On the spectral features of robust probing security

Maria Chiara Molteni[1] Vittorio Zaccaria[2]

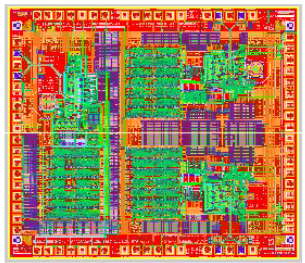
[1]Dipartimento di Informatica "Giovanni Degli Antoni"
Università degli Studi di Milano

[2]Department of Electronics, Information and Bioengineering
Politecnico di Milano

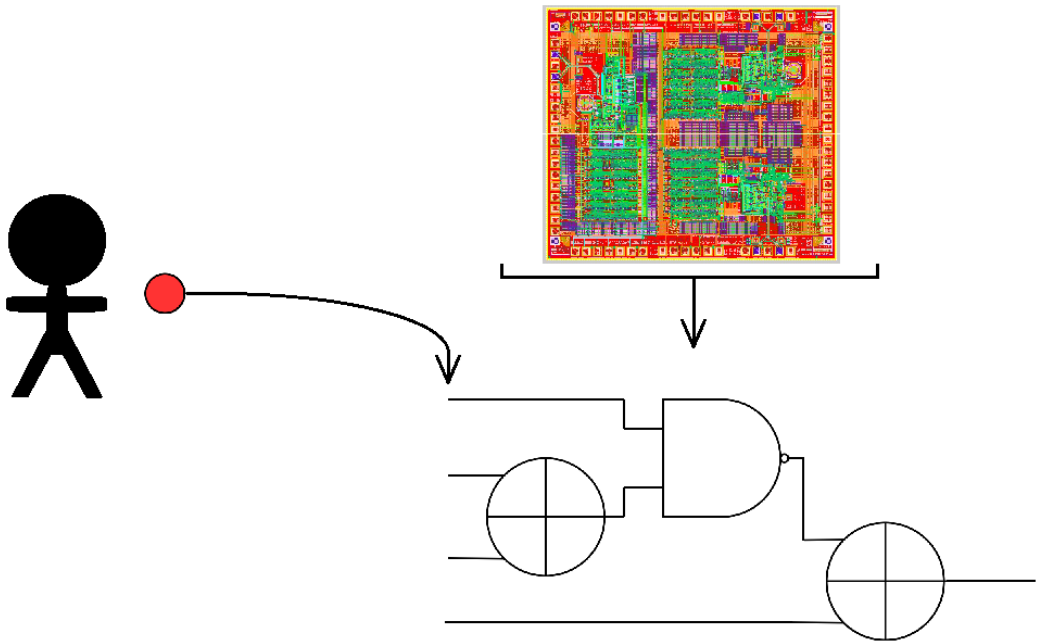
Cryptographic Hardware and Embedded Systems (CHES)
September 2020

Overview

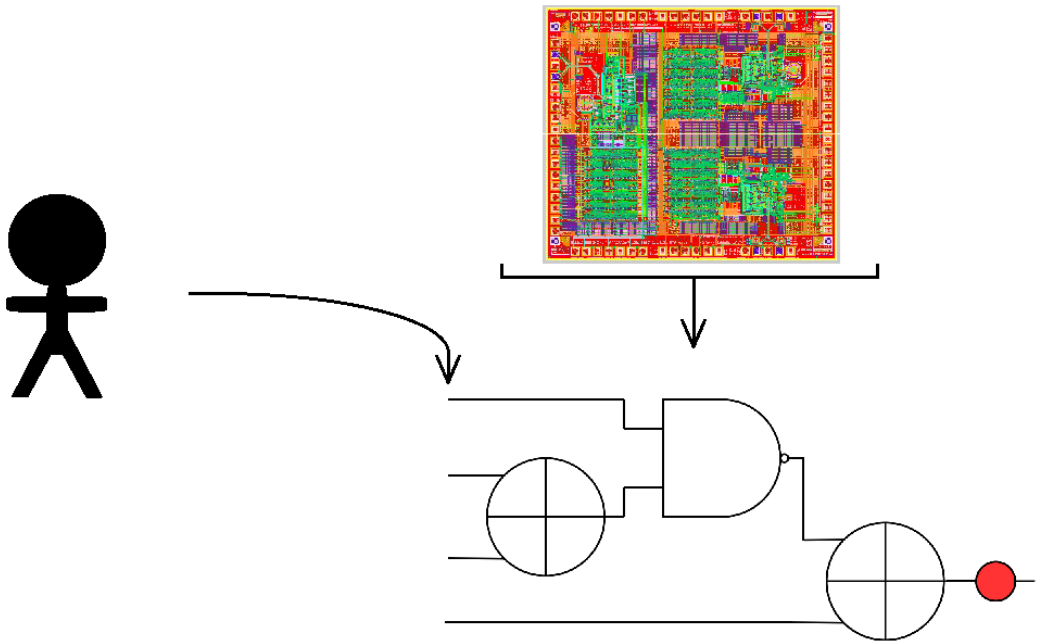
d-PROBING SECURITY



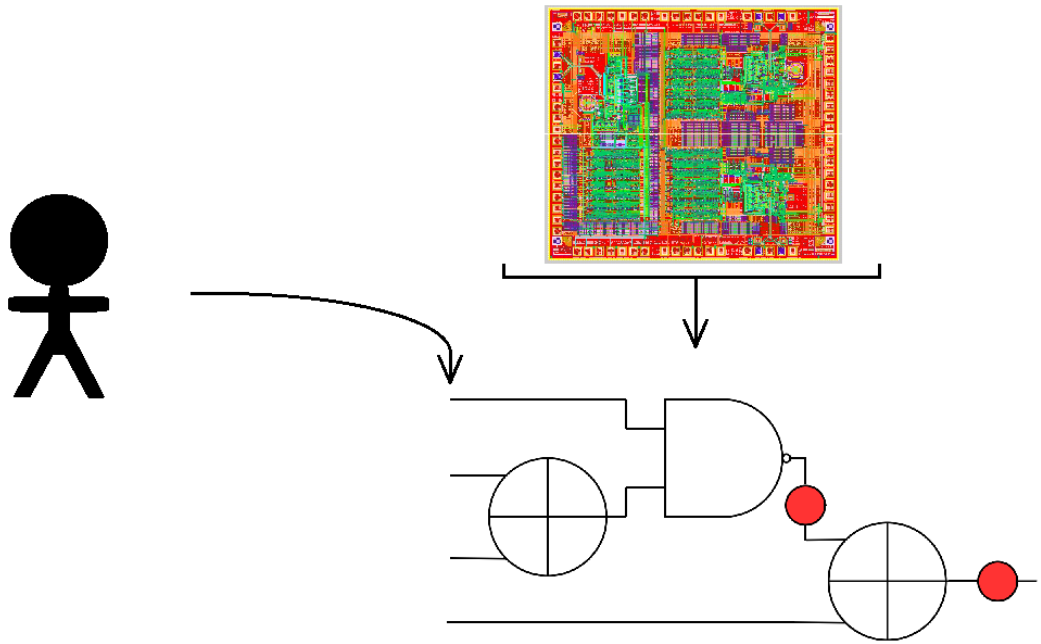
d-PROBING SECURITY



d-PROBING SECURITY



d-probing security



Probing attack

The attacker places a *probe* on a wire of interest and recover some information about the value carried along that wire during computation.

d-probing security

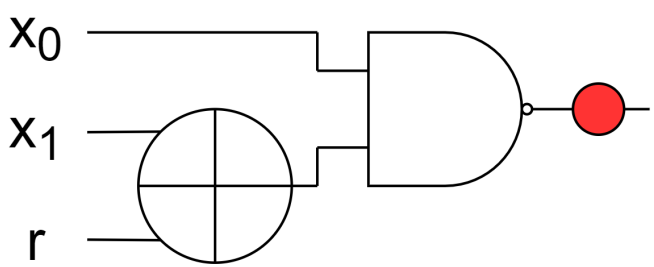
Definition

A gadget is d-**probing secure** if, given at most d probes, it is impossible to derive information about the secret values, also encoded in the masks/shares.

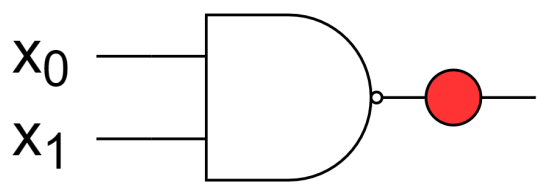
Example

x secret, x_0 and x_1 shares such that $x = x_0 + x_1$

1-probing secure



NOT 1-probing secure



d-Non Interference security

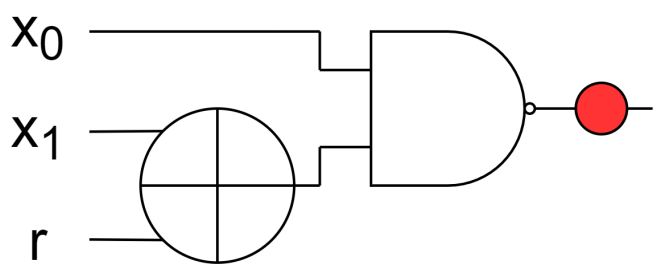
Definition

A gadget is d-**NI** if, given at most d probes, it is possible to derive information about at most d masks/shares of any secret value.

Example

x secret, x_0 and x_1 shares such that $x = x_0 + x_1$

1-NI



d-Strong Non Interference security

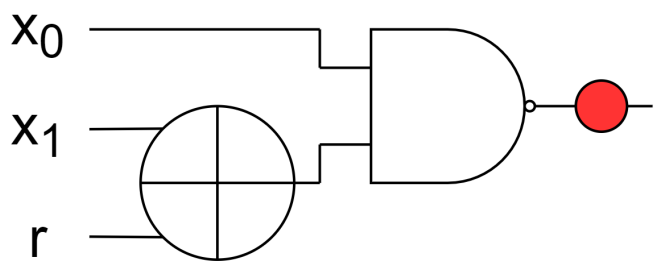
Definition

A gadget is d-**SNI** if, given at most d_1 **internal probes** and d_2 **output probes** such that $d_1 + d_2 = d$, it is possible to derive information about at most d_1 masks/shares of any secret value.

Example

x secret, x_0 and x_1 shares such that $x = x_0 + x_1$

NOT 1-SNI



d-Strong Non Interference security

Definition

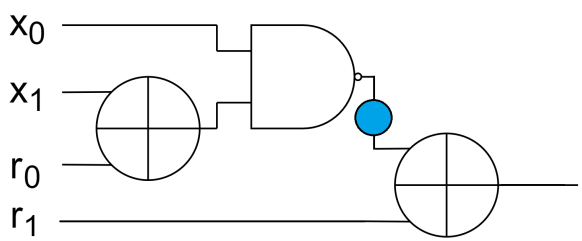
A gadget is d-**SNI** if, given at most d_1 **internal probes** and d_2 **output probes** such that $d_1 + d_2 = d$, it is possible to derive information about at most d_1 secret values, also encoded in the masks/shares.

Example

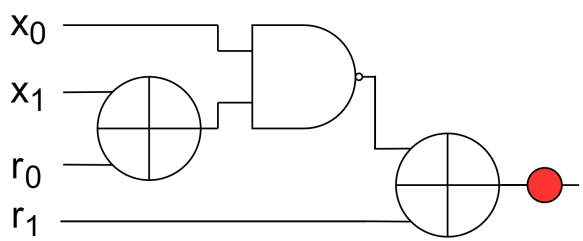
x secret, x_0 and x_1 shares such that $x = x_0 + x_1$

1-SNI

Internal probe



Output probe



Robust Probing Security

Extended Probes

Probes that model the leakage situation in presence of some physical defaults.

Types od Extended probes[1]

- Modelling glitches, i.e. combinatorial recombination
- Modelling transitions, i.e. memory recombinations
- Modelling couplings, i.e.routing recombinations

[1] S. Faust et Al., *Composable Masking Schemes in the Presence of Physical Defaults and the Robust Probing Model*

Motivation: mathematical improvement

Research standpoint

- Previous works: instance-by-instance approaches or tools (maskVerif[2])
- Our work: new conceptual tools to derive general solutions and rules

Development standpoint

- Previous works: efficient approaches might need validation
- Our work: further verification approach based on the exact theory of Boolean Functions

[2] G. Barthe et Al., *maskVerif: automated analysis of software and hardware higher-order masked implementations.*

Our contribution

Exploited tools

- Boolean Function Theory
  - Walsh Matrices
  - Tensor Product
  - String Diagrams

New contributions

- Vulnerability Profile
- Composition Rules
- Classification of Extended Probes

Our method

Walsh Matrix

- Given a Boolean function f, with m inputs and n outputs, any element of its Walsh matrix is:

$$\hat{f}_{\omega,\alpha} = \sum_{x \in \mathbb{F}_2^n} (-1)^{\omega^T f(x) \oplus \alpha^T x}$$

- Matrix that describes the results profile of a Boolean Function
- To any matrix corresponds only one function and viceversa
- Its dimension is $2^n \times 2^m$

Correlation Matrix

Matrix computed from the Walsh matrix:

$$\widetilde{W_f}(\omega, \alpha) := (\hat{f}_{\omega,\alpha} \neq 0)$$

Our method

Example

$$f(a_0, a_1, r_0, r_1) = \begin{bmatrix} o_0 \\ o_1 \\ p_0 \end{bmatrix} = \begin{bmatrix} a_0 + r_0 + r_1 \\ a_1 + r_0 + r_1 \\ a_1 + r_0 \end{bmatrix}$$

Correlation matrix $\widetilde{W_f}$:

	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	
	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	γ_{r_1}
	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	γ_{r_0}
	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	γ_{a_1}
γ_{p_0}	γ_{o_1}	γ_{o_0}															γ_{a_0}
0	0	0	1														
0	0	1												1			
0	1	0													1		
0	1	1			1												
1	0	0					1										
1	0	1										1					
1	1	0							1								
1	1	1				1											

Our method

Compact representation of $\widetilde{W_f}$

Reshaping of the Correlation matrix $\widetilde{W_f}$, by compacting the spectral coefficients, taking into account only the number of shares of each original variable.

Example

		0	0	0	1	1	1	2	2	2	ρ
		0	1	2	0	1	2	0	1	2	α
π	ω										
0	0	1									
0	1								1		
0	2			❶							
1	0					1					
1	1				1		1				
1	2					1					

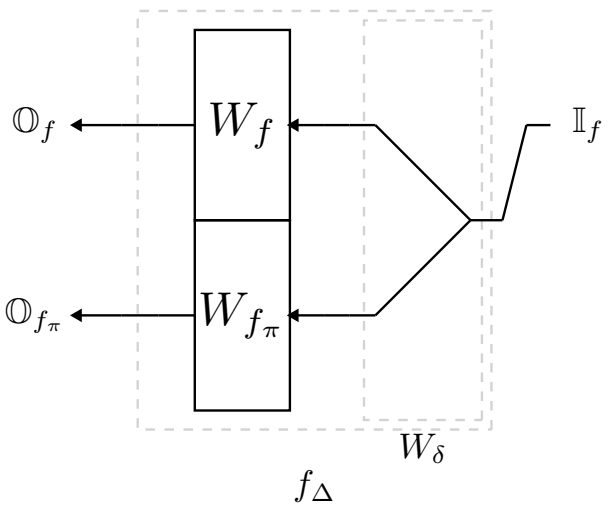
α,ρ, ω and ϕ are called the *compact spectral indexes* of the input, randoms, output and probe respectively

Vulnerability Profile

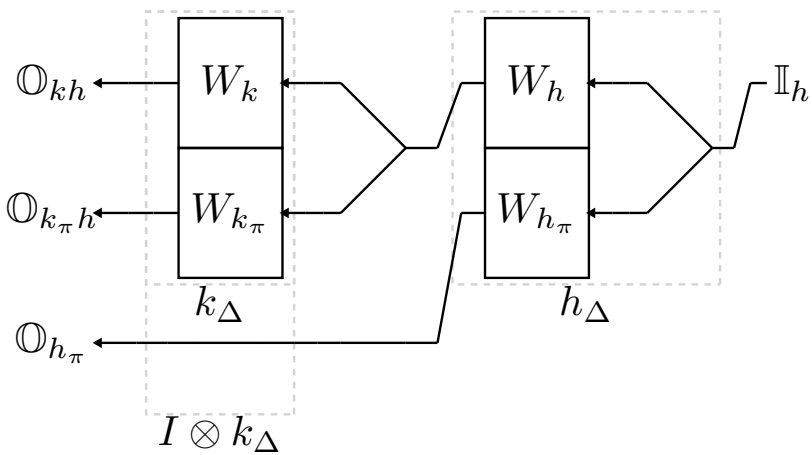
Vulnerability Profile of a function

Tensor product of the regular Walsh transform of a function f and of its probes f_π, multiplied by W_δ

Function f



Composition $h \bullet k$

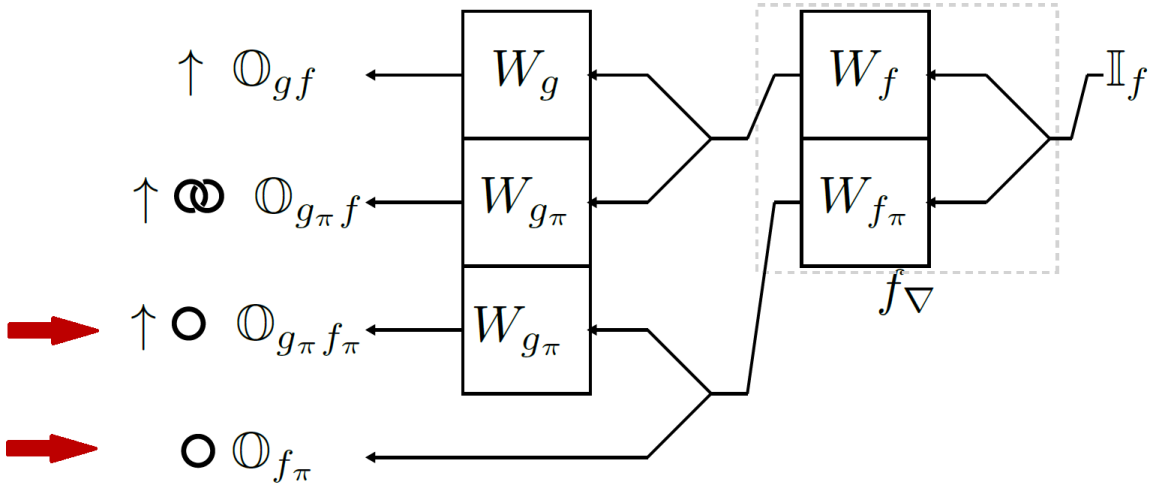


Classification of the Extended Probes

Classification

1. *Pure Probe* ($\circ$): placed on a wire computing $w(x)$, it gives information about all the inputs of the function:

$$w_\pi(x) = \bigwedge_{x_i \in \text{support}(w)} x_i$$



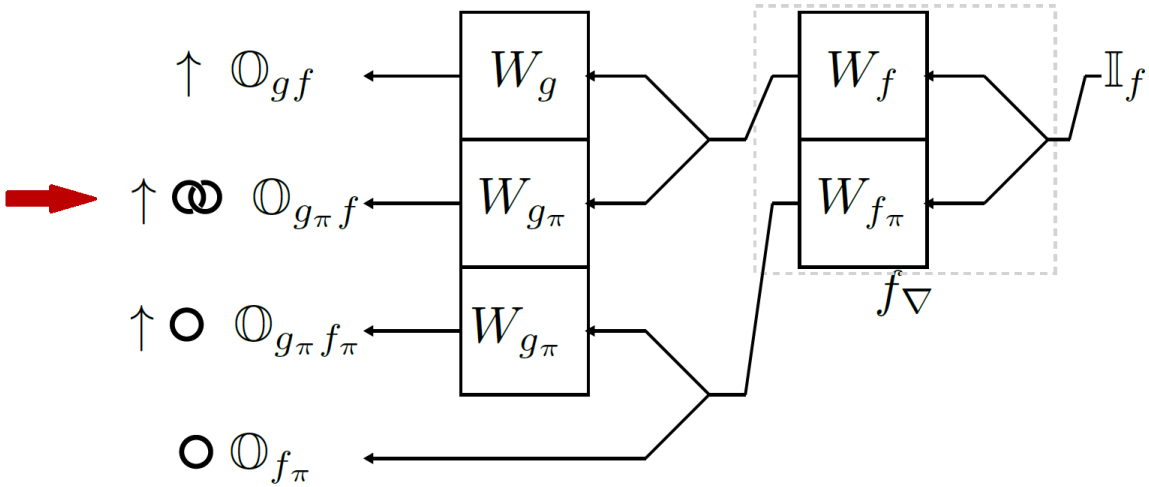
Classification of the Extended Probes

Classification

2. *Composed Probe* (⊚): placed on a wire computing $w(x) = w^a \bullet w^b$, it gives information about the values:

$$w_k(x) = (w^a_\pi \bullet w^b)(x)$$

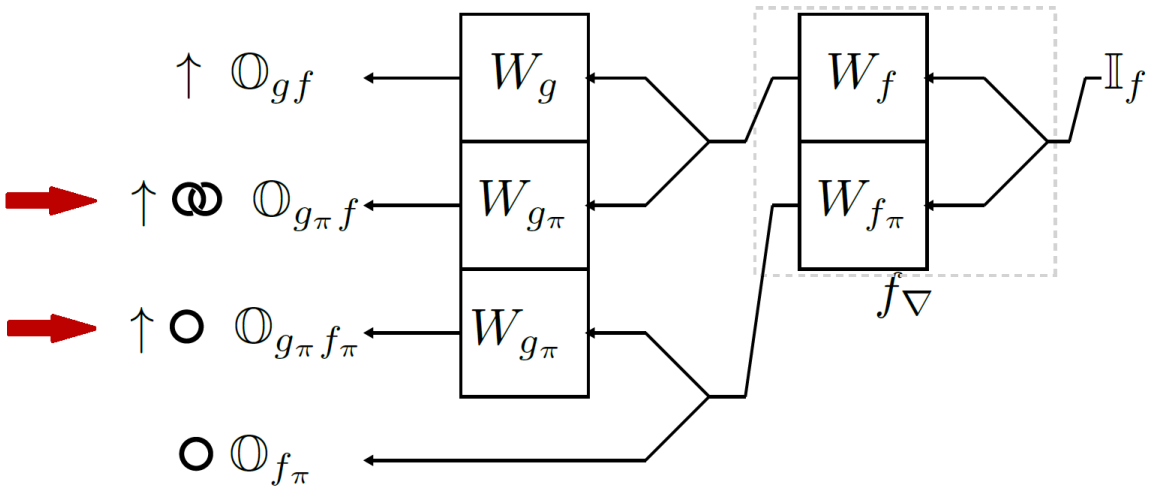
where $w^b(x)$ is different from the identity.



Classification of the Extended Probes

Classification

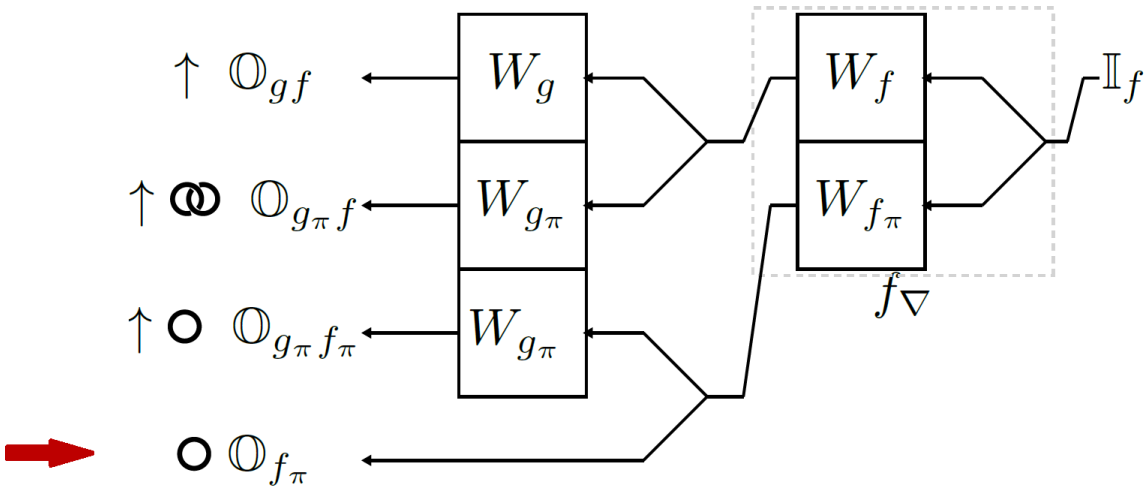
3. *Output Probe* (↑): placed on an actual output of the function; during composition of functions, it could produce new probes



Classification of the Extended Probes

Classification

4. *Internal Probe*: placed on an internal wire; it couldn't produce new probes when composing functions



Applications

Applications to multiplication gadgets

- CMS: analysis and improvement
- DOM-indep: analysis

Consolidating Masking Scheme

CMS[3] multiplication scheme

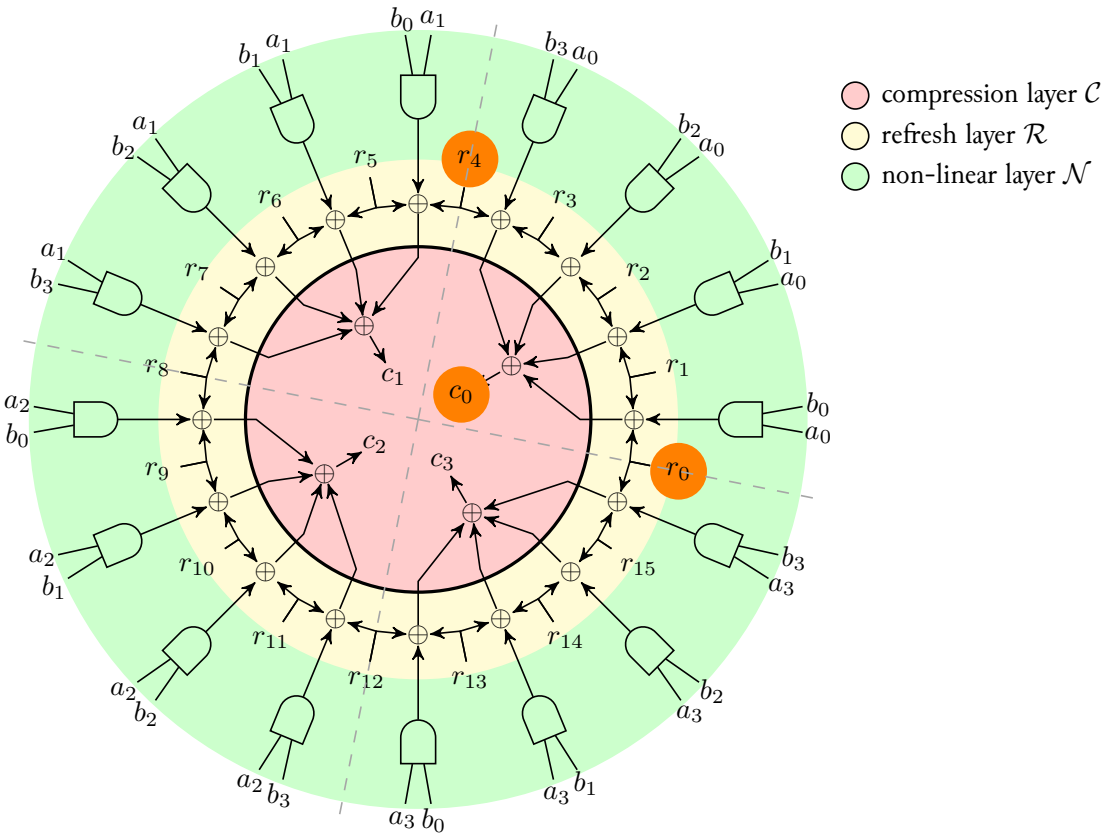
- Evolution of the ISW scheme, meant to provide d-probing security and protection against glitches
- $s = d + 1$ is the number of shares, a_i and b_i are the inputs' shares and c_i are the output's shares
- Every c_i is computed in a *logic cone*, which involves s pairs (a_i, b_h)
- *Adjacent cones* share only a random bit
- Internal bits within a cone preserve uniformity
- Three layers: non-linear ($\mathcal{N}$), refresh ($\mathcal{R}$) and compression ($\mathcal{C}$), the latter two separated by a register

[3] O. Reparaz et Al., *Consolidating Masking Schemes*

CMS and probing security

Problem

This scheme is not robust-d-probing secure for $d \geq 3$ [4]



[4] T. Moos et Al., *Glitch-Resistant Masking Revisited*

Analysis of the CMS probing security

through our classification of extended probes

Types of probes

- **Pure internal probes** at the output of $\mathcal{R}$: information about $\{a_i, b_j, r_{h_1}, r_{h_2}\}$
- **Composed output probes** at the output of $\mathcal{C}$: information about d values computed as $a_i \cdot b_j + r_{h_1} + r_{h_2}$

Fail of CMS, for $d \geq 3$

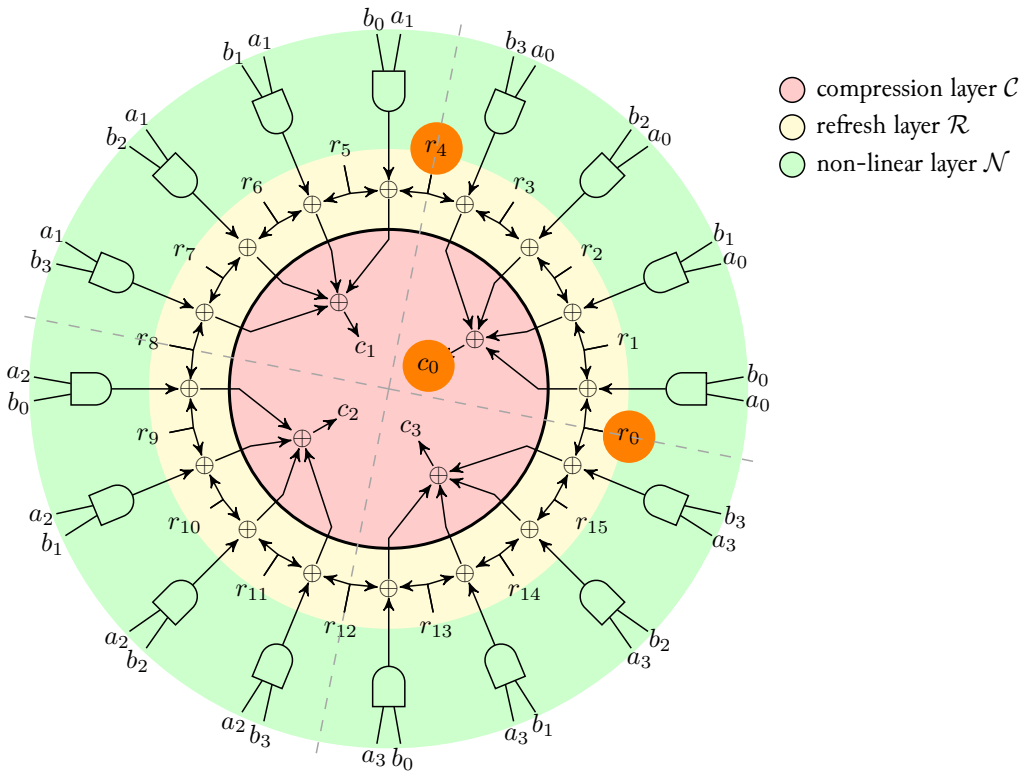
	b_0	b_1	b_2	...	b_d
a_0	c_0	c_0	c_0	...	c_0
a_1	c_1	c_1	c_1	...	c_1
a_2	c_2	c_2	c_2	...	c_2
$\vdots$					
a_d	c_d	c_d	c_d	...	c_d

Secret b placing only one composed probe and two pure probes

Analysis of the CMS probing security

through our classification of extended probes

Example



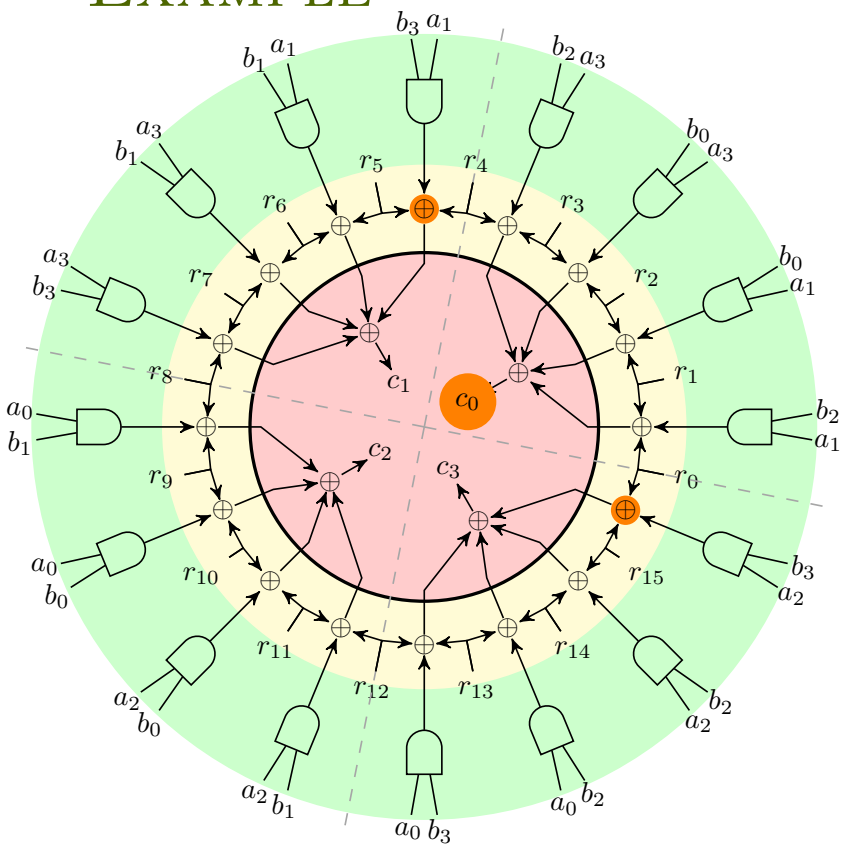
	b_0	b_1	b_2	b_3
a_0	c_0	c_0	c_0	c_0
a_1	c_1	c_1	c_1	c_1
a_2	c_2	c_2	c_2	c_2
a_3	c_3	c_3	c_3	c_3

- Output composed probe c_0
- Internal pure probes to recover r_0 and r_4

1st solution: CMS robust-d-probing secure

Non-completeness

Example



	b_0	b_1	b_2	b_3
a_0	c_2	c_2	c_3	c_3
a_1	c_0	c_1	c_0	c_1
a_2	c_2	c_2	c_3	c_3
a_3	c_0	c_1	c_0	c_1

- No information from any combination of 3 probes

1st solution: CMS robust-d-probing secure

Non-completeness

Example

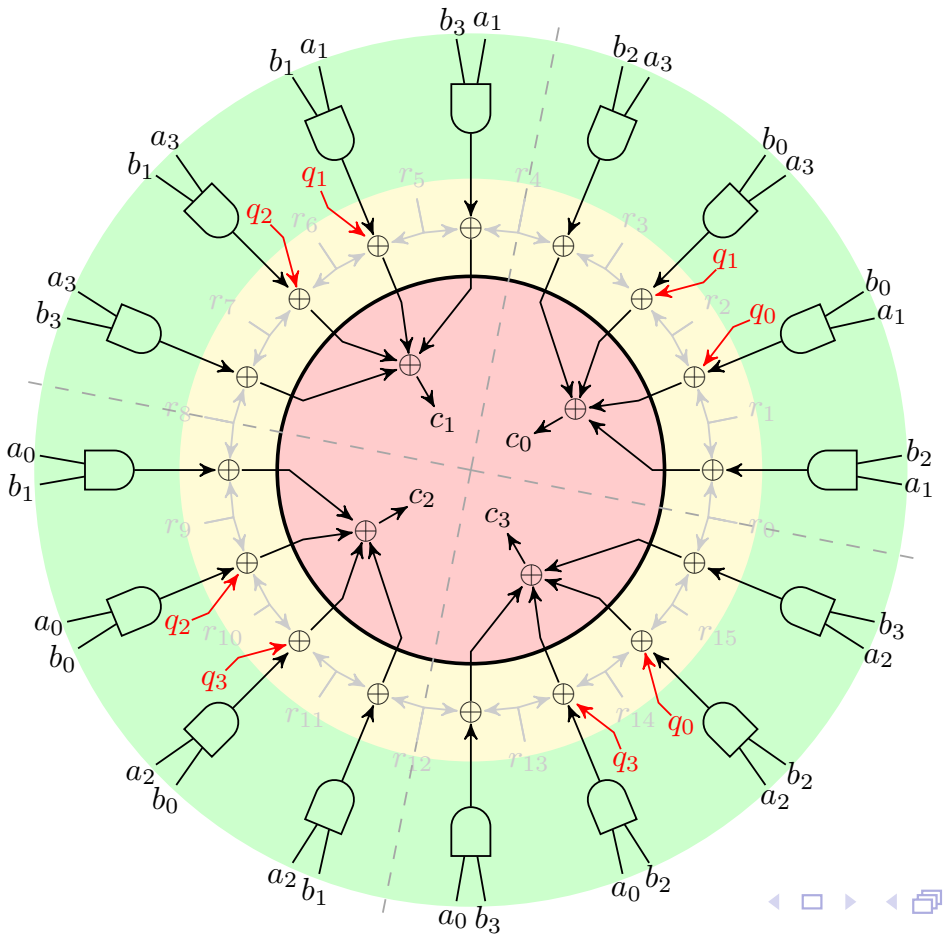
The Compact correlation matrix highlights that, in our first solution, the scheme with $s = 4$ is robust-3-probing secure but not robust-3-SNI

		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	$\dots \rho$
		0	0	0	0	0	1	1	1	1	1	2	2	2	2	2	3	3	3	3	3	4	4	4	4	$\dots \beta$
		0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	$\dots \alpha$
ω_{f_π}	$\omega_{g_\pi f}$																									
$\dots$	$\dots$																									
0	3																									
$\dots$	$\dots$																									
1	2																									
$\dots$	$\dots$																									
2	1	1	1	1	❶		1	1	1	❶		1	1	1	❶		1	1	1	❶						
$\dots$	$\dots$																									
3	0	1	1	1	1		1	1	1	1		1	1	1	1		1	1	1	1						
$\dots$	$\dots$																									

2nd solution: CMS robust-d-SNI

Non-completeness + more randoms

Example



2nd solution: CMS robust-d-SNI

Non-completeness + more randoms

Example

The Compact correlation matrix highlights that, in our second solution, the scheme with $s = 4$ is robust-3-SNI

		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	$\ldots \rho$
		0	0	0	0	0	1	1	1	1	1	2	2	2	2	2	3	3	3	3	3	4	4	4	4	4	$\ldots \beta$
		0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	$\ldots \alpha$
ω_{f_π}	$\omega_{g_\pi f}$																									
$\ldots$	$\ldots$																									
0	3																									
$\ldots$	$\ldots$																									
1	2																									
$\ldots$	$\ldots$																									
2	1																									
$\ldots$	$\ldots$																									
3	0	1	1	1	1		1	1	1	1		1	1	1	1		1	1	1	1						
$\ldots$	$\ldots$																									

2nd solution: CMS robust-d-SNI

Non-completeness + more randoms

Generalization for any d

Let s be the number of shares ($s \geq 4$); any generalized CMS scheme can become robust-$(s-1)$-SNI by adding $s \cdot (\lfloor \frac{s}{2} \rfloor - 1)$ randoms to the refresh layer such that each pair of adjacent cones shares $\lfloor \frac{s}{2} \rfloor - 1$ of them

Domain Oriented Masking

DOM[5] multiplication scheme

- d-probing security by using $\frac{d(d+1)}{2}$ random bits
- $s = d + 1$ is the number of shares, a_i and b_i are the inputs' shares and c_i are the output's shares
- DOM with independent shares is called DOM-indep
- Terms in the DOM-indep equations are inner-domain terms $(a_i b_i)$ and cross-domain $(a_i b_j)$; cross-domain are masked by random bits
- Before the compression phase, partial solutions are saved in registers

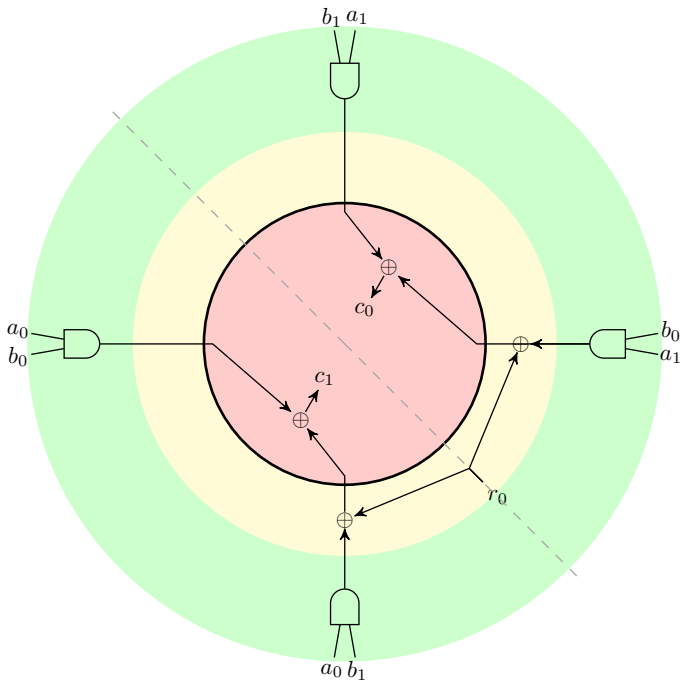
[5] H. Gross et Al., *Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order.*

DOM-indep and probing security

Problem

This scheme is not robust-d-SNI, for any d [6]

Example



[6] T. Moos et Al., *Glitch-Resistant Masking Revisited*

DOM-indep and probing security

Example

The Compact correlation matrix highlights that the scheme with $s = 2$ is robust-1-probing secure but not robust-1-SNI

		0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	ρ
		0	0	0	1	1	1	2	2	2	0	0	0	1	1	1	2	2	2	β
		0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	α
ω_i	ω_o																			
0	0	1																		
0	1	1	❶		❶	❶					1	1		1	1		1	1		
...	...																			
4	4	1	1					1	1						1					

DOM-indep robust-d-SNI

Output registers[7]

Example

The Compact correlation matrix highlights that, with an output register, the scheme with $s = 2$ is robust-1-SNI

		0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	ρ
		0	0	0	1	1	1	2	2	2	0	0	0	1	1	1	2	2	2	β
		0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	α
ω_i	ω_o																			
0	0	1																		
0	1										1	1					1	1		
0	2	1		1				1		1										
1	0	1	1		1	1					1	1		1	1		1	1		
...	...																			
6	2	1	1					1	1						1					

[7] S. Faust et Al., *Composable Masking Schemes in the Presence of Physical Defaults and the Robust Probing Model*

Trade off randomness / registers

To ensure the robust-d-SNI:

- CMS: addition of random bits
- DOM-indep: addition of output registers

Trade off randomness / registers

To ensure the robust-d-SNI:

- CMS: addition of random bits
- DOM-indep: addition of output registers

Example

With $d = 3$:

	random	register (per bit)
CMS	+4	+0
DOM	+0	+4

Trade off randomness / registers

To ensure the robust-d-SNI:

- CMS: addition of random bits
- DOM-indep: addition of output registers

Example

With $d = 3$:

	random	register (per bit)
CMS	$+4$	$+0$
DOM	$+0$	$+4$

Ratio of random usage

$$\frac{2\left(\frac{s^2}{2} + \left(\frac{s}{2} + 1\right) s\right)}{(s-1)\, s}$$

Complexity of the proposed approach

Complexity problem

With the increasing of the variables, the number of elements in the Walsh matrices becomes too large $\rightarrow$ its complete computation becomes impracticable

Complexity of the proposed approach

Complexity problem

With the increasing of the variables, the number of elements in the Walsh matrices becomes too large $\rightarrow$ its complete computation becomes impracticable

Solution

- Store only the rows that refer to single outputs and probes

Complexity of the proposed approach

Complexity problem

With the increasing of the variables, the number of elements in the Walsh matrices becomes too large $\rightarrow$ its complete computation becomes impracticable

Solution

- Store only the rows that refer to single outputs and probes
- Compute on-demand the remaining rows by using convolution

Complexity of the proposed approach

Complexity problem

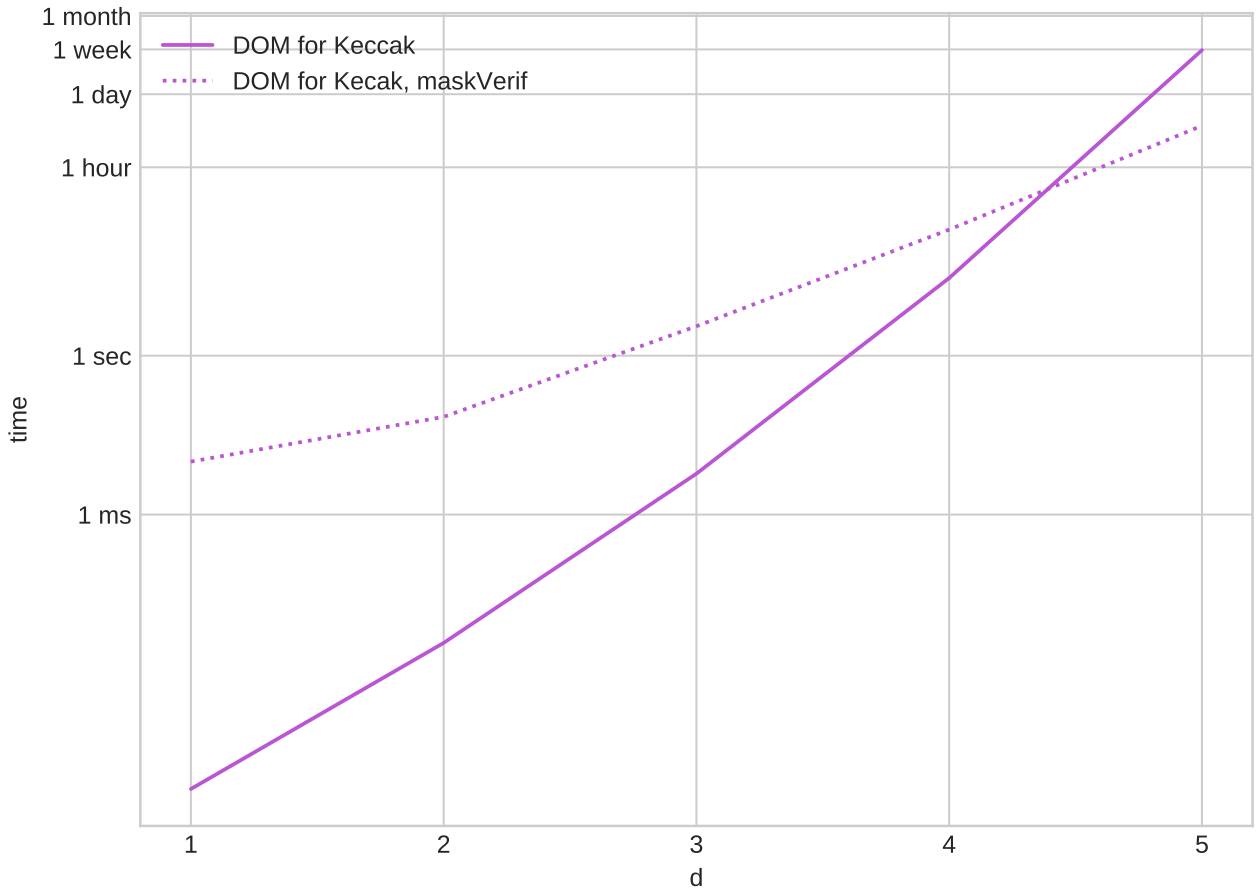
With the increasing of the variables, the number of elements in the Walsh matrices becomes too large $\rightarrow$ its complete computation becomes impracticable

Solution

- Store only the rows that refer to single outputs and probes
- Compute on-demand the remaining rows by using convolution
- Exploit the sparsity of the correlation matrices

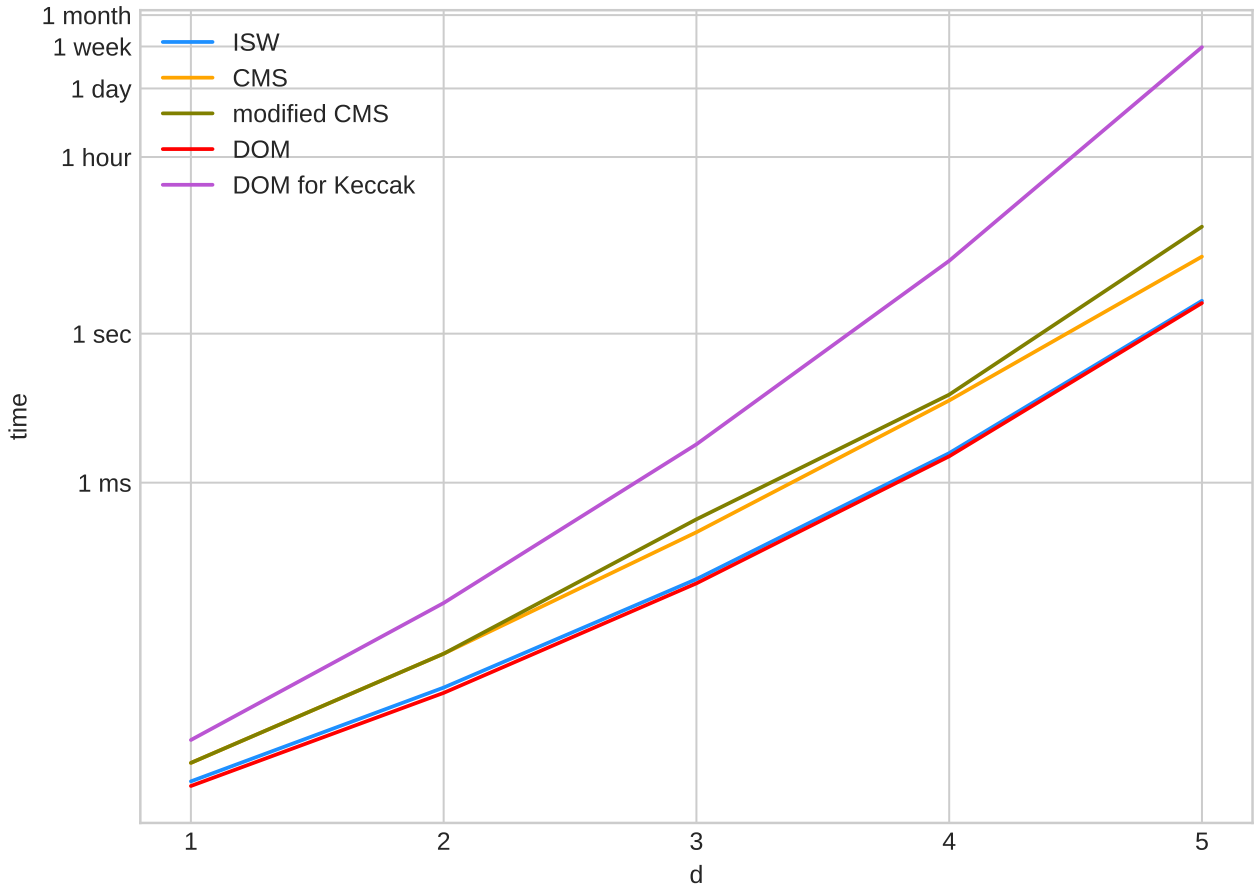
Scalability of the proposed approach

Security verification of χ of Keccak with DOM-indep



Scalability of the proposed approach

Estimated time to compute the compact correlation matrix for gadgets



Conclusion

- Alternative view of robust probing security

Conclusion

- Alternative view of robust probing security
- New mathematical framework and approach, based on the Walsh matrices

Conclusion

- Alternative view of robust probing security
- New mathematical framework and approach, based on the Walsh matrices
- Classification of extended probes, to deal with gadget composability

Conclusion

- Alternative view of robust probing security
- New mathematical framework and approach, based on the Walsh matrices
- Classification of extended probes, to deal with gadget composability
- Applications to multiplication gadgets:
  - improvement of CMS
  - analysis of DOM-indep

Future Works

- More efficient computations, with the use of sparse matrices properties

Future Works

- More efficient computations, with the use of sparse matrices properties
- Inquire the minimum number of randoms to achieve robust-d-SNI

Future Works

- More efficient computations, with the use of sparse matrices properties
- Inquire the minimum number of randoms to achieve robust-d-SNI
- Investigate the ring structure of multiplication gadgets: more efficient refresh layers?

THANK YOU FOR THE ATTENTION

Any question?

You can also write to me at the address
maria.molteni@unimi.it