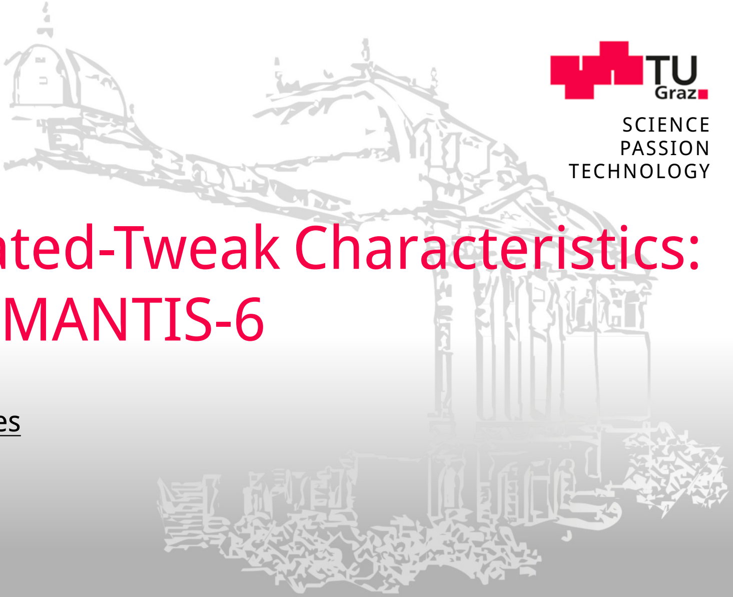
SCIENCE
PASSION
TECHNOLOGY



Clustering Related-Tweak Characteristics: Application to MANTIS-6

Maria Eichlseder   Daniel Kales

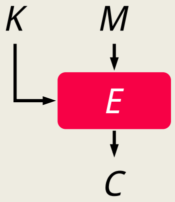
Paris, March 27th, 2019

Overview

- Context, target cipher `MANTIS`
- Differential attack strategy
- Probability Calculation for Clustered Differentials
- Experiments

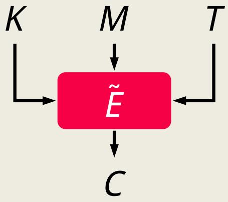
Primitive: Tweakable Block Cipher

Block Ciphers



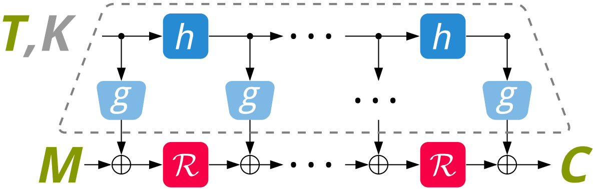
AES, DES, ...

Tweakable Block Ciphers



Skinny, MANTIS, QARMA, ...

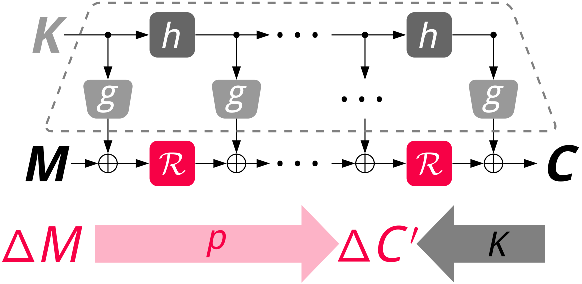
The TWEAKEY/STK framework [JNP14]



Cryptanalytically interesting properties:

- Linear tweak schedule
- Attacker controls tweak → related-tweak attacks

Differential Cryptanalysis [BS90]



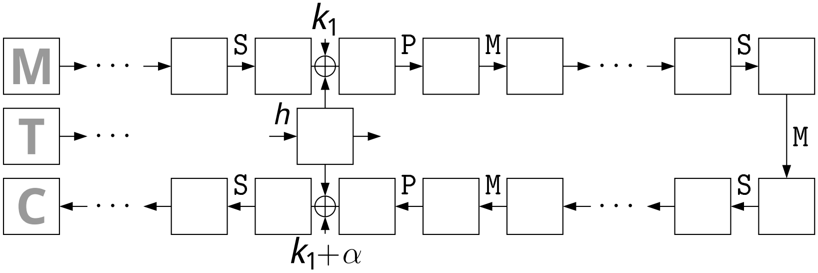
MANTIS

- CRYPTO 2016 [BJK+16]: Tweakable block cipher with low latency
- MANTIS-5 (12 rounds), MANTIS-7 (16 rounds)

MANTIS

CRYPTO 2016 [BJK+16]: Tweakable block cipher with low latency

MANTIS-5 (12 rounds), MANTIS-7 (16 rounds)

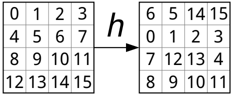


`MANTIS` – Round function $\mathcal{R}_i$

- `S` `SubCells`: involutive 4-bit S-box $\mathcal{S}$
- `A` `AddTweakey`$_i$, `AddConstant`$_i$: Xor key k_1 (for $\mathcal{R}_i$) or $k_1 + \alpha$ (for $\mathcal{R}_i^{-1}$), permuted tweak $h^i(T)$, and round constant C_i
- `P` `PermuteCells`: fast permutation of state cells
- `M` `MixColumns`: involutive near-MDS matrix `M` over $\mathbb{F}_{2^4}$

0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
c	a	d	3	e	b	f	7	8	9	1	5	0	2	4	6

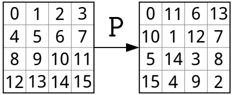
(a) S-box



0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

6	5	14	15
0	1	2	3
7	12	13	4
8	9	10	11

(b) Tweak schedule



0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

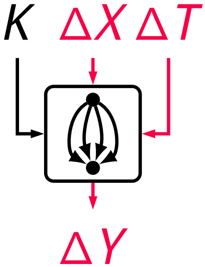
0	11	6	13
10	1	12	7
5	14	3	8
15	4	9	2

(c) `PermuteCells`

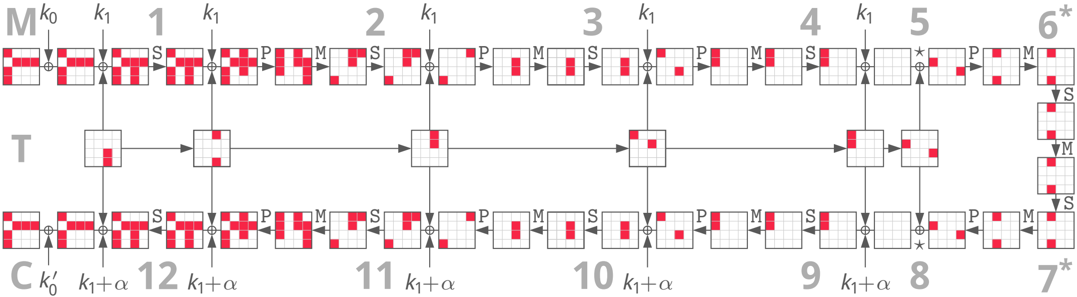
$$\mathtt{M} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

(d) `MixColumns`

Attack strategy

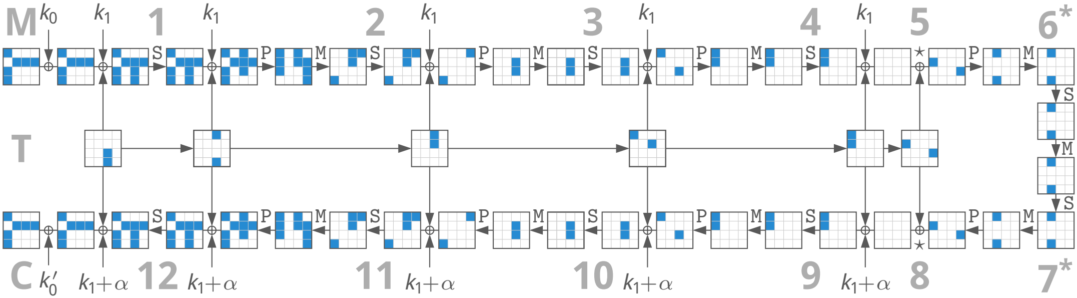


Previous strategy for MANTIS-5, FSE 2017 [DEKM16]



🟥 $1 = |\chi_i|$ Differential characteristic 2^{-72}

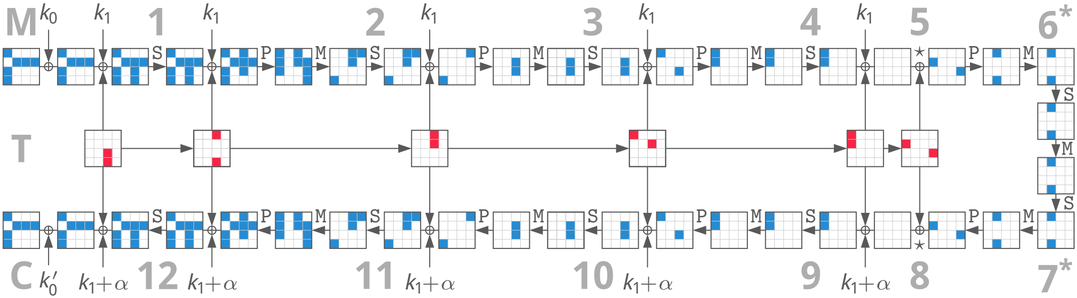
Previous strategy for MANTIS-5, FSE 2017 [DEKM16]



🟥 $1 = |\chi_i|$ Differential characteristic 2^{-72}

🟦 15 or 16 Truncated differential characteristic 2^{-100}

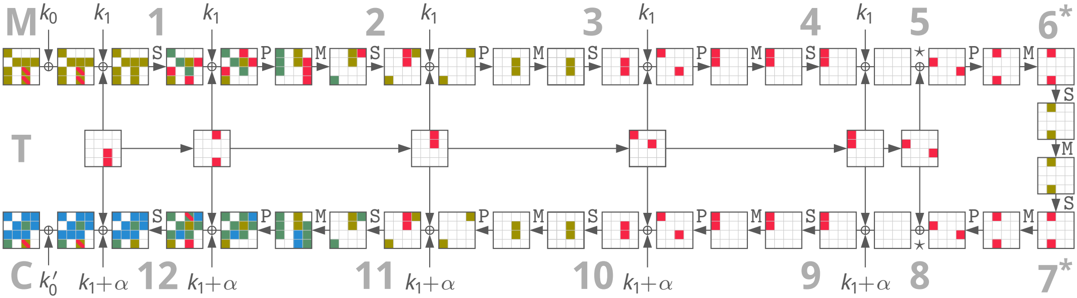
Previous strategy for MANTIS-5, FSE 2017 [DEKM16]



🟥 $1 = |\chi_i|$ Differential characteristic 2^{-72}

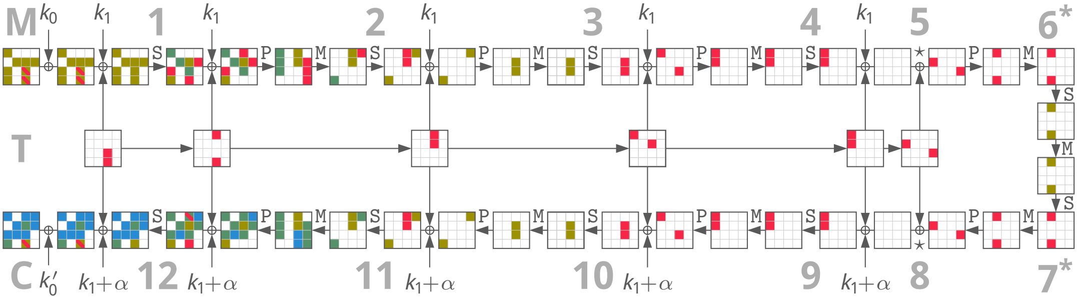
🟦 15 or 16 Truncated differential characteristic 2^{-100}

Previous strategy for MANTIS-5, FSE 2017 [DEKM16]



🟥	$1 = \lvert\chi_i\rvert$	Differential characteristic	2^{-72}
🟨	4	This cluster	2^{-39}
🟩	13		
🟦	15 or 16	Truncated differential characteristic	2^{-100}

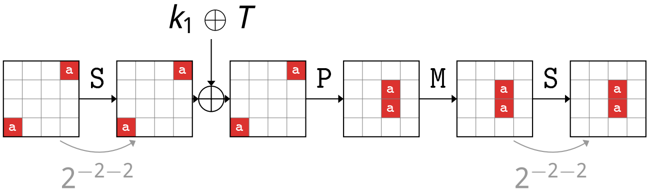
Previous strategy for `MANTIS-5`, FSE 2017 [DEKM16]



🟥	$1 = \lvert\chi_i\rvert$	Differential characteristic	2^{-72}
🟨	4	This cluster	2^{-39}
🟩	13	Data complexity per solution	$2^{\approx 25}$
🟦	15 or 16	Truncated differential characteristic	2^{-100}

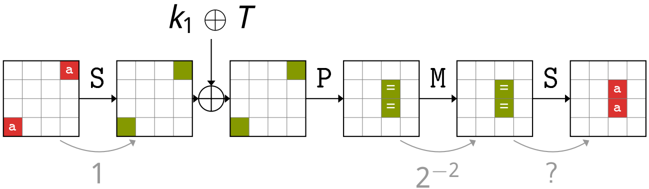
Probability of Differential Clusters

Probability of Differential Clusters



🟥 $\chi_i = \{\mathtt{a}\}$

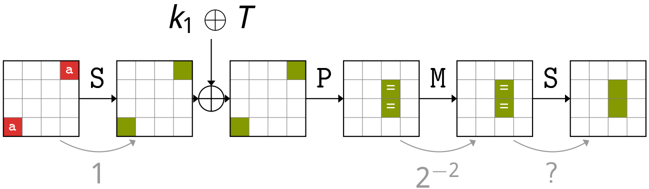
Probability of Differential Clusters



🟥 $\chi_i = \{\mathtt{a}\}$

🟩 $\chi_i = \sigma(\{\mathtt{a}\})$
$= \{\mathtt{a}, \mathtt{f}, \mathtt{d}, \mathtt{5}\}$

Probability of Differential Clusters

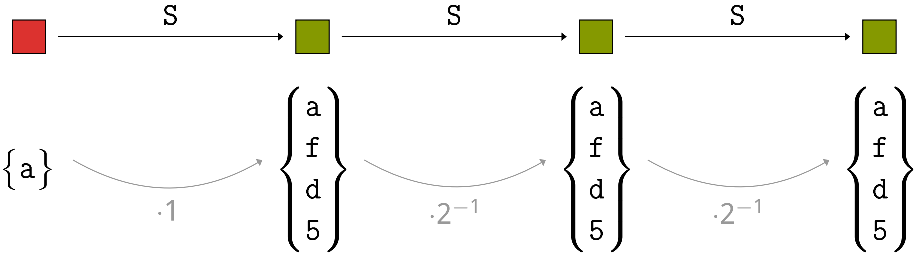


🟥 $\chi_i = \{\mathtt{a}\}$

🟩 $\chi_i = \sigma(\{\mathtt{a}\})$
$= \{\mathtt{a}, \mathtt{f}, \mathtt{d}, \mathtt{5}\}$

Probability of Differential Clusters

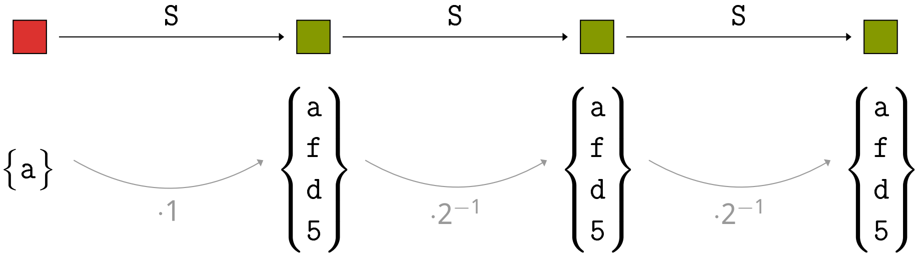
Compute transition probability based on DDT [DEKM16]



Probability of Differential Clusters

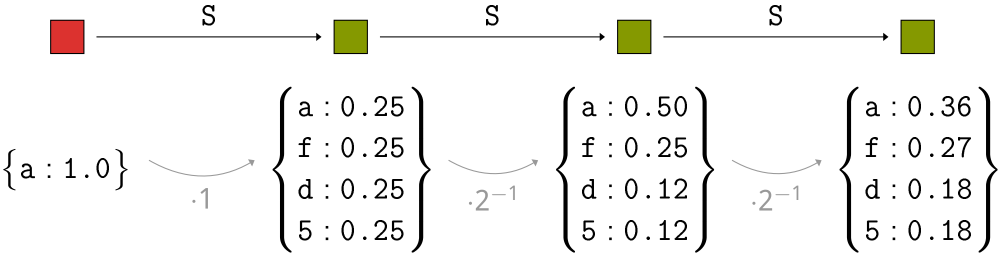
Compute transition probability based on DDT [DEKM16]

Assumes uniform distribution of differences!



Probability of Differential Clusters

Extend calulation with probability distribution.

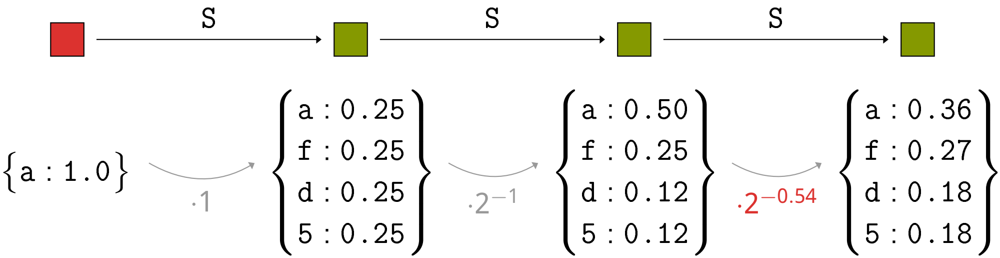


S S S

$$\{a : 1.0\} \xrightarrow{\cdot 1} \left\{\begin{array}{l} a : 0.25 \\ f : 0.25 \\ d : 0.25 \\ 5 : 0.25 \end{array}\right\} \xrightarrow{\cdot 2^{-1}} \left\{\begin{array}{l} a : 0.50 \\ f : 0.25 \\ d : 0.12 \\ 5 : 0.12 \end{array}\right\} \xrightarrow{\cdot 2^{-1}} \left\{\begin{array}{l} a : 0.36 \\ f : 0.27 \\ d : 0.18 \\ 5 : 0.18 \end{array}\right\}$$

Probability of Differential Clusters

Extend calulation with probability distribution.



$$\{a:1.0\} \xrightarrow{\cdot 1} \left\{\begin{matrix} a:0.25 \\ f:0.25 \\ d:0.25 \\ 5:0.25 \end{matrix}\right\} \xrightarrow{\cdot 2^{-1}} \left\{\begin{matrix} a:0.50 \\ f:0.25 \\ d:0.12 \\ 5:0.12 \end{matrix}\right\} \xrightarrow{\cdot 2^{-0.54}} \left\{\begin{matrix} a:0.36 \\ f:0.27 \\ d:0.18 \\ 5:0.18 \end{matrix}\right\}$$

Automated Search for Differential Clusters

- Multi-step process (automated by toolchain)

1. Search for promising truncated characteristic (MILP/SAT/. . .)
2. Fix a promising tweak difference
3. Propagate constraints throughout the cipher
    - cell-wise for `S`, `A`, `P`
    - column-wise for `M`
4. Calculate probability and data-complexity

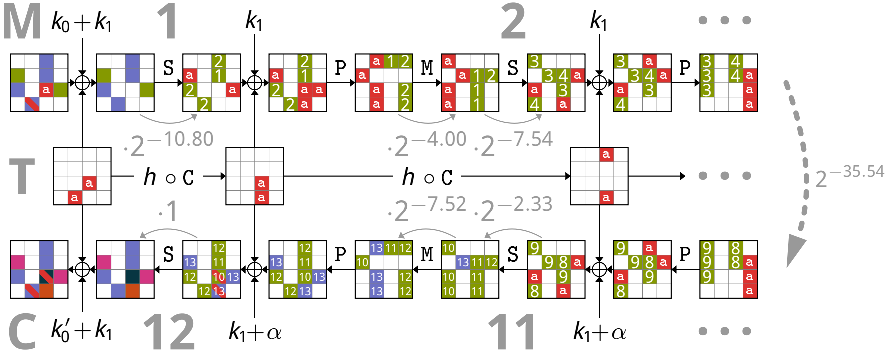
Automated Search for Differential Clusters

- Multi-step process (automated by toolchain)

  1. Search for promising truncated characteristic (MILP/SAT/...)
  2. Fix a promising tweak difference
  3. Propagate constraints throughout the cipher
     - cell-wise for `S`, `A`, `P`
     - column-wise for `M`
  4. Calculate probability and data-complexity

https://github.com/dkales/clusterfk

Key-Recovery Attack on $\texttt{MANTIS}_6$



🟥 $\Delta = \texttt{a}$ 🟩 $\Delta \in \sigma(\{\texttt{a}\}) = \{\texttt{a}, \texttt{f}, \texttt{d}, \texttt{5}\}$ 🟦 $\Delta \in \sigma(\{\texttt{a}, \texttt{f}, \texttt{d}, \texttt{5}\})$ 🟧 ⬛ 🟪 $\cdots$

- Average probability of cluster $\chi^M \to \chi^C$: $2^{-67.73}$ (data: $2^{46.73}$ per solution)
- Attack complexity (data × time): $2^{55.1} \times 2^{55.5} = 2^{110.6} \ll 2^{126}$

Key-Recovery Attack on $\mathtt{MANTIS}_6$

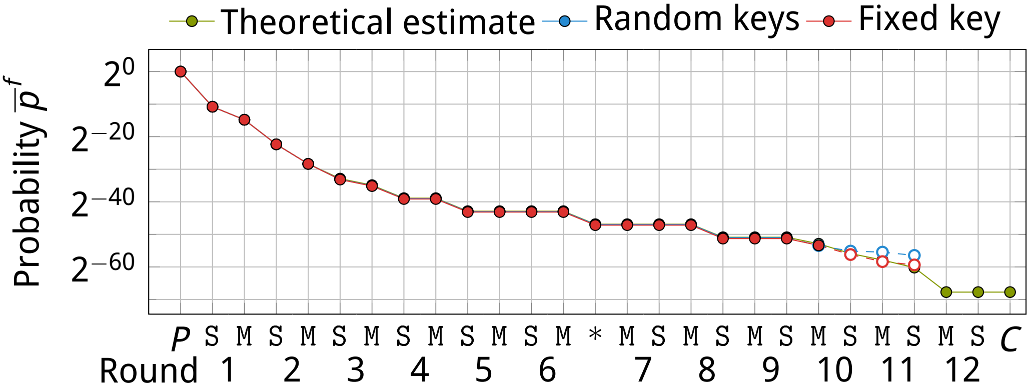
- Complex multi-phase key-recovery attack
  - Guess parts of first round key & apply filter
  - Guess parts of last round key & apply filter
  - Guess parts of combined round 2,11 key & apply filter
  - Intersect key guesses from multiple iterations

Key-Recovery Attack on $\texttt{MANTIS}_6$

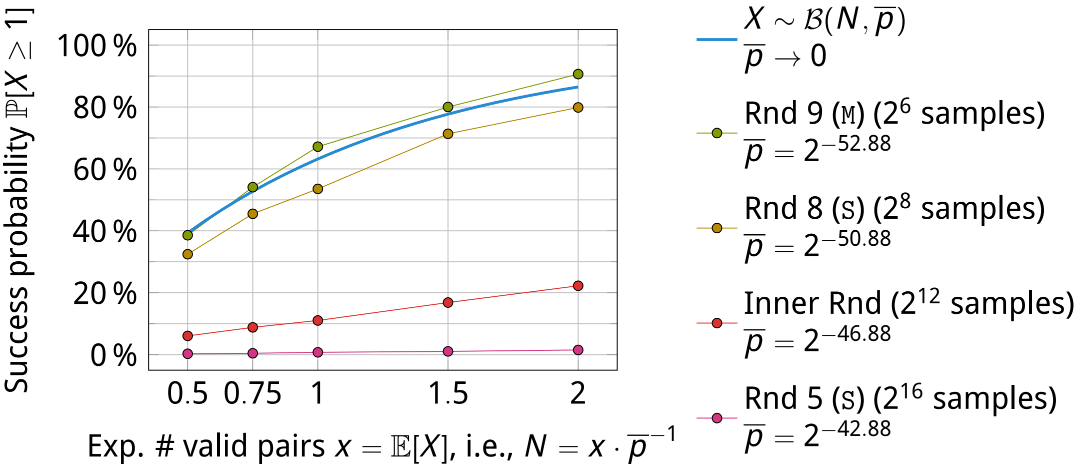
- Complex multi-phase key-recovery attack
  - Guess parts of first round key & apply filter
  - Guess parts of last round key & apply filter
  - Guess parts of combined round 2,11 key & apply filter
  - Intersect key guesses from multiple iterations
- Improved probability calculation used to calculate filter probability
  - compute backward, starting from the ciphertext

Experiments

Experiments – Probability of the characteristic



Experiments – Attack success probability $\mathbb{P}[X \geq 1]$



Conclusions

- Clustered related-tweak differentials
  - General method to find and evaluate clusters
  - Improved probability calculation for clusters
- New attack on $\texttt{MANTIS}_6$
- Extensive experiments to verify validity

Bibliography I

[BS90] E. Biham and A. Shamir
Differential Cryptanalysis of DES-like Cryptosystems
Advances in Cryptology – CRYPTO 1990

[BS97] E. Biham and A. Shamir
Differential Fault Analysis of Secret Key Cryptosystems
Advances in Cryptology – CRYPTO '97

[BG11] C. Blondeau and B. Gérard
Multiple Differential Cryptanalysis: Theory and Practice
FSE 2011

Bibliography II

[BCG+12] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. S. Thomsen, and T. Yalçın
PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications
ASIACRYPT 2012

[FJLT13] T. Fuhr, É. Jaulmes, V. Lomné, and A. Thillard
Fault Attacks on AES with Faulty Ciphertexts Only
Fault Diagnosis and Tolerance in Cryptography – FDTC 2013

[CFG+14] A. Canteaut, T. Fuhr, H. Gilbert, M. Naya-Plasencia, and J.-R. Reinhard
Multiple Differential Cryptanalysis of Round-Reduced PRINCE
FSE 2014

[JNP14] J. Jean, I. Nikolić, and T. Peyrin
Tweaks and Keys for Block Ciphers: The TWEAKEY Framework
ASIACRYPT 2014

Bibliography III

[BBI+15] S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni
Midori: A Block Cipher for Low Energy
ASIACRYPT 2015

[BDP15] A. Biryukov, P. Derbez, and L. Perrin
Differential Analysis and Meet-in-the-Middle Attack Against Round-Reduced TWINE
FSE 2015

[Leu15] G. Leurent
Differential Forgery Attack Against LAC
SAC 2015

[BJK+16] C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. M. Sim
The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS
CRYPTO 2016

Bibliography IV

[DEKM16] C. Dobraunig, M. Eichlseder, D. Kales, and F. Mendel
Practical Key-Recovery Attack on MANTIS5
IACR Transactions on Symmetric Cryptology 2016:2, 2016

[Ava17] R. Avanzi
The QARMA Block Cipher Family – Almost MDS Matrices Over Rings With Zero Divisors, Nearly Symmetric Even-Mansour Constructions With Non-Involutory Central Rounds, and Search Heuristics for Low-Latency S-Boxes
IACR Transactions on Symmetric Cryptology 2017:1, 2017

[CHP+17] C. Cid, T. Huang, T. Peyrin, Y. Sasaki, and L. Song
A Security Analysis of Deoxys and its Internal Tweakable Block Ciphers
IACR Transactions on Symmetric Cryptology 2017:3, 2017

Bibliography V

[EK17] M. Eichlseder and D. Kales
Clustering Related-Tweak Characteristics: Application to MANTIS-6
IACR Cryptology ePrint Archive, Report 2017/1136, 2017

[DEG+18] C. Dobraunig, M. Eichlseder, H. Gross, S. Mangard, F. Mendel, and R. Primas
Statistical Ineffective Fault Attacks on Masked AES with Fault Countermeasures
IACR Cryptology ePrint Archive, Report 2018/357, 2018

[DEK+18] C. Dobraunig, M. Eichlseder, T. Korak, S. Mangard, F. Mendel, and R. Primas
Exploiting Ineffective Fault Inductions on Symmetric Cryptography
IACR Cryptology ePrint Archive, Report 2018/071, 2018