TU Graz

SCIENCE
PASSION
TECHNOLOGY

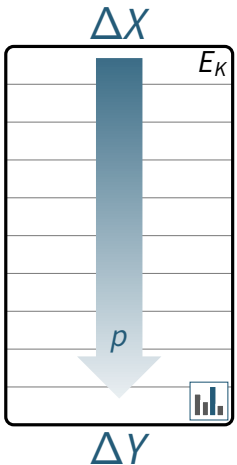
SAT-Based Verification of Differential Characteristics

Marcel Nageler, Shibam Ghosh, Maria Eichlseder

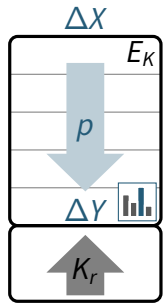
Beating Real Time Crypto 2024 – Lorentz Center, Leiden 

Differential Characteristics

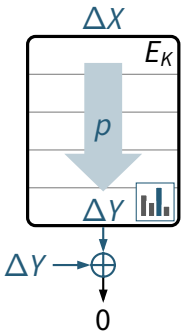
Method



Attack Goals



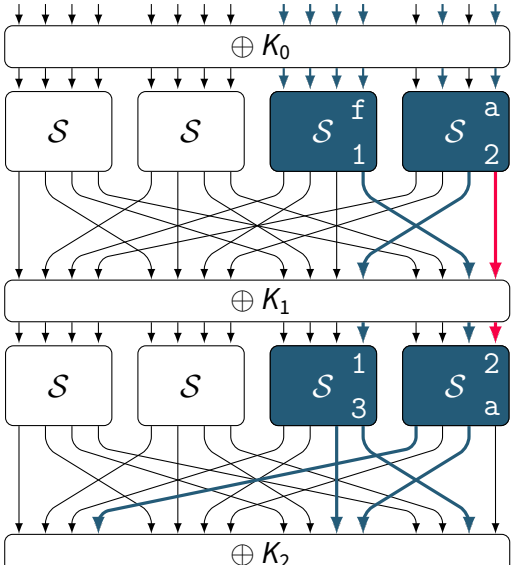
key recovery



collision, forgery

. . .

Key-dependency in a Differential Characteristic



$\mathcal{YDDT}(\mathtt{a}, 2) = \{0, 2\}$

$K_{1,0}$ must be 0

$\mathcal{XDDT}(2, \mathtt{a}) = \{0, 2\}$

Potential Remedies

- Experimental verification
  - Infeasible for low-probability characteristics
- Identifying and checking constraints [PT22]
  - Cumbersome to implement
  - Experimental verification of probability is hard
- SAT-based verification
  - Create simple cipher model in SAT
  - Recover more information about characteristic

Our Tool

- Input
  - Cipher description as CNF
  - Differential Characteristic
- Output
  - Estimated probability averaged over all keys / specific key
  - Estimate number of valid keys
  - Find necessary conditions for valid keys

Creating the Cipher Description

- Encode block cipher as a CNF
  - Linear layer
  - S-boxes
  - Key schedule with round constants
- Active S-boxes need additional constraints
  - Must follow solution set $\{x, y : \mathcal{S}(x) = y \wedge \mathcal{S}(x \oplus \Delta_i) = y \oplus \Delta_o\}$

Applying a SAT Solver

- Use a SAT solver to verify whether any solution exists
  - can detect impossible characteristics
- Solve with a SAT solver for many random keys
  - approximate the number of valid keys
  - SAT Solver might learn clauses over the key

Background: Approximate Model Counting

- We use ApproxMC [SGM20]
- Given tolerance ϵ, confidence δ and a CNF formula F
- output approximate number of solutions c
- $(1+\epsilon)^{-1} \cdot |\mathrm{sol}(F)| \leq c \leq (1+\epsilon) \cdot |\mathrm{sol}(F)|$ with probability $p \geq 1-\delta$

use this to count probability

Counting number of valid keys

- The model counter provides one extra input:
  - the sampling set

  $\rightarrow$ count how many assignments for this subset of variables exist
- use this to count key space

Results

- MIDORI-64 with characteristic [ZHWW20, Fig. 2] ($p = 2^{-52}$)
  - ✔ verify probability = 2^{-52} (11 seconds with $\delta = \epsilon = 0.1$)
  - ✔ estimate key space: 2^{111} (10 seconds with $\delta = \epsilon = 0.1$)
  - ✔ find 17 linear conditions on key bits (2.5 seconds)
- GIFT-64 with characteristic [ZDY18, Table 4] ($p = 2^{-59}$)
  - ✔ estimate key space: 2^{125}
  - ✔ $K_{8,0} = K_{10,0}$, $K_{24,1} = K_{26,1}$, $K_{25,1} = K_{27,1}$ (5 seconds)
- GIFT-64 with characteristic [LWZZ19, Table 2] ($p = 2^{-42}$)
  - ✔ estimate key space: 2^{124} (4 seconds with $\delta = 0.1, \epsilon = 0.1$)
  - ✔ $K_{8,1} = K_{10,1}$, $K_{9,1} = K_{11,1}$, $K_{24,0} = K_{26,0}$, $K_{25,0} = K_{27,0}$ (3 seconds)

Conclusion

- Framework for verification of differential characteristics
- Easily extensible for more ciphers
- Many different use-cases
  - Verify probability for average / fixed key
  - Measure size of key space
  - Find necessary conditions on key bits

Bibliography I

[LWZZ19] Lingchen Li, Wenling Wu, Yafei Zheng, and Lei Zhang. **The Relationship between the Construction and Solution of the MILP Models and Applications.** Cryptology ePrint Archive, Paper 2019/049. https://eprint.iacr.org/2019/049. 2019. URL: https://eprint.iacr.org/2019/049.

[PT22] Thomas Peyrin and Quan Quan Tan. **Mind Your Path: On (Key) Dependencies in Differential Characteristics.** IACR Trans. Symmetric Cryptol. 2022.4 (2022), pp. 179–207. DOI: 10.46586/TOSC.V2022.I4.179-207. URL: https://doi.org/10.46586/tosc.v2022.i4.179-207.

[SGM20] Mate Soos, Stephan Gocht, and Kuldeep S. Meel. **Tinted, Detached, and Lazy CNF-XOR Solving and Its Applications to Counting and Sampling.** Computer Aided Verification - 32nd International Conference, CAV 2020, Los Angeles, CA, USA, July 21-24, 2020, Proceedings, Part I. Vol. 12224. Lecture Notes in Computer Science. Springer, 2020, pp. 463–484. DOI: 10.1007/978-3-030-53288-8_22. URL: https://doi.org/10.1007/978-3-030-53288-8%5C_22.

Bibliography II

[ZDY18] Baoyu Zhu, Xiaoyang Dong, and Hongbo Yu. **MILP-based Differential Attack on Round-reduced GIFT.** Cryptology ePrint Archive, Paper 2018/390. https://eprint.iacr.org/2018/390. 2018. URL: https://eprint.iacr.org/2018/390.

[ZHWW20] Hongluan Zhao, Guoyong Han, Letian Wang, and Wen Wang. **MILP-Based Differential Cryptanalysis on Round-Reduced Midori64.** IEEE Access 8 (2020), pp. 95888–95896. DOI: 10.1109/ACCESS.2020.2995795. URL: https://doi.org/10.1109/ACCESS.2020.2995795.