SCIENCE CHINA
Information Sciences

• HIGHLIGHT •

March 2018, Vol. 61 038103:1–038103:3
doi: 10.1007/s11432-016-9104-3

Improved automatic search of impossible differentials for camellia with FL/FL^{-1} layers

Yaoling DING[1], Xiaoyun WANG[2,3,4*], Ning WANG[3,4] & Wei WANG[3,5]

[1]*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084*, China;*
[2]*Institute for Advanced Study, Tsinghua University, Beijing* 100084*, China;*
[3]*Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan* 250100*, China;*
[4]*School of Mathematics, Shandong University, Jinan* 250100*, China;*
[5]*School of Computer Science and Technology, Shandong University, Jinan* 250100*, China*

Received 4 February 2017/Revised 19 April 2017/Accepted 16 May 2017/Published online 23 August 2017

Citation Ding Y L, Wang X Y, Wang N, et al. Improved automatic search of impossible differentials for camellia with FL/FL^{-1} layers. Sci China Inf Sci, 2018, 61(3): 038103, doi: 10.1007/s11432-016-9104-3

Camellia is an international standard adopted by ISO/IEC and is recommended by CRYPTREC and NESSIE project. Wu et al. [1] presented an effective tool to search truncated impossible differentials for word-oriented block ciphers with bijective Sboxes. However, their method only adopted Sbox as the nonlinear part and cannot be applied to Camellia with FL/FL^{-1} layers. We discover the difference propagation of three basic components employed in the FL/FL^{-1} layers, i.e., AND, OR, ROTATION operations, and generalize the automatic search to consider more nonlinear operations. Using this system, we search for impossible differentials of round-reduced Camellia with FL/FL^{-1} layers. Moreover, by some changes in the nonlinear subsystem, our algorithm can be easily adjusted to be compatible with searching for impossible differentials which are with restrictions on input/output differences or subkeys. Table 1 summaries our searching results and compares them with the previous results. In order to demonstrate that our algorithm is effective, we launch an impossible differential attack on 14-round Camellia-256 with FL/FL^{-1} layers using the new impossible differential obtained by our algorithm. Compared to the previous best attack achieved by Boura et al. [6], our attack improves the time and memory complexity a lot.

Brief description of Camellia. Camellia [7] is a 128-bit block cipher with variable key lengths of 128, 192 and 256, which can be denoted as Camellia-128/192/256, and the corresponding numbers of round r are 18/24/24. For Camellia-192/256, the 128-bit input is divided into two 64-bit values L^0 and R^0. Then, for $i = 1$ to 24, except for $i = 6$, 12 and 18, the round function is $L^i = R^{i-1} \oplus F(L^{i-1}, k^i)$ $R^i = L^{i-1}$. While, for $i =$

Table 1 Summary of impossible differentials (IDs) of Camellia with FL/FL^{-1} layers[a)]

# FL/FL^{-1}	Pos	L	Previous results		This article
			# IDs	Source	# IDs
1	6	7	4	[2]	120
	5	7	4	[3]	16
	5	7	–	–	32
2	0, 6	7	–	–	52
	0, 6	7	4	[4]	12
	1, 7	7	4	[5]	12
	1, 7	8	4	[3]	16

a) Pos: the position of FL/FL^{-1} layers, 0 stands for the IDs with FL/FL^{-1} layers before round 1. L: the length of the impossible differentials.

* Corresponding author (email: xiaoyunwang@mail.tsinghua.edu.cn)
The authors declare that they have no conflict of interest.

6,12,18, the round function performs one more layer, FL/FL^{-1} layer, which is defined as $L^{i'} = R^{i-1} \oplus F(L^{i-1}, k^i)$, $R^{i'} = L^{i-1}$, $L^i = FL(L^{i'}, kf_L, kf_R)$, $R^i = FL^{-1}(R^{i'}, kf_L, kf_R)$. FL function does $(X_{L(32)} \parallel X_{R(32)}, kf_{L(32)} \parallel kf_{R(32)}) \mapsto (Y_{L(32)} \parallel Y_{R(32)})$, where $Y_{R(32)} = ((X_{L(32)} \cap kl_{L(32)}) \lll 1) \oplus X_{R(32)}$, $Y_{L(32)} = (Y_{R(32)} \cup kl_{R(32)}) \oplus X_{L(32)}$. The FL^{-1} function is the inverse of FL. Before the first round and after the last round, there are whitening-key layers, which is omitted in the following cryptanalysis.

Automatic search of impossible differentials. The basic idea of Wu et al.'s method is to treat a cipher as an entirety instead of the miss-in-the-middle approach, and build the difference propagation system according to the encryption/decryption function. The system takes the plaintext/ciphertext differences as the initial information, and predicts information about unknown variables from the known ones iteratively with probability one. Once there is a contradiction, an impossible differential trail is obtained and the iteration is over. To build a difference propagation system, Wu et al. presented the difference propagation of four basic primitives, i.e., branch, xor, Sbox and linear operations which are often employed as parts of a block cipher.

For Camellia, the FL/FL^{-1} layers bring new differential propagation properties which makes it hard to apply Wu et al.'s method. Since the components of FL/FL^{-1} layers are AND-operation, ROTATION-operation and OR-operation with unkown keys, we treat these operations as non-linear operations. Suppose Δx, Δy and Δz are row vectors in $\mathbb{F}_{2^8}$. Then, the equations to define the difference propagation of these non-linear operations are as follows, which can be easily proved.

Proposition 1. The AND operation in FL/FL^{-1} layers is described as $\Delta x \cap k = \Delta y$. $\Delta x = 0$ is a sufficient but not necessary condition for $\Delta y = 0$, and $\Delta y \neq 0$ is a sufficient but not necessary condition for $\Delta x \neq 0$. We build a formal equation $\overline{A}(\Delta x, \Delta y) = 0$ to indicate this relation between Δx and Δy.

Proposition 2. The bitwise ROTATION operation in FL/FL^{-1} layers is described as $\Delta(x_0||x_1||x_2||x_3) \lll 1 = \Delta(y_0||y_1||y_2||y_3)$. $\Delta x_i = 0$ and $\Delta x_{(i+1)\bmod 4} = 0$ are sufficient but not necessary conditions for $\Delta y_i = 0$. $\Delta y_{(i-1)\bmod 4} = 0$ and $\Delta y_i = 0$ are sufficient but not necessary conditions for $\Delta x_i = 0$. We build 8 formal equations $\overline{R}(\Delta x_i, \Delta x_{(i+1)\bmod 4}, \Delta y_i) = 0$, $\overline{R}(\Delta y_{(i-1)\bmod 4}, \Delta y_i, \Delta x_i) = 0$ $(i = 0, 1, 2, 3)$ to indicate these relations between Δx_i and Δy_i.

In order to simplify the expression of the equations, we consider the AND and the ROTATION operations together, and obtain Proposition 3.

Proposition 3. For the AND-ROTATION operation, only half of the property of the AND operation and the ROTATION operation are used, that is to say, $\Delta x_i = 0$ and $\Delta x_{(i+1)\bmod 4} = 0$ are sufficient but not necessary condition for $\Delta y_i = 0$. We build 4 formal equations $\overline{AR}(\Delta x_i, \Delta x_{(i+1)\bmod 4}, \Delta y_i) = 0$ $(i = 0, 1, 2, 3)$ to indicate these relations between the input and output differences of the AND-ROTATION operation.

Proposition 4. The OR operation in FL/FL^{-1} layers is described as $\Delta x \oplus (\Delta x \cap k) = \Delta z$. Denote $\Delta y = \Delta x \cap k$, then we can demonstrate it by a linear equation and a formal equation defined in the AND-operation, which are $\Delta x \oplus \Delta y \oplus \Delta z = 0$ and $\overline{A}(\Delta x, \Delta y) = 0$.

To sum up, the difference propagation of the three basic components of FL/FL^{-1} layers can be expressed by one linear equation and two formal equations. We denote the input differences of the FL and FL^{-1} after the i-th round as $\Delta L^{i'}$ and $\Delta R^{i'}$, and their output differences as ΔL^i and ΔR^i. We introduce ΔY^{Li} and ΔY^{Ri} to denote the intermediate differences of FL and FL^{-1}, respectively. $\Delta Y^{Li}_{0\sim 3}$ and $\Delta Y^{Ri}_{0\sim 3}$ represent the differences after the AND-ROTATION operation, and $\Delta Y^{Li}_{4\sim 7}$ and $\Delta Y^{Ri}_{4\sim 7}$ stand for the differences of the non-linear part of the OR operation. We get the difference propagation of FL as follows with $1 \leqslant i \leqslant r$ and $0 \leqslant j \leqslant 3$:

$$\begin{cases} \overline{AR}(\Delta {L^{i'}}_j, \Delta {L^{i'}}_{(j+1)\bmod 4}, \Delta Y^{Li}_j) = 0, \\ \Delta Y^{Li}_j \oplus \Delta {L^{i'}}_{j+4} \oplus \Delta L^i_{j+4} = 0, \\ \overline{A}(\Delta L^i_{j+4}, \Delta Y^{Li}_{j+4}) = 0, \\ \Delta Y^{Li}_{j+4} \oplus \Delta L^i_{j+4} \oplus \Delta {L^{i'}}_j \oplus \Delta L^i_j = 0. \end{cases}$$

Similarly, the difference propagation system of FL^{-1} is

$$\begin{cases} \overline{A}(\Delta {R^{i'}}_{j+4}, \Delta Y^{Ri}_{j+4}) = 0, \\ \Delta {Y^{Ri}}_{j+4} \oplus \Delta {R^{i'}}_{j+4} \oplus \Delta {R^{i'}}_j \oplus \Delta R^i_j = 0, \\ \overline{AR}(\Delta R^i_j, \Delta R^i_{(j+1)\bmod 4}, \Delta {Y^{Ri}}_j) = 0, \\ \Delta Y^{Ri}_j \oplus \Delta {R^{i'}}_{j+4} \oplus \Delta R^i_{j+4} = 0. \end{cases}$$

We build the difference propagation system as described in [1], except that we add the equations of FL/FL^{-1} into it. The system is divided into linear subsystem $\mathcal{L}$ and non-linear subsystem $\mathcal{NL}$. $\mathcal{L}$ is treated as a homogeneous linear system $A\boldsymbol{x} = 0$, where A is the coefficient matrix, and $\boldsymbol{x}$ is the vector of all variables in the difference propagation system. A can be processed by Gauss-Jordan Elimination algorithm to an equivalent Reduced Echelon Form, then the solution set

is decided according to the linear algebra. For $\mathcal{NL}$, different operations are treated, respectively. The details are in the following manner:

• AND-operation. Suppose Δx_i and Δy_i represent the input and output differences of the AND operation, and $\mathcal{T}_{\text{and}}$ indicates a table for the AND operation which stores $(\Delta x_i, \Delta y_i)$. Then for each record in $\mathcal{T}_{\text{and}}$, Λ_0 and Λ_1 are updated by Proposition 1: If $\Delta x_i \in \Lambda_0$, then $\Lambda_0 = \Lambda_0 \cup \Delta y_i$, and the corresponding column of A is updated to zero; If $\Delta y_i \in \Lambda_1$, $\Lambda_1 = \Lambda_1 \cup \Delta x_i$.

• AND-ROTATION operation. Suppose $(\Delta x_0, \Delta x_1, \Delta x_2, \Delta x_3)$ and $(\Delta y_0, \Delta y_1, \Delta y_2, \Delta y_3)$ are the input and output differences of AND-ROTAION operation, and $\mathcal{T}_{\text{androt}}$ indicates a table for the AND-ROTATION operation where we store $(\Delta x_i, \Delta x_{(i+1)\text{mod}4}, \Delta y_i)$. Then for each record in $\mathcal{T}_{\text{androt}}$, $(A, \Lambda_0, \Lambda_1)$ are updated by Proposition 3: If $\Delta x_i \in \Lambda_0$, $\Delta x_{(i+1)\text{mod}4} \in \Lambda_0$ $(i = 0, 1, 2, 3)$, then $\Lambda_0 = \Lambda_0 \cup \Delta y_i$ $(i = 0, 1, 2, 3)$, and the corresponding column of A is updated to zero.

• Sbox operation. This operation has been considered in Wu et al.'s work, so we omit it here.

Internal difference prediction with restrictions. Some analysis results of Camellia with FL/FL^{-1} layers are based on weak keys or with restrictions on input/output differences of FL/FL^{-1} layers. We analyze the properties presented in [3,4,8], and adjust our algorithm to be compatible with these restrictions by some changes in the algorithm.

We generalize Property 2 in [4] and Proposition 3 in [3] to Proposition 5.

Proposition 5. Suppose $(\Delta x_0, \ldots, \Delta x_7)$ and $(\Delta y_0, \ldots, \Delta y_7)$ are the input and output differences of the FL function, if $\Delta x_i = 0$ and the most significant bit of $kf_{L(i+1)\text{mod}4}$ (or $x_{(i+1)\text{mod}4}$) is zero, then we have $\Delta y_{i+4} = \Delta x_{i+4}$, $0 \leqslant i \leqslant 3$.

We can update $(A, \Lambda_0, \Lambda_1)$ by building a table $\mathcal{T}_{wk}$ to locate the weak keys (or the input/output differences with restrictions) and to guide the AND-ROTATION predicting procedure. The details are: If $\Delta x_{(i+1)\text{mod}4} \in \mathcal{T}_{\text{wk}}$ and $\Delta x_i \in \Lambda_0$ $(i = 0, 1, 2, 3)$, then $\Lambda_0 = \Lambda_0 \cup \Delta y_i$ $(i = 0, 1, 2, 3)$, and the corresponding column of A is updated to zero. If $\Delta x_{(i+1)\text{mod}4} \notin \mathcal{T}_{\text{wk}}$ and $\Delta x_i \in \Lambda_0$, $\Delta x_{(i+1)\text{mod}4} \in \Lambda_0$ $(i = 0, 1, 2, 3)$, then $\Lambda_0 = \Lambda_0 \cup \Delta y_i$ $(i = 0, 1, 2, 3)$, and the corresponding column of A is updated to zero.

The Observation 1 in [8] and the Proposition 4 in [3] can be programmed by building tables similarly.

Impossible differential attack on Camellia-256 reduced to 14 rounds. Using the new automatic search tool, we get a new distinguisher of 7-round Camellia with two FL/FL^{-1} layers before rounds 1 and 7, shown in Proposition 6.

Proposition 6. For 7-round Camellia with two FL/FL^{-1} layers before the 1st round and the 7th round, $[(0,0,0,0,0,0,0,0), (a,0,0,0,0,0,0,0)]$ is the input difference, where a is any non-zero value with the most significant bit being zero, then the output difference after 7-round cannot be $[(d,0,0,0,0,0,0,0), (0,0,0,0,0,0,0,0)]$, where d is any non-zero value with the most significant bit being zero.

Based on this impossible differential, we launch the impossible differential attack on 14-round Camellia-256 by adding 3 rounds at the top and appending 4 rounds at the bottom, which needs $2^{120.5}$ chosen plaintexts, $2^{205.7}$ encryptions and 2^{117} memory.

Acknowledgements This work was supported by National Basic Research Program of China (973 Program) (Grant No. 2013CB834205), National Natural Science Foundation of China (Grant No. 61402256) and Zhejiang Province Key R & D Project (Grant No. 2017C01062).

References

1 Wu S, Wang M. Automatic search of truncated impossible differentials for word-oriented block ciphers. In: Proceedings of International Conference on Cryptology in India, Kolkata, 2012. 283–302
2 Chen J. Cryptanalysis of several block ciphers. Dissertation for Ph.D. Degree. Jinan: Shandong Univercity, 2012
3 Liu Y, Li L, Gu D, et al. New observations on impossible differential cryptanalysis of reduced-round Camellia. In: Proceedings of the 19th International Conference on Fast Software Encryption, Washington, 2012. 90–109
4 Bai D, Li L. New impossible differential attacks on camellia. In: Proceedings of International Conference on Information Security Practice and Experience, Hangzhou, 2012. 80–96
5 Blondeau C. Impossible differential attack on 13-round Camellia-192. Inf Process Lett, 2015, 115: 660–666
6 Boura C, Naya-Plasencia M, Suder V. Scrutinizing and improving impossible differential attacks: applications to CLEFIA, Camellia, LBlock and Simon. In: Advances in Cryptology — ASIACRYPT. Berlin: Springer, 2014. 8873: 179–199
7 Aoki K, Ichikawa T, Kanda M, et al. Camellia: a 128-bit block cipher suitable for multiple platforms design and analysis. In: Proceedings of International Workshop on Selected Areas in Cryptography, Ontario, 2000. 39–56
8 Li L, Jia K, Wang X, et al. Meet-in-the-middle technique for truncated differential and its applications to CLEFIA and camellia. In: Proceedings of International Workshop on Fast Software Encryption, Istanbul, 2015. 48–70