SECURE-IC
THE SECURITY SCIENCE COMPANY

Low-entropy masking scheme compatible for ARX

Speaker: Sylvain GUILLEY

Date: September 18, 2025

Location: CHES, Kuala Lumpur Convention Center, Malaysia

Version 2

AGENDA

1. Introduction
2. Low-entropy masking scheme compliant with Boolean and Arithmetic computations
3. Security of low-entropy masking schemes
4. Second-order evaluation of low-entropy masking schemes?
5. Conclusion and perspectives

2025 All Rights Reserved I Confidential I Property of Secure-IC

AGENDA

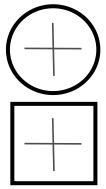
1. Introduction
2. Low-entropy masking scheme compliant with Boolean and Arithmetic computations
3. Security of low-entropy masking schemes
4. Second-order evaluation of low-entropy masking schemes?
5. Conclusion and perspectives

2025 All Rights Reserved I Confidential I Property of Secure-IC

Cryptographic computations *vs* side-channel attacks

- Sensitive computations must be secured against **non-invasive attacks**, which attempt to correlate the leakage of some operations with a hypothetical model.
- A protection against this threat is the **masking countermeasure**.
- Masking consists in changing the **intermediate variables** of the computation into **randomized** versions, which are thus decorrelated from the unprotected variables, each being a potential target for a side-channel attack.

Protection schemes have proposed when operations are either:



- **Boolean**, or
- **Arithmetic**.

Both of which are additive groups.

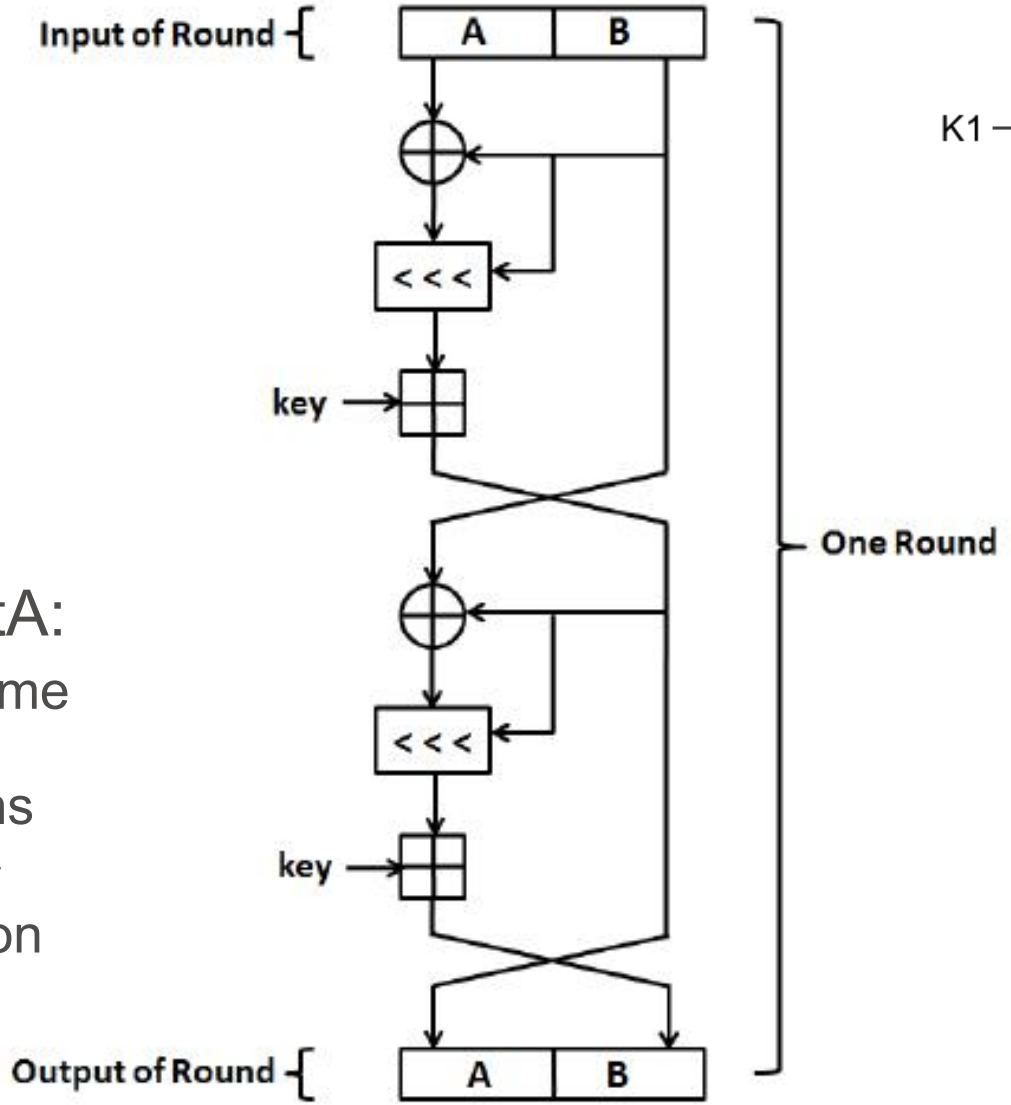
2025 All Rights Reserved I Confidential I Property of Secure-IC

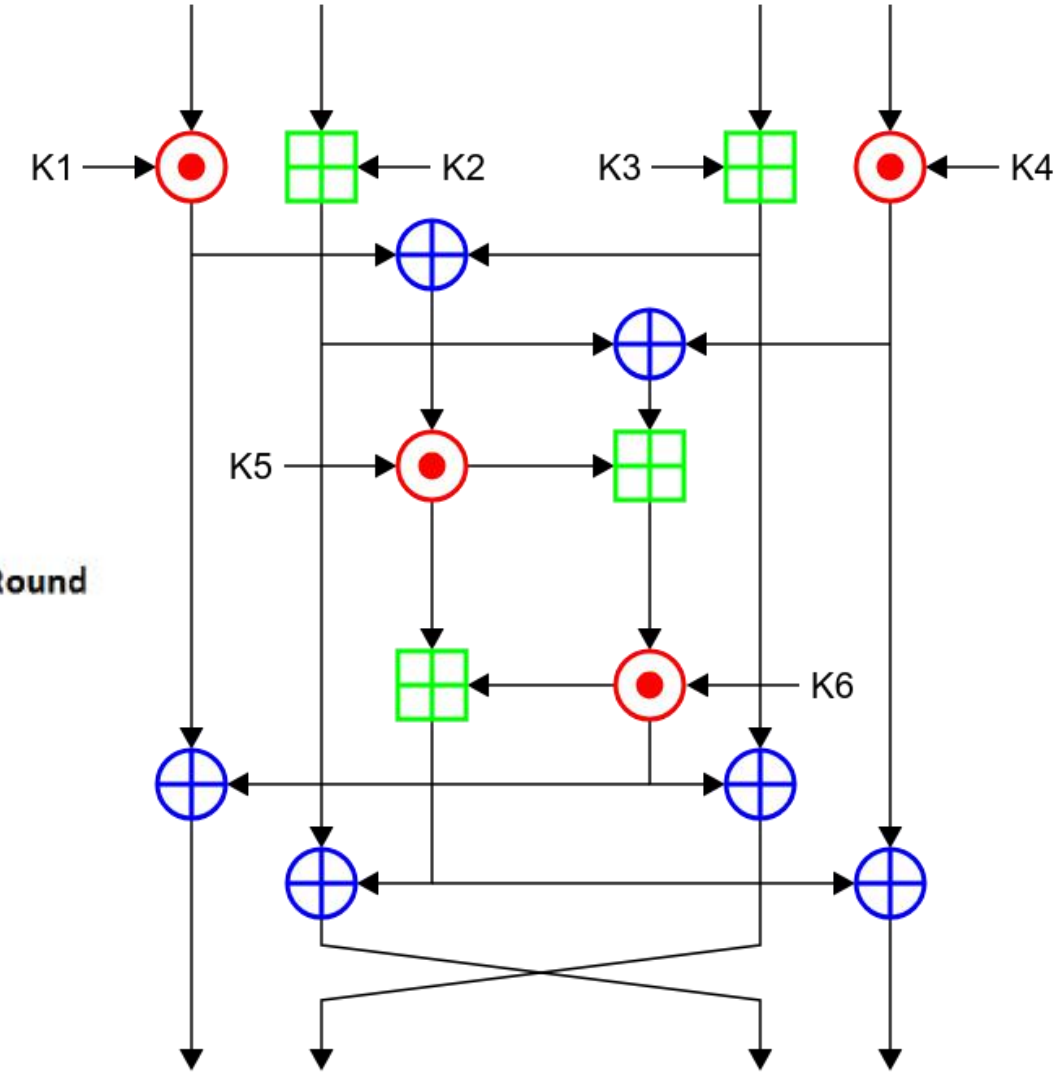
Mixed Boolean & Arithmetic Cryptography

ARX: Add, Rotatate, Xor

- IDEA
- RC5
- XTEA
- SipHash
- ...

- Masking SotA:
  - Cumbersome A2B, B2A conversions
  - No latency preservation





2025 All Rights Reserved I Confidential I Property of Secure-IC

SECURE-IC
THE SECURITY SCIENCE COMPANY

AGENDA

1. Introduction
2. Low-entropy masking scheme compliant with Boolean and Arithmetic computations
3. Security of low-entropy masking schemes
4. Second-order evaluation of low-entropy masking schemes?
5. Conclusion and perspectives

2025 All Rights Reserved I Confidential I Property of Secure-IC

Addition: Arithmetic wrt Boolean operations

2.1 Addition

Let $a = (a_{n-1}, \ldots, a_0)_2$ and $b = (b_{n-1}, \ldots, b_0)_2$ two n-bit integers, represented as a string of bits.

The bitwise operations for arithmetic addition are

- $d_i = a_i \oplus b_i \oplus c_i$,
- $c_{i+1} = \mathsf{MAJ}(a_i, b_i, c_i)$,

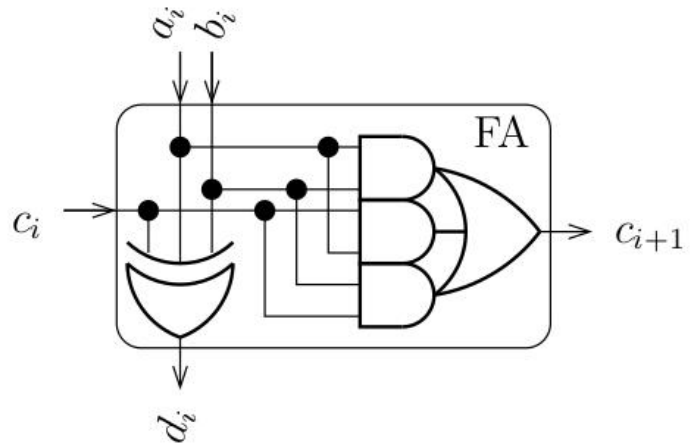


Figure 1: Schematic for the Full Adder

where MAJ is the majority function, namely

$$\begin{aligned}\mathsf{MAJ}(a_i, b_i, c_i) &= (a_i \wedge b_i) \vee (b_i \wedge c_i) \vee (c_i \wedge a_i) \\ &= (a_i \wedge b_i) \oplus (b_i \wedge c_i) \oplus (c_i \wedge a_i).\end{aligned}$$

The FA (Full Adder) is the one-bit slice of an adder, depicted in Fig. 1.

Addition: Masking arithmetic operations

Now have the nice property that, for all $m \in \{0,1\}$,

- $d_i \oplus m = (a_i \oplus m) \oplus (b_i \oplus m) \oplus (c_i \oplus m)$,
- $c_{i+1} \oplus m = \mathsf{MAJ}(a_i \oplus m, b_i \oplus m, c_i \oplus m)$.

The first property is due to the associativity of the XOR, namely $(a_i \oplus b_i) \oplus c_i = a_i \oplus (b_i \oplus c_i) = a_i \oplus b_i \oplus c_i$. The second property is inherent to the majority: its dual function is also the majority. The majority of ones (at least two ones amongst three bits) is the opposite of the majority of zeroes (at least two zeroes amongst three bits). Mathematically, this writes:

$$\mathsf{MAJ}(\neg a_i, \neg b_i, \neg c_i) = \neg \mathsf{MAJ}(a_i, b_i, c_i).$$

So, all in one:

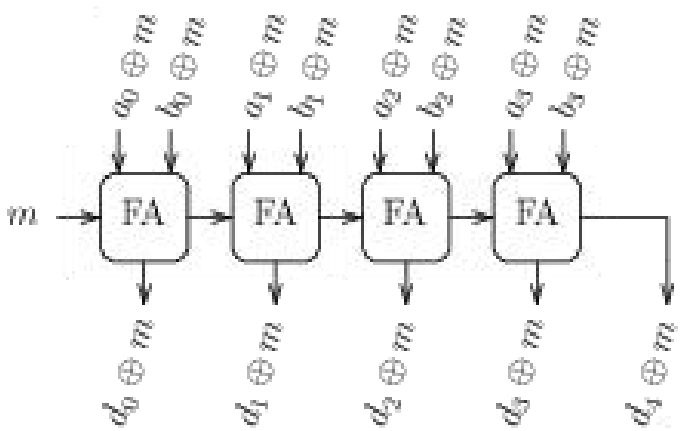
$$\forall m \in \{0,1\}, \quad \mathsf{MAJ}(a_i \oplus m, b_i \oplus m, c_i \oplus m) = \mathsf{MAJ}(a_i, b_i, c_i) \oplus m.$$

This means that the addition is transparent to masking, provided the carries are also inverted. This is illustrated in Fig. 2 when the same mask is shared for both operands and all the bits.

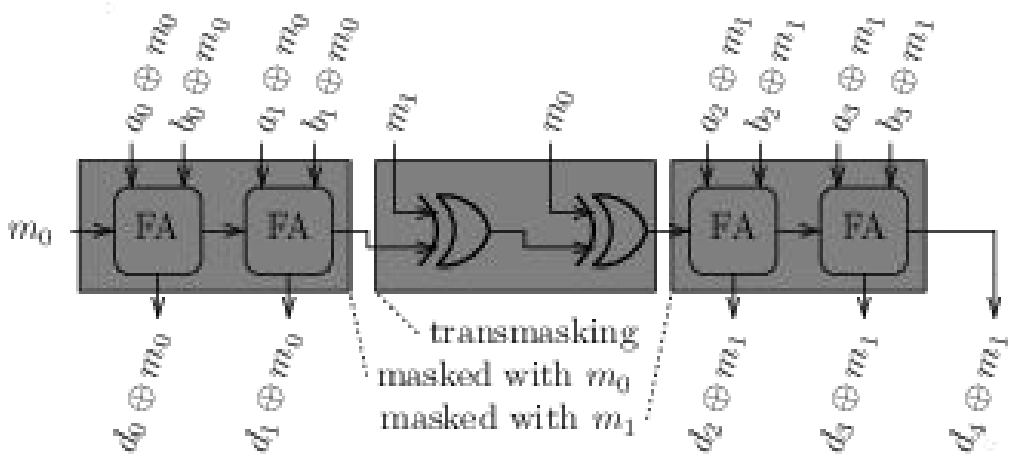
Remark 1. *This masking is first-order secure provided the two operands are independent, and also provided that the leakage model is linear (bits or words are pairwise not combined by the leakage function).*

Dual Boolean and arithmetic masking

- **Boolean operations**
  - XOR on bit-vectors
- **Arithmetic operations**
  - Modulo 2^{32} or 2^{64} additions (with carry) on integers



n=4, k=1



n=4, k=2

Drop the outbound carry if computing not in **Z** but in $\mathbf{Z}/2^n\mathbf{Z}$

2025 All Rights Reserved I Confidential I Property of Secure-IC

SECURE-iC
THE SECURITY SCIENCE COMPANY

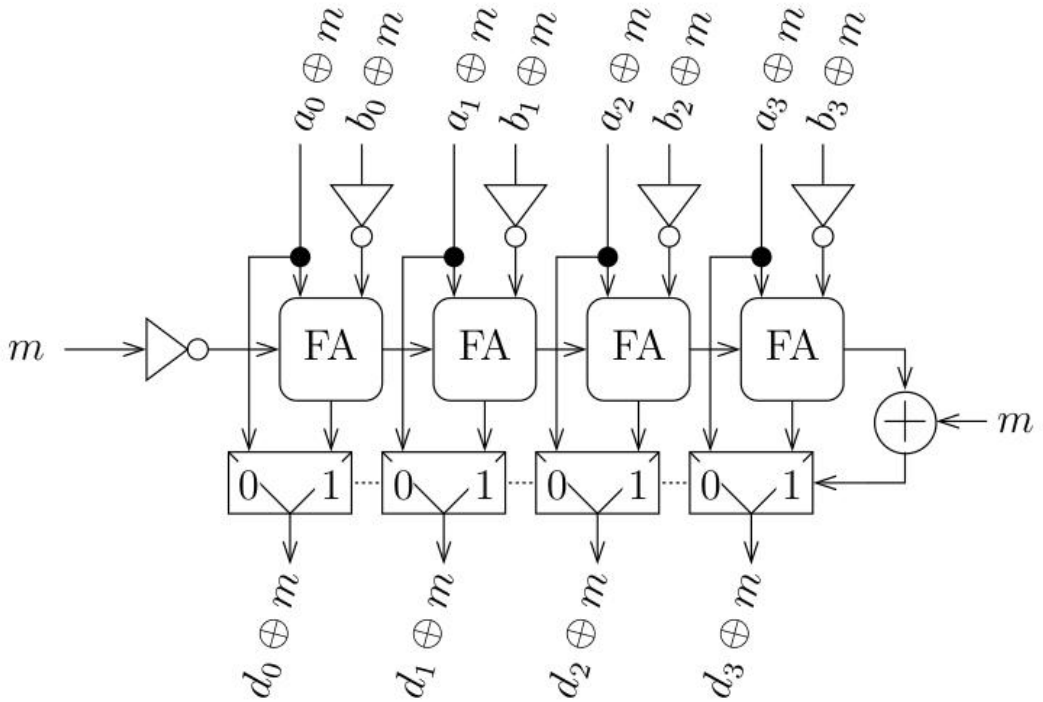
Bonus: reduction / subtraction

2.2 Reduction

In some algorithms, it might be demanded to *reduce* a number a *modulo* another number b. Let us further assume that $a = (a_{n-1}, \ldots, a_0)_2$ and $b = (b_{n-1}, \ldots, b_0)_2$ fit on n bits. The result of the reduction is denoted by $d = (d_{n-1}, \ldots, d_0)_2$, which is such that $d = a \bmod b$. Here, we consider the case where the MSB b_{n-1} of b is set to 1. Then:

$$d = a \bmod b = \begin{cases} a - b & \text{if } a \geq b, \text{ or} \\ a & \text{otherwise.} \end{cases} \quad (1)$$

Indeed, -b = ¬(b-1). e.g., on 4 bits:
-3 = 16-3 = 13 and ¬2 = ¬$(0010)_2$ = $(1101)_2$ = 13.
-2 = 16-2 = 14 and ¬1 = ¬$(0001)_2$ = $(1110)_2$ = 14.



See in the paper how to protect MUX functions.

SECURE-IC
THE SECURITY SCIENCE COMPANY

AGENDA

1. Introduction
2. Low-entropy masking scheme compliant with Boolean and Arithmetic computations
3. Security of low-entropy masking schemes
4. Second-order evaluation of low-entropy masking schemes?
5. Conclusion and perspectives

2025 All Rights Reserved I Confidential I Property of Secure-IC

Masking scheme

- Security model

§ **This scheme is first order secure**
  § SPA, DPA, DEMA, etc. will fail (whatever the number of traces)
  § If leakage function is symmetrical, E[L(X+M) | X=x] = 1/2 (L(x) + L(¬x)) = constant

§ **Second-order attacks are possible**
  § Combining the information "a + m" with mask "m"
  § The optimal distinguisher is given below:

Let $n = 8$ and $k|n$, typically $k = 1, 2, 4, 8$. Let us call $\phi : \mathbb{F}_2^k \to \mathbb{F}_2^n$ the injective masking function, such that

$$\phi(m) = \underbrace{(m, \ldots, m)}_{n/k \text{ times}}.$$

The optimal bi-variate distinguisher is:

$$\hat{k} = \arg\max_k \sum_q \log \sum_m \exp -\frac{1}{2\sigma^2} \left\{ \left(X_q^{(0)} - w_H(\phi(m) \oplus S[t_q \oplus k]) \right)^2 + \left(X_q^{(1)} - w_H(m) \right)^2 \right\}$$

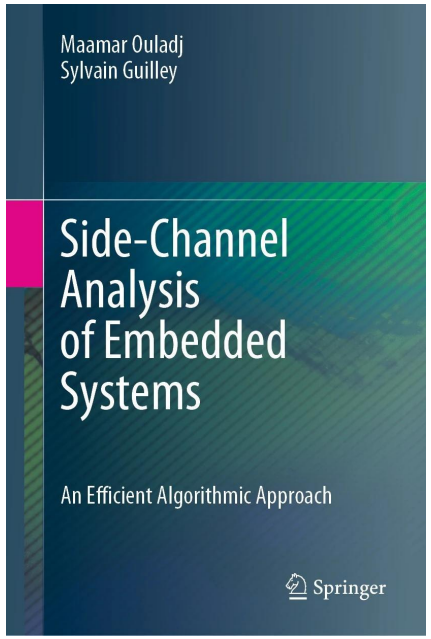
2025 All Rights Reserved I Confidential I Property of Secure-IC

SECURE-IC
THE SECURITY SCIENCE COMPANY

Security evaluation

Computational speed-up:

- The convolution can be optimized with a Fourier transform.
  - On bitvectors, the Fourier transform is called the Walsh-Hadamard transform, denoted by the «hat» notation
- See also our book:



Let f and g two functions $\mathbb{F}_2^k \to \mathbb{R}$. Typically,

$$f(m) = \exp -\frac{1}{2\sigma^2}\left(X_q^{(0)} - w_H(\phi(m) \oplus S[t_q \oplus k])\right)^2$$

and

$$g(m) = \exp -\frac{1}{2\sigma^2}\left(X_q^{(1)} - w_H(m)\right)^2$$

where:

- q is the trace index,
- X_q is the bivariate trace measurement,
- t_q is the plaintext,
- S is the substitution box.

The optimal distinguisher also consists in computing:

$$\begin{aligned}
&\sum_{m \in \mathbb{F}_2^k} f(\phi(m) \oplus S) g(m) \\
&= \sum_{m' \in \mathrm{Im}(\phi)} f(m' \oplus S) g(\phi^{-1}(m')) \\
&= \sum_{m' \in \mathbb{F}_2^n} 1_{\mathrm{Im}(\phi)}(m') f(m' \oplus S) g \circ \phi^{-1}(m') \qquad (2)
\end{aligned}$$

where, for example, $\phi^{-1}(m_1, \ldots, m_{n/k}) = m_1$.

The line (2) is amenable to be computed efficiently leveraging Walsh-Hadamard transform [3] as:

$$\widehat{f 1_{\mathrm{Im}(\phi)}} \widehat{\times} \widehat{g \circ \phi^{-1}}(S).$$

SECURE-IC
THE SECURITY SCIENCE COMPANY

AGENDA

1. Introduction
2. Low-entropy masking scheme compliant with Boolean and Arithmetic computations
3. Security of low-entropy masking schemes
4. Second-order evaluation of low-entropy masking schemes?
5. Conclusion and perspectives

2025 All Rights Reserved I Confidential I Property of Secure-IC

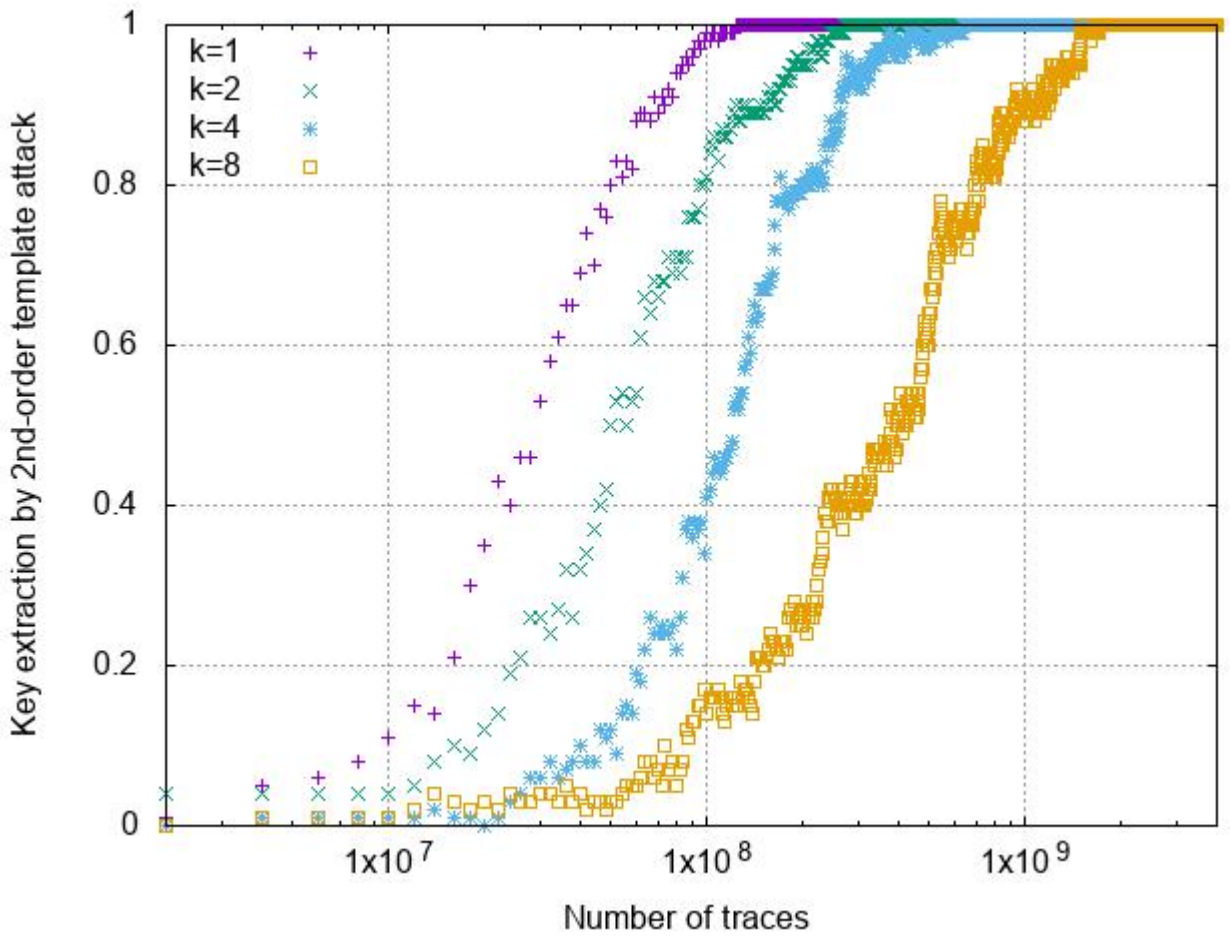
Security evaluation

Results

- Simulations

Entropy	128 bits	64 bits	32 bits	16 bits
Area	100	70	50	35
Security level	800 million traces	400 million traces	200 million traces	100 million traces

- **Hamming weight model:**
  - k out of n=8 bits of entropy
- **The area is defined where the base index is 100 for the 128-bit entropy version. The security level is defined for 2nd order zero-offset attack (with SNR=10^{-4}), the model is derived from ISO/IEC 20085-2:2020(E).**



2025 All Rights Reserved I Confidential I Property of Secure-IC

SECURE-IC
THE SECURITY SCIENCE COMPANY

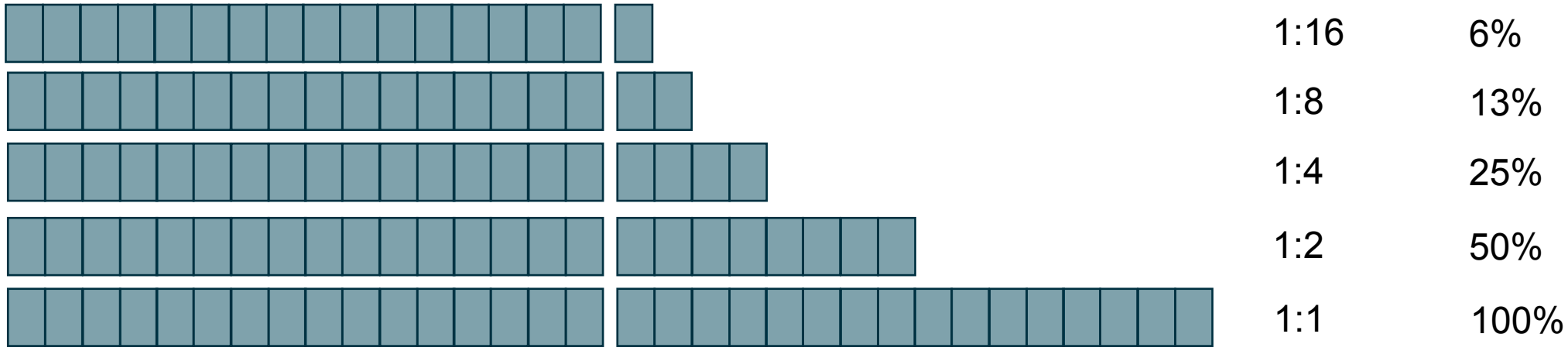
AGENDA

1. Introduction
2. Low-entropy masking scheme compliant with Boolean and Arithmetic computations
3. Security of low-entropy masking schemes
4. Second-order evaluation of low-entropy masking schemes?
5. Conclusion and perspectives

2025 All Rights Reserved I Confidential I Property of Secure-IC

Conclusion & Perspectives

- Another perspective on Arithmetic to Boolean (and vice-versa) masking conversions
- Amenable to some lightweight algorithms
- Scalable masking:



2025 All Rights Reserved I Confidential I Property of Secure-IC

SECURE-IC
THE SECURITY SCIENCE COMPANY

THANK YOU FOR YOUR ATTENTION

CONTACTS

EMEA	sales-EMEA@secure-IC.com
APAC	sales-APAC@secure-IC.com
CHINA	sales-CHINA@secure-IC.com
JAPAN	sales-JAPAN@secure-IC.com
AMERICAS	sales-US@secure-IC.com