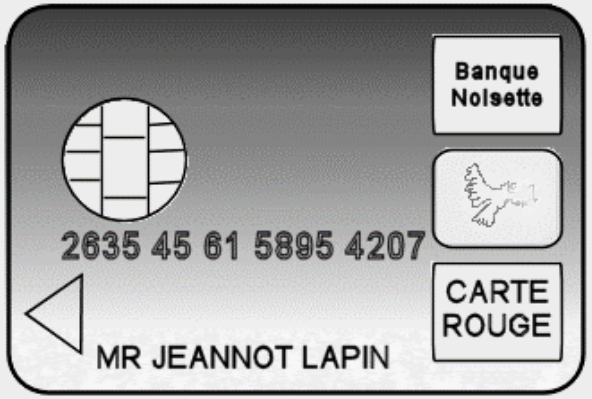
Randomness Complexity of Private Circuits for Multiplication

Sonia Belaïd, Fabrice Benhamouda, Alain Passelègue, Emmanuel Prouff, **Adrian Thillard**, Damien Vergnaud

electronic devices

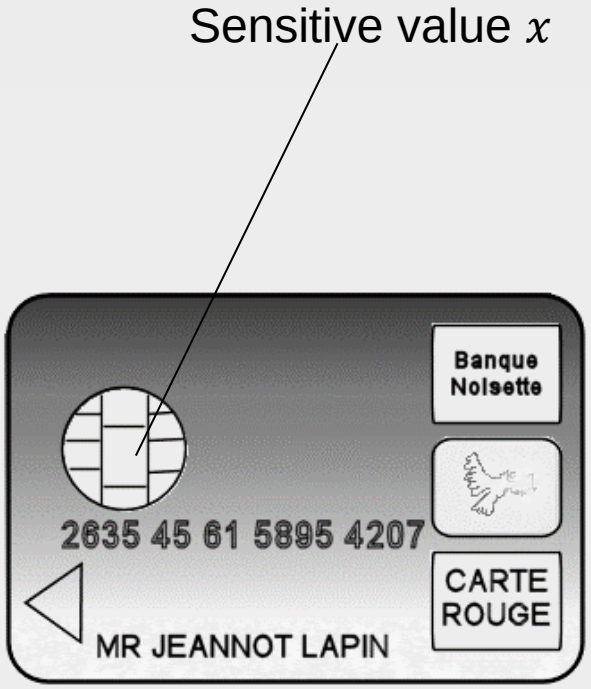


- cryptography is implemented

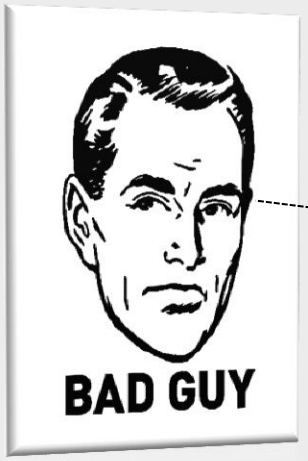
- intermediate values actually exist !

- physical phenomenons
(consumption, EM, timing…)
[Koc 90s]

noisy leakage model

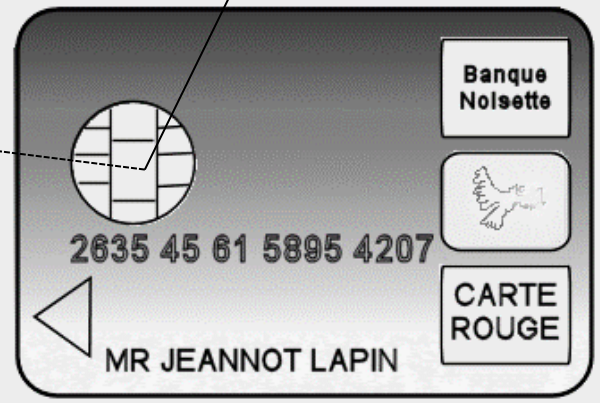


noisy leakage model

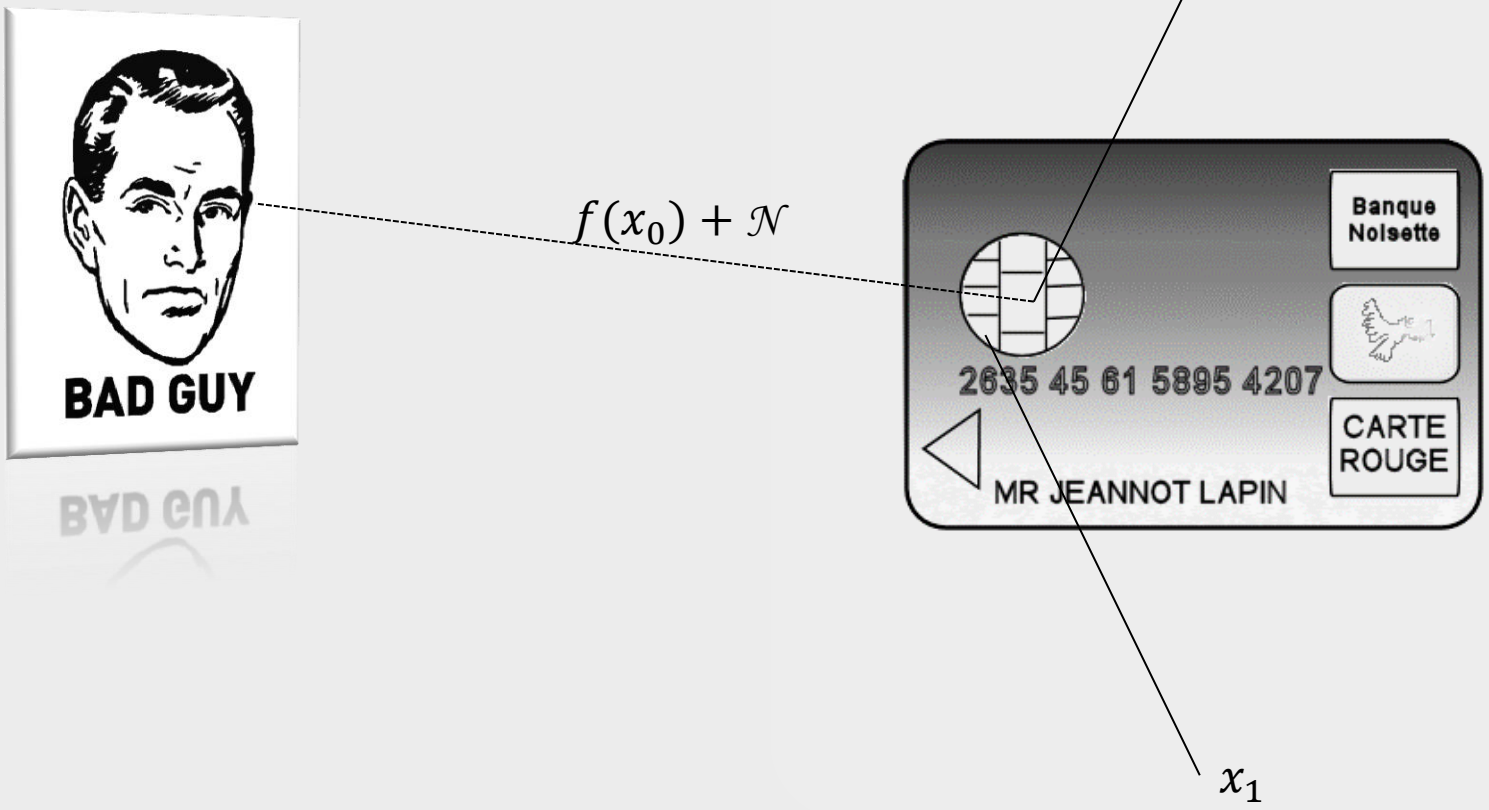


$f(x) + \mathcal{N}$

x

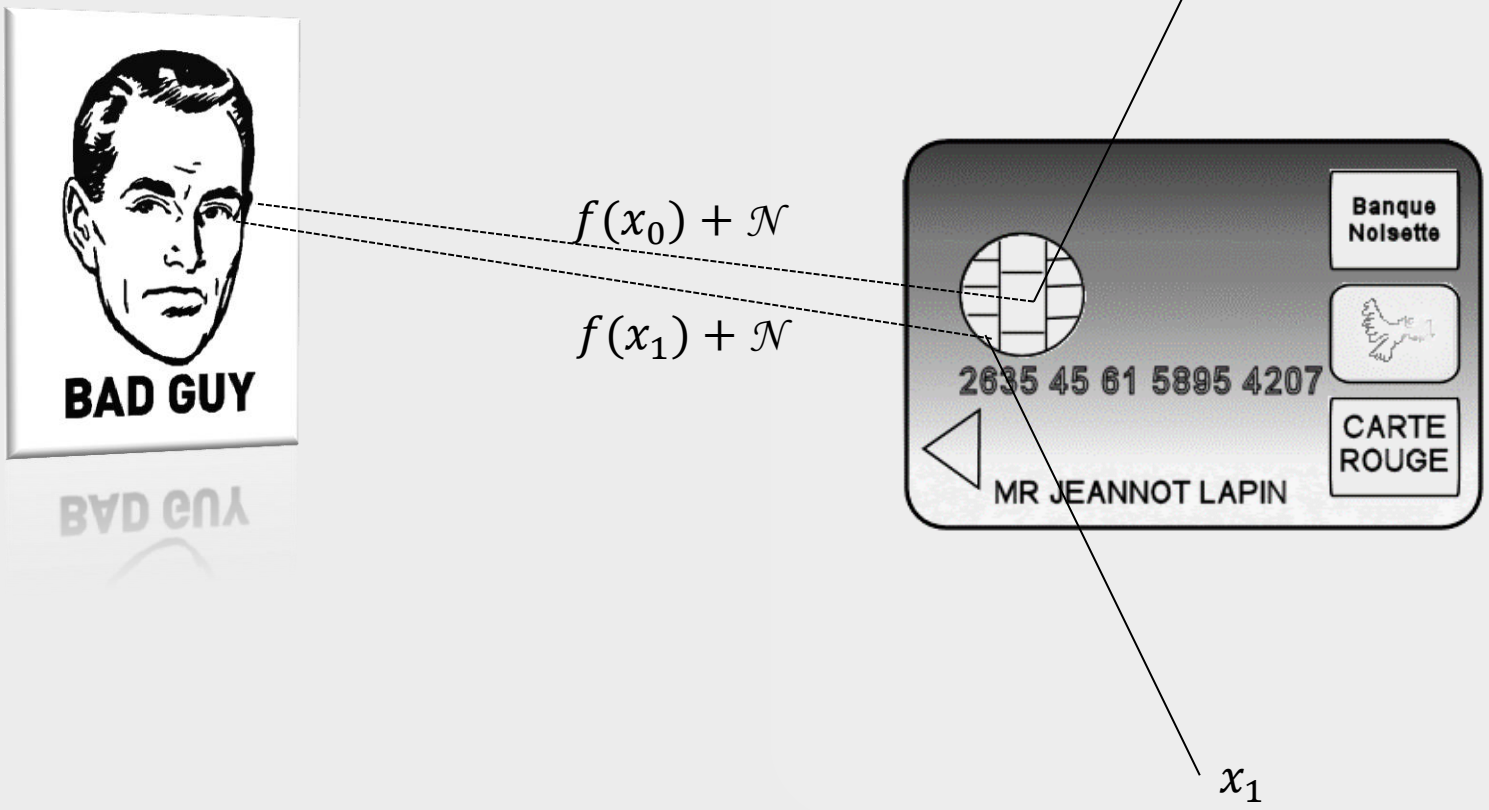


noisy leakage model



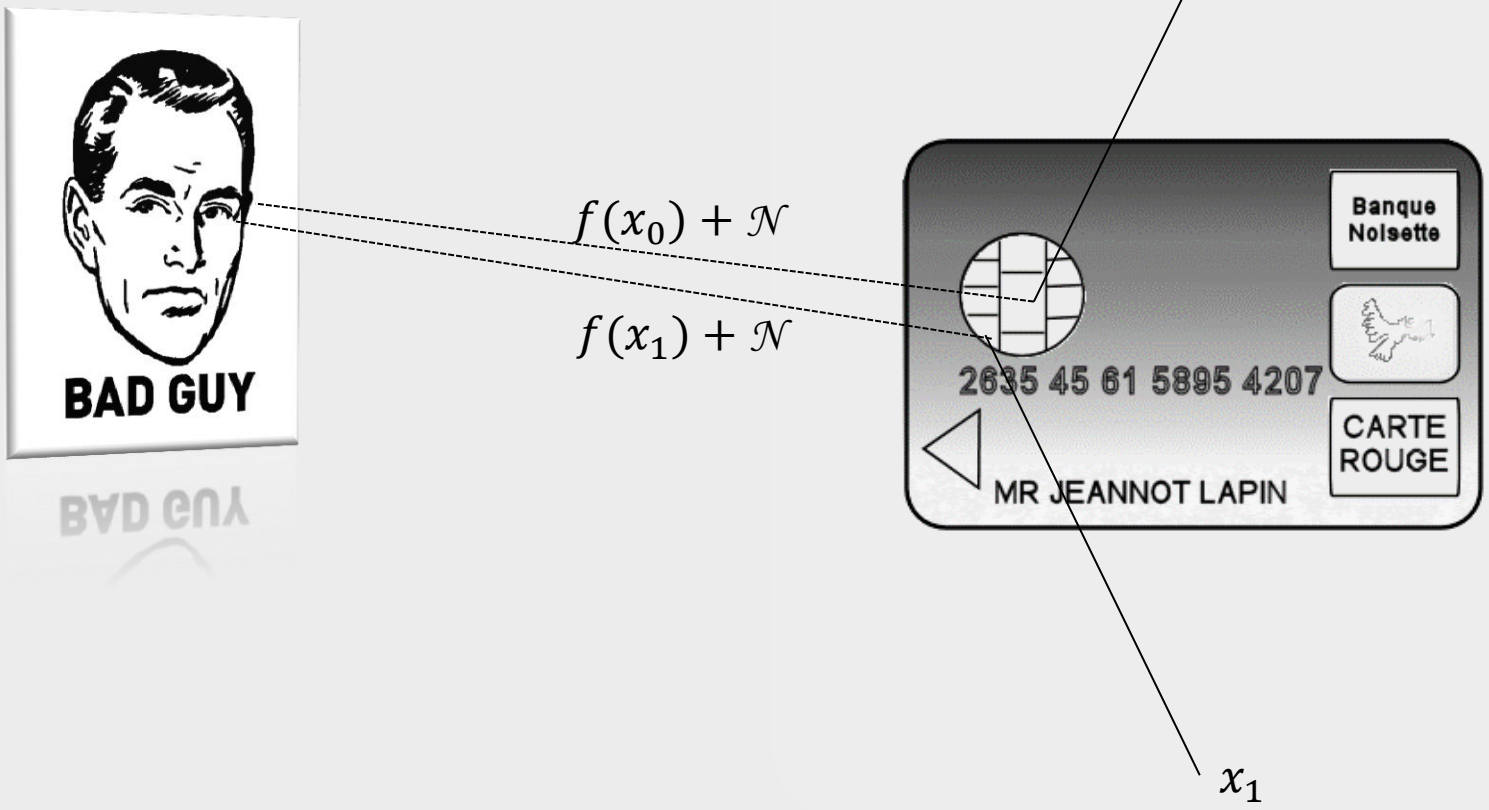
we split the sensitive value such that $x = x_0 \oplus x_1$

noisy leakage model



we split the sensitive value such that $x = x_0 \oplus x_1$

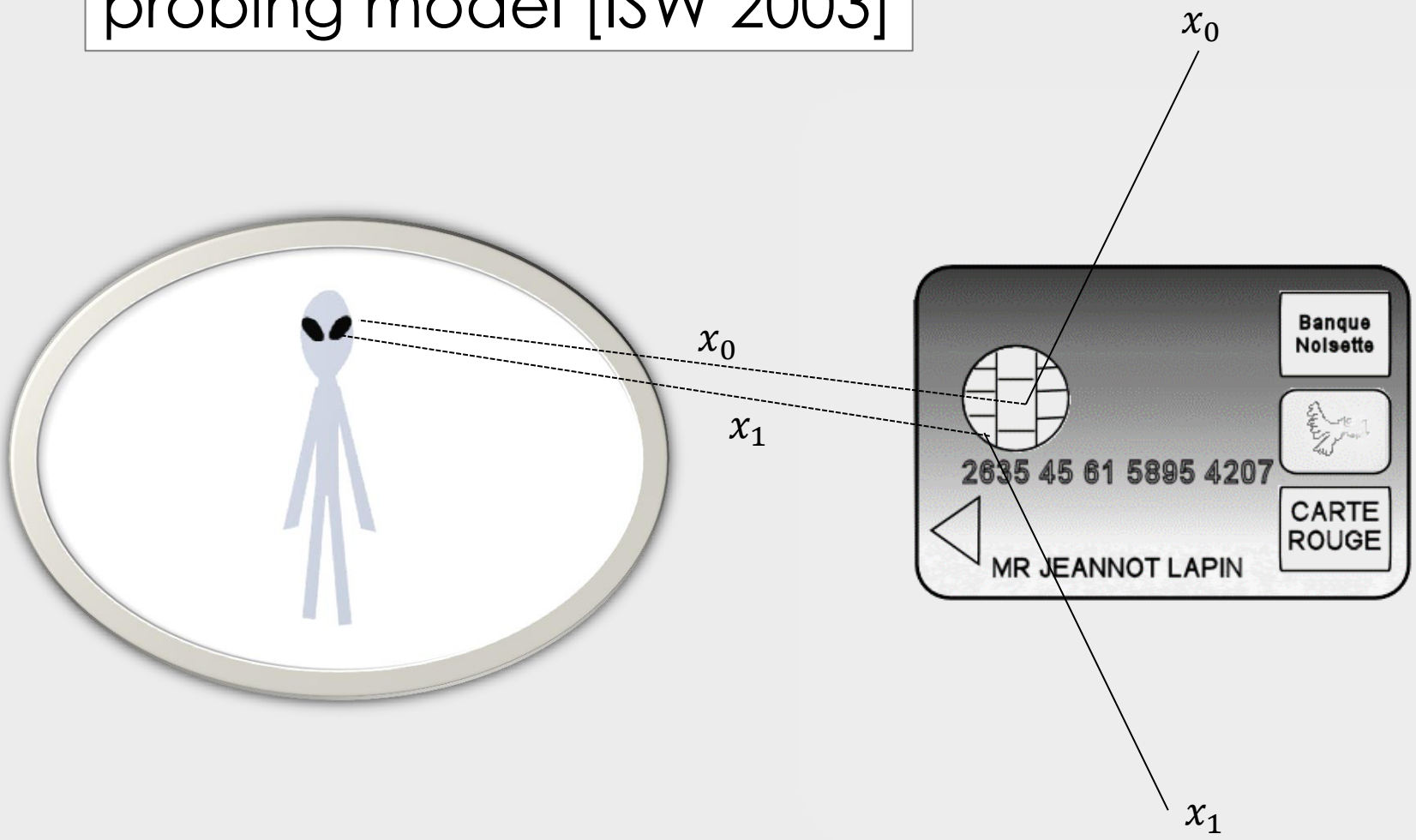
noisy leakage model



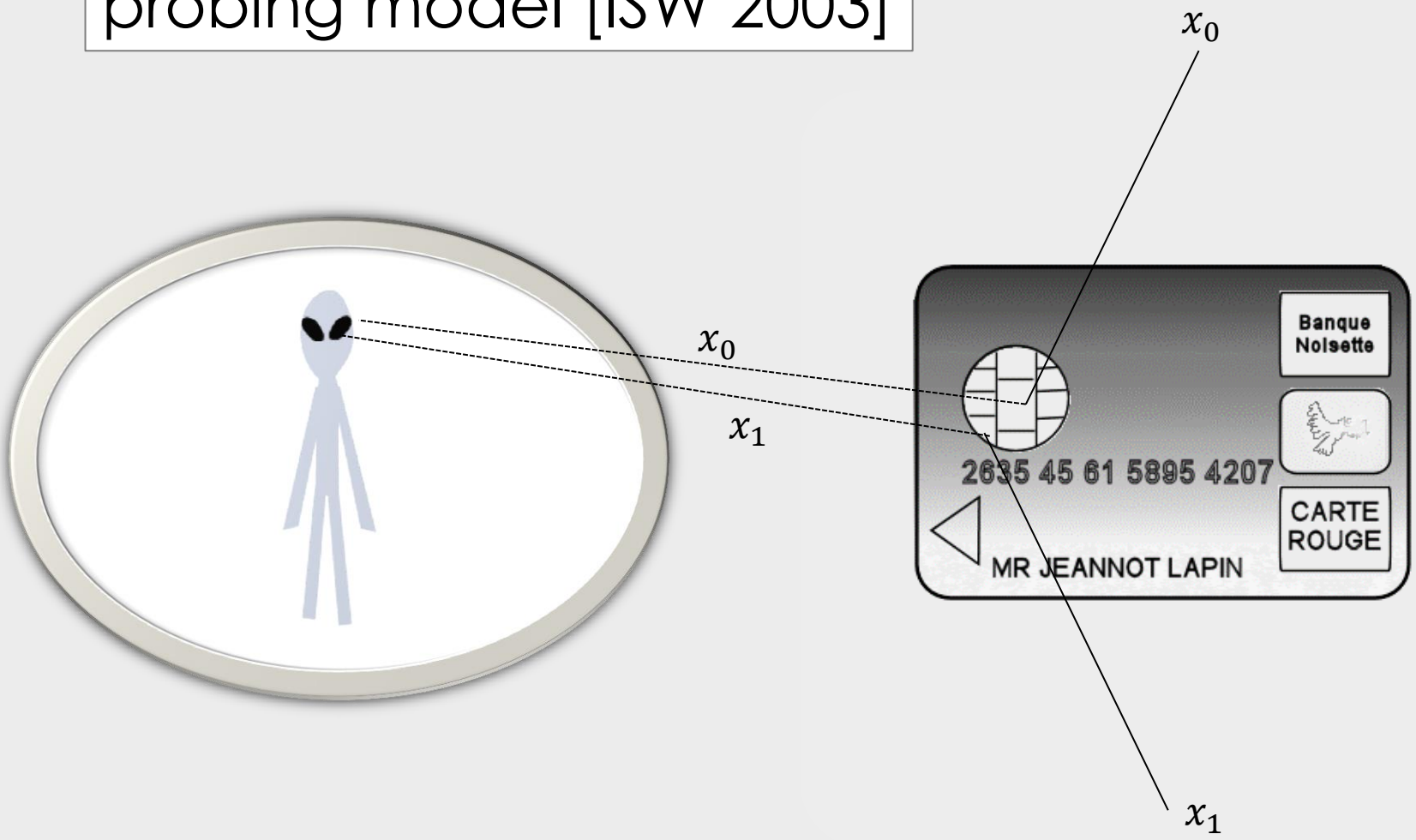
we split the sensitive value such that $x = x_0 \oplus x_1$

information is bounded, bound exponential in nb of observations [Chari et al.99, PR13]

probing model [ISW 2003]



probing model [ISW 2003]



secure against probing ⇒ secure against noisy leakage for a certain amount of $\mathcal{N}$ [Duc et al14]

key-idea:

for security at order d, split sensitive data x into $d + 1$ **random** variables (shares) s.t.

$$x = x_0 \oplus x_1 \oplus \cdots \oplus x_d$$

key-idea:
for security at order d, split sensitive data x into $d + 1$ **random** variables (shares) s.t.

$$x = x_0 \oplus x_1 \oplus \cdots \oplus x_d$$

d -privacy:
compute $f(x)$ from $x_0, x_1, \ldots, x_d$ s.t. the computation still resists to d observations

key-idea:
for security at order d, split sensitive data x into $d + 1$ **random** variables (shares) s.t.

$$x = x_0 \oplus x_1 \oplus \cdots \oplus x_d$$

d -privacy:
compute $f(x)$ from $x_0, x_1, \ldots, x_d$ s.t. the computation still resists to d observations

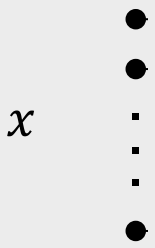
for two computations on two inputs, the two sets of d observations must follow the same statistical distribution

private circuits

$f: \{0,1\}^n \to \{0,1\}^m$

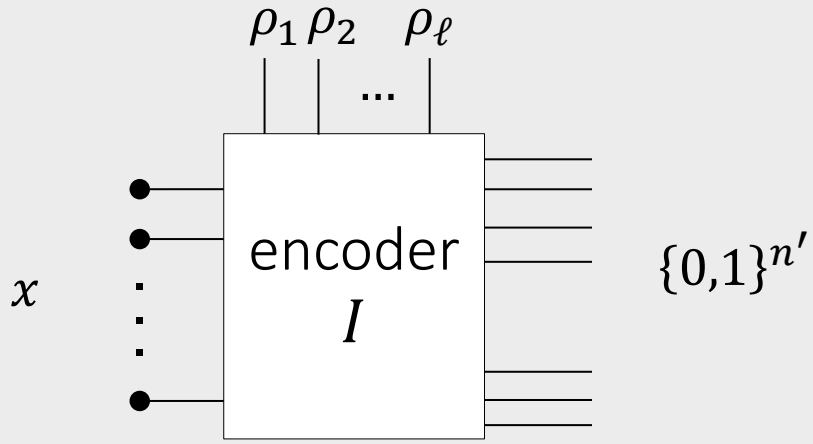
private circuits

$f: \{0,1\}^n \to \{0,1\}^m$



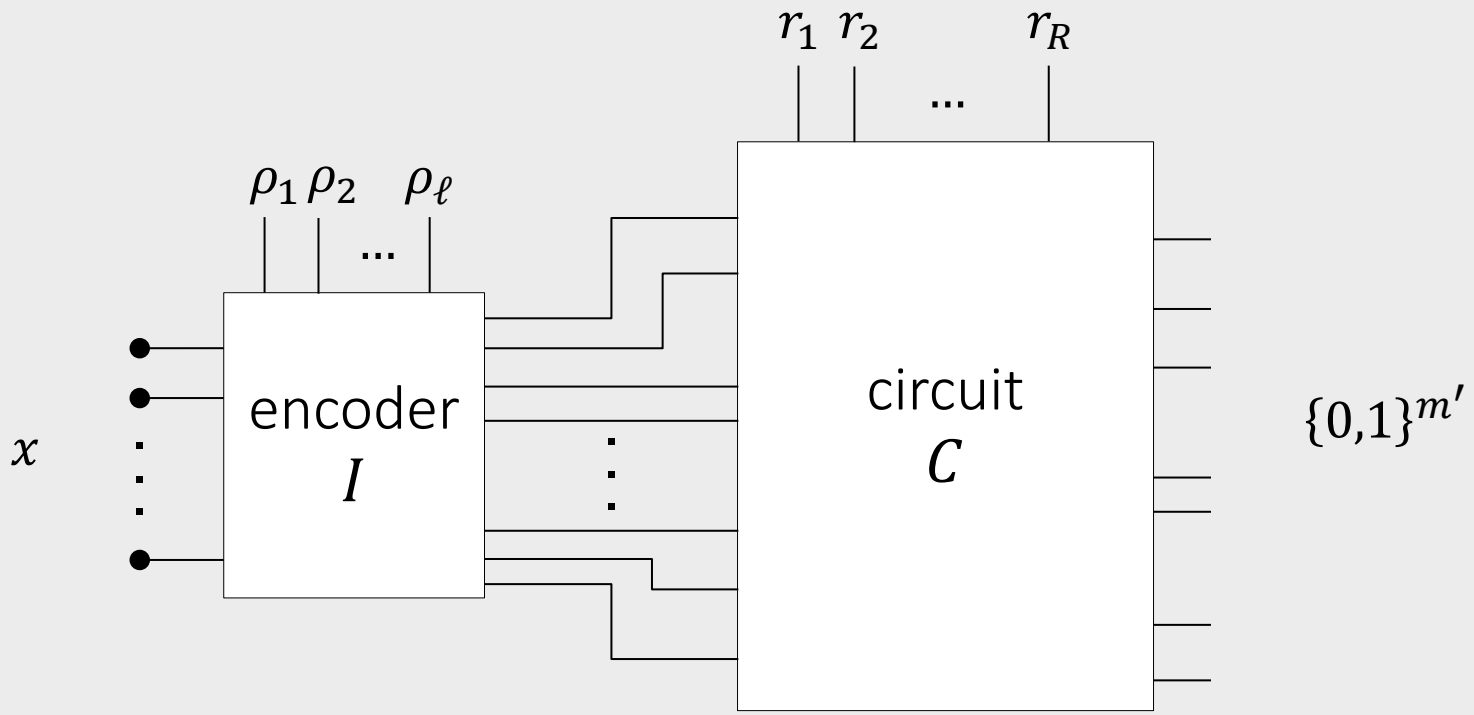
private circuits

$f: \{0,1\}^n \to \{0,1\}^m$



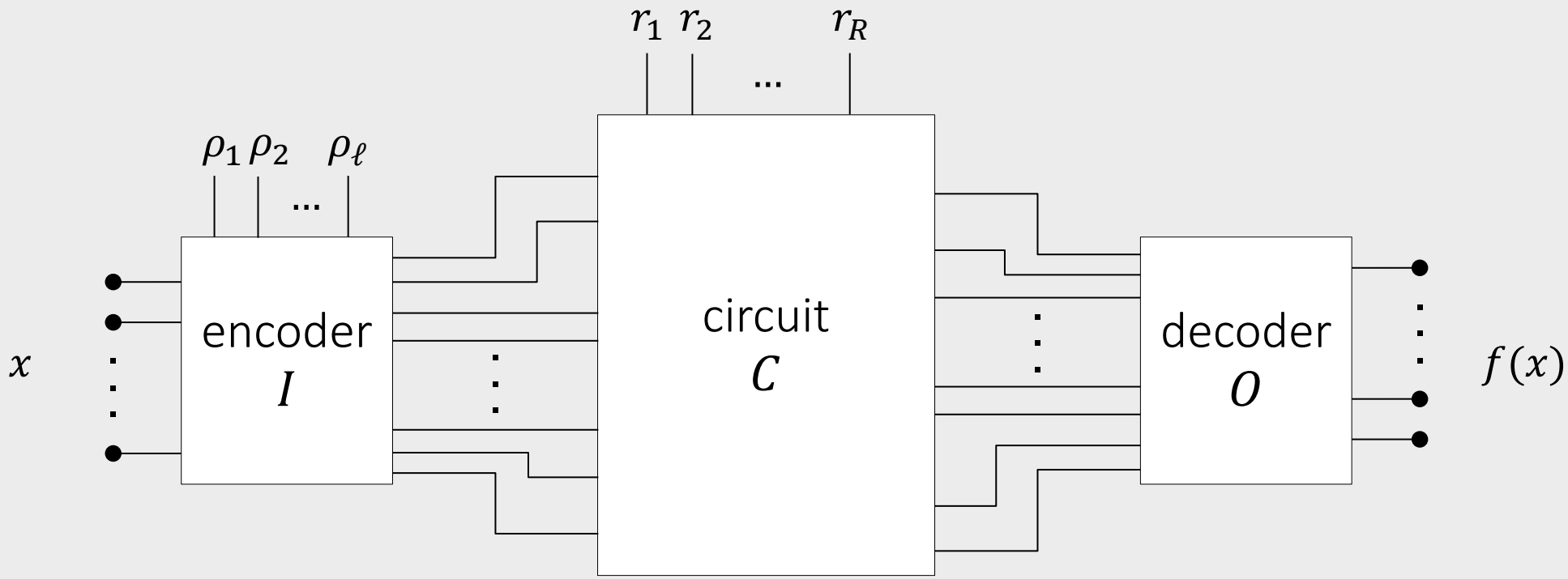
private circuits

$f: \{0,1\}^n \to \{0,1\}^m$



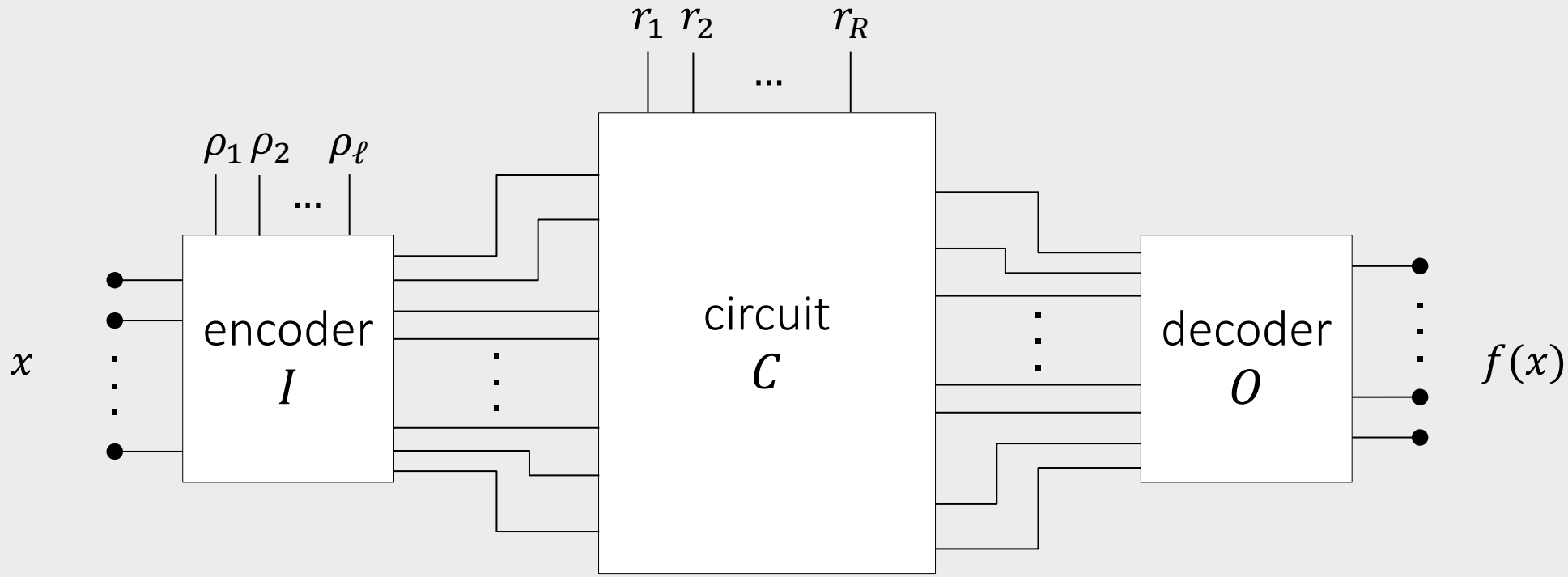
private circuits

$f: \{0,1\}^n \to \{0,1\}^m$



private circuits

$f: \{0,1\}^n \to \{0,1\}^m$



correctness

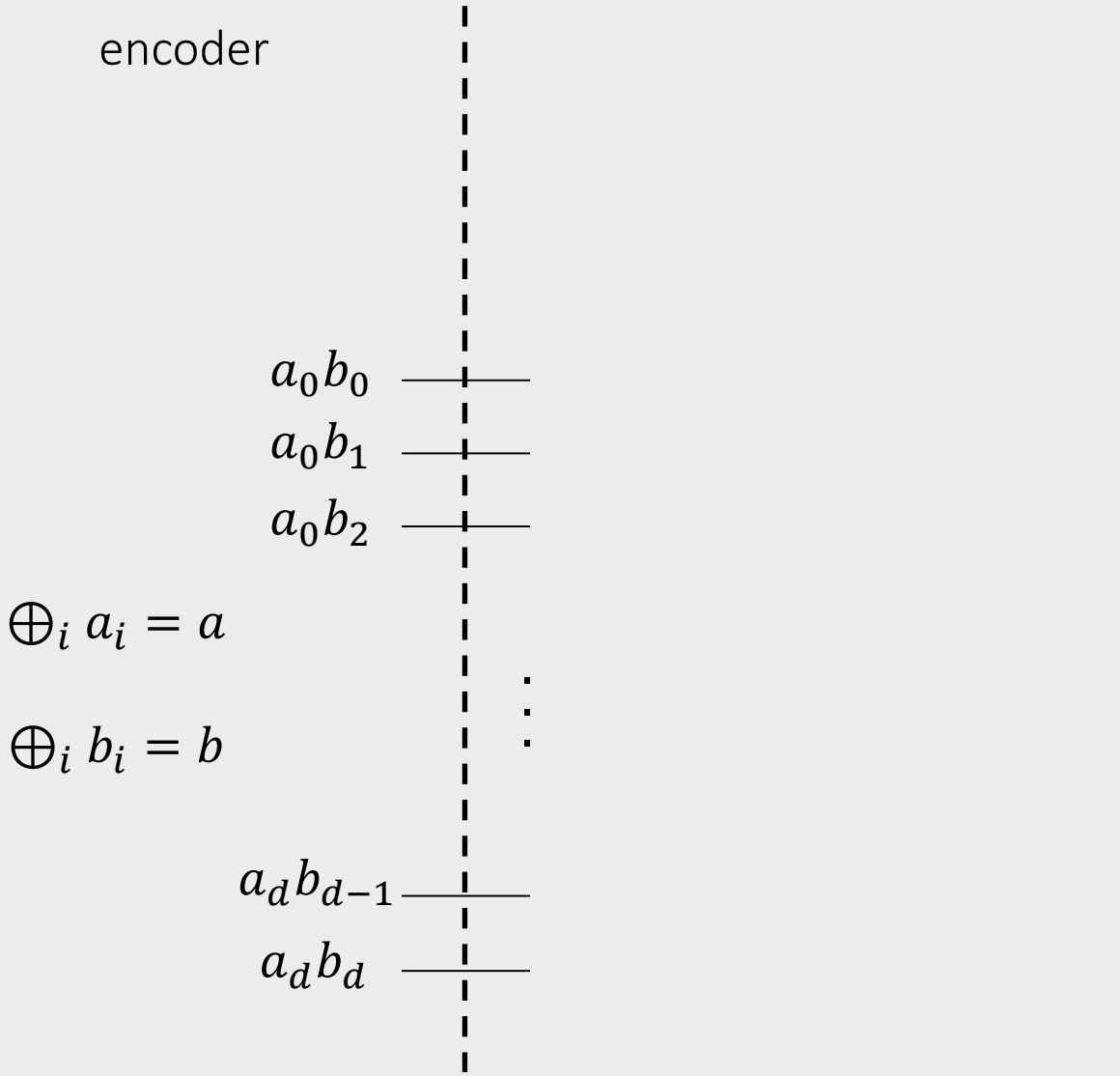
d-privacy

this paper

$$(a, b) \in \{0,1\}^2 \mapsto a \cdot b \in \{0,1\}$$

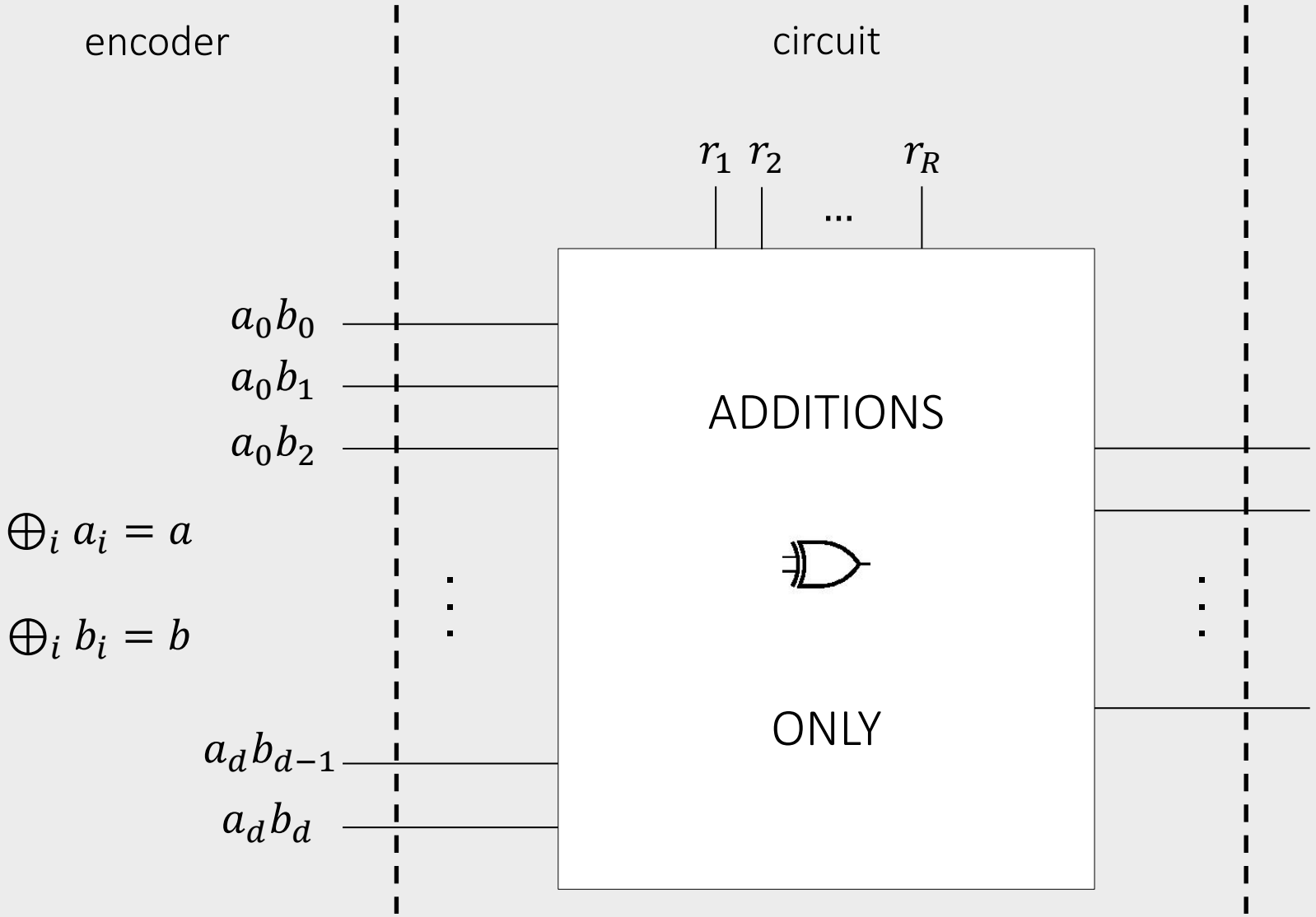
this paper

$$(a, b) \in \{0,1\}^2 \mapsto a \cdot b \in \{0,1\}$$



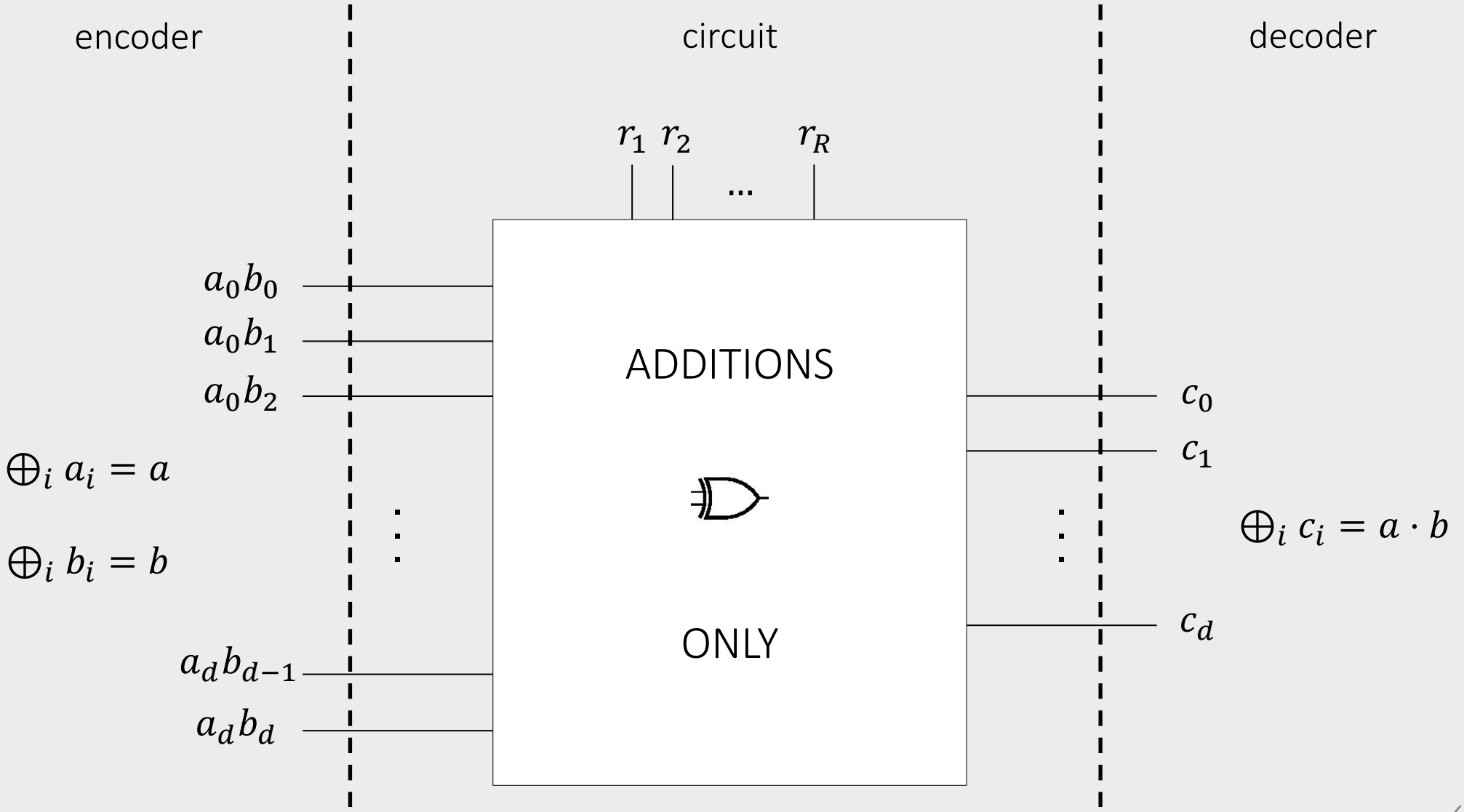
this paper

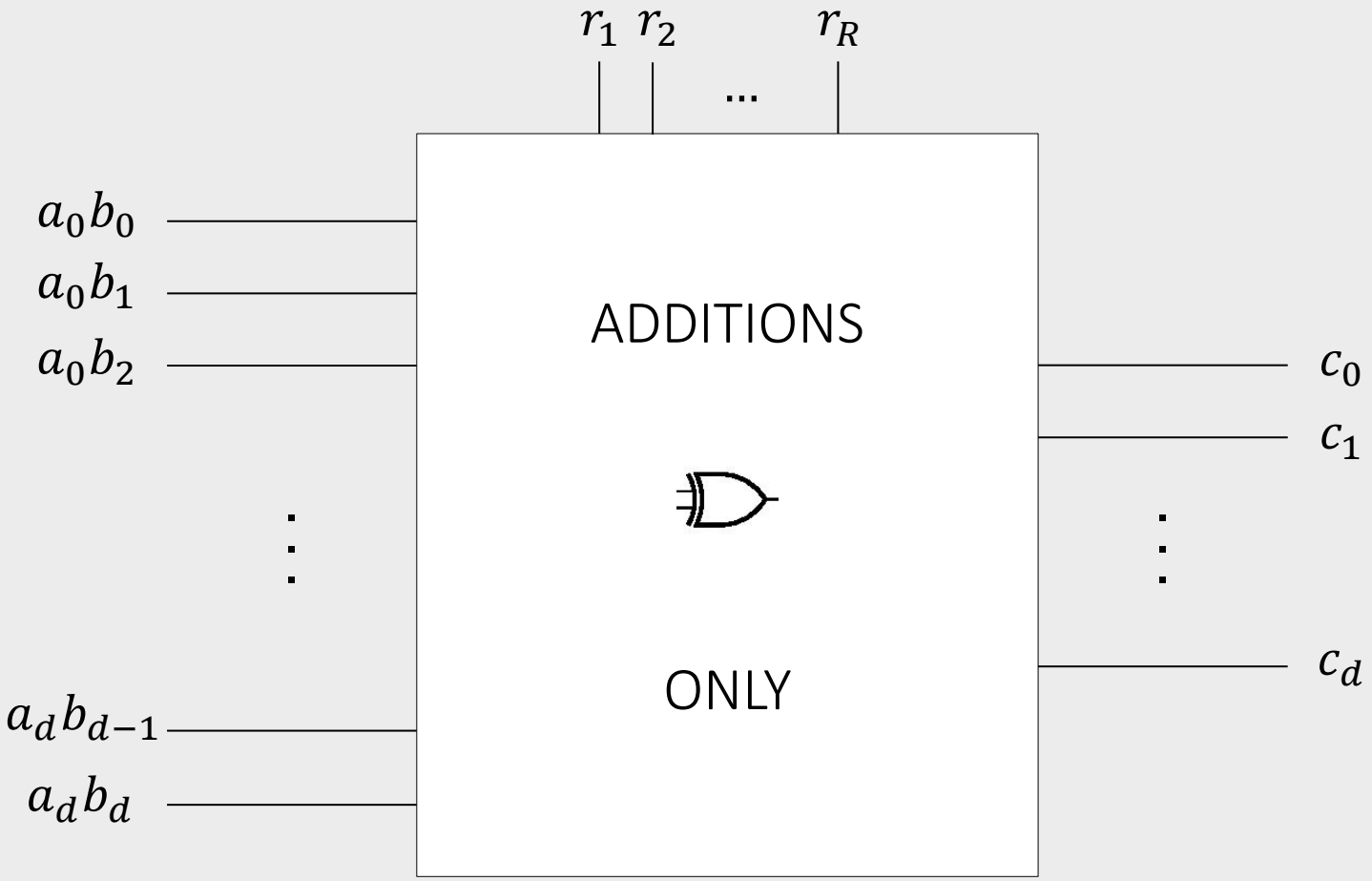
$$(a, b) \in \{0,1\}^2 \mapsto a \cdot b \in \{0,1\}$$

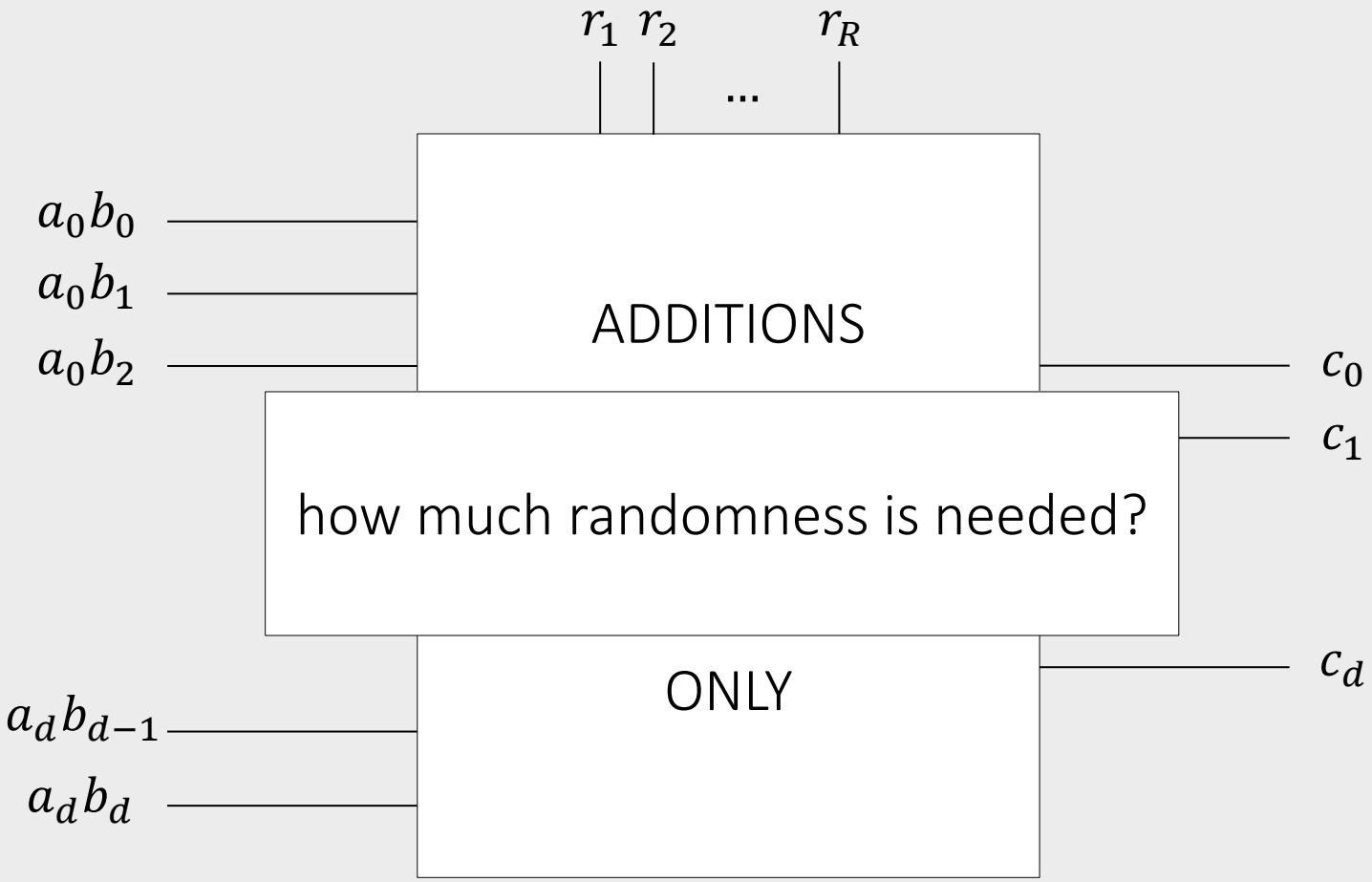


this paper

$$(a, b) \in \{0,1\}^2 \mapsto a \cdot b \in \{0,1\}$$




r_1 r_2 ... r_R
a_0b_0
a_0b_1
a_0b_2
ADDITIONS
ONLY
a_db_{d-1}
a_db_d
c_0
c_1
c_d


r_1 r_2 ... r_R
a_0b_0
a_0b_1
a_0b_2
ADDITIONS
c_0
c_1
how much randomness is needed?
ONLY
c_d
a_db_{d-1}
a_db_d

randomness in cryptography

used everywhere:

- keys
- RSA prime factors
- ...

randomness in cryptography

used everywhere:
- keys
- RSA prime factors
- ...

strong properties:
- uniformly distributed
- independent
- ...

where does it come from?

where does it come from?

in the real world: natural randomness

where does it come from?

in the real world: natural randomness

in practice:

- need special hardware
- slow
- bias or uneven distribution

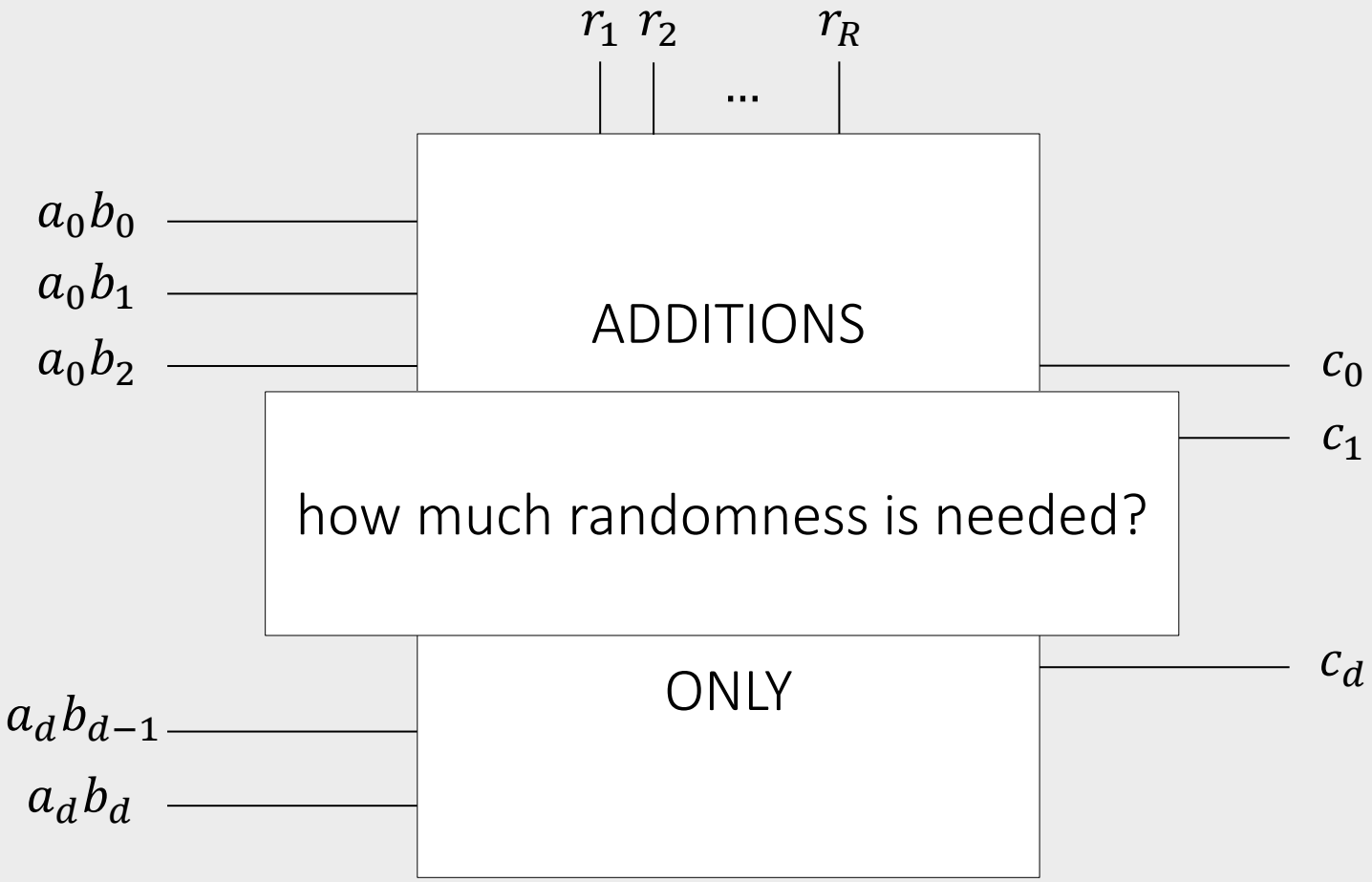
where does it come from?

in the real world: natural randomness

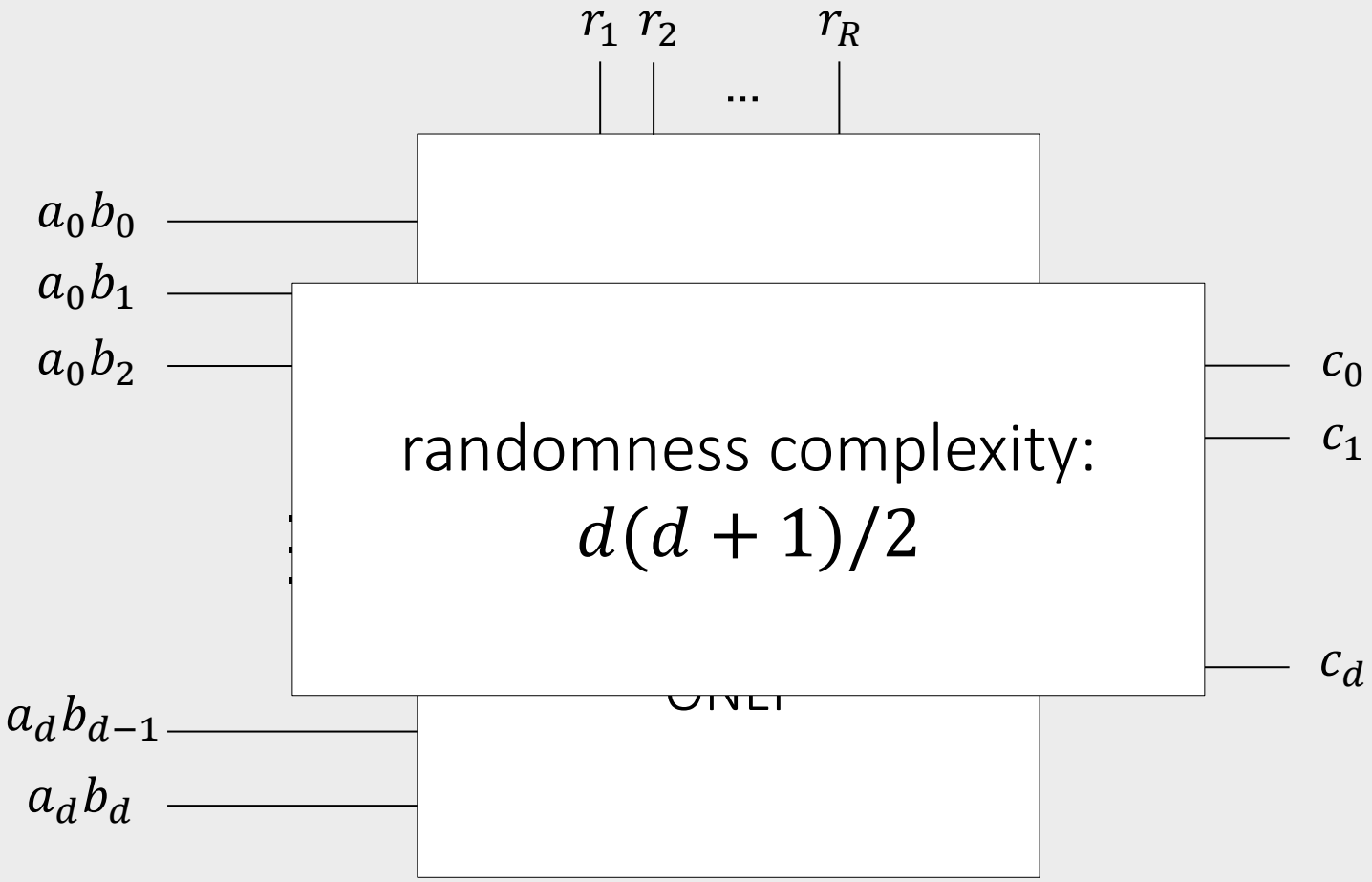
in practic

- need s
- slow
- bias or uneven distribution

randomness should be considered as a resource, like space and time


r_1 r_2 ... r_R
a_0b_0
a_0b_1
a_0b_2
ADDITIONS
c_0
c_1
how much randomness is needed?
ONLY
c_d
a_db_{d-1}
a_db_d

Ishai-Sahai-Wagner scheme (Crypto 2003)



main contributions

problem Characterization ⇒ linear algebra

legend:
blablah: speaker will talk about it ☺
blablah: you have to read the paper ☹

main contributions

problem Characterization ⇒ linear algebra

upper Bound ⇒ quasi-linear

;

legend:
blablah: speaker will talk about it ☺
blablah: you have to read the paper ☹

main contributions

problem Characterization ⇒ linear algebra

upper Bound ⇒ quasi-linear

lower Bound ⇒ linear

legend:
blablah: speaker will talk about it ☺
blablah: you have to read the paper ☹

main contributions

problem Characterization ⇒ linear algebra

upper Bound ⇒ quasi-linear

lower Bound ⇒ linear

constructions for small d ⇒ reach lower bound

legend:
blablah: speaker will talk about it ☺
blablah: you have to read the paper ☹

main contributions

problem Characterization ⇒ linear algebra

upper Bound ⇒ quasi-linear

lower Bound ⇒ linear

constructions for small d ⇒ reach lower bound

generic construction ⇒ halves ISW randomness cost

legend:
blablah: speaker will talk about it ☺
blablah: you have to read the paper ☹

main contributions

problem Characterization ⇒ linear algebra

upper Bound ⇒ quasi-linear

lower Bound ⇒ linear

constructions for small d ⇒ reach lower bound

generic construction ⇒ halves ISW randomness cost

composition

legend:
blablah: speaker will talk about it ☺
blablah: you have to read the paper ☹

main contributions

problem Characterization ⇒ linear algebra

upper Bound ⇒ quasi-linear

lower Bound ⇒ linear

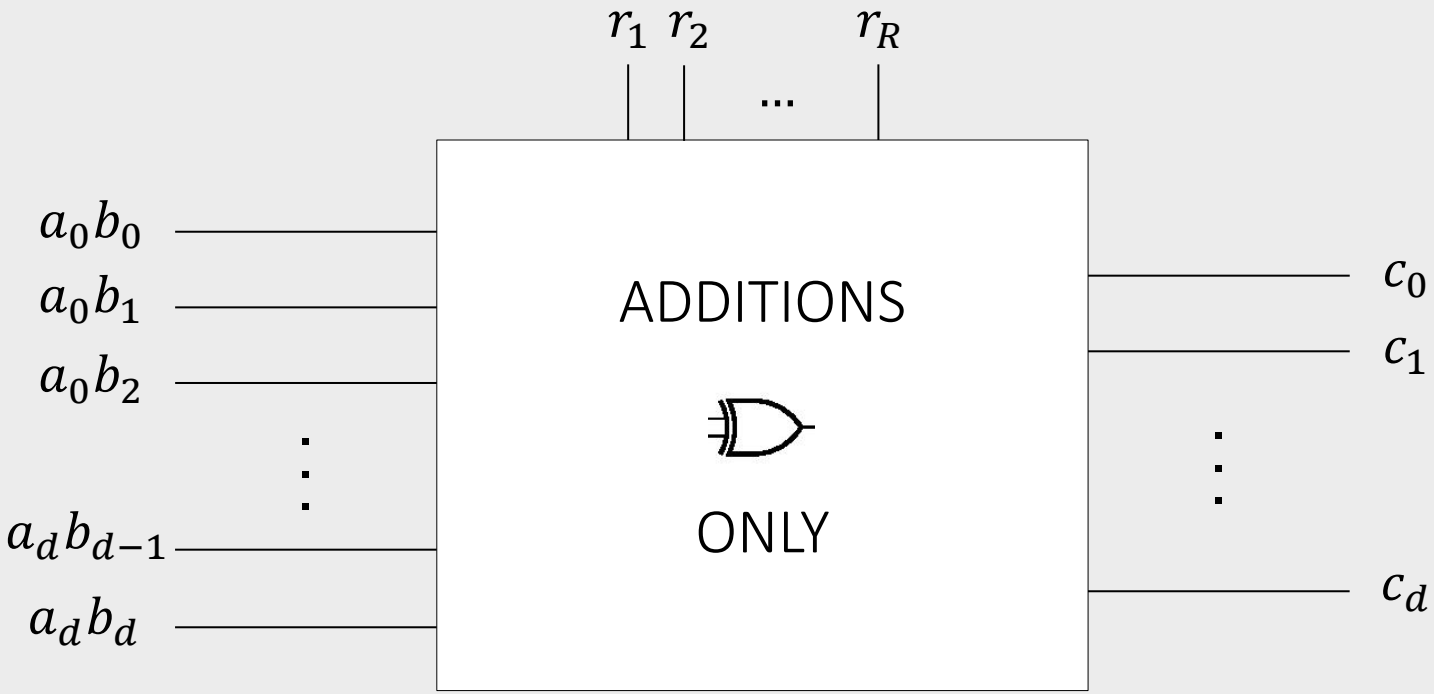
constructions for small d ⇒ reach lower bound

generic construction ⇒ halves ISW randomness cost

composition

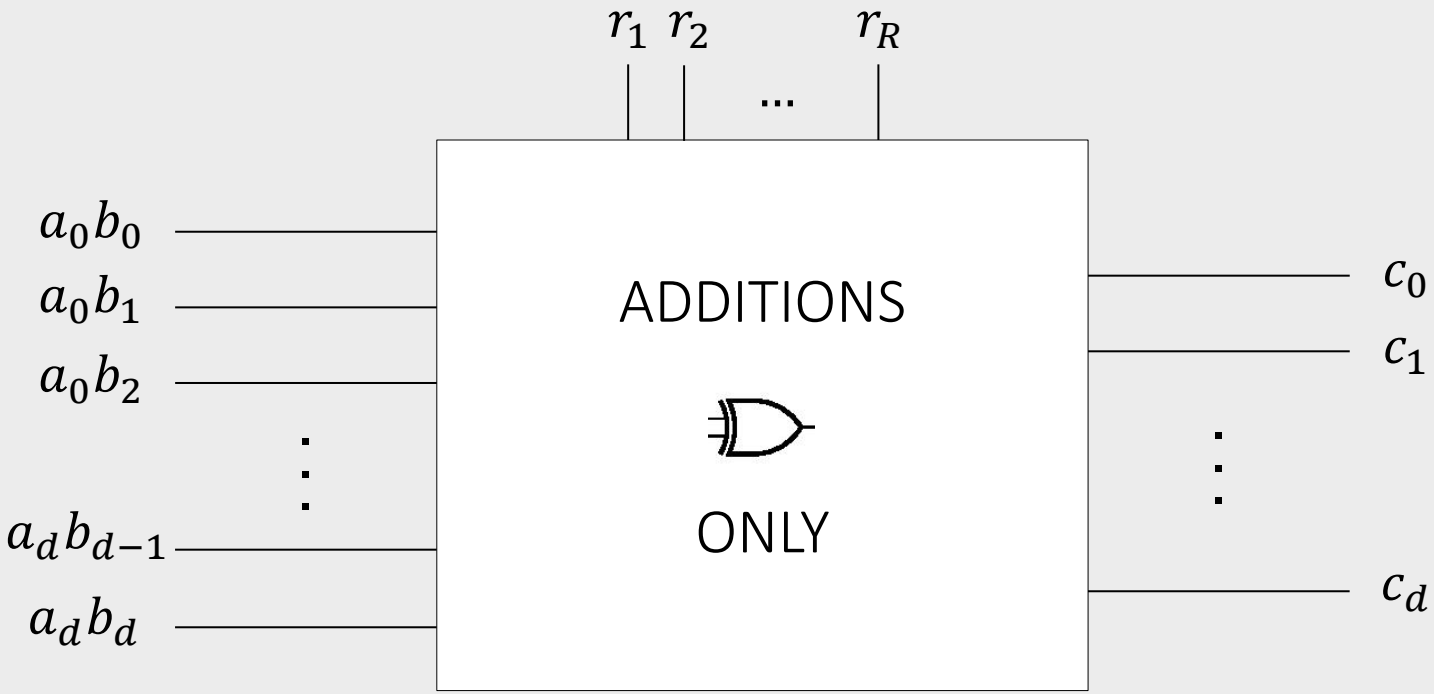
automatic Tool

legend:
blablah: speaker will talk about it ☺
blablah: you have to read the paper ☹


r_1 r_2 ... r_R
a_0b_0
a_0b_1
a_0b_2
a_db_{d-1}
a_db_d
ADDITIONS
ONLY
c_0
c_1
c_d

any wire value (aka probe) has the form:

$$p = \left(\bigoplus_{(i,j) \in X \subseteq \{0,\ldots,d\}^2} a_i b_j \right) \oplus \left(\bigoplus_{k \in Y \subseteq \{1,\ldots,R\}} r_k \right)$$



any wire value (aka probe) has the form:

$$p = \left(\bigoplus_{(i,j) \in X \subseteq \{0,\ldots,d\}^2} a_i b_j \right) \oplus \left(\bigoplus_{k \in Y \subseteq \{1,\ldots,R\}} r_k \right)$$

$$= \vec{a}^t \cdot M_p \cdot \vec{b} \ \oplus \ \vec{s}_p^t \cdot \vec{r}$$

with $M_p \in \{0,1\}^{(d+1)\times(d+1)}, \vec{s}_p \in \{0,1\}^R$

any wire value (aka probe) has the form:

$$p = \left(\bigoplus_{(i,j) \in X \subseteq \{0,\ldots,d\}^2} a_i b_j \right) \oplus \left(\bigoplus_{k \in Y \subseteq \{1,\ldots,R\}} r_k \right)$$

any sum of probes has the form:

$$\vec{a}^t \cdot M \cdot \vec{b} \ \oplus \ \vec{s}^t \cdot \vec{r}$$

algebraic characterization

condition 1:

a set of probes $P = \{p_1, \ldots, p_\ell\}$ satisfies condition 1 iff:

$$\oplus_{i=1}^{\ell} p_i = \vec{a}^t \cdot M \cdot \vec{b}$$

and $(1, \ldots, 1)$ is in the row (or column) space of M

algebraic characterization

condition 1:

a set of probes $P = \{p_1, \ldots, p_\ell\}$ satisfies condition 1 iff:

$$\oplus_{i=1}^{\ell} p_i = \vec{a}^t \cdot M \cdot \vec{b}$$

and $(1, \ldots, 1)$ is in the row (or column) space of M

theorem:

C is d-private

$\Leftrightarrow$

there does not exist $P = \{p_1, \ldots, p_\ell\}, \ell \leq d$ that satisfies condition 1

proof sketch

⇒ assume $\{p_1, \ldots, p_\ell\}$ such that:

$$\oplus_{i=1}^{\ell} p_i = \vec{a}^t \cdot M \cdot \vec{b}$$

and $(1, \ldots, 1)$ is in the column space of M

proof sketch

⇒ assume $\{p_1, \ldots, p_\ell\}$ such that:

$$\oplus_{i=1}^{\ell} p_i = \vec{a}^t \cdot M \cdot \vec{b}$$

and $(1, \ldots, 1)$ is in the column space of M

⇒ there exists $\vec{b}' \in \{0,1\}^{d+1}$ s.t. $M \cdot \vec{b}' = (1, \ldots, 1)$

proof sketch

⇒ assume $\{p_1, \ldots, p_\ell\}$ such that:

$$\oplus_{i=1}^{\ell} p_i = \vec{a}^t \cdot M \cdot \vec{b}$$

and $(1, \ldots, 1)$ is in the column space of M

⇒ there exists $\vec{b}' \in \{0,1\}^{d+1}$ s.t. $M \cdot \vec{b}' = (1, \ldots, 1)$

$$\Pr\left[\vec{a}^t \cdot M \cdot \vec{b} = a\right] = \begin{cases} \frac{1}{2} & \text{if } M \cdot \vec{b} \neq (1, \ldots, 1) \\ 1 & \text{if } M \cdot \vec{b} = (1, \ldots, 1) \end{cases}$$

proof sketch

⇒ assume $\{p_1, \dots, p_\ell\}$ such that:

$$\oplus_{i=1}^{\ell} p_i = \vec{a}^t \cdot M \cdot \vec{b}$$

and $(1, \dots, 1)$ is in the column space of M

⇒ there exists $\vec{b}' \in \{0,1\}^{d+1}$ s.t. $M \cdot \vec{b}' = (1, \dots, 1)$

$$\Pr\left[\vec{a}^t \cdot M \cdot \vec{b} = a\right] = \begin{cases} \frac{1}{2} & \text{if } M \cdot \vec{b} \neq (1, \dots, 1) \\ 1 & \text{if } M \cdot \vec{b} = (1, \dots, 1) \end{cases}$$

then, $\Pr\left[\vec{a}^t \cdot M \cdot \vec{b} = a\right] > \Pr\left[\vec{a}^t \cdot M \cdot \vec{b} = 1 - a\right]$

proof sketch

⇒ assume $\{p_1, \ldots, p_\ell\}$ such that:

$$\oplus_{i=1}^{\ell} p_i = \vec{a}^t \cdot M \cdot \vec{b}$$

and $(1, \ldots, 1)$ is in the column space of M

⇒ there exists $\vec{b}' \in \{0,1\}^{d+1}$ s.t. $M \cdot \vec{b}' = (1, \ldots, 1)$

$$\Pr\left[\vec{a}^t \cdot M \cdot \vec{b} = a\right] = \begin{cases} \frac{1}{2} & \text{if } M \cdot \vec{b} \neq (1, \ldots, 1) \\ 1 & \text{if } M \cdot \vec{b} = (1, \ldots, 1) \end{cases}$$

then, $\Pr\left[\vec{a}^t \cdot M \cdot \vec{b} = a\right] > \Pr\left[\vec{a}^t \cdot M \cdot \vec{b} = 1 - a\right]$

⇐ a lot more technical...

□

upper bound

upper bound

randomness complexity of ISW: $O(d^2)$

needs for a quadratic complexity?

theorem:
there exists a d-private circuit for multiplication with randomness complexity $\tilde{O}(d)$.

proof sketch

probabilistic method: non-constructive!

proof sketch

probabilistic method: non-constructive!

$r_1, \ldots, r_R$ random bits

$\Rightarrow \rho_{i,j} = \bigoplus_{1 \le k \le R} \alpha_{i,j,k} \cdot r_i$ with $\alpha_{i,j,k} \in \{0,1\}$

proof sketch

probabilistic method: non-constructive!

$r_1, \ldots, r_R$ random bits

$\Rightarrow \rho_{i,j} = \bigoplus_{1 \le k \le R} \alpha_{i,j,k} \cdot r_i$ with $\alpha_{i,j,k} \in \{0,1\}$

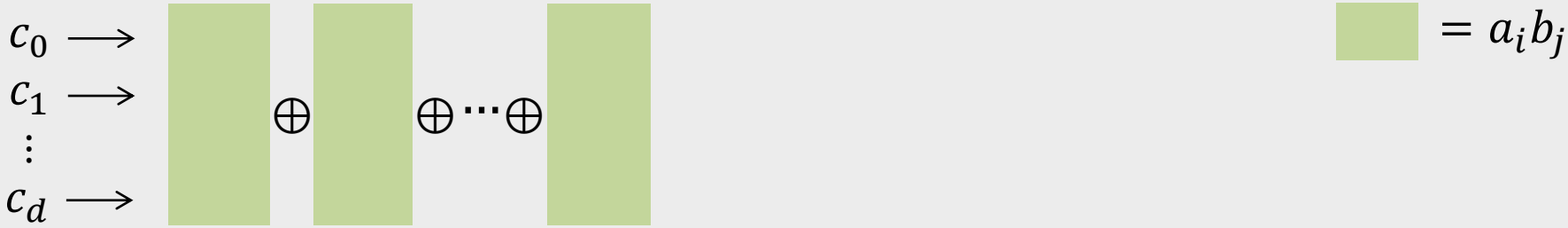
$$\begin{matrix} c_0 \\ c_1 \\ \vdots \\ c_d \end{matrix} \longrightarrow \begin{pmatrix} a_0 b_0 & a_0 b_1 & \cdots & a_0 b_d \\ a_1 b_0 & a_1 b_1 & & a_1 b_d \\ \vdots & \vdots & \ddots & \vdots \\ a_d b_0 & a_d b_1 & \cdots & a_d b_d \end{pmatrix}$$

proof sketch

probabilistic method: non-constructive!

$r_1, \ldots, r_R$ random bits

$\Rightarrow \rho_{i,j} = \bigoplus_{1 \le k \le R} \alpha_{i,j,k} \cdot r_i$ with $\alpha_{i,j,k} \in \{0,1\}$

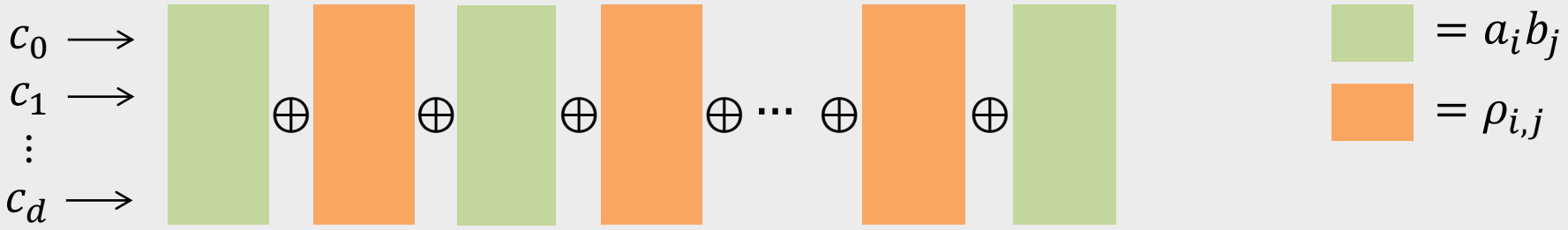


proof sketch

probabilistic method: non-constructive!

$r_1, \ldots, r_R$ random bits

$\Rightarrow \rho_{i,j} = \bigoplus_{1 \le k \le R} \alpha_{i,j,k} \cdot r_i$ with $\alpha_{i,j,k} \in \{0,1\}$

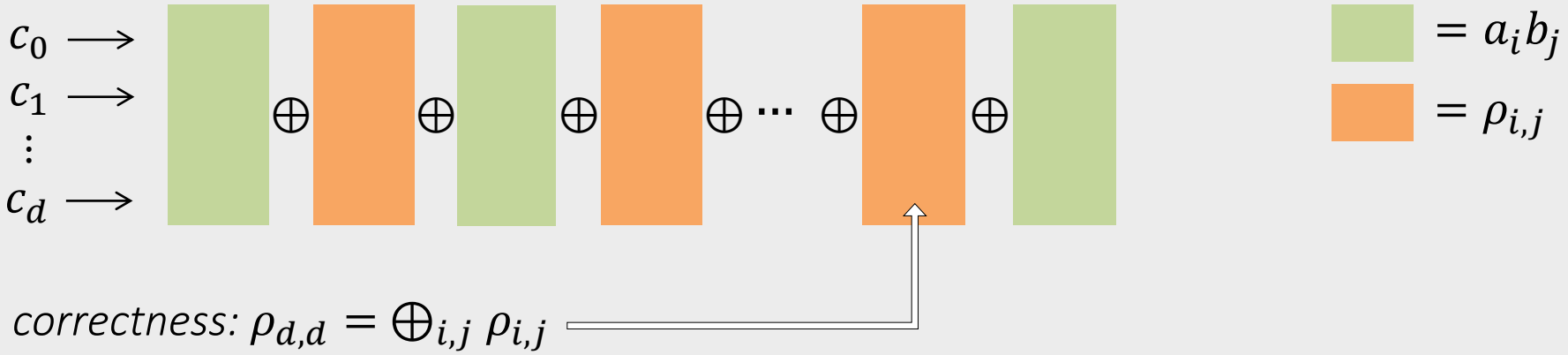


proof sketch

probabilistic method: non-constructive!

$r_1, \ldots, r_R$ random bits

$\Rightarrow \rho_{i,j} = \bigoplus_{1 \le k \le R} \alpha_{i,j,k} \cdot r_i$ with $\alpha_{i,j,k} \in \{0,1\}$



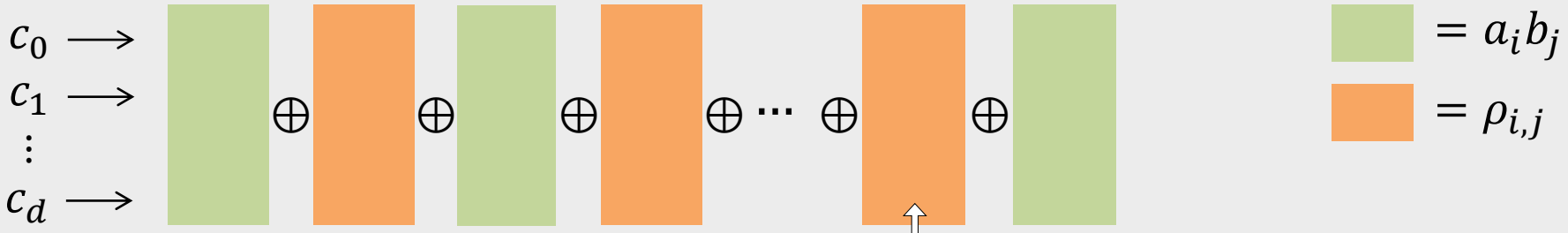
correctness: $\rho_{d,d} = \bigoplus_{i,j} \rho_{i,j}$

proof sketch

probabilistic method: non-constructive!

$r_1, \dots, r_R$ random bits

$\Rightarrow \rho_{i,j} = \bigoplus_{1 \le k \le R} \alpha_{i,j,k} \cdot r_i$ with $\alpha_{i,j,k} \in \{0,1\}$



correctness: $\rho_{d,d} = \bigoplus_{i,j} \rho_{i,j}$

d-privacy: if $R = \Omega(d), \Pr(is\ secure) > 0 \Rightarrow$ at least one algorithm is d-private

□

lower bounds

lower bounds

theorem:

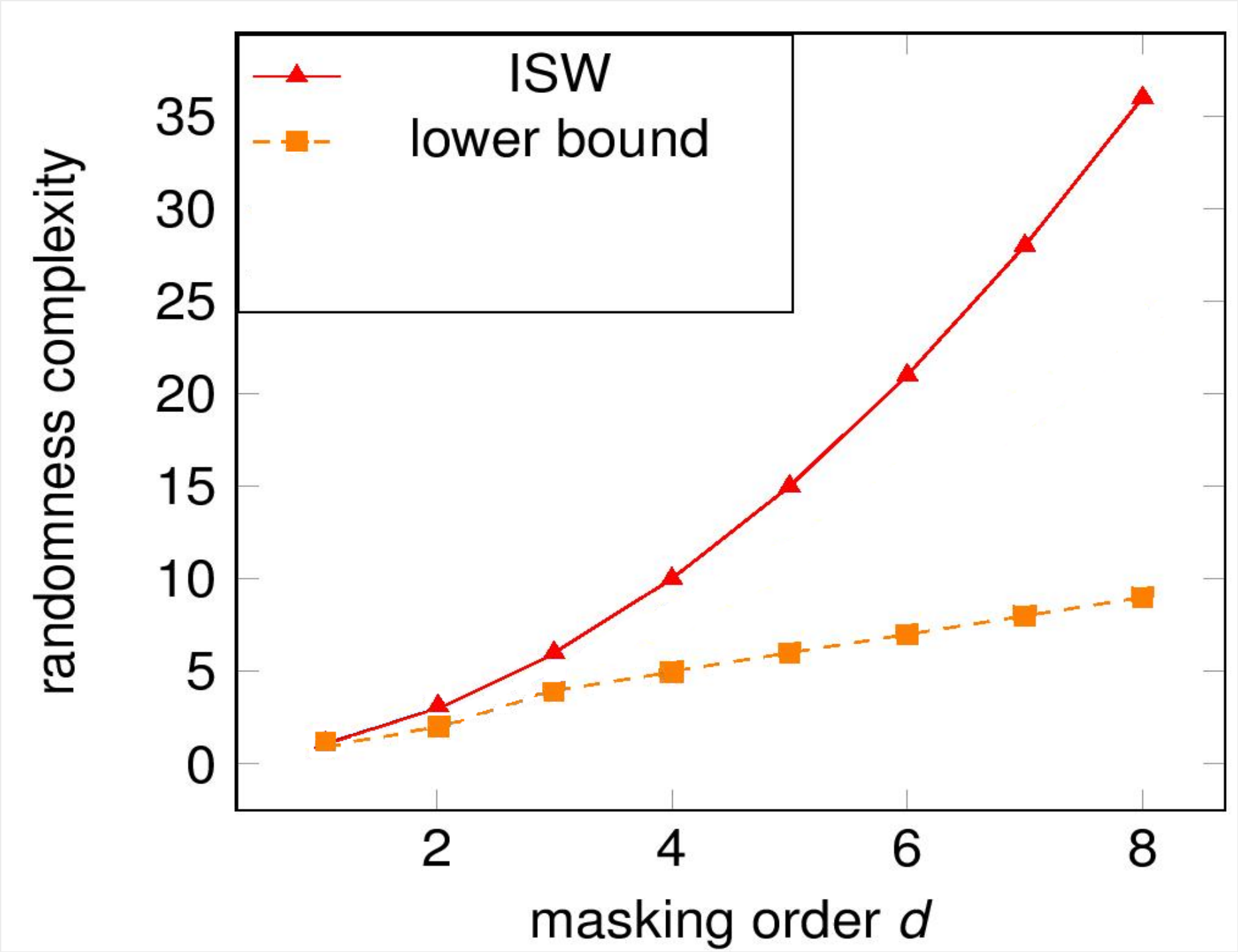
1. d-privacy $\Rightarrow$ at least d random bits (for $d \geq 2$)
2. d-privacy $\Rightarrow$ at least $d + 1$ random bits (for $d \geq 3$)

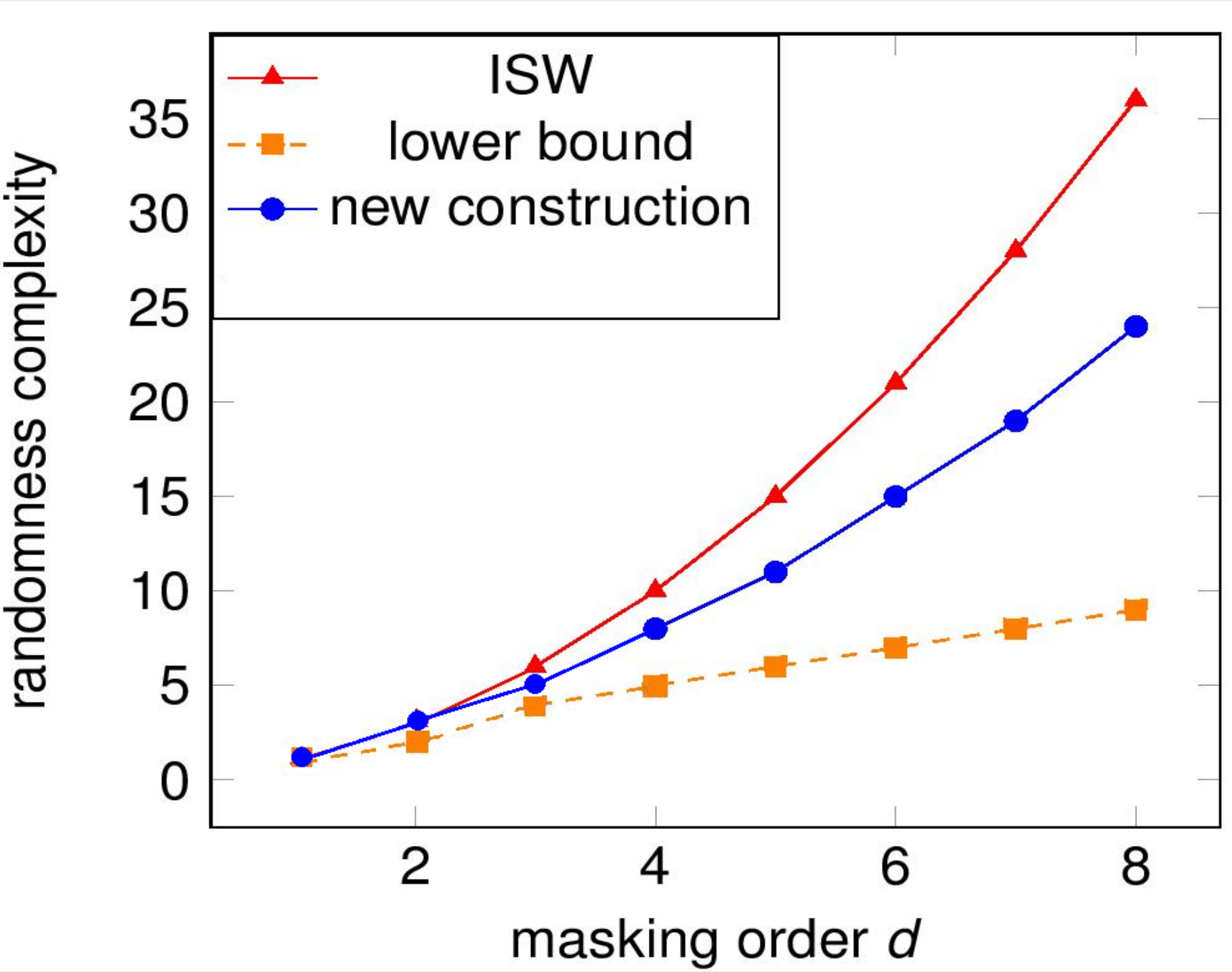
automatic tool for finding attacks

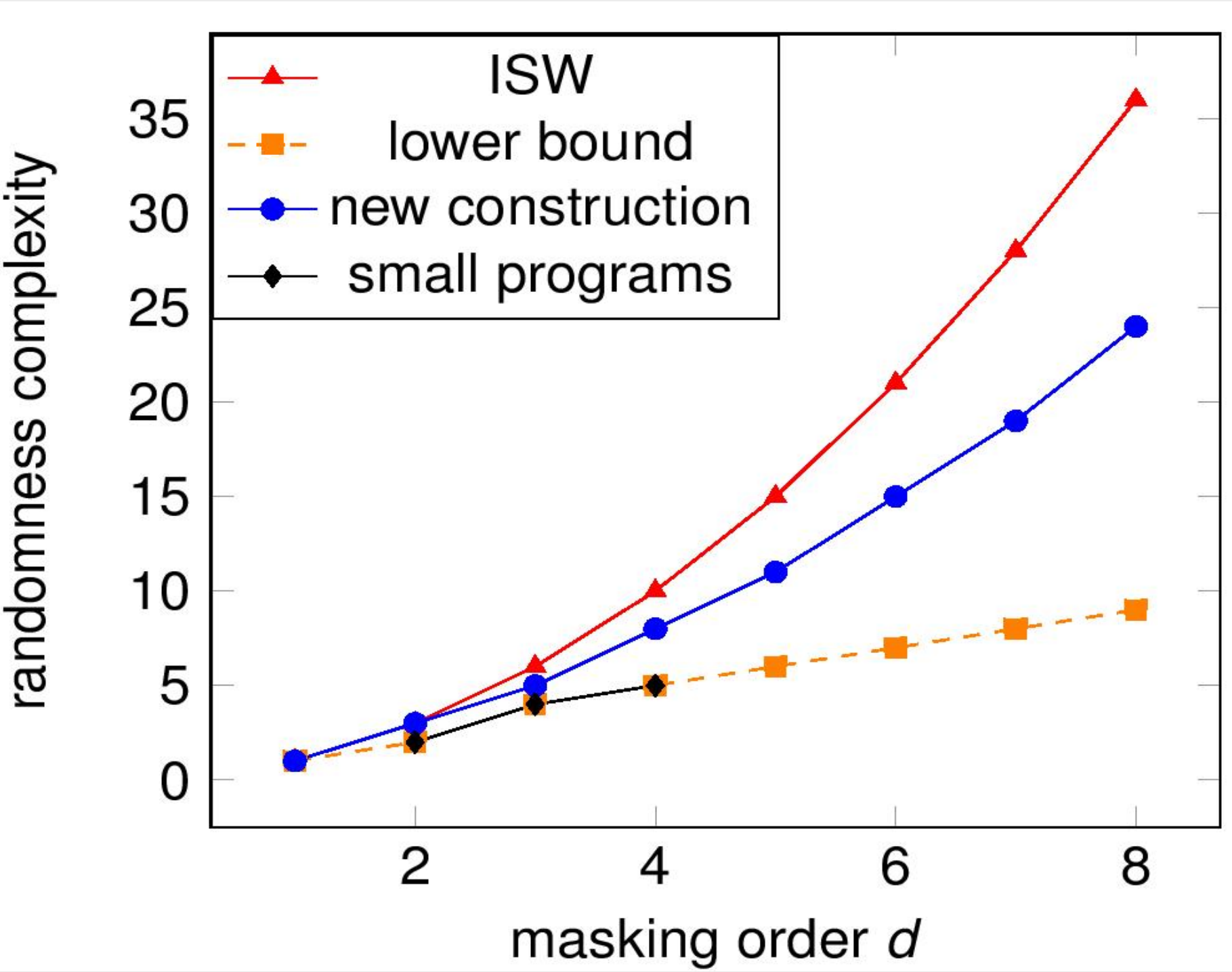
- based on the algebraic characterization
- relies on coding theory (information set decoding algorithms)
- not perfectly sound...
- much faster than Easycrypt-based [Barthe et al. 15]

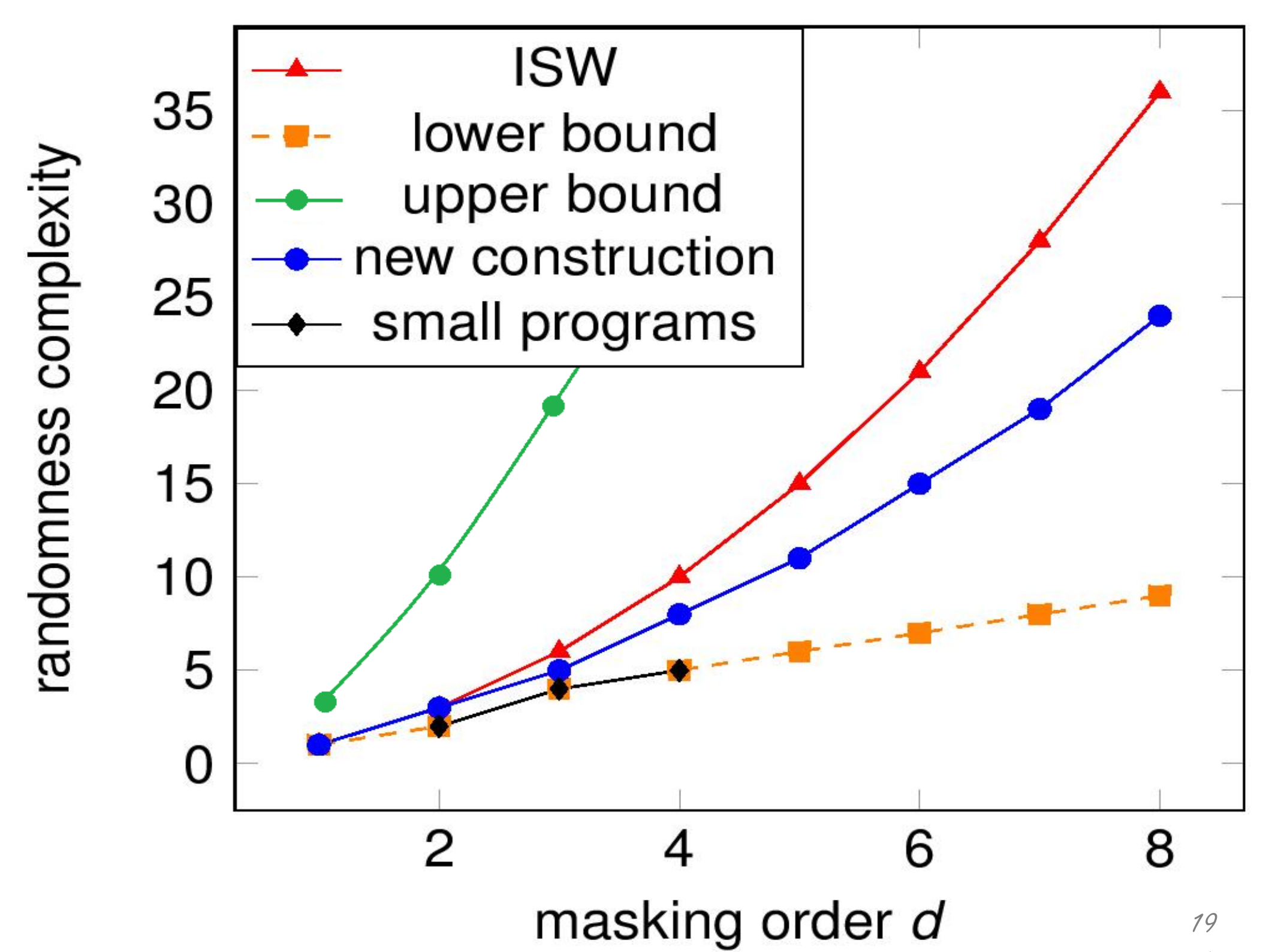
order	2	3	4	5	6
[Barthe&al]	<1 ms	36 ms	108 ms	6,3 s	26 min
this paper	<10 ms	<10 ms	<10 ms	<100 ms	<300 ms

table: time to find an attack


ISW
lower bound
randomness complexity
masking order d
0
5
10
15
20
25
30
35
2
4
6
8


ISW
lower bound
new construction
randomness complexity
masking order d
0
5
10
15
20
25
30
35
2
4
6
8


ISW
lower bound
new construction
small programs
randomness complexity
masking order d
0
5
10
15
20
25
30
35
2
4
6
8


ISW
lower bound
upper bound
new construction
small programs
randomness complexity
masking order d
0
5
10
15
20
25
30
35
2
4
6
8

proof sketch of 1.

lemma:

S_0, S_1 two sets of at most d probes and $s_b = \bigoplus_{p \in S_b} p$

$(r_i \notin s_b, \forall i, b) \wedge (s_0 \oplus s_1 = a \cdot b) \Rightarrow C$ is not d-private

proof sketch of 1.

lemma:

S_0, S_1 two sets of at most d probes and $s_b = \bigoplus_{p \in S_b} p$

$(r_i \notin s_b, \forall i, b) \wedge (s_0 \oplus s_1 = a \cdot b) \Rightarrow C$ is not d-private

suppose an algorithm C with only $r_1, \dots, r_{d-1}$ and let $c_0, \dots, c_d$ the output of C

let $N = \left(n_{i,j}\right)_{\substack{1 \le i \le d-1 \\ 1 \le j \le d}} \in \{0,1\}^{(d-1)\times d}$ s.t. $n_{i,j} = 1 \Leftrightarrow r_i \in c_j$

proof sketch of 1.

lemma:

S_0, S_1 two sets of at most d probes and $s_b = \bigoplus_{p \in S_b} p$

$(r_i \notin s_b, \forall i, b) \wedge (s_0 \oplus s_1 = a \cdot b) \Rightarrow C$ is not d-private

suppose an algorithm C with only $r_1, \ldots, r_{d-1}$ and let $c_0, \ldots, c_d$ the output of C

let $N = \left(n_{i,j}\right)_{\substack{1 \le i \le d-1 \\ 1 \le j \le d}} \in \{0,1\}^{(d-1)\times d}$ s.t. $n_{i,j} = 1 \Leftrightarrow r_i \in c_j$

N has dimension $(d-1) \times d \Rightarrow Ker(N) \neq \{\vec{0}\}$

proof sketch of 1.

lemma:

S_0, S_1 two sets of at most d probes and $s_b = \bigoplus_{p \in S_b} p$

$(r_i \notin s_b, \forall i, b) \wedge (s_0 \oplus s_1 = a \cdot b) \Rightarrow C$ is not d-private

suppose an algorithm C with only $r_1, \ldots, r_{d-1}$ and let $c_0, \ldots, c_d$ the output of C

let $N = \left(n_{i,j}\right)_{\substack{1 \le i \le d-1 \\ 1 \le j \le d}} \in \{0,1\}^{(d-1)\times d}$ s.t. $n_{i,j} = 1 \Leftrightarrow r_i \in c_j$

N has dimension $(d-1) \times d \Rightarrow Ker(N) \neq \{\vec{0}\}$

let $w \in Ker(N) - \{\vec{0}\}$

$S_0 = \{c_0\} \cup \{c_i | w_i = 0\}$ and $S_1 = \{c_i | w_i = 1\}$ satisfy requirements of lemma... □