



# Low-Latency Hardware Masking with Application to AES

Pascal Sasdrich

Begül Bilgin

Michael Hutter

Mark E. Marson

CHES 2020




# RESEARCH QUESTION & PROBLEMS

“Can we implement masked hardware circuits that can be evaluated securely with low (zero) latency overhead?”

What is a suitable hardware masking scheme?

Can we build a secure single-cycle-per-round AES implementation with this approach?

What is the latency overhead of the masking scheme?

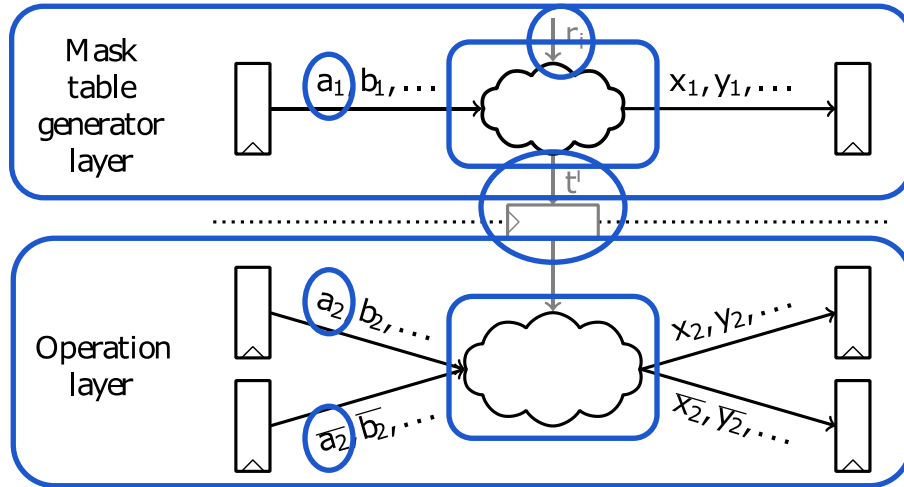


What is a suitable hardware  
masking scheme?

**Rambus**  
Data • Faster • Safer

# LUT-BASED MASKED DUAL-RAIL PRE-CHARGE LOGIC (LMDPL)

*First-order secure gate-level masking technique to build masked gadgets (CHES'14).*



## GADGET CONSTRUCTION:

- Two Boolean shares (first-order secure)
- Complement of second share
- Structure separated into two layers:
  - Mask table generator layer
  - Operation layer
- Gray components only for non-linear gadgets (linear gadgets have independent layers)
- Fully combinational data path in each gadget

## RESTRICTIONS:

- Only monotonic gates in operation layer
- Two phase operation (pre-charge & evaluation)

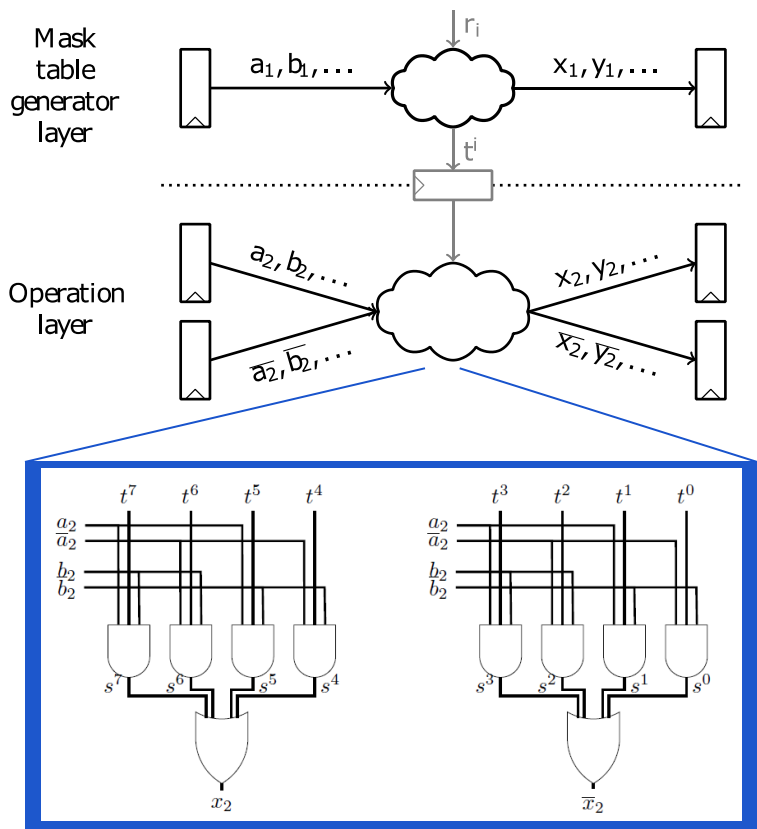
Is the masking scheme  
composable and robust  
against glitches?



# THEORETICAL SECURITY ANALYSIS

- CHES'14: Activity image analysis
- Here: 1-glitch extended probing security (practical first-order security)
  - 1-glitch extended strong non-interference (GSNI) of non-linear gadgets (e.g. AND)
  - 1-glitch extended non-interference of linear gadgets
  - Observe when synchronization is needed and enforced
  - Argue first-order compossibility given the above information
- Reminder: 1-GSNI
  - distinguish intermediate and output probes
  - intermediate probe is independent of at least one input share
  - output probe is independent of all input shares

# THEORETICAL SECURITY ANALYSIS



## Assumption on operation layer:

- Only pre-charged monotonic gates
- Don't touch constraints

## Observations on a shared AND gadget:

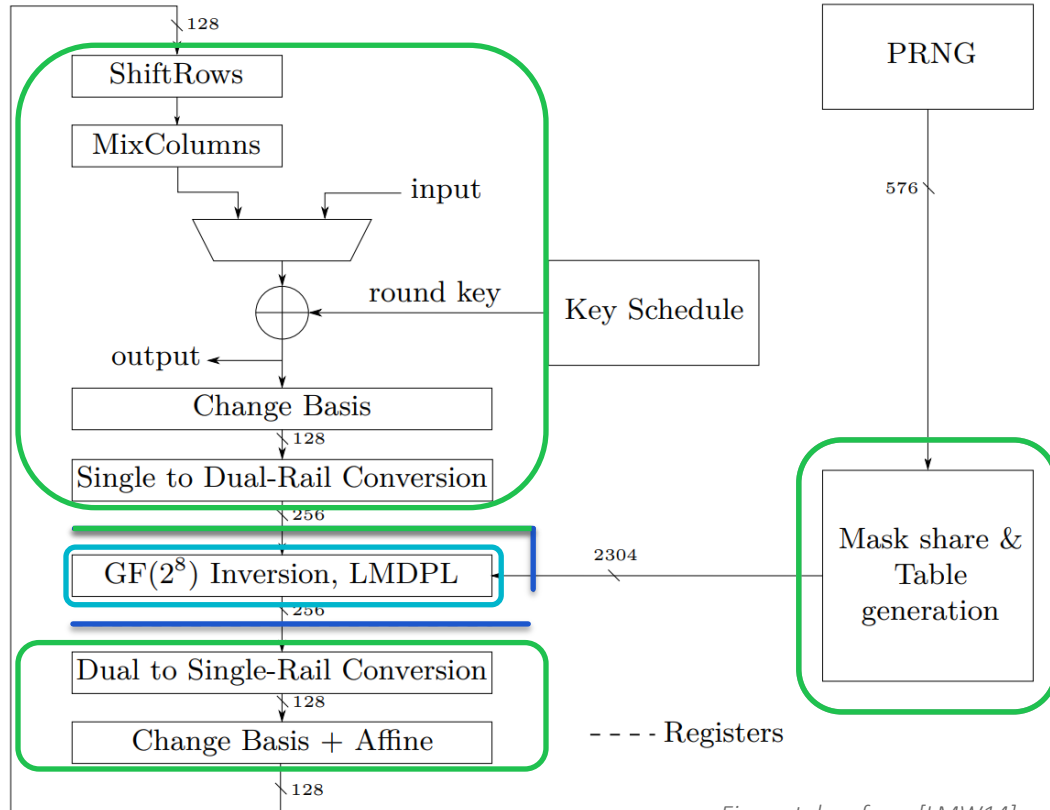
- Operation layer
  - Both  $s^i$  and  $x_2$  toggles only once (no glitch)
    - Probing output doesn't give info on each input
  - Output does not need to be registered
- Mask table generator layer
  - Depends on a single share
  - Output independent of inputs and does not need to be registered
- $t^i$  crosses domain and needs to be registered.

What is the latency  
overhead of the scheme?





# LOW-LATENCY IMPLEMENTATIONS USING LMDPL: ORIGINAL



## ORIGINAL LMDPL CONSTRUCTION:

*Two register stages = two phase operation.*

### CYCLE 0:

- Registers before inversion are pre-charged
- Mask share & table generation active

### CYCLE 1:

- Field inversion (non-linear) is evaluated
- Mask share & table generation inactive and stable

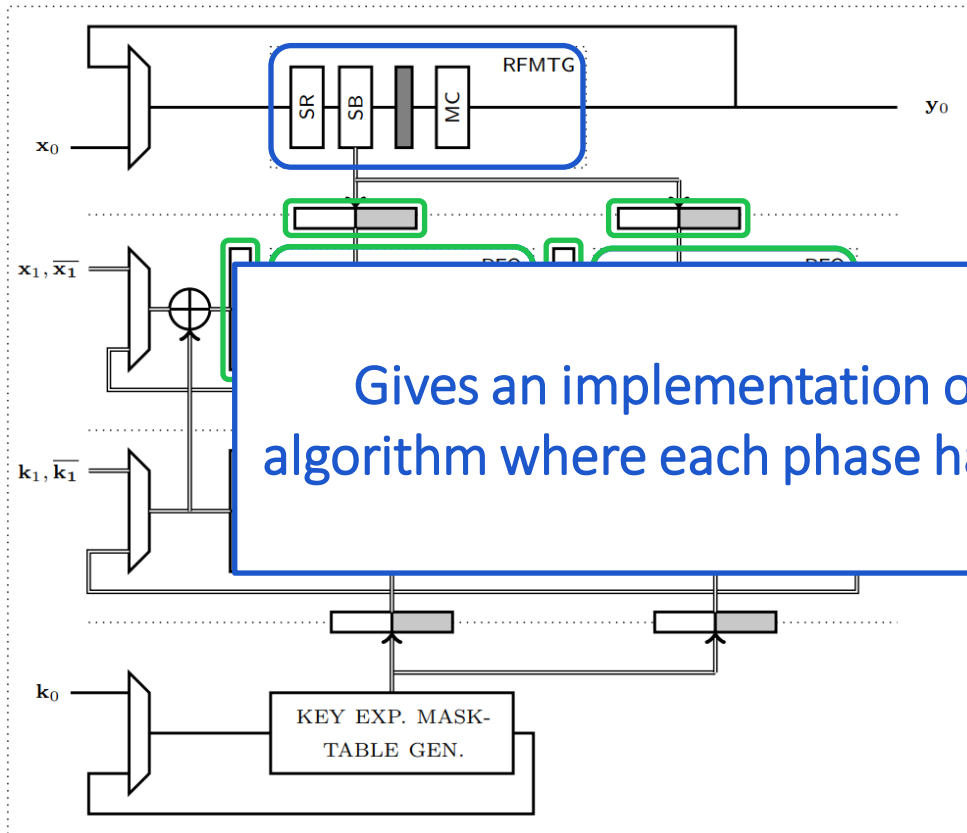
### CYCLE 2:

- AES round operations (linear) are evaluated
- Mask share & table generation active
- Registers before inversion pre-charged

**Two phase operation ensures and maintains glitch-free evaluation.**

Figure taken from [LMW14].

# LOW-LATENCY IMPLEMENTATIONS USING LMDPL: THIS WORK



## LOW-LATENCY LMDPL CONSTRUCTION:

- If: operation layer is pre-charged, and
- If: table generation is synchronized
- Then: gadgets are freely composable
- Duality: alternating evaluation of two operation layers (hides pre-charge phase)

Gives an implementation of  $m/n$  cycles for an  $m$ -round algorithm where each phase has an  $n$ -round evaluation circuit.

### CYCLE 1:

- RFO1: evaluation
- RFO2: pre-charge & mask generation

### CYCLE 2:

- RFO1: pre-charge & mask generation
- RFO2: evaluation

Practical application to AES.



**Rambus**  
Data • Faster • Safer

# IMPLEMENTATION RESULTS

Module	Protected Key Expansion			Standard Key Expansion		
	Enc./Dec.	Enc.	Dec.	Enc./Dec.	Enc.	Dec.
	[kGE]	[kGE]	[kGE]	[kGE]	[kGE]	[kGE]
<b>Cryptographic Engine (AES)</b>	<b>174.4</b>	<b>157.5</b>	<b>167.2</b>	<b>136.3</b>	<b>123.1</b>	<b>129.2</b>
<i>control &amp; connection</i>	0.4	0.5	0.5	0.4	0.4	0.5
<i>data mask-table generation</i>	14.9	12.2	12.9	14.1	11.7	12.2
<i>data operation layer</i>	114.4	103.8	109.1	114.3	103.8	109.0
<i>key mask-table generation</i>	5.3	5.1	5.3	-	-	-
<i>key operation layer</i>	39.4	35.9	39.4	7.5	7.2	7.5
<b>Entropy Engine (PRNG)</b>	<b>14.8</b>	<b>14.8</b>	<b>14.8</b>	<b>11.2</b>	<b>11.2</b>	<b>11.2</b>
<b>Power Consumption [mW]</b>	<b>4.728</b>	<b>4.517</b>	<b>4.661</b>	<b>3.627</b>	<b>3.494</b>	<b>3.608</b>

*Area and power results at 100 MHz after synthesis using GF28nm.*

# COMPARISON TO EXISTING S-BOXES

Works	Area [kGE]	Latency [cycles]	Randomness [bits]
Gross et al. [GIB18]	60.73	1	2,048
Gross et al. [GIB18]	6.74	2	416
Moradi et al. [MPL <sup>+</sup> 11]	4.24	4	48
Wegener and Moradi. [WM18]	4.20	16	0
Bilgin et al. [BGN <sup>+</sup> 14b]	3.71	3	44
Sugawara [Sug19]	3.50	4	0
Ghoshal and De Cnudde [GC17]	2.91	3	20
Bilgin et al. [BGN <sup>+</sup> 15]	2.84	3	32
Leiserson et al. [LMW14]	2.83	2	36
Gross et al. [GM18]	2.20	8	18
De Cnudde et al. [DCRB <sup>+</sup> 16]	1.98	6	54
De Meyer et al. [DRB18]	1.69	2+3	19
Ueno et al. [UHA17]	1.42	5	64
<b>Our Solution</b>	<b>3.48</b>	<b>1</b>	<b>36</b>

## OUR SOLUTION: 3.45 kGE (GF28NM)

- S-box operation: 1,137 GE
- Mask table generation: 611 GE
- 288-bit mask-table register: 1,728 GE
- 1-cycle latency with 36bit rnd./cycle

## RELATED WORK:

- 1-cycle latency: only Gross et al., but:
  - 60 kGE area
  - 2,048 Bit rnd./S-box/cycle
- 2-cycle latency constructions:
  - Leiserson et al.: *original LMDPL design*
  - Gross et al.: *6.74 kGE but still 416bit rnd.*
  - De Meyer et al.: *1.69 kGE and 19bit rnd., but 3 cycle latency in full AES (zero-value problem)*

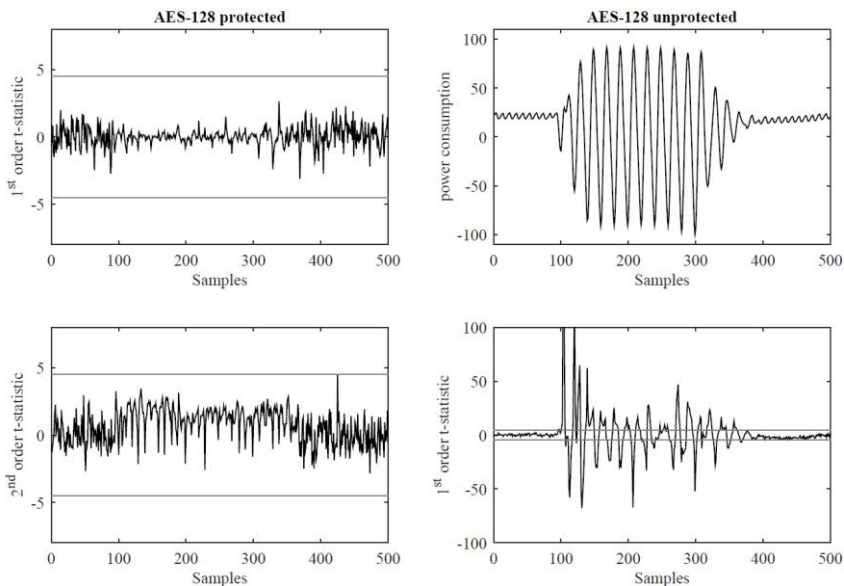


Practical security  
evaluations based on TVLA.



**Rambus**  
Data • Faster • Safer

# PRACTICAL SECURITY ANALYSIS



## GLOBAL SECURITY GOAL:

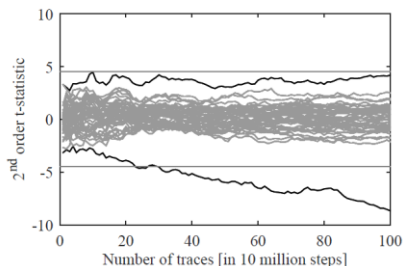
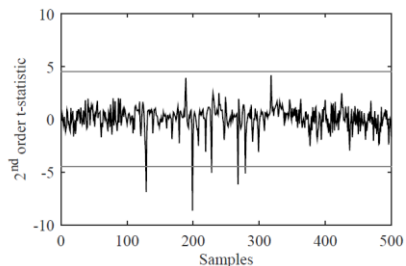
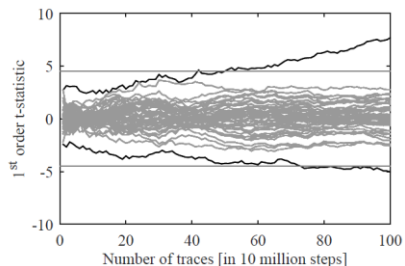
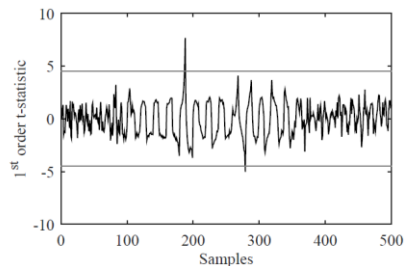
*Resistance with up to 100M power traces.*

- Left side results:
  - First-order statistical moment
  - Second-order statistical moment
- Right side results:
  - Average trace over 1M power traces
  - First-order statistical moment (unprotected)

## CONCLUSION:

*No significant leakage in any of the observed statistical moments.*

# PRACTICAL SECURITY ANALYSIS



## EXTENDED SECURITY GOAL:

*Resistance with up to 1B power traces.*

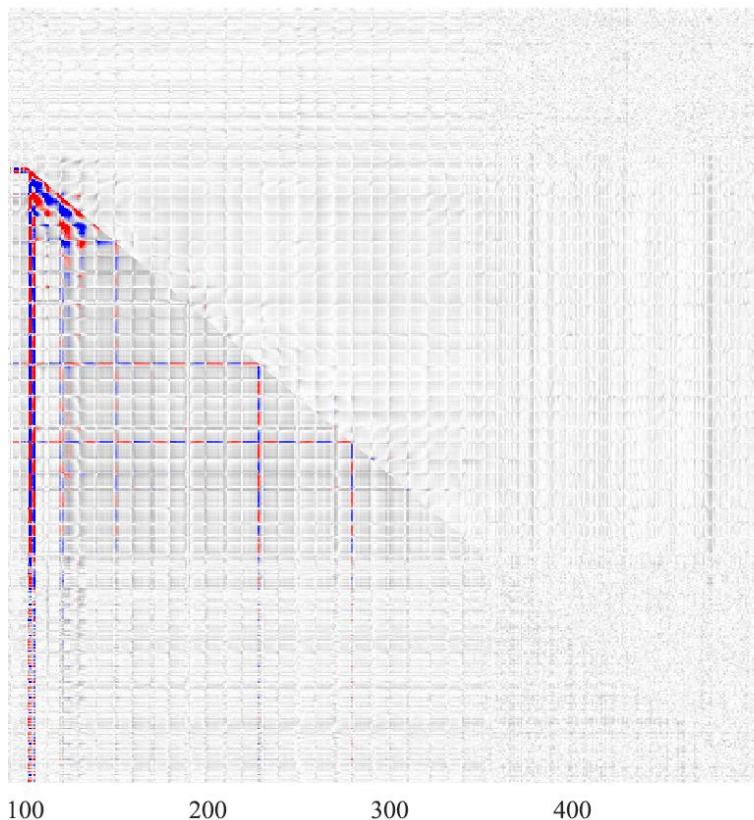
- Left side results:
  - First-order statistical moment
  - Second-order statistical moment
- Right side results:
  - Leakage as function over number of traces (1<sup>st</sup> and 2<sup>nd</sup> order)

## CONCLUSION:

*Leakage detectable after 400M (220M) traces for 1<sup>st</sup>-(2<sup>nd</sup>)-order statistical moment. Key recovery still not successful.*



# PRACTICAL SECURITY ANALYSIS



## MULTIVARIATE SECURITY ANALYSIS:

*Analysis based on bivariate statistics.*

- Full AES: 500 Samples/Trace
- Normalize: *subtract mean samples*
- Combine: *multiply normalized samples*

## RESULTS:

- Gray: t-statistics within thresholds
- Red/blue: significant t-statistics
- Lower triangle: *unprotected results, 100K traces*
- Upper triangle: *protected results, 1B traces*

## CONCLUSION:

*Weak but expected leakage is observed (but only using up to 1B traces).*

# CONCLUSION

We presented a hardware-masked, single-cycle-per-round AES implementation and proved its first-order security under the d-glitch extended probing model.





Thank You  
pascal.sasdrich@rub.de

**Rambus**  
Data • Faster • Safer

# REFERENCES

- [GIB18] Hannes Groß, Rinat Iusupov, and Roderick Bloem. Generic low-latency masking in hardware. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018(2):1–21, 2018.
- [MPL+11] Amir Moradi, Axel Poschmann, San Ling, Christof Paar, and Huaxiong Wang. Pushing the limits: A very compact and a threshold implementation of AES. In *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, pages 69–88, 2011.
- [WM18] Felix Wegener and Amir Moradi. A first-order SCA resistant AES without fresh randomness. In Junfeng Fan and Benedikt Gierlichs, editors, *Constructive Side-Channel Analysis and Secure Design - 9th International Workshop, COSADE 2018, Singapore, April 23-24, 2018, Proceedings*, volume 10815 of *Lecture Notes in Computer Science*, pages 245–262. Springer, 2018.
- [BGN+14b] Begül Bilgin, Benedikt Gierlichs, Svetla Nikova, Ventzislav Nikov, and Vincent Rijmen. A more efficient AES threshold implementation. In David Pointcheval and Damien Vergnaud, editors, *Progress in Cryptology – AFRICACRYPT 2014*, pages 267–284, Cham, 2014. Springer International Publishing.
- [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.
- [GC17] Ashrujit Ghoshal and Thomas De Cnudde. Several masked implementations of the Boyar-Peralta AES s-box. In *Progress in Cryptology – INDOCRYPT 2017 - 18th International Conference on Cryptology in India, Chennai, India, December 10-13, 2017, Proceedings*, pages 384–402, 2017.
- [BGN+15] Begül Bilgin, Benedikt Gierlichs, Svetla Nikova, Nikov Ventzislav, and Vincent Rijmen. Trade-offs for threshold implementations illustrated on AES. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 34(7):1188–1200, July 2015.
- [LMW14] Andrew J. Leiserson, Mark E. Marson, and Megan A. Wachs. Gate-level masking under a path-based leakage metric. In Lejla Batina and Matthew Robshaw, editors, *Cryptographic Hardware and Embedded Systems – CHES 2014 - 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings*, volume 8731 of *Lecture Notes in Computer Science*, pages 580–597. Springer, 2014.
- [GM18] Hannes Groß and Stefan Mangard. A unified masking approach. *J. Cryptographic Engineering*, 8(2):109–124, 2018.
- [DCRB+16] Thomas De Cnudde, Oscar Reparaz, Begül Bilgin, Svetla Nikova, Ventzislav Nikov, and Vincent Rijmen. Masking AES with  $d+1$  shares in hardware. In *Proceedings of the 2016 ACM Workshop on Theory of Implementation Security, TIS'16*, pages 43–43, New York, NY, USA, 2016. ACM.
- [DRB18] Lauren De Meyer, Oscar Reparaz, and Begül Bilgin. Multiplicative masking for AES in hardware. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018(3):431–468, 2018.
- [UHA17] Rei Ueno, Naofumi Homma, and Takafumi Aoki. Toward more efficient DPA-resistant AES hardware architecture based on threshold implementation. In Sylvain Guilley, editor, *Constructive Side-Channel Analysis and Secure Design*, pages 50–64, Cham, 2017. Springer International Publishing.