CryptArchi 2023

Is ASCON the best choice regarding the Side-channel Analysis?

Ing. Matúš Olekšák
FIT CTU, Prague, Czech Republic

Agenda

- Motivation
- NIST Lightweight cryptography standard
- ASCON overview
- Other Finalists
- Conclusion

Motivation

- Internet of Things (IoT) is getting popular.
- There was no encryption standard for lightweight cryptography.
- National Institute of Standards and Technology (NIST) started challenge for the new standard of lightweight encryption to meet the requirements of IoT.
- One of the requirements for the upcoming standard was resistance against side-channel attacks.

NIST Lightweight cryptography standard

- The winner was chosen from 10 finalists.
- In February 2023 NIST announced the winner of the challenge.
- **ASCON** was announced as the winner of challenge.

Overview of side-channel attacks on ASCON

Side-channel attacks on ASCON

[Gross, Wenger, Dobraunig, Ehrenhöfer, 2017]

- Attack on S-Box output of ASCON-x-low-area design.
- Successful attack on unprotected implementation with 500 power traces on average.
- With ASCON-fast design, authors had to attack on whole round transformation.
- Combined 128 distinct power analysis attacks using SAT solver and found secret key with 1,000 power traces on average.
- Attack on protected implementation was not successful even with over 1 million power traces captured.

Side-channel attacks on ASCON

[Ramezanpour, Ampadu, Diehl, 2020]

- ASCON was implemented on Artix-7 FPGA.

- Differential power analysis (DPA)
  - unsuccessful with 40,000 power traces

- Correlation Power Analysis (CPA)
  - unsuccessful with 40,000 power traces

- Side-Channel Analysis with Reinforcement Learning (SCARL)
  - successful with 24,000 power traces

Overview of side-channel attacks on other finalists

Side-channel attacks on Elephant

[Vialar, 2022]

- Based on CPA.
- Reference C implementation was used without any protection on ARM Cortex-M4 microcontroller.
- Only around 30 power traces were needed for full key discovery.
- The attack is meant only for Dumbo and Jumbo variants.
    - Delirium variant uses different permutation.

Side-channel attacks on GIFT-COFB

[Hou, Breier, Bhasin, 2021]

- Successful attack on GIFT-COFB.
- Differential No-Fault Analysis of Bit Permutation-Based Ciphers Assisted by Side Channel.
- It combines Differential Fault Analysis with Side-Channel Assisted Differential Plaintext Attacks.
- The attacker needs $2^{18.39}$ (~343,512) encryptions.

Side-channel attacks on Grain-128AEAD

[Chakraborty, Mazumdar, Mukhopadhay, 2015]

- Successful attack realized on protected variants of Grain family algorithms.

- Combination of DPA and clock glitching.

- Trade-off between
  - number of resynchronizations of the cipher
  - exhaustive search for the remaining undetermined key bits.

Side-channel attacks on ISAP

[Ji, 2022]

- Side-channel evaluation of ISAP.

- Implementations used
  - software implementation by ISAP team
  - hardware implementation by IAIK
  - hardware implementation by Ruhr-University Bochum

- CPA attack was not able to recover private key under given implementations.

Side-channel attacks on PHOTON-Beetle

[Amit, Goutam, 2022]

- Fault attack with two different models
  - random fault
  - known fault

- Random fault model needs $2^{37.15}$ (~152 billion) of faulty queries.

- Known fault model needs only $2^{11.05}$ (~2,120), but the attacker needs to know faulty value.

- Both models resulted in successful attacks.

Side-channel attacks on Romulus

[Vialar, 2022]

- CPA attack on Romulus-N variant.
- Author attacked on SubCells of the second round to discover the 8 most significant bytes of the key.
- To get the rest of the key, it was needed to attack on SubCells at the third round.
- The attack is successful between 69% and 85% with number of traces between 1,800 and 2,400.

Side-channel attacks on SPARKLE

[Chen, et al., 2022]

- CPA and Deep Learning Power Analysis (DLPA) on SCHWAEMM256-128 variant.
- Authors measured 2,000 traces for each of 320 different private keys.
- They were unable to recover keys through CPA nor DLPA.

Side-channel attacks on TinyJambu

[Bhasin, et al., 2022]

- Differential Analysis aided Power Attack.
- In case of 32-bit architecture, authors were capable of discovery of 32 bits of private key.
- It is because of possibility to affect only 32 bits of Nonlinear Feedback Shift Register (NFSR).
- With 1-bit implementation authors retrieved full secret key.

Side-channel attacks on Xoodyak

[Batina, et al, 2022]

- CPA inspired by DPA attack called Keyak, which was based on Keccak-p.
- Measurement was made on Piñata development board with STM32F4.
- The publication is quite brief on Xoodyak CPA attack description.
- Conclusion is also missing in this publication.
  - It did not result in a successful attack.

Available side-channel related publications

Algorithm	Publications	Attacks	Successful Attacks
ASCON	4	3	3
Elephant	3	2	1
GIFT-COFB	3	3	3
Grain-128AEAD	3	3	3
ISAP	3	1	0
PHOTON-Beetle	2	2	2
Romulus	2	1	1
Sparkle	2	1	0
TinyJAMBU	2	1	1
Xoodyak	3	1	0

Table summarizing number of side-channel related publications.

Conclusion

⚠ Side-channel attacks against ASCON has already been proposed and proved to be effective.

There are other finalists, which were not successfully attacked using side-channel attacks yet.

! This may represent a weak spot of this standard in the future.

Thank you!

Do you have any questions?