On Ascon and Isap

About Two Authenticated Encryption Schemes

Christoph Dobraunig

October 2018

Designed by:

Ascon: C. Dobraunig, M. Eichlseder, F. Mendel, M. Schläffer

Isap: C. Dobraunig, M. Eichlseder, S. Mangard, F. Mendel, T. Unterluggauer

Introduction to Authenticated Encryption

Interface

- Encryption & Authentication
  - $\mathcal{E}(K, N, A, P) \rightarrow (C, T)$
- Decryption & Verification
  - $\mathcal{D}(K, N, A, C, T) \rightarrow \{P, \perp\}$

Motivation

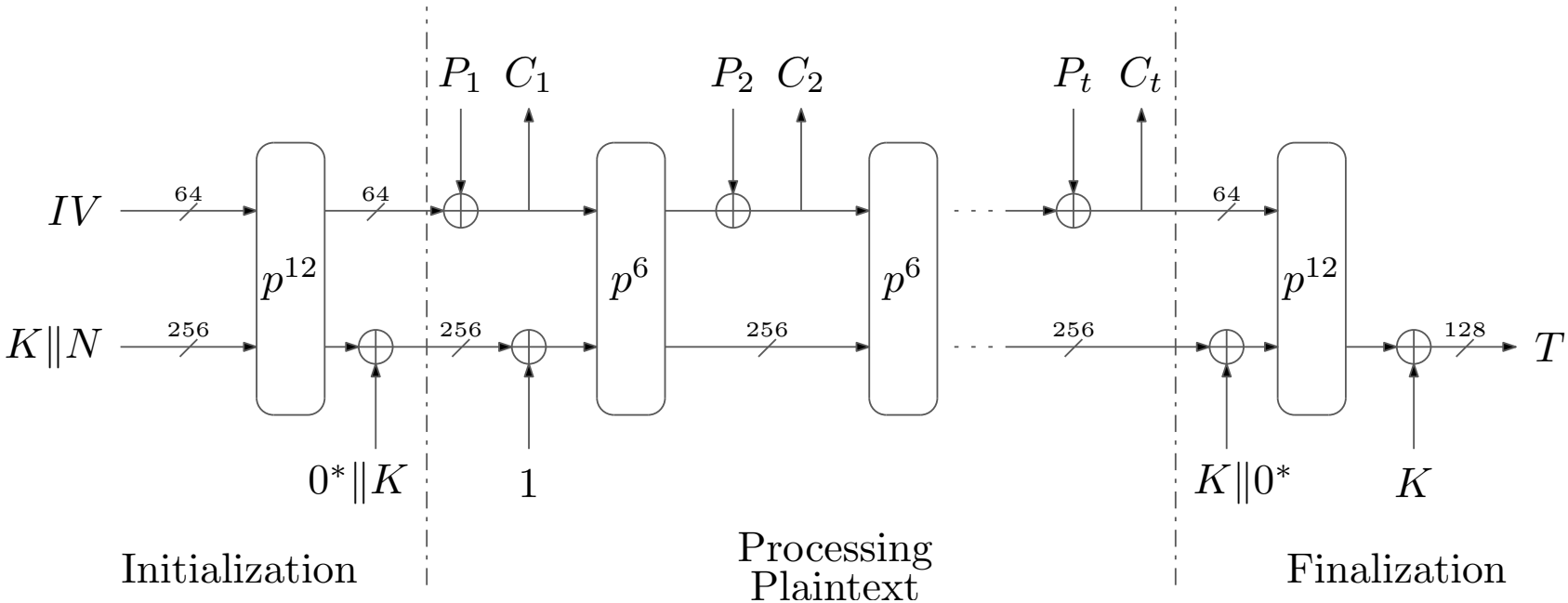
- Generic composition
  - E.g., Encrypt-then-MAC
- Dedicated mode
  - E.g., standards like GCM, CCM, OCB, ...
- Which one to use?
- Can we do better?

Competitions

- AES, SHA-3, eStream...
- CAESAR: Competition for Authenticated Encryption – Security, Applicability, and Robustness
  - http://competitions.cr.yp.to/caesar.html
- 57 submissions in 2014
- 7 finalists remaining
- One of them is ASCON

ASCON: A Finalist of CAESAR

ASCON – Mode

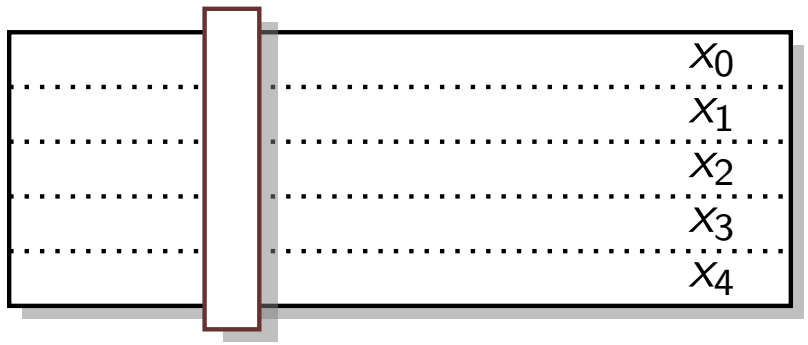

P_1 C_1
P_2 C_2
P_t C_t
IV
$K\|N$
64
256
p^{12}
p^6
$0^*\|K$
1
$K\|0^*$
K
128
T
Initialization
Processing Plaintext
Finalization

ASCON – Permutation

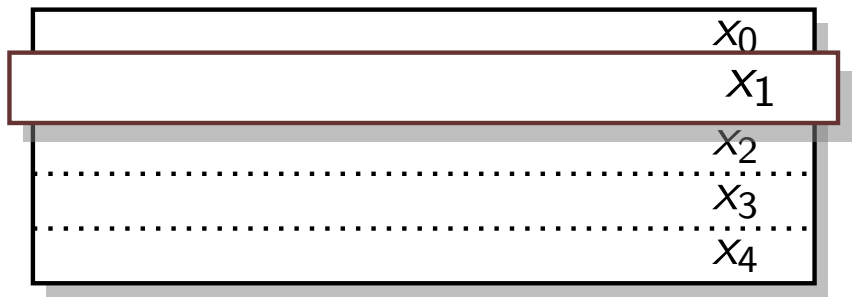
- Iterative application of round function
- One round
  - Constant addition
  - Substitution layer
  - Linear layer

ASCON – Round

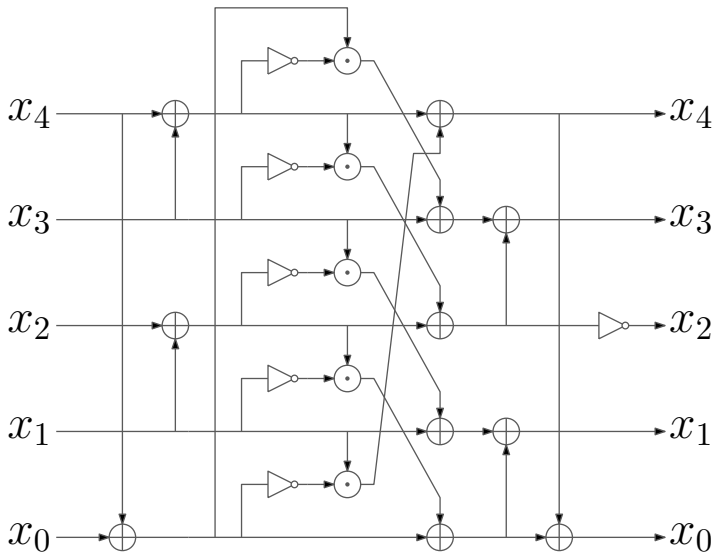
- Substitution layer



- Linear layer



ASCON – Round



S-box

$$x_4 \oplus (x_4 \ggg 7) \oplus (x_4 \ggg 41) \rightarrow x_4$$

$$x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17) \rightarrow x_3$$

$$x_2 \oplus (x_2 \ggg 1) \oplus (x_2 \ggg 6) \rightarrow x_2$$

$$x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 39) \rightarrow x_1$$

$$x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28) \rightarrow x_0$$

Linear transformation

ASCON – Benefits

- Simplicity
  - Defined on 64-bit words
  - Using bitwise Boolean functions
- Online and Single-Pass (duplex-based [BDPV12])
- Bitsliced in Software
  - Utilize 64-bit words
  - Up to 5 instructions in parallel
  - Bit interleaving [BDPVV12] for 32-bit processors
- Flexible in hardware
  - Small area (2.5 kGE) to high speed (13.2 Gbps) [GWDE15]
- Balanced design
  - E.g., lightweight devices communicate to back-end server

ASCON – Benefits

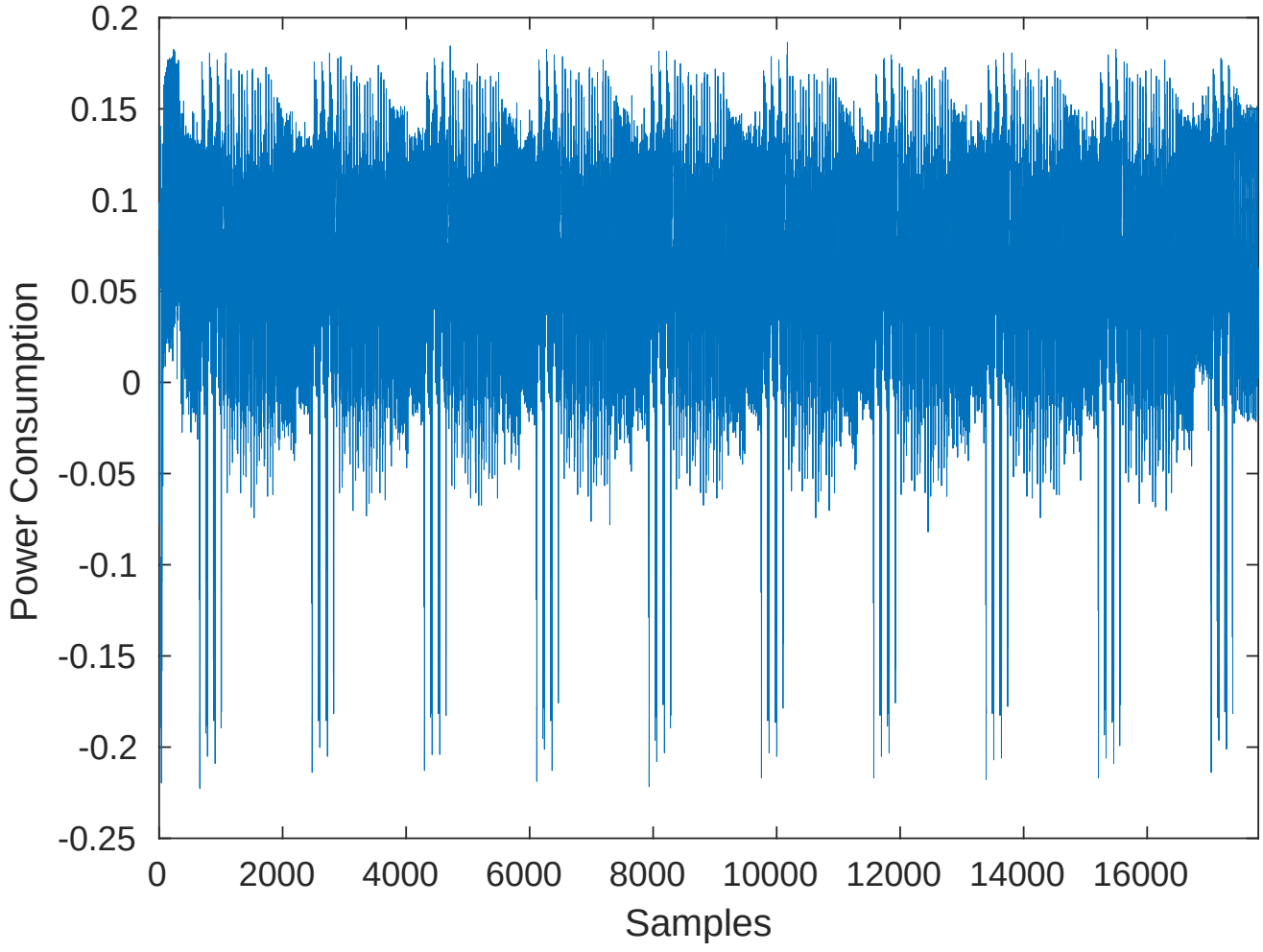
- Easy integration of side-channel countermeasures
  - No look-up tables
  - Low degree Sbox using KECCAK's χ [BDPV11] as core
  - Easy to mask, e.g., DOM implementations [GM18]

Protection Order	Pipelined		Parallel	
	GE	Mbit/s	GE	Mbit/s
1	10 855	108	28 887	2246
2	16 186	108	52 995	1896
3	21 586	110	81 209	1903
4	27 124	71	118 264	1786
5	32 757	95	161 870	1868
	...			
13	81 194	70	725 994	1833
14	87 749	71	828 183	1439
15	94 235	50	926 332	1480

Simple Power Analysis (SPA) [KJJ99]

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

Simple Power Analysis (SPA) [KJJ99]

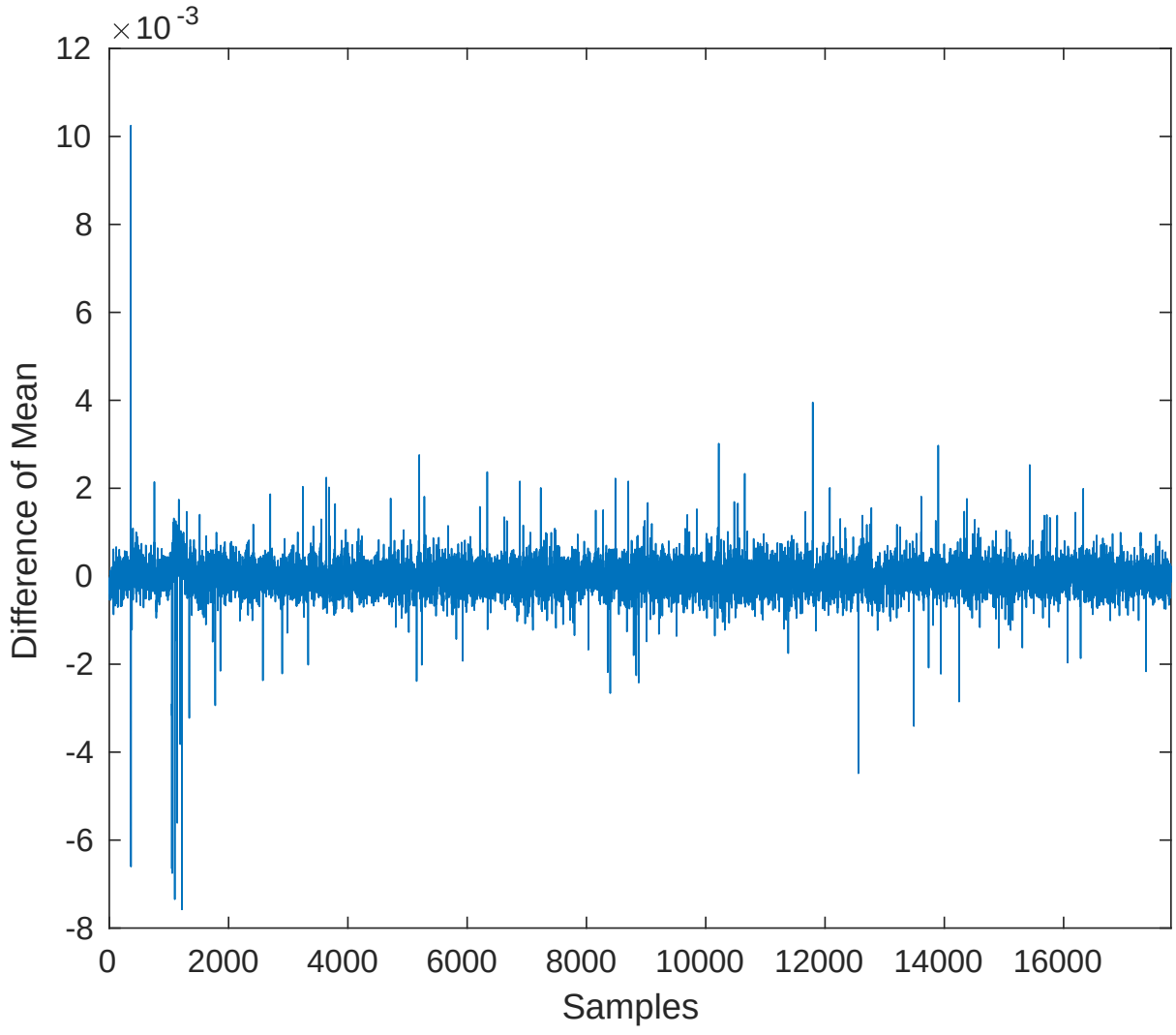


by Robert Primas

Differential Power Analysis (DPA) [KJJ99]

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

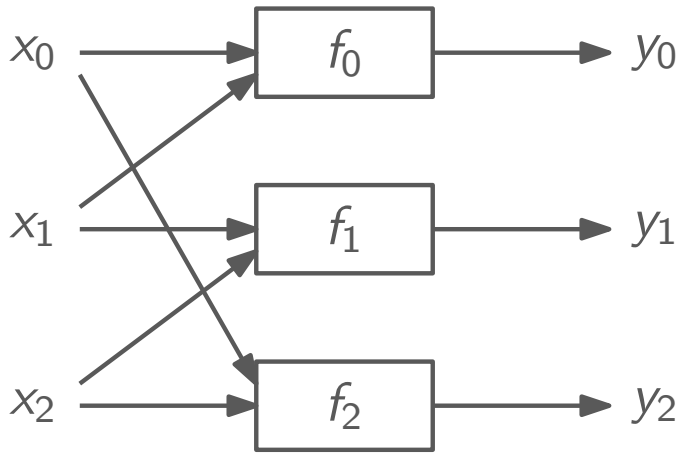
Differential Power Analysis (DPA) [KJJ99]



by Robert Primas

Masking and Threshold Implementations [NRR06]

Masking and Threshold Implementations [NRR06]

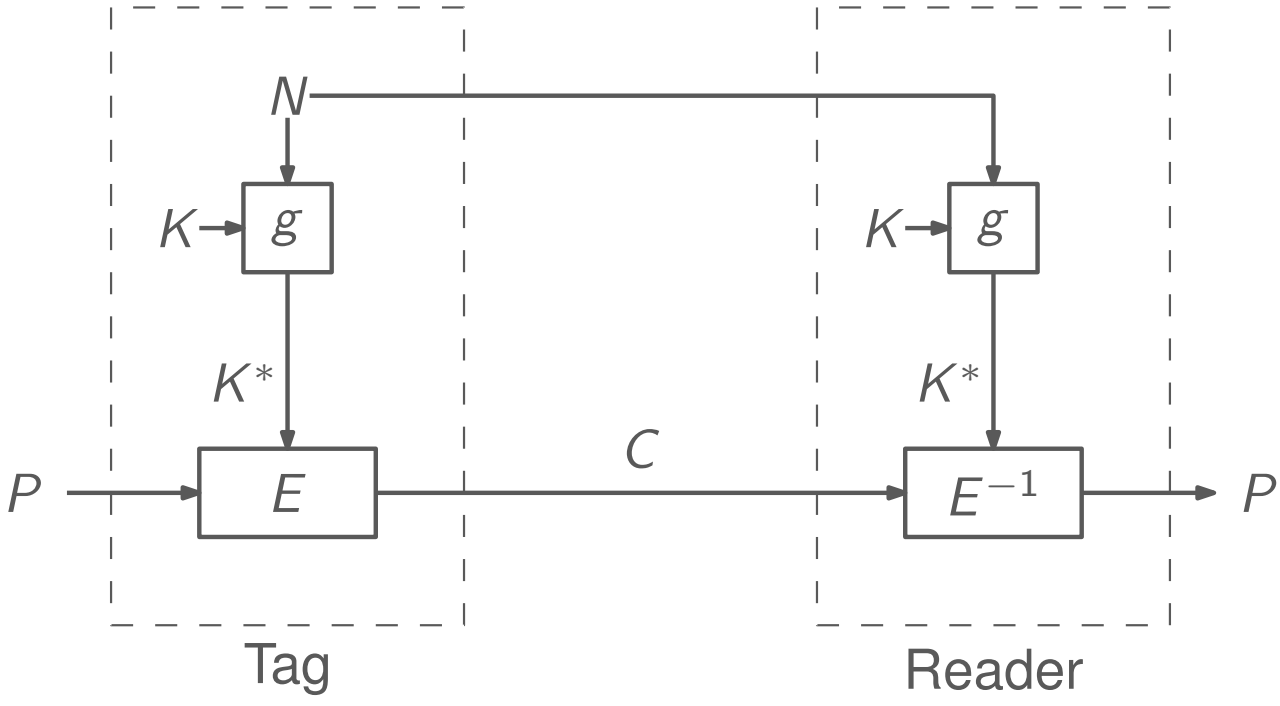


ISAP: Designed to Withstand Side-channel Attacks

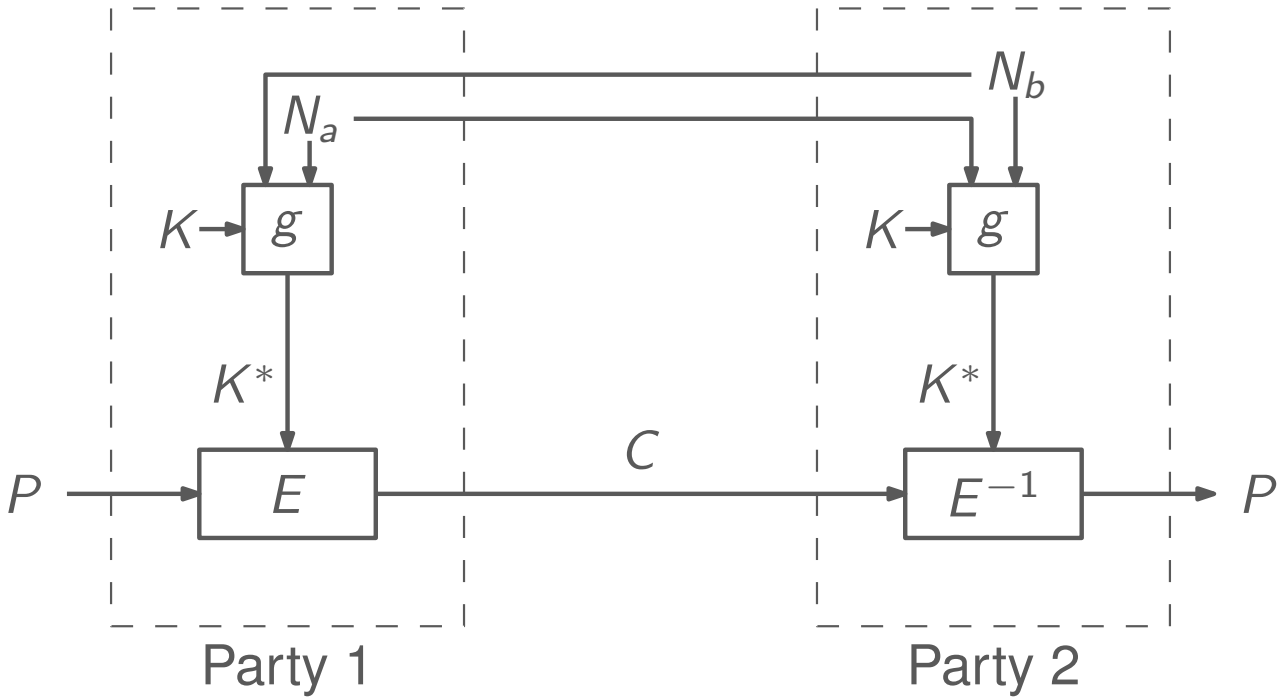
ISAP

- 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

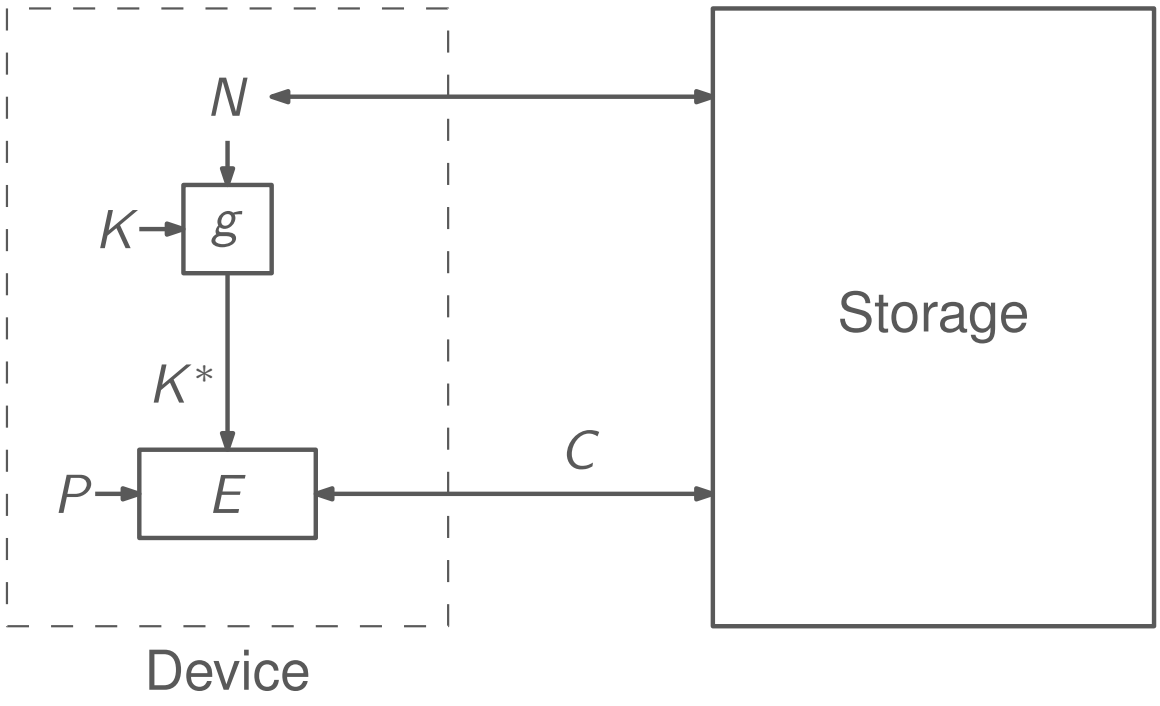
Fresh Re-keying [MSGR10]



Fresh Re-keying [MPRRS11]



What About Storage?



- Encryption still fine
- Decryption causes problems

How to Protect Decryption?

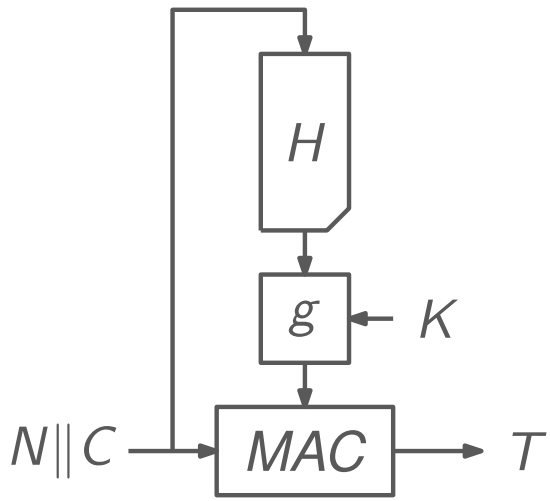
- Solely rely on implementation countermeasures
  - Makes re-keying for encryption kind of obsolete
- Limit to one decryption
  - Keep track of the nonce
  - Re-encrypt data
  - Time consuming
  - Damaging

Priciple of ISAP's Decryption

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

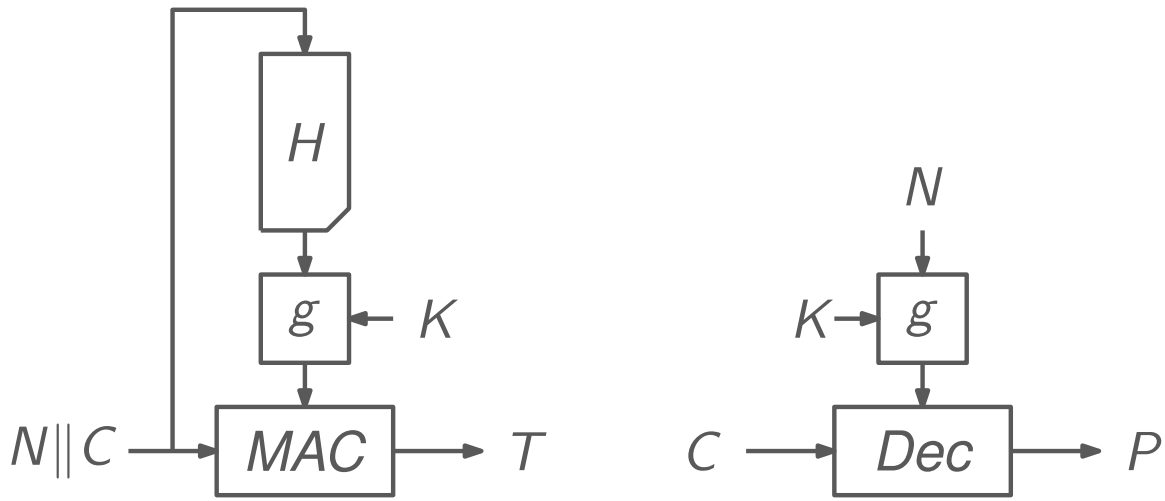
Priciple of ISAP's Decryption

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

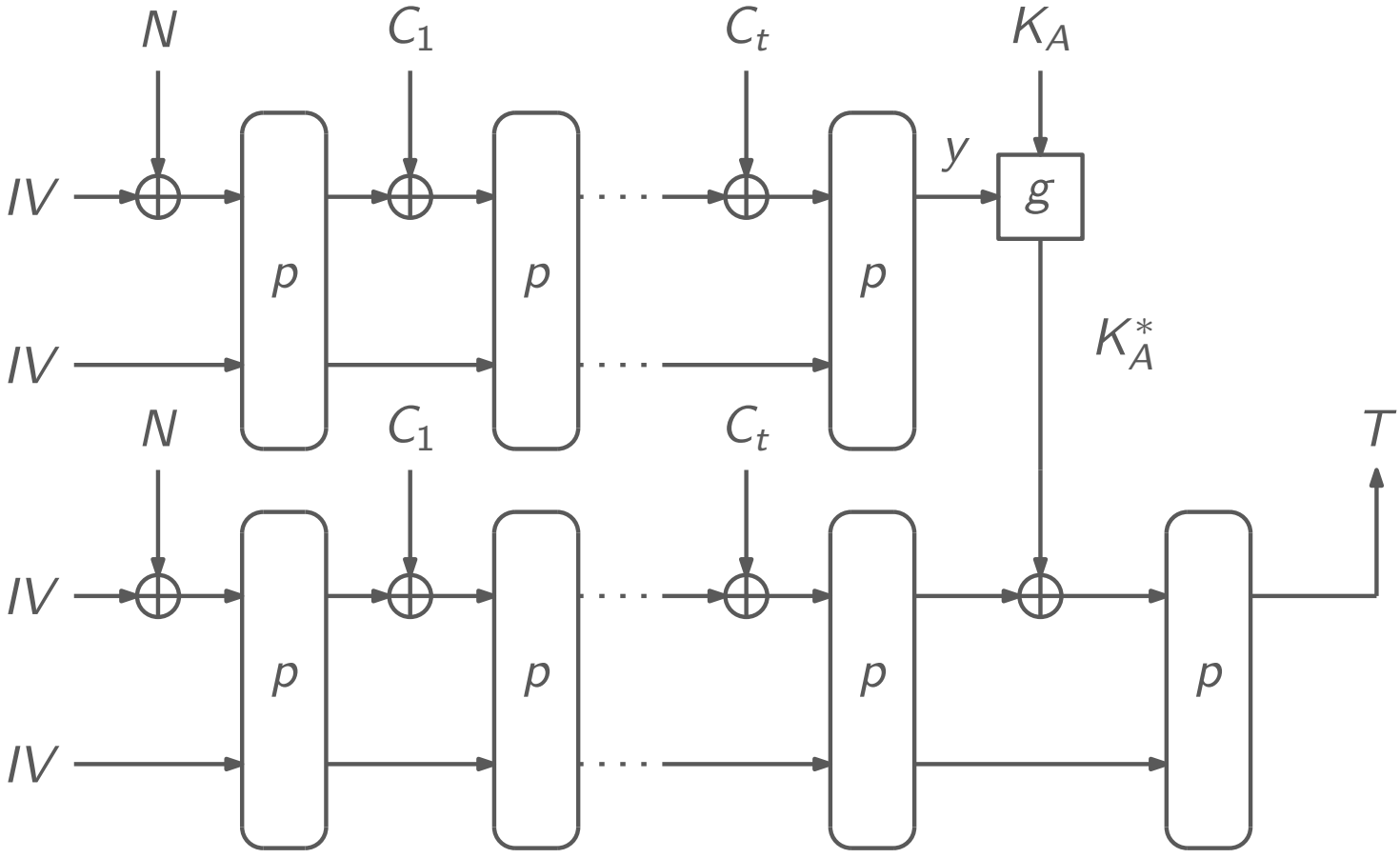


Priciple of ISAP's Decryption

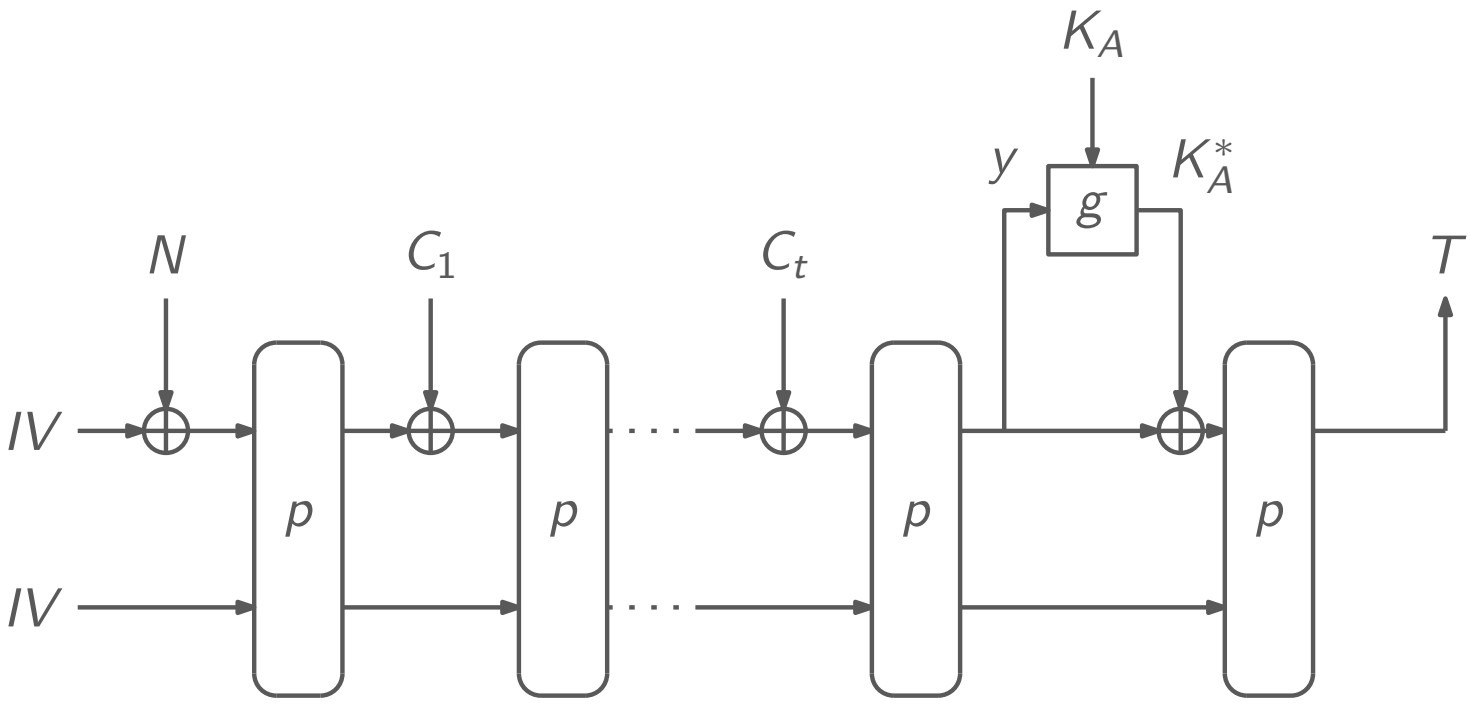
"Bind" the session key to the data that is decrypted



ISAP's Authentication/Verification

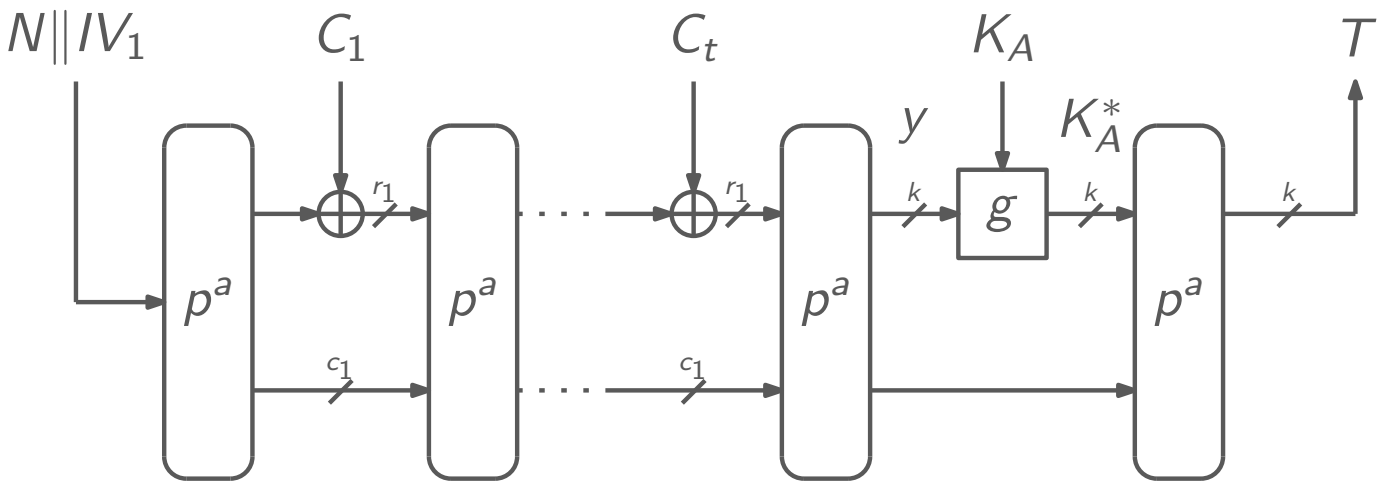


ISAP's Authentication/Verification



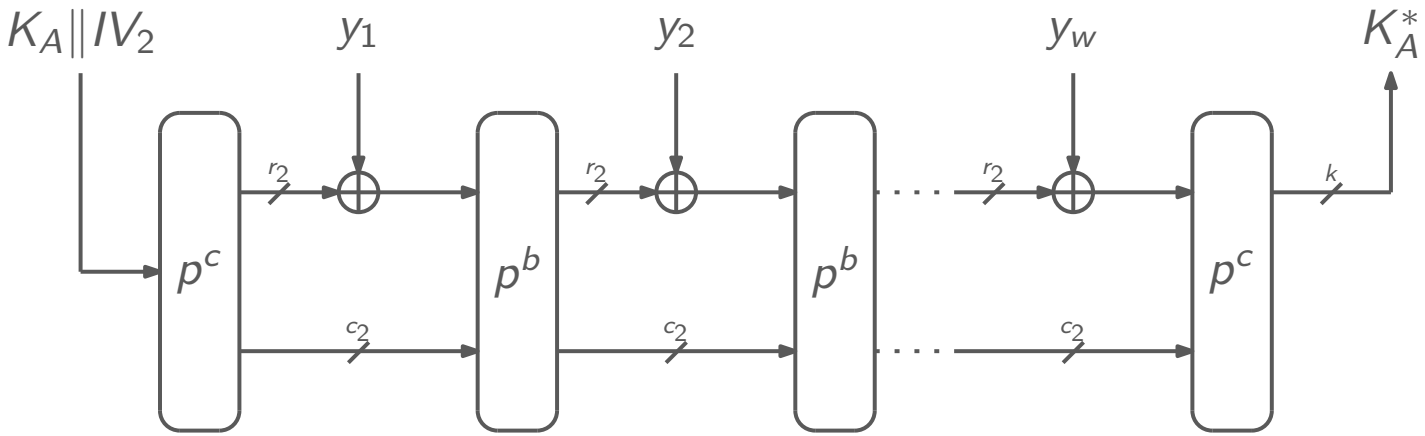
ISAP's Authentication/Verification

Use suffix MAC instead of hash-then-MAC

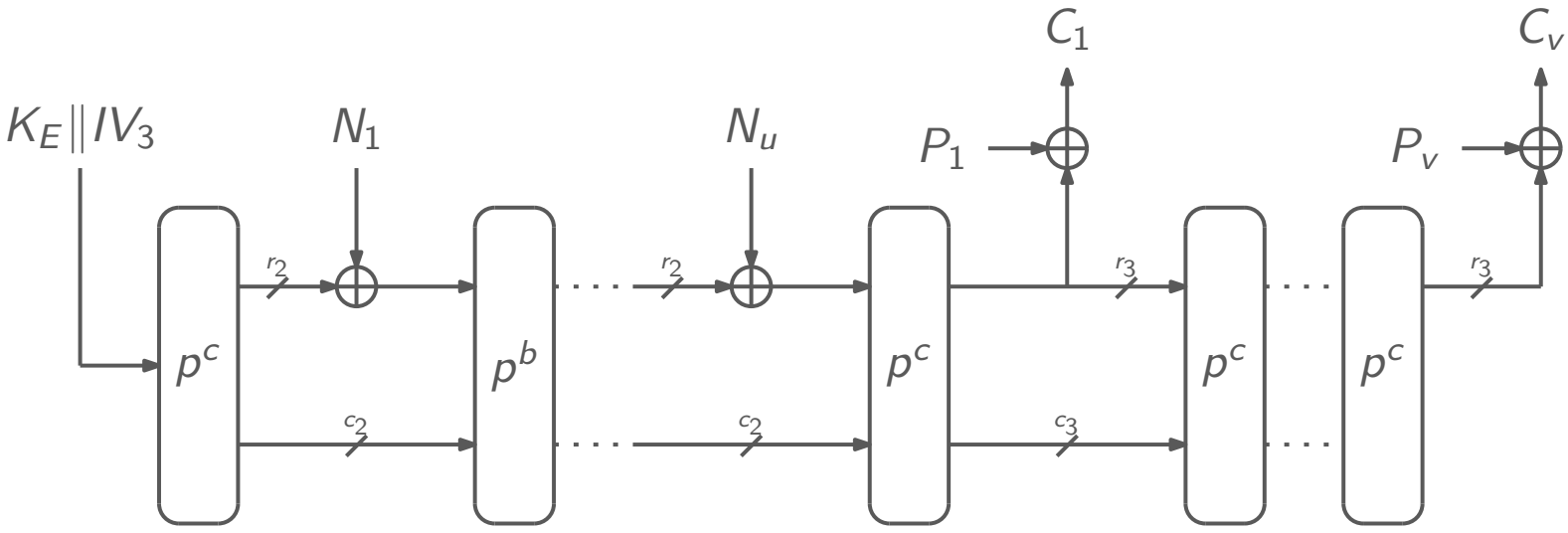


Absorbing the Key

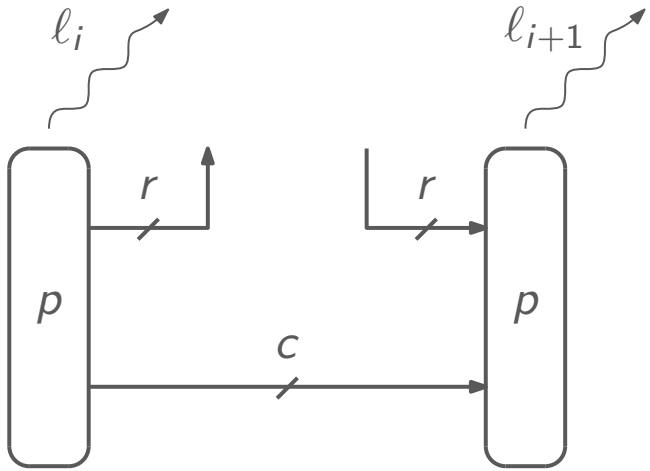
Idea: Reduce rate to a minimum [TS14]
Related to the classical GGM construction [GGM86]



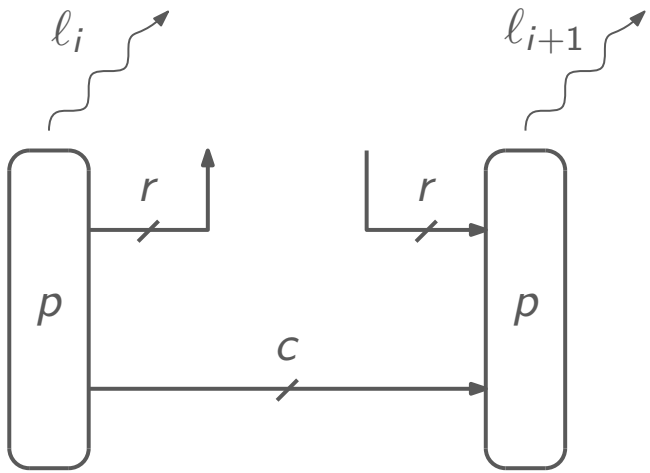
ISAP's En-/Decryption

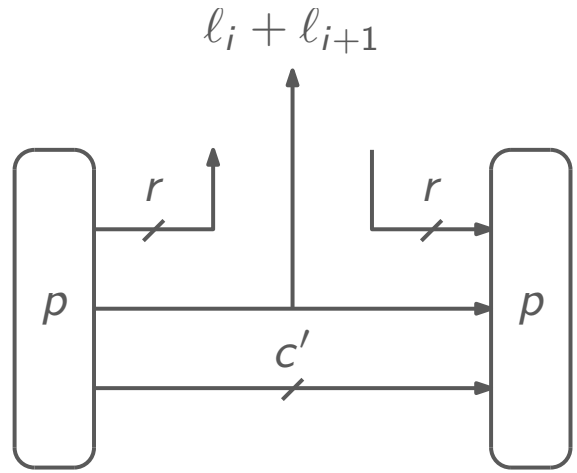


Sponges and Side-channel Leakage



Sponges and Side-channel Leakage





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

Properties

- AE scheme following requirements of CAESAR call
- Provides protection against DPA
  - Encryption
  - Decryption
- Two-pass
- Cannot turn protection off

Thank you

Bibliography I

[BDPV11] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche
The Keccak SHA-3 submission (Version 3.0)
http://keccak.noekeon.org/Keccak-submission-3.pdf, 2011

[BDPV12] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche
Duplexing the Sponge: Single-Pass Authenticated Encryption and Other Applications
Selected Areas in Cryptography, SAC 2011

[BDPVV12] G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, and R. Van Keer
Keccak implementation overview
https://keccak.team/files/Keccak-implementation-3.2.pdf, 2012

Bibliography II

[DEMMU17] C. Dobraunig, M. Eichlseder, S. Mangard, F. Mendel, and T. Unterluggauer
ISAP – Towards Side-Channel Secure Authenticated Encryption
IACR Transactions on Symmetric Cryptology 2017:1, 2017

[DEMS14] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer
Ascon
Submission to the CAESAR competition: `http://competitions.cr.yp.to`, 2014

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

[GM18] H. Groß and S. Mangard
A unified masking approach
J. Cryptographic Engineering 8:2, 2018

Bibliography III

[GWDE15] H. Groß, E. Wenger, C. Dobraunig, and C. Ehrenhöfer
Suit up! - Made-to-Measure Hardware Implementations of ASCON
DSD 2015

[KJJ99] P. C. Kocher, J. Jaffe, and B. Jun
Differential Power Analysis
CRYPTO '99

[MPRRS11] 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
Smart Card Research and Advanced Applications, CARDIS 2011

Bibliography IV

[MSGR10] 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

[NRR06] S. Nikova, C. Rechberger, and V. Rijmen
Threshold Implementations Against Side-Channel Attacks and Glitches
Information and Communications Security, ICICS 2006

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