Practical Key-Recovery Attack on MANTIS-5

Christoph Dobraunig Maria Eichlseder Daniel Kales Florian Mendel

FSE 2017

Overview

MANTIS

Tweakable	$\rightarrow$	TWEAKEY tweak schedule	[JNP14]
Low latency	$\rightarrow$	PRINCE cipher structure	[Bor+12]
Bounds	$\rightarrow$	Midori round transformations	[Ban+15]

[Bei+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

Our results

- Differential fixed points lead to clustering effects
- Find 128-bit key of MANTIS_5 with 2^{30} CP in 1 hour ($< 2^{96}$)

The Tweakable Block Cipher MANTIS I

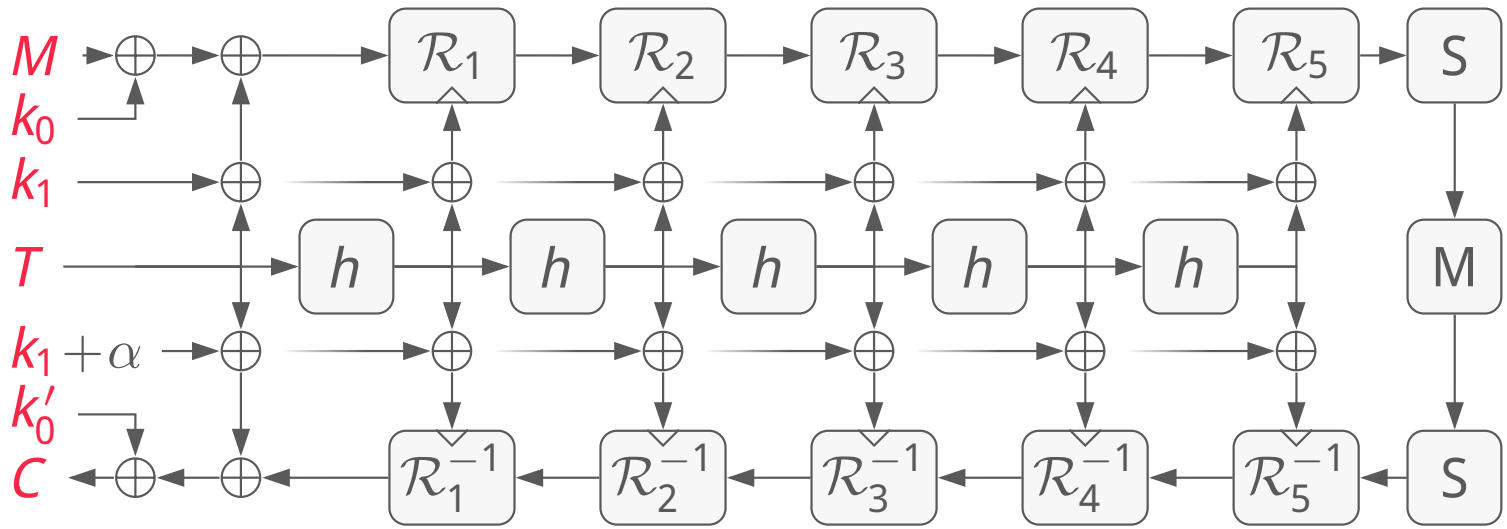
- $4 \times 4 \times 4 = 64$-bit message M, tweak T, keys k_0 and k_1: 
- Lightweight round functions:

$$\begin{cases} \mathcal{R}_i = \text{S} \to \oplus \to \text{P} \to \text{M} \\ \mathcal{R}_i^{-1} = \text{M} \to \text{P}^{-1} \to \oplus \to \text{S} \end{cases}$$

  - S SubCells: involutive 4-bit S-box $\mathcal{S}$
  - P PermuteCells: faster diffusion than ShiftRows
  - M MixColumns: involutive binary near-MDS matrix M over $\mathbb{F}_{2^4}$
  - $\oplus$ AddTweakey$_i$: add constant C_i, key k_1, permuted tweak $h^i(T)$

The Tweakable Block Cipher MANTIS II

- α-reflective structure (MANTIS$_r$ = $2r+2$ S-box layers):



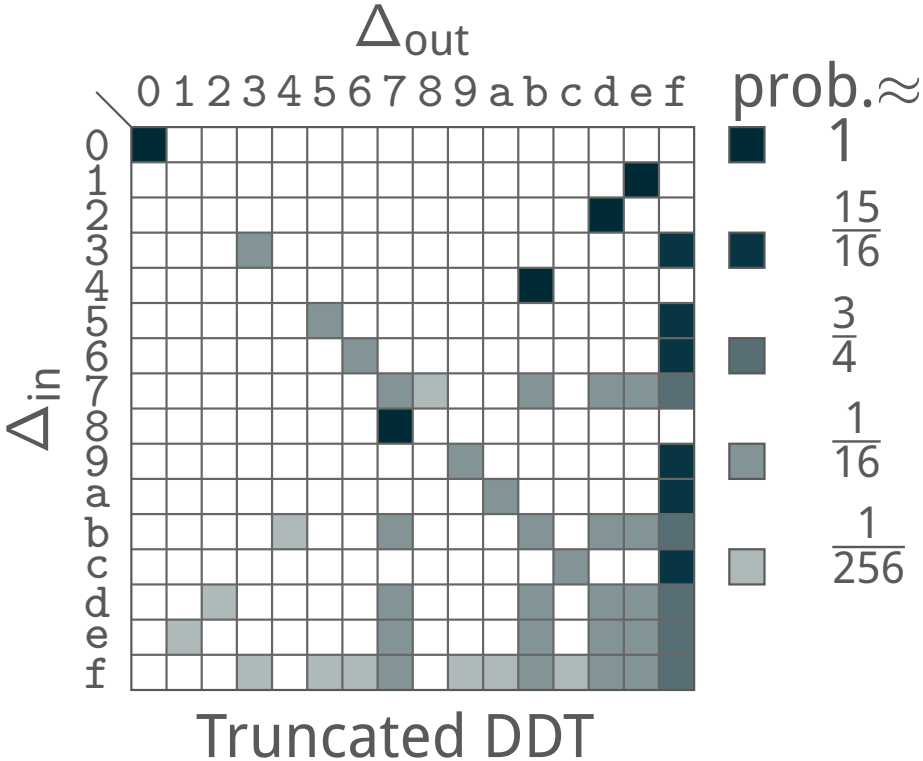
Designers' Analysis and Security Claim

Related-tweak model

- Min number of active S-boxes (MILP):
  - MANTIS_5: ≥ 34
  - MANTIS_7: ≥ 50
- Max prob of any differential characteristic (MDP 2^{-2}):
  - MANTIS_5: $\leq 2^{-68}$
  - MANTIS_7: $\leq 2^{-100}$
- Security claim: No attacks below...
  - MANTIS_5: D data and $T \leq 2^{126}/D$ time, where $D \leq 2^{30}$ CP
  - MANTIS_7: D data and $T \leq 2^{126}/D$ time

Properties of the MANTIS Transformations

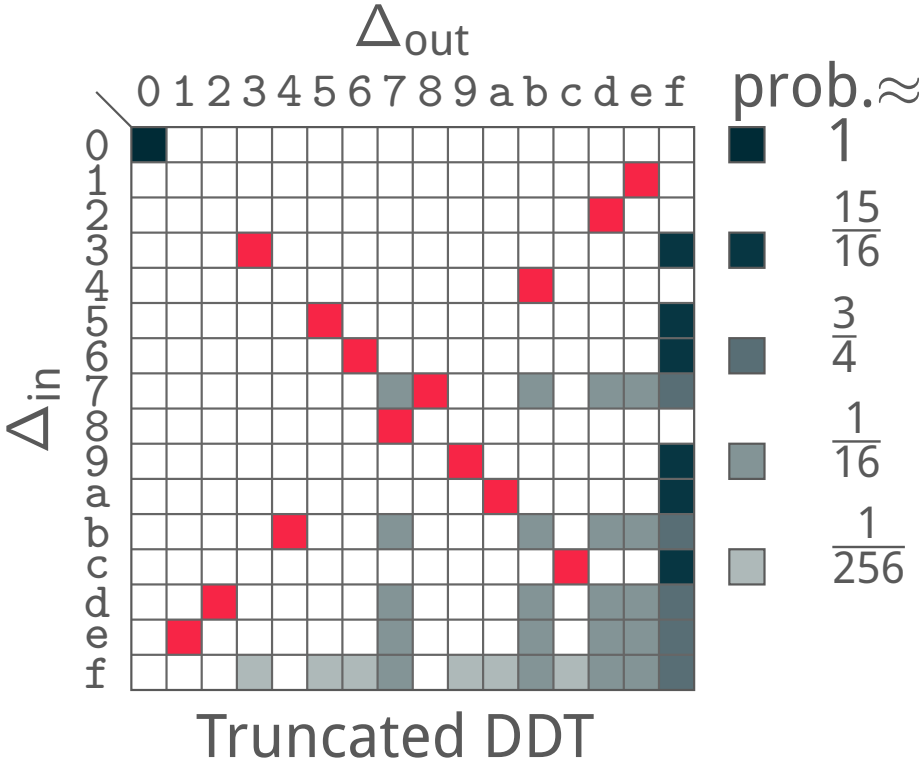
Properties of MixColumns



- Binary coefficients:

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

Properties of MixColumns

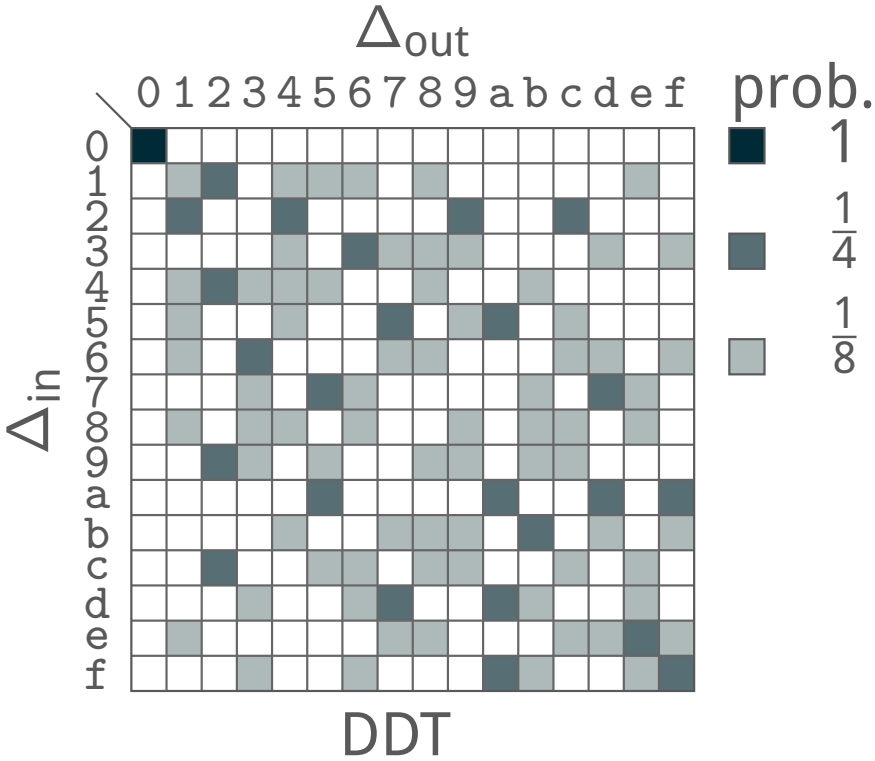


- Binary coefficients:

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

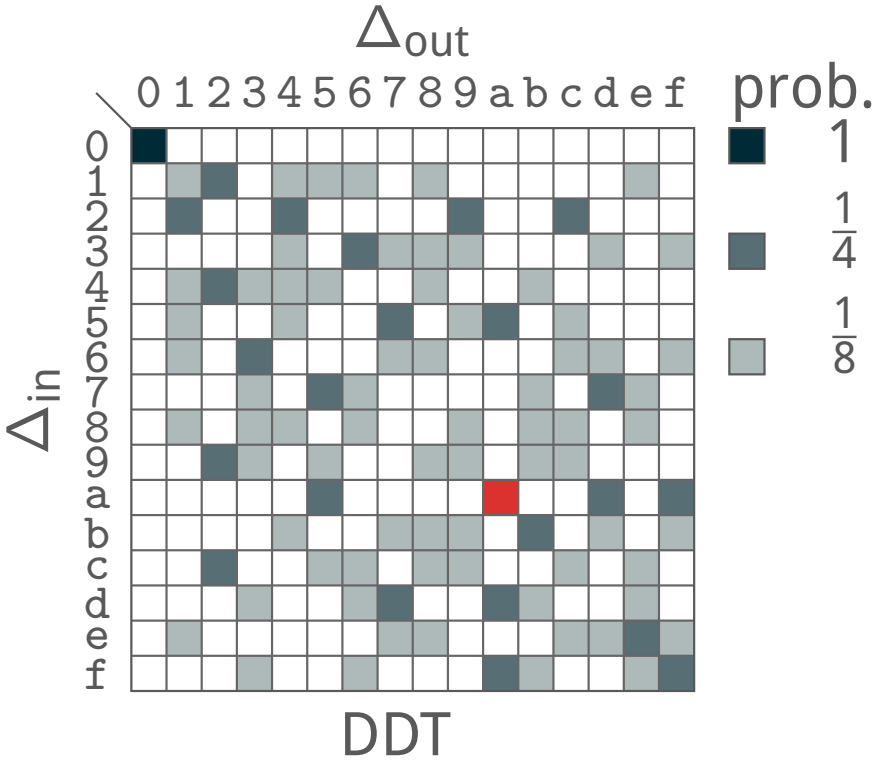
- Branch number 4:
  $1 \to 3, \quad 2 \to 2, \quad 3 \to 1$
- Satisfied with $\delta, \delta, \delta, \delta$
- Differential fixed points

Properties of SubCells



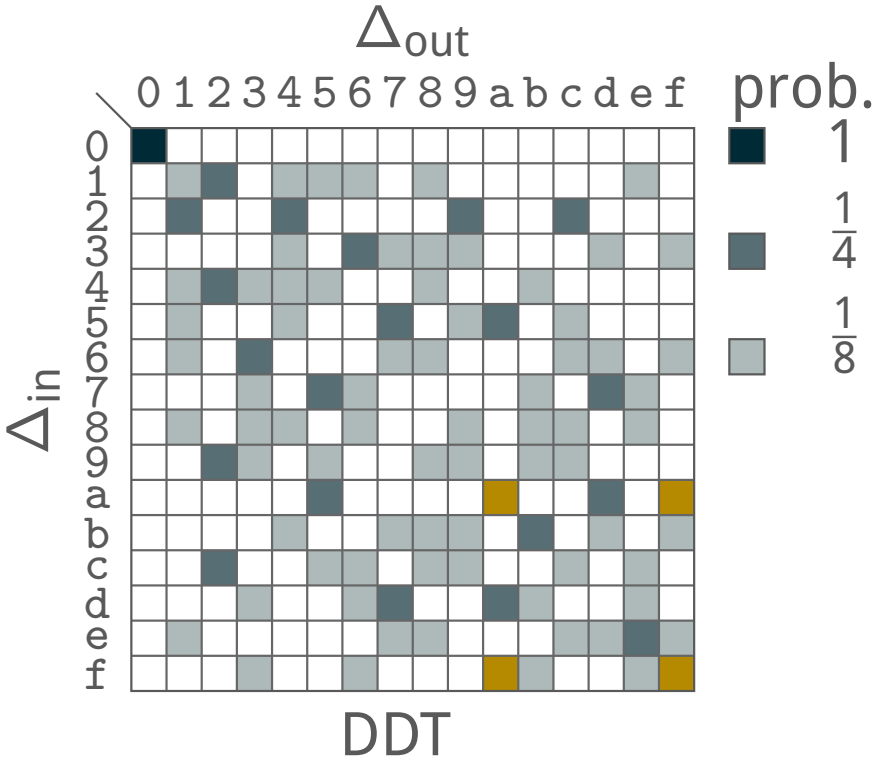
- 4-bit, involutive

Properties of SubCells



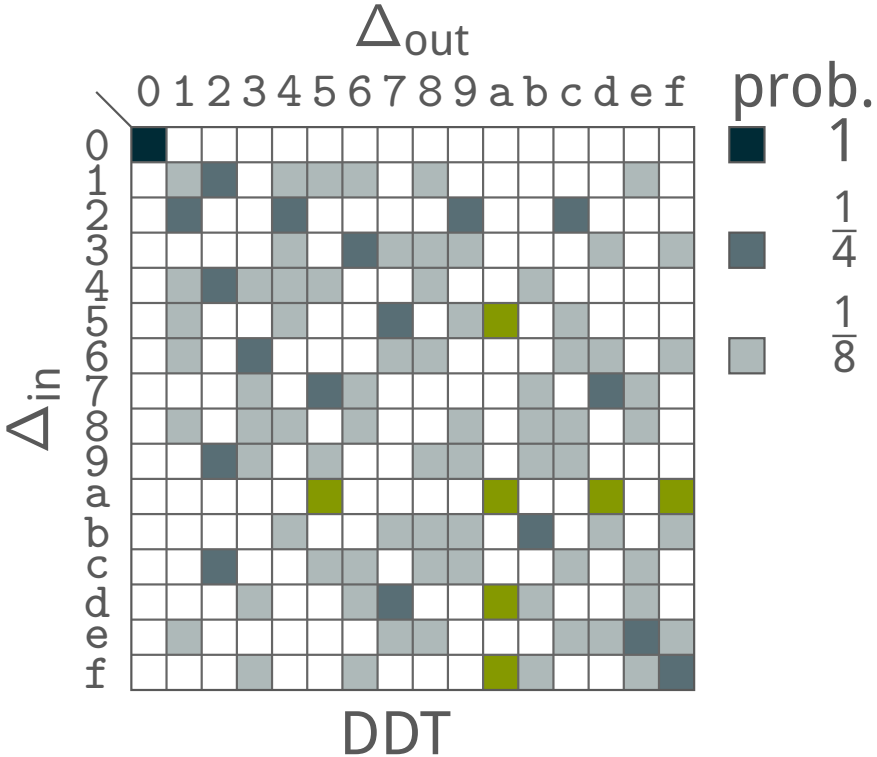
- 4-bit, involutive
- Differential fixed points:
  - $\mathbb{P}[\mathtt{a} \rightarrow \mathtt{a}] = \frac{1}{4}$

Properties of SubCells



- 4-bit, involutive
- Differential fixed points:
  - $\mathbb{P}[\mathtt{a} \to \mathtt{a}] = \frac{1}{4}$
  - $\mathbb{P}[\{\mathtt{a}, \mathtt{f}\} \to \{\mathtt{a}, \mathtt{f}\}] = \frac{1}{2}$

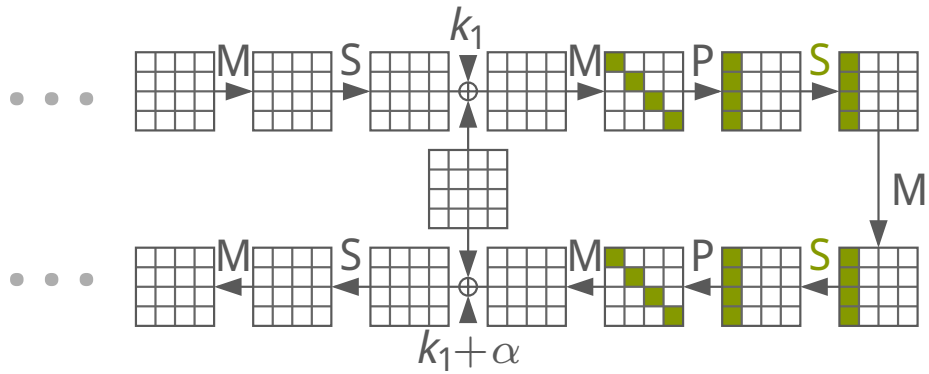
Properties of SubCells



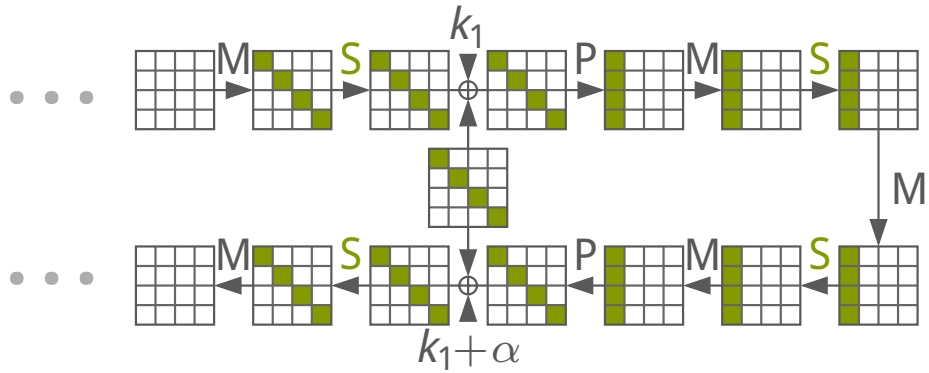
- 4-bit, involutive
- Differential fixed points:
  - $\mathbb{P}[\mathtt{a} \to \mathtt{a}] = \frac{1}{4}$
  - $\mathbb{P}[\{\mathtt{a}, \mathtt{f}\} \to \{\mathtt{a}, \mathtt{f}\}] = \frac{1}{2}$
  - $\mathbb{P}[\mathtt{a} \to \{\mathtt{a}, \mathtt{f}, \mathtt{d}, \mathtt{5}\}] = 1$,
    $\mathbb{P}[\{\mathtt{a}, \mathtt{f}, \mathtt{d}, \mathtt{5}\} \to \mathtt{a}] = \frac{1}{4}$

Properties of the Inner Rounds

- Order of operations in PRINCE: Mix-then-Permute



- Order of operations in MANTIS: Permute-then-Mix

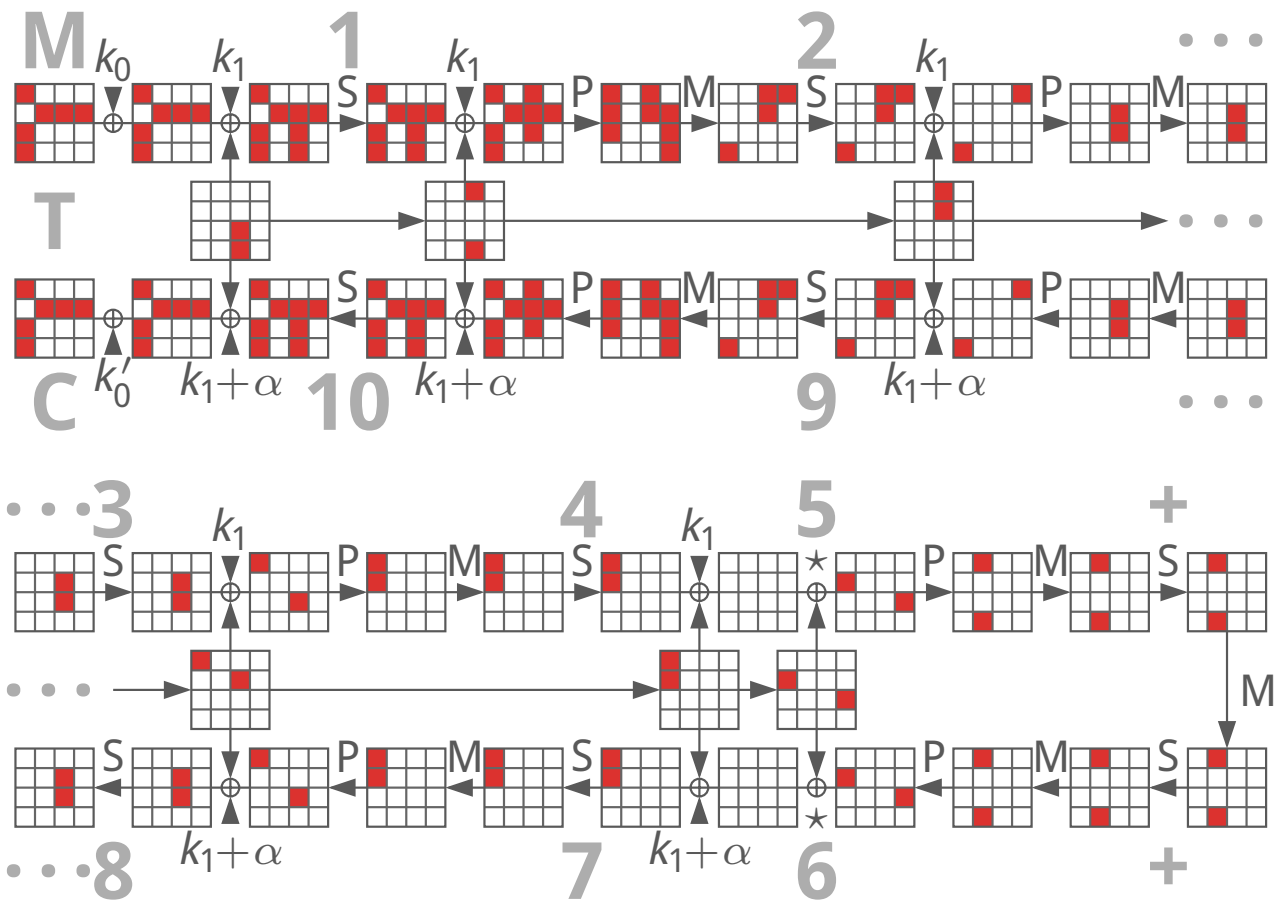


Superboxes over 4 (instead of 2) S-box layers!

A Family of Differential Characteristics

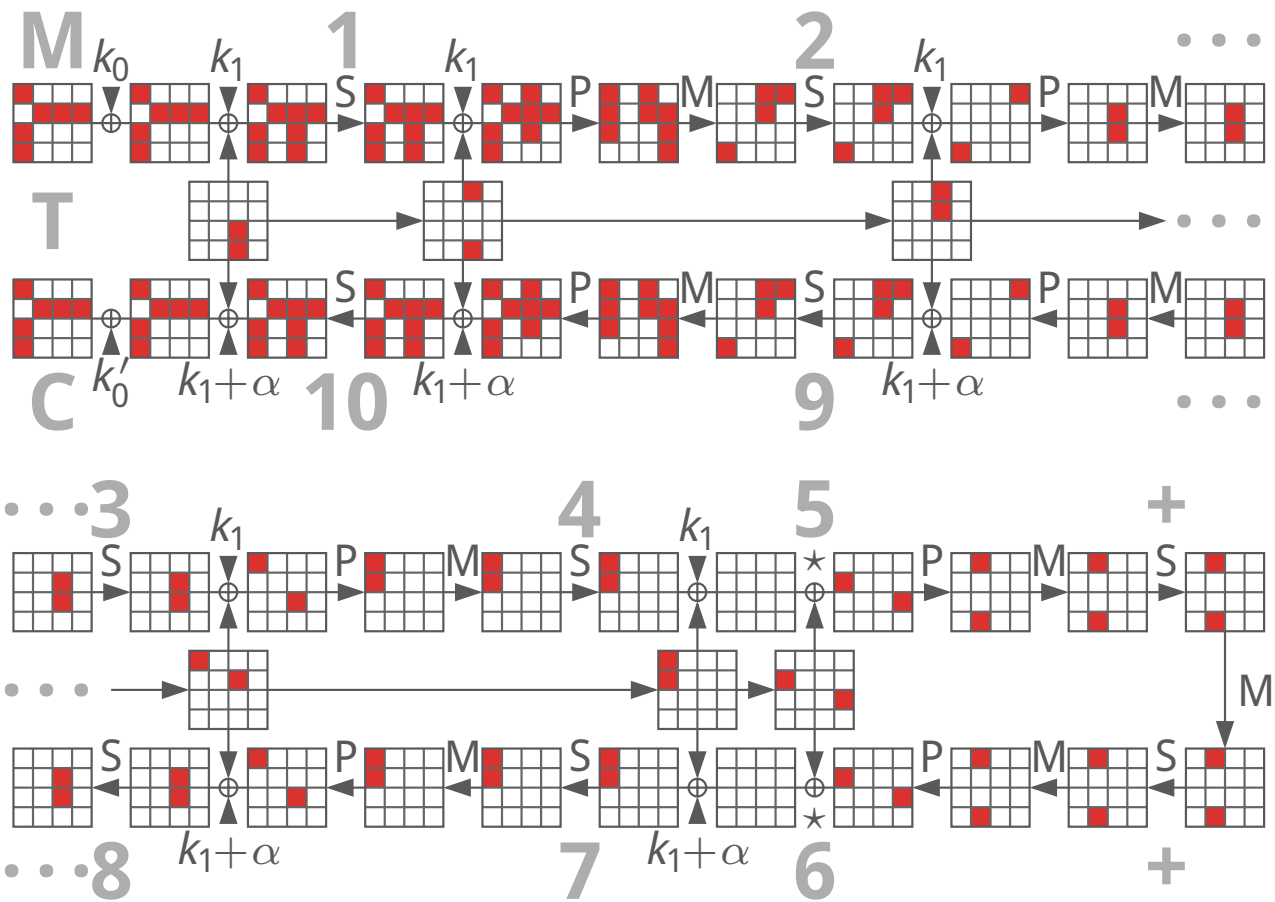
A (Nearly) Optimal Characteristic

MILP: Truncated char with 34 (or 36) active S-boxes



A (Nearly) Optimal Characteristic

MILP: Truncated char with 34 (or 36) active S-boxes



Set ■ = a

⇓

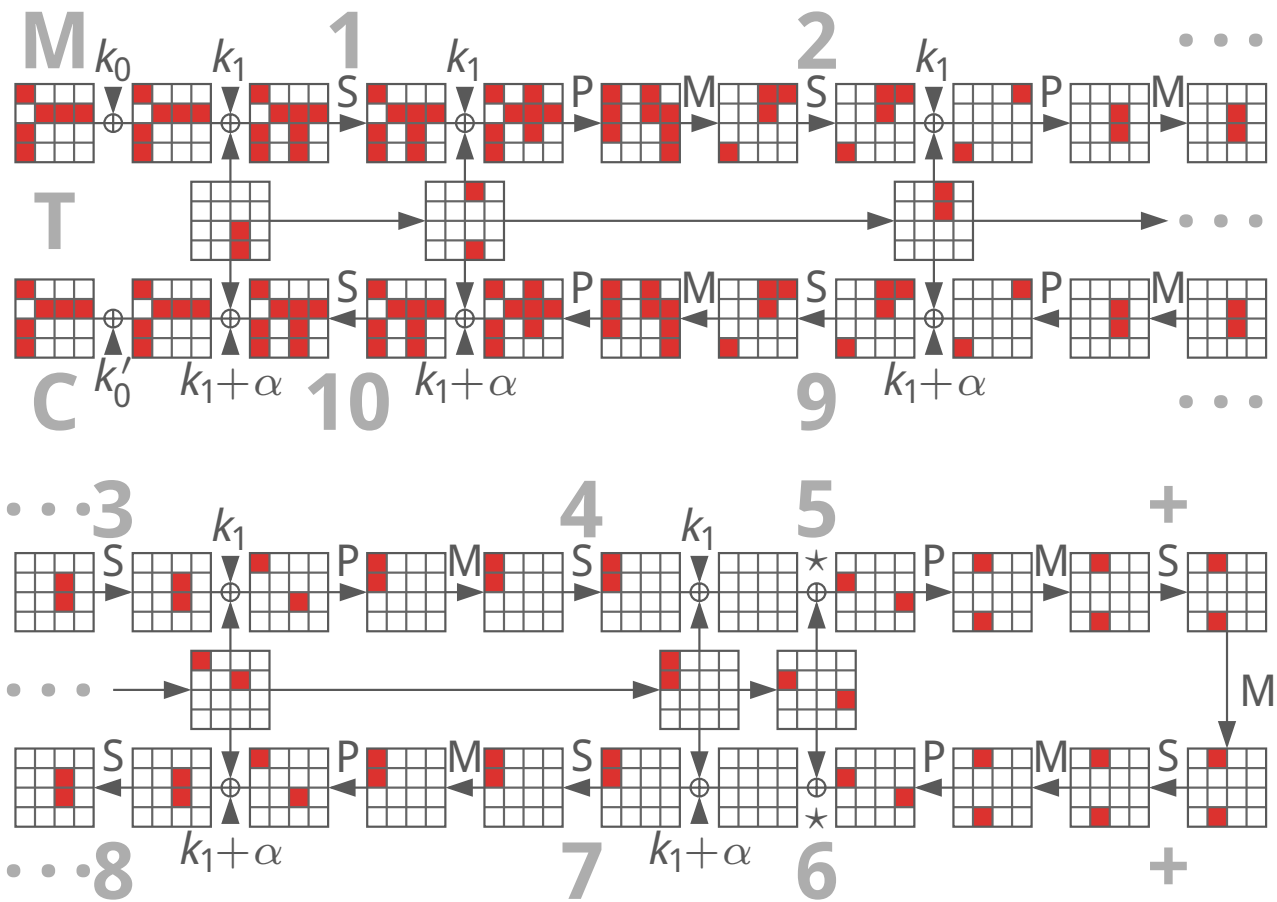
max probability

2^{-68} (or 2^{-72})

⇓

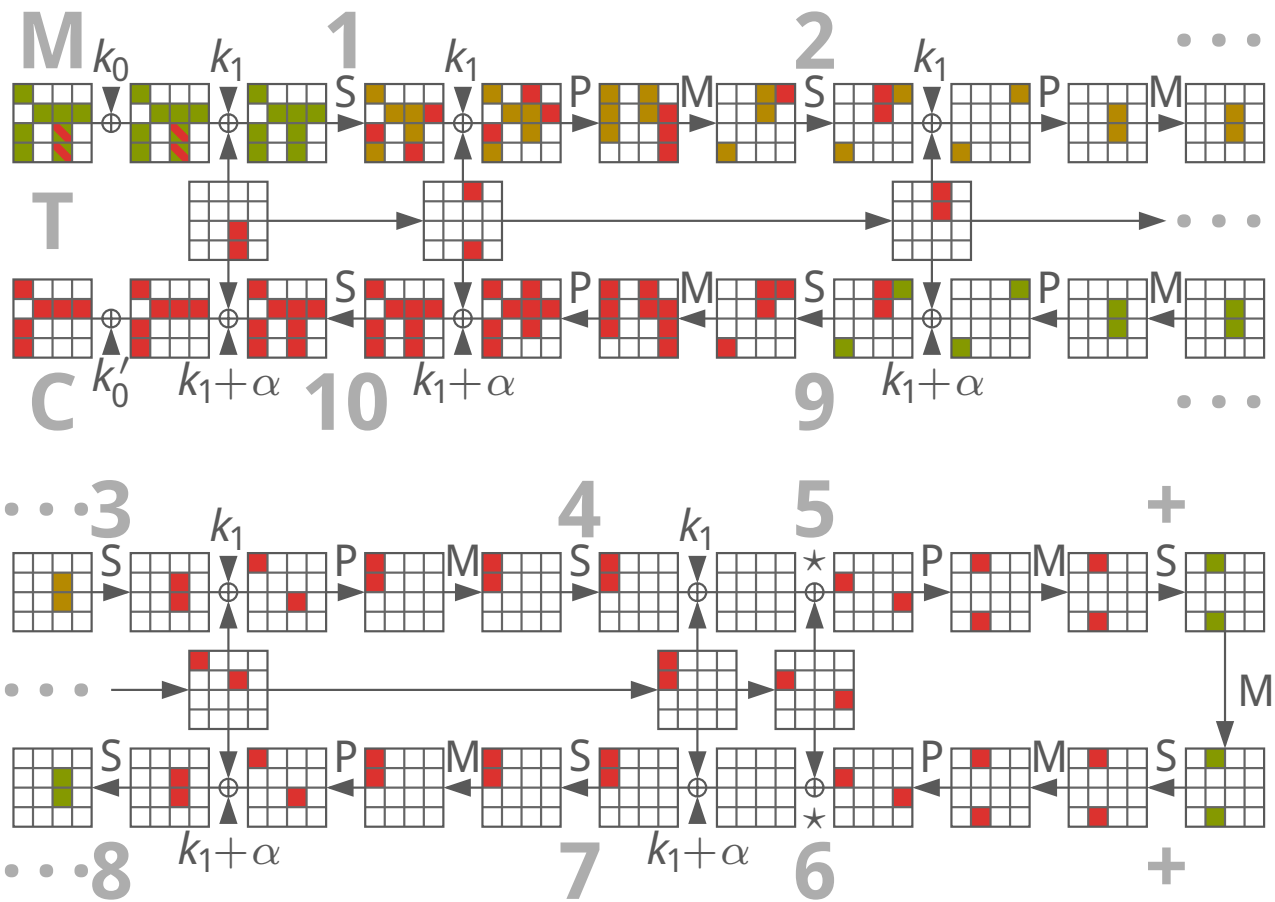
2^{-72}

Relaxing (Clustering) Characteristics



2^{-72}

Relaxing (Clustering) Characteristics



$$a \xrightarrow{S} a \xrightarrow{S} a$$

can be relaxed to

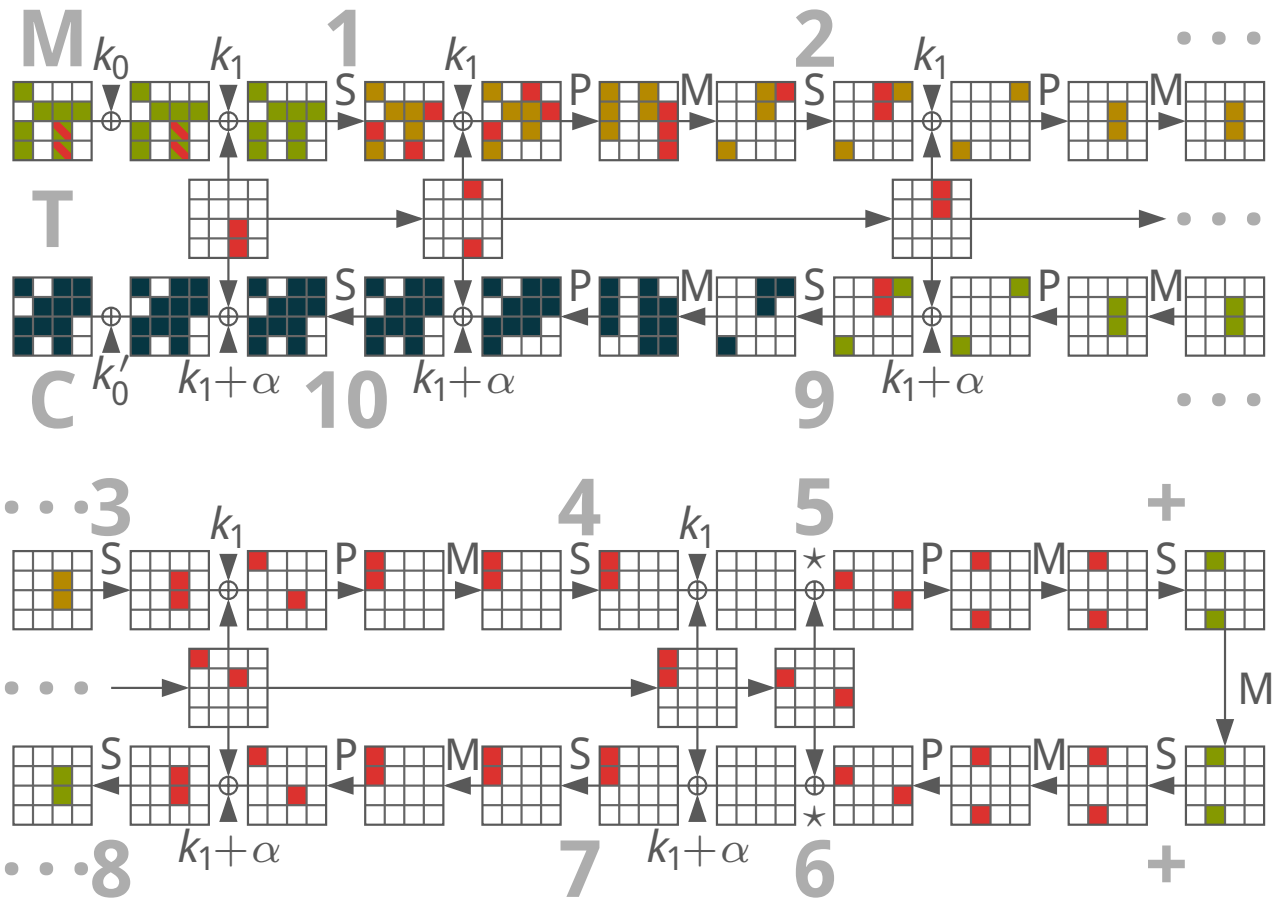
$$a \xrightarrow{S} \left\{ \begin{matrix} a \\ f \\ d \\ 5 \end{matrix} \right\} \xrightarrow{S} a,$$

$$a \xrightarrow{S} \left\{ \begin{matrix} a \\ f \end{matrix} \right\} \xrightarrow{S} \left\{ \begin{matrix} a \\ f \end{matrix} \right\}$$

$$\Downarrow$$

$$2^{-64.51}$$

Relaxing (Clustering) Characteristics



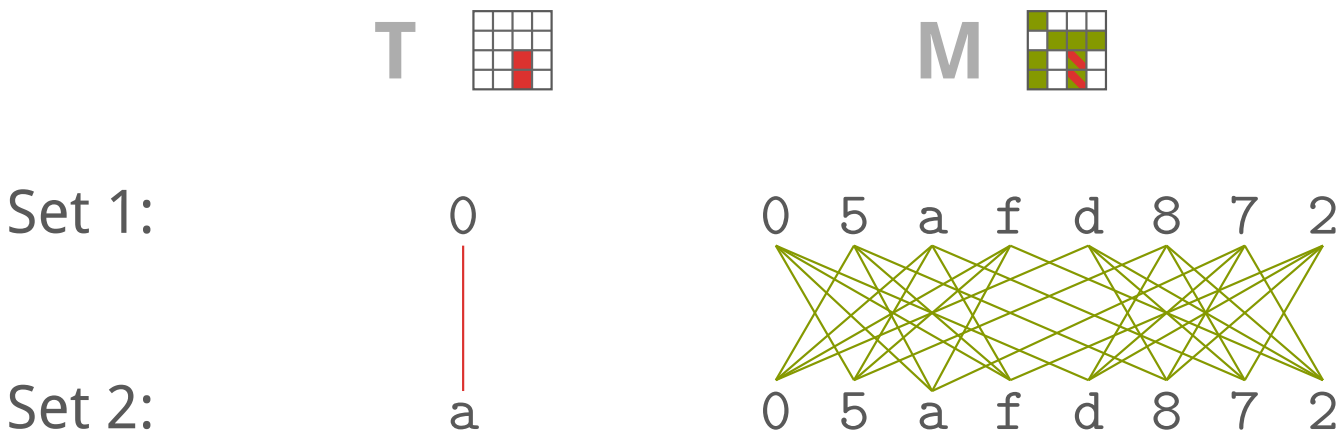
Key recovery

⇓

$2^{-40.51}$

Initial Structure for Data Limit $D \leq 2^{30}$

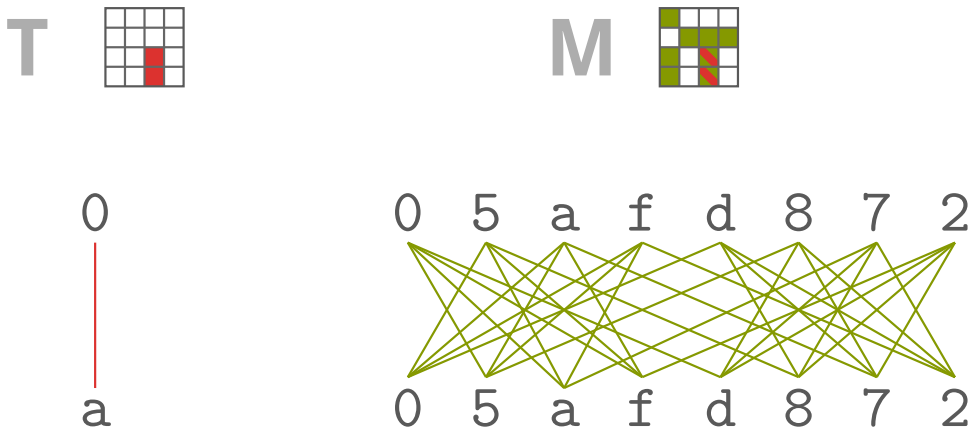
Efficiently generate differences $\{\mathtt{a}, \mathtt{f}, \mathtt{d}, \mathtt{5}\}$ (note $\mathtt{a} + \mathtt{5} = \mathtt{f}$):



$(8 \cdot 4)^8 =$ 2^{40} pairs from $2 \cdot 8^8 =$ 2^{25} CP

Initial Structure for Data Limit $D \leq 2^{30}$

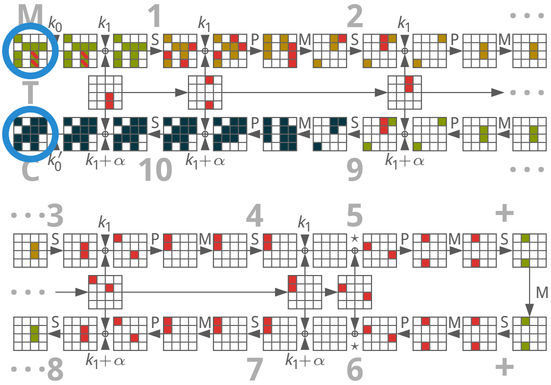
Efficiently generate differences $\{\mathtt{a}, \mathtt{f}, \mathtt{d}, \mathtt{5}\}$ (note $\mathtt{a} + \mathtt{5} = \mathtt{f}$):



$k \cdot (8 \cdot 4)^8 = k \cdot 2^{40}$ pairs from $k \cdot 2 \cdot 8^8 = k \cdot 2^{25}$ CP

Staged Key Recovery Attack

Key Recovery Attack

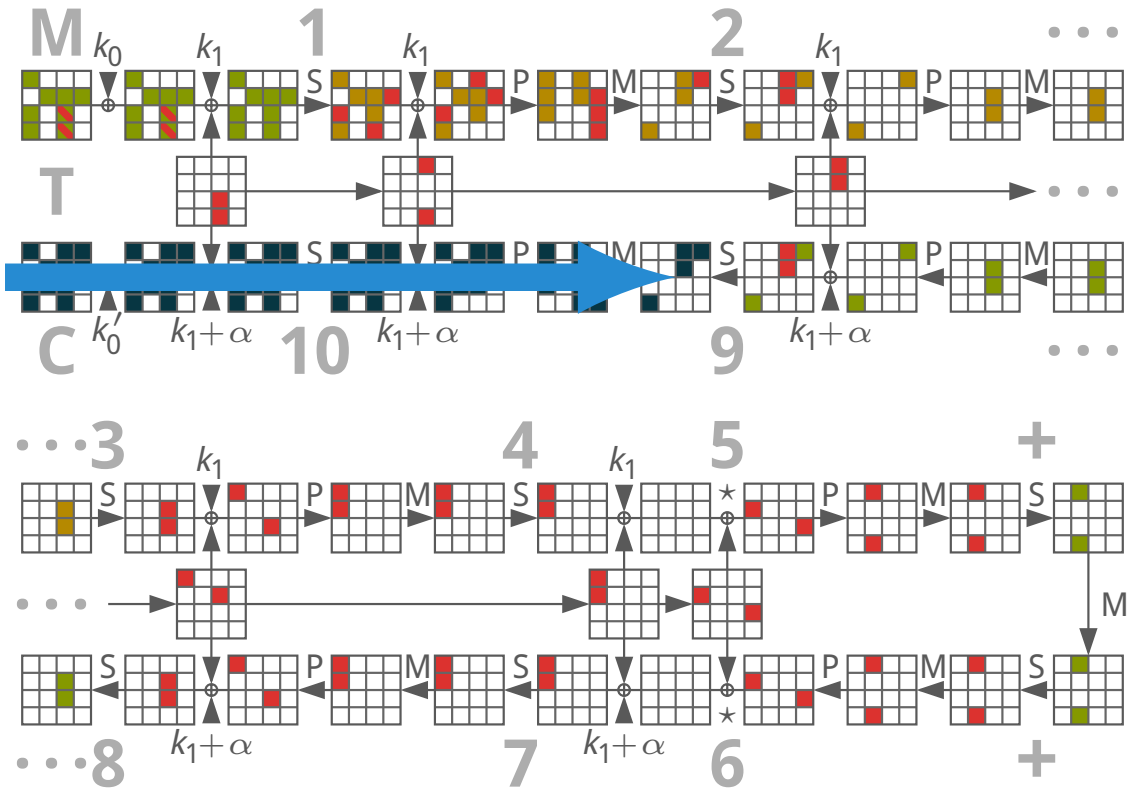


1 Query and pre-filter

a. Query 4×2^{26} CP to get 4×2^{41} **M**-pairs ($\approx 4 \times 1$ right pair)

b. Pre-filter **C**-pairs to about $4 \times 2^{41-22} = 4 \times 2^{19}$ pairs

Key Recovery Attack

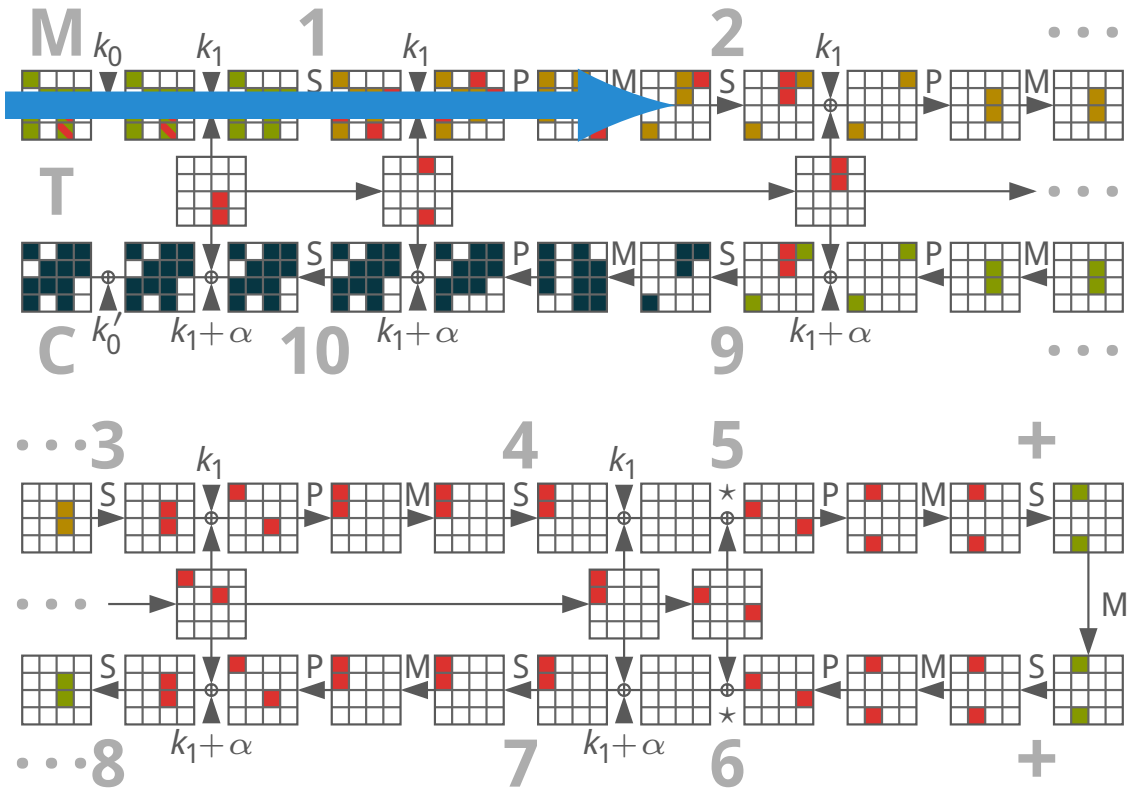


2 Recover final key

a. Guess 44-bit key $k_0' + k_1$ and test 30-bit filter

c. Repeat $4\times$ and intersect candidate sets ($\approx 2^{19+14}$ keys each)

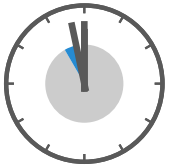
Key Recovery Attack



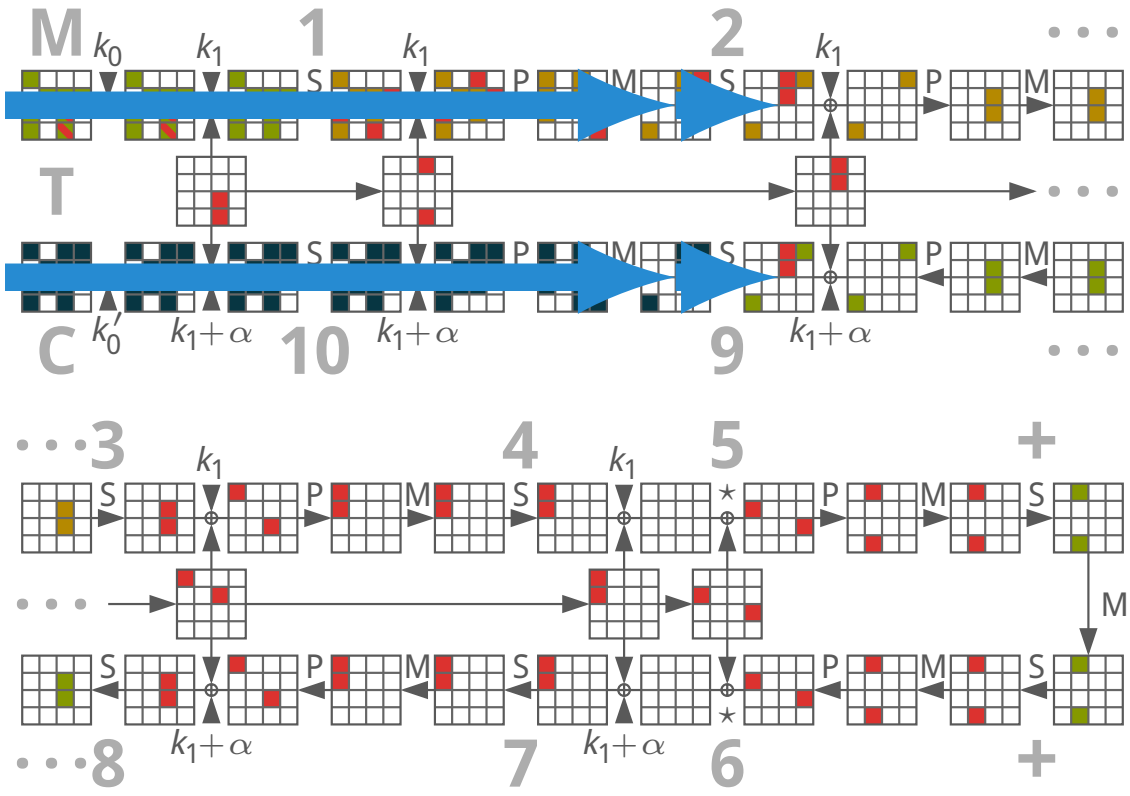
3 Recover initial key

a. Filter for right pairs (≈ 4)

b. Guess 32-bit key $k_0 + k_1$ and test 15-bit filter



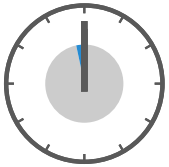
Key Recovery Attack



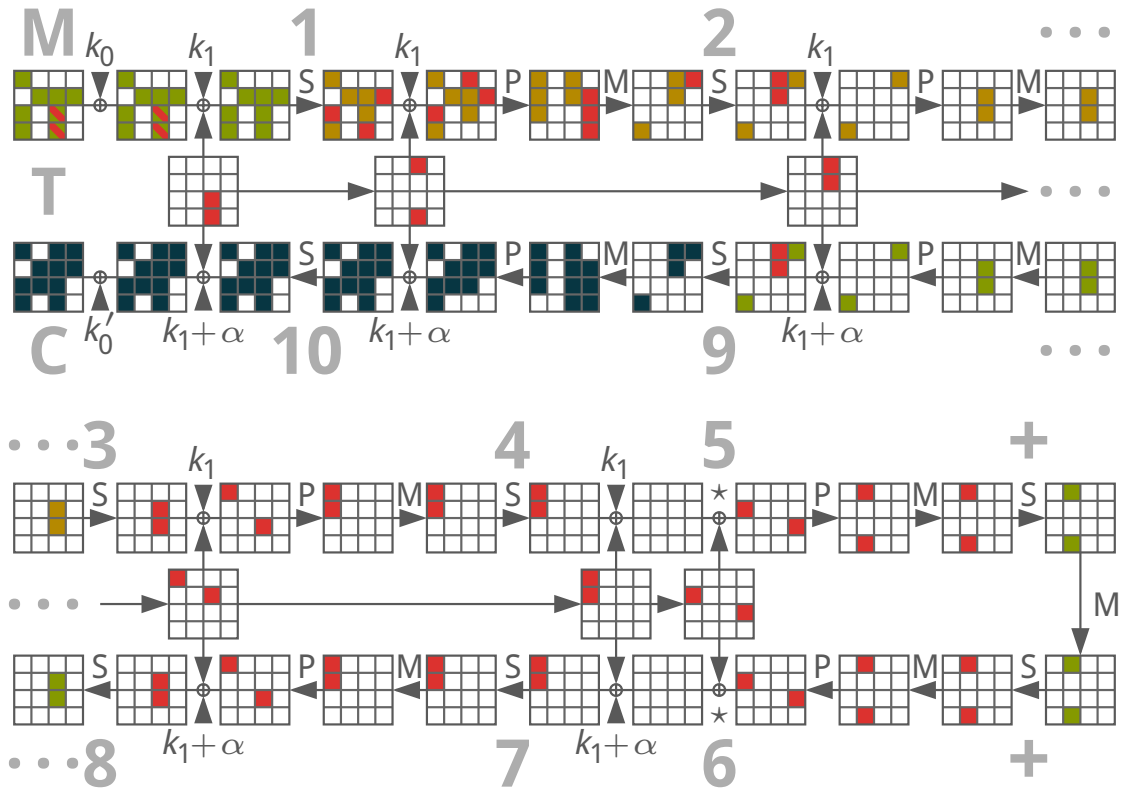
4 Combine and complete

a. Recover 14 more bits, solve $44+32+14 = 90$ linear equations

b. Brute-force remaining 38 bits



Key Recovery Attack

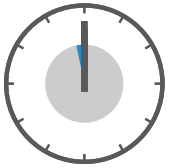


4 Combine and complete

a. Recover 14 more bits, solve $44+32+14=90$ linear equations

b. Brute-force remaining 38 bits

SAT Solver



Conclusions

Practical Verification

- Estimates and validity confirmed
- Two issues, though:
  1. Statistical variance: Right pairs appear in clusters.
     Some repetitions have no right pairs, some have many...
     Fix: Adjust generation of pairs (increase to $2^{30-\varepsilon}$ CP)
  2. Equivalent key candidates: Both k^* and $k^* + \mathtt{a}$ pass test

  Both caused by the same invariance property of SubCells:
  If (x, x') follows $\{\mathtt{a}, \mathtt{f}, \mathtt{d}, 5\} \rightarrow \{\mathtt{a}, \mathtt{f}\}$, then so does $(x + \mathtt{a}, x' + \mathtt{a})$

Conclusion

- Low-latency + tweakable = interesting design challenge
- Possible complications:
  - Differential fixed points
  - Lightweight tweakey schedule
  - Superbox effect in inner rounds
  - Data limit not as effective as expected (multiple differentials)
  - Security margin for key recovery
- See also: QARMA, Session V, tomorrow morning

Bibliography

[Bor+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

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

[Ban+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

[Bei+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