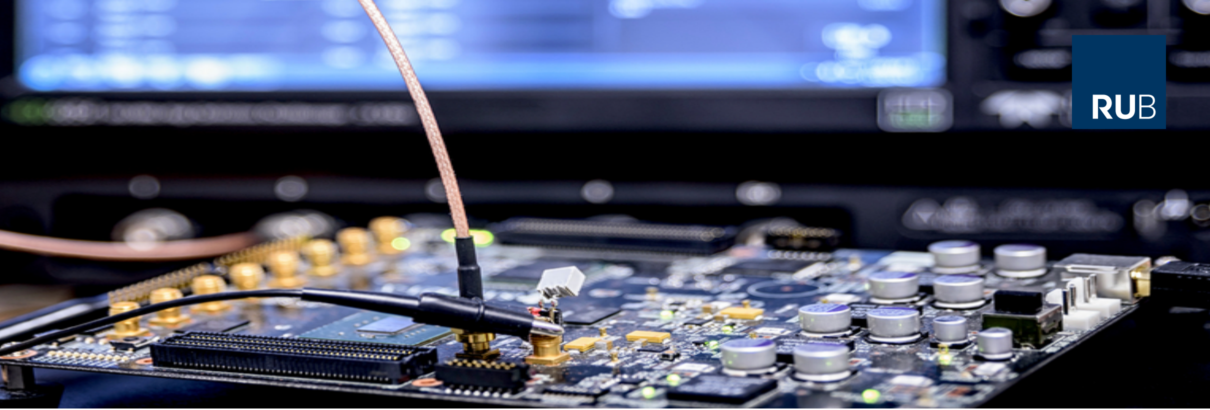


RUHR-UNIVERSITÄT BOCHUM

A Tale of Snakes and Horses: Amplifying Correlation Power Analysis on Quadratic Maps

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Conference on Cryptographic Hardware and Embedded Systems 2024

Anna Guinet[1] **Georg Land[1]** **Gabriel Ioan Bucur[2]** **Tim Güneysu[1]**

[1]Chair of Security Engineering, Faculty of Computer Science, Ruhr-University Bochum, Germany
[2]Institute for Computing and Information Sciences, Radboud University, The Netherlands

September 6, 2024

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Contents

Introduction

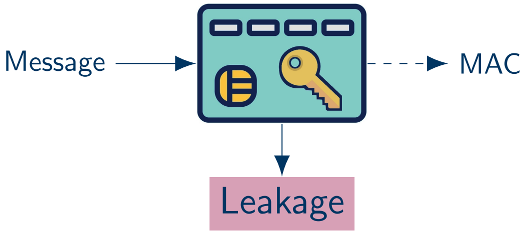
Correlation Power Analysis

Permutation-based Algorithms with a Quadratic S-box

Combined CPA or *Snake* Attack

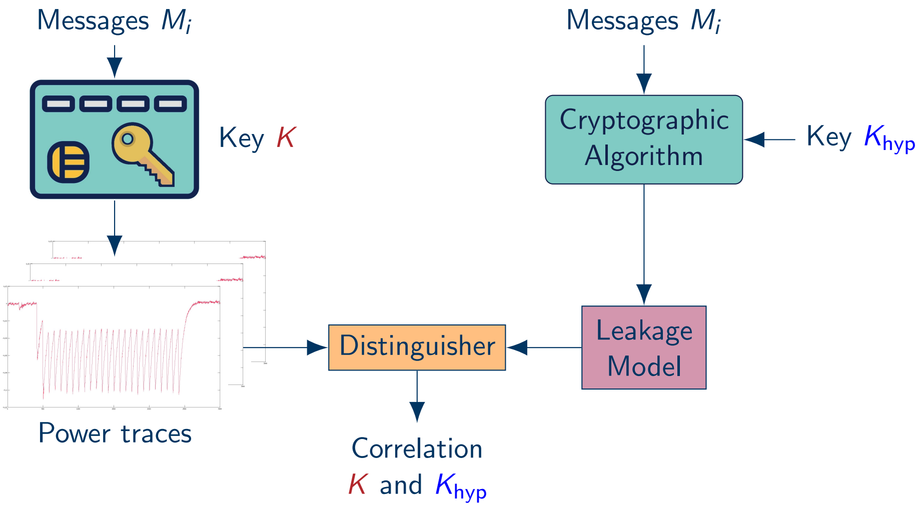
Practical Evaluation

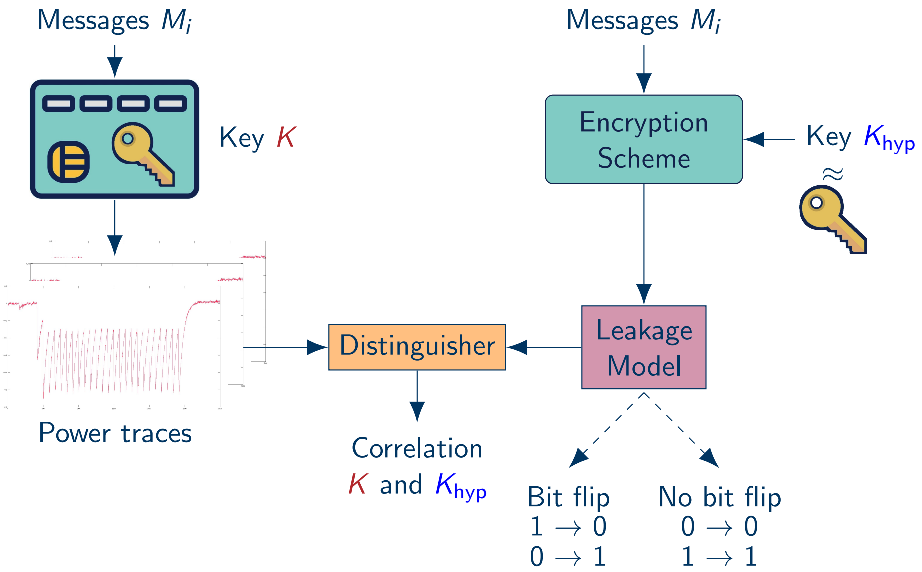
Correlation Power Analysis - An Overview



Recover secret data or key 

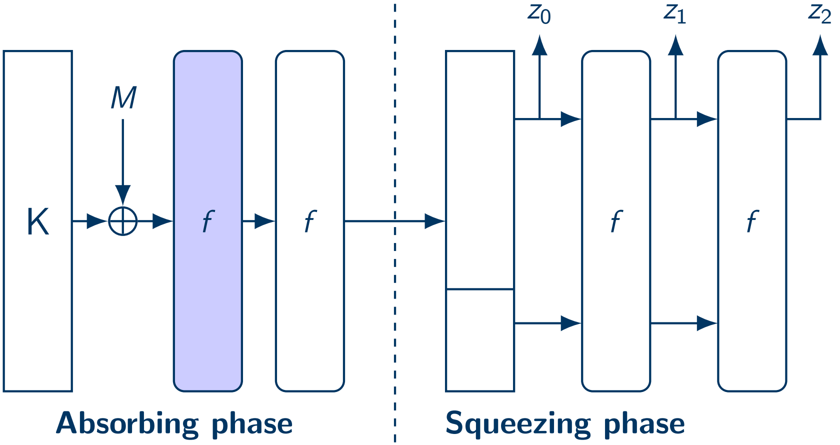
- Power consumption varies according to activity of device components
- **Correlation Power Analysis (CPA)**: statistical analysis of power consumption measurements (traces)

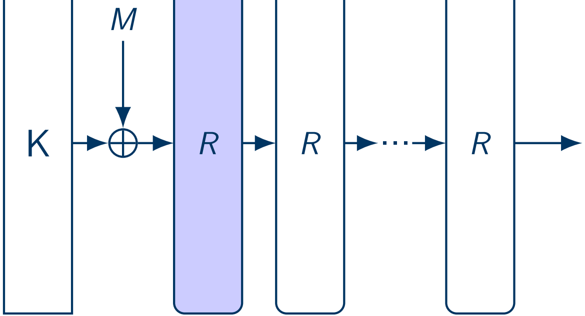

Messages M_i
Key K
Power traces
Messages M_i
Cryptographic Algorithm
Key K_{hyp}
Leakage Model
Distinguisher
Correlation
K and K_{hyp}



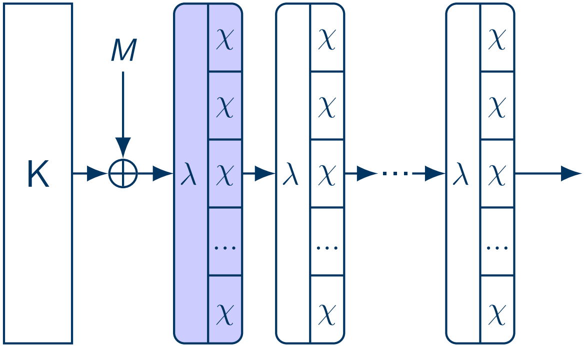
Messages M_i
Key K
Power traces
Messages M_i
Encryption Scheme
Key K_{hyp}
≈
Distinguisher
Leakage Model
Correlation
K and K_{hyp}
Bit flip
$1 \rightarrow 0$
$0 \rightarrow 1$
No bit flip
$0 \rightarrow 0$
$1 \rightarrow 1$

Full State Keyed Sponge-based MAC



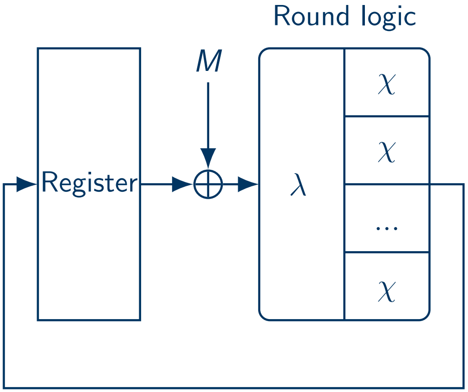


- A permutation f consists of several rounds R

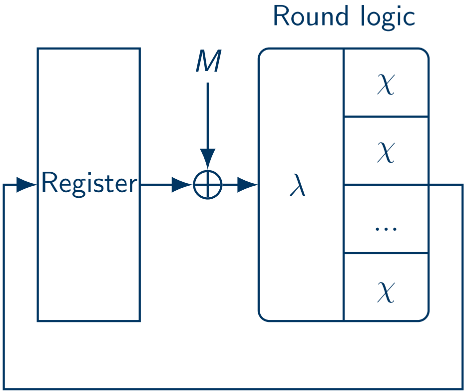


- A round R consists of a linear layer λ and a non-linear one
- **Non-linear layer** consists of χ mappings in parallel (S-boxes)

Round-based Hardware Architecture

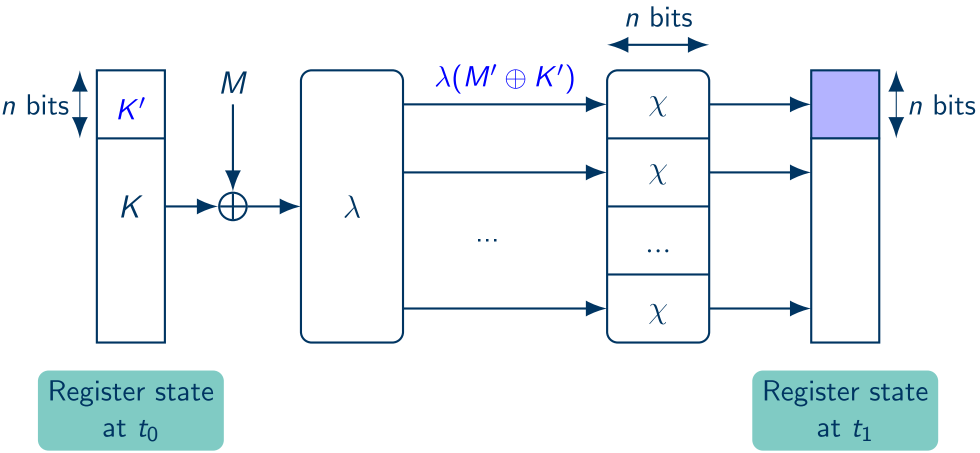


Round-based Hardware Architecture

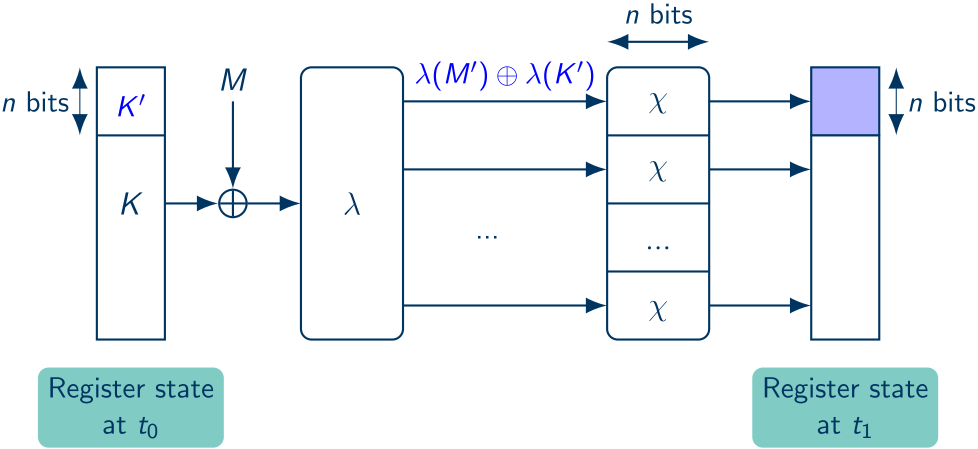


- **Leakage model**:
  - No power consumption from round logic
  - Exploit leakage from register
  - Quantifying noise from somewhere in the device

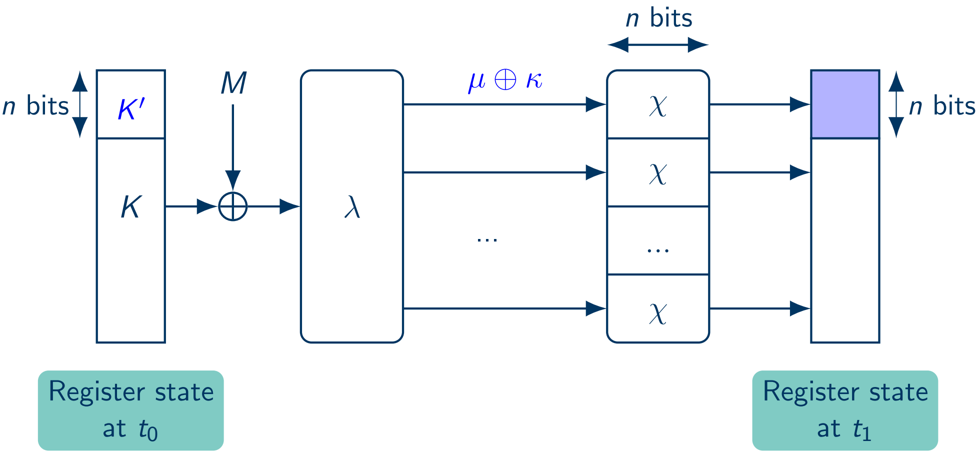
First Round of First Permutation



First Round of First Permutation



First Round of First Permutation



Leakage Model

- Activity of a storage cell: $d_i(K', \kappa, \mu) \in \mathbb{F}_2$ with $i \in \mathbb{Z}/n\mathbb{Z}$

Bit flip	No bit flip
$1 \to 0$	$0 \to 0$
$0 \to 1$	$1 \to 1$
$d_i(K', \kappa, \mu) = 1$	$d_i(K', \kappa, \mu) = 0$

Leakage Model

- Activity of a storage cell: $d_i(K', \kappa, \mu) \in \mathbb{F}_2$ with $i \in \mathbb{Z}/n\mathbb{Z}$

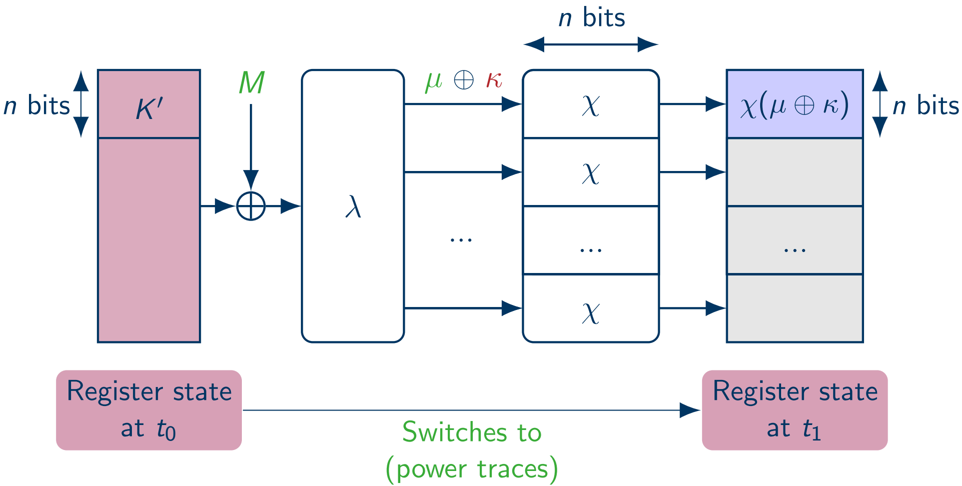
Bit flip	No bit flip
$1 \rightarrow 0$	$0 \rightarrow 0$
$0 \rightarrow 1$	$1 \rightarrow 1$
$d_i(K', \kappa, \mu) = 1$	$d_i(K', \kappa, \mu) = 0$

- Activity of all register bits contributes to **power consumption**:

$$\boxed{P(K', \kappa, \mu) = \sum_i (-1)^{d_i(K', \kappa, \mu)}}$$

Bit flip	No bit flip
$P(K', \kappa, \mu) = -1$	$P(K', \kappa, \mu) = +1$

First n Bits of Register



For the first n bits: $\mu \oplus \kappa = \lambda(M') \oplus \lambda(K') = \lambda(M' \oplus K')$

Refine Leakage Model

- Activity of register after a round for the first storage cell:

$$d_0(K_0', \kappa, \mu) = K_0' \oplus \underbrace{\kappa_0 \oplus \mu_0 \oplus (\kappa_1 \oplus \mu_1 \oplus 1)(\kappa_2 \oplus \mu_2)}_{\textit{first bit of } \chi(\mu \oplus \kappa)}$$

Refine Leakage Model

- Activity of register after a round for the first storage cell:

$$d_0(K_0', \kappa, \mu) = K_0' \oplus \underbrace{\kappa_0 \oplus \mu_0 \oplus (\kappa_1 \oplus \mu_1 \oplus 1)(\kappa_2 \oplus \mu_2)}_{\textit{first bit of } \chi(\mu \oplus \kappa)}$$

- Power consumption $P = S + R$ of a trace

Signal part

$$S(\mu) = \underbrace{\sum_{i=0}^{n-1}}_{n \text{ bits}} (-1)^{d_i\,(K_i, \kappa, \mu)}$$

Noise part

$$R \sim \mathcal{N}(0, \sigma^2)$$

$$\sigma = 1$$

Refine Leakage Model

- Activity of register after a round for the first storage cell:

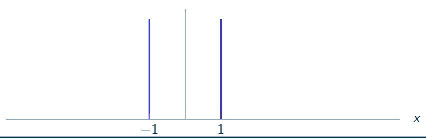
$$d_0(K'_0, \kappa, \mu) = K'_0 \oplus \underbrace{\kappa_0 \oplus \mu_0 \oplus (\kappa_1 \oplus \mu_1 \oplus 1)(\kappa_2 \oplus \mu_2)}_{\textit{first bit of } \chi(\mu \oplus \kappa)}$$

- Power consumption $\boxed{P = S + R}$ of a trace

Signal part

$$S(\mu) = \sum_{i=0}^{n-1} (-1)^{d_i\,(K_i,\kappa,\mu)}$$

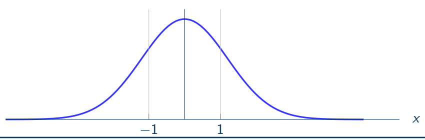
$n = 1$ bit



Noise part

$$R \sim \mathcal{N}(0, \sigma^2)$$

$$\sigma = 1$$



Refine Leakage Model

- Activity of register after a round for the first storage cell:

$$d_0(K'_0, \kappa, \mu) = K'_0 \oplus \underbrace{\kappa_0 \oplus \mu_0 \oplus (\kappa_1 \oplus \mu_1 \oplus 1)(\kappa_2 \oplus \mu_2)}_{\textit{first bit of } \chi(\mu \oplus \kappa)}$$

- Power consumption $P = S + R$ of a trace

Signal part

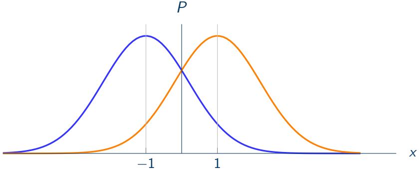
$$S(\mu) = \sum_{i=0}^{n-1} (-1)^{d_i\,(K_i, \kappa, \mu)}$$

$n = 1$ bit

Noise part

$$R \sim \mathcal{N}(0, \sigma^2)$$

$$\sigma = 1$$



Partitioning Power Traces

Messages	Power consumption	Partitions
$\mu_1 = \lambda(M_1)$	$P_1 = S(\mu_1) + R_1$	
$\mu_2 = \lambda(M_2)$	$P_2 = S(\mu_2) + R_2$	
$\mu_3 = \lambda(M_3)$	$P_3 = S(\mu_3) + R_3$	
$\mu_4 = \lambda(M_4)$	$P_4 = S(\mu_4) + R_4$	
$\mu_5 = \lambda(M_5)$	$P_5 = S(\mu_5) + R_5$	Bit flip
$\mu_6 = \lambda(M_6)$	$P_6 = S(\mu_6) + R_6$	
$\mu_7 = \lambda(M_7)$	$P_7 = S(\mu_7) + R_7$	
$\mu_8 = \lambda(M_8)$	$P_8 = S(\mu_8) + R_8$	
$\mu_9 = \lambda(M_9)$	$P_9 = S(\mu_9) + R_9$	No bit flip
$\mu_{10} = \lambda(M_{10})$	$P_{10} = S(\mu_{10}) + R_{10}$	
$\mu_{11} = \lambda(M_{11})$	$P_{11} = S(\mu_{11}) + R_{11}$	
$\mu_{12} = \lambda(M_{12})$	$P_{12} = S(\mu_{12}) + R_{12}$	
$\dots$	$\dots$	
M_{Many}	P_{Many}	

Partitioning Power Traces

RUB

Messages	Power consumption	Partitions
$\mu_1 = \lambda(M_1)$	$P_1 = S(\mu_1) + R_1$	$\mu = 000$
$\mu_2 = \lambda(M_2)$	$P_2 = S(\mu_2) + R_2$	$\mu = 001$
$\mu_3 = \lambda(M_3)$	$P_3 = S(\mu_3) + R_3$	$\mu = 010$
$\mu_4 = \lambda(M_4)$	$P_4 = S(\mu_4) + R_4$	$\mu = 011$
$\mu_5 = \lambda(M_5)$	$P_5 = S(\mu_5) + R_5$	$\mu = 100$
$\mu_6 = \lambda(M_6)$	$P_6 = S(\mu_6) + R_6$	$\mu = 101$
$\mu_7 = \lambda(M_7)$	$P_7 = S(\mu_7) + R_7$	$\mu = 110$
$\mu_8 = \lambda(M_8)$	$P_8 = S(\mu_8) + R_8$	$\mu = 111$
$\mu_9 = \lambda(M_9)$	$P_9 = S(\mu_9) + R_9$	
$\mu_{10} = \lambda(M_{10})$	$P_{10} = S(\mu_{10}) + R_{10}$	
$\mu_{11} = \lambda(M_{11})$	$P_{11} = S(\mu_{11}) + R_{11}$	
$\mu_{12} = \lambda(M_{12})$	$P_{12} = S(\mu_{12}) + R_{12}$	
$\dots$	$\dots$	
M_{Many}	P_{Many}	

Partitioning Power Traces

RUB

Messages

$\mu_1 = \lambda(M_1)$
$\mu_2 = \lambda(M_2)$
$\mu_3 = \lambda(M_3)$
$\mu_4 = \lambda(M_4)$
$\mu_5 = \lambda(M_5)$
$\mu_6 = \lambda(M_6)$
$\mu_7 = \lambda(M_7)$
$\mu_8 = \lambda(M_8)$
$\mu_9 = \lambda(M_9)$
$\mu_{10} = \lambda(M_{10})$
$\mu_{11} = \lambda(M_{11})$
$\mu_{12} = \lambda(M_{12})$
$\dots$
M_{Many}

Power consumption

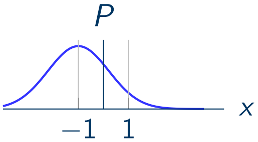
$P_1 = S(\mu_1) + R_1$
$P_2 = S(\mu_2) + R_2$
$P_3 = S(\mu_3) + R_3$
$P_4 = S(\mu_4) + R_4$
$P_5 = S(\mu_5) + R_5$
$P_6 = S(\mu_6) + R_6$
$P_7 = S(\mu_7) + R_7$
$P_8 = S(\mu_8) + R_8$
$P_9 = S(\mu_9) + R_9$
$P_{10} = S(\mu_{10}) + R_{10}$
$P_{11} = S(\mu_{11}) + R_{11}$
$P_{12} = S(\mu_{12}) + R_{12}$
$\dots$
P_{Many}

Partitions

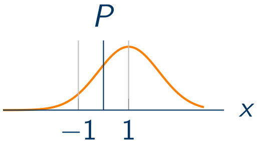
$\mu = 000$
$\mu = 001$
$\mu = 010$
$\mu = 011$
$\mu = 100$
$\mu = 101$
$\mu = 110$
$\mu = 111$

$\rightarrow$ Average of each partition

Few traces



Bit flip



No bit flip

Partitioning Power Traces

Messages

$$\mu_1 = \lambda(M_1)$$
$$\mu_2 = \lambda(M_2)$$
$$\mu_3 = \lambda(M_3)$$
$$\mu_4 = \lambda(M_4)$$
$$\mu_5 = \lambda(M_5)$$
$$\mu_6 = \lambda(M_6)$$
$$\mu_7 = \lambda(M_7)$$
$$\mu_8 = \lambda(M_8)$$
$$\mu_9 = \lambda(M_9)$$
$$\mu_{10} = \lambda(M_{10})$$
$$\mu_{11} = \lambda(M_{11})$$
$$\mu_{12} = \lambda(M_{12})$$
$$\dots$$
$$M_{\mathrm{Many}}$$

Power consumption

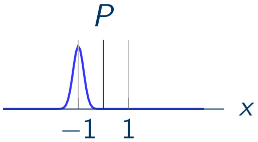
$$P_1 = S(\mu_1) + R_1$$
$$P_2 = S(\mu_2) + R_2$$
$$P_3 = S(\mu_3) + R_3$$
$$P_4 = S(\mu_4) + R_4$$
$$P_5 = S(\mu_5) + R_5$$
$$P_6 = S(\mu_6) + R_6$$
$$P_7 = S(\mu_7) + R_7$$
$$P_8 = S(\mu_8) + R_8$$
$$P_9 = S(\mu_9) + R_9$$
$$P_{10} = S(\mu_{10}) + R_{10}$$
$$P_{11} = S(\mu_{11}) + R_{11}$$
$$P_{12} = S(\mu_{12}) + R_{12}$$
$$\dots$$
$$P_{\mathrm{Many}}$$

Partitions

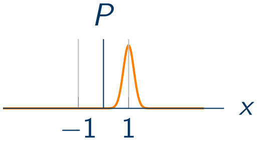
$$\mu = 000$$
$$\mu = 001$$
$$\mu = 010$$
$$\mu = 011$$
$$\mu = 100$$
$$\mu = 101$$
$$\mu = 110$$
$$\mu = 111$$

$\rightarrow$ Average of each partition

Many traces



Bit flip



No bit flip

Correlation

- Activity $d_0(K'_0, \kappa, \mu) = K'_0 \oplus \kappa_0 \oplus \mu_0 \oplus (\kappa_1 \oplus \mu_1 \oplus 1)(\kappa_2 \oplus \mu_2)$

Correlation

- Activity $d_0(K'_0, \kappa, \mu) = K'_0 \oplus \kappa_0 \oplus \mu_0 \oplus (\kappa_1 \oplus \mu_1 \oplus 1)(\kappa_2 \oplus \mu_2)$
- Signal power consumption values S_{ref} for all (κ, μ) possibilities for K'_0

$\mu_0\mu_1\mu_2$	$K'_0 \oplus \kappa_0\ \kappa_1\kappa_2$							
	000	001	010	011	100	101	110	111
000	$+1$	-1	$+1$	$+1$	-1	$+1$	-1	-1
001	-1	$+1$	$+1$	$+1$	$+1$	-1	-1	-1
010	$+1$	$+1$	$+1$	-1	-1	-1	-1	$+1$
011	$+1$	$+1$	-1	$+1$	-1	-1	$+1$	-1
100	-1	$+1$	-1	-1	$+1$	-1	$+1$	$+1$
101	$+1$	-1	-1	-1	-1	$+1$	$+1$	$+1$
110	-1	-1	-1	$+1$	$+1$	$+1$	$+1$	-1
111	-1	-1	$+1$	-1	$+1$	$+1$	-1	$+1$

Correlation

- Activity $d_0(K_0', \kappa, \mu) = K_0' \oplus \kappa_0 \oplus \mu_0 \oplus (\kappa_1 \oplus \mu_1 \oplus 1)(\kappa_2 \oplus \mu_2)$
- Signal power consumption values S_{ref} for all (κ, μ) possibilities for K_0'

$\mu_0\mu_1\mu_2$	$K_0' \oplus \kappa_0\ \kappa_1\kappa_2$							
	000	001	010	011	100	101	110	111
000	$+1$	-1	$+1$	$+1$	-1	$+1$	-1	-1
001	-1	$+1$	$+1$	$+1$	$+1$	-1	-1	-1
010	$+1$	$+1$	$+1$	-1	-1	-1	-1	$+1$
011	$+1$	$+1$	-1	$+1$	-1	-1	$+1$	-1
100	-1	$+1$	-1	-1	$+1$	-1	$+1$	$+1$
101	$+1$	-1	-1	-1	-1	$+1$	$+1$	$+1$
110	-1	-1	-1	$+1$	$+1$	$+1$	$+1$	-1
111	-1	-1	$+1$	-1	$+1$	$+1$	-1	$+1$

- Pearson correlation coefficient $\rho(P, S_{\text{ref}})$: Highest correlation result $max(\rho(P, S_{\text{ref}}))$

Correlation

- Activity $d_0(K'_0, \kappa, \mu) = K'_0 \oplus \kappa_0 \oplus \mu_0 \oplus (\kappa_1 \oplus \mu_1 \oplus 1)(\kappa_2 \oplus \mu_2)$
- Signal power consumption values S_{ref} for all (κ, μ) possibilities for K'_0

$\mu_0\mu_1\mu_2$	$K'_0 \oplus \kappa_0\ \kappa_1\kappa_2$							
	000	001	010	011	100	101	110	111
000	$+1$	-1	$+1$	$+1$	-1	$+1$	-1	-1
001	-1	$+1$	$+1$	$+1$	$+1$	-1	-1	-1
010	$+1$	$+1$	$+1$	-1	-1	-1	-1	$+1$
011	$+1$	$+1$	-1	$+1$	-1	-1	$+1$	-1
100	-1	$+1$	-1	-1	$+1$	-1	$+1$	$+1$
101	$+1$	-1	-1	-1	-1	$+1$	$+1$	$+1$
110	-1	-1	-1	$+1$	$+1$	$+1$	$+1$	-1
111	-1	-1	$+1$	-1	$+1$	$+1$	-1	$+1$

- Pearson correlation coefficient $\rho(P, S_{\mathrm{ref}})$: Highest correlation result $max(\rho(P, S_{\mathrm{ref}}))$

Correlation

- Activity $d_0(K_0', \kappa, \mu) = K_0' \oplus \kappa_0 \oplus \mu_0 \oplus (\kappa_1 \oplus \mu_1 \oplus 1)(\kappa_2 \oplus \mu_2)$
- Signal power consumption values S_{ref} for all (κ, μ) possibilities for K_0'

$\mu_0\mu_1\mu_2$	$* \kappa_1\kappa_2$							
	000	001	010	011	100	101	110	111
000	$+1$	-1	$+1$	$+1$	–	–	–	–
001	-1	$+1$	$+1$	$+1$	–	–	–	–
010	$+1$	$+1$	$+1$	-1	–	–	–	–
011	$+1$	$+1$	-1	$+1$	–	–	–	–
100	-1	$+1$	-1	-1	–	–	–	–
101	$+1$	-1	-1	-1	–	–	–	–
110	-1	-1	-1	$+1$	–	–	–	–
111	-1	-1	$+1$	-1	–	–	–	–

- Pearson correlation coefficient $\rho(P, S_{\text{ref}})$: $max(\rho(P, S_{\text{ref}})^2)$ or $max(|\rho(P, S_{\text{ref}})|)$

Correlation

- Activity $d_0(K_0', \kappa, \mu) = K_0' \oplus \kappa_0 \oplus \mu_0 \oplus (\kappa_1 \oplus \mu_1 \oplus 1)(\kappa_2 \oplus \mu_2)$
- Signal power consumption values S_{ref} for all (κ, μ) possibilities for K_0'

$\mu_0\mu_1\mu_2$	$* \kappa_1\kappa_2$ 000	001	010	011	100	101	110	111
000	$+1$	-1	$+1$	$+1$	–	–	–	–
001	-1	$+1$	$+1$	$+1$	–	–	–	–
010	$+1$	$+1$	$+1$	-1	–	–	–	–
011	$+1$	$+1$	-1	$+1$	–	–	–	–
100	-1	$+1$	-1	-1	–	–	–	–
101	$+1$	-1	-1	-1	–	–	–	–
110	-1	-1	-1	$+1$	–	–	–	–
111	-1	-1	$+1$	-1	–	–	–	–

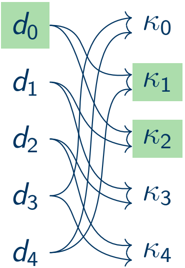
- Pearson correlation coefficient $\rho(P, S_{\text{ref}})$: $max(\rho(P, S_{\text{ref}})^2)$ or $max(|\rho(P, S_{\text{ref}})|)$

Combined CPA or Snake attack: Recovering κ

- Activity function $d_i(K', \kappa, \mu) = K'_i \oplus \kappa_i \oplus \mu_i \oplus (\kappa_{i+1} \oplus \mu_{i+1} \oplus 1)(\kappa_{i+2} \oplus \mu_{i+2})$

$n = 5$ bits

1 attack



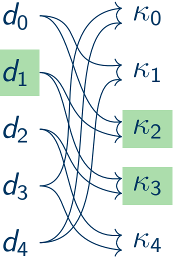
*00**	*01**	*10**	*11**
**00*	**01*	**10*	**11*
***00	***01	***10	***11
0***0	0***1	1***0	1***1
00***	01***	10***	11***

Combined CPA or Snake attack: Recovering κ

- Activity function $d_i(K', \kappa, \mu) = K'_i \oplus \kappa_i \oplus \mu_i \oplus (\kappa_{i+1} \oplus \mu_{i+1} \oplus 1)(\kappa_{i+2} \oplus \mu_{i+2})$

$n = 5$ bits

1 attack



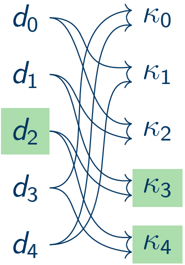
∗00∗∗	∗01∗∗	∗10∗∗	∗11∗∗
∗∗00∗	∗∗01∗	∗∗10∗	∗∗11∗
∗∗∗00	∗∗∗01	∗∗∗10	∗∗∗11
0∗∗∗0	0∗∗∗1	1∗∗∗0	1∗∗∗1
00∗∗∗	01∗∗∗	10∗∗∗	11∗∗∗

Combined CPA or Snake attack: Recovering κ

- Activity function $d_i(K', \kappa, \mu) = K'_i \oplus \kappa_i \oplus \mu_i \oplus (\kappa_{i+1} \oplus \mu_{i+1} \oplus 1)(\kappa_{i+2} \oplus \mu_{i+2})$

$n = 5$ bits

1 attack



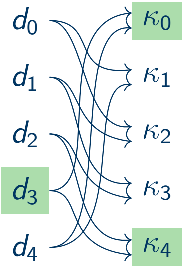
*00**	*01**	*10**	*11**
**00*	**01*	**10*	**11*
***00	***01	***10	***11
0***0	0***1	1***0	1***1
00***	01***	10***	11***

Combined CPA or Snake attack: Recovering κ

- Activity function $d_i(K', \kappa, \mu) = K'_i \oplus \kappa_i \oplus \mu_i \oplus (\kappa_{i+1} \oplus \mu_{i+1} \oplus 1)(\kappa_{i+2} \oplus \mu_{i+2})$

$n = 5$ bits

1 attack



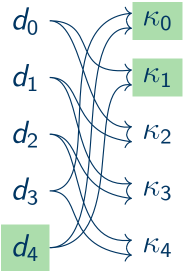
*00**	*01**	*10**	*11**
**00*	**01*	**10*	**11*
***00	***01	***10	***11
0***0	0***1	1***0	1***1
00***	01***	10***	11***

Combined CPA or Snake attack: Recovering κ

- Activity function $d_i(K', \kappa, \mu) = K'_i \oplus \kappa_i \oplus \mu_i \oplus (\kappa_{i+1} \oplus \mu_{i+1} \oplus 1)(\kappa_{i+2} \oplus \mu_{i+2})$

$n = 5$ bits

1 attack



*00**	*01**	*10**	*11**
**00*	**01*	**10*	**11*
***00	***01	***10	***11
0***0	0***1	1***0	1***1
00***	01***	10***	11***

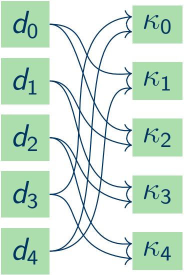
Combined CPA or Snake attack: Recovering κ

RUB

- Activity function $d_i(K', \kappa, \mu) = K'_i \oplus \kappa_i \oplus \mu_i \oplus (\kappa_{i+1} \oplus \mu_{i+1} \oplus 1)(\kappa_{i+2} \oplus \mu_{i+2})$

$n = 5$ bits

5 attacks



∗00∗∗	∗01∗∗	∗10∗∗	∗11∗∗
∗∗00∗	∗∗01∗	∗∗10∗	∗∗11∗
∗∗∗00	∗∗∗01	∗∗∗10	∗∗∗11
0∗∗∗0	0∗∗∗1	1∗∗∗0	1∗∗∗1
00∗∗∗	01∗∗∗	10∗∗∗	11∗∗∗

$\kappa = 00000$ $\quad$ $\kappa = 10101$

The *Snake* Walk

$$\sum \rho(P, S_{ref})^2 \quad \text{or} \quad \sum |\rho(P, S_{ref})|$$

Combined CPA or Snake Attack: Recovering K'

RUB

$n = 5$ bits

Correlation result for $i = 0$:	$K'_0 \oplus \kappa_0$	κ_1	κ_2	–	–
Correlation result for $i = 1$:	–	$K'_1 \oplus \kappa_1$	κ_2	κ_3	–
Correlation result for $i = 2$:	–	–	$K'_2 \oplus \kappa_2$	κ_3	κ_4
Correlation result for $i = 3$:	κ_0	–	–	$K'_3 \oplus \kappa_3$	κ_4
Correlation result for $i = 4$:	κ_0	κ_1	–	–	$K'_4 \oplus \kappa_4$

Combined CPA or Snake Attack: Recovering K'

$n = 5$ bits

Correlation result for $i = 0$:	$K'_0 \oplus \kappa_0$	$\boxed{\kappa_1}$	κ_2	—	—
Correlation result for $i = 1$:	—	$K'_1 \oplus \kappa_1$	κ_2	κ_3	—
Correlation result for $i = 2$:	—	—	$K'_2 \oplus \kappa_2$	κ_3	κ_4
Correlation result for $i = 3$:	κ_0	—	—	$K'_3 \oplus \kappa_3$	κ_4
Correlation result for $i = 4$:	κ_0	$\boxed{\kappa_1}$	—	—	$K'_4 \oplus \kappa_4$

Combined CPA or Snake Attack: Recovering K'

$n = 5$ bits

Correlation result for $i = 0$:	$K'_0 \oplus \kappa_0$	κ_1	κ_2	–	–
Correlation result for $i = 1$:	–	$K'_1 \oplus \kappa_1$	κ_2	κ_3	–
Correlation result for $i = 2$:	–	–	$K'_2 \oplus \kappa_2$	κ_3	κ_4
Correlation result for $i = 3$:	κ_0	–	–	$K'_3 \oplus \kappa_3$	κ_4
Correlation result for $i = 4$:	κ_0	κ_1	–	–	$K'_4 \oplus \kappa_4$

- For each bit i: $K'_i = \underbrace{\epsilon_i}_{\text{known}} \oplus \underbrace{\kappa_i}_{\text{guess}}$ with $\epsilon_i = 1$ if $\rho(P, S_{ref_i}) < 0$, otherwise $\epsilon_i = 0$.

Combined CPA or Snake Attack: Recovering K'

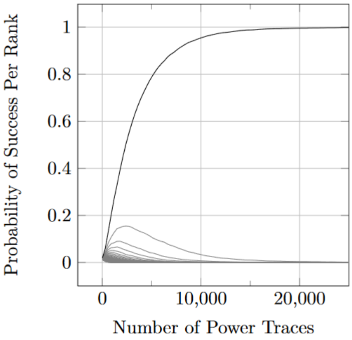
$n = 5$ bits

Correlation result for $i = 0$:	$K'_0 \oplus \kappa_0$	κ_1	κ_2	—	—
Correlation result for $i = 1$:	—	$K'_1 \oplus \kappa_1$	κ_2	κ_3	—
Correlation result for $i = 2$:	—	—	$K'_2 \oplus \kappa_2$	κ_3	κ_4
Correlation result for $i = 3$:	κ_0	—	—	$K'_3 \oplus \kappa_3$	κ_4
Correlation result for $i = 4$:	κ_0	κ_1	—	—	$K'_4 \oplus \kappa_4$

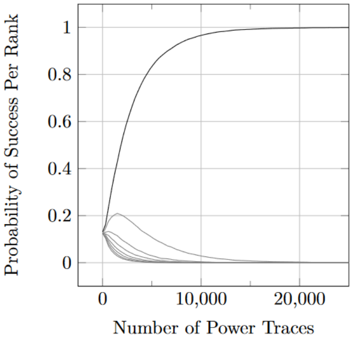
- For each bit i: $K'_i = \underbrace{\epsilon_i}_{\text{known}} \oplus \underbrace{\kappa_i}_{\text{guess}}$ with $\epsilon_i = 1$ if $\rho(P, S_{ref_i}) < 0$, otherwise $\epsilon_i = 0$.
- Reduce computational complexity from 2^{2n} intermediate results to $n2^2 + n$ ones.

Ranked Probabilities of Success for One χ_3 Sequence

$n = 3$ bits



(a) CPA, recovering (K', κ).

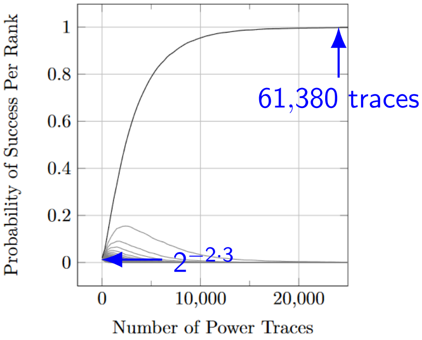


(b) Combined CPA or *Snake* attack recovering κ. Squared correlation coefficient.

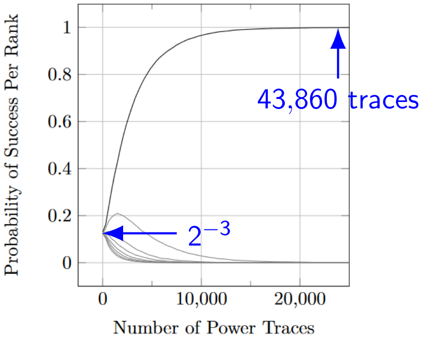
Figure: Ranked success probabilities targeting one χ_3 sequence (Xoodoo).

Ranked Probabilities of Success for One χ_3 Sequence

$n = 3$ bits



(a) CPA, recovering (K', κ).

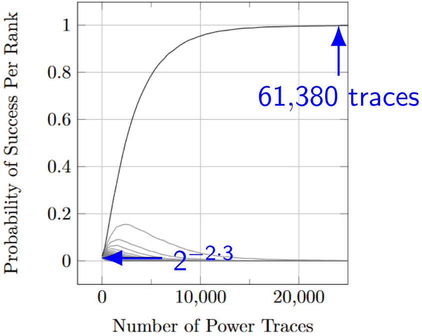


(b) Combined CPA or *Snake* attack recovering κ. Squared correlation coefficient.

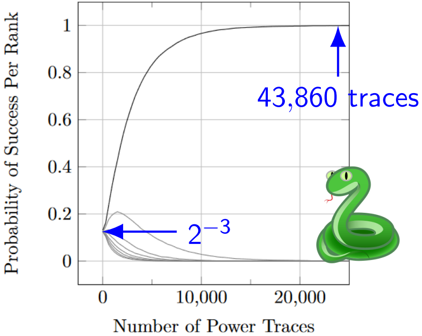
Figure: Ranked success probabilities targeting one χ_3 sequence (Xoodoo).

Ranked Probabilities of Success for One χ_3 Sequence

$n = 3$ bits



(a) CPA, recovering (K', κ).

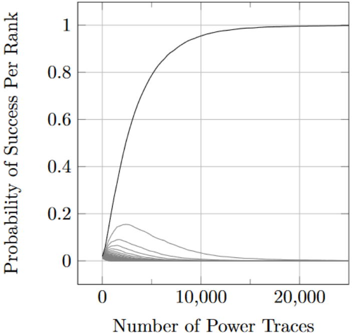


(b) Combined CPA or *Snake* attack recovering κ. Squared correlation coefficient.

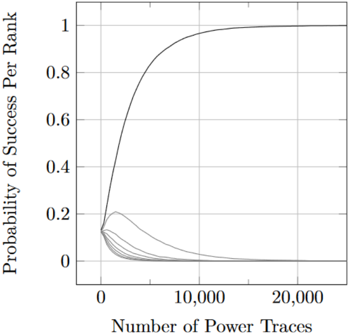
Figure: Ranked success probabilities targeting one χ_3 sequence (Xoodoo).

Ranked Probabilities of Success for One χ_3 Sequence

$n = 3$ bits



(a) CPA, recovering (K', κ).



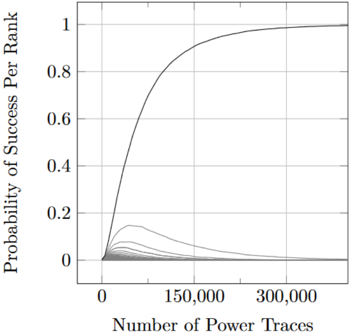
(b) Combined CPA or *Snake* attack recovering κ. Squared correlation coefficient.

Figure: Ranked success probabilities targeting one χ_3 sequence (Xoodoo).

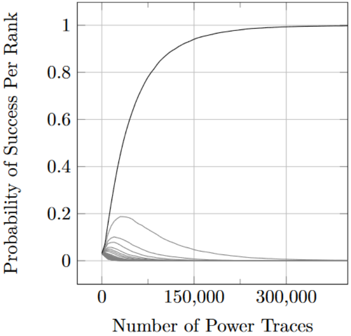
Ranked Probabilities of Success for One χ_5 Sequence

$n = 5$ bits

RUB



(a) CPA, recovering (K', κ).

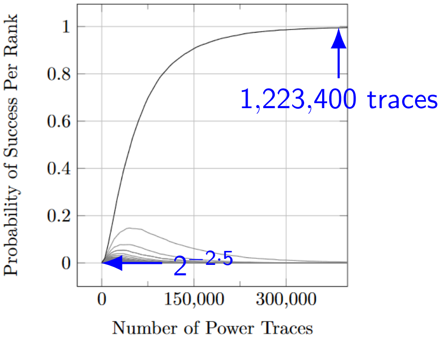


(b) Combined CPA or *Snake* attack recovering κ. Squared correlation coefficient.

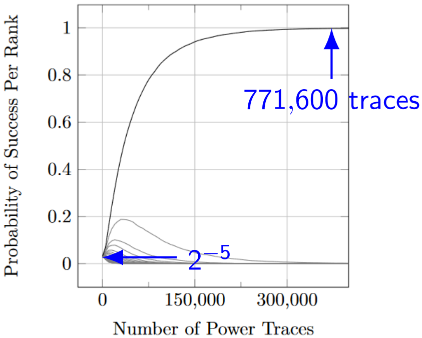
Figure: Ranked success probabilities targeting one χ_5 sequence (Keccak-p).

Ranked Probabilities of Success for One χ_5 Sequence

$n = 5$ bits



(a) CPA, recovering (K', κ).

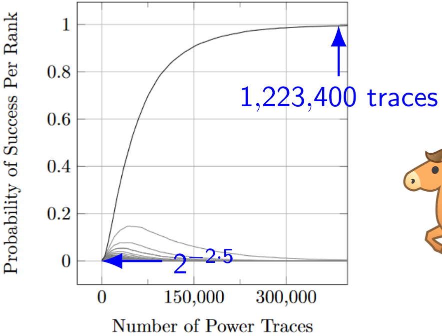


(b) Combined CPA or *Snake* attack recovering κ. Squared correlation coefficient.

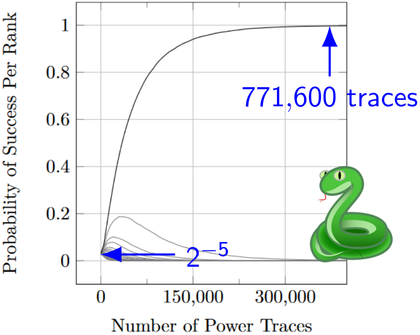
Figure: Ranked success probabilities targeting one χ_5 sequence (Keccak-p).

Ranked Probabilities of Success for One χ_5 Sequence

$n = 5$ bits



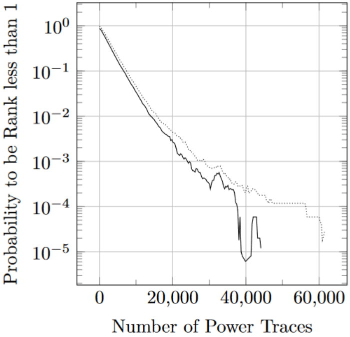
(a) CPA, recovering (K', κ).



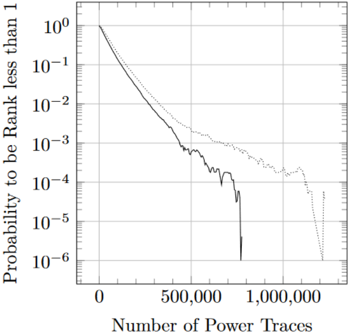
(b) Combined CPA or *Snake* attack recovering κ. Squared correlation coefficient.

Figure: Ranked success probabilities targeting one χ_5 sequence (Keccak-p).

Probability of Not Being Correct: CPA vs. Combined CPA (Snake Attack)



(a) $n = 3$



(b) $n = 5$

Figure: Comparison between CPA (dotted line) and *Snake* attack (solid line) for the probability of the correct hypothesis to *not* be rank 1.

Conclusion

- Improve the CPA computational complexity from 2^{2n} to $n2^2 + n$ intermediate results.
- Combined CPA or *Snake* attack has a higher probability of success than traditional CPA for the same number of power traces.

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Conclusion

- Improve the CPA computational complexity from 2^{2n} to $n2^2 + n$ intermediate results.
- Combined CPA or *Snake* attack has a higher probability of success than traditional CPA for the same number of power traces.

Thank you for your attention

Paper

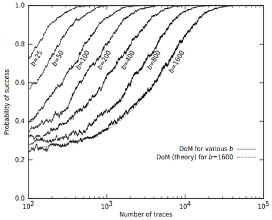
Artifact

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

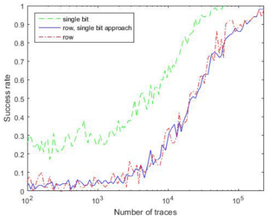
CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Previous work

- Previous work with DPA on one χ_5 row



Bertoni, Daemen, et al. 2012. Power Analysis of Hardware Implementations Protected with Secret Sharing. MICROW'12.



Samwel and Daemen. 2017. DPA on hardware implementations of Ascon and Keyak. CF'17.