LABORATOIRE HUBERT CURIEN

UMR • CNRS • 5516 • SAINT-ETIENNE

Asynchronous S-Boxes: Designing Clockless First-Order Masked Functions

Mateus Simões

Agenda

1 Introduction

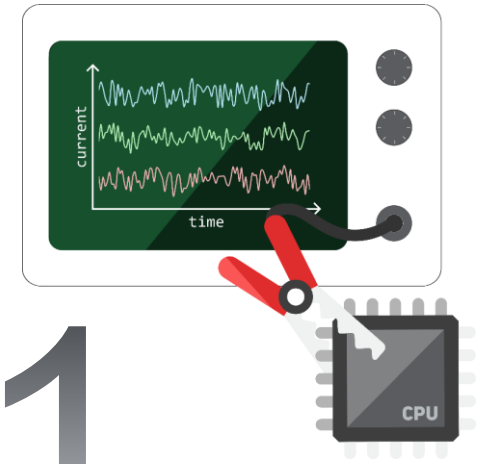
2 Self-Timed Masking

3 Implementation Results

4 Conclusion

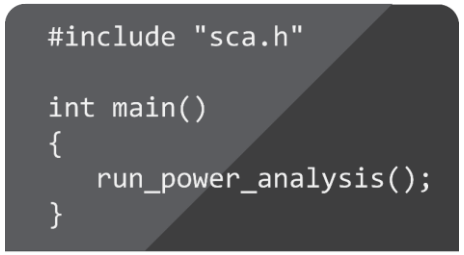
life.augmented

Side-Channel Attacks (SCA) [KJJ99]



1

The attacker measures the device's power consumption during the encryption

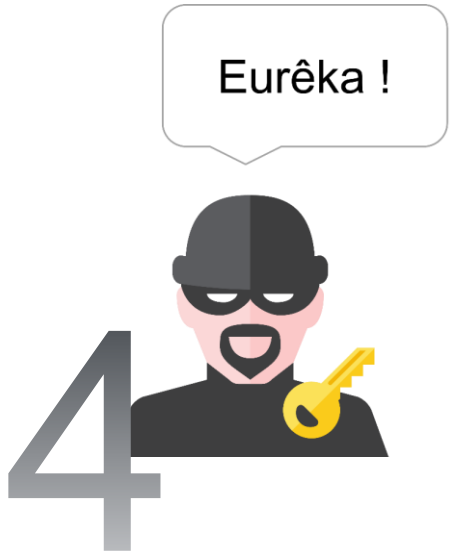


2

From the acquired data, the attacker performs several side-channel analysis.

3

The analysis rank all possible key hypothesis, in order to find the secret key.



4

If the analysis is successful, the attacker has therefore access to the encrypted data.

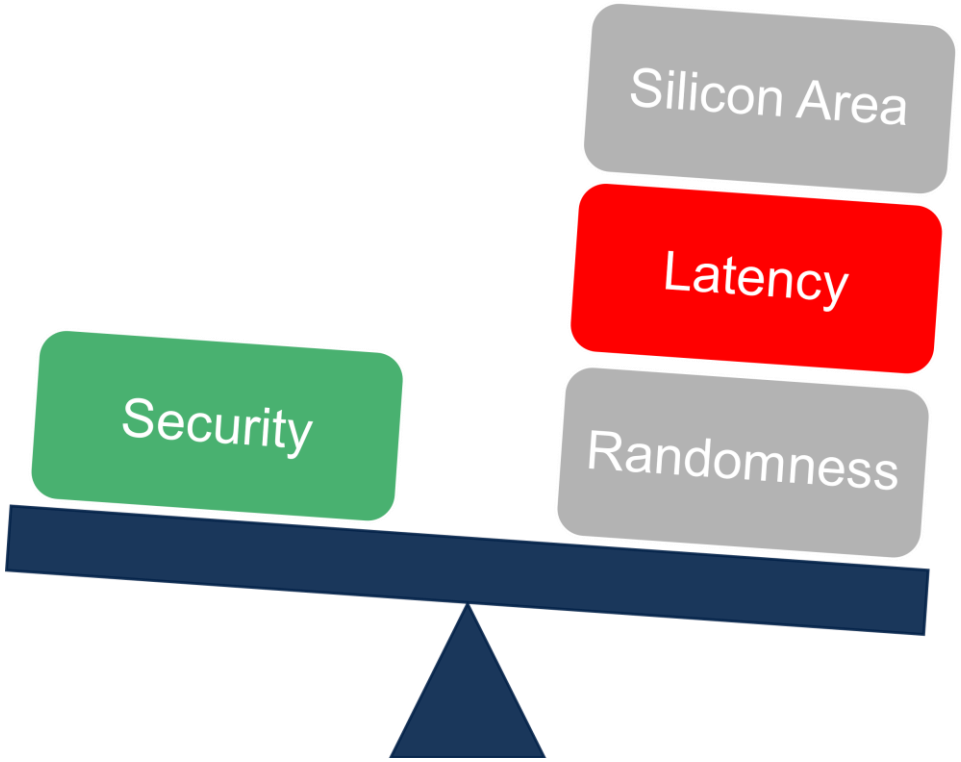
life.augmented

d-Order Boolean Masking [GP99]

A secret Boolean variable x is split into $d + 1$ shares x_i:

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

The side-channel behavior depends on the random shares of x, not on x itself.



Objectives

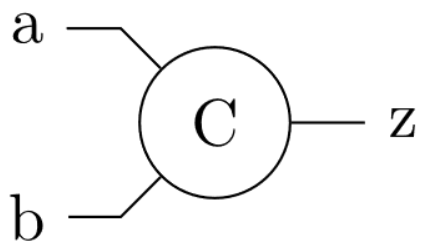
1	Replace registers with asynchronous latches in order to obtain self-timed masking schemes.
2	Evaluate the performance of secure masked schemes operating as self-timed circuits.
3	Evaluate the importance of fresh randomness in self-timed masked implementations.

life.augmented

Self-Timed Masking

Self-Timed Latches [MB59]

Built upon Muller c-elements [MB59].



a	b	z_{n+1}
0	0	**0**
0	1	z_n
1	0	z_n
1	1	**1**

Figure: A Muller c-element's symbol and its truth table.

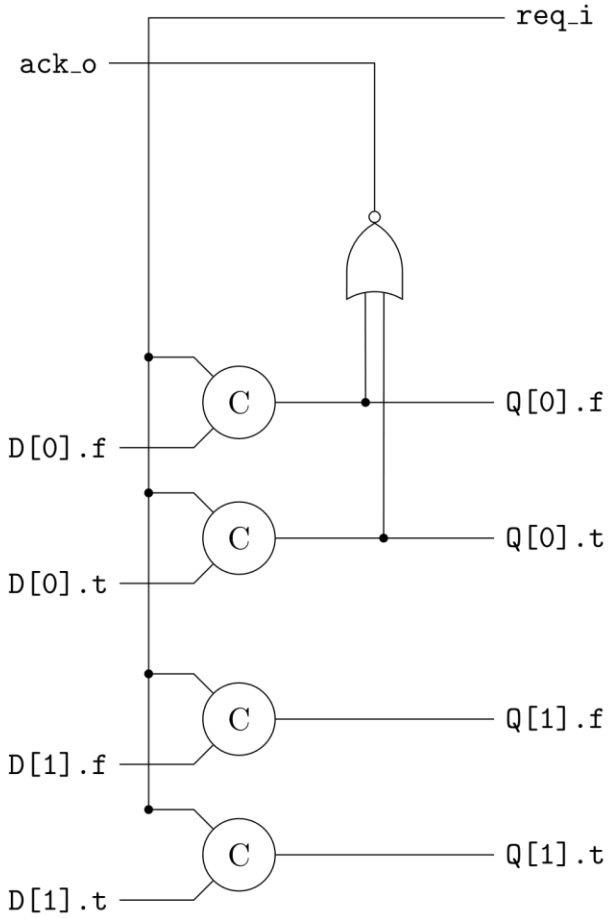


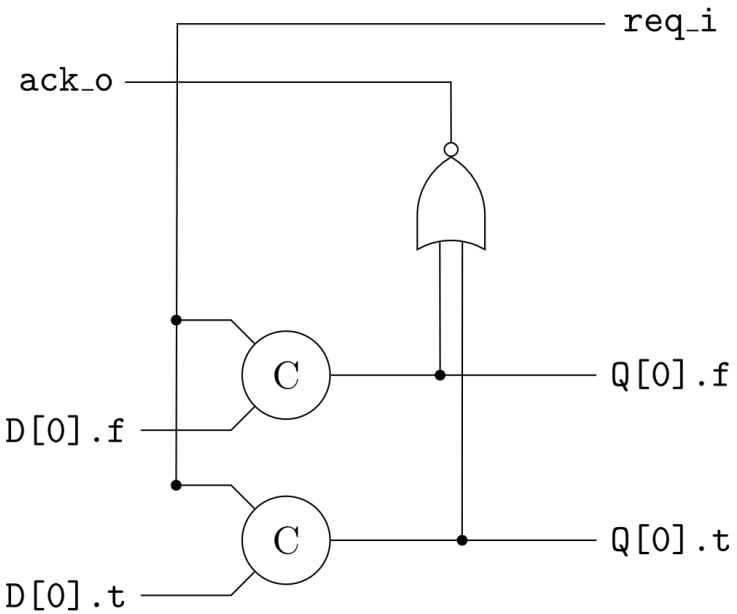
Figure: The self-timed latch.

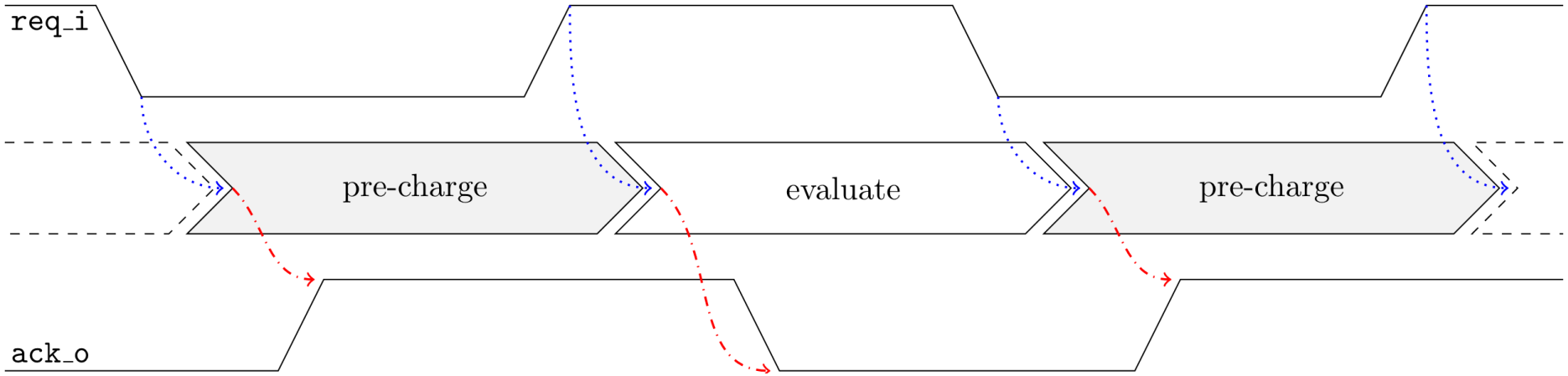
life.augmented

Dual-Rail Protocol with Pre-Charge / Evaluate Logic

Encodes a bit using two signals [DN95].

Token x	x.t	x.f
Null (Ø)	0	0
0	0	1
1	1	0
Not Used	1	1





life.augmented

The Danger of Glitches

A glitchy function may leak the secret variable [MPG05, MPO05].

$$f_0(x_0, y_0, y_1) = x_0 y_0 \oplus x_0 y_1 \rightarrow \text{⚡} \rightarrow x_0 \oplus y$$

f_0 depends on the secret y

Let us suppose a signal b is faster than a:

Input Transition		Dual-Rail Function		
$a_I \rightarrow a_F$	$b_I \rightarrow b_F$		$z = a\ AND\ b$	$z = a\ XOR\ b$
$1 \rightarrow 0$	$0 \rightarrow 1$	z.t	$0 \rightarrow 1 \rightarrow 0$ ⚠	$1 \rightarrow 0 \rightarrow 1$ ⚠
$1 \rightarrow 0$	$1 \rightarrow 0$		$1 \rightarrow 0$	$0 \rightarrow 1 \rightarrow 0$ ⚠

life.augmented

Avoiding Glitches [Juk21]

Dual-Rail Functions

a	b	z
∅	∅	∅
∅	valid	∅
valid	∅	∅
valid	valid	valid

Pre-Charge / Evaluate Logic

+

Dual-Rail Monotonic Functions

No Glitches

Stage	Input Transition		Dual-Rail Function	
	$a_I \rightarrow a_F$	$b_I \rightarrow b_F$	$z = a\ AND\ b$	$z = a\ XOR\ b$
Pre-Charge	$1 \rightarrow \emptyset$	$0 \rightarrow \emptyset$	$0 \rightarrow \emptyset$	$1 \rightarrow \emptyset$
	$1 \rightarrow \emptyset$	$1 \rightarrow \emptyset$	$1 \rightarrow \emptyset$	$0 \rightarrow \emptyset$
Evaluate	$\emptyset \rightarrow 1$	$\emptyset \rightarrow 1$	$\emptyset \rightarrow 0$	$\emptyset \rightarrow 0$
	$\emptyset \rightarrow 1$	$\emptyset \rightarrow 0$	$\emptyset \rightarrow 0$	$\emptyset \rightarrow 1$

life.augmented

Single-Cycle Processing

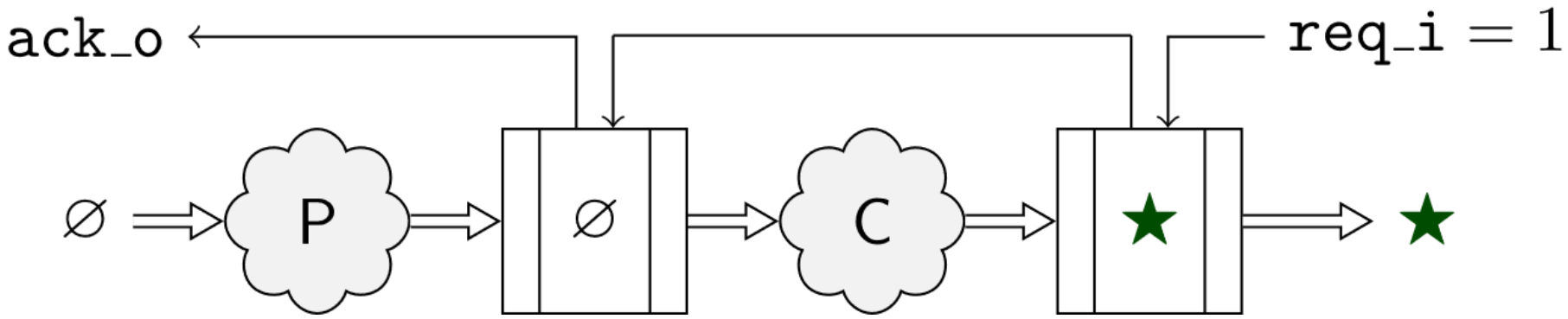
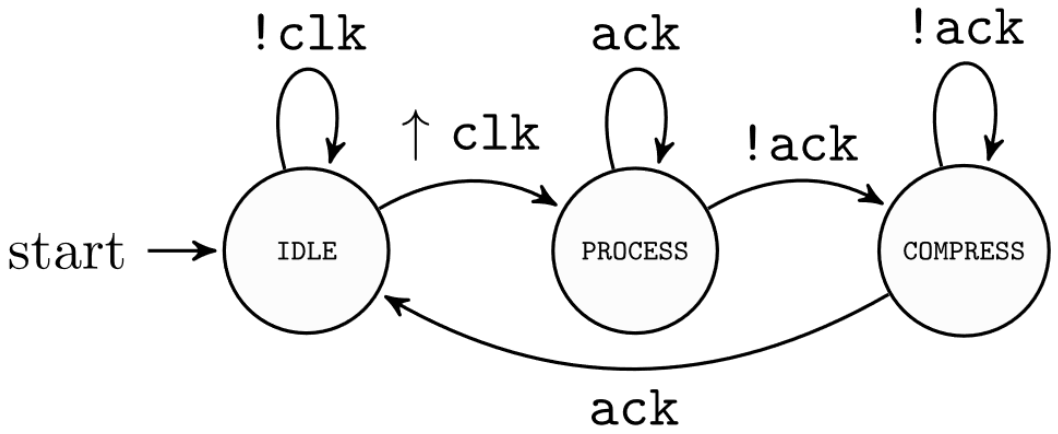


Figure: The self-timed PRESENT S-box.



State	S-box Inputs	
	token	req_i
IDLE	∅	1
PROCESS	⋆	0
COMPRESS	∅	1

Self-Timed Gadgets

Replacing Registers with Self-Timed Latches

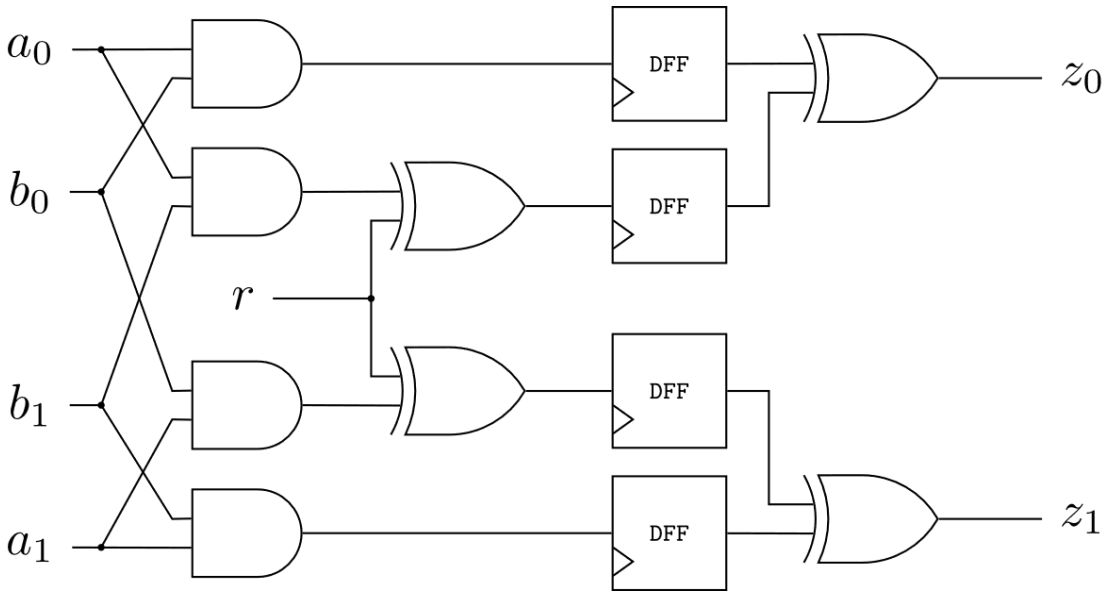


Figure: Original DOM Gadget [GMK16].

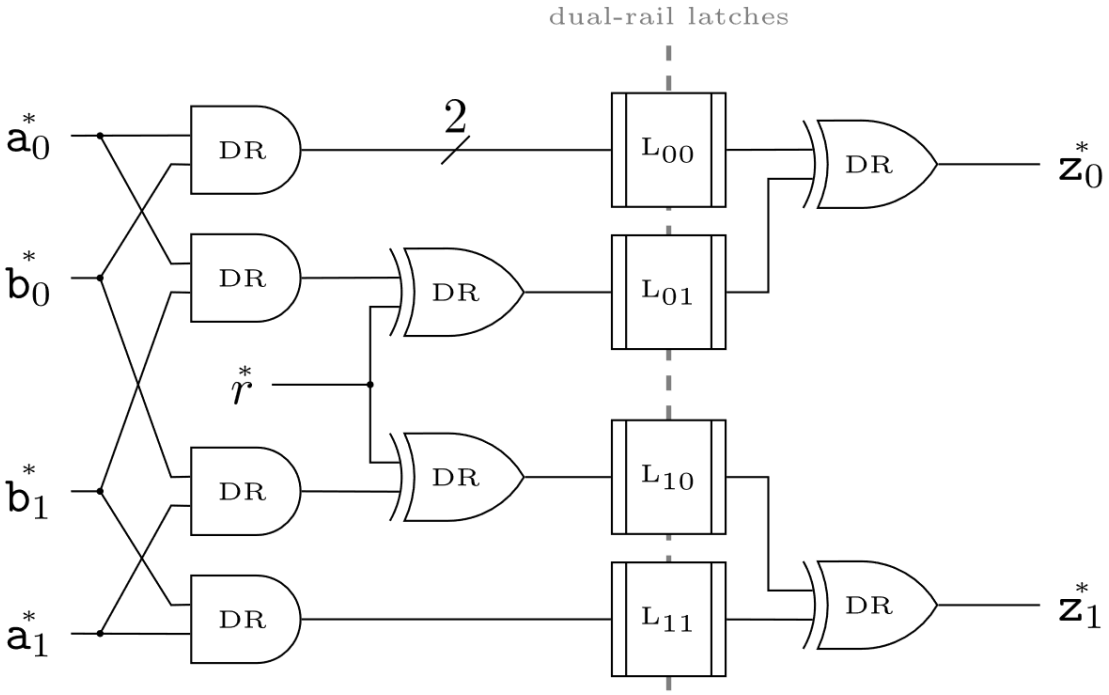


Figure: Self-Timed DOM Gadget.

life.augmented

Randomness *vs* Self-Timed Masking

Data dependent evaluation time may be a threat to self-timed circuits.

Does the self-timed feature guarantee first-order masking security?

S-boxes without random refresh bits	S-boxes with random refresh bits
❑PRESENT [SM21] ❑AES [SM21]	❑TI PRESENT ❑DOM AES [GMK16]

Implementation Results

Implementation Results | PRESENT and AES S-boxes

Design	Shares	Area [1] [kGE]	Refresh [bits]	Latency [cycles]	Standard Cell Library
PRESENT [PMK+11]	3	0.36	0	1	UCM 180-nm
PRESENT [this work]	**2**	**0.99**	**0**	**1**	**STM 40-nm**
PRESENT [this work]	**2**	**1.02**	**8**	**1**	**STM 40-nm**
AES [UHA17]	2	1.40	64	5	TMSC 65-nm
AES [WM18]	4	4.20	0	16	UCM 180-nm
AES [Sug19]	3	3.50	0	4	NanGate 45-nm
AES [GMK16]	2	2.80	28	5	UCM 180-nm
AES [GMK16]	2	2.60	18	8	UCM 180-nm
AES [this work]	**2**	**7.79**	**0**	**1**	**STM 40-nm**
AES [this work]	**2**	**6.07**	**18**	**1**	**STM 40-nm**

[1] ***based on a 2-input NAND gate.***

life.augmented

Simulating Side-Channel Behavior

- ✓ Test Vector Leakage Assessment (TVLA) [GJJR11]
- ✓ 2 million fixed *vs* random simulated traces
- ✓ Noiseless analysis
- ✓ 1 ps time span

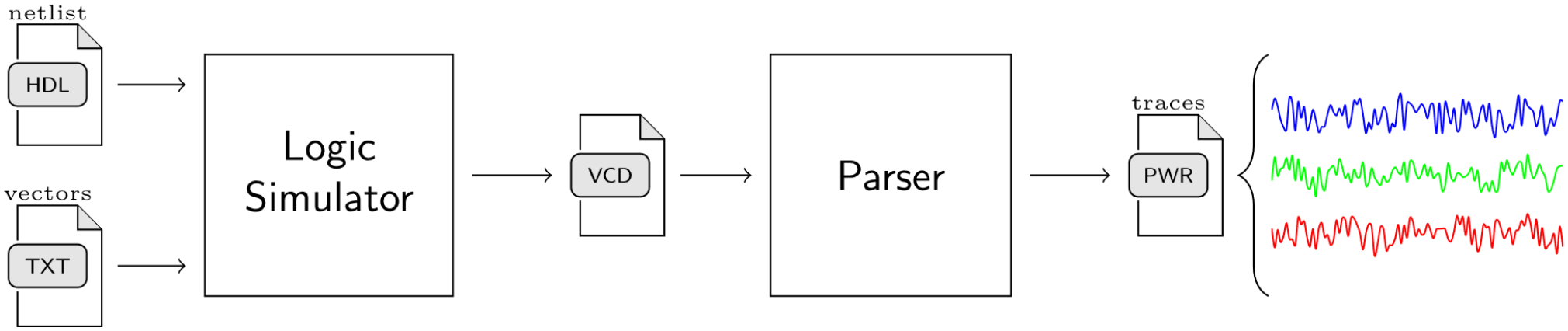


Figure: Modeling the power consumption based on the system's toggling activity.

TVLA: PRESENT S-boxes

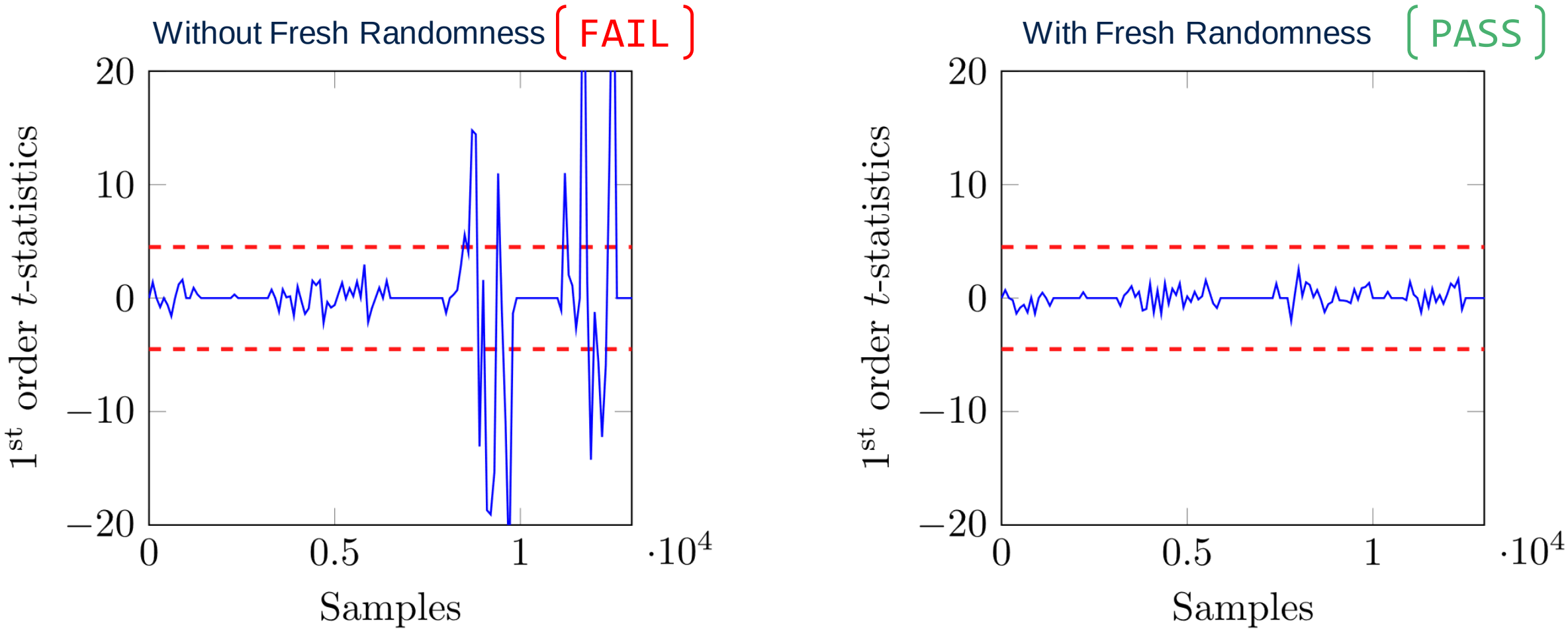


Figure: Based on two million simulated traces.

TVLA: AES S-boxes

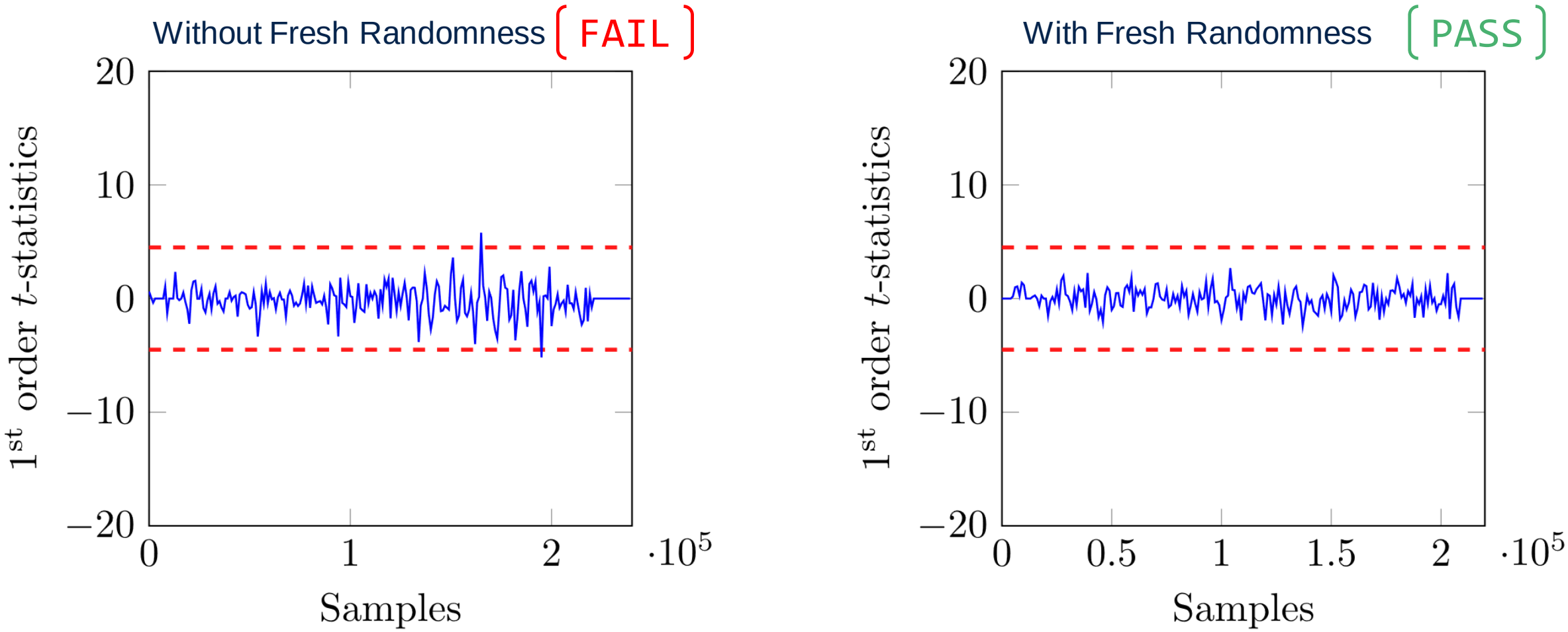


Figure: Based on two million simulated traces.

Conclusion

Conclusion

1. Use of self-timed latches to obtain single-cycle hardware masked S-boxes.
2. Implementation of glitch-free circuits using monotonic logic.
3. How to avoid the early propagation effect in dual-rail gadgets.
4. Locally-asynchronous globally synchronous implementation.
5. Needs fresh randomness in order to be first order secure.

life.augmented

Possible Future Work

1	Implement self-timed higher-order hardware masked S-boxes.
2	From the self-timed S-boxes, design their respective ciphers.
3	Obtain the performance figures from simulation and FPGA.

life.augmented

Our technology starts with You

life.augmented

Bibliography

[DN95] Al Davis and Steven M Nowick, Asynchronous circuit design: Motivation, background, & methods, Asynchronous Digital Circuit Design, Springer, 1995, pp. 1–49.

[GJJR11] Gilbert Goodwill, Benjamin Jun, Joshua Jaffe, and Pankaj Rohatgi, A testing methodology for side channel resistance, 2011.

[GMK16] Hannes Groß, Stefan Mangard, Thomas Korak: Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order. TIS@CCS 2016: 3

[GP99] Louis Goubin, Jacques Patarin: DES and Differential Power Analysis (The "Duplication" Method). CHES 1999: 158-172

[Juk21] Stasys Jukna. Notes on hazard-free circuits. SIAM J. Discret. Math., 35(2):770–787, 2021.

[KJJ99] Paul C. Kocher, Joshua Jaffe, Benjamin Jun: Differential Power Analysis. CRYPTO 1999: 388-397

[MB59] David E. Muller and W. S. Bartky, A theory of asynchronous circuits, Proceedings of an International Symposium on the Theory of Switchinge, April 1957, Part I, the annals of the computation laboratory of Harvard University

[MPG05] Stefan Mangard, Thomas Popp, Berndt M. Gammel: Side-Channel Leakage of Masked CMOS Gates. CT-RSA 2005: 351-365

Bibliography

[MPO05] Stefan Mangard, Norbert Pramstaller, Elisabeth Oswald: Successfully Attacking Masked AES Hardware Implementations. CHES 2005: 157-171

[PMK+11] Axel Poschmann, Amir Moradi, Khoongming Khoo, Chu-Wee Lim, Huaxiong Wang, San Ling: Side-Channel Resistant Crypto for Less than 2, 300 GE. J. Cryptol. 24(2): 322-345 (2011)

[SM21] Aein Rezaei Shahmirzadi, Amir Moradi: Re-Consolidating First-Order Masking Schemes Nullifying Fresh Randomness. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2021(1): 305-342 (2021)

[Sug19] Takeshi Sugawara: 3-Share Threshold Implementation of AES S-box without Fresh Randomness. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2019(1): 123-145 (2019)

[UHA17] Rei Ueno, Naofumi Homma, Takafumi Aoki: A Systematic Design of Tamper-Resistant Galois-Field Arithmetic Circuits Based on Threshold Implementation with (d + 1) Input Shares. ISMVL 2017: 136-141

[WM18] Felix Wegener, Amir Moradi: A First-Order SCA Resistant AES Without Fresh Randomness. COSADE 2018: 245-262

Self-Timed Latches

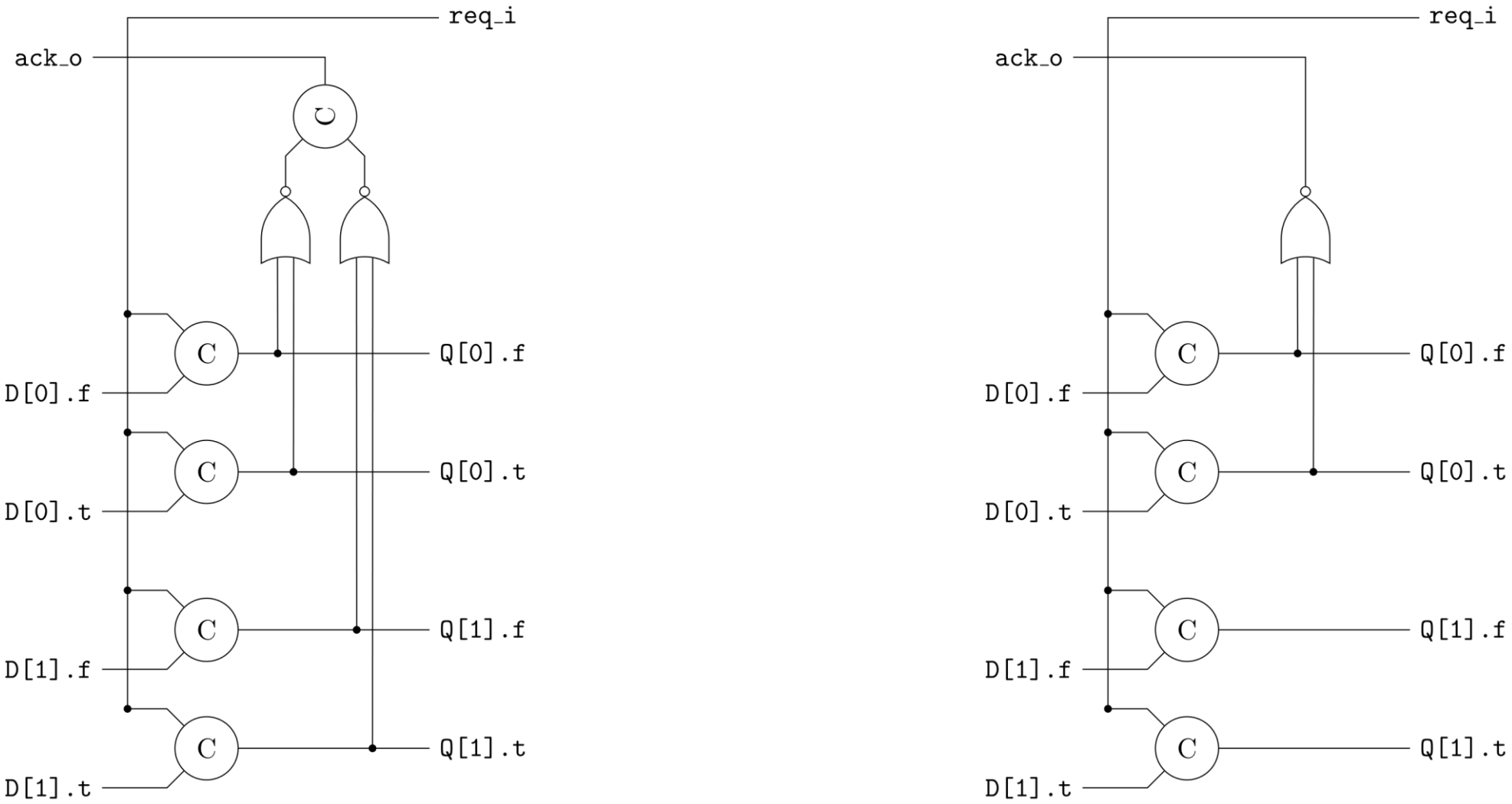
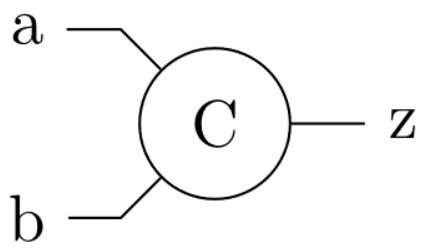


Figure: Strongly indicating (left) and weakly indicating (right) latches.

Muller c-Element [MB59]



a	b	z_{n+1}
0	0	**0**
0	1	z_n
1	0	z_n
1	1	**1**

Figure: The Muller c-element symbol and truth table.

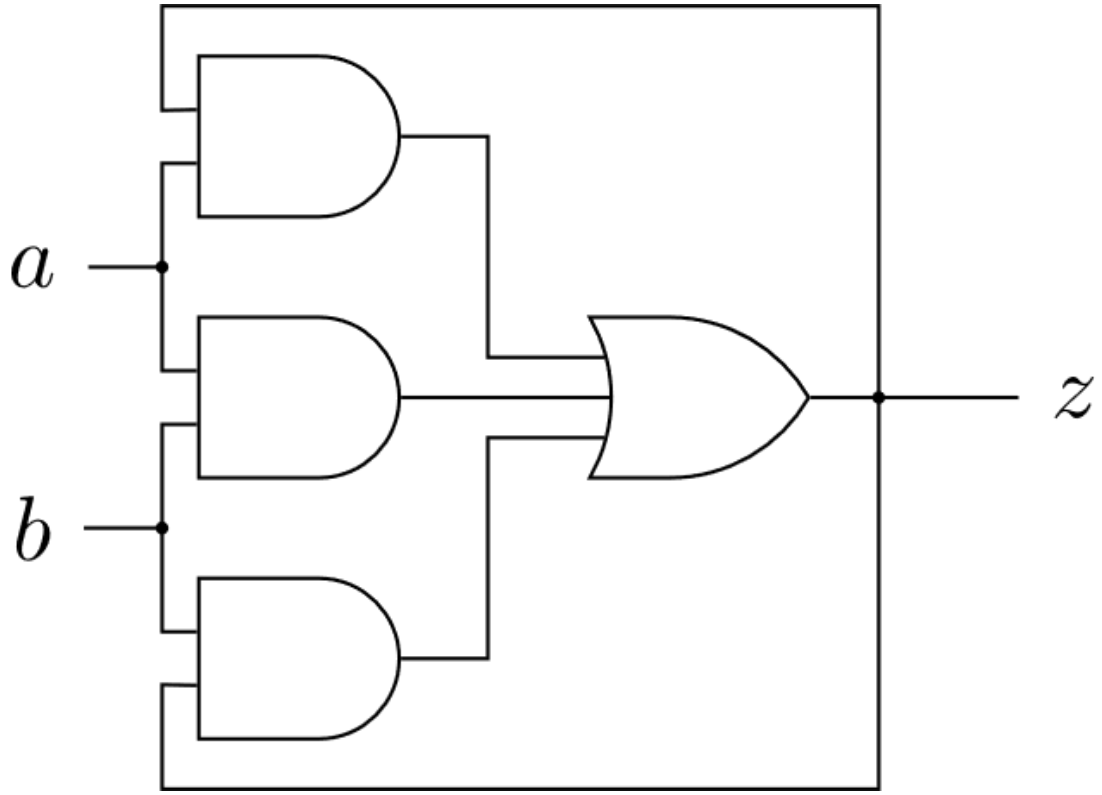


Figure: gate-level implantation.

life.augmented

The Danger of Glitches

A glitchy function may leak the secret variable [MPG05, MPO05].

$$f_0(x_0, y_0, y_1) = x_0 y_0 \oplus x_0 y_1 \rightarrow \text{⚡} \rightarrow x_0 \oplus y$$

Input Transition		Dual-Rail Function		
$a_I \rightarrow a_F$	$b_I \rightarrow b_F$		$z = a\ AND\ b$	$z = a\ XOR\ b$
$0 \rightarrow 1$	$0 \rightarrow 1$	z.t	$0 \rightarrow 1$	$0 \rightarrow 1 \rightarrow 0$ ⚠
$0 \rightarrow 1$	$1 \rightarrow 0$		0	$1 \rightarrow 0 \rightarrow 1$ ⚠
$1 \rightarrow 0$	$0 \rightarrow 1$		$0 \rightarrow 1 \rightarrow 0$ ⚠	$1 \rightarrow 0 \rightarrow 1$ ⚠
$1 \rightarrow 0$	$1 \rightarrow 0$		$1 \rightarrow 0$	$0 \rightarrow 1 \rightarrow 0$ ⚠
$0 \rightarrow 1$	$0 \rightarrow 1$	z.f	$1 \rightarrow 0$	$1 \rightarrow 0 \rightarrow 1$ ⚠
$0 \rightarrow 1$	$1 \rightarrow 0$		1	$0 \rightarrow 1 \rightarrow 0$ ⚠
$1 \rightarrow 0$	$0 \rightarrow 1$		$1 \rightarrow 0 \rightarrow 1$ ⚠	$0 \rightarrow 1 \rightarrow 0$ ⚠
$1 \rightarrow 0$	$1 \rightarrow 0$		$0 \rightarrow 1$	$1 \rightarrow 0 \rightarrow 1$ ⚠

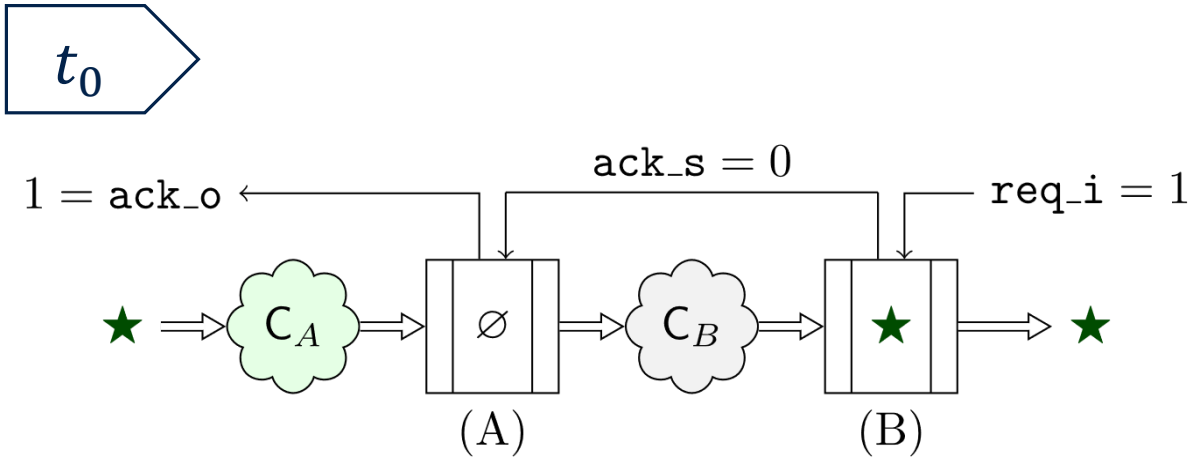
life.augmented

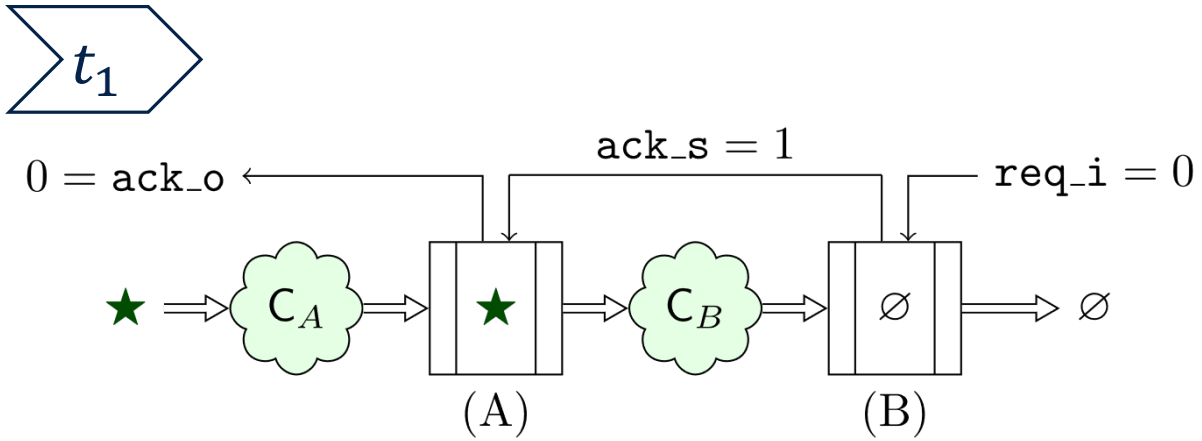
Avoiding Glitches

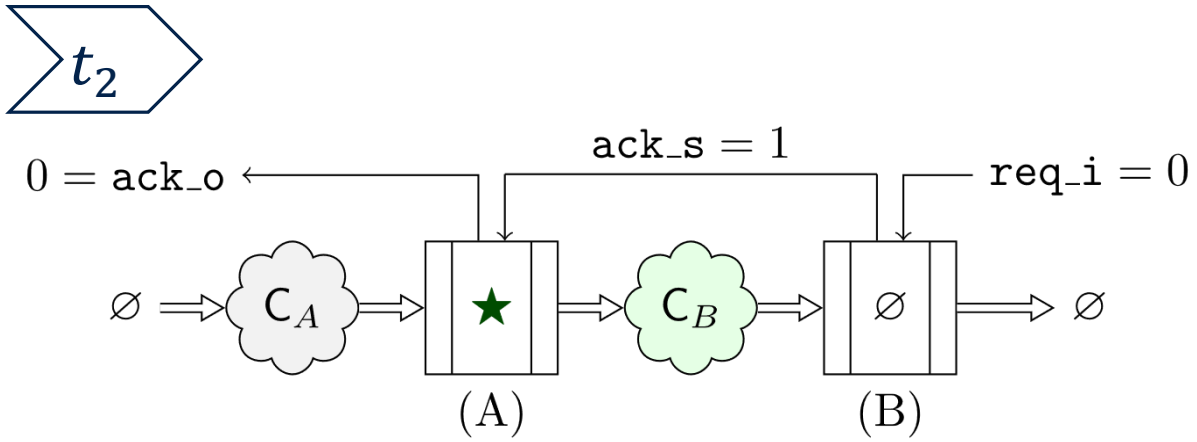
Pre-Charge Evaluate Logic + Monotonic Functions [PBM+20]

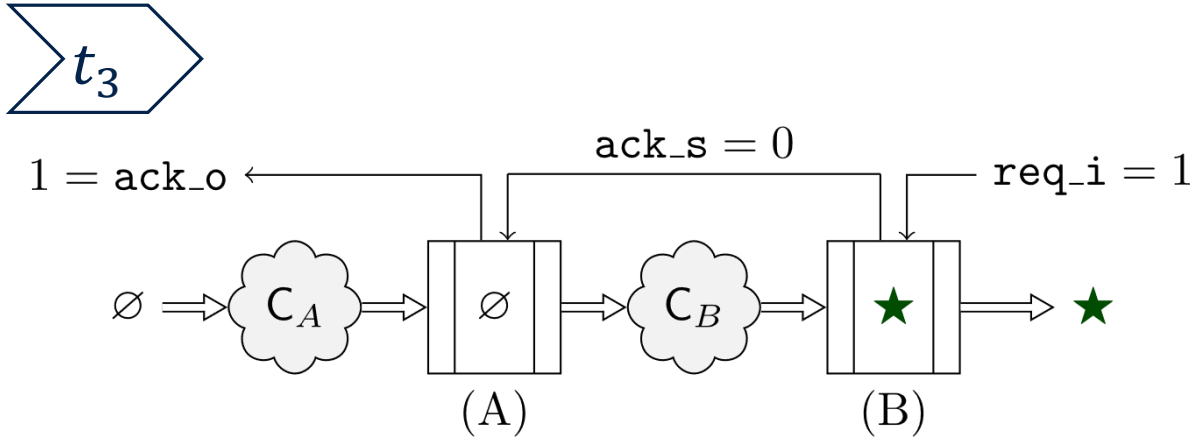
Stage	Input Transition		Dual-Rail Function	
	$a_I \rightarrow a_F$	$b_I \rightarrow b_F$	$z = a\ AND\ b$	$z = a\ XOR\ b$
Pre-charge	$0 \rightarrow \emptyset$	$0 \rightarrow \emptyset$	$0 \rightarrow \emptyset$	$0 \rightarrow \emptyset$
	$0 \rightarrow \emptyset$	$1 \rightarrow \emptyset$	$0 \rightarrow \emptyset$	$1 \rightarrow \emptyset$
	$1 \rightarrow \emptyset$	$0 \rightarrow \emptyset$	$0 \rightarrow \emptyset$	$1 \rightarrow \emptyset$
	$1 \rightarrow \emptyset$	$1 \rightarrow \emptyset$	$1 \rightarrow \emptyset$	$0 \rightarrow \emptyset$
Evaluate	$\emptyset \rightarrow 1$	$\emptyset \rightarrow 1$	$\emptyset \rightarrow 0$	$\emptyset \rightarrow 0$
	$\emptyset \rightarrow 1$	$\emptyset \rightarrow 0$	$\emptyset \rightarrow 0$	$\emptyset \rightarrow 1$
	$\emptyset \rightarrow 0$	$\emptyset \rightarrow 1$	$\emptyset \rightarrow 0$	$\emptyset \rightarrow 1$
	$\emptyset \rightarrow 0$	$\emptyset \rightarrow 0$	$\emptyset \rightarrow 1$	$\emptyset \rightarrow 0$

Self-Timed Masking



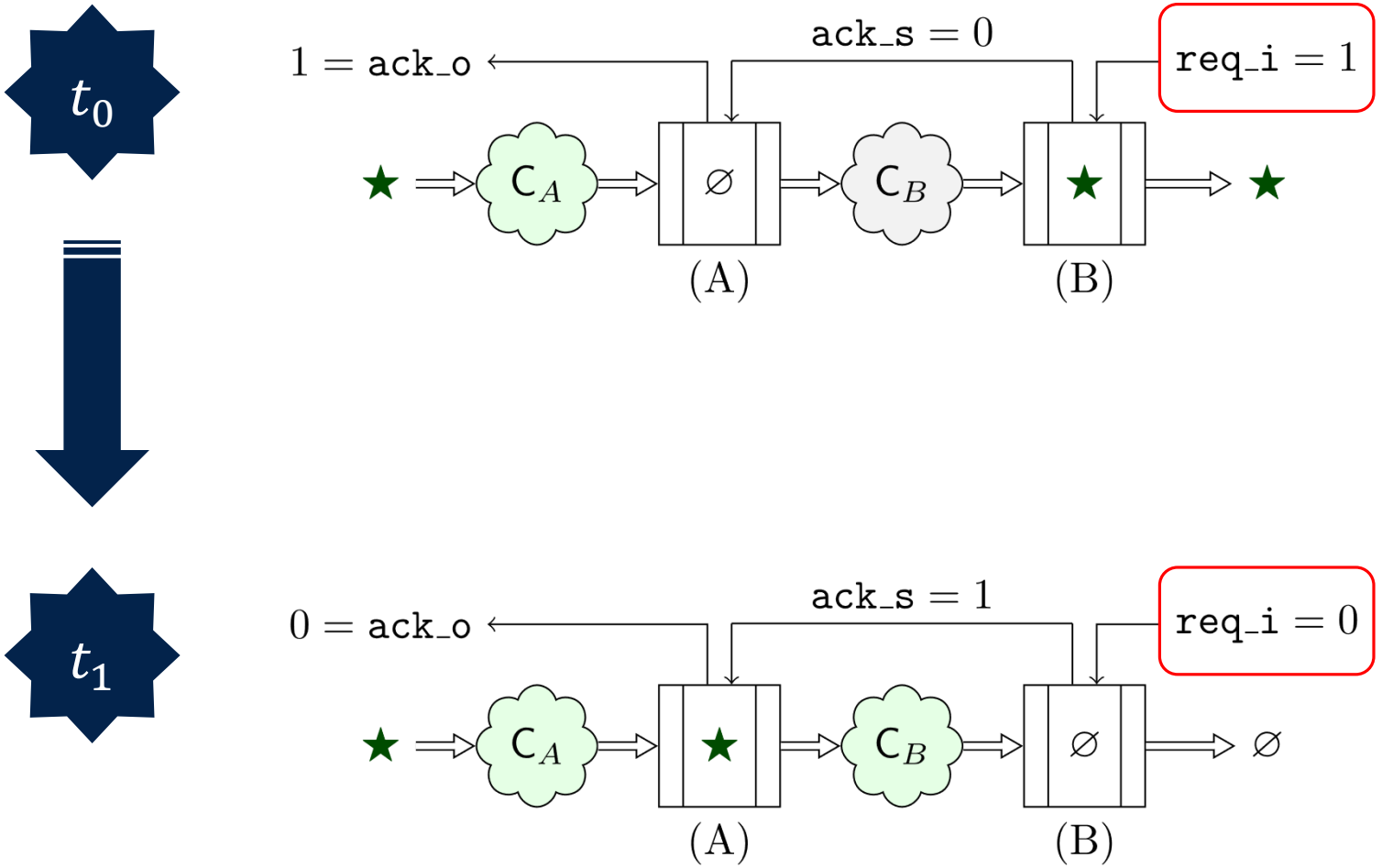






life.augmented

Self-Timed Masking



`req_i` paces the data flow in the pipeline

`ack_o` indicates the first latch state