SCIENCE CHINA
Information Sciences

• HIGHLIGHT •

May 2018, Vol. 61 058102:1–058102:3
doi: 10.1007/s11432-017-9181-4

A non-alternate 3D structure and its practical security evaluation against differential and linear cryptanalysis

Qian WANG* & Chenhui JIN

Information Science and Technology Institute, Zhengzhou 450001*, China*

Received 12 January 2017/Accepted 21 June 2017/Published online 21 November 2017

Citation Wang Q, Jin C H. A non-alternate 3D structure and its practical security evaluation against differential and linear cryptanalysis. Sci China Inf Sci, 2018, 61(5): 058102, doi: 10.1007/s11432-017-9181-4

The building blocks of the original 3D block cipher structure, first proposed by Nakahara [1] and generalized in [2], are four different invertible transformations that are similar to AES (advanced encryption standard [3]) but operate in a 3D array A: RoundKeyAddition κ_i; ByteSubstitution γ; ShiftRows θ_0 and θ_1, which are applied in alternate rounds; and MixColumns π. Owing to the alternate application of two different ShiftRows transformations θ_0 and θ_1, the 3D block cipher [1] achieves quick diffusion and guarantees enough active S-boxes to resist differential and linear cryptanalysis [4].

However, the alternate use of two different round functions causes more expense with respect to software and hardware implementation as compared with the cipher that iterates the same round function. In the software implementation, we require different code segments to implement the alternately used round functions, which increases the code size and memory consumption. In the hardware implementation, we require different circuits to implement the alternately used round functions, which increases the chip area. Furthermore, a multiplexer of block size is required to choose the transformation into which the data should be input at different rounds, which increases the chip area and time delay. The design of a 3D structure that employs a non-alternate structure but retains the same cryptographic properties as the original 3D structure and exhibits better implementing performance than the original 3D structure, is worth investigating.

Definition 1. Let the state cube $A = \{a_{i,j,t}\}_{i,j,t=0}^{n-1} = (a_{i,j,t})$, $a_{i,j,t} \in F_{2^m}$, then for $0 \leqslant i, j, t < n$, $a_{i,\cdot,\cdot} = \{a_{i,j,t}\}_{j,t=0}^{n-1}$, $a_{\cdot,j,\cdot} = \{a_{i,j,t}\}_{i,t=0}^{n-1}$, and $a_{\cdot,\cdot,t} = \{a_{i,j,t}\}_{i,j=0}^{n-1}$ are called an X-layer, a Y-layer, and a Z-layer of cube A, respectively. Similarly, $a_{i,j,\cdot} = \{a_{i,j,t}\}_{t=0}^{n-1}$, $a_{i,\cdot,t} = \{a_{i,j,t}\}_{j=0}^{n-1}$, and $a_{\cdot,j,t} = \{a_{i,j,t}\}_{i=0}^{n-1}$ are called a Z-column, a Y-column, and an X-column of the cube A, respectively.

New 3D structure. The transformations θ_0 and θ_1 in the original 3D structure operate within each X-layer and Y-layer, respectively, and thus, using them alternately can produce a good diffusion effect. Daemen et al. [5] mentioned a "cube rotation" transformation (see Figure 1), which may be a better choice for the 3D structure: replacing the two alternately used ShiftRows transformations with such a fixed "cube rotation" transformation might result in the same diffusion effect and resistance against differential and linear cryptanalysis as that of the original 3D structure.

A general word permutation that changes the positions of the words within the state cube A is defined as follows.

* Corresponding author (email: e_alpha@163.com)
The authors declare that they have no conflict of interest.

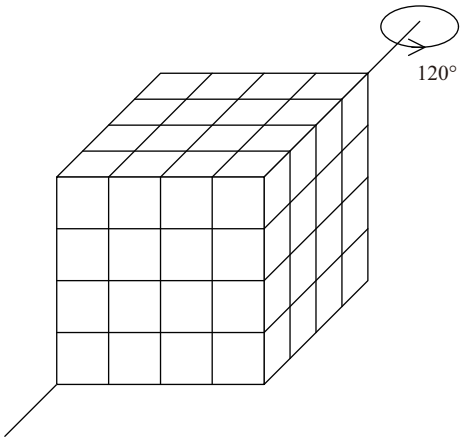

Figure 1 "Cube rotation" transformation for $n = 4$ [5].

Definition 2 (Word permutation)**.** For a word permutation θ, $\theta(\{a_{i,j,t}\}_{i,j,t=0}^{n-1}) = \{a_{\sigma(i,j,t)}\}_{i,j,t=0}^{n-1}$, $\sigma(i,j,t) = (\sigma_1(i,j,t), \sigma_2(i,j,t), \sigma_3(i,j,t))$, where σ is a permutation defined over the index space $I = \{(i,j,t) : 0 \leqslant i,j,t < n\}$, and σ_1, σ_2, and σ_3 are three component functions of σ. The inverse of σ is denoted by σ^{-1}.

Our target word permutations. Among all the word permutations on a state cube A, we focus our attention on two classes of them, which are denoted by τ_1 and τ_2: $\tau_1 = \{\theta : \sigma(i,j,t) = (\sigma_1(t), \sigma_2(i), \sigma_3(j))\}$ and $\tau_2 = \{\theta : \sigma(i,j,t) = (\sigma_1(j), \sigma_2(t), \sigma_3(i))\}$. It should be noted that the "cube rotation" transformation shown in Figure 1 can be written as $\sigma(i,j,t) = (t,i,j)$ and belongs to τ_1. Furthermore, if $\theta \in \tau_1$, then $\theta^{-1} \in \tau_2$.

On choosing a permutation $\theta \in \tau_1 \bigcup \tau_2$ and replacing the two alternately used permutations θ_1 and θ_2 with θ, we obtain a new round function ${\rho'}_r = \pi \circ \theta \circ \gamma \circ \kappa_r$. The iteration of this new round function results in a new 3D structure.

With respect to the diffusion effect of the new 3D structure, we have the following theorem, which is easy to verify.

Theorem 1. If the MixColumn transformation adopts the MDS (maximum distance separable) matrix, then three rounds of the new 3D structure provide "full diffusion".

Differential/linear security of the new 3D structure. The minimum number of differential and linear active S-boxes provides a measure of the practical security for a block cipher against differential and linear cryptanalysis. By analyzing the lower bounds on the number of active S-boxes in the differential and linear trails of the new 3D structure, we prove that the new 3D structure possesses the same resistance against differential and linear cryptanalysis as the original 3D structure. A new technique that is different from the one used in [4] will be employed.

As the discussions on differential and linear active S-boxes are similar, it is sufficient to treat the differential trails. All the results also hold for the linear trails.

It should be noted that we neglected the effect of the round key addition transformation κ_r. The differential branch number of the MixColumns is denoted by B_d.

The bound for a four-round differential trail can be easily deduced.

Theorem 2. The lower bound on the number of active S-boxes in a four-round non-trivial differential trail of the new 3D structure is ${B_d}^2$.

Proof. This bound is a direct result of the "wide trail" strategy [6].

However, for differential trails with more than four rounds, obtaining tighter bounds on the number of active S-boxes becomes more difficult [7]. Simply using a bound on the four-round trail to obtain a bound for a $4r$-round trail (namely $r{B_d}^2$) would not result in a tighter bound on the $4r$-round trail of the 3D structure. Based on the "wide trail" strategy, a few variables are used to characterize the differential trail. The number of active S-boxes of the trail could then be bounded by a function of these variables. As the number of variables is sufficiently small, we could manually deduce bounds for the trail.

Notations. The input differences of 10 consecutive rounds are denoted by A^1, A^2, ..., A^{10}, respectively. Then the front nine-round differential trail can be denoted by

$$A^1 \overset{\gamma}{\sim} A^1_\gamma \xrightarrow{\pi\circ\theta} A^2 \overset{\gamma}{\sim} A^2_\gamma \xrightarrow{\pi\circ\theta} A^3 \overset{\gamma}{\sim} A^3_\gamma \xrightarrow{\pi\circ\theta} A^4 \overset{\gamma}{\sim} A^4_\gamma \xrightarrow{\pi\circ\theta} A^5 \overset{\gamma}{\sim} A^5_\gamma \xrightarrow{\pi\circ\theta} A^6 \overset{\gamma}{\sim} A^6_\gamma \xrightarrow{\pi\circ\theta} A^7 \overset{\gamma}{\sim} A^7_\gamma \xrightarrow{\pi\circ\theta} A^8 \overset{\gamma}{\sim} A^8_\gamma \xrightarrow{\pi\circ\theta} A^9 \overset{\gamma}{\sim} A^9_\gamma \xrightarrow{\pi\circ\theta} A^{10}.$$

As the order of θ and γ can be exchanged, the above trail is equivalent to the following one:

$$A^1_\theta \overset{\gamma}{\sim} A^1_{\gamma,\theta} \xrightarrow{\pi} A^2 \overset{\gamma}{\sim} A^2_\gamma \xrightarrow{\theta\circ\pi\circ\theta} A^3_\theta \overset{\gamma}{\sim} A^3_{\gamma,\theta} \xrightarrow{\pi} A^4 \overset{\gamma}{\sim} A^4_\gamma \xrightarrow{\theta\circ\pi\circ\theta} A^5_\theta \overset{\gamma}{\sim} A^5_{\gamma,\theta} \xrightarrow{\pi} A^6 \overset{\gamma}{\sim} A^6_\gamma \xrightarrow{\theta\circ\pi\circ\theta} A^7_\theta \overset{\gamma}{\sim} A^7_{\gamma,\theta} \xrightarrow{\pi} A^8 \overset{\gamma}{\sim} A^8_\gamma \xrightarrow{\theta\circ\pi\circ\theta} A^9_\theta \overset{\gamma}{\sim} A^9_{\gamma,\theta} \xrightarrow{\pi} A^{10} \ (*).$$

The following ten parameters are introduced in order to characterize the trail (*):

(1) $t_1 = \min\{N_{XY}(a^{5,\theta}_{\cdot,j,\cdot}) : 0 \leqslant j < n, a^{5,\theta}_{\cdot,j,\cdot} \neq 0\}$, $u = \max\{N_{XY}(a^{5,\theta}_{\cdot,j,\cdot}) : 0 \leqslant j < n\}$;

(2) $t_2 = \min\{N_{XY}(a^{6,\gamma}_{i,\cdot,\cdot}) : 0 \leqslant i < n, a^{6,\gamma}_{i,\cdot,\cdot} \neq 0\}$, $v = \max\{N_{XY}(a^{6,\gamma}_{i,\cdot,\cdot}) : 0 \leqslant i < n\}$;

(3) $r = N_Z(A^3_{\gamma,\theta})$, $M = N_Z(A^4)$, $p = N_Z(A^5_\theta)$, $q = N_Z(A^6)$, $N = N_Z(A^7_\theta)$, $h = N_Z(A^8)$.

Here, $N_{XY}(\cdot)$ and $N_X(\cdot)$ denote the number of nonzero Z-columns and X-layers, respectively. The meanings of $N_{XZ}(\cdot)$, $N_{YZ}(\cdot)$, $N_Y(\cdot)$, and $N_Z(\cdot)$ are similar.

It should be noted that trail (*) is symmetrical, that is, the encryption direction and decryption direction of the trail are similar. We need only consider the situation where $\theta \in \tau_1$, as we can obtain a matching conclusion for $\theta \in \tau_2$ by applying the conclusion for $\theta \in \tau_1$ to the inverse trail of the trail (*). Therefore, the following discussion will be limited to the condition that $\theta \in \tau_1$; however, the results are also valid for $\theta \in \tau_2$.

For the trail (*), by the definitions of these ten parameters, we obtain $N_X(A^4) = p$, $N_Y(A_\theta^7) = q$, $N_X(A_\theta^5) = N_X(A^6) = N_Z(A_\theta^7) = N$, and $N_Z(A^4) = N_Y(A_\theta^5) = N_Y(A^6) = M$.

There are some constraints on these ten parameters, and they must be taken into consideration,

$$p + q \geqslant B_d,\ n \geqslant p \geqslant 1,\ n \geqslant q \geqslant 1, \quad \text{(a)}$$

$$n \geqslant N \geqslant u \geqslant t_1 \geqslant 1,\ n \geqslant M \geqslant v \geqslant t_2 \geqslant 1, \quad \text{(b)}$$

$$N + h \geqslant B_d,\ n \geqslant h \geqslant 1, \quad \text{(c)}$$

$$M + r \geqslant B_d,\ n \geqslant r \geqslant 1. \quad \text{(d)}$$

Further investigation shows that the lower bound on the number of active S-boxes in a trail can be expressed as a function of the above ten parameters, and the lower bound is then equivalent to the conditional minimum value of this function under the conditions (a) – (d). We can easily derive the following theorems.

Theorem 3. The lower bounds on the number of active S-boxes in six-round, eight-round, and ten-round non-trivial differential trails of the new 3D structure are $3B_d(B_d - 1)$, $4B_d(B_d - 1)$, and $5B_d(B_d - 1)$, respectively.

Theorem 3 provides theoretical proof to confirm the claim in [5] that there are at least 18 active S-boxes in a six-round differential trail of the 3D structure with $n = 2$ and $B_d = 3$, which was not proved in [5].

By cutting a $2k(k \geqslant 3)$-round differential trail into some six-round, eight-round, and ten-round subtrails, we could obtain the bound for a $2k(k \geqslant 3)$-round trail.

Theorem 4. The lower bound of the number of active S-boxes in a $2k(k \geqslant 3)$-round non-trivial differential trail of the new 3D structure is $kB_d(B_d - 1)$, where B_d is the differential branch number of the MixColumns transformation.

For the original 3D structure, Liu et al. [4] proved that there are at least ${B_d}^2$ and $kB_d(B_d-1)$ differential active S-boxes in four and $2k$ $(k \geqslant 3)$ consecutive rounds respectively, where B_d is the differential branch number of the MixColumns transformation. We obtain the same lower bounds for the new 3D structure.

Conclusion. The 3D structure was designed for use as building blocks for compression functions in hash functions and block ciphers with a large block size. 3D structures with $n = 4$ and $m = 4$, can be used to construct block ciphers with a 256-bit block. A 3D structure with $n = 4$ and $m = 8$ can be used to construct compression functions with a 512-bit state. We propose a better round function for the 3D structure.

Detailed proofs of all the above theorems can be found in Appendixes A and B.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61272488, 61402523, 61672031). We would like to thank the anonymous referees for their patience and constructive suggestions.

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 Nakahara J. 3D: a three-dimensional block cipher. In: Proceedings of the 7th International Conference on Cyptgoloy and Network Security. Berlin: Springer, 2008. 252–267
2 Cui T, Jin C H. Finding impossible differentials for rijndael-like and 3D-like structures. Trans Internet Inf Syst, 2013, 7: 509–521
3 Daemen J, Rijmen V. AES proposal: rijndael. 1999. http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf
4 Liu H C, Jin C H. Lower bounds of differential and linear active S-boxes for 3D-like structure. Comput J, 2015, 58: 904–921
5 Daemen J, Knudsen L R, Rijmen V. Linear frameworks for block ciphers. Des Codes Crypt, 2001, 22: 65–87
6 Daemen J, Rijmen V. Security of a wide trail design. In: Proceedings of the 3rd International Conference on Cryptology in India, Hyderabad, 2002. 1–11
7 Sajadieh M, Mirzaei A, Mala H, et al. A new counting method to bound the number of active S-boxes in Rijndael and 3D. Des Codes Crypt, 2017, 83: 327–343