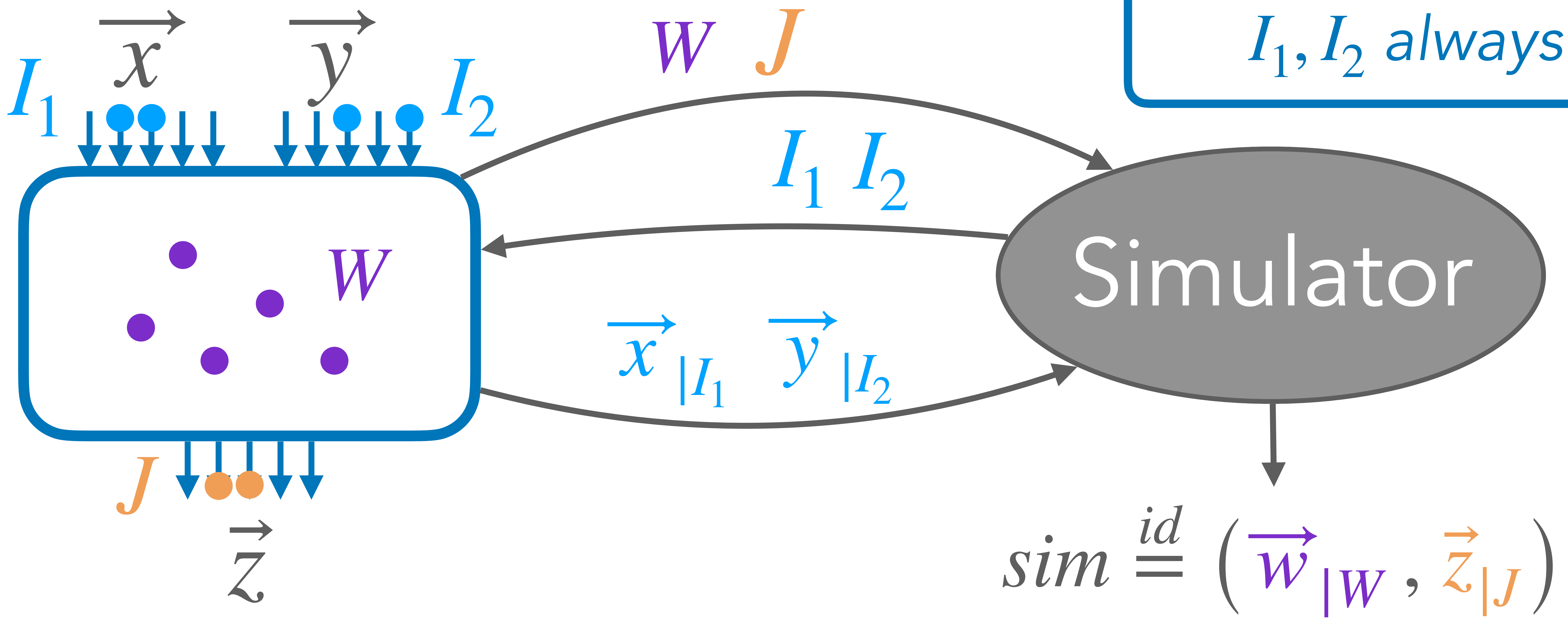
Random probing expandability (RPE)



Random probing expandability (RPE)



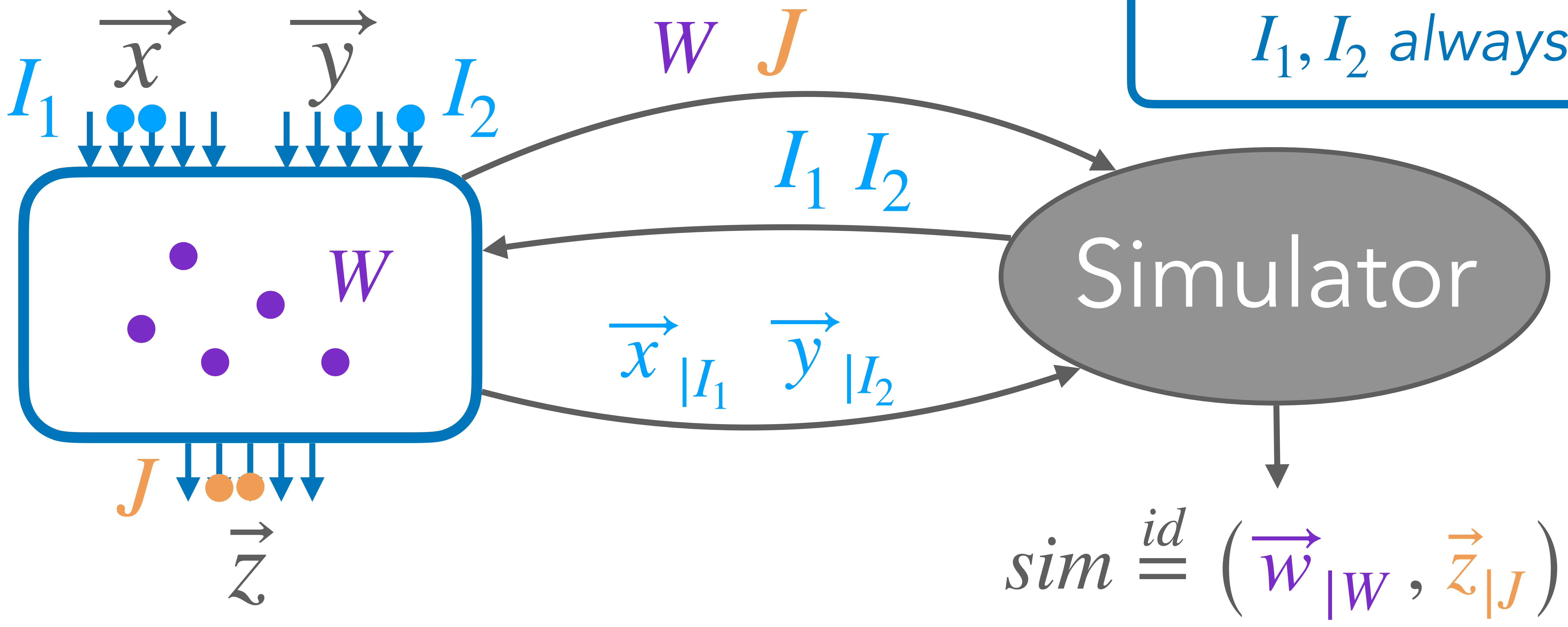
Random probing expandability (RPE)



I_1, I_2 *always exist*

Random probing expandability (RPE)

I_1, I_2 *always exist*

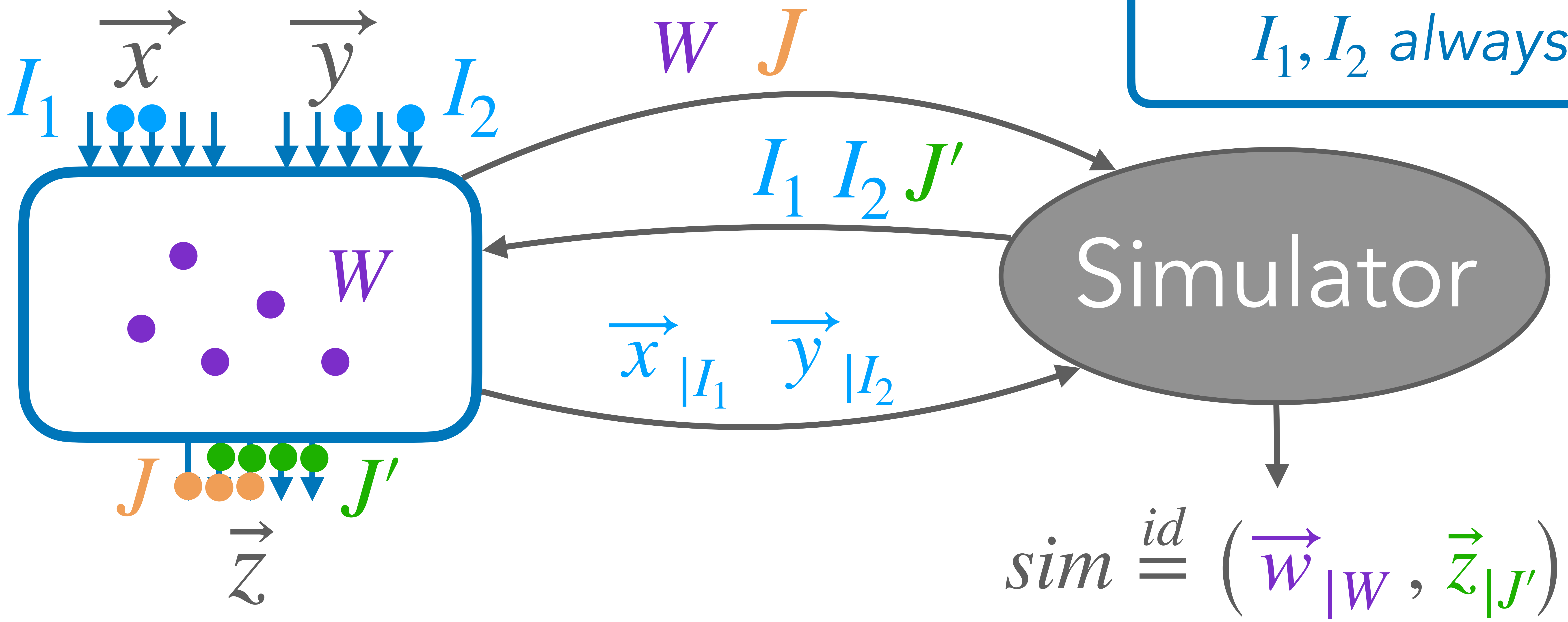


RPE threshold t: $|J| \leq t$,

$(|I_1| > t$ *or* $|I_2| > t)$ = *simulation failure*

Random probing expandability (RPE)

I_1, I_2 *always exist*



<u>RPE threshold t:</u> $|J| \leq t$,

$(|I_1| > t$ *or* $|I_2| > t)$ = *simulation failure*

if $|J| > t$, *sim. can choose*

J' *s.t.* $|J'| = n - 1$

Random probing expandability (RPE)

- Failure events:

$$\mathcal{F}_1 := (|I_1| > t) \qquad \mathcal{F}_2 := (|I_2| > t)$$

- The gadget is ε-RPE if

$$\Pr(\mathcal{F}_1) \leq \varepsilon\,,\ \Pr(\mathcal{F}_2) \leq \varepsilon\,,\ \Pr(\mathcal{F}_1 \cap \mathcal{F}_2) \leq \varepsilon^2$$

$\forall J$ and w.r.t. random $W \leftarrow \mathsf{LeakingWires}(p)$

Random probing expandability (RPE)

- Failure events:

$$\mathcal{F}_1 := (|I_1| > t) \qquad \mathcal{F}_2 := (|I_2| > t)$$

- The gadget is ε-RPE if

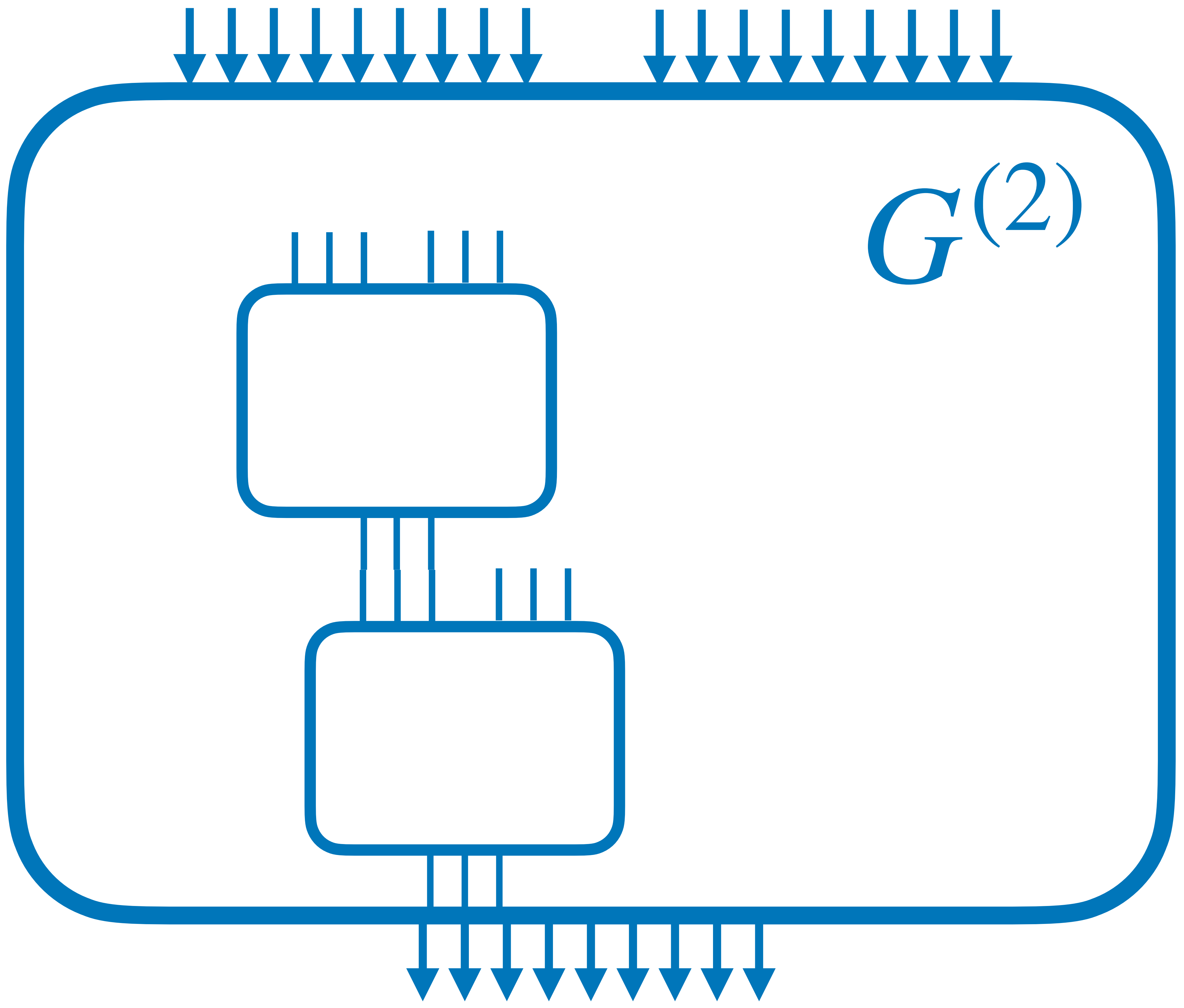
$$\Pr(\mathcal{F}_1) \leq \varepsilon\,,\ \Pr(\mathcal{F}_2) \leq \varepsilon\,,\ \Pr(\mathcal{F}_1 \cap \mathcal{F}_2) \leq \varepsilon^2$$

$\forall J$ and w.r.t. random $W \leftarrow$ LeakingWires(p)

- The gadget if f-RPE if $\varepsilon = f(p)$

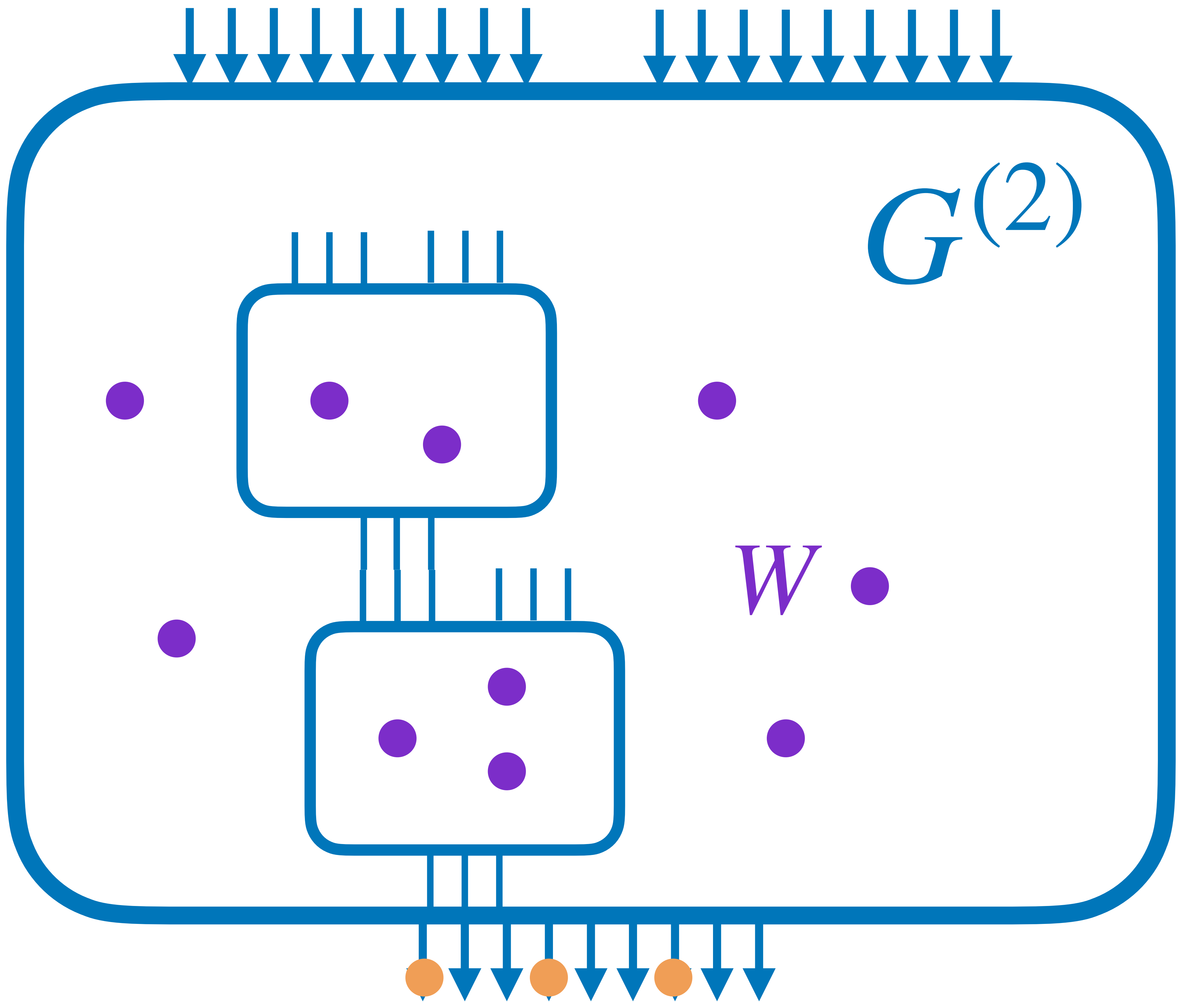
Expansion security

Base gadget $\{G\}$ f-RPE $\Rightarrow$ expanded gadgets $\{G^{(2)}\}$ f^2-RPE



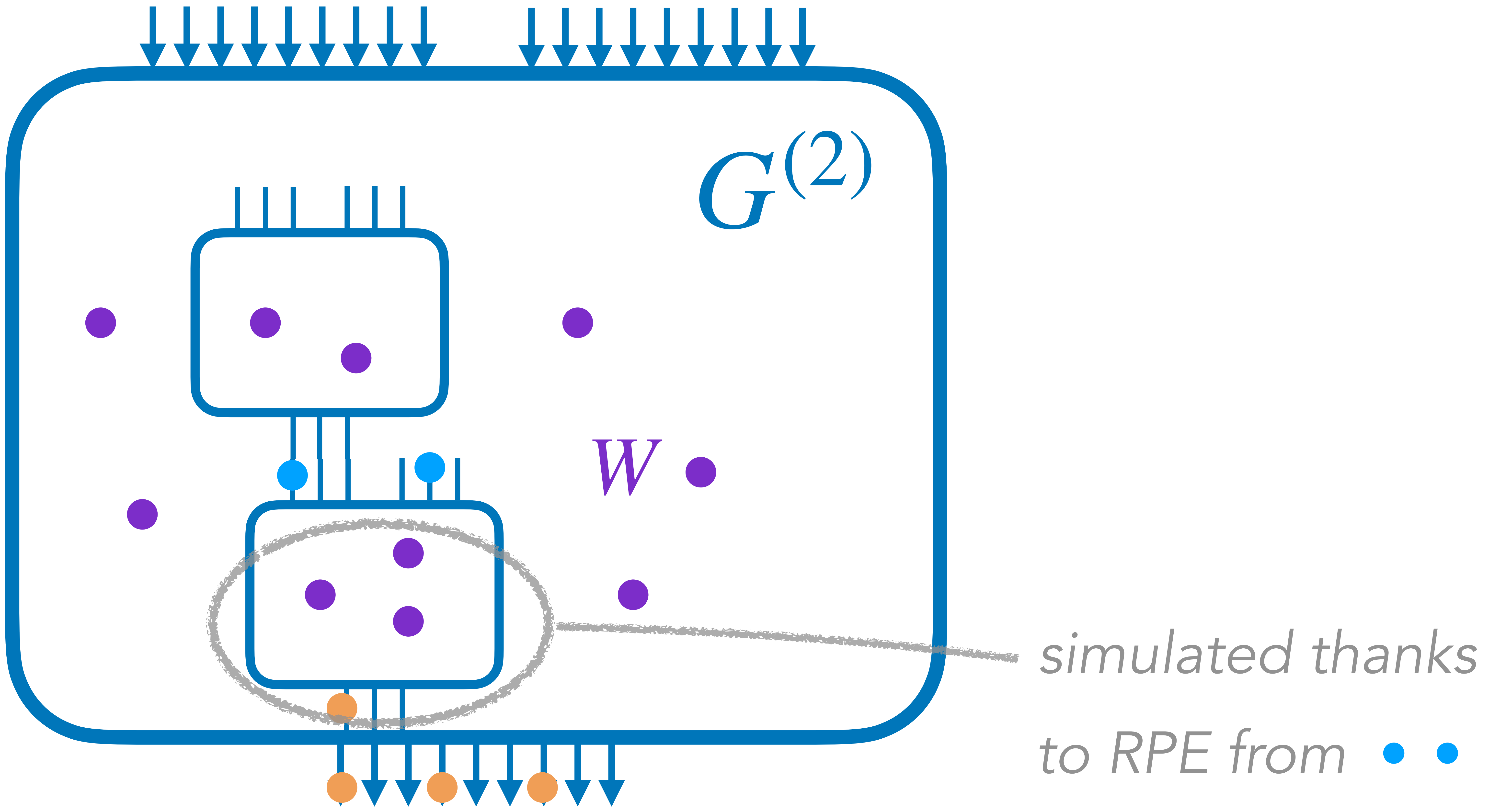
Expansion security

Base gadget $\{G\}$ f-RPE $\Rightarrow$ expanded gadgets $\{G^{(2)}\}$ f^2-RPE



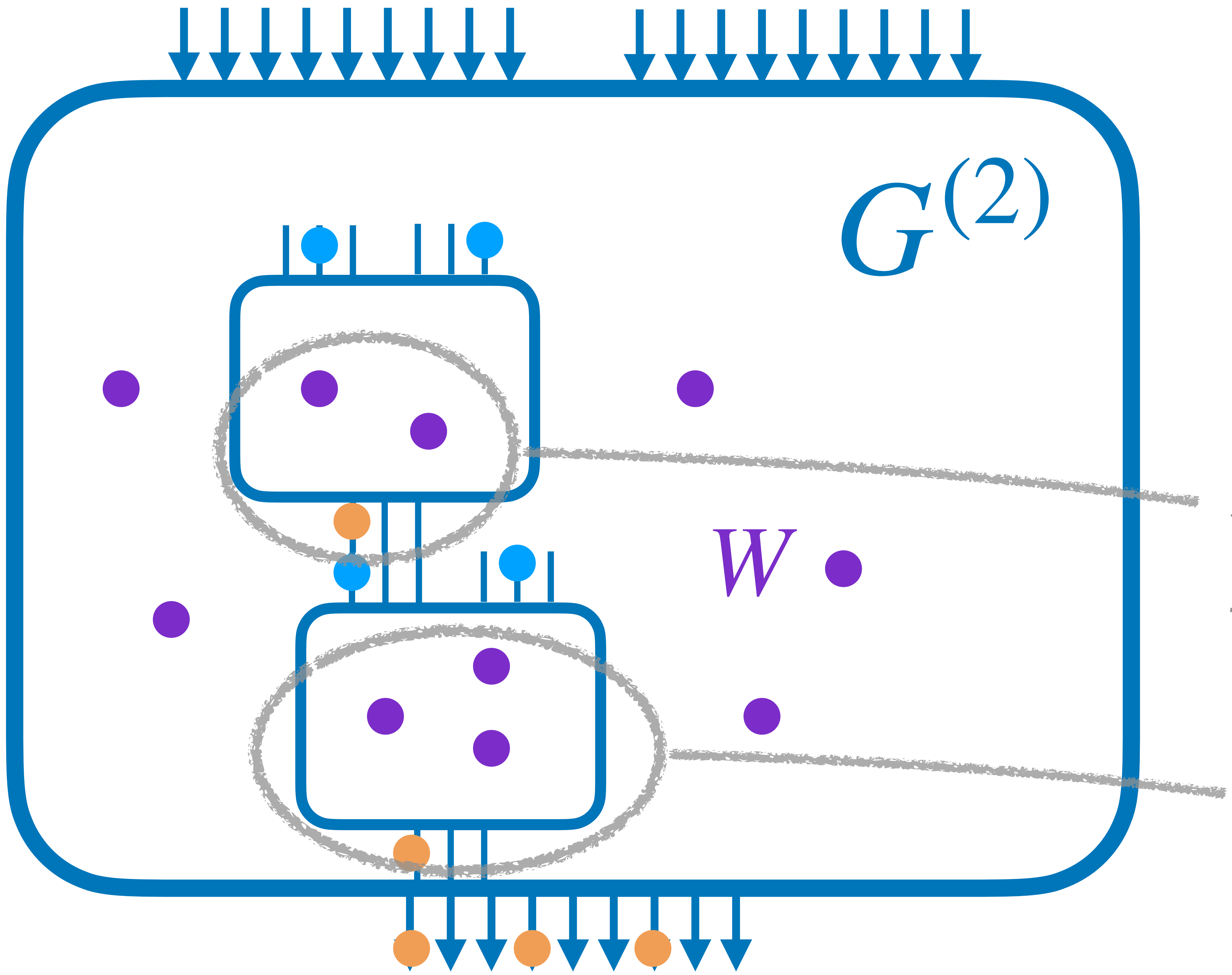
Expansion security

Base gadget $\{G\}$ f-RPE $\Rightarrow$ expanded gadgets $\{G^{(2)}\}$ f^2-RPE



Expansion security

Base gadget $\{G\}$ f-RPE $\Rightarrow$ expanded gadgets $\{G^{(2)}\}$ f^2-RPE

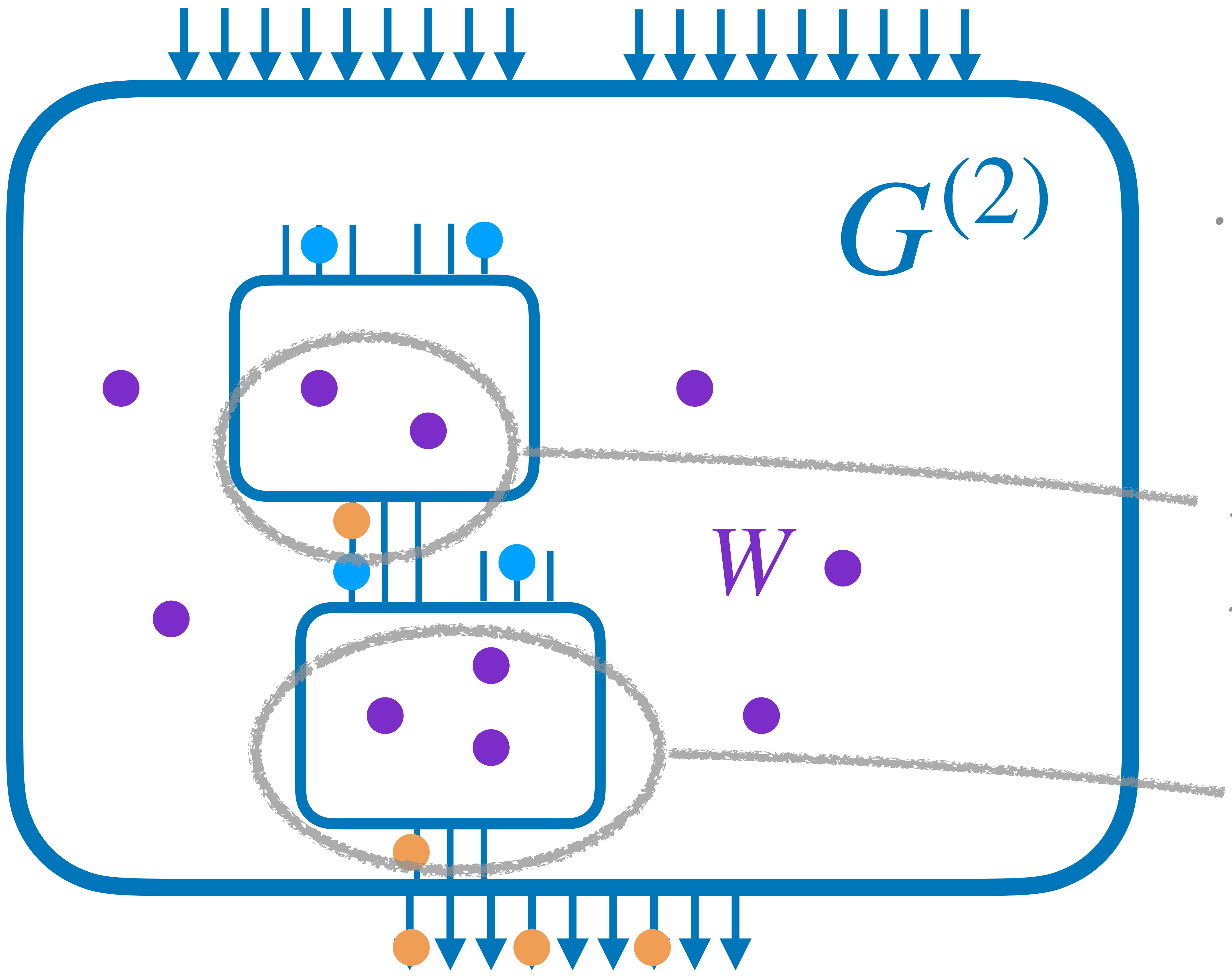


simulated thanks to RPE from

simulated thanks to RPE from

Expansion security

Base gadget $\{G\}$ f-RPE $\Rightarrow$ expanded gadgets $\{G^{(2)}\}$ f^2-RPE



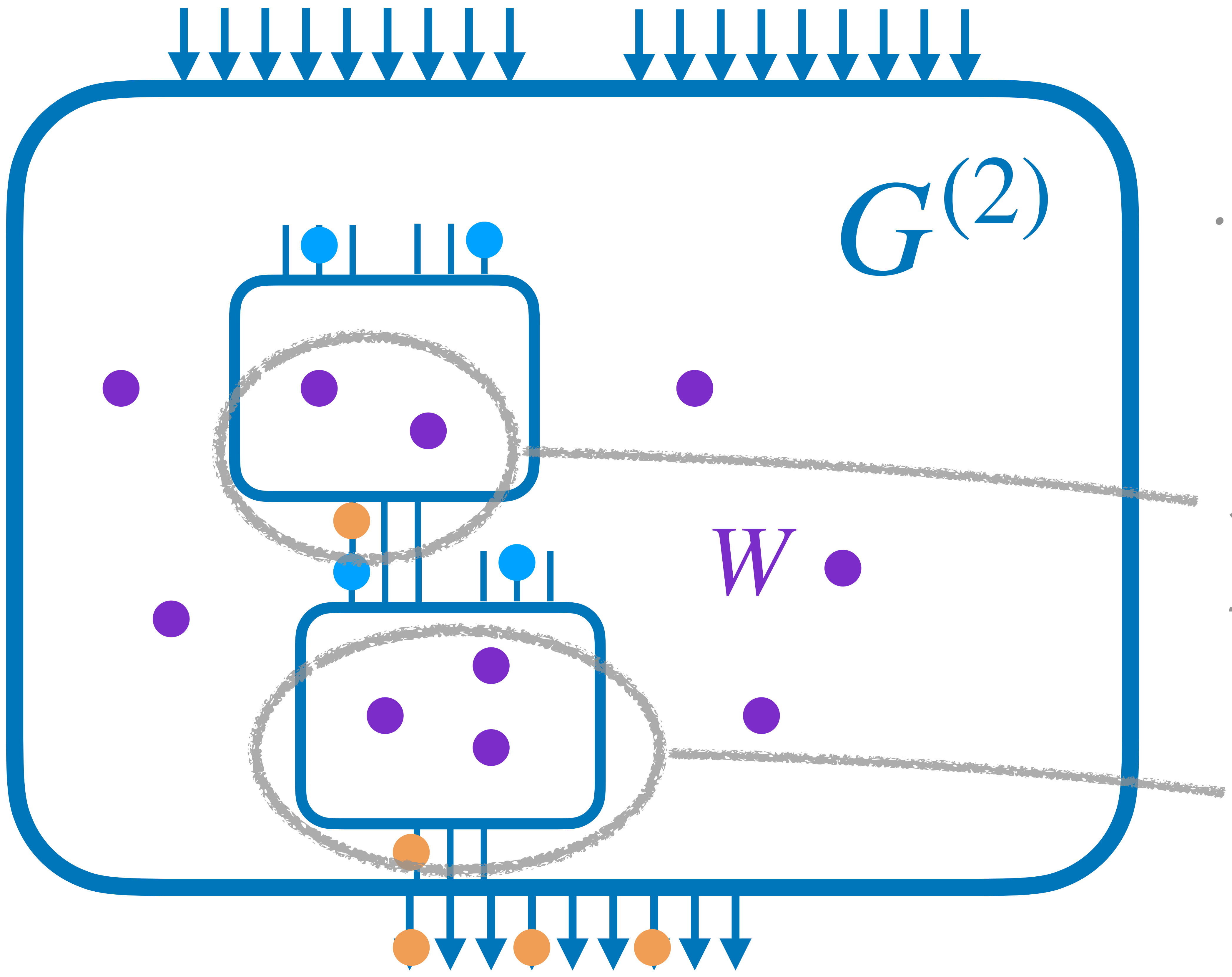
… and so on from bottom to top

simulated thanks to RPE from • •

simulated thanks to RPE from • •

Expansion security

Base gadget $\{G\}$ f-RPE $\Rightarrow$ expanded gadgets $\{G^{(2)}\}$ f^2-RPE



Now what if a failure occurs ?

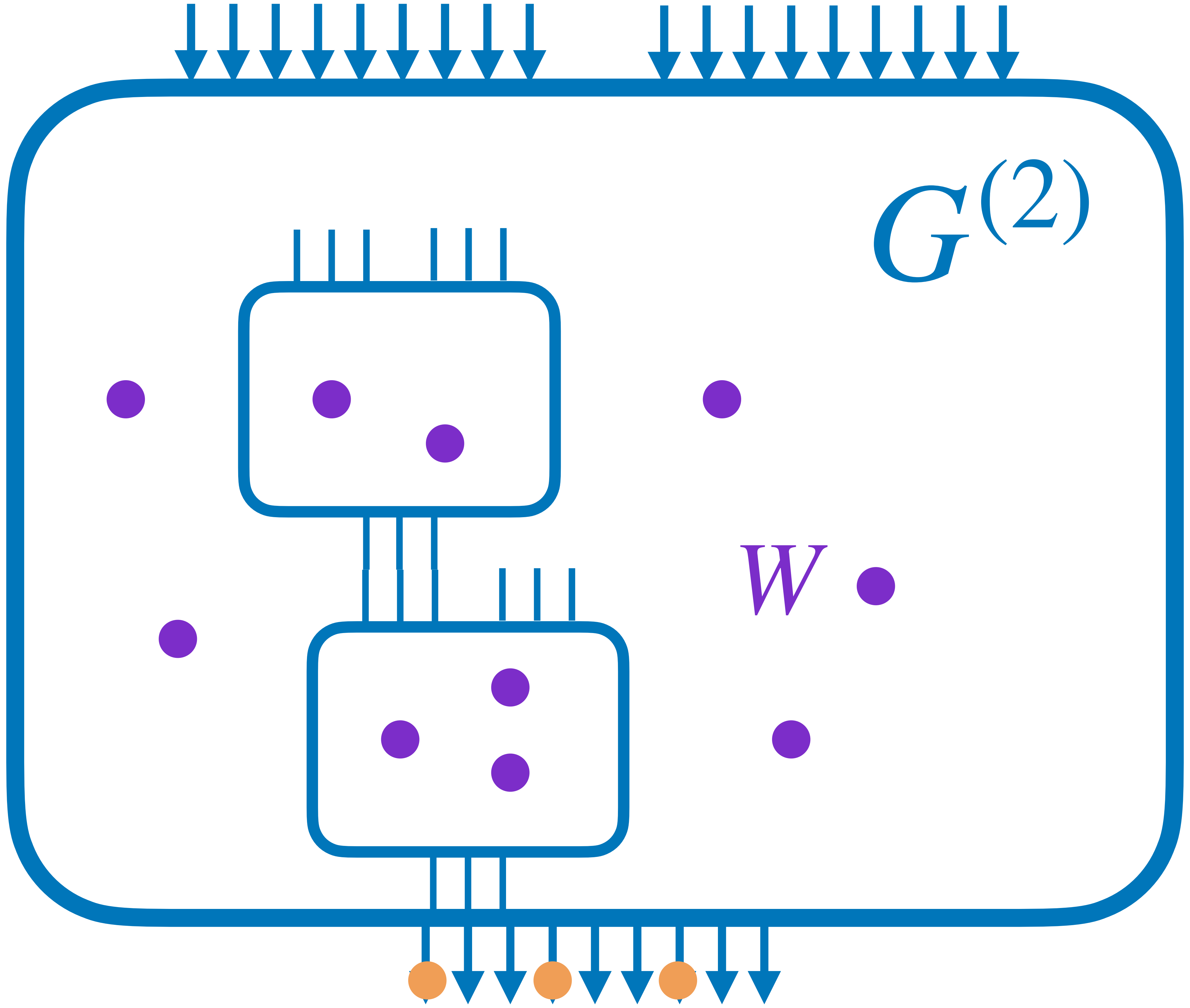
… and so on from bottom to top

simulated thanks to RPE from

simulated thanks to RPE from

Expansion security

Base gadget $\{G\}$ f-RPE $\Rightarrow$ expanded gadgets $\{G^{(2)}\}$ f^2-RPE

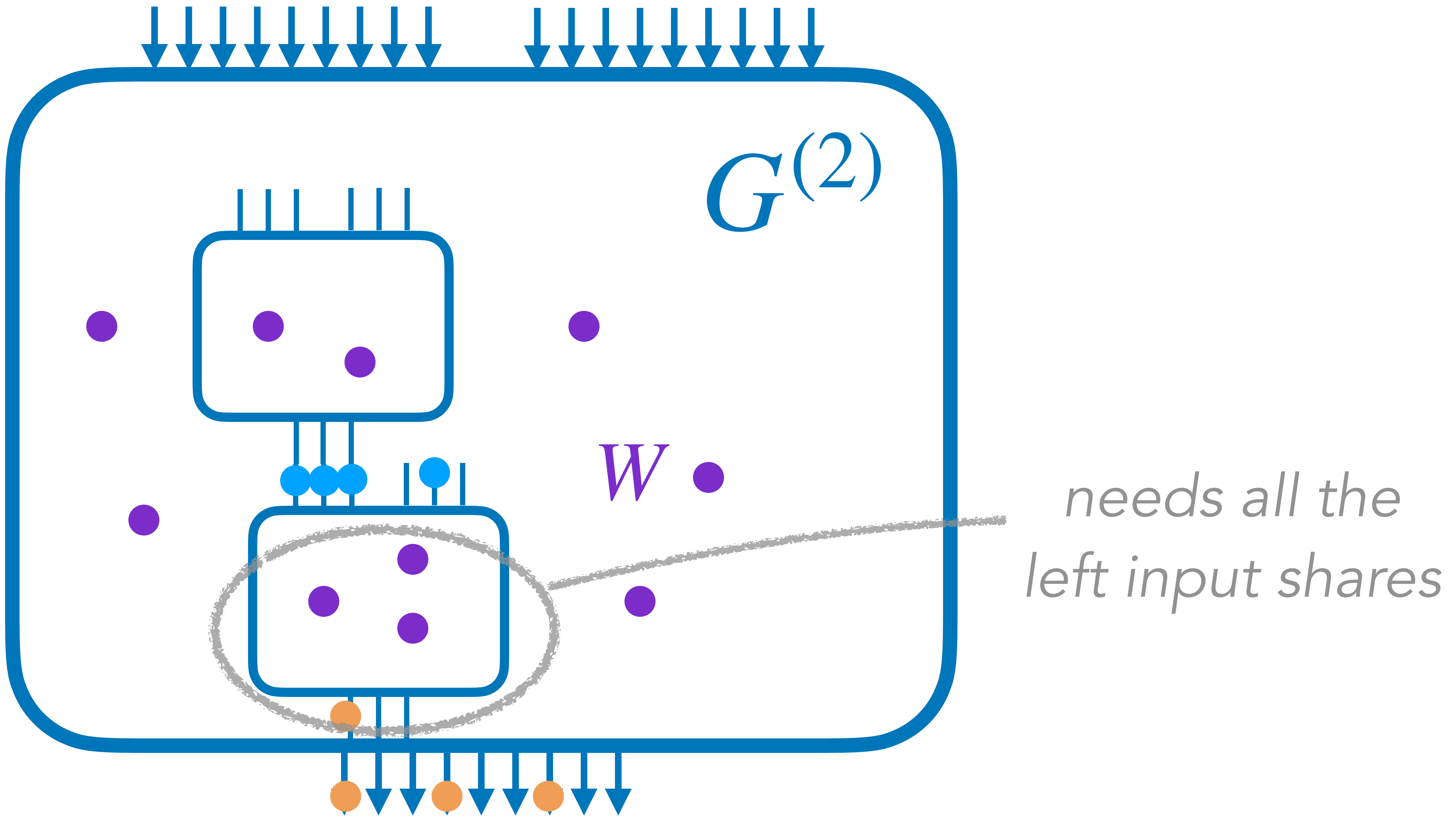


Now what if a failure occurs ?

Expansion security

Base gadget $\{G\}$ f-RPE $\Rightarrow$ expanded gadgets $\{G^{(2)}\}$ f^2-RPE

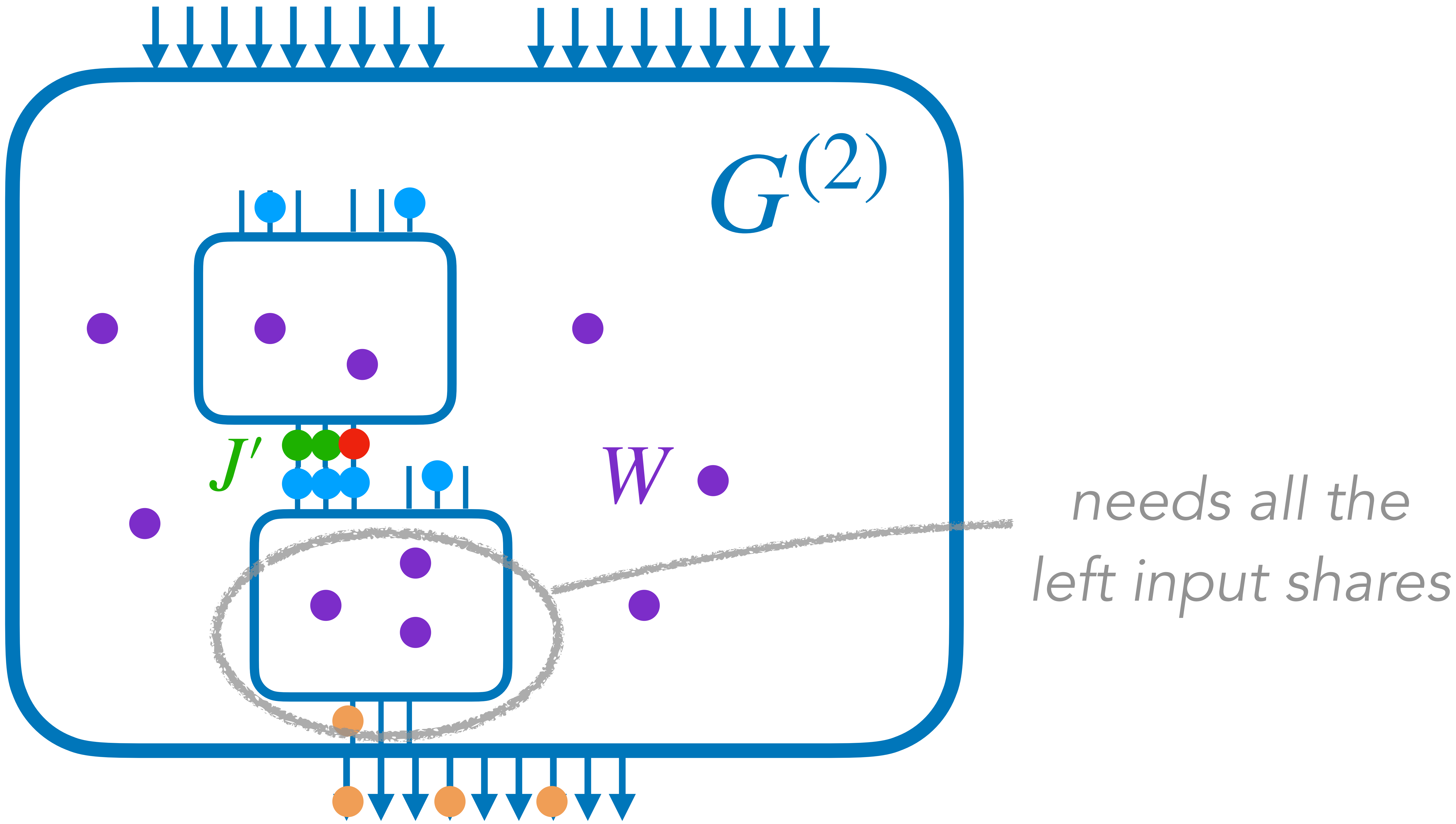
Now what if a failure occurs ?



Expansion security

Base gadget $\{G\}$ f-RPE $\Rightarrow$ expanded gadgets $\{G^{(2)}\}$ f^2-RPE

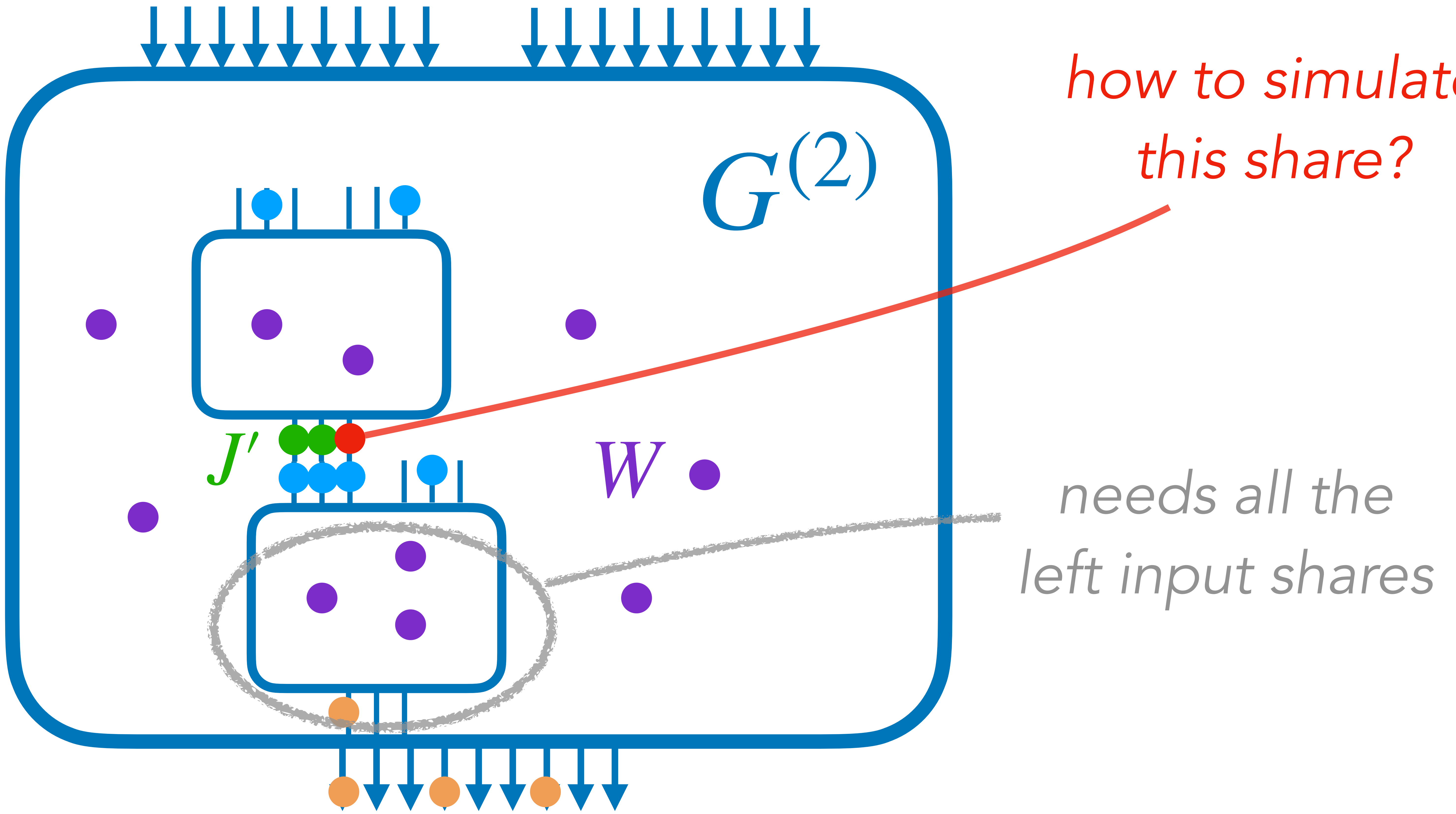
Now what if a failure occurs ?



Expansion security

Base gadget $\{G\}$ f-RPE $\Rightarrow$ expanded gadgets $\{G^{(2)}\}$ f^2-RPE

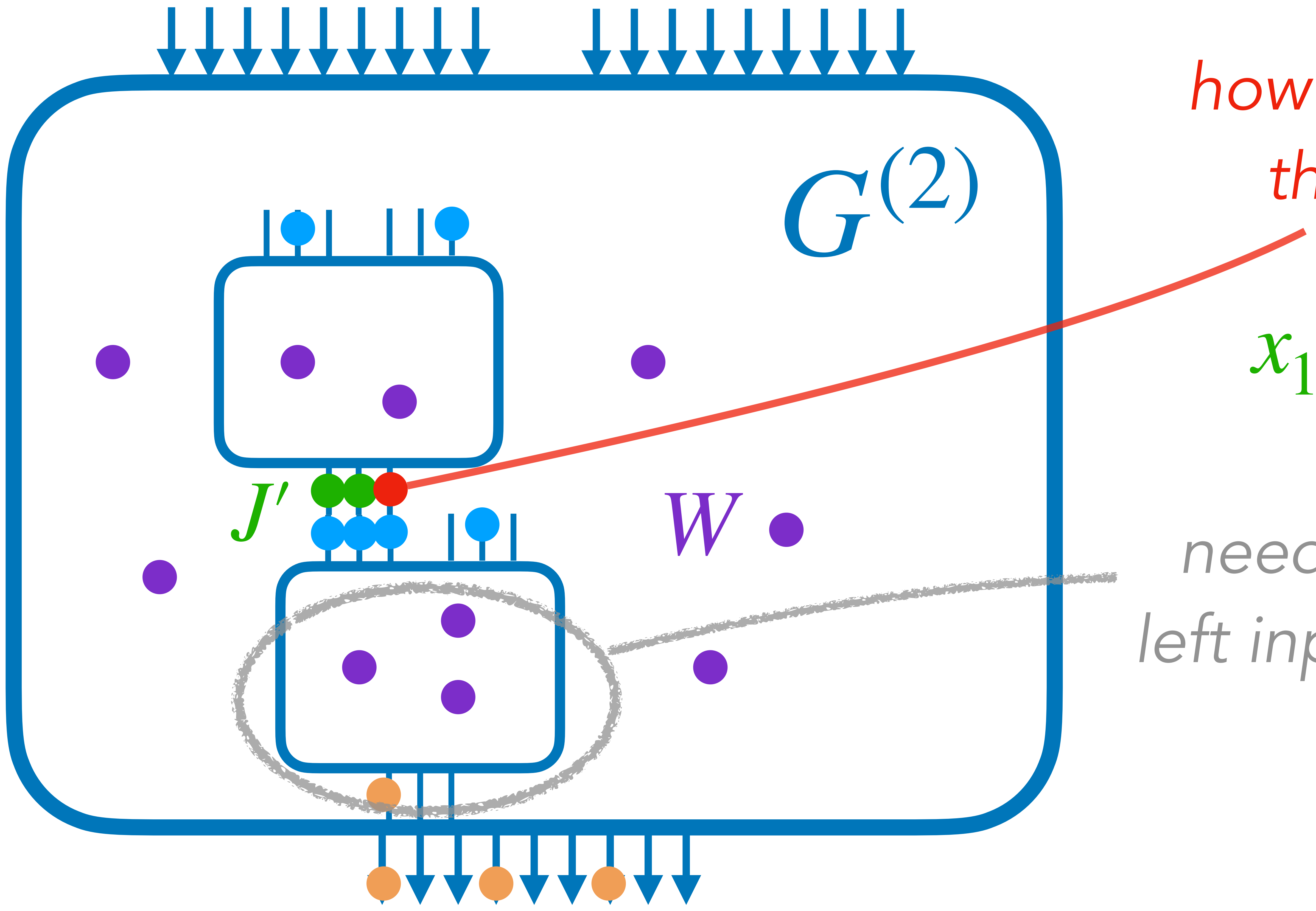
Now what if a failure occurs ?



Expansion security

Base gadget $\{G\}$ f-RPE $\Rightarrow$ expanded gadgets $\{G^{(2)}\}$ f^2-RPE

Now what if a failure occurs ?



how to simulate this share?

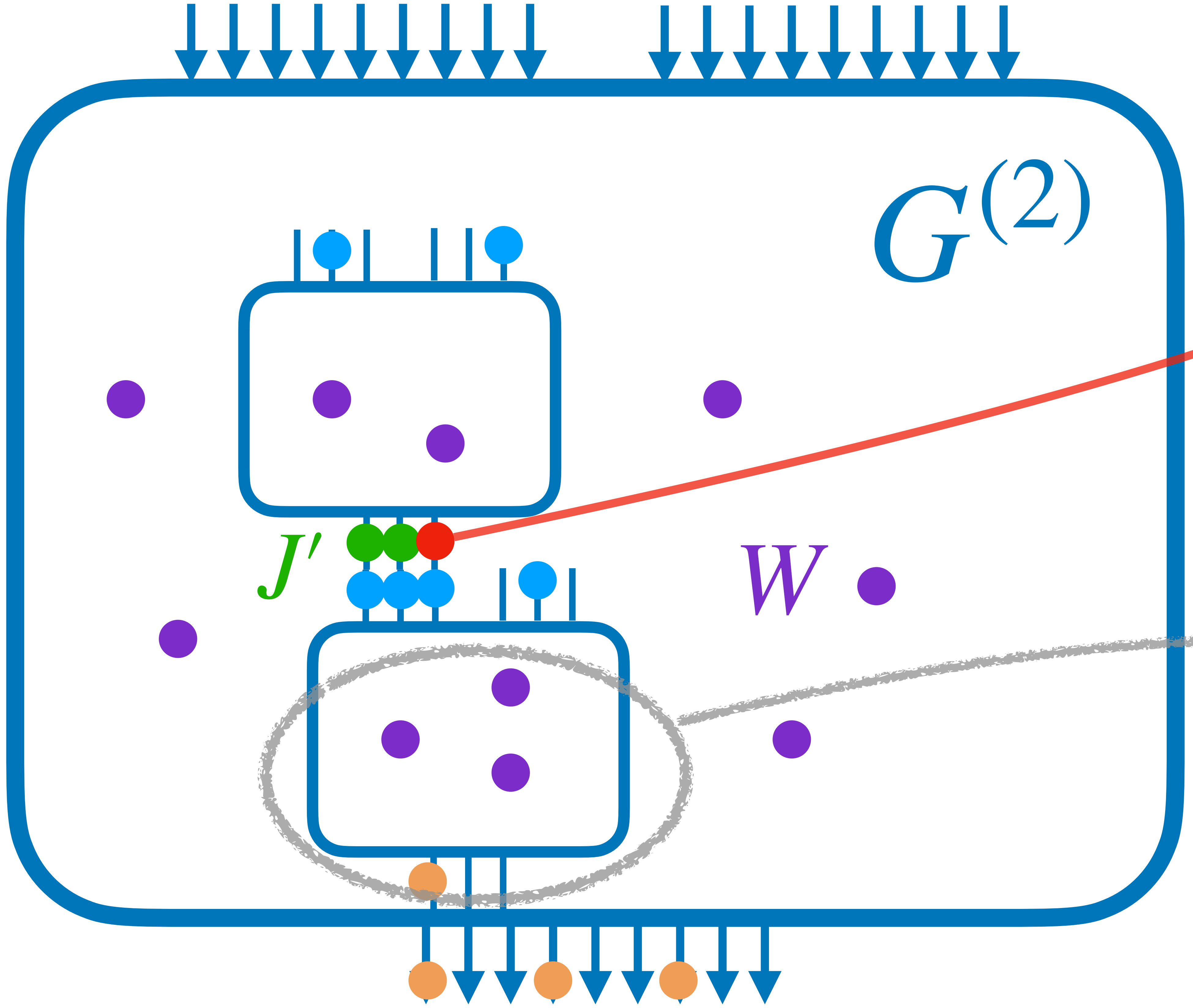
$$x_1 + x_2 + x_3 = x$$

needs all the left input shares

Expansion security

Base gadget $\{G\}$ f-RPE $\Rightarrow$ expanded gadgets $\{G^{(2)}\}$ f^2-RPE

Now what if a failure occurs ?

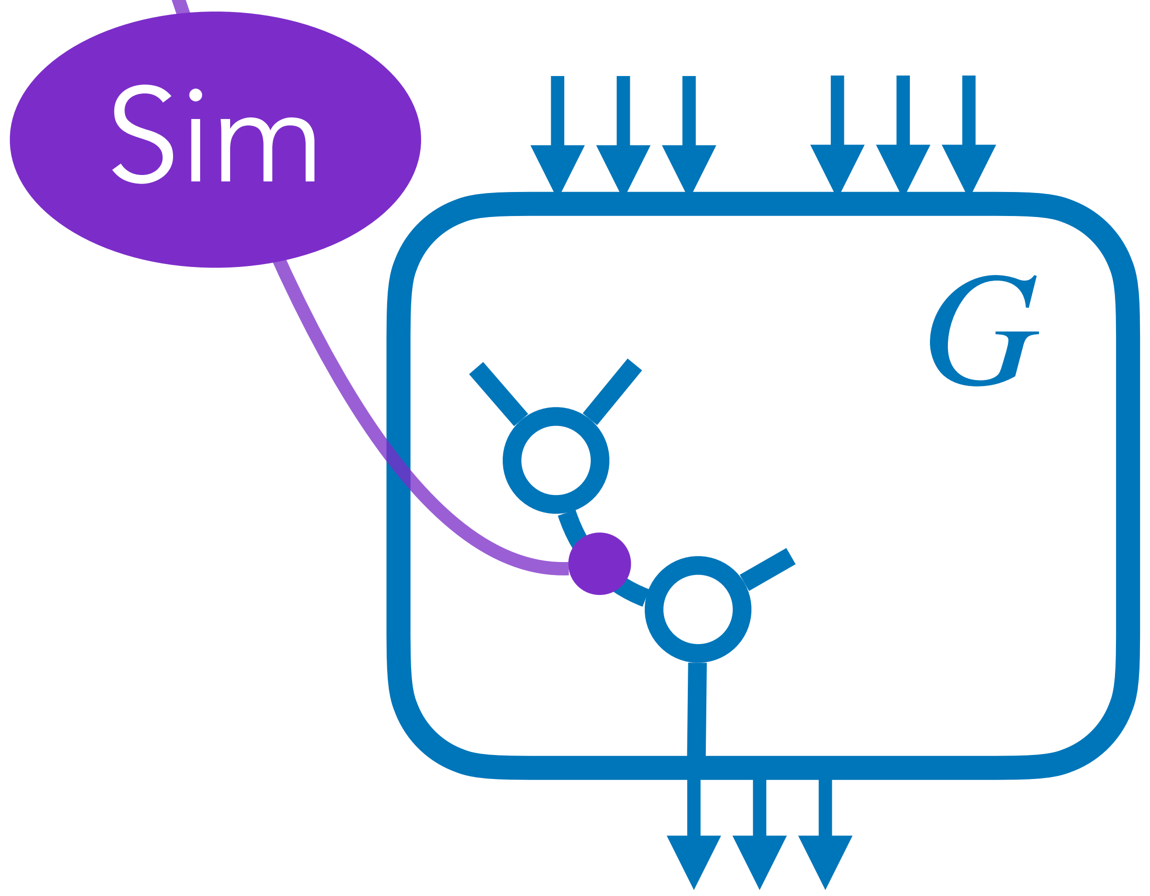


how to simulate this share?

$x_1 + x_2 + x_3 = x$

💡 *ask x to the simulation of G*

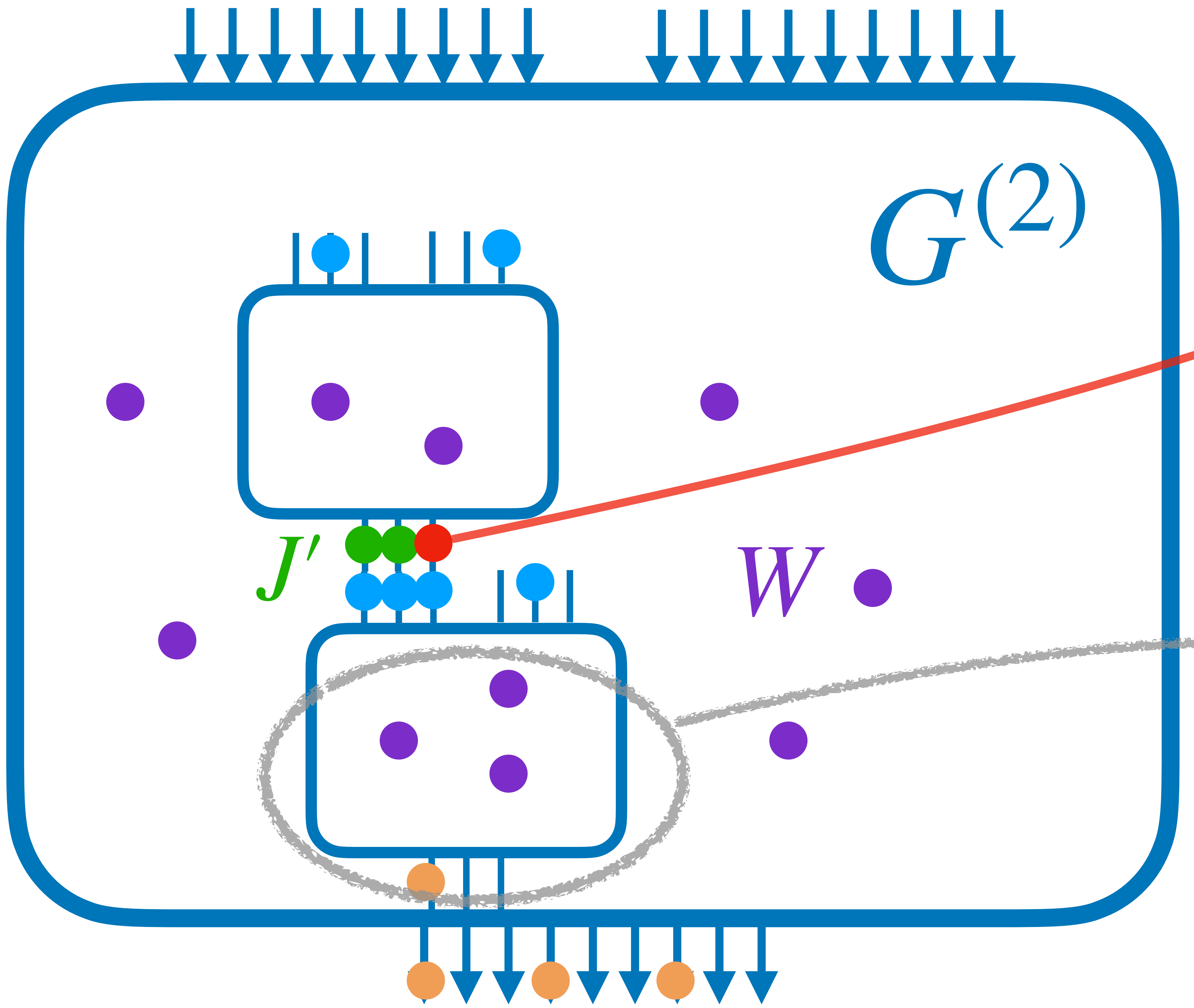
needs all the left input shares



Expansion security

Base gadget $\{G\}$ f-RPE $\Rightarrow$ expanded gadgets $\{G^{(2)}\}$ f^2-RPE

Now what if a failure occurs ?

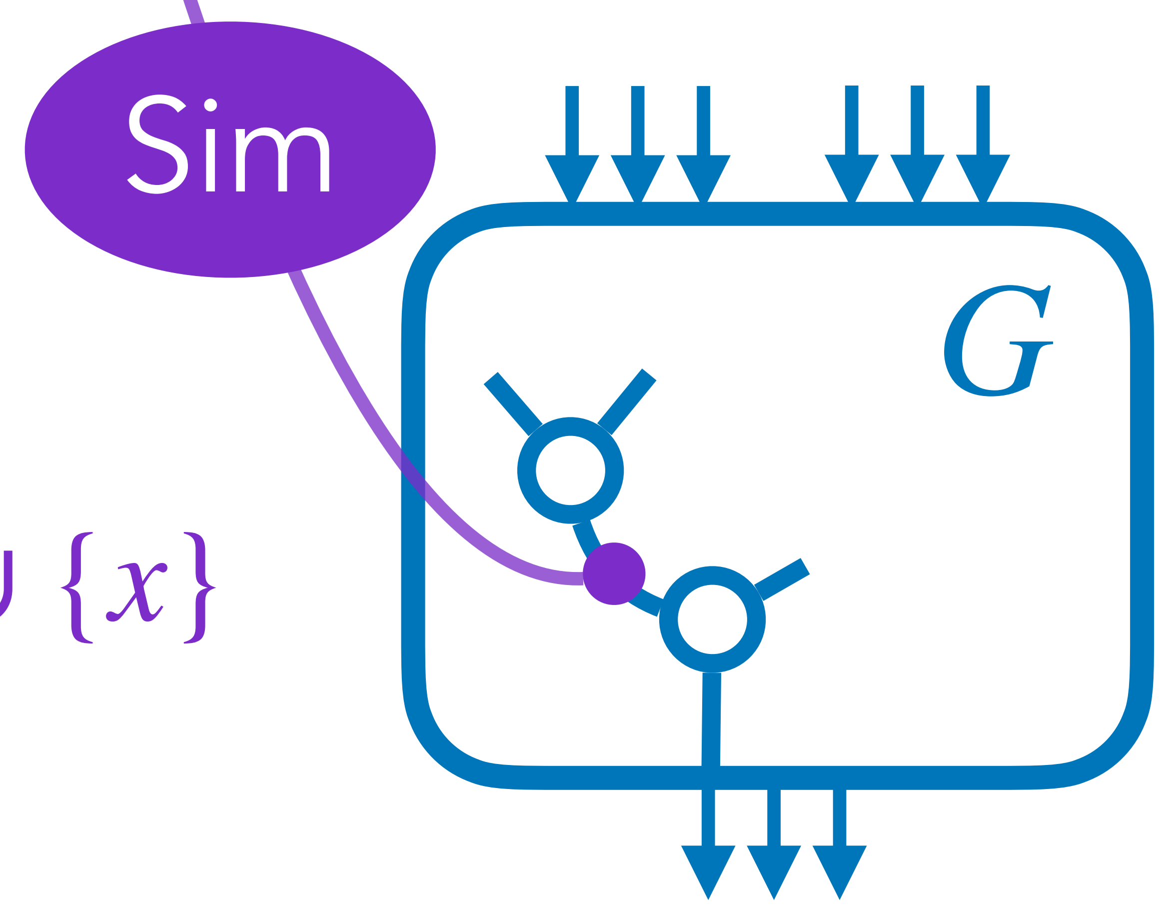


how to simulate this share?

$x_1 + x_2 + x_3 = x$

ask x to the simulation of G

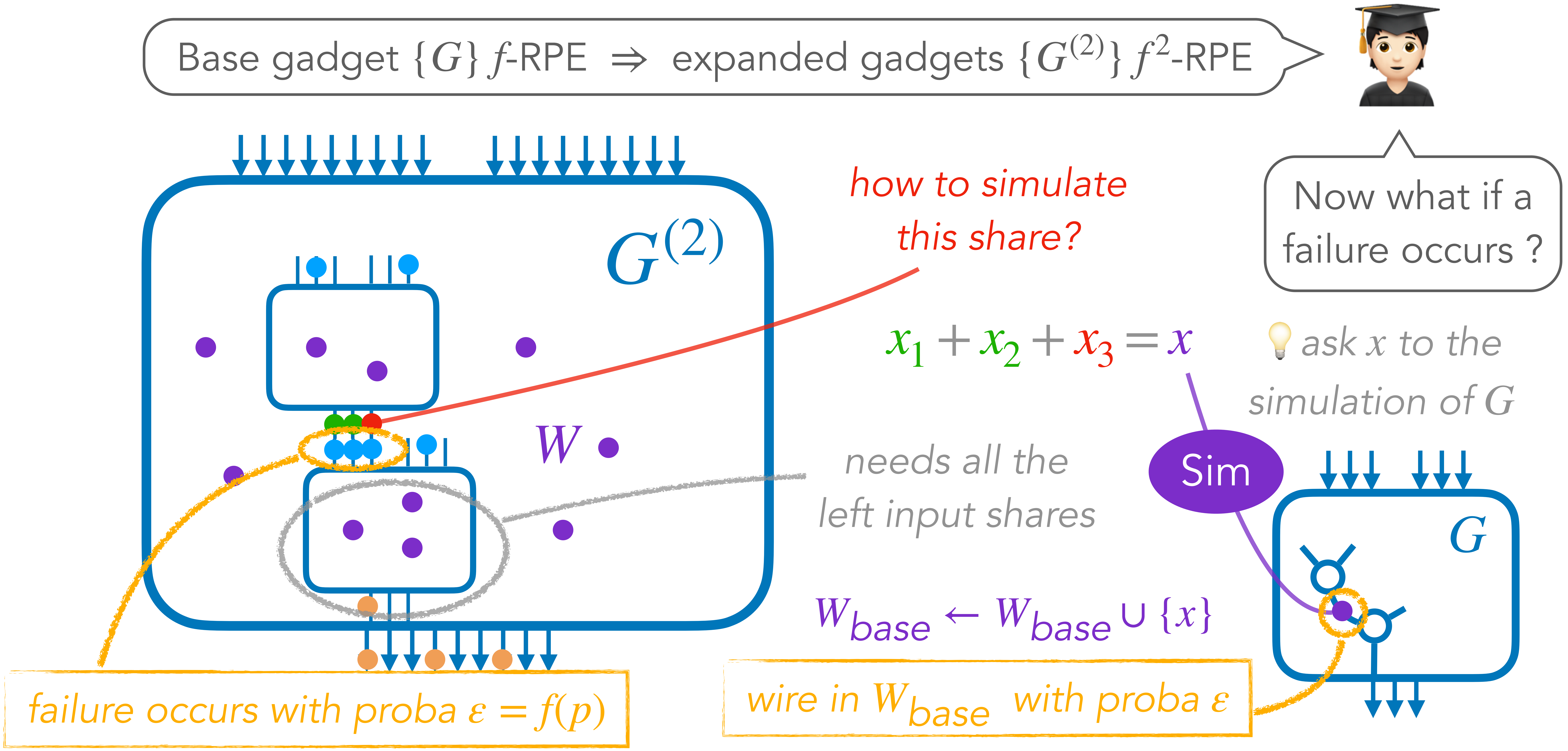
needs all the left input shares



$W_{base} \leftarrow W_{base} \cup \{x\}$

Expansion security

Base gadget $\{G\}$ f-RPE $\Rightarrow$ expanded gadgets $\{G^{(2)}\}$ f^2-RPE



Expansion security

- Failure probability:

$$\Pr\left(\text{Sim-}G^{(2)}\text{ fails}\right) = \Pr\left(\text{Sim-}G\text{ fails on }W_{\text{base}}\right)$$

Expansion security

$\sim \mathsf{LeakingWires}(\varepsilon)$

- Failure probability:

$$\Pr\left(\text{Sim-}G^{(2)} \text{ fails}\right) = \Pr\left(\text{Sim-}G \text{ fails on } W_{\text{base}}\right)$$

Expansion security

$\sim \text{LeakingWires}(\varepsilon)$

- Failure probability:

$$\Pr\left(\text{Sim-}G^{(2)} \text{ fails}\right) = \Pr\left(\text{Sim-}G \text{ fails on } W_{\text{base}}\right)$$
$$= f(\varepsilon) = f\left(f(p)\right)$$

Expansion security

$\sim$ LeakingWires(ε)

- Failure probability:

$$\Pr\left(\text{Sim-}G^{(2)} \text{ fails}\right) = \Pr\left(\text{Sim-}G \text{ fails on } W_{\text{base}}\right)$$
$$= f(\varepsilon) = f\left(f(p)\right)$$

- $G^{(2)}$ is $f^{(2)}$-RPE

Expansion security

$\sim$ LeakingWires(ε)

- Failure probability:

$$\Pr\left(\text{Sim-}G^{(2)}\text{ fails}\right) = \Pr\left(\text{Sim-}G\text{ fails on }W_{\text{base}}\right)$$
$$= f(\varepsilon) = f\left(f(p)\right)$$

- $G^{(2)}$ is $f^{(2)}$-RPE

- By induction $G^{(k)}$ is $f^{(k)}$-RPE

Complexity analysis

Choosing k s.t. $f^{(k)}(p) \leq 2^{-\kappa}$

$$\Rightarrow \quad |\hat{C}| = \mathcal{O}(|C| \cdot \kappa^{e}) \quad \text{with} \quad e = \frac{\log \lambda_{max}}{\log d}$$

Complexity analysis

κ-bit security

Choosing k s.t. $f^{(k)}(p) \leq 2^{-\kappa}$

$$\Rightarrow \quad |\hat{C}| = \mathcal{O}(|C| \cdot \kappa^e) \quad \text{with} \quad e = \frac{\log \lambda_{max}}{\log d}$$

Complexity analysis

κ-bit security

max eigenvalue
in gate-count
matrix

Choosing k s.t. $f^{(k)}(p) \leq 2^{-\kappa}$

$$\Rightarrow \quad |\hat{C}| = \mathcal{O}(|C| \cdot \kappa^{e}) \quad \text{with} \quad e = \frac{\log \lambda_{max}}{\log d}$$

Complexity analysis

κ-bit security

max eigenvalue
in gate-count
matrix

Choosing k s.t. $f^{(k)}(p) \leq 2^{-\kappa}$

$$\Rightarrow \quad |\hat{C}| = \mathcal{O}(|C| \cdot \kappa^{e}) \quad \text{with} \quad e = \frac{\log \lambda_{max}}{\log d}$$

amplification order

$$\boxed{f(p) = c_d\, p^d + \mathcal{O}(p^{d+o(1)})}$$

Complexity analysis

Design guidelines:

- maximize amplification order d
- minimize max eigenvalue λ_{max}

Complexity analysis

Upper bound: $d \leq \dfrac{n+1}{2}$

Design guidelines:

- maximize amplification order d
- minimize max eigenvalue λ_{max}

Complexity analysis

Upper bound: $d \leq \dfrac{n+1}{2}$

Design guidelines:

- maximize amplification order d
- minimize max eigenvalue λ_{max}

$$M = \begin{pmatrix} aa & ac & * & 0 \\ ca & cc & * & 0 \\ 0 & 0 & n^2 & 0 \\ * & * & * & n \end{pmatrix} \quad \Rightarrow \begin{cases} (\lambda_1, \lambda_2) = \mathrm{ev}\begin{pmatrix} aa & ac \\ ca & cc \end{pmatrix} \\ \lambda_3 = n^2, \quad \lambda_4 = n \end{cases}$$

Complexity analysis

Upper bound: $d \leq \dfrac{n+1}{2}$

Design guidelines:

- maximize amplification order d
- minimize max eigenvalue λ_{max}

$$M = \begin{pmatrix} \boxed{\begin{matrix} aa & ac \\ ca & cc \end{matrix}} & \begin{matrix} * \\ * \end{matrix} & \begin{matrix} 0 \\ 0 \end{matrix} \\ \begin{matrix} 0 & \quad 0 \end{matrix} & \boxed{n^2} & 0 \\ \begin{matrix} * & \quad * \end{matrix} & * & \boxed{n} \end{pmatrix} \quad \Rightarrow \quad \begin{cases} (\lambda_1, \lambda_2) = \text{ev}\begin{pmatrix} \boxed{\begin{matrix} aa & ac \\ ca & cc \end{matrix}} \end{pmatrix} \\ \lambda_3 = \boxed{n^2}, \quad \lambda_4 = \boxed{n} \end{cases}$$

Complexity analysis

Upper bound: $d \leq \dfrac{n+1}{2}$

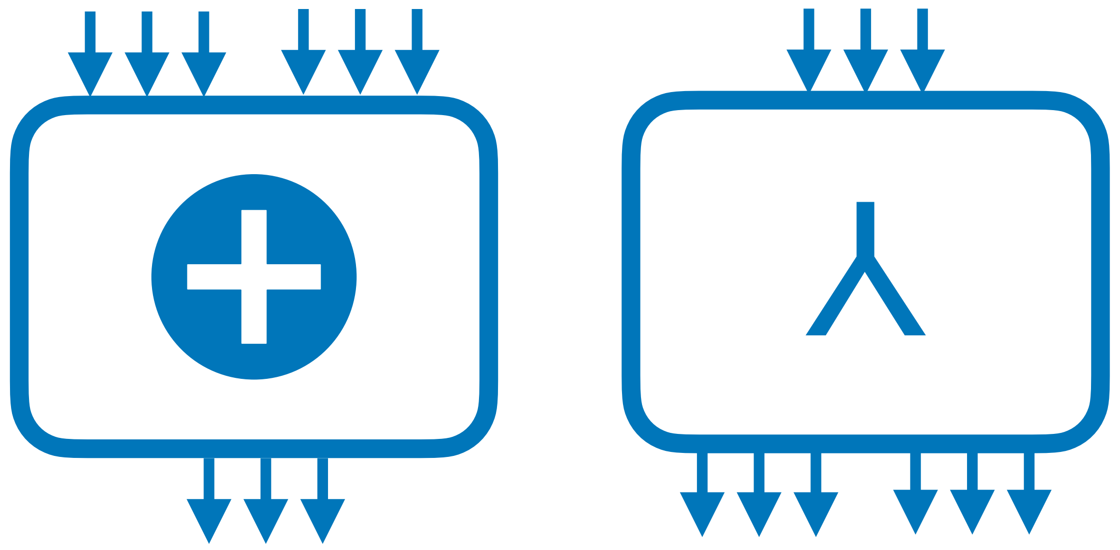
Design guidelines:

- maximize amplification order d
- minimize max eigenvalue λ_{max}

$$M = \begin{pmatrix} aa & ac & * & 0 \\ ca & cc & * & 0 \\ 0 & 0 & n^2 & 0 \\ * & * & * & n \end{pmatrix} \quad \Rightarrow \quad \begin{cases} (\lambda_1, \lambda_2) = \text{ev} \begin{pmatrix} aa & ac \\ ca & cc \end{pmatrix} \\ \lambda_3 = n^2, \quad \lambda_4 = n \end{cases}$$

💡 *we can be greedy in randomness*

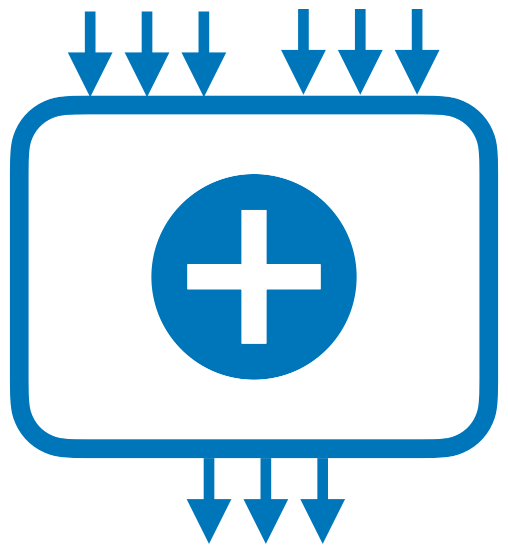
Generic constructions

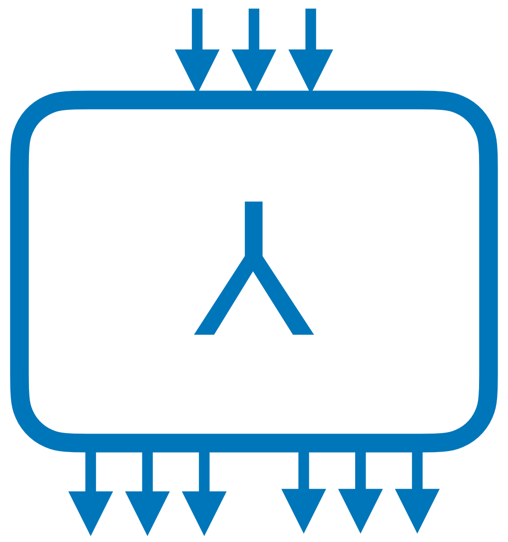


$$G_{\oplus}(\overrightarrow{x}, \overrightarrow{y}) = G_{\mathsf{R}}(\overrightarrow{x}) + G_{\mathsf{R}}(\overrightarrow{y})$$

$$G_{\curlywedge}(\overrightarrow{x}) = (G_{\mathsf{R}}(\overrightarrow{x}), G_{\mathsf{R}}(\overrightarrow{x}))$$

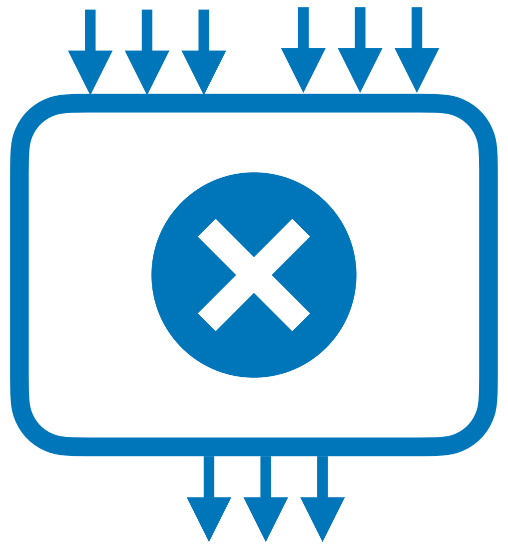
Generic constructions





$$G_{\oplus}(\overrightarrow{x}, \overrightarrow{y}) = G_{\mathsf{R}}(\overrightarrow{x}) + G_{\mathsf{R}}(\overrightarrow{y})$$

$$G_{\curlywedge}(\overrightarrow{x}) = (G_{\mathsf{R}}(\overrightarrow{x}), G_{\mathsf{R}}(\overrightarrow{x}))$$



$$G_{\otimes}(\overrightarrow{x}, \overrightarrow{y}) \mapsto \begin{pmatrix} x_1 \cdot G_{\mathsf{R}}(\overrightarrow{y}) \\ x_2 \cdot G_{\mathsf{R}}(\overrightarrow{y}) \\ \vdots \\ x_n \cdot G_{\mathsf{R}}(\overrightarrow{y}) \end{pmatrix} \; + \text{ greedy use of randomness}$$

Generic constructions

- Optimal amplification order $d = \dfrac{n+1}{2}$
- Max eigenvalue:

$$M = \begin{pmatrix} aa & ac & * & 0 \\ ca & cc & * & 0 \\ 0 & 0 & n^2 & 0 \\ * & * & * & n \end{pmatrix} \Rightarrow \begin{cases} (\lambda_1, \lambda_2) = \mathrm{ev}\begin{pmatrix} aa & ac \\ ca & cc \end{pmatrix} \\ \lambda_3 = n^2, \quad \lambda_4 = n \end{cases}$$

$\mathcal{O}(n \log n)$

$n^2 \Rightarrow$ *asymptotic bottleneck*

- Complexity $\mathcal{O}(|C| \cdot \kappa^e)$ with $e = \dfrac{\log \lambda_{max}}{\log d} \xrightarrow{n\to\infty} 2$

Generic constructions

- Optimal amplification order $d = \dfrac{n+1}{2}$

For some large enough $\mathbb{F}$

Belaïd, Rivain, Taleb, Vergnaud - ASIACRYPT 2021

- Max eigenvalue:

$$M = \begin{pmatrix} aa & ac & * & 0 \\ ca & cc & * & 0 \\ 0 & 0 & n^2 & 0 \\ * & * & * & n \end{pmatrix} \Rightarrow \begin{cases} (\lambda_1, \lambda_2) = \text{ev}\begin{pmatrix} aa & ac \\ ca & cc \end{pmatrix} \\ \lambda_3 = \mathcal{O}(n) \end{cases}$$

$\mathcal{O}(n \log n)$

$n^2 \Rightarrow$ *asymptotic bottleneck*

- Complexity $\mathcal{O}(|C| \cdot \kappa^e)$ with $e = \dfrac{\log \lambda_{max}}{\log d} \xrightarrow{n \to \infty} 1$

Efficient instantiations

3-share gadgets

$$\left.\begin{aligned} G_{\mathsf{R}} : z_1 &\leftarrow r_1 + x_1 \\ z_2 &\leftarrow r_2 + x_2 \\ z_3 &\leftarrow (r_1 + r_2) + x_3 \end{aligned}\right\} \Rightarrow \mathcal{O}(|C|\kappa^{3.9}), \quad p_{max} = 2^{-7.5}$$

5-share gadgets

$$\left.\begin{aligned} G_{\mathsf{R}} : z_1 &\leftarrow (r_1 + r_2) + x_1 \\ z_2 &\leftarrow (r_2 + r_3) + x_2 \\ z_3 &\leftarrow (r_3 + r_4) + x_3 \\ z_4 &\leftarrow (r_4 + r_5) + x_4 \\ z_5 &\leftarrow (r_5 + r_1) + x_5 \end{aligned}\right\} \Rightarrow \mathcal{O}(|C|\kappa^{3.2}), \quad p_{max} = 2^{-12}$$

Conclusion

Contributions

- Efficient tight probing-secure masked implementations
- Formalisation of noisy side-channel leakage
- Provable security against noisy leakage

Perspectives

- Bridging the gap between theory and practice
- Improving the practical efficiency of noisy-leakage secure schemes
- Formal verification methods for noisy-leakage secure schemes
- Provable security against more powerful adversary (fault attacks / white-box model)