SCIENCE CHINA
Information Sciences

• LETTER •

March 2021, Vol. 64 139103:1–139103:3
https://doi.org/10.1007/s11432-018-9798-8

Key-dependent cube attack on reduced Frit permutation in Duplex-AE modes

Lingyue QIN[1], Xiaoyang DONG[1], Keting JIA[2*] & Rui ZONG[1]

[1]*Institute for Advanced Study, Tsinghua University, Beijing* 100084, *China;*
[2]*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*

Received 26 November 2018/Accepted 14 February 2019/Published online 1 February 2021

Citation Qin L Y, Dong X Y, Jia K T, et al. Key-dependent cube attack on reduced Frit permutation in Duplex-AE modes. Sci China Inf Sci, 2021, 64(3): 139103, https://doi.org/10.1007/s11432-018-9798-8

Dear editor,

Recently, the permutation-based cryptology becomes a good topic in symmetric-key research groups. Many dedicated ciphers are permutation-based, and researchers introduced lots of cryptographic permutations which were suitable for different applications (collision-resistant hashing, preimage-resistant hashing, message authentication, message encryption, etc.). Frit (fault-resistant iterative transformation) is a new lightweight 384-bit cryptographic permutation proposed by Simon et al. [1] recently. Dobraunig et al. [2] first studied the Frit cipher against algebraic attacks and gave some key-recovery attacks on Frit in EM constructions. In the end of their study, they left an open problem that if Frit is used in MonkeyDuplex [3] construction (denoted as Frit-AE, i.e., Frit-based authenticated encryption), what is the security level of Frit-AE against the algebraic attacks, such as cube-like or conditional cube attacks. In this study, we focus on this open question.

We first give the brief description that the possible implementations of Frit with MonkeyDuplex. We place the 16-round Frit in the initialization phase, whose input is a 384-bit concatenation of 128-bit key (one limb) and 256-bit nonce (two limbs). Then, a 128-bit limb is XORed with 128-bit plaintext and output 128-bit ciphertext. Since there are three limbs (a, b, c) in the state of Frit, we denote nine possible versions as Frit_α^β-AE, where $\alpha, \beta \in \{a, b, c\}$ indicate the limb positions of 128-bit key and 128-bit ciphertext, respectively.

At EUROCRYPT 2017, Huang et al. [4] introduced conditional cube attacks on Keccak sponge function. Then, several cube-like attacks [5–8] were proposed on permutation based AE schemes, i.e., Ketje, Keyak and Ascon. By exploring bit conditions involving both public bits and key bits, they could reduce the diffusion of cube variables. We introduce new key-dependent cube attacks, which also exploit cube testers with constraints similar to [4]. However, the difference is that the new attacks only consider the conditions which only involve secret key bits. In our attacks on Frit_α^β-AE, we find many different cube testers for different key-dependent bit conditions with the help of MILP (mixed-integer linear programming) method. So we could detect many key-dependent equations by exploring different cube testers. Based on this idea, we give round-reduced attacks on all nine versions of Frit_α^β-AE, which are summarised in Table 1.

Table 1 Summary of cryptanalysis results

α	β	Attacked round	Time complexity
a	a	9	2^{29}
	b	10	2^{29}
	c	9	2^{29}
b	a	8	2^{29}
		9	2^{42}
		10	2^{63}
		11	2^{97}
	b	9	2^{29}
		10	2^{42}
		11	2^{63}
		12	2^{97}
	c	8	2^{29}
		9	2^{42}
		10	2^{63}
		11	2^{97}
c	a	10	2^{29}
	b	11	2^{29}
	c	10	2^{29}

Brief description of Frit and algebraic property. Frit operates on a state of three limbs a, b, c in $\{0,1\}^{128}$ updated in 16 rounds. Each round the state is updated in 6 bitwise operations: the round constant addition, a mixing operation σ_a of limb a, the only nonlinear operation $\odot$ used as a Toffoli gate, a mixing operation σ_c of limb c, a switch operation and a transposition.

The only nonlinear operation of Frit is a bitwise $\odot$, so the round function's degree is 2. Let Frit_r denote the r-round Frit and $(a_r, b_r, c_r) = \text{Frit}_1(a_{r-1}, b_{r-1}, c_{r-1}) = \text{Frit}_r(a_0, b_0, c_0)$. We obtain the properties that $\deg a_r \leqslant \deg a_{r-1} + \deg b_{r-1}$, $\deg b_r = \deg a_{r-1}$ and $\deg c_r \leqslant \deg a_r$.

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

Setting $\deg a_0 = \deg b_0 = \deg c_0 = 1$, we observe that the degrees of a_r, b_r, c_r follow the Fibonacci sequence $F_r = F_{r-1} + F_{r-2}$ ($F_0 = 0, F_1 = 1$). By induction we deduce that $\deg a_r \leqslant F_{r+2}$, $\deg c_r \leqslant F_{r+2}$, $\deg b_r \leqslant F_{r+1}$.

Key-dependent cube attack. In Frit$_\alpha^\beta$-AE, the initialization phase produces l-bit output. Each of the output bits is written as a polynomial $f_i(k_0, \ldots, k_{n-1}, v_0, \ldots, v_{m-1})$, $i = 0, 1, \ldots, l-1$. Choose a common cube C_T, e.g., $(v_0, \ldots, v_{s-1})$, $1 \leqslant s \leqslant m$, then $f_i = T \cdot P_i + Q_i$, $i = 0, 1, \ldots, l-1$. In our key-dependent cube attack, a common divisor of all P_i is found, which is a polynomial $g(k_0, \ldots, k_{n-1})$ that only involves some key bits. Then the cube sum of f_i over all values of the cube C_T is $P_i = g(k_0, \ldots, k_{n-1}) \cdot P_i'$.

We introduce the cube tester, which has the Property 1 and Assumption 1.

Property 1. If at least one nonzero cube sum occurs among the cube sums of f_i ($i \in \{0, 1, \ldots, l-1\}$), we will determine that $g = 1$. It is guaranteed to be right.

Assumption 1. If the cube sums of f_i ($i \in \{0, 1, \ldots, l-1\}$) all equal to 0, we will determine that $g = 0$. Note that, in a random oracle, $g = 0$ is wrong with probability of 2^{-l}, because P_i' is zero with probability of about $\frac{1}{2}$.

With the help of MILP method, we could find many different key-dependent gs corresponding to different cubes, which are all linear with key bits. At last, we could recover the full key by solving a set of linear equations on key bits.

Attacks on Frit$_a^b$-AE. The cipher Frit$_a^b$-AE sets the 128-bit key K to limb a_0 and the 256-bit nonce to limbs b_0 and c_0. We give a 3-round initial structure by keeping the limb b_0 to constants 0 and setting variable vector $\sigma_c^{-1}\sigma_a^{-1}(v)$ to limb c_0. After 2-round Frit the output expressions of a_2, b_2, c_2 are linear with v. To linearize the output expressions of a_3, c_3, the expression $b_2 \odot b_3 = \sigma_a\sigma_c(\sigma_a(K) \odot v + \sigma_a^{-1}(v)) \odot v$ should not involve quadratic terms.

We notice that the mixing operation σ_a^{-1} is much more complicated than σ_a, where σ_a^{-1} has 65 rotations but σ_a only has 3 rotations. Both the mixing operations σ_a and σ_c can be regarded as cyclic matrices, which are also commutative matrices. So it is clear that

$$\begin{aligned} b_2 \odot b_3 &= \sigma_a\sigma_c(\sigma_a(K) \odot v + \sigma_a^{-1}(v)) \odot v \\ &= \sigma_a\sigma_c(\sigma_a(K) \odot v) \odot v + \sigma_c\sigma_a(\sigma_a^{-1}(v)) \odot v \\ &= \sigma_a\sigma_c(\sigma_a(K) \odot v) \odot v + \sigma_c(v) \odot v. \end{aligned}$$

Without the complicated mixing operation σ_a^{-1}, it's easier to guarantee there are no quadratic terms in $b_2 \odot b_3 = \sigma_a\sigma_c(\sigma_a(K) \odot v) \odot v + \sigma_c(v) \odot v$. We use MILP method to find as many variables v as possible, which does not multiply with each other. This method was first introduced by Li et al. [6] to attack Keccak based ciphers. In our MILP model, each variable v_i ($i \in [0, 127]$) is assigned with a variable $x_i \in \{0, 1\}$. Then the case $x_i = 1$ represents that v_i can be chosen as a cube variables candidate. We generate the constraints set CF of $\{x_i\}$ to guarantee there are no quadratic terms in a_3, c_3. For each term v_iv_j in expression $\sigma_a\sigma_c(\sigma_a(K) \odot v) \odot v + \sigma_c(v) \odot v$, if the coefficient $g_{i,j}(K)$ of v_iv_j ($i \neq j$) is not 0, we add a constraint $x_i + x_j \leqslant 1$ to CF.

Then our problem is modeled into a binary linear programming problem

$$\text{Maximize} \sum_{i=0}^{127} x_i$$

$$\text{s.t. } AX \leqslant b,\ X = \{x_i | x_i \in \{0, 1\}, 0 \leqslant i \leqslant 127\},$$

where the $AX \leqslant b$ describe the constraints set CF. Using the Gurobi optimizer to solve the problem, we get the variable set S, in which every variable v_i does not multiply with each other. The output limbs a_3 and c_3 are linear by assigning the other variables to constants 0. When setting one variable $v_j \notin S$ to be a cube variable and carefully choosing the other cube variables from S, we can get only one quadratic term $g_{i,j}(K)v_iv_j$ ($v_i \in S$) in a_3 and c_3, where $g_{i,j}(K)$ is linear function over key bits.

Adding r-round after the 3-round initial structure, we use the $d = (F_{r+1} + 1)$-dimension cube testers to attack the $(r+3)$-round Frit$_a^b$-AE. If $g_{i,j}(K) = 0$, the expressions of a_3, b_3 and c_3 are linear, and the degree of b_{r+3} is F_{r+1}. Otherwise, the expression of b_{r+3} has terms of degree $F_{r+1} + 1$, which must involve $g_{i,j}(K)v_iv_j$. By calculating the cube sums of all bit positions of the output limb after $(r+3)$-round Frit, the two cases $g_{i,j}(K) = 0$ and $g_{i,j}(K) = 1$ can be distinguished according to Property 1 and Assumption 1. By testing different cube testers we can get 128 linearly independent bit conditions and solve the set of equations to recover the 128-bit key. The time complexity of recovering the 128-bit key is $2^d \times 2^7 = 2^{7+d}$ (The time to solving the linear system can be omitted).

Finally, we could get a key-recovery attack on 10-round Frit$_a^b$-AE with $d = 22$. The time complexity is 2^{29}. The cube indexes are {0, 1, 4, 7, 8, 15, 16, 23, 30, 31, 38, 39, 45, 46, 53, 60, 61, 68, 69, 75, 76, 83}, with $g = K_4 + K_{91} + K_{114}$. Note that choosing different indexes, we could get more cubes with different gs.

Attacks on Frit$_b^b$-AE. In Frit$_b^b$-AE, the 128-bit key K is put in limb b_0 and the 256-bit nonce is put in limbs a_0 and c_0. Setting variable vector v' to limb a_0 and $\sigma_c^{-1}\sigma_a^{-1}(v)$ to limb c_0, we get a 2-round initial structure for Frit$_b^b$-AE. To linearize a_2 and c_2, we need to keep that the expression $b_1 \odot b_2 = \sigma_a(v') \odot v + \sigma_a(v') \odot \sigma_a\sigma_c(K \odot \sigma_a(v'))$ does not have quadratic terms.

By our observation, let cube variables set $C_i = \{v_i', v_{i+1}', v_{j_0}, \ldots, v_{j_{d-3}}\}$[1)], where set $\{j_0, \ldots, j_{d-3}\}$ does not have any elements of $\{i, i+18, i+41, i+1, i+19, i+42\}$. Assigning the other variables of v, v' except for the cube C_i to constants, we find the only quadratic term of a_2, c_2 is $K_{i+1}v_i'v_{i+1}'$. Adding r-round after the 2-round initial structure, we try to attack the $(r+2)$-round Frit$_b^b$-AE with $d = F_{r+1} + 1$-dimension cube. Similar to the attack on Frit$_a^b$-AE, the K_{i+1} is deduced by calculating the cube sums. The time complexity of recovering 1-bit key is 2^d, and the time to get the whole 128-bit key is $2^d \times 2^7 = 2^{7+d}$ by traversing i from 0 to 127. According to algebraic degree of Frit, we could apply key-dependent cube attack to no more than 12-round Frit$_b^b$-AE.

Attacks on Frit$_c^b$-AE. The cipher Frit$_c^b$-AE sets the 128-bit key K to limb c_0 and the 256-bit nonce to limbs a_0 and b_0. We give a 4-round initial structure of Frit$_c^b$-AE by keeping the limb a_0 to constants 0 and setting $\sigma_c^{-1}\sigma_a^{-1}(v)$ to limb b_0. To linearize the expression $b_3 \odot b_4$, we find the procedure is similar to the attacks on Frit$_a^b$-AE. The only difference is the coefficient $g_{i,j}(K)$ of each term v_iv_j. So our attack could be applied to 11-round Frit$_a^b$-AE with time complexity 2^{29}.

For the other six versions, because the property that $a_{r+1} = \sigma_a^{-1}(b_{r+2})$ and $c_{r+1} = a_{r+1} + a_r + b_r$, the cube testers for $(r+2)$-round Frit$_\alpha^b$-AE could be used to attack

1) The addition + is in GF(2^7), i.e., $i + 1$ means $(i + 1) \mod 128$.

$(r+1)$-round Frit_{α}^{a}-AE and Frit_{α}^{c}-AE. For more details, please refer to Appendix A.

Conclusion. We give some key-recovery attacks on reduced Frit in duplex-AE mode. Our results cover all the versions of $\text{Frit}_{\alpha}^{\beta}$-AE and include some practical key-recovery attacks that could recover the key within several minutes.

Acknowledgements This work was supported by National Key Research and Development Program of China (Grant No. 2017YFA0303903), National Natural Science Foundation of China (Grant No. 62072270), National Cryptography Development Fund (Grant Nos. MMJJ20170121, MMJJ20180101), and Zhejiang Province Key R&D Project (Grant No. 2017C01062).

Supporting information Appendix A. 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 Simon T, Batina L, Daemen J, et al. Towards lightweight cryptographic primitives with built-in fault-detection. IACR Cryptology ePrint Archive, Report 2018/729, 2018. https://eprint.iacr.org

2 Dobraunig C, Eichlseder M, Mendel F, et al. Algebraic cryptanalysis of frit. IACR Cryptology ePrint Archive, Report 2018/809, 2018. https://eprint.iacr.org

3 Bertoni G, Daemen J, Peeters M, et al. Duplexing the sponge: single-pass authenticated encryption and other applications. In: Proceedings of International Workshop on Selected Areas in Cryptography, 2012. 320–337

4 Huang S Y, Wang X Y, Xu G W, et al. Conditional cube attack on reduced-round keccak sponge function. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2017. 259–288

5 Dong X Y, Li Z, Wang X Y, et al. Cube-like attack on round-reduced initialization of Ketje Sr. IACR Trans Symmetric Cryptol, 2017, 2017: 259–280

6 Li Z, Bi W Q, Dong X Y, et al. Improved conditional cube attacks on keccak keyed modes with MILP method. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, 2017. 99–127

7 Li Z, Dong X Y, Wang X Y. Conditional cube attack on round-reduced ASCON. IACR Trans Symmetric Cryptol, 2017, 2017: 175–202

8 Bi W, Dong X, Li Z, et al. MILP-aided cube-attack-like cryptanalysis on Keccak Keyed modes. Des Codes Cryptogr, 2018, 86: 1–26