A Key Management Scheme for DPA-Protected Authenticated Encryption

Mostafa Taha and Patrick Schaumont

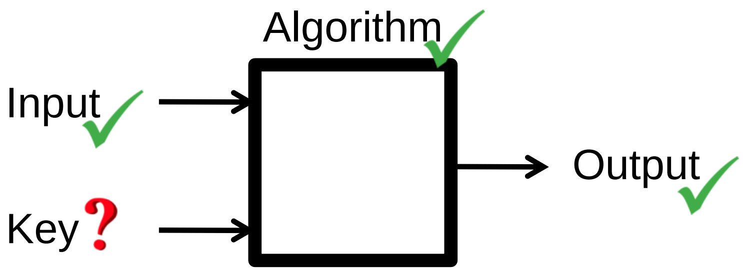
Virginia Tech

DIAC-2013

This research was supported in part by the VT-MENA program of Egypt, and by NSF grant no. 1115839.

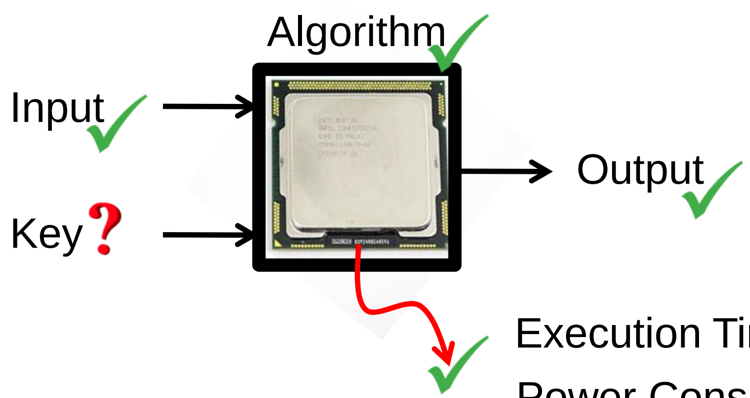
Leakage-Resilient Cryptography

Classical Cryptography



Leakage-Resilient Cryptography

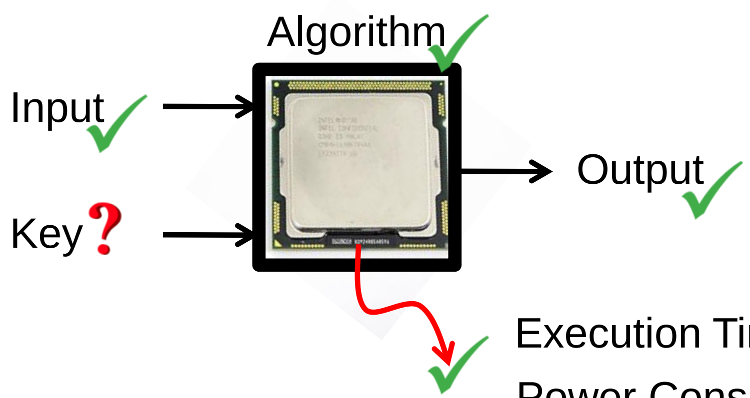
Side-Channel Analysis



Execution Time
Power Consumption
Electromagnetic Radiation
Acoustic Waves
Photonic Emission
Fault Detection

Leakage-Resilient Cryptography

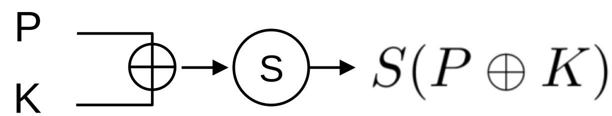
Side-Channel Analysis



Execution Time
Power Consumption
Electromagnetic Radiation
Acoustic Waves
Photonic Emission
Fault Detection

Is this a problem?

Differential Power Analysis

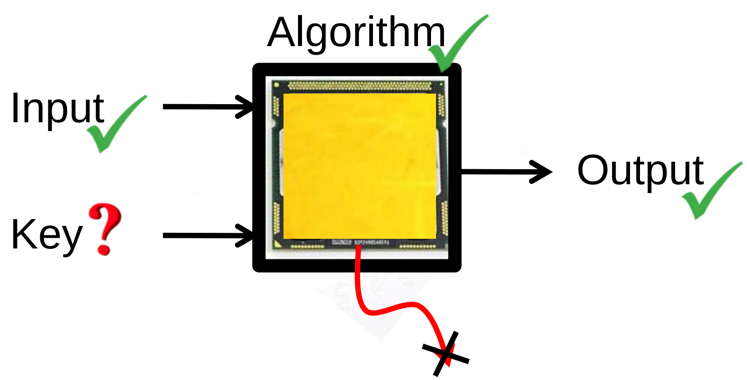


- The key in DPA is to find a sensitive intermediate variable that depends on:
  - a controllable/observable input.
  - and a fixed unknown.

  Where the unknown is affected by a small part of the key.

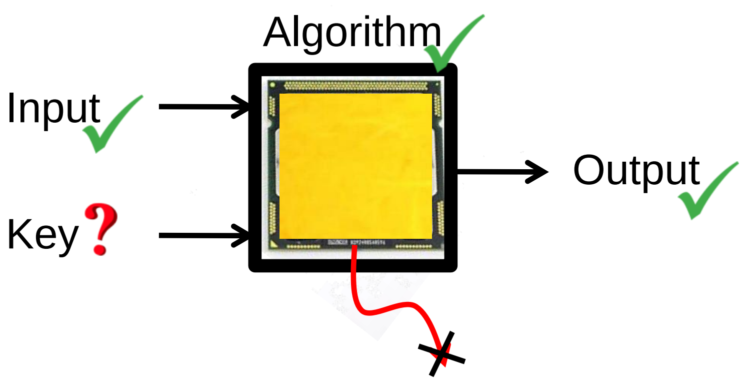
Leakage-Resilient Cryptography

1- Hardware Protection



Leakage-Resilient Cryptography

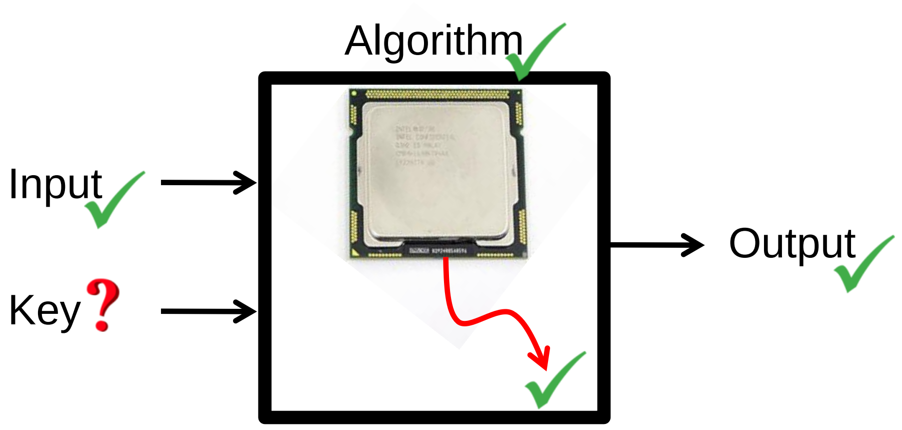
1- Hardware Protection



- Typically at High Cost (typically 2x).

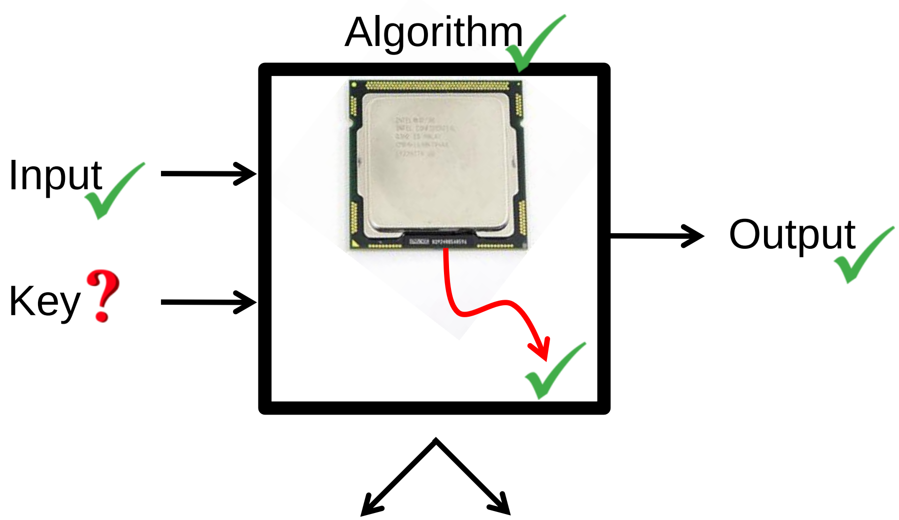
Leakage-Resilient Cryptography

2- Leakage-Resilient Cryptography



Leakage-Resilient Cryptography

2- Leakage-Resilient Cryptography



New Primitive

Special Mode of operation (compatible with current modes)

Leakage-Resilient Cryptographic Primitive

- Stream Ciphers: [DP08, P09, YSPY10]
- Block Ciphers: [FPS12]
- Digital Signatures: [BSW11]
- Public-Key Encryption: [NS12]

and many more

Leakage-Resilient Cryptographic Primitive

- Stream Ciphers: [DP08, P09, YSPY10]
- Block Ciphers: [FPS12]
- Digital Signatures: [BSW11]
- Public-Key Encryption: [NS12]

and many more

However:

- The assumptions used are controversial.
- High-overhead initialization procedure.
- Not a current solution (still needs standardization).

Leakage-Resilient Mode of Operation

- Are current modes DPA-protected?

Leakage-Resilient Mode of Operation

- Are current modes DPA-protected?
- No
  - Different design requirement.
  - The IV/nonce is not secret, hence the same attack methodology can be used.

Leakage-Resilient Mode of Operation

- Are current modes DPA-protected?
- No
  - Different design requirement.
  - The IV/nonce is not secret, hence the same attack methodology can be used.

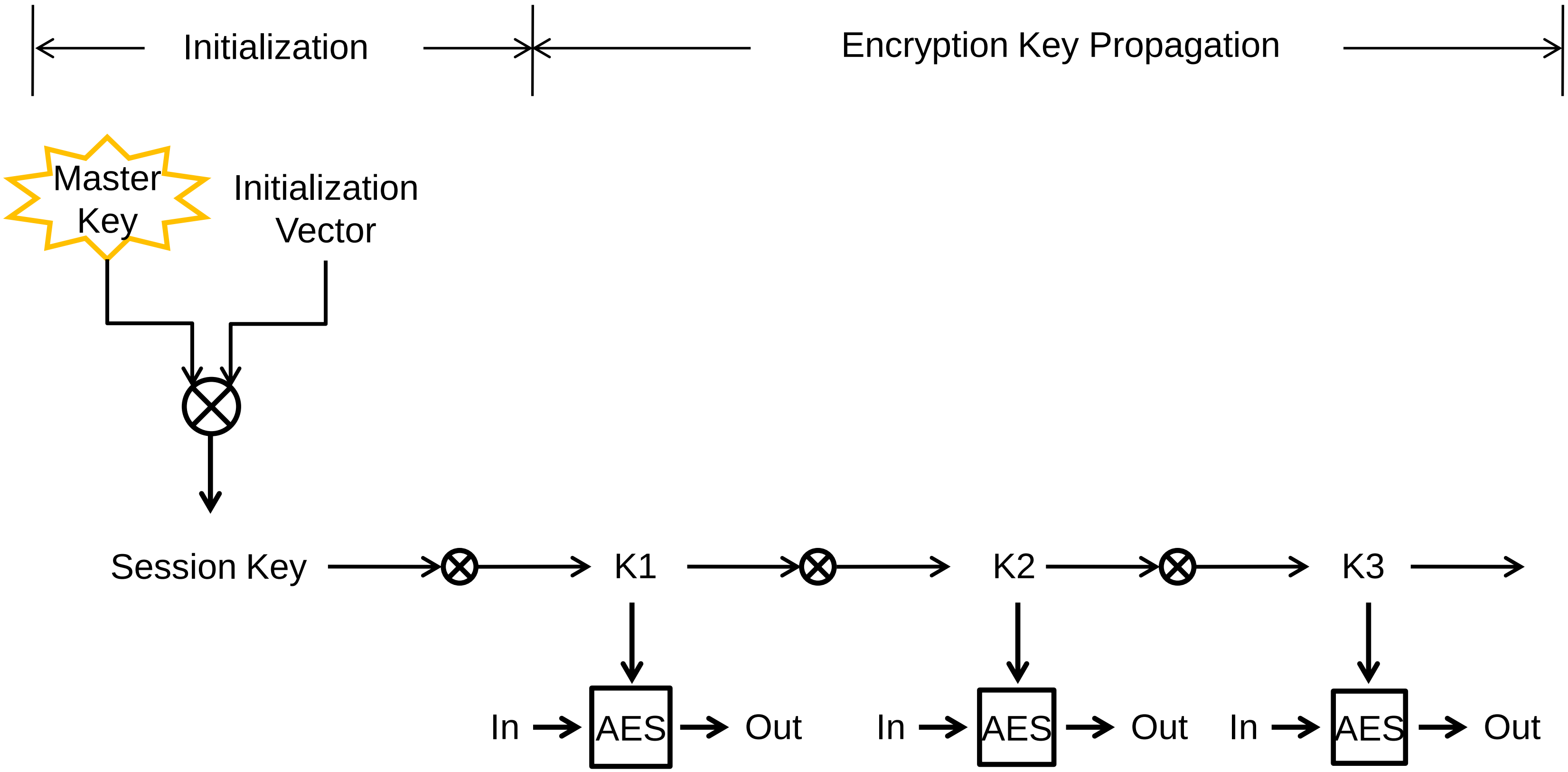
- Research Goals:
  - Current: Design a compatible DPA-protection add-on.
  - Future: Include the DPA-protection in a new AE mode.

Outline

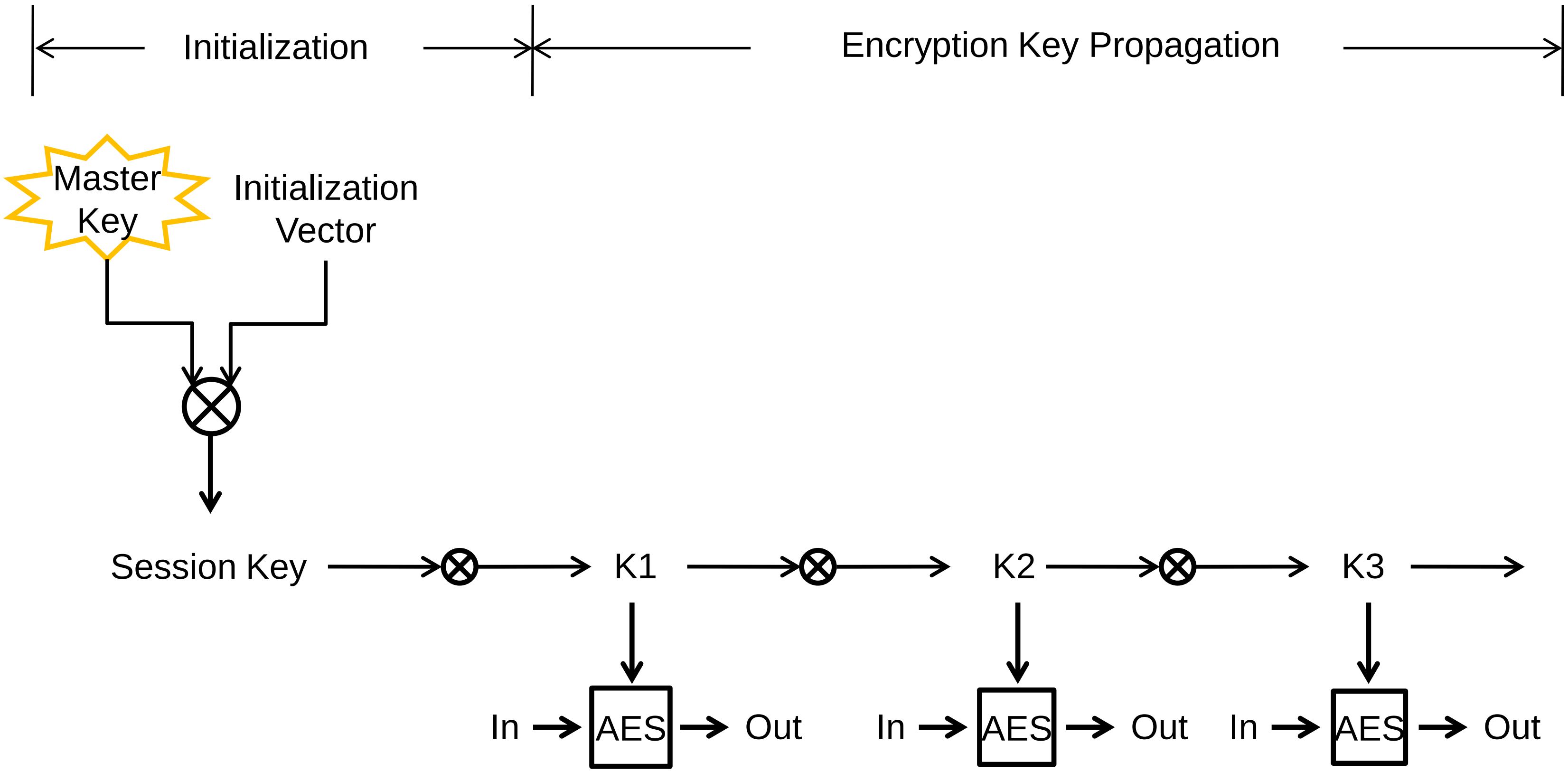
Introduction

- Design Model
- Security Requirements of the New Scheme
- Previous Work
- NLFSR-Based Scheme
- Concluding Remarks

Design Model

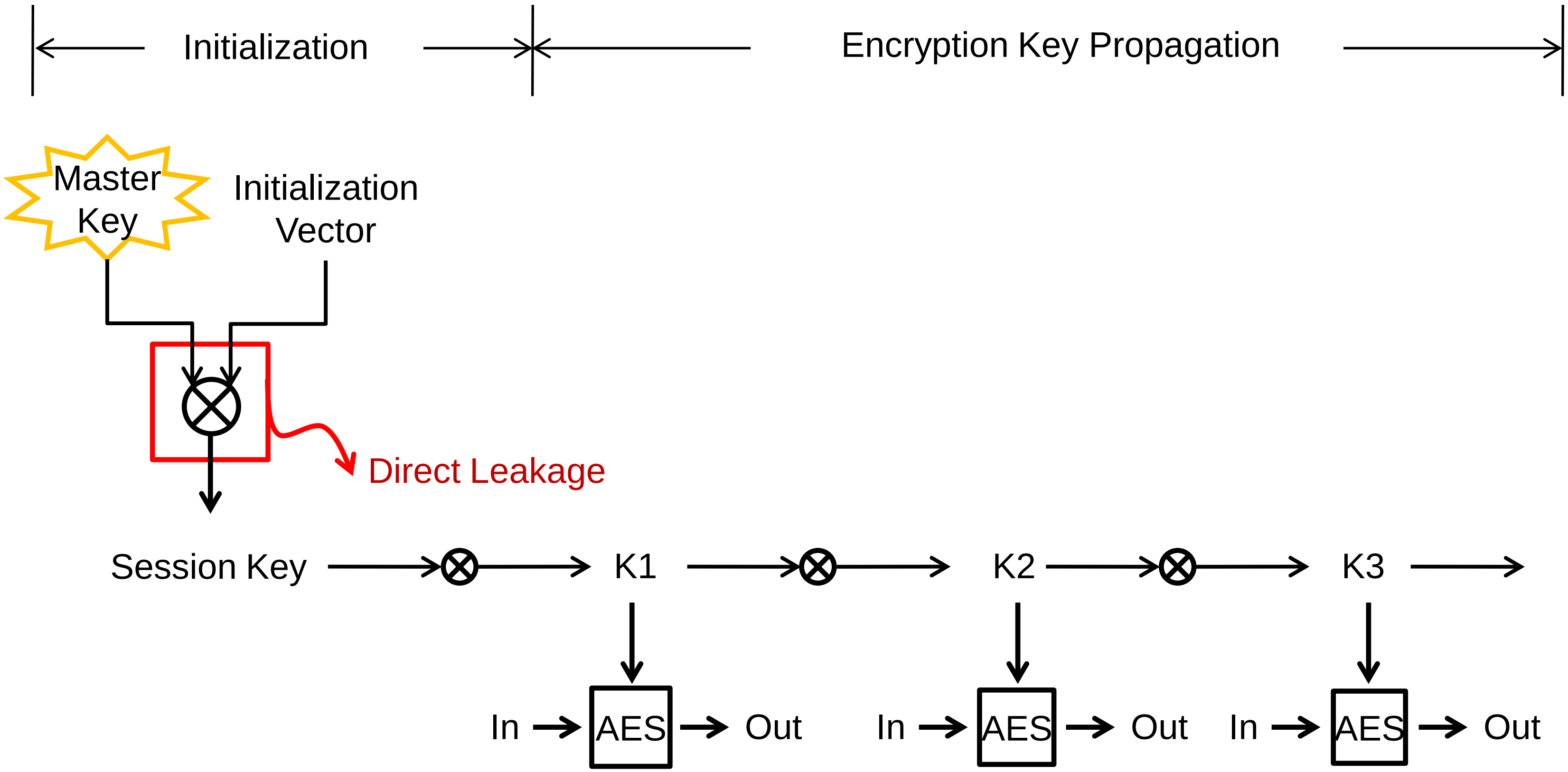


Design Model



Goal: protection against any “differential” attack.
This is NOT shifting the problem, but separating it.

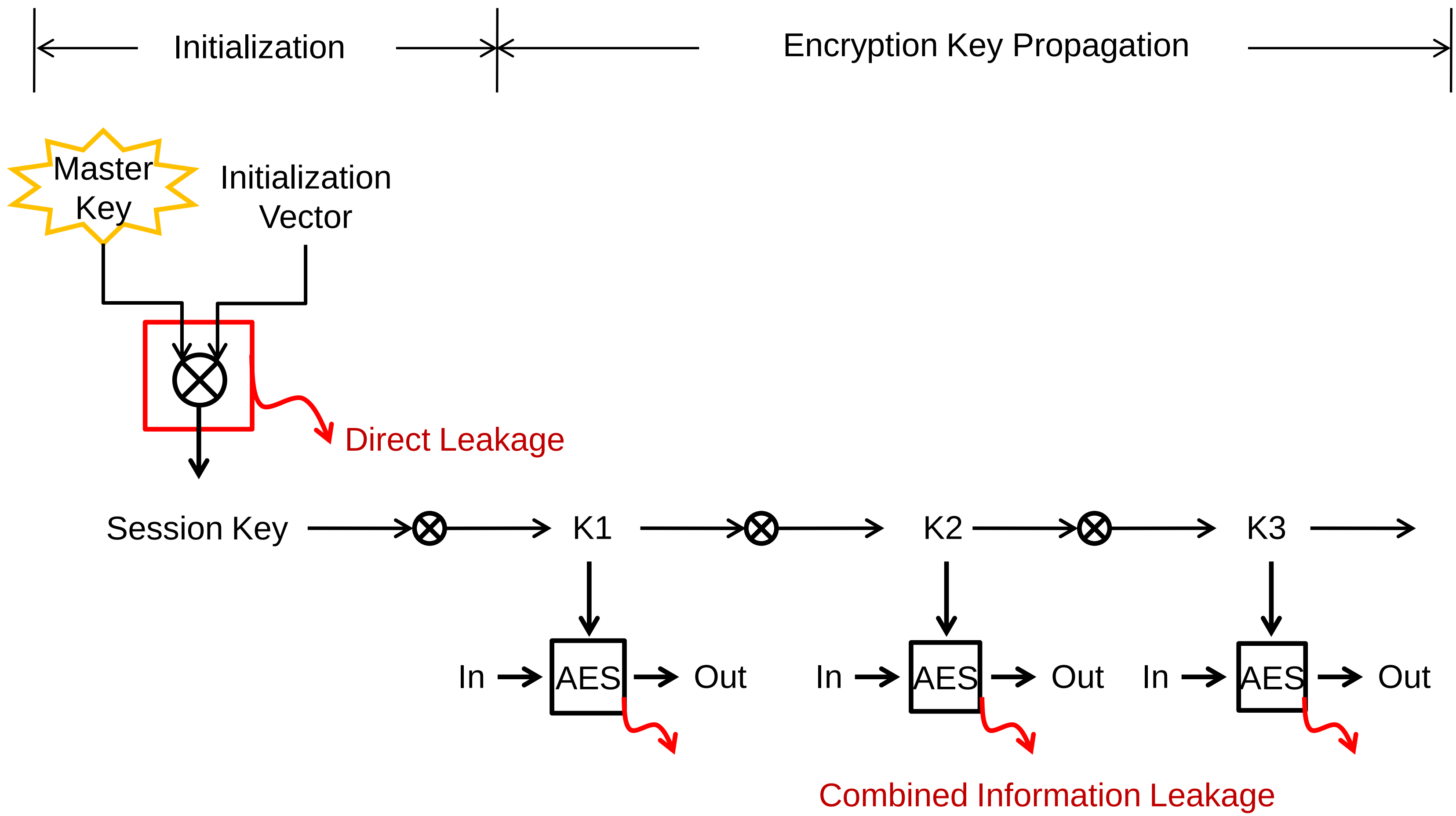
Design Model



Goal: protection against any “differential” attack.

This is NOT shifting the problem, but separating it.

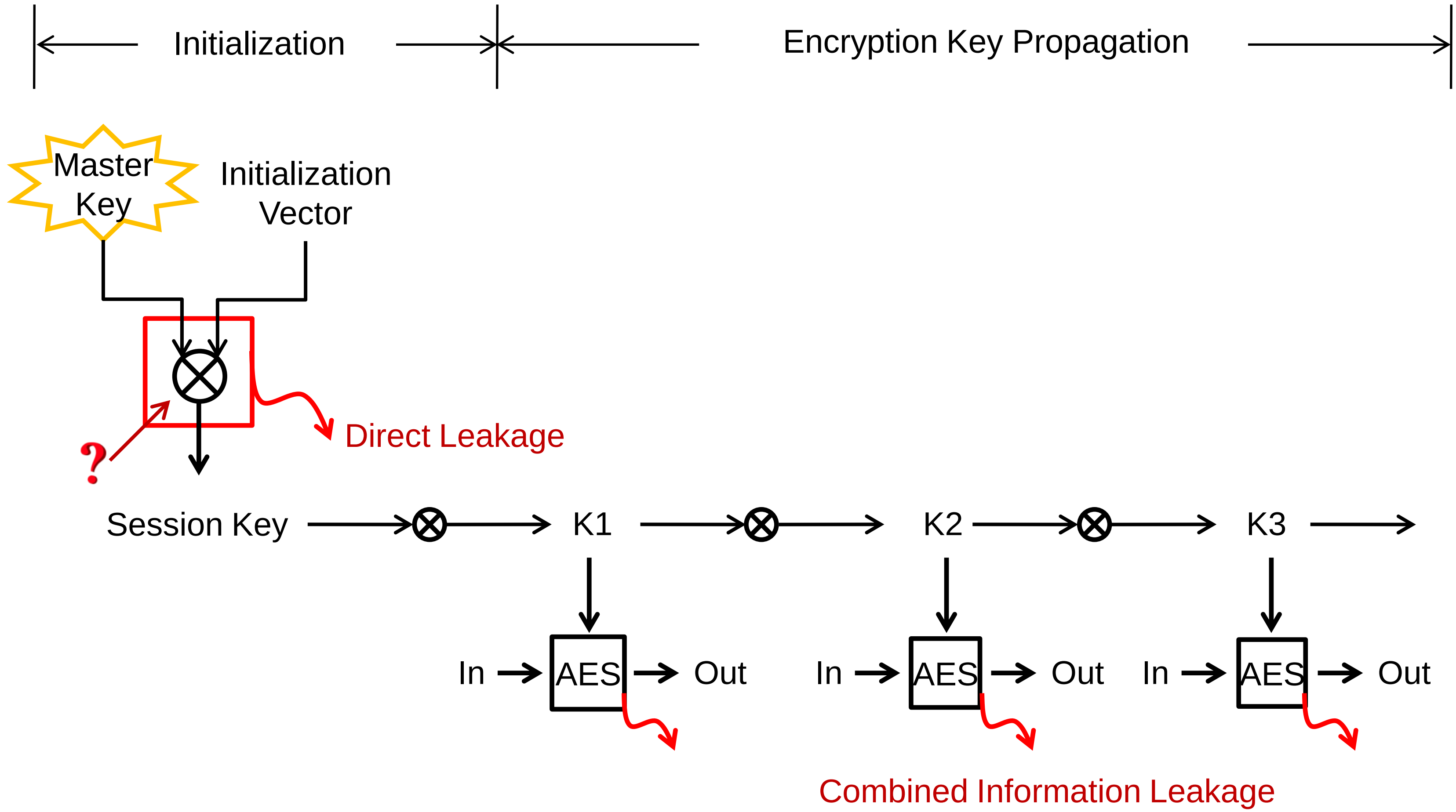
Design Model



Goal: protection against any “differential” attack.

This is NOT shifting the problem, but separating it.

Design Model

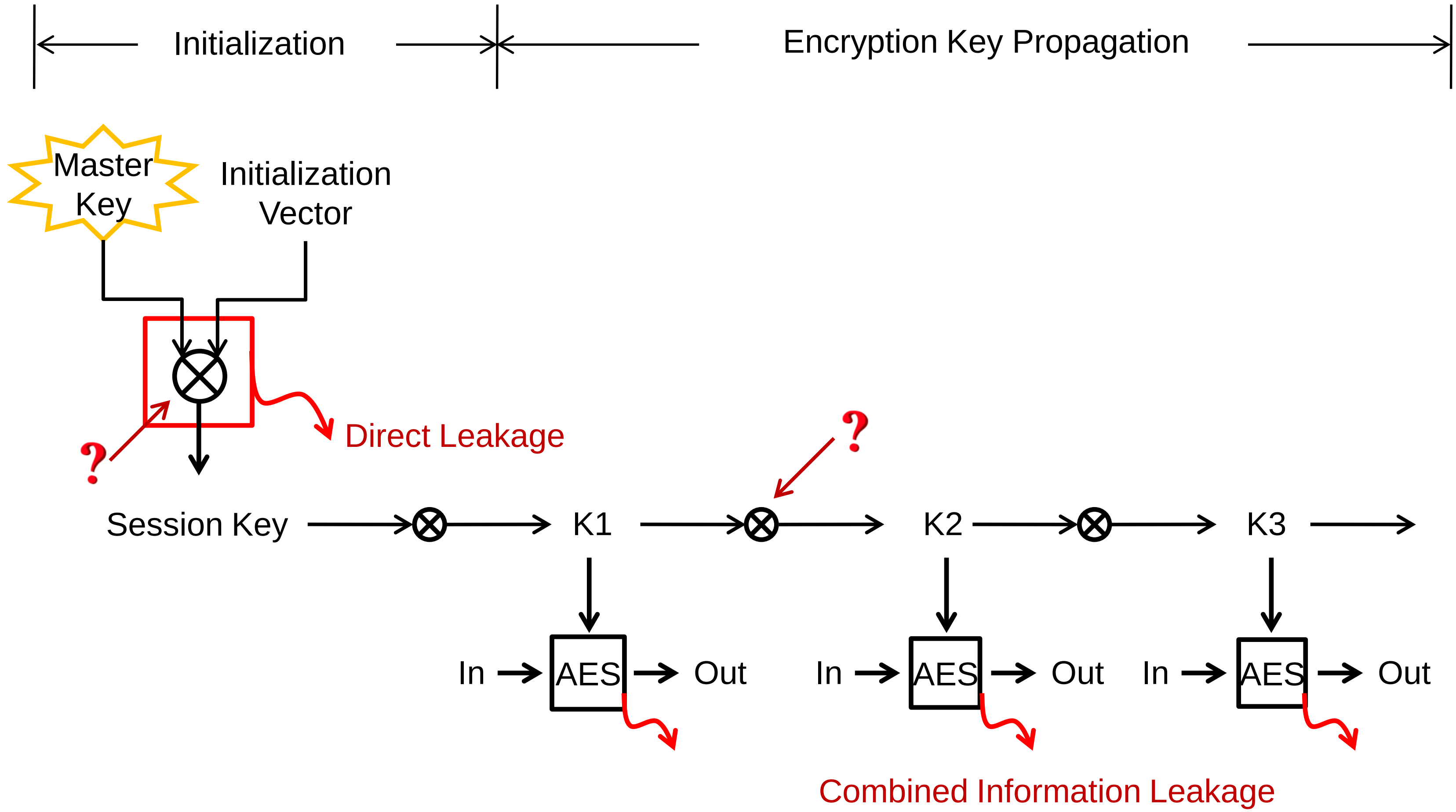


Goal: protection against any "differential" attack.

This is NOT shifting the problem, but separating it.

VirginiaTech Invent the Future

Design Model

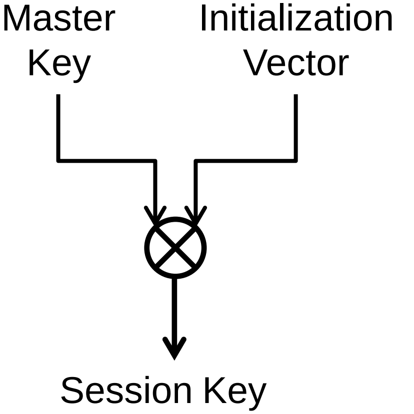


Goal: protection against any “differential” attack.

This is NOT shifting the problem, but separating it.

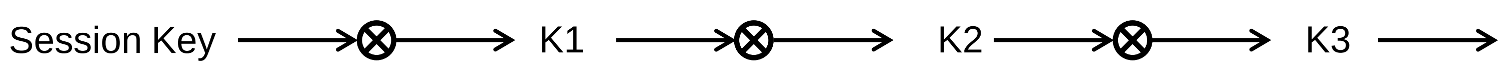
Security Requirements

- Initialization:
  - Maximum Diffusion.
  - Compatible with current AES modes .
    (no additional secrets or exchanged variables)
  - One-wayness.
  - DPA-hard, without depending on the Hardware.
  - Small hardware overhead.



Security Requirements

- Key Propagation:
  - Non-linearity.
  - Prevent divide-and-conquer.
  - Forward Security (better).
  - Small hardware overhead.



Previous Work

Contribution	Initialization	Propagation
[Kocher03]	DES	DES
[MSGR10]	Modular Multiplication	———
[GFM10]	NLM and AES	AES
[Kocher11]	Tree structure of Hashing	Hashing
[MSJ12]	Improved tree of AES	———
[BSH..13]	Minimum SP Network	———
Current Proposal	NLFSR-based scheme	

- They are all:
  - High cost.
  - Or, depend on other hardware protections.

Current Proposal

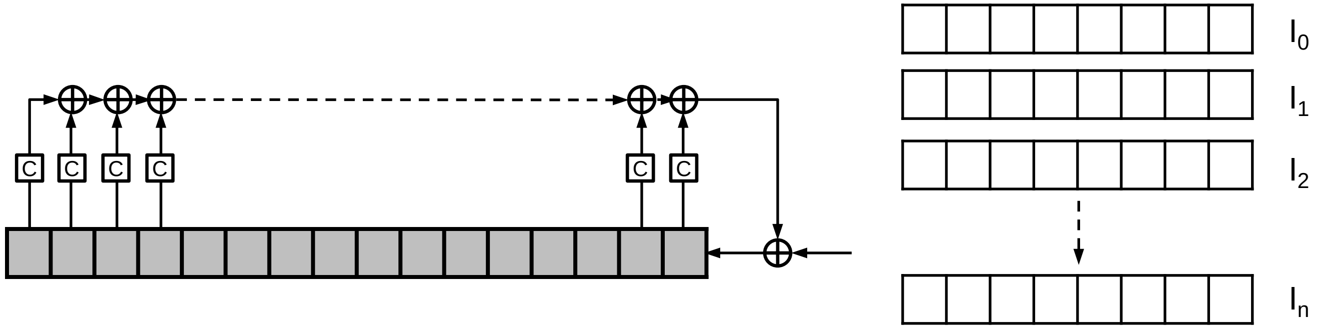
- Why NLFSR?
  - High DPA-attack complexity.

    Current DPA attack on Grain leaves 30 bits of the key for exhaustive search [FGKV07].
  - High diffusion and one-wayness.
  - High non-linearity.
  - Low hardware overhead,

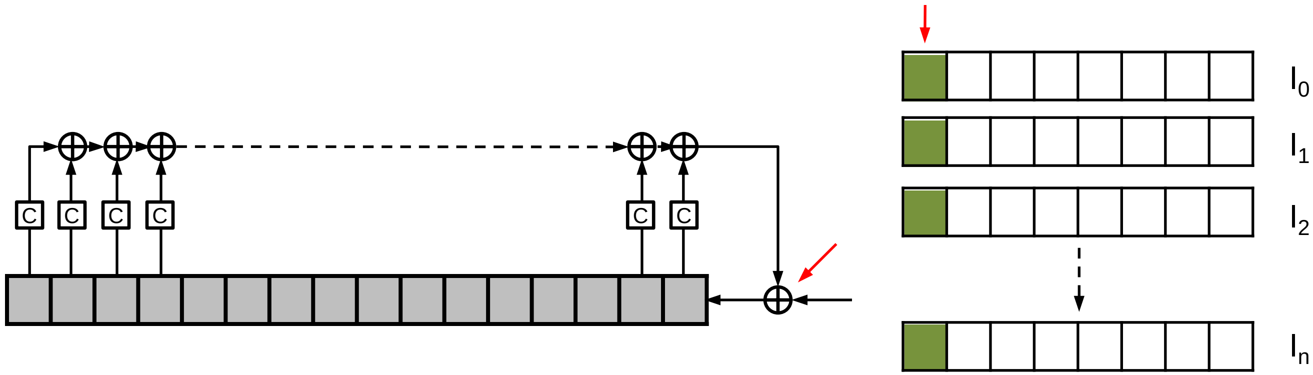
    as learned from the eSTREAM results.

- What are the preferred properties of the NLFSR for the best DPA-protection?

DPA of a Generic LFSRs



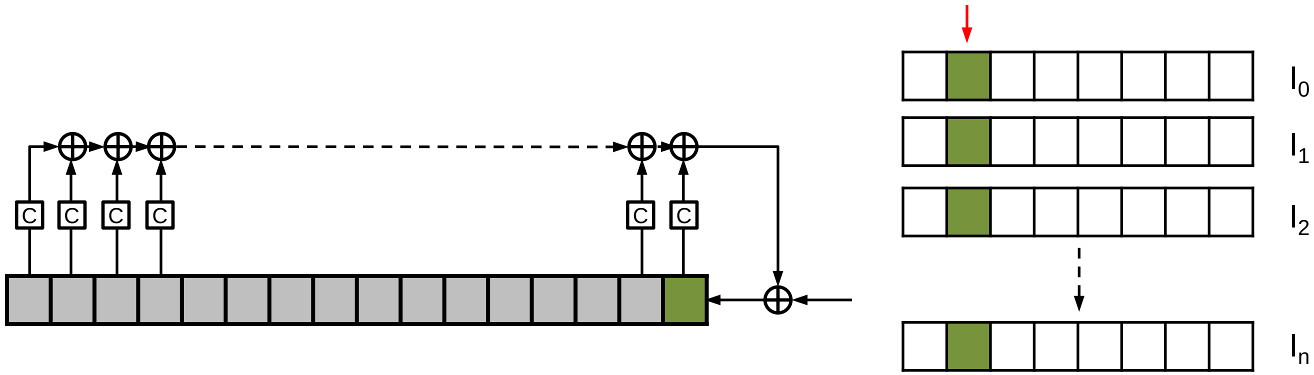
DPA of a Generic LFSRs



- 1^{st} input bit:
  - One sensitive variable of <u>high</u> leakage.

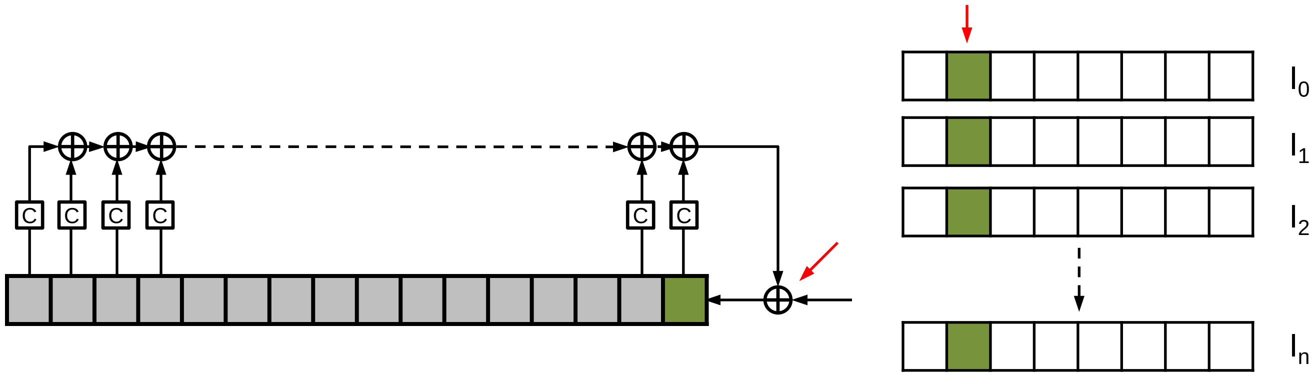
    The output of the feedback function can be found.

DPA of a Generic LFSRs



- 1^{st} input bit.
- 2^{nd} input bit:

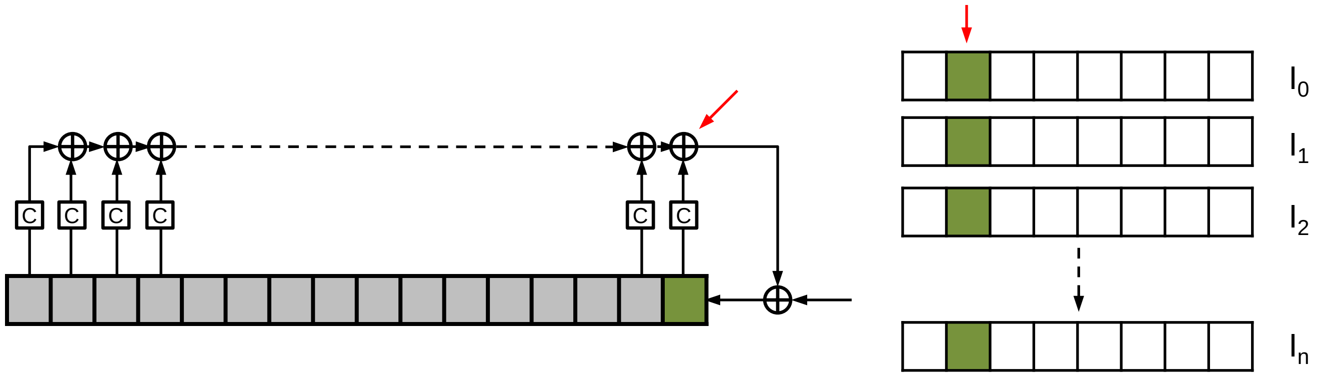
DPA of a Generic LFSRs



- 1^{st} input bit.
- 2^{nd} input bit:
  - Sensitive variable of <u>high</u> leakage.

    The output of the feedback function can be found.

DPA of a Generic LFSRs

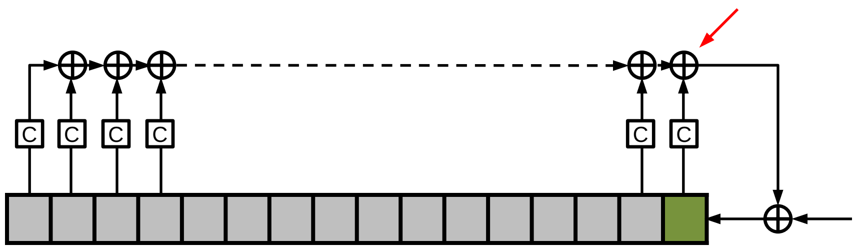


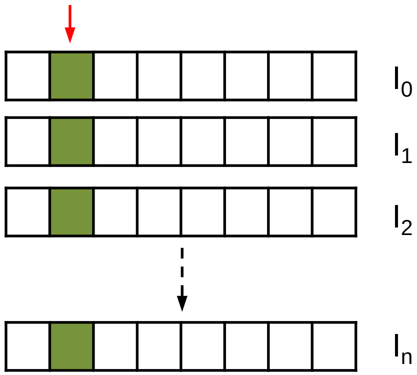
- 1^{st} input bit.
- 2^{nd} input bit:
  - Sensitive variable of <u>high</u> leakage.

    The output of the feedback function can be found.
  - Sensitive variable of <u>low</u> leakage.

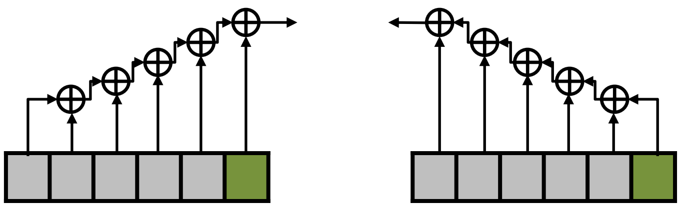
    Intermediate unknown can be found.

DPA of a Generic LFSRs

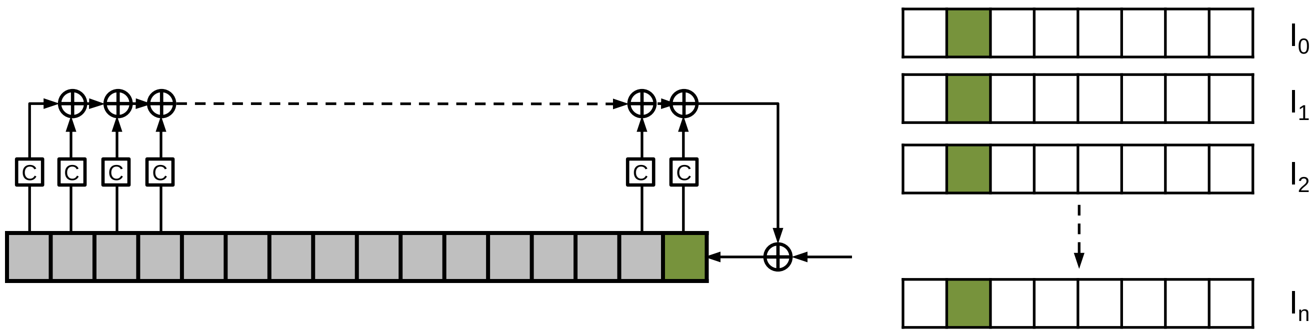




- 1^{st} input bit.
- 2^{nd} input bit:
  - Sensitive variable of <u>high</u> leak
    The output of the feedback functio
  - Sensitive variable of <u>low</u> leaka
    Intermediate unknown can be foun
    Is it useful? depends on the computational hierarchy.

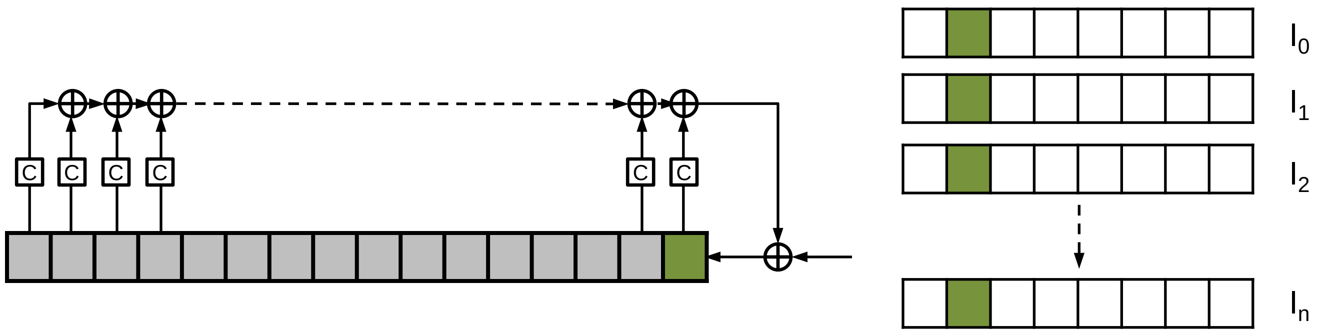


DPA of a Generic LFSRs



- 1^{st} input bit.
- 2^{nd} input bit.
- n^{th} input bit:
  - A linear equation of n unknowns.

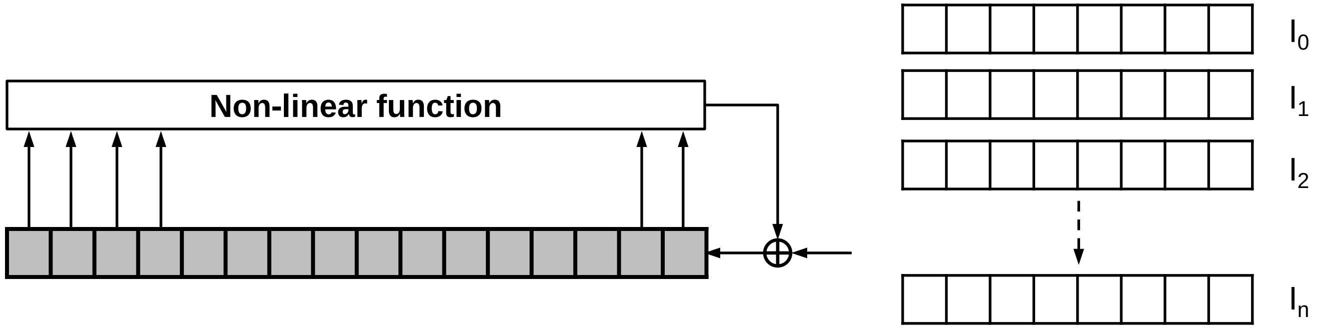
DPA of a Generic LFSRs



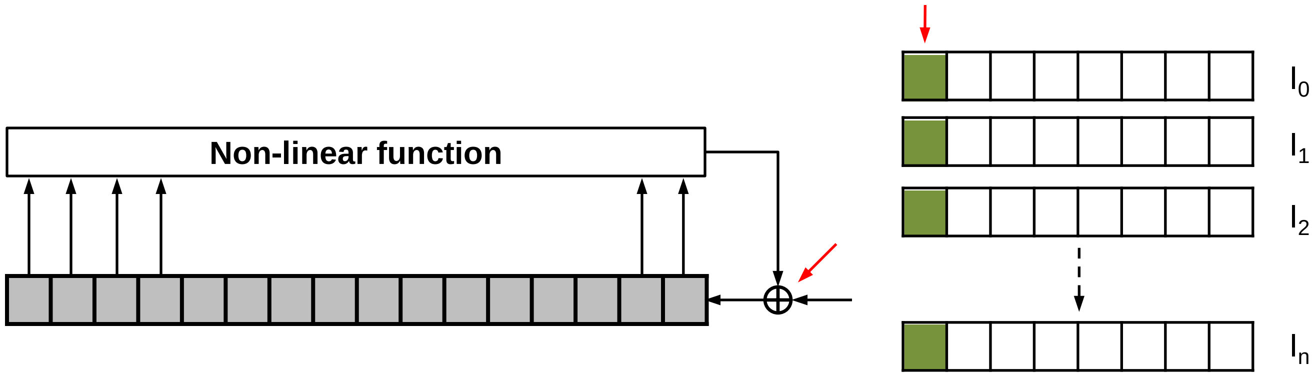
- 1^{st} input bit.
- 2^{nd} input bit.
- n^{th} input bit:
  - A linear equation of n unknowns.

LFSRs are directly breakable after reaching all state bits

DPA of a Generic NLFSRs



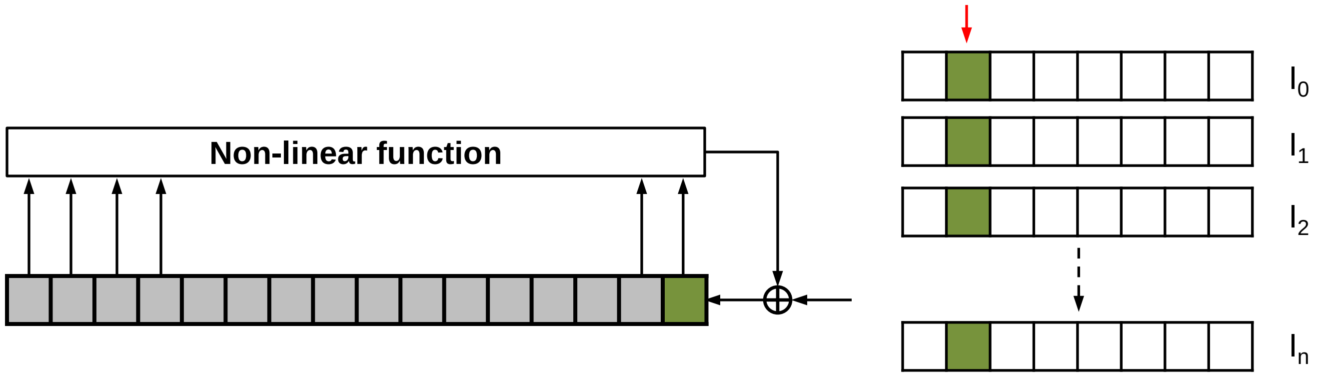
DPA of a Generic NLFSRs



- 1^{st} input bit:
  - One sensitive variable of high leakage.

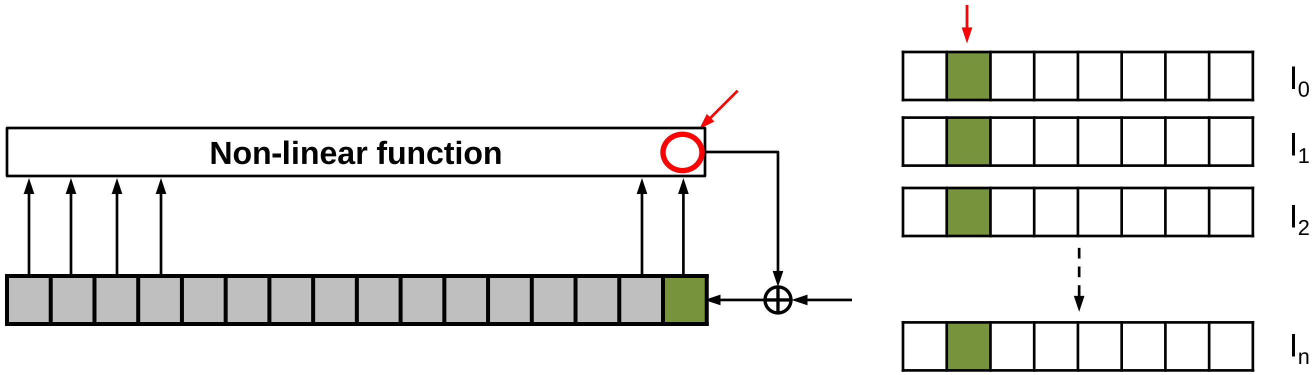
    The output of the feedback function can be found.

DPA of a Generic LFSRs



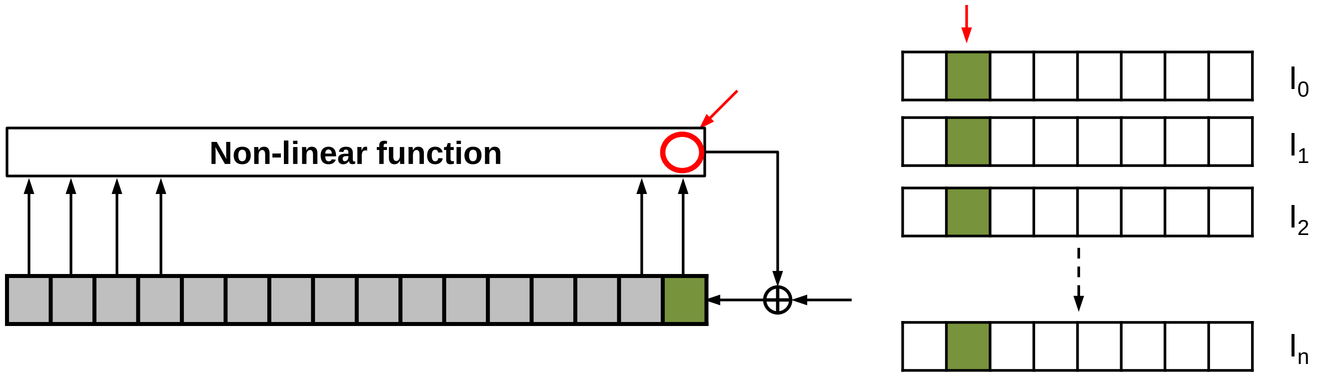
- 1^{st} input bit.
- 2^{nd} input bit: Operation at the known bit:

DPA of a Generic LFSRs



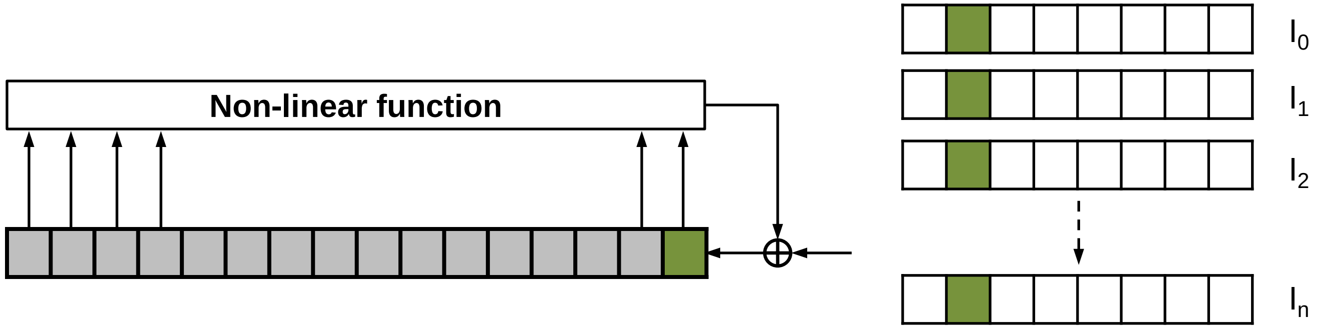
- 1^{st} input bit.
- 2^{nd} input bit: Operation at the known bit:
  - XOR: The output of the feedback function can be found.
    Intermediate unknown can be found. Is it useful?
  - AND: Only the intermediate unknown (low leakage) can be found.
    Is it useful? depends on the computational hierarchy.

DPA of a Generic LFSRs



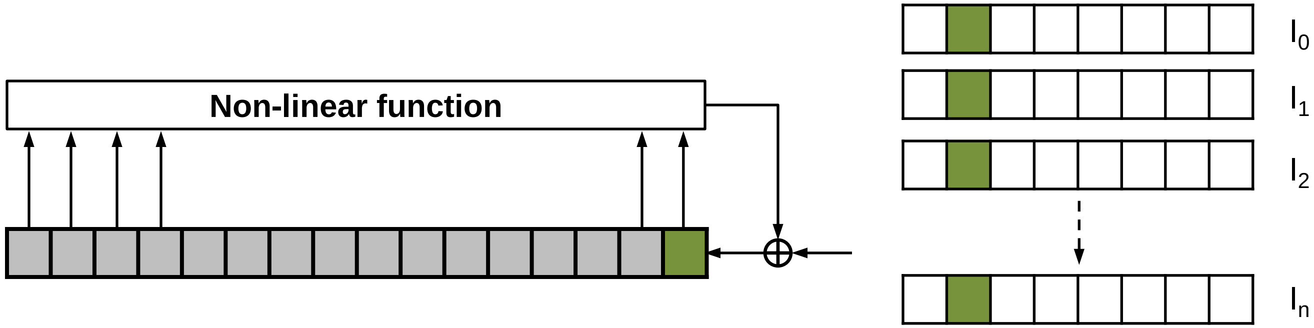
- 1^{st} input bit.
- 2^{nd} input bit: Operation at the known bit:
  - XOR: The output of the feedback function can be found.
    Intermediate unknown can be found. Is it useful?
  - ✓ AND: Only the intermediate unknown (<u>low leakage</u>) can be found.
    Is it useful? depends on the computational hierarchy.

DPA of a Generic LFSRs



- 1^{st} input bit.
- 2^{nd} input bit.
- n^{th} input bit:
  - Only an intermediate variable within the feedback function

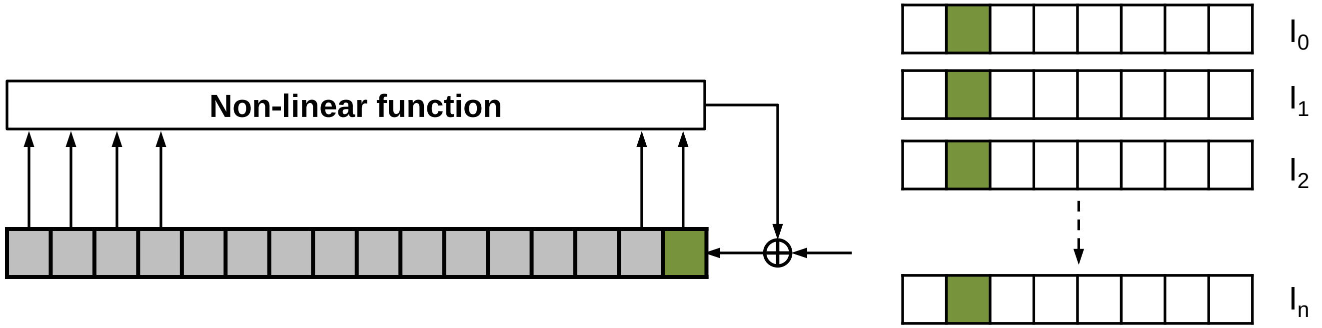
DPA of a Generic LFSRs



- 1^{st} input bit.
- 2^{nd} input bit.
- n^{th} input bit:
  - Only an intermediate variable within the feedback function

NLFSRs can still be broken by focusing on small operations within the feedback function

DPA of a Generic LFSRs



- Solution:

  Implement the feedback function in memory.

DPA of a Generic NLFSRs

- Preferred properties:
  - Large internal state.
  - High number of feedback taps.
  - Feedback function includes the first state bit.
  - Either:
    - The first bit is ANDed at the top of computational hierarchy.
    - Or, the feedback function is implemented using memory.
  - Maximum period.

Comparison between NLFSRs

	Grain	Trivium	KeeLoq	[D12]	[RSWZ12]	Best
Internal State	80	288	32	4:24	25,27	27
Feedback taps	13	3*5	7	3:7	18:21	21
Include 1^{st} bit	No	No	Yes	Yes	Yes	Yes
1^{st} bit ANDed	No	No	Yes	No	No	No
Maximum period	?	?	?	Yes	Yes	Yes

Comparison between NLFSRs

	Grain	Trivium	KeeLoq	[D12]	[RSWZ12]	Best
Internal State	80	288	32	4:24	25,27	27
Feedback taps	13	3*5	7	3:7	18:21	21
Include 1st bit	No	No	Yes	Yes	Yes	Yes
1st bit ANDed	No	No	Yes	No	No	No
Maximum period	?	?	?	Yes	Yes	Yes

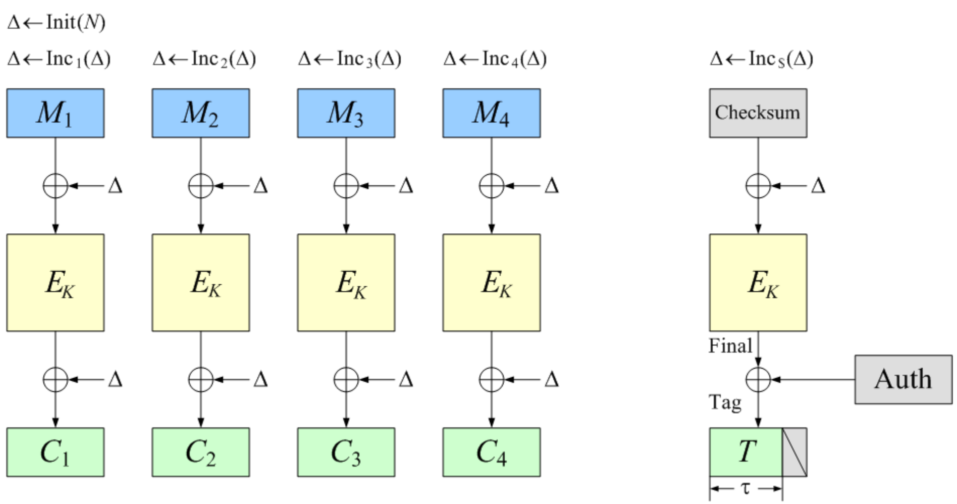
- The best available NLFSR is still not optimal.

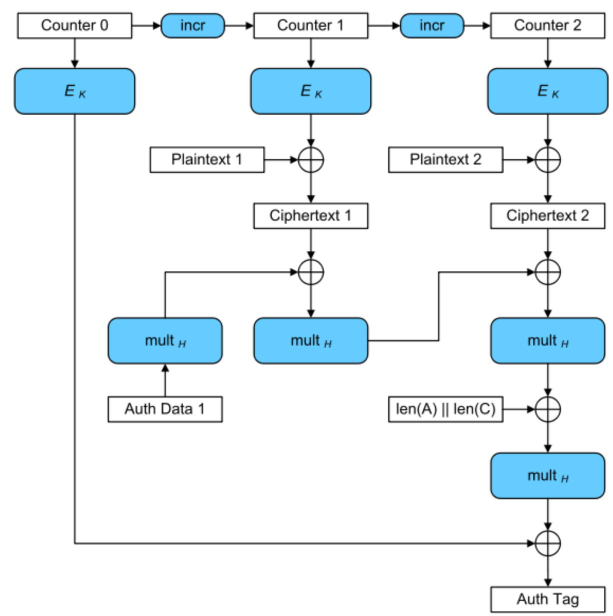
Current Work

- Choose a new feedback function.
- Increase the parallelism.
- Implementation
- Practical DPA attack.

Future Work

- Include the DPA-protection in a new AE mode
  - Most modes of operation including major AE modes keep the Key as a constant.
  - Updating the Key can provide a free DPA-protection in new designs.





Concluding Remaks

- DPA-protection can be achieved by a special mode of operation.
- We propose a light-weight primitive that can achieve a high level of DPA security.
- We are working on including the DPA-protection in a new AE mode.

✓Collaborations are welcomed✓

Thank You
Questions?