Mind Your Path: On (Key) Dependencies in Differential Characteristics

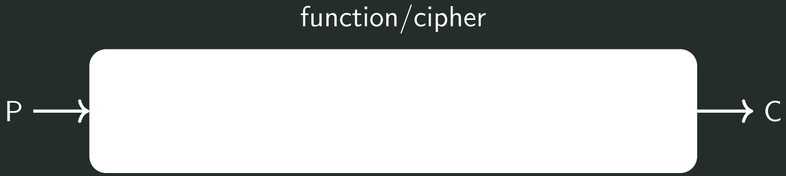
Thomas Peyrin[1] Quan Quan Tan[1]

Nanyang Technological University, Singapore

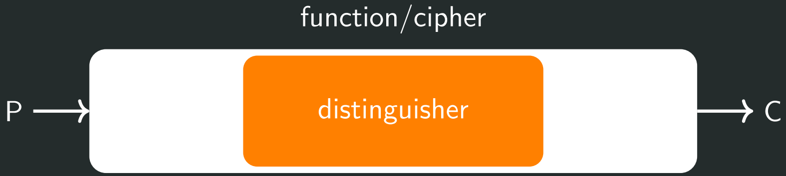
FSE 2023

Outline

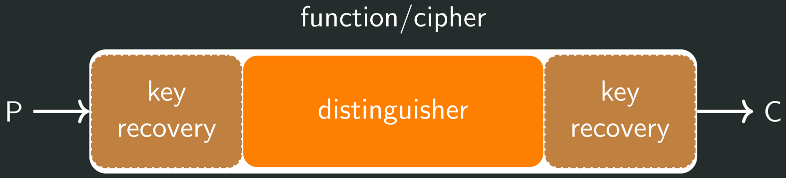
Differential cryptanalysis



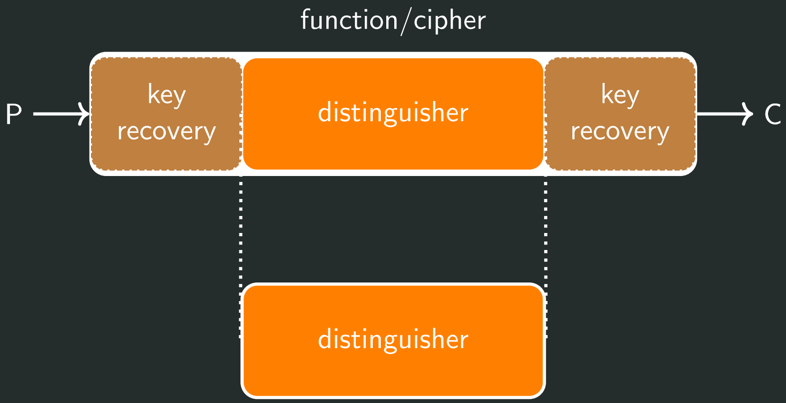
Differential cryptanalysis



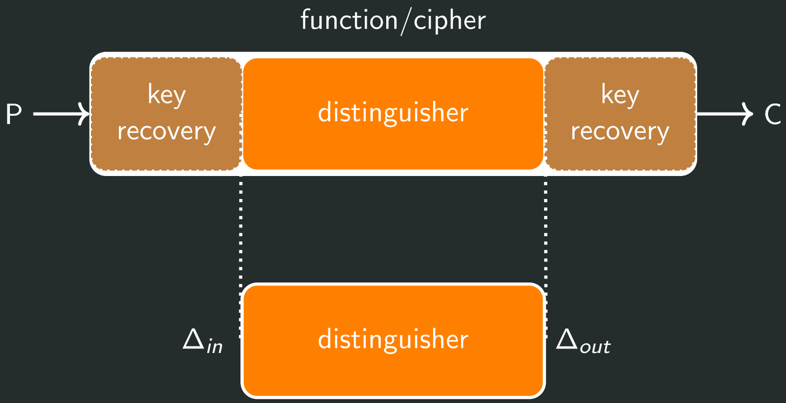
Differential cryptanalysis



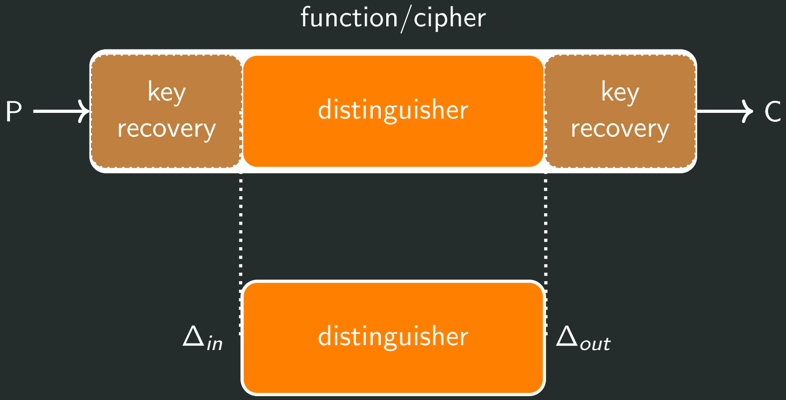
Differential cryptanalysis



Differential cryptanalysis



Differential cryptanalysis



$$\arg\max_{\Delta_{in},\Delta_{out}} \mathbb{P}(\Delta_{in} \to \Delta_{out})$$

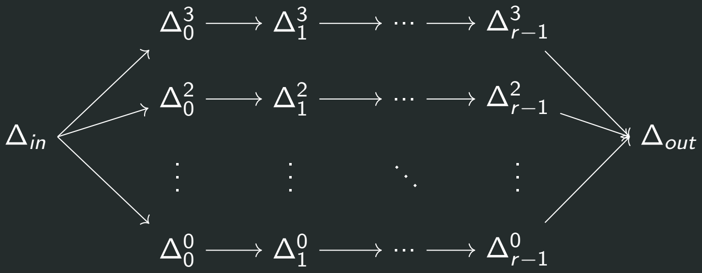
How to compute $\arg\max_{\Delta_{in},\Delta_{out}} \mathbb{P}(\Delta_{in} \rightarrow \Delta_{out})$?

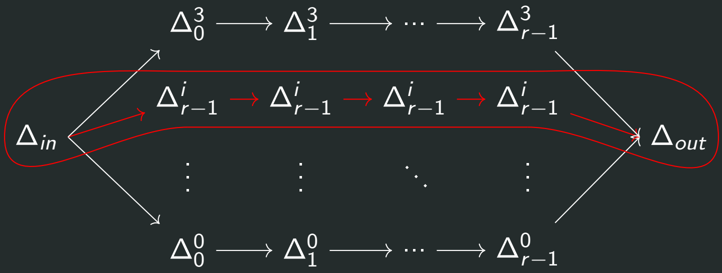
How to compute $\arg\max_{\Delta_{in},\Delta_{out}} \mathbb{P}(\Delta_{in} \to \Delta_{out})$?

$$\mathbb{P}(\Delta_{in} \to \Delta_{out}) = \sum_i \mathbb{P}(\Delta_{in} \to \Delta_1^i \to \ldots \to \Delta_{r-2}^i \to \Delta_{out})$$

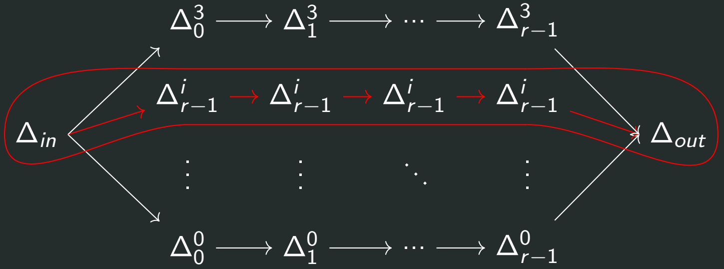
How to compute $\arg\max_{\Delta_{in},\Delta_{out}} \mathbb{P}(\Delta_{in} \to \Delta_{out})$?

$$\mathbb{P}(\Delta_{in} \to \Delta_{out}) = \sum_i \mathbb{P}(\Delta_{in} \to \Delta_1^i \to \ldots \to \Delta_{r-2}^i \to \Delta_{out})$$



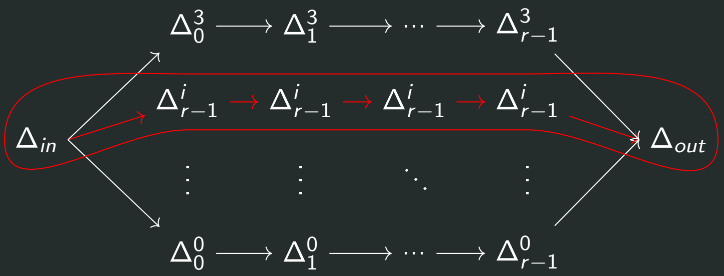


Most of the time, we look at the dominant differential characteristic



Most of the time, we look at the dominant differential characteristic

$$\begin{aligned}\mathbb{P}(\Delta_{in} \to \Delta_{out}) &= \sum_i \mathbb{P}(\Delta_{in} \to \Delta_1^i \to \ldots \to \Delta_{r-2}^i \to \Delta_{out}) \\ &\geq \mathbb{P}(\Delta_{in} \to \Delta_1^* \to \ldots \to \Delta_{r-2}^* \to \Delta_{out})\end{aligned}$$



Most of the time, we look at the dominant differential characteristic

$$\begin{aligned}\mathbb{P}(\Delta_{in} \to \Delta_{out}) &= \sum_i \mathbb{P}(\Delta_{in} \to \Delta_1^i \to \dots \to \Delta_{r-2}^i \to \Delta_{out}) \\ &\geq \mathbb{P}(\Delta_{in} \to \Delta_1^* \to \dots \to \Delta_{r-2}^* \to \Delta_{out})\end{aligned}$$

How to compute $\mathbb{P}(\Delta_{in} \to \Delta_1^* \to \dots \to \Delta_{r-2}^* \to \Delta_{out})$?

How to compute $\mathbb{P}(\Delta_{in} \to \Delta_1^* \to \ldots \to \Delta_{r-2}^* \to \Delta_{out})$?

How to compute $\mathbb{P}(\Delta_{in} \rightarrow \Delta_1^* \rightarrow ... \rightarrow \Delta_{r-2}^* \rightarrow \Delta_{out})$?

Differential probability of a round function is independent of the value, assuming the subkey k is uniformly random [LMM91]. Under this assumption,

$$\mathbb{P}(\Delta_{in} \rightarrow \Delta_1^* \rightarrow ... \rightarrow \Delta_{r-2}^* \rightarrow \Delta_{out})$$
$$\approx \mathbb{P}(\Delta_{in} \rightarrow \Delta_1^*) * \mathbb{P}(\Delta_1^* \rightarrow \Delta_2^*) * ... * \mathbb{P}(\Delta_{n-2}^* \rightarrow \Delta_{out})$$

How to compute $\mathbb{P}(\Delta_{in} \rightarrow \Delta_1^* \rightarrow \ldots \rightarrow \Delta_{r-2}^* \rightarrow \Delta_{out})$?

Differential probability of a round function is independent of the value, assuming the subkey k is uniformly random [LMM91]. Under this assumption,

$$\begin{aligned}&\mathbb{P}(\Delta_{in} \rightarrow \Delta_1^* \rightarrow \ldots \rightarrow \Delta_{r-2}^* \rightarrow \Delta_{out})\\ \approx&\mathbb{P}(\Delta_{in} \rightarrow \Delta_1^*) * \mathbb{P}(\Delta_1^* \rightarrow \Delta_2^*) * \ldots * \mathbb{P}(\Delta_{n-2}^* \rightarrow \Delta_{out})\end{aligned}$$

- Difference Distribution Table
- Automated methods (SAT,MILP,CP)

Related works

Is this assumption valid?

Related works

Is this assumption valid?

- Permutations (Gimli) [LIM20]
- Hash functions (SHA-2) [MNS11]

Related works

Is this assumption valid?

- Permutations (Gimli) [LIM20]
- Hash functions (SHA-2) [MNS11]
- Finding exact probabilities under unkeyed/fixed key model [CLN+17]
- Singular characteristics [LZS+20]

Related works

Is this assumption valid?

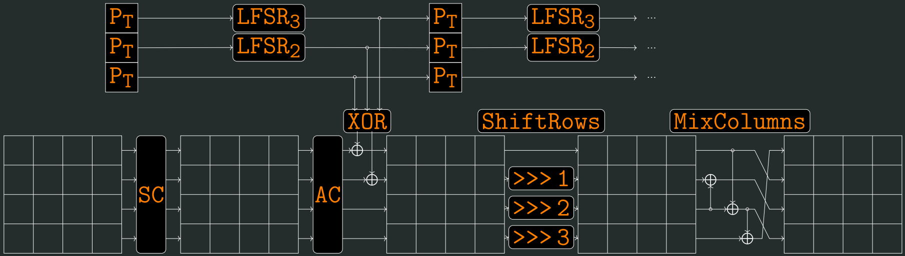
- Permutations (Gimli) [LIM20]
- Hash functions (SHA-2) [MNS11]
- Finding exact probabilities under unkeyed/fixed key model [CLN+17]
- Singular characteristics [LZS+20]
- LED analysis [MRTV12, NWW15, SWW18]

Related works

Is this assumption valid?

- Permutations (Gimli) [LIM20]
- Hash functions (SHA-2) [MNS11]
- Finding exact probabilities under unkeyed/fixed key model [CLN+17]
- Singular characteristics [LZS+20]
- LED analysis [MRTV12, NWW15, SWW18]
- On ARX/RX ciphers [SRB21, Leu12, XLJ+22]

SKINNY round function [BJK+16]



- Block size $n = 64$ or 128 bits
- Tweakable block cipher (tweakey size is $n, 2n$ or $3n$)

Outline

Motivation

- We want to find out all the possible constraints that lead to necessary conditions on the keys

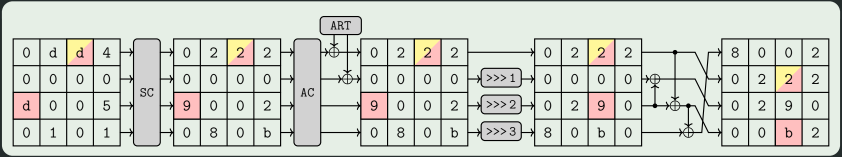
Motivation

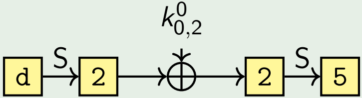
- We want to find out all the possible constraints that lead to necessary conditions on the keys
- For dependencies that are not too complex, we want to approximate the size of the valid key space

Motivation

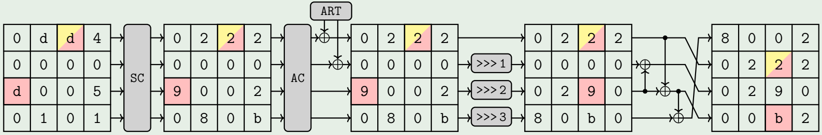
- We want to find out all the possible constraints that lead to necessary conditions on the keys
- For dependencies that are not too complex, we want to approximate the size of the valid key space
- A search method for differential characteristics that also avoid some of these key dependencies (particularly those that invalidate them)

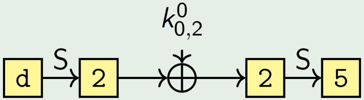
Linear constraints





Linear constraints



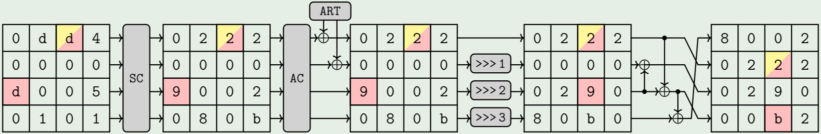


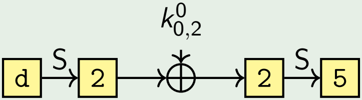
$$\mathcal{Y}_{DDT}(\texttt{0xd}, \texttt{0x2}) = \{\texttt{4,6,c,e}\}$$

$$\mathcal{X}_{DDT}(\texttt{0x2}, \texttt{0x5}) = \{\texttt{0,2,9,b}\}$$

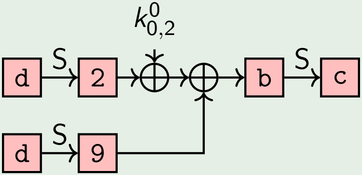
$$\implies k^0_{0,2} \in \{\texttt{4,5,6,7,c,d,e,f}\}$$

Linear constraints



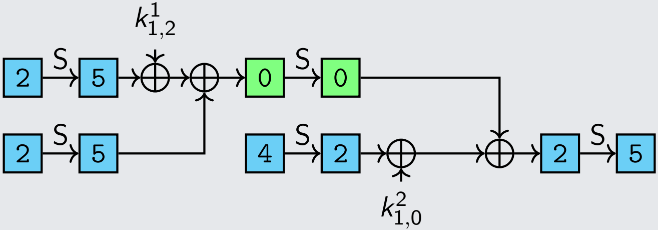


$$\mathcal{Y}_{DDT}(\texttt{0xd}, \texttt{0x2}) = \{\texttt{4,6,c,e}\}$$
$$\mathcal{X}_{DDT}(\texttt{0x2}, \texttt{0x5}) = \{\texttt{0,2,9,b}\}$$
$$\implies k^0_{0,2} \in \{\texttt{4,5,6,7,c,d,e,f}\}$$



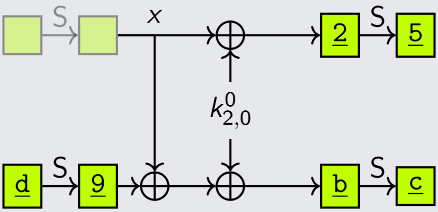
$$k^0_{0,2} \in \{\texttt{0,1,2,3,8,9,a,b}\}$$

Nonlinear constraints



$(k^1_{1,2}, k^2_{1,0}) \in \ldots$

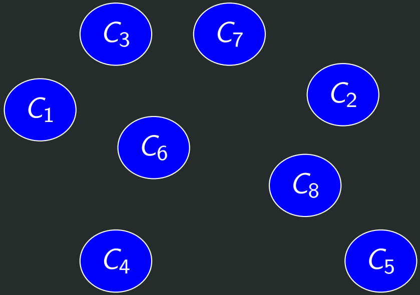
Higher-order constraints



$$x \oplus k^0_{2,0} \in \mathcal{X}_{DDT}(\texttt{0x2}, \texttt{0x5})$$

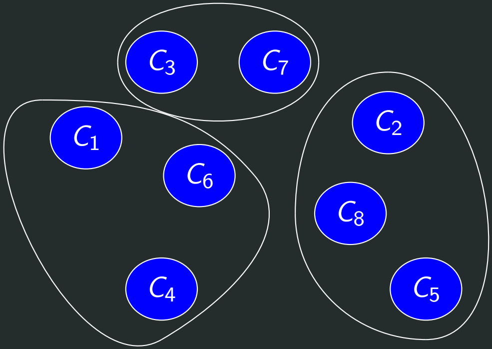
$$x \oplus k^0_{2,0} \oplus y \in \mathcal{X}_{DDT}(\texttt{0x2}, \texttt{0x5}) \text{ where } y \in \mathcal{Y}_{DDT}(\texttt{0xd}, \texttt{0x9})$$

Combining constraints



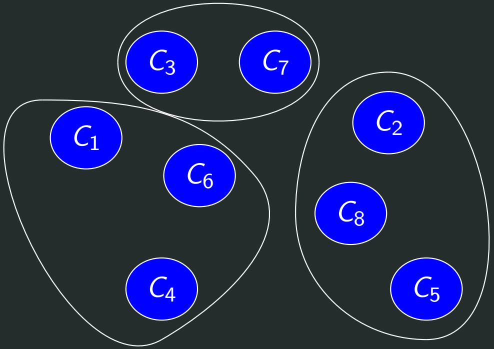
these constraints (may) limit the possible key space and change the probability distribution

Combining constraints



these constraints (may) limit the possible key space and change the probability distribution

Combining constraints



these constraints (may) limit the possible key space and change the probability distribution

C_i and C_j are in the same group if at least one of the following conditions is fulfilled:

- They share at least one key cell (up to key schedule)
- They share at least one Sbox

Optimizing

When the groups are small, we can compute the change in probability distribution

Optimizing

When the groups are small, we can compute the change in probability distribution

- If we are dealing with TK2/TK3, we can split a group further
  - $k_i^n = tk_{i,1}^n \oplus tk_{i,2}^n$

$$k^n \in A \to (k_1^n \oplus k_2^n) \in A$$

$$k^n \in A \rightarrow (k_1^n \oplus k_2^n) \in A$$
$$k^{n+2*r} \in B \rightarrow (k_1^{n+2*r} z \oplus k_2^{n+2*r}) \in B$$
$$= (k_1^n \oplus LFSR^r(k_2^n)) \in B$$

$$k^n \in A \rightarrow (k_1^n \oplus k_2^n) \in A$$

$$k^{n+2*r} \in B \rightarrow (k_1^{n+2*r} z \oplus k_2^{n+2*r}) \in B$$

$$= (k_1^n \oplus LFSR^r(k_2^n)) \in B$$

- LFSR has length 15
- This ensures that within the first 30 rounds, after applying a constraint on the XORed key,

$$k^n \in A \rightarrow (k_1^n \oplus k_2^n) \in A$$
$$k^{n+2*r} \in B \rightarrow (k_1^{n+2*r} z \oplus k_2^{n+2*r}) \in B$$
$$= (k_1^n \oplus LFSR^r(k_2^n)) \in B$$

- LFSR has length 15
- This ensures that within the first 30 rounds, after applying a constraint on the XORed key,
  - All XORed keys are still possible after an application of LFSR
  - The key distribution is uniform

Optimizing

When the groups are small, we can compute the change in probability distribution

- If we are dealing with TK2/TK3, we can split a group further
  - $k_i^n = tk_{i,1}^n \oplus tk_{i,2}^n$
- If only one Sbox is common, we can use a hash-table to record the values/distribution that C_i allows, then use it to compute C_j

Optimizing

When the groups are small, we can compute the change in probability distribution

- If we are dealing with TK2/TK3, we can split a group further
  - $k_i^n = tk_{i,1}^n \oplus tk_{i,2}^n$
- If only one Sbox is common, we can use a hash-table to record the values/distribution that C_i allows, then use it to compute C_j

Otherwise, we can conduct an experimental search

A summary of results for SKINNY

- SKINNY-64

A summary of results for SKINNY

- SKINNY-64
  - 10 out of 21 tested differential characteristics are impossible

A summary of results for SKINNY

- SKINNY-64
  - 10 out of 21 tested differential characteristics are impossible
  - The remaining differential characteristics work for a small key space

A summary of results for SKINNY

- SKINNY-64
  - 10 out of 21 tested differential characteristics are impossible
  - The remaining differential characteristics work for a small key space
  - We can plot the estimated theoretical probability distribution

Prob. in $-\log_2$	35.415	36.415	37	37.415	38	39
Percentage	5.56%	22.2%	5.56%	22.2%	22.2%	22.2%

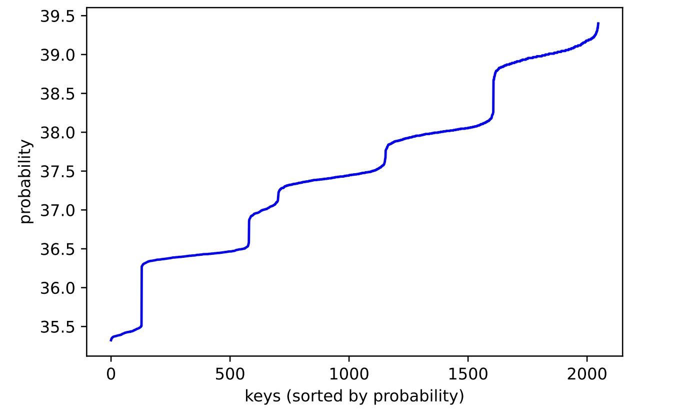


Figure 1: Experimental probability distribution across 2048 random but valid keys

A summary of results for SKINNY

- SKINNY-64
  - 10 out of 21 tested differential characteristics are impossible
  - The remaining differential characteristics work for a small key space
  - We can plot the estimated theoretical probability distribution
- SKINNY-128
  - 11 out of 22 differential characteristics are impossible

A summary of results for SKINNY

- SKINNY-64
  - 10 out of 21 tested differential characteristics are impossible
  - The remaining differential characteristics work for a small key space
  - We can plot the estimated theoretical probability distribution
- SKINNY-128
  - 11 out of 22 differential characteristics are impossible
  - Most of the remaining differential characteristics work with a very small key space

A summary of results for SKINNY

- SKINNY-64
  - 10 out of 21 tested differential characteristics are impossible
  - The remaining differential characteristics work for a small key space
  - We can plot the estimated theoretical probability distribution
- SKINNY-128
  - 11 out of 22 differential characteristics are impossible
  - Most of the remaining differential characteristics work with a very small key space
  - Experimentally determined probability distribution

GIFT [BPP+17]

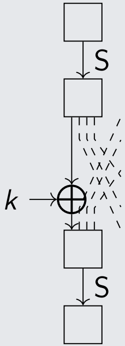


Figure 2: Linear constraint

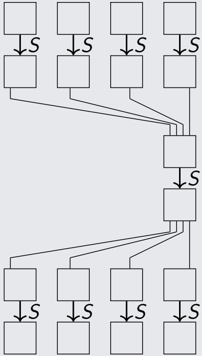


Figure 3: Nonlinear constraints

A summary of results for GIFT

For GIFT-64 and GIFT-128,

A summary of results for GIFT

For GIFT-64 and GIFT-128,

- 1 out of 15 tested differential characteristics is impossible

A summary of results for GIFT

For GIFT-64 and GIFT-128,

- 1 out of 15 tested differential characteristics is impossible
- Most of the remaining tested differential characteristics have key-dependent constraints

Impact on differentials

- Our study focused mainly on differential characteristics.

Impact on differentials

- Our study focused mainly on differential characteristics.
- Even if a differential characteristic is not valid. It does not mean that the differential or (boomerang/rectangle is impossible)

Impact on differentials

- Our study focused mainly on differential characteristics.
- Even if a differential characteristic is not valid. It does not mean that the differential or (boomerang/rectangle is impossible)

However

- Probability of the dominant characteristic may change
- Experiments show that there is a possibility that there is no valid keys for all the differential characteristics in a differential

Integrating with Constraint Programming (CP)

- Looking for right pairs directly might be hard in some scenarios

Integrating with Constraint Programming (CP)

- Looking for right pairs directly might be hard in some scenarios
- Incorporate additional constraints in CP which uses the input and output values of active Sboxes to verify the validity of the propagation.

Thank you for you attention!

References I

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.
In *CRYPTO 2016*, pages 123–153.

S. Banik, S. K. Pandey, T. Peyrin, Y. Sasaki, S. M. Sim, and Y. Todo.
GIFT: A small present - towards reaching the limit of lightweight encryption.
In *CHES 2017*, pages 321–345.

A. Canteaut, E. Lambooij, S. Neves, S. Rasoolzadeh, Y. Sasaki, and M. Stevens.
Refined Probability of Differential Characteristics Including Dependency Between Multiple Rounds.
IACR Trans. Symmetric Cryptol., 2017(2):203–227, 2017.

G. Leurent.
Analysis of Differential Attacks in ARX Constructions.
In *ASIACRYPT 2012*, pages 226–243.

F. Liu, T. Isobe, and W. Meier.
Automatic Verification of Differential Characteristics: Application to Reduced Gimli.
In *CRYPTO 2020*, pages 219–248.

References II

X. Lai, J. L. Massey, and S. Murphy.
Markov ciphers and differential cryptanalysis.
In *EUROCRYPT '91*, pages 17–38.

Y. Liu, W. Zhang, B. Sun, V. Rijmen, G. Liu, C. Li, S. Fu, and M. Cao.
The phantom of differential characteristics.
Des. Codes Cryptogr., 88(11):2289–2311, 2020.

F. Mendel, T. Nad, and M. Schläffer.
Finding SHA-2 Characteristics: Searching through a Minefield of Contradictions.
In *ASIACRYPT 2011*, pages 288–307.

F. Mendel, V. Rijmen, D. Toz, and K. Varici.
Differential Analysis of the LED Block Cipher.
In *ASIACRYPT 2012*, pages 190–207.

I. Nikolic, L. Wang, and S. Wu.
Cryptanalysis of Round-Reduced LED.
IACR Cryptol. ePrint Arch., page 429, 2015.

References III

- S. Sadeghi, V. Rijmen, and N. Bagheri.
  Proposing an MILP-based method for the experimental verification of difference-based trails: application to SPECK, SIMECK.
  Des. Codes Cryptogr., 89(9):2113–2155, 2021.
- L. Sun, W. Wang, and M. Wang.
  More Accurate Differential Properties of LED64 and Midori64.
  IACR Trans. Symmetric Cryptol., 2018(3):93–123, 2018.
- Z. Xu, Y. Li, L. Jiao, M. Wang, and W. Meier.
  Do NOT Misuse the Markov Cipher Assumption - Automatic Search for Differential and Impossible Differential Characteristics in ARX Ciphers.
  Cryptology ePrint Archive, Report 2022/135, 2022.
  `https://ia.cr/2022/135`.