ISAP

Towards Side-channel Secure AE

Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, Florian Mendel, Thomas Unterluggauer

FSE 2017

Introduction

Problem: side-channel attacks

Countermeasures: hiding, masking, TI ...

Introduction

Problem: side-channel attacks

Countermeasures: hiding, masking, TI ...

Reduce overhead of countermeasures

- ASCON, KETJE/KEYAK, PRIMATES, SCREAM, ...

Introduction

Problem: side-channel attacks

Countermeasures: hiding, masking, TI ...

Reduce overhead of countermeasures

- ASCON, KETJE/KEYAK, PRIMATES, SCREAM, ...

Can we do more?

- LR and MR AE [Ber+16]
- ISAP

ISAP

Authenticated encryption scheme

- Following requirements of CAESAR call
- No assumptions on choice of the nonce

Provides protection against DPA for:

- Encryption
- Decryption

Solely based on sponges

- Limits the attack surface against SPA

SPA and DPA

Simple Power Analysis (SPA)

- Observe device processing the same or a few inputs
- Techniques directly interpreting measurements

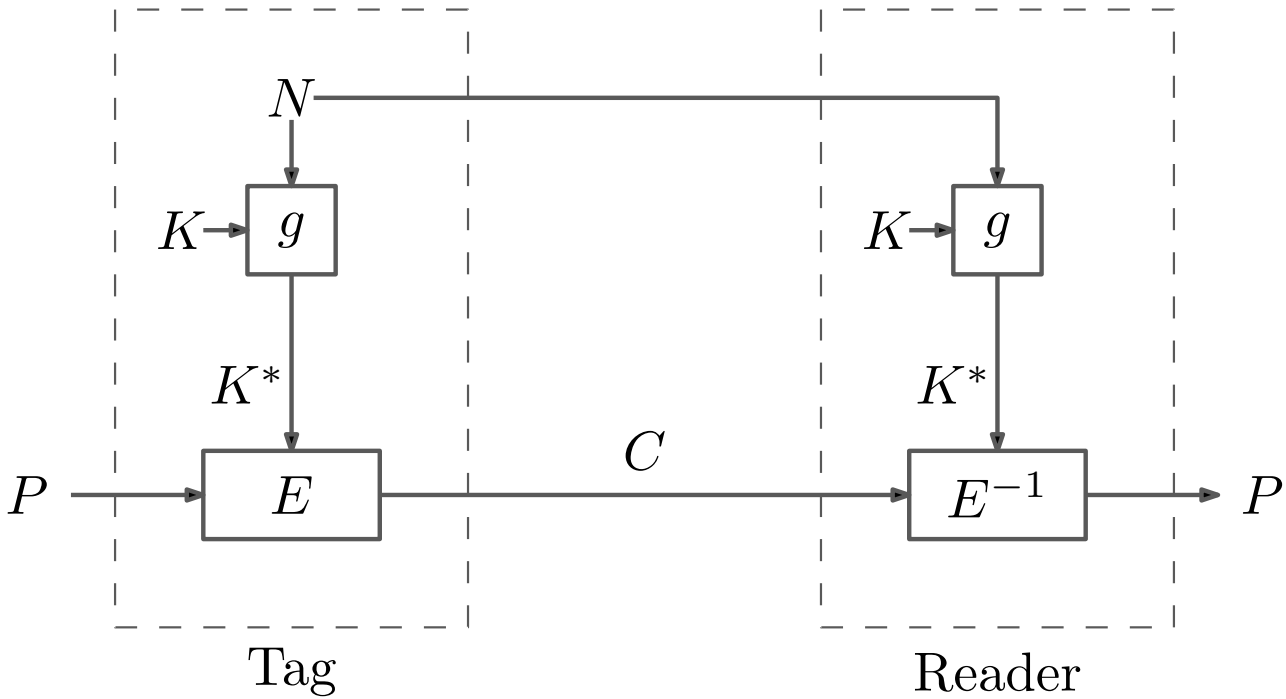
Differential Power Analysis (DPA)

- Observe device processing many different inputs
- Allows for the use of statistical techniques

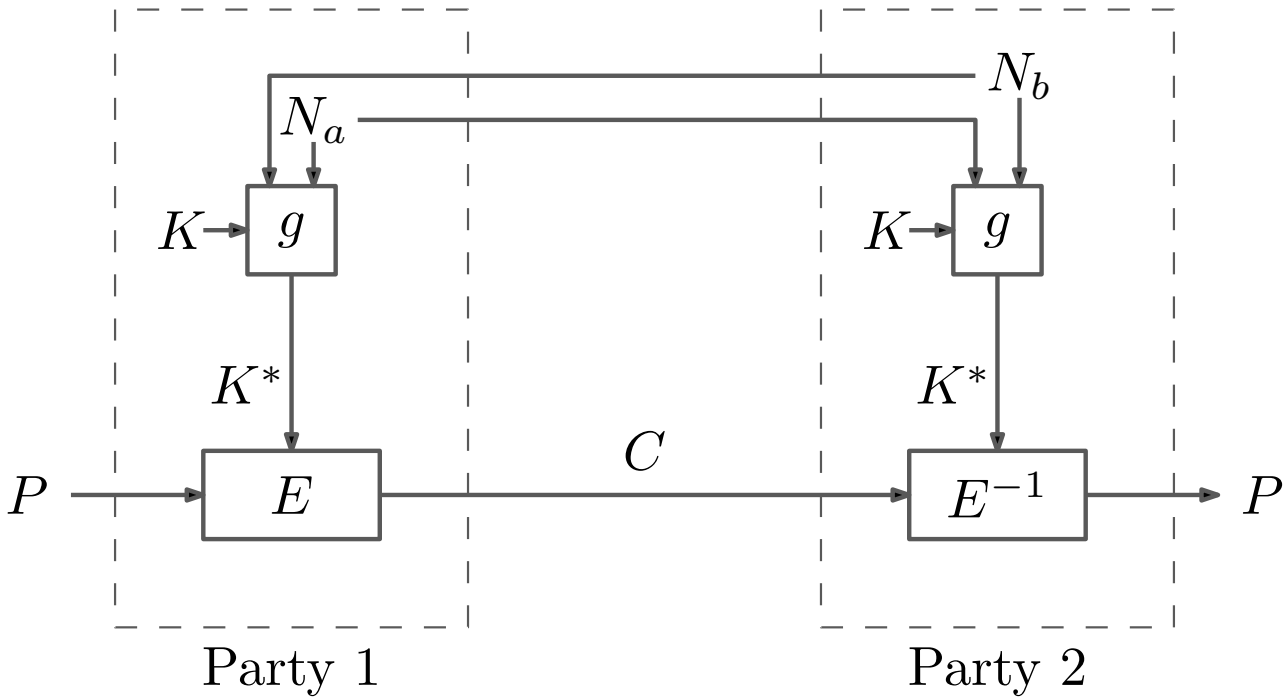
Is DPA Still a Threat?

- A. Moradi and T. Schneider Improved Side-Channel Analysis Attacks on Xilinx Bitstream Encryption of 5, 6, and 7 Series COSADE 2016
- E. Ronen, C. O'Flynn, A. Shamir, and A.-O. Weingarten IoT Goes Nuclear: Creating a ZigBee Chain Reaction Cryptology ePrint Archive, Report 2016/1047, 2016

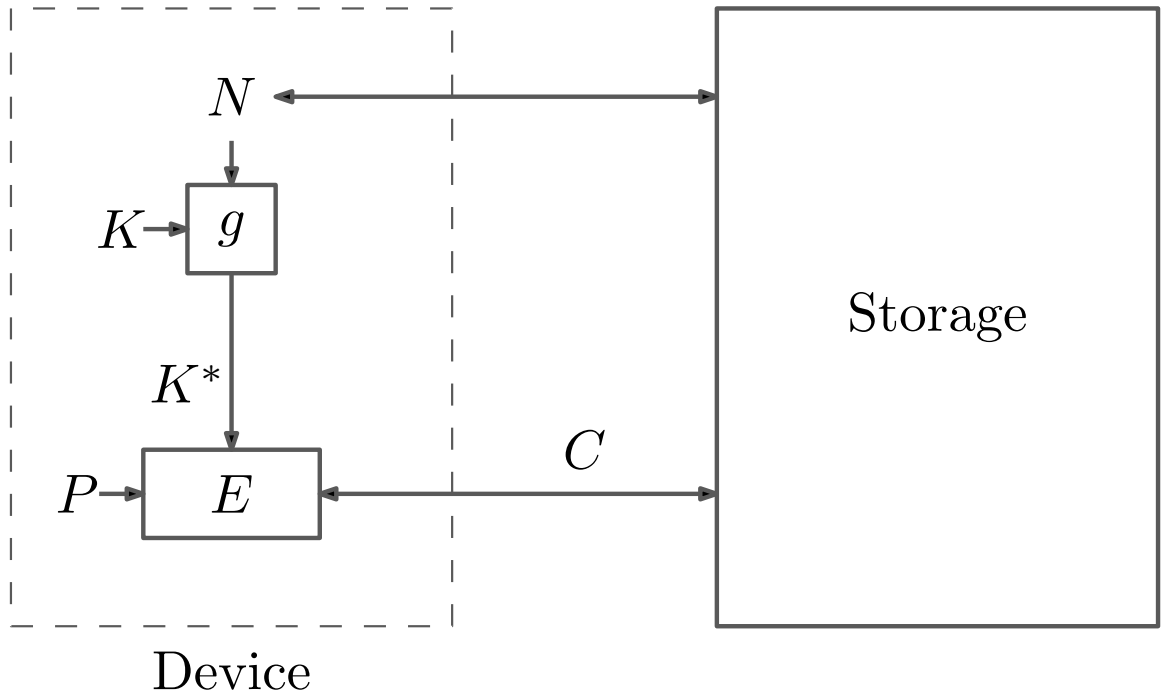
Fresh Re-keying [Med+10]



Fresh Re-keying [Med+11]



What About Storage?



- Encryption still fine
- Decryption causes problems

Multiple Decryption

Retain principles of fresh re-keying allowing multiple decryption

Multiple Decryption

Retain principles of fresh re-keying allowing multiple decryption

DPA protection in storage settings

- A. Moradi and T. Schneider Improved Side-Channel Analysis Attacks on Xilinx Bitstream Encryption of 5, 6, and 7 Series COSADE 2016

DPA protection in unidirectional/broadcast settings

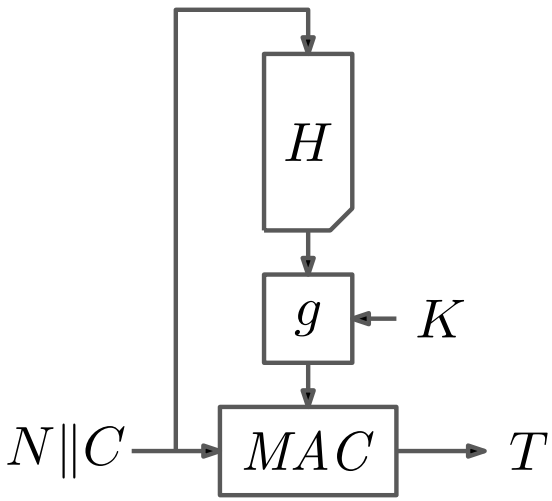
- E. Ronen, C. O'Flynn, A. Shamir, and A.-O. Weingarten IoT Goes Nuclear: Creating a ZigBee Chain Reaction Cryptology ePrint Archive, Report 2016/1047, 2016

Priciple of ISAP's Decryption

"Bind" the session key to the data that is decrypted

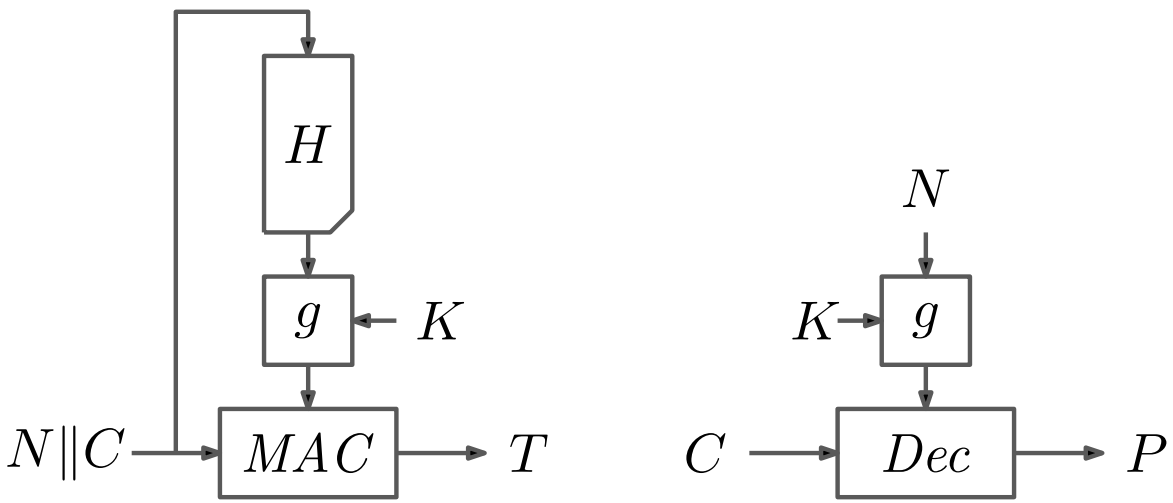
Priciple of ISAP's Decryption

"Bind" the session key to the data that is decrypted

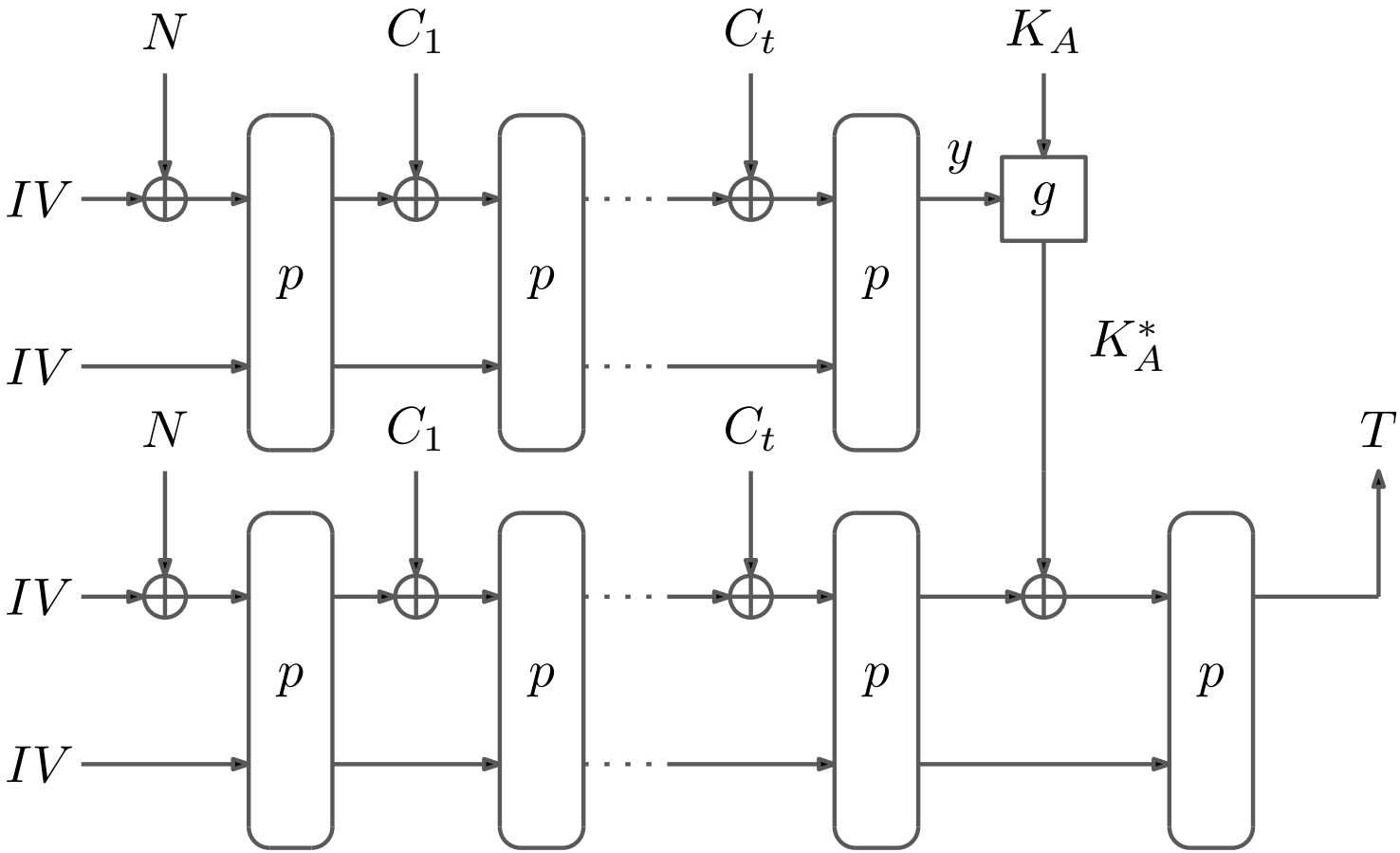


Priciple of ISAP's Decryption

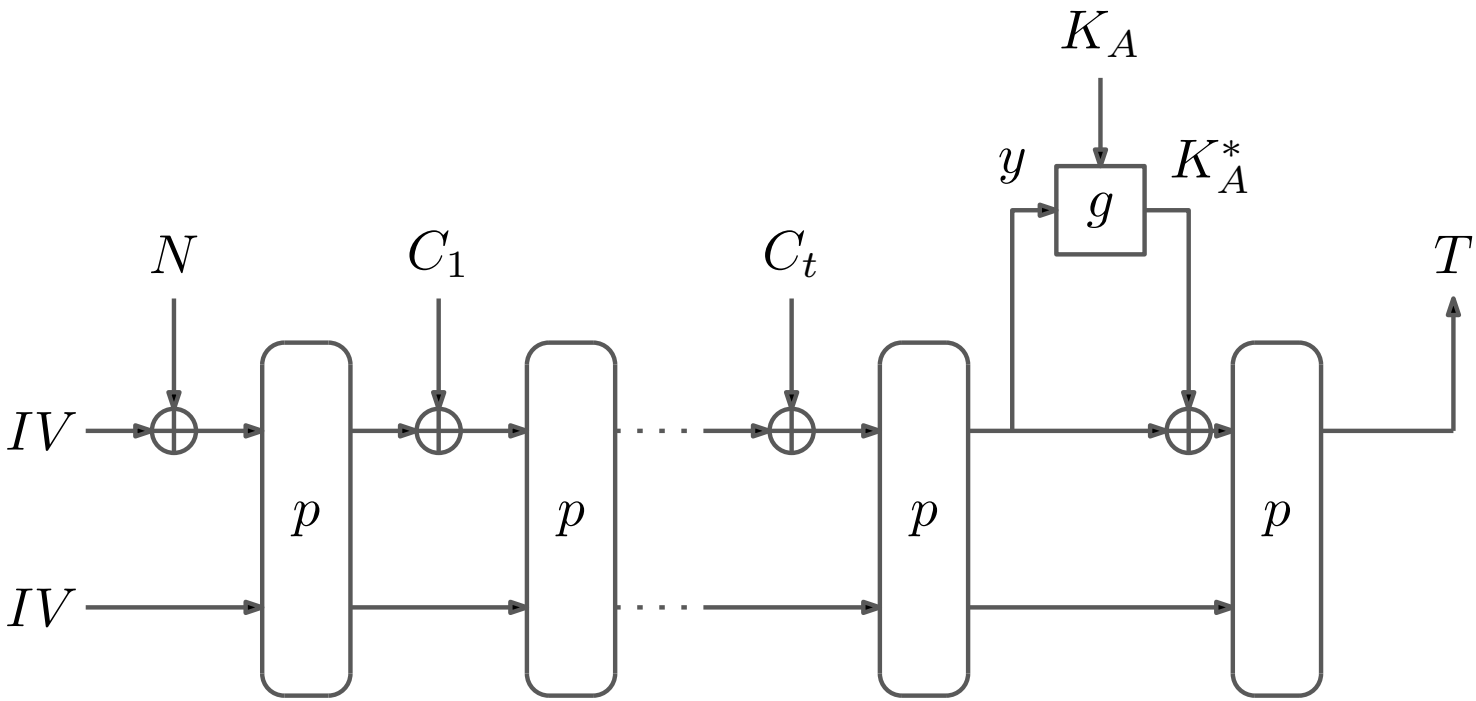
"Bind" the session key to the data that is decrypted



ISAP's Authentication/Verification

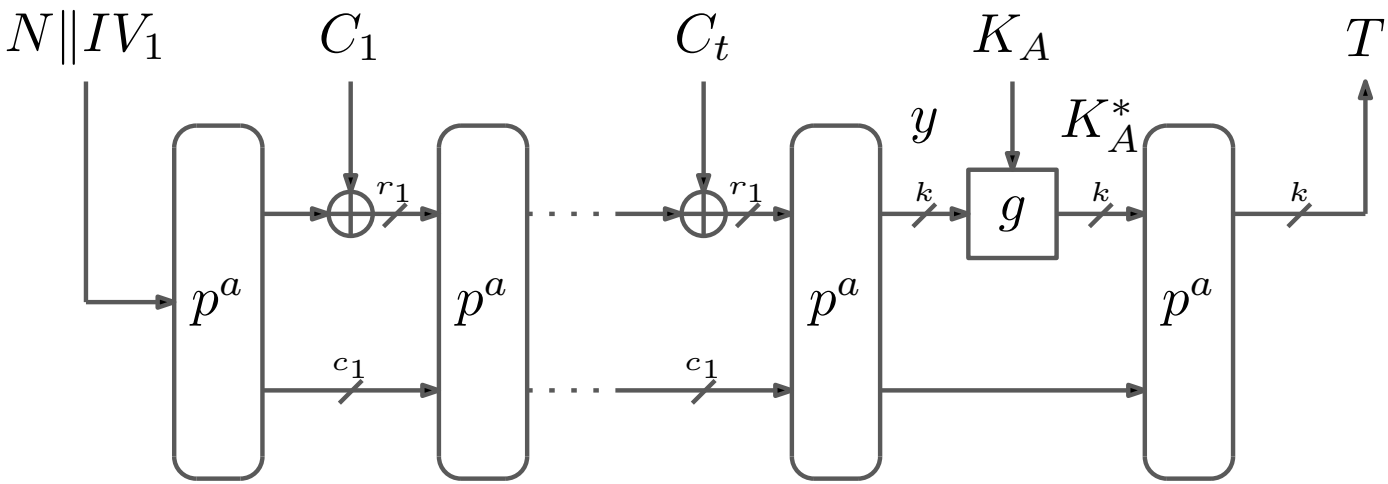


ISAP's Authentication/Verification



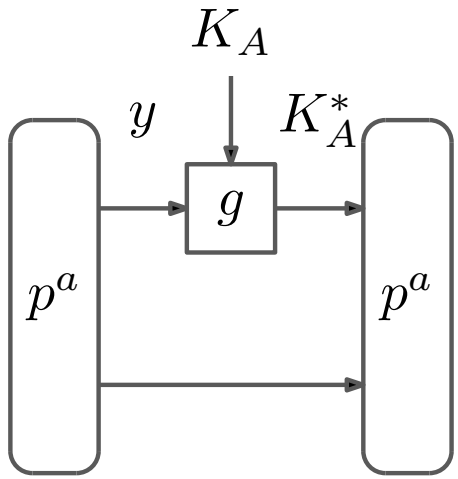
ISAP's Authentication/Verification

Use suffix MAC instead of hash-then-MAC



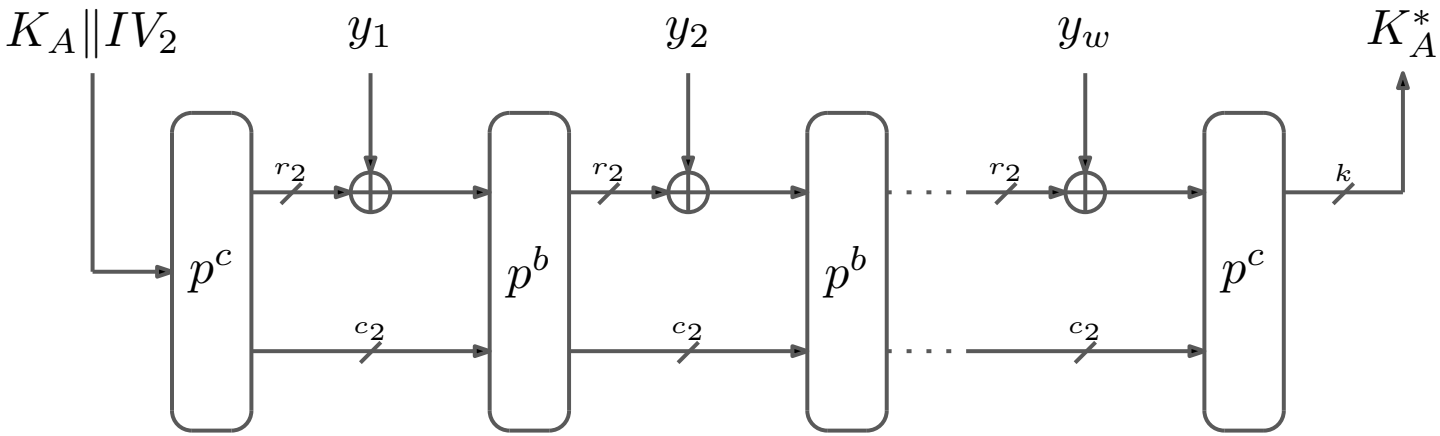
Possible *g* to Absorb Key

- Modular multiplication [Med+10]
- LPL and LWE [Dzi+16]
- Sponges [TS14]

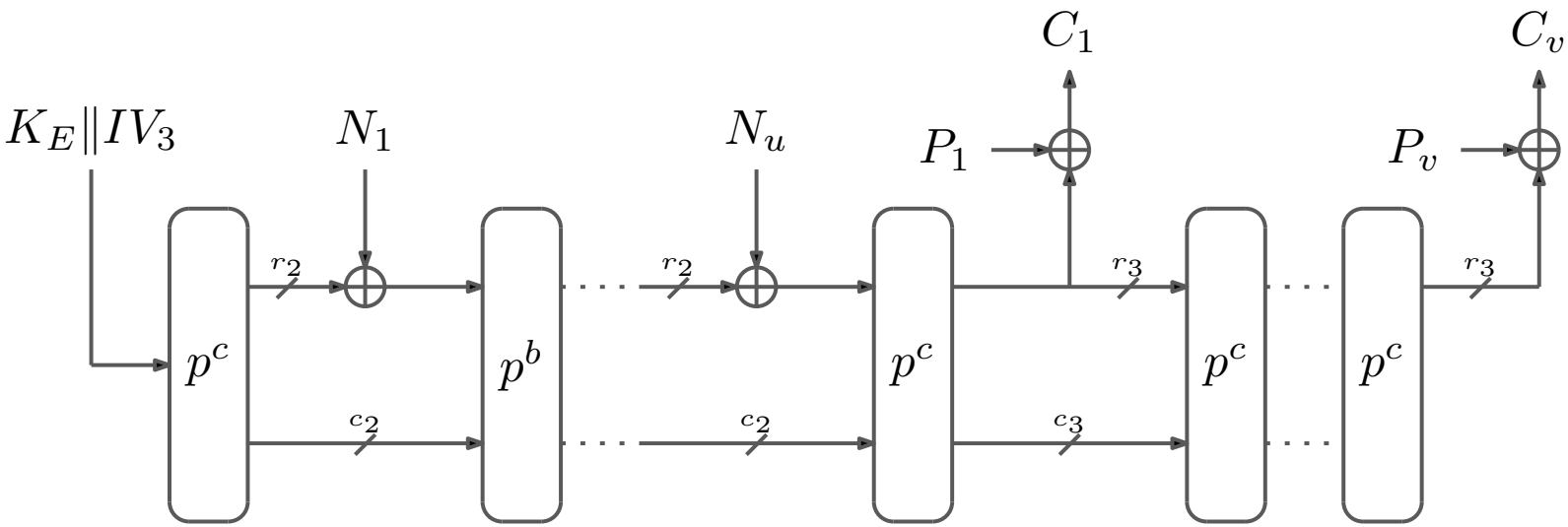


Absorbing the Key

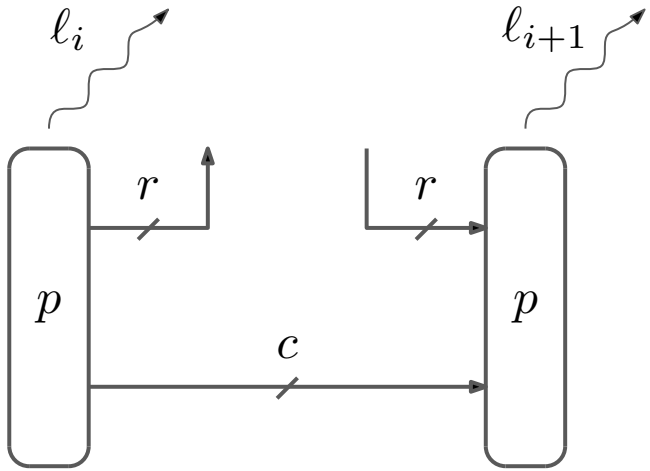
Idea: Reduce rate to a minimum [TS14]
Related to the classical GGM construction [GGM86]



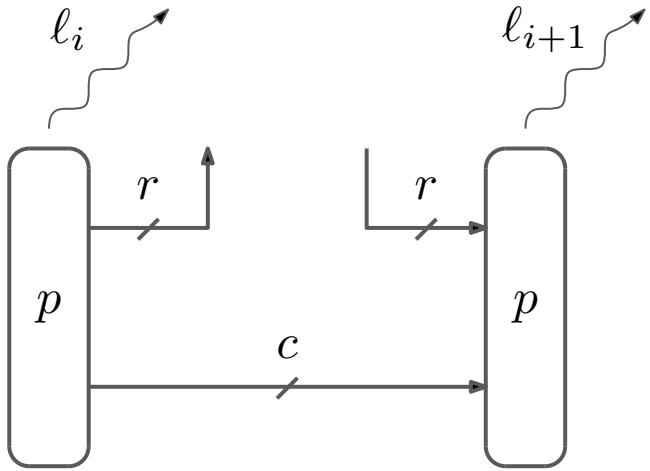
ISAP's En-/Decryption

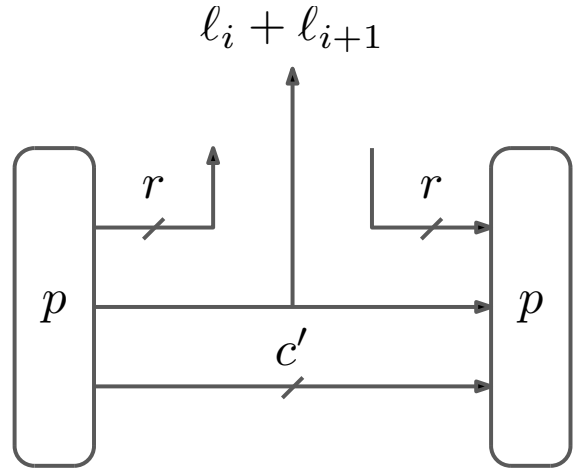


Sponges and Side-channel Leakage



Sponges and Side-channel Leakage





$$c' = c - (\ell_i + \ell_{i+1})$$

Instances

KECCAK-p[400,n_r] as permutation [Ber+14]

Name	Security level	Bit size of			Rounds		
	k	r_1	r_2	r_3	a	b	c
ISAP-128	128	144	1	144	20	12	12
ISAP-128a	128	144	1	144	16	1	8

Implementation

One round per cycle

Function	Area [kGE]	Initialization [cycles]	Initialization [μs]	Runtime per Block [cycles]	Runtime per Block [μs]
ISAP-128	14.0	3 401	20.1	36	0.20
ISAP-128a	14.0	564	3.3	28	0.16

Conclusion

- AE scheme following requirements of CAESAR call
- Provides protection against DPA
  - Encryption
  - Decryption
- Enables several use-cases
  - Multiple decryption of stored data
  - Unidirectional/Broadcast communication

Thank you

References I

[Ber+14] G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, and R. Van Keer
Ketje
Submission to the CAESAR competition: http://competitions.cr.yp.to, 2014

[Ber+16] F. Berti, F. Koeune, O. Pereira, T. Peters, and F.-X. Standaert
Leakage-Resilient and Misuse-Resistant Authenticated Encryption
Cryptology ePrint Archive, Report 2016/996, 2016

[Dzi+16] S. Dziembowski, S. Faust, G. Herold, A. Journault, D. Masny, and F.-X. Standaert
Towards Sound Fresh Re-keying with Hard (Physical) Learning Problems
CRYPTO 2016

References II

[GGM86] O. Goldreich, S. Goldwasser, and S. Micali
How to construct random functions
J. ACM 33:4, 1986

[Med+10] M. Medwed, F.-X. Standaert, J. Großschädl, and F. Regazzoni
Fresh Re-keying: Security against Side-Channel and Fault Attacks for Low-Cost Devices
AFRICACRYPT 2010

[Med+11] M. Medwed, C. Petit, F. Regazzoni, M. Renauld, and F.-X. Standaert
Fresh Re-keying II: Securing Multiple Parties against Side-Channel and Fault Attacks
CARDIS 2011

[MS16] A. Moradi and T. Schneider
Improved Side-Channel Analysis Attacks on Xilinx Bitstream Encryption of 5, 6, and 7 Series
COSADE 2016

References III

[Ron+16] E. Ronen, C. O'Flynn, A. Shamir, and A.-O. Weingarten
IoT Goes Nuclear: Creating a ZigBee Chain Reaction
Cryptology ePrint Archive, Report 2016/1047, 2016

[TS14] M. M. I. Taha and P. Schaumont
Side-channel countermeasure for SHA-3 at almost-zero area overhead
HOST 2014