SCIENCE CHINA
Information Sciences

• **Supplementary File** •

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*

Appendix A Algorithm to Verify the IDs and ZCLAs

We propose a method to search impossible differentials (IDs) and zero-correlation linear approximations (ZCLAs) by judging whether the model is infeasible or not. However, with this method, we can not directly find out the contradictory place, even we can not judge whether infeasible status is caused by writing wrong code or not. What's more, the contradictions found by this method are often not traditional contradiction between 0 and 1 on a certain bit, but two sets of differences on some bits calculated from input and output differences respectively which have no intersection. So in this section, we propose an algorithm to verify the corretness of IDs and ZCLAs searched by our new tools.

The idea of our new search method for IDs and ZCLAs based on MILP is that the differential propagation on cipher can be exactly described by inequalities system. Specifically, we first set variables on both sides of each operation in the cipher to represent the possible differences, then link them with suitable inequalities system so that the solutions' set of this system is exactly the set of all possible differential patterns. Without loss of generality, assume that there is a R-round impossible differential for the target cipher. Obviously, if we remove some inequalities from its MILP model such that the infeasible model becomes feasible, the contradiction must be happened on the variables existed in those removed inequalities. In our method, we find the contradiction between the $\lceil\frac{R}{2}\rceil$-th and $\lceil\frac{R}{2}\rceil+1$-th rounds[1)], i.e. that consider the contradiction on the input difference of $\lceil\frac{R}{2}\rceil+1$-th round. Based on such observation, we propose a method to verify the IDs and ZCLAs. Take the verification process of an impossible differential as an example, see algorithm 1. So does the verification process for the ZCLA.

To search the related-key impossible differential of a target cipher, the process is similar to that under single key setting, except that the key schedule and conditions on master key should be described into the MILP model. However, note that in the phase of finding out sets A and B, the set of linear inequalities for whole key schedule and constraints on master key must be put into two small models for rounds $1\sim\lceil\frac{R}{2}\rceil$ and rounds $\lceil\frac{R}{2}\rceil+1\sim R$ simultaneously.

Appendix B Applications on HIGHT, SHACAL-2, LEA and LBlock

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

1) Actually, we can find out a contradiction between any two adjacent round functions. However, we believe that the contradictions happen between the $\lceil\frac{R}{2}\rceil$-th and $\lceil\frac{R}{2}\rceil+1$-th rounds are more intuitive and cover less related bits.

Algorithm 1: Verification process of an impossible differential

```
Input: The MILP model of this impossible differential. Assume that the input and output
       differences are $\Delta x_{in}$ and $\Delta x_{out}$ respectively;
Output: The detailed contradiction.
Collect all inequalities linking the $\lceil \frac{R}{2} \rceil$-th and $\lceil \frac{R}{2} \rceil + 1$-th rounds, then put those into a set $\mathbb{I}_{mid}$;
for Each inequality in $\mathbb{I}_{mid}$ do
    Remove the same inequality from the MILP model;
    Solve the new model;
    if The model is infeasible then
        Delete this inequality from set $\mathbb{I}_{mid}$;
        Continue;
    else
        Put this inequality back to MILP model;
Extract all variables corresponding to the input difference of $\lceil \frac{R}{2} \rceil + 1$-th round from remained set
    $\mathbb{I}_{mid}$, and put them into a set $Var_{contradiction}$;
// The contradiction happens on $Var_{contradiction}$.
Output $Var_{contradiction}$;
Set two empty set $A$ and $B$;
for Each possible difference value $\Delta x_{contradiction}$ on $Var_{contradiction}$ do
    if $\Delta x_{in} \rightarrow \Delta x_{contradiction}$ is possible then
        put $\Delta x_{contradiction}$ into set $A$;
    if $\Delta x_{contradiction} \rightarrow \Delta x_{out}$ is possible then
        put $\Delta x_{contradiction}$ into set $B$;
Output sets $A$ and $B$.
```

Round 1	e_7	0	0	0	0	0	0	0
Round 2	0	0	0	0	0	0	0	e_7
Round 3	0	0	0	0	0	nzb	e_7	0
Round 4	0	0	0	nzb	nzb	e_7	0	0
Round 5	0	nzb	nzb	nzb	e_7	0	0	0
Round 6	nzb	?	nzb	e_7	0	0	0	nzb
Round 7	?	nzb	e_7	0	0	nzb	nzb	?
Round 8	nzb	e_7	0	nzb	nzb	?	?	?
Round 9	e_7	nzb	nzb	?	?	?	?	nzb
Round 10	nzb	?	?	?	?	?	nzb	$\neq e_7$
Round 10	?	?	?	?	?	?	nzb	e_7
Round 11	?	?	?	?	?	nzb	e_7	0
Round 12	?	?	?	?	nzb	e_7	0	0
Round 13	?	?	?	nzb	e_7	0	0	0
Round 14	?	nzb	nzb	e_7	0	0	0	0
Round 15	nzb	nzb	e_7	0	0	0	0	0
Round 16	nzb	e_7	0	0	0	0	0	0
Round 17	e_7	0	0	0	0	0	0	0
Round 18	0	0	0	0	0	0	0	e_7

Table B1 17-round impossible differential of HIGHT, where e_7, nzb and ? denote $0x80$, nonzero byte and unknown byte respectively. The byte with red color on the input of round 10 is the contradiction point.

Round 1	0	e_0	0	0	0	0	0	0
Round 2	e_0	0	0	0	0	0	0	0
Round 3	nzb	0	0	0	0	0	0	e_0
Round 4	nzb	0	0	0	0	0	e_0	nzb
Round 5	nzb	0	0	0	0	e_0	?	nzb
Round 6	nzb	0	0	0	e_0	?	?	nzb
Round 7	nzb	0	0	e_0	?	?	?	nzb
Round 8	nzb	0	e_0	?	?	?	?	nzb
Round 9	nzb	e_0	?	?	?	?	?	nzb
Round 10	$\neq e_0$	?	?	?	?	?	?	nzb
Round 10	e_0	?	?	?	?	?	?	?
Round 11	?	?	?	?	?	?	0	e_0
Round 12	?	?	?	?	0	0	e_0	?
Round 13	?	?	0	0	0	e_0	?	?
Round 14	0	0	0	0	e_0	?	?	?
Round 15	0	0	0	e_0	nzb	nzb	0	0
Round 16	0	0	e_0	nzb	0	0	0	0
Round 17	0	e_0	0	0	0	0	0	0
Round 18	e_0	0	0	0	0	0	0	0

Table B2 17-round zero-correlation linear approximation of HIGHT, where e_0, nzb and ? denote $0x01$, nonzero byte and unknown byte respectively. The byte with red color on the input of round 10 is the contradiction point.

Round 1	0	0	0	e_{31}	0	0	0	e_{31}
Round 2	e_{31}	0	0	0	0	0	0	0
Round 3	$e_{9\sim}$	e_{31}	0	0	0	0	0	0
Round 4	-	$e_{9\sim}$	e_{31}	0	0	0	0	0
Round 5	-	-	$e_{9\sim}$	e_{31}	0	0	0	0
Round 6	-	-	-	$e_{9\sim}$	e_{31}	0	0	0
Round 7	-	-	-	-	$e_{6\sim}$	e_{31}	0	0
Round 8	-	-	-	-	-	$e_{6\sim}$	e_{31}	0
Round 8	-	-	-	-	-	$e_{9\sim}$	-	-
Round 9	-	-	-	-	-	-	$e_{9\sim}$	-
Round 10	e_{31}	$*_{31}$	$*_{31}$	$e_{9\sim}$	0	$*_{31}$	$*_{31}$	$e_{9\sim}$
Round 11	0	e_{31}	$*_{31}$	$*_{31}$	0	0	$*_{31}$	$*_{31}$
Round 12	0	0	e_{31}	$*_{31}$	0	0	0	$*_{31}$
Round 13	0	0	0	e_{31}	0	0	0	0
Round 14	0	0	0	0	e_{31}	0	0	0

Table B3 13-round impossible differential of SHACAL-2, where $e_{i\sim}$ denotes that the i-th bit is 1 and the least significant i bits are all 0, e_{31} ($*_{31}$) denotes that the most significant bit is 1 (unknown) while other bits are all 0, and "-" denotes uncertained word. The word with red color on the input of round 8 is the contradiction point.

Round 0	0	e_0	0	0	Round 5	$e_{\sim 8}$	$e_{\sim 15}$	$e_{\sim 15}$	$e_{\sim 12}$
Round 1	e_9	0	0	e_0	Round 6	0	$e_{\sim 10}$	$e_{\sim 10}$	$e_{\sim 8}$
Round 2	e_9	e_{27}	e_{29}	$e_{9,0}$	Round 7	0	$e_{\sim 5}$	$e_{\sim 5}$	0
Round 3	-	-	-	$e_{\sim 29}$	Round 8	0	e_0	0	0
Round 4	-	-	$?^3001?^{26}$	-	Round 9	e_9	0	0	e_0
Round 4	-	-	$e_{\sim 20}$	$e_{\sim 18}$	Round 10	e_9	e_{27}	e_{29}	$e_{9,0}$

Table B4 10-round zero-correlation linear approximation of LEA. $e_{i,j}$ denotes that only the i-th and j-th bits are 1, other bits are all 0. $e_{\sim i}$ denotes the i-th bit is 1 while the most significant $31 - i$ bits are all 0. $?^l$ denotes l unknown bits. The word with red color on the input of round 4 is the contradiction point.

Round	Input (left)	Input (right)	Subkey	Round	Input (left)	Input (right)	Subkey
1	0000 0000	0000 0000	0000 0000	9	???? ?*??	???? ????	0*00 0000
2	0000 0000	0000 0000	0000 0000	10	*?0? ???*	???? ?*??	0000 0000
3	0000 0000	0000 0000	0000 0400	11	?0?* **00	*?0? ???*	0000 00?*
4	0000 *000	0000 0000	0000 0000	12	0?*0 ?000	?0?* **00	*000 0000
5	0000 00*0	0000 *000	0000 0000	13	?*00 00?0	0?*0 ?000	0000 0000
6	00*0 000*	0000 00*0	0002 0000	14	0000 0000	?*00 00?0	0000 ??*0
7	0*0* **00	00*0 000*	0000 0000	15	0000 0000	0000 0000	0000 0000
8	?*00 ***0	0*0* **00	0000 0000	16	0000 0000	0000 0000	0000 0000
9	**?* *0*?	?*00 ***0	0*00 0000	17	0000 0000	0000 0000	0000 0000

Table B5 16-round related-key impossible differential of LBlock. "*" and "?" denotes nonzero nibble and unknown nibble respectively. The nibble with red color on the input of round 9 is the contradiction point.