SCIENCE CHINA Information Sciences

New automatic tool for finding impossible differentials and zero-correlation linear approximations

Tingting CUI[1], Shiyao CHEN[2], Kai FU[4], Meiqin WANG[2] and Keting JIA[3,*]

Citation: SCIENCE CHINA Information Sciences **64**, 129103 (2021); doi: 10.1007/s11432-018-1506-4

View online: https://engine.scichina.com/doi/10.1007/s11432-018-1506-4

View Table of Contents: https://engine.scichina.com/publisher/scp/journal/SCIS/64/2

Published by the Science China Press

SCIENCE CHINA
Information Sciences

• LETTER •

February 2021, Vol. 64 129103:1–129103:3
https://doi.org/10.1007/s11432-018-1506-4

New automatic tool for finding impossible differentials and zero-correlation linear approximations

Tingting CUI[1], Shiyao CHEN[2], Kai FU[4], Meiqin WANG[2] & Keting JIA[3*]

[1]*School of Cyberspace, Hangzhou Dianzi University, Hangzhou* 310018*, China;*
[2]*Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan* 250100*, China;*
[3]*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084*, China;*
[4]*China Academy of Information and Communications Technology, Beijing* 100191*, China*

Received 7 November 2018/Revised 27 March 2019/Accepted 2 August 2019/Published online 27 October 2020

Citation Cui T T, Chen S Y, Fu K, et al. New automatic tool for finding impossible differentials and zero-correlation linear approximations. Sci China Inf Sci, 2021, 64(2): 129103, https://doi.org/10.1007/s11432-018-1506-4

Dear editor,

Impossible differential cryptanalysis and zero-correlation linear cryptanalysis are two powerful methods in the block cipher field. Herein, we present an automatic tool to find impossible differentials (IDs) and zero-correlation linear approximations (ZCLAs) for both ARX and S-box-based ciphers. Similar to the idea of using mixed-integer linear programming (MILP) models for differential cryptanalysis in [1], we first use linear inequalities to describe all the target cipher's components exactly. However, we are indifferent to the objective function and only interested in knowing whether a solution to the whole system of inequalities for given input and output differences (masks) is present. If not, these input and output differences can yield an ID (ZCLA), as expected. Herein, we describe the search process in detail for IDs, but the process for finding ZCLAs is similar.

First, we describe all the target cipher's components exactly using linear inequalities. Herein, we focus on describing the differential patterns for modular addition and omit the linear operation and S-box descriptions [1, 2]. Because we are not interested in the probabilities of each differential pattern for non-linear components, we rewrite the modular addition constraints in terms of eight linear inequalities, about 40% fewer than the number proposed by Fu et al. [2] to search differentials. Assume that there is a differential $(\alpha, \beta \rightarrow \gamma)$ on the modular addition operation. To determine whether this differential is possible, we have two step according to the Theorem 1 in [2].

Firstly, to satisfy the condition on the least significant bit, $\alpha_0 \oplus \beta_0 \oplus \gamma_0 = 0$, we use the following equality:

$$\alpha_0 + \beta_0 + \gamma_0 = 2d_{\oplus},$$

where $d_{\oplus}$ is a dummy bit variable.

Secondly, for each $i \in [1, n-1]$, there are 56 possible patterns for $(\alpha_i, \beta_i, \gamma_i, \alpha_{i+1}, \beta_{i+1}, \gamma_{i+1})$. Herein, we use the following eight linear inequalities, whose solution set comprises exactly these 56 possible patterns.

$$\begin{aligned}
-\alpha_i - \beta_i - \gamma_i + \alpha_{i+1} + \beta_{i+1} + \gamma_{i+1} &\geqslant -2,\\
\alpha_i + \beta_i + \gamma_i - \alpha_{i+1} - \beta_{i+1} - \gamma_{i+1} &\geqslant -2,\\
\alpha_i + \beta_i + \gamma_i + \alpha_{i+1} + \beta_{i+1} - \gamma_{i+1} &\geqslant 0,\\
\alpha_i + \beta_i + \gamma_i + \alpha_{i+1} - \beta_{i+1} + \gamma_{i+1} &\geqslant 0,\\
\alpha_i + \beta_i + \gamma_i - \alpha_{i+1} + \beta_{i+1} + \gamma_{i+1} &\geqslant 0,\\
-\alpha_i - \beta_i - \gamma_i + \alpha_{i+1} - \beta_{i+1} - \gamma_{i+1} &\geqslant -4,\\
-\alpha_i - \beta_i - \gamma_i - \alpha_{i+1} + \beta_{i+1} - \gamma_{i+1} &\geqslant -4,\\
-\alpha_i - \beta_i - \gamma_i - \alpha_{i+1} - \beta_{i+1} + \gamma_{i+1} &\geqslant -4.
\end{aligned}$$

Thirdly, by representing the input and output differences of each target cipher operation using corresponding binary variables and constructing a suitable system of linear inequalities involving these variables, we can exactly describe all possible differential patterns for each operation. Taken together, the complete inequality system perfectly describes the target cipher's differential propagation process, and every solution is a differential characteristic. If the inequality system is infeasible for the given input and output differences, it indicates that the differential is impossible.

By traversing a special set of input/output differences using the MILP model, we can confirm whether there is an ID within the set for a certain reduced-round cipher. Notably, covering all possible input/output differences is difficult owing to the time complexity; thus, this special set must be carefully selected, and it always depends on the features of the given cipher. Without loss of generality, we denote such a set as $(\Delta \rightarrow \Gamma)$, where Δ and Γ are the chosen sets of input and output differences, respectively. Algorithm 1 illustrates how the ID search process is implemented.

Using this new method, we cannot directly identify where the contradiction appears or even determine whether the in-

* Corresponding author (email: ktjia@mail.tsinghua.edu.cn)

Table 1 Summary of results for the HIGHT, SHACAL-2, LEA, and LBlock ciphers

Cipher	Type	Round	Reference
HIGHT	Impossible differential	16	[3]
	Impossible differential	17	[4]
	Impossible differential	17	Ours
	Zero-correlation linear approximation	16	[5]
	Zero-correlation linear approximation	17	[4]
	Zero-correlation linear approximation	17	Ours
SHACAL-2	Zero-correlation linear approximation	12	[6]
	Impossible differential	14	[7]
	Impossible differential	15	Ours
LEA	Zero-correlation linear approximation	7	[8]
	Zero-correlation linear approximation	9	[4]
	Zero-correlation linear approximation	10	Ours
LBlock	Related-key impossible differential[a)]	16	[9]
	Related-key impossible differential	16	Ours

a) indicates that this is only a related-key impossible differential for some master key pairs with the given master key difference.

Algorithm 1 General impossible differential search process

```
// Step 1: Construct the MILP model.
Represent the input and output differences for each operation as binary variables.
Link the binary variables by adding linear inequalities for each target cipher operation.
// Step 2: Find all the impossible differentials within a given set of input and output differences.
Determine the sets of input differences Δ and output differences Γ.
for input difference Δx_i ∈ Δ do
    for output difference Δy_j ∈ Γ do
        Add all constraints related to the current input and output differences to the MILP model.
        Attempt to solve the model.
        if solver found a solution then
            // The current input and output differences represent a possible differential.
            Break;
        else
            // The current input and output differences yield an impossible differential.
            Store the current input and output differences.
        end if
    end for
end for
```

feasible state is caused by a bug in the code. To deal with this issue, we propose a verification approach. Assume that there is an R-round ID for the target cipher. Clearly, if removing certain inequalities from the MILP model indicates that the infeasible model becomes feasible, the contradiction must be related to the variables present in those inequalities. Using this approach, we can find a contradiction between the $(\lceil \frac{R}{2} \rceil)$-th and $(\lceil \frac{R}{2} \rceil + 1)$-th rounds by removing some linked inequalities between these two rounds.

Finally, we apply our new model to the HIGHT, SHACAL-2, LEA, and LBlock ciphers. The results are summarized in Table 1 [3–9]. Actually, this tool is useful in search of IDs and ZCLAs for most ARX ciphers and lightweight block ciphers, more details see Appendixes A and B. Additionally, it can be used in evaluating the security of stream cipher and hash functions as well. However, there are still two problems in this tool to be solved in the future. Firstly, the search for cipher with 8-bit S-box is slow because of lots of linear inequalities to describe such S-box. Secondly, searching all case of target rounds of a cipher is difficult due to the time complexity, how to shrink searching scope to find the longest trail in suitable time is another meanful problem, especially under related-key setting. In the future, we will focus on these problems and improve this tool.

Acknowledgements This work was supported by National Key Research and Development Program of China (Grant No. 2017YFA0303903), National Cryptography Development Fund (Grant Nos. MMJJ20170121, MMJJ20170102), Zhejiang Province Key R&D Project (Grant No. 2017C01062), National Natural Science Foundation of China (Grant Nos. 61572293, 61502276, 61692276), Major Scientific and Technological Innovation Projects of Shandong Province (Grant No. 2017CXGC0704), and National Natural Science Foundation of Shandong Province (Grant No. ZR2016FM22).

Supporting information Appendixes A and B. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Sun S W, Hu L, Wang P, et al. Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES (L) and other bit-oriented block ciphers. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, Taiwan, 2014. 8873: 158–178

2 Fu K, Wang M Q, Guo Y H, et al. MILP-based automatic search algorithms for differential and linear trails for speck.

In: Proceedings of International Workshop on Fast Software Encryption, Bochum, 2016. 9783: 268–288
3 Lu J Q. Cryptanalysis of reduced versions of the HIGHT block cipher from CHES 2006. In: Proceedings of International Conference on Information Security and Cryptology, Seoul, 2007. 4817: 11–26
4 Zhang K, Guan J, Hu B. Automatic search of impossible differentials and zero-correlation linear hulls for ARX ciphers. China Commun, 2018, 15: 54–66
5 Wen L, Wang M Q, Bogdanov A, et al. Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: improved cryptanalysis of an ISO standard. Inf Process Lett, 2014, 114: 322–330
6 Wen L, Wang M Q. Integral zero-correlation distinguisher for ARX block cipher, with application to SHACAL-2. In: Proceedings of Australasian Conference on Information Security and Privacy, Wollongong, 2014. 8544: 454–461
7 Hong S, Kim J, Kim G, et al. Impossible differential attack on 30-round SHACAL-2. In: Proceedings of International Conference on Cryptology in India, New Delhi, 2003. 2904: 97–106
8 Hong D, Lee J-K, Kim D-C, et al. LEA: a 128-bit block cipher for fast encryption on common processors. In: Proceedings of International Workshop on Information Security Applications, Jeju Island, 2013. 8267: 3–27
9 Wen L, Wang M Q, Zhao J Y. Related-key impossible differential attack on reduced-round LBlock. J Comput Sci Technol, 2014, 29: 165–176