Blind Side Channel Attack against AEAD with a Belief Propagation Approach

Modou Sarry, Eïd Maalouf, Hélène Le Bouder and Gaël Thomas

IMT ATLANTIQUE - OCIF - IRISA - DGA-MI

CARDIS 2023

November 15, 2023

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Section

1. Context and motivation
2. Belief propagation (BP)
3. BSCA with BP on ELEPHANT
4. BSCA with BP on SPARKLE
5. Conclusion

Plan

1. Context and motivation
2. Belief propagation (BP)
3. BSCA with BP on ELEPHANT
4. BSCA with BP on SPARKLE
5. Conclusion

Context

Contrained devices

- e.g., RFID tags, sensors,IoT devices

New applications

- e.g.,Healthcare, home automation, smart city

Private Information

- e.g., Location, health data

Lacks of Cryptography standard

- Nist crypto standards are optimised for general purpose computer

Context

Contrained devices

- e.g., RFID tags, sensors,IoT devices

New applications

- e.g.,Healthcare, home automation, smart city

The solution is to create a new algorithms that fit into these devises.

Private Information

- e.g., Location, health data

Lacks of Cryptography standard

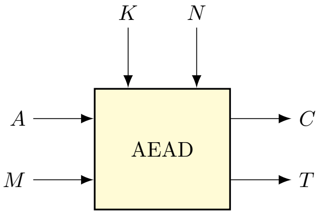
- Nist crypto standards are optimised for general purpose computer

AEAD

In August 2018, NIST launched the competition for lightweight cryptography. All candidates are **AEAD**.

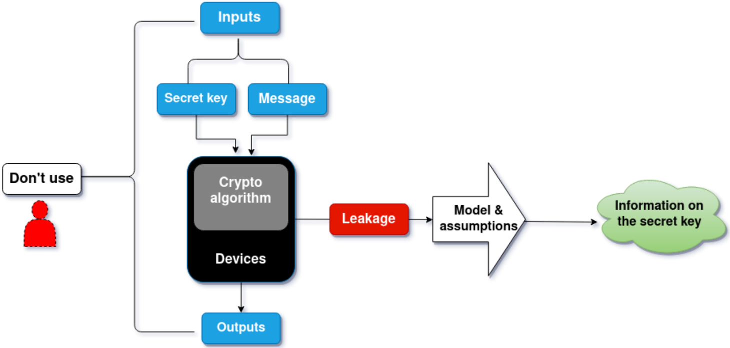
AEAD: Authenticated encrytion with associated data

- Inputs: M (message), A (associated data), K (secret key), N (Nonce)
- Outputs: C (ciphertext), T (tag)



- Two finalists in the competition are targeted: **ELEPHANT** and **SPARKLE**.

Blind side channel attacks



Leakage model

HW(B)	0	1	2	3	4	5	6	7	8
$\#B$	1	8	28	56	70	56	28	8	1

Table 1: Number of possible values for a byte B according to its Hamming weight(HW).

- Our model is a noise HW:

$$\tilde{\mathrm{HW}}(B) = \mathrm{HW}(B) + \sigma_{B,t} \quad ;$$

with $\sigma_{B,t}$ an event of the Gaussian random variable $\mathcal{N}\left(0, \sigma^2\right)$ at a time t.

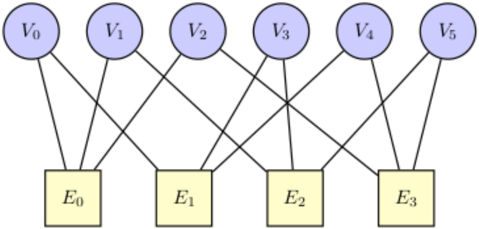
Plan

1. Context and motivation
2. Belief propagation (BP)
3. BSCA with BP on ELEPHANT
4. BSCA with BP on SPARKLE
5. Conclusion

Tanner graph

The nodes of a tanner graph are of two kinds

- variable nodes V representing the variables handled by the algorithm under attack;
- factor nodes, representing the equations E between these variables.



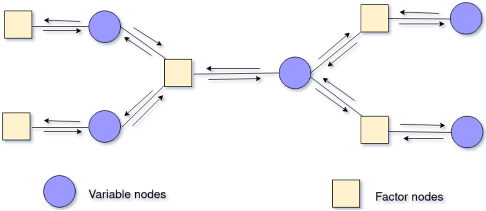
Belief propagation

The BP algorithm

- Input: the Tanner graph and prior probabilities $\mathbb{P}_A(V = v)$ on the different variable nodes V.
- Output: posterior probability $\mathbb{P}_P(V = v)$

BP: Exchange of information between variable and factor nodes

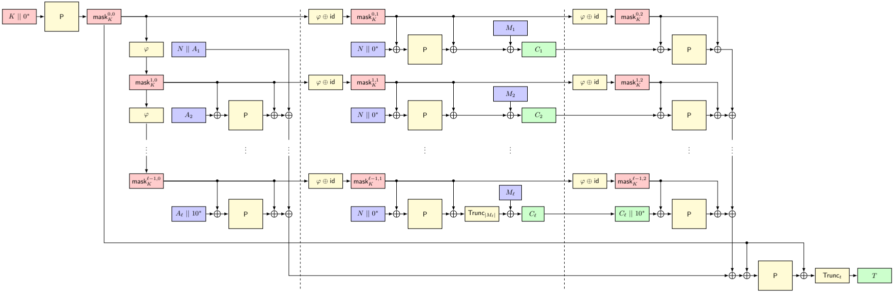
- $\mu_{E \to V}$: law of total probability
- $\mu_{V \to E}$: Bayes' rule



Plan

1. Context and motivation
2. Belief propagation (BP)
3. BSCA with BP on ELEPHANT
4. BSCA with BP on SPARKLE
5. Conclusion

ELEPHANT


K || 0*
P
mask$_K^{0,0}$
φ
N || A$_1$
mask$_K^{1,0}$
A$_2$
mask$_K^{\ell-1,0}$
A$_\ell$ || 10*
φ ⊕ id
mask$_K^{0,1}$
mask$_K^{1,1}$
mask$_K^{\ell-1,1}$
N || 0*
M$_1$
M$_2$
M$_\ell$
C$_1$
C$_2$
C$_\ell$
Trunc$_{|M_\ell|}$
mask$_K^{0,2}$
mask$_K^{1,2}$
mask$_K^{\ell-1,2}$
C$_\ell$ || 10*
Trunc$_t$
T

BSCA on ELEPHANT

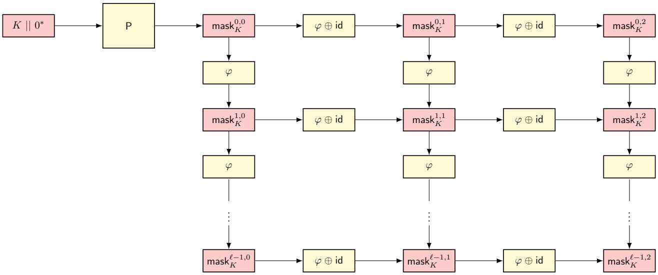
Retrieving the initial state of the LFSR ($= mask_K^{0,0}$).

To retrieving the secret key.

Attacks vectors and attacker model

Attack vectors

- Vertical evolution of the mask (LFSR iterations).
- Horizontal evolution of the mask (domain separation).

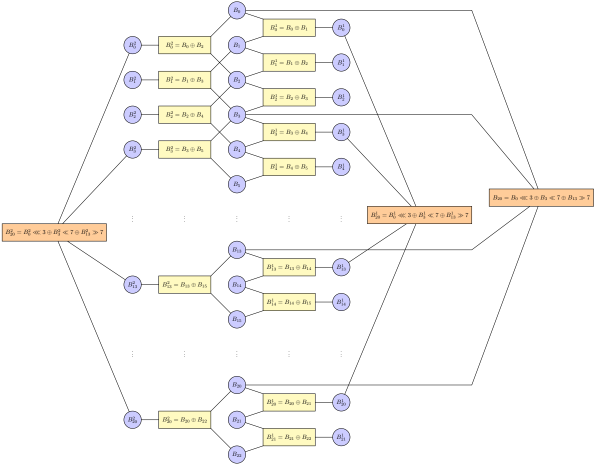


Attack model

- Noisy Hamming weights of all bytes of the LFSR.

Tanner graph Elephant attack

- Variable nodes:
  - bytes LFRSs B_i.
- Factor nodes:
  - retroaction equations ;
  - equations linking the masks.



Result

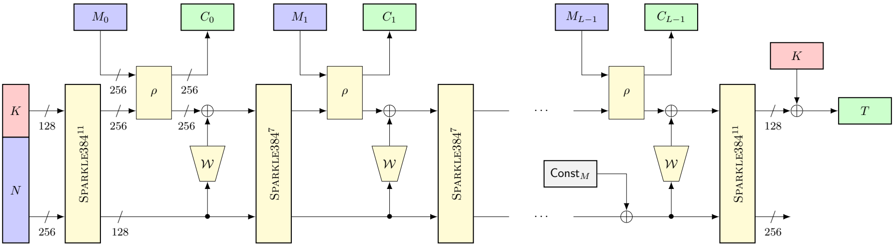
Rank for all 20 key bytes on 1000 randomly generated keys and for different noise levels σ.

σ	Mean	Standard Deviation	Quartile Q1	Median	Quartile Q3	Max
0.1	3.54	5.97	0	3	3	27
0.15	3.54	5.97	0	3	3	27
0.2	3.67	6.11	0	3	3	31
0.25	4.95	9.31	0	3	3	97
0.3	6.00	10.76	0	3	3	97
0.35	7.46	13.10	0	3	8	97
0.4	9.59	15.72	0	3	8	97
0.5	15.97	23.03	3	8	31	153
0.6	23.65	31.41	3	8	31	157
0.7	33.73	40.11	3	27	36	213
1	70.68	61.42	31	36	92	246

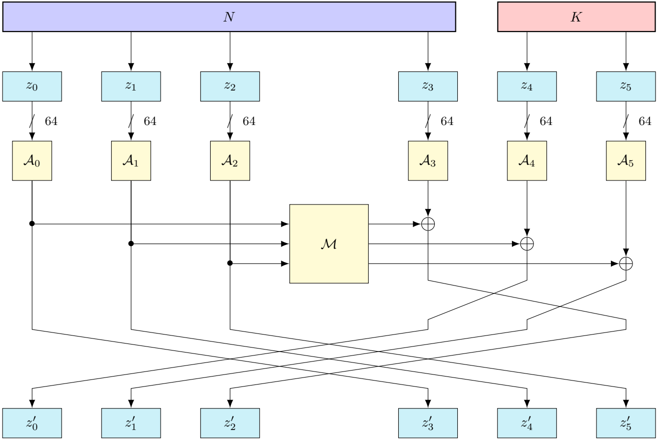
Plan

1. Context and motivation
2. Belief propagation (BP)
3. BSCA with BP on ELEPHANT
4. BSCA with BP on SPARKLE
5. Conclusion

Schwaemm256-128



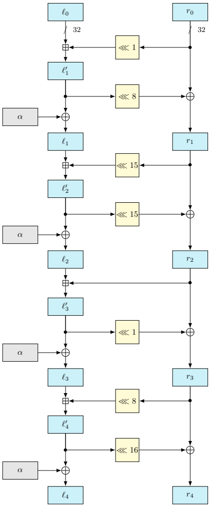
Zoom on Sparkle384_{11}



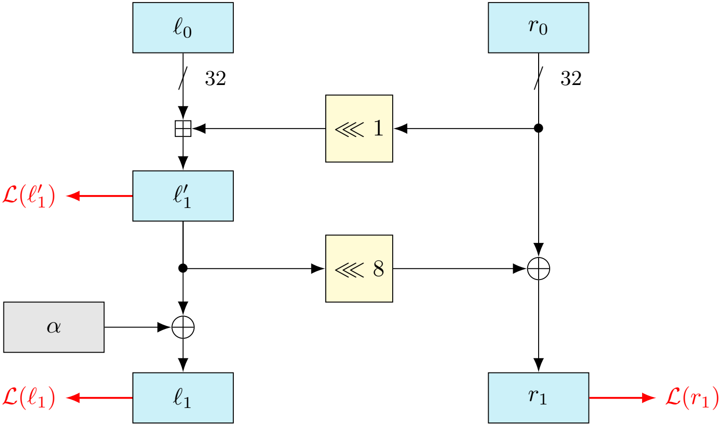
$\mathcal{K}_1 = z_4, \mathcal{K}_2 = z_5$ and $K = \mathcal{K}_1 || \mathcal{K}_2$

Zoom on Alzette

The Alzette S-box $\mathcal{A}_i$ used in Sparkle.



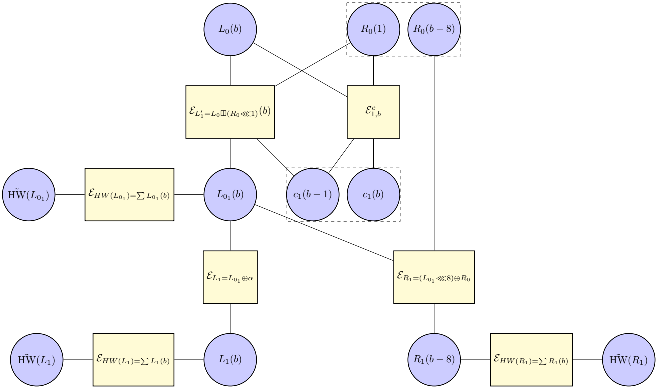
Path of attack



$$\mathcal{L}(x) = HW(x) + \sigma_x \text{ with } \sigma_x \in \mathcal{N}(0, \sigma^2)$$

Measurement leakage in the first round of Alzette

Tanner Graph of Sparkle



Tanner graph on first round Alzette

Results: First Alzette

The number of recovered bits of the 64-bit $\mathcal{K}_1$ input of the Alzette $\mathcal{A}_4$, with 1000 different keys.

σ	Mean	Standard Deviantion	Min	Quartile Q1	Median	Quartile Q3	Max
0.1	57.08	3.02	36	56	57	59	63
0.15	57.16	2.66	38	56	57	59	63
0.2	57.20	2.57	40	56	57	59	64
0.25	57.15	2.76	38	56	57	59	64
0.3	57.07	2.74	40	56	57	59	64
0.35	56.77	2.94	36	55	57	58	64
0.4	56.63	2.81	39	55	57	58	64
0.45	56.12	3.01	35	55	56	58	64
0.5	55.81	2.81	39	54	56	57	64
0.6	54.83	2.94	36	53	55	56	64
0.7	54.19	2.68	36	53	54	56	62
1	52.86	3.47	35	52	54	55	59

Results: Second Alzette

The number of recovered bits of the 64-bit $\mathcal{K}_2$ input of the Alzette $\mathcal{A}_5$, with 1000 different keys.

σ	Mean	Standard Deviantion	Min	Quartile Q1	Median	Quartile Q3	Max
0.1	56.98	2.78	36	56	57	59	63
0.15	57.05	2.40	39	56	57	59	63
0.2	57.05	2.43	39	56	57	59	63
0.25	56.96	2.55	39	55	57	59	63
0.3	56.82	2.53	40	55	57	58	63
0.35	56.59	2.64	39	55	57	58	64
0.4	56.29	2.67	40	55	56	58	64
0.45	55.92	2.75	37	54	56	58	64
0.5	55.53	2.66	38	54	55	57	64
0.6	54.64	2.70	36	53	55	56	63
0.7	53.86	2.79	36	53	54	55	61
1	52.78	3.29	33	52	54	54	59

Plan

1. Context and motivation
2. Belief propagation (BP)
3. BSCA with BP on ELEPHANT
4. BSCA with BP on SPARKLE
5. Conclusion

Conclusion

First BSCA on Elephant with noisy hamming weight model.

First BSCA on Sparkle with noisy hamming weight model.

The power of the BP was also highlighted in our research.

Future works

Future works

- Practical implementations of this attacks.
- We targeted ASCON to explore its security.

Thank you for attention, Questions?