SCIENCE CHINA
Information Sciences

• LETTER •

January 2021, Vol. 64 119103:1–119103:3
https://doi.org/10.1007/s11432-019-9938-0

Secure key-alternating Feistel ciphers without key schedule

Yaobin SHEN[1], Hailun YAN[1], Lei WANG[1,2*] & Xuejia LAI[1,2]

[1]*Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai* 200240*, China;*
[2]*Westone Cryptologic Research Center, Beijing* 100070*, China*

Received 23 April 2019/Accepted 19 July 2019/Published online 27 October 2020

Citation Shen Y B, Yan H L, Wang L, et al. Secure key-alternating Feistel ciphers without key schedule. Sci China Inf Sci, 2021, 64(1): 119103, https://doi.org/10.1007/s11432-019-9938-0

Dear editor,

Blockciphers play an fundamental role for cryptography in information security, which usually consist of round functions and key schedules. As one of the significant modules in blockciphers, key schedules have not received deserved attention. Commonly, the key schedule takes as input a master key and outputs the so-called round keys that are used in each round. In the case of AES-128, the master key is a 128-bit string and the total length of the round keys is $11 \times 128 = 1408$ bits. The AES-128 key schedule can be seen as a function from $\{0,1\}^{128}$ to $\{0,1\}^{1408}$.

Scientifically designing the key schedule part of block ciphers is an important but not well-understood subject. In general, it is not yet clear what practical and necessary principles a good key schedule has to follow. In order to resist some existing attacks, there are some properties on what a key schedule should not have, e.g., avoiding (semi-) weak keys, equivalent keys, symmetry and complementation properties [1]. Moreover, it should not be possible to mount trivial guess-and-determine attack attacks, meet-in-the-middle attacks, related-key attacks, slide-attacks or invariant subspace attacks. Considering the key schedule from the view of provable security is another direction. Chen et al. [2] used a lovely key schedule instantiated with a linear orthomorphism to minimize a two-round Even-Mansour cipher from just one n-bit master key and one n-bit permutation. They proved such AES-like construction can achieve beyond the birthday bound security. Recently, Guo and Wang (GW) [3] also used a linear-orthomorphism key schedule to obtain a birthday-bound secure four-round key-alternating Feistel (KAF) cipher from just one n-bit master key and one n-bit function. They claimed this four-round construction is theoretically minimal in the sense that removing any component of this construction would ruin the security.

In addition to providing necessary cryptographic security, the efficiency of the key schedule is also of great significance, especially for lightweight blockciphers which are often employed in source constrained environments such as radio-frequency identification (RFID) tags and sensor networks. In these lightweight ciphers, key schedules are commonly highly simplified to optimize the software and hardware efficiency. Some key schedules have round-by-round iterations with low diffusion [4,5], or do simple permutation or linear operations on master keys [6]. In particular, some lightweight ciphers have ultra-light (in fact non-existent) key schedule, and directly use master keys in each round [7,8].

• Our contributions. We start with an interesting question of how to design a as light as possible key schedule from the view of provable security and revisit the four-round KAF by GW (see Figure 1(a)). Although the key schedule instantiated with linear orthomorphism can be efficient in some instances, it is still unsatisfying for lightweight ciphers when applied in many source constrained environments. In this study, we optimize the construction by GW and propose a new four-round KAF with an ultra-light (non-existent) key schedule. Interestingly, we find the orthomorphism in their construction can be removed with a slight modification on the first round, i.e., applying one-bit rotation after the first round function. We prove this refined construction can achieve the birthday-bound security. Compared with GW's construction, our proposal has two advantages. The most significant one is that the key schedule is ultra-light (non-existent), which needs no computation/memory costs. One can simply bitwise exclusive-or (xor) the n-bit master key in corresponding rounds without bothering to any round-key derive function. Secondly, the one-bit rotation is more efficient than the linear orthomorphism used in GW's construction in most applications, because it only costs a one-bit shift rather than addition or field multiplication. We believe our construction is theoretically minimal (or even lighter than GW's construction) because removing the one-bit rotation or any other components would make it totally insecure. To the best of our knowledge, this is the first provably secure KAF using identical round functions and n-bit master key but without any key schedule.

On the other hand, we also investigate whether the same one-bit rotation works for three-round single-key KAF with identical round functions. This time we find such three-

* Corresponding author (email: wanglei_hb@sjtu.edu.cn)

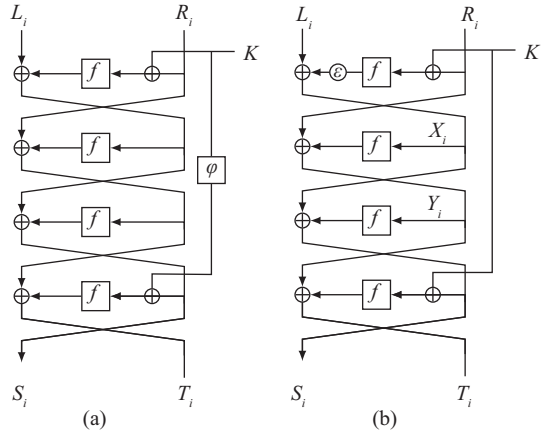

Figure 1 (a) Guo and Wang's four-round single-key KAFSF with key-schedule function φ; (b) our four-round single-key KAFSF without key schedule, where ε is the rotation of one bit.

round construction is not a pseudorandom permutation (PRP) and show a distinguishing attack on it with only four encryption queries. On the positive side, we prove that three-round KAF with a suitable key schedule can achieve PRP security. This is also the first provable-security result for three-round KAF, which may be independent of the interest.

Below we describe our results more concretely and denote by KAFSF the variant of KAF with identical round function. The proofs of all the following theorems can be found in Appendixes A–C.

Four-round single-key KAFSF without key schedule. We propose a four-round single-key KAFSF without a key schedule and prove that it is a strong pseudorandom permutation (SPRP). See Figure 1(b) for an illustration.

Our security result for four-round KAF is as follows.

Theorem 1. For the four-round single-key KAFSF without key schedule, it holds

$$\mathrm{Adv}^{\mathrm{sprp}}_{\mathrm{KAFSF}}(q_e, q_f) \leqslant \frac{4q_eq_f}{N} + \frac{13q_e^2}{N} + \frac{q_e^2}{2N^2}.$$

Remark. Note that the security result of our four-round KAFSF can also be generalized to multiuser security via a similar analysis of Guo and Wang [3], i.e., partitioning the key into two good and bad sets instead of partitioning transcripts, while the security result of our three-round KAFSF (will be analyzed in next section) cannot since there exists certain bad transcripts.

Three-round single-key KAFSF. One natural question is whether our refinement works for three-round key-alternating Feistel cipher. To address this question, we will show a distinguishing attack on three-round KAFSF without key schedule. After that, we present a PRP-secure three-round single-key KAFSF with a suitable key schedule.

• Attack on three-round KAFSF without key schedule. We show a distinguishing attack on three-round KAFSF without key schedule where the one-bit rotation ε is applied after the first round function (See Figure C1 in Appendix C for an illustration). This attack is similar to that in [9]. Same analysis will work when the rotation ε is applied after the last round function. Our attack on three-round KAFSF requires four forward queries, and is as follows:

(1) The adversary first asks $L_1\|R_1$ and $L_2\|R_1$ to the three-round KAFSF, and receives the responses $S_1\|T_1$ and $S_2\|T_2$, respectively.

(2) Let $\Delta = \varepsilon(L_1 \oplus L_2 \oplus T_1 \oplus T_2)$. The adversary then asks $S_1\|0$ and $S_2\|\Delta$ to KAFSF, and receives the responses $S_3\|T_3$ and $S_4\|T_4$, respectively. One can check the equation $S_3 \oplus S_4 = S_1 \oplus S_2$ holds with probability 1.

When the adversary is interacting with an $2n$-bit random permutation, the probability of the event $S_3 \oplus S_4 = S_1 \oplus S_2$ occurring is about $1/N^2$. Hence the success probability to distinguish this KAFSF from an $2n$-bit random permutation is about $1 - 1/N^2 \approx 1$.

Remark. As pointed out by Nandi [9], a similar attack still works for the other simple variants of function ε, e.g., when $\varepsilon(x) = \alpha \cdot x$ (the Galois field multiplication by a primitive element α) or any other linear function ε as long as $\Pr[x \xleftarrow{\$} \{0,1\}^n : \varepsilon(\varepsilon(x \oplus c_1)) \oplus \varepsilon(\varepsilon(x \oplus c_2)) = \Delta]$ is non-negligible for some fixed constants Δ, c_1, and c_2.

• PRP-secure three-round single-key KAFSF with a suitable key schedule. Besides providing an attack on three-round single-key KAFSF without a key schedule, on the positive side, we propose a three-round single-key KAFSF with a key-schedule function φ and prove that it achieves PRP security. See the figure in Appendix C for an illustration.

We begin by defining the key schedule used in our construction.

Definition 1 (Orthomorphism)**.** We say φ is an orthomorphism if both φ and $x \mapsto x \oplus \varphi(x)$ are a permutation on $\{0,1\}^n$.

Note that $\varphi(x_L\|x_R) = x_L\|x_L \oplus x_R$ and $\varphi(x) = c \odot x$ (where $\odot$ is the extension field multiplication) are two instances of orthomorphisms. Orthomorphisms have found many cryptographic applications, e.g., in [2, 3].

Our construction achieves PRP security when scheduling the key by the orthomorphism φ. The security result for three-round single-key KAFSF is as follows.

Theorem 2. For three-round single-key KAFSF using an orthomorphism φ as the key-schedule function, it holds

$$\mathrm{Adv}^{\mathrm{prp}}_{\mathrm{KAFSF}}(q_e, q_f) \leqslant \frac{3q_eq_f}{N} + \frac{6q_e^2}{N} + \frac{q_e^2}{2N^2}.$$

Conclusion. We optimize the four-round key-alternating Feistel by Guo and Wang [3] and propose a new four-round key-alternating Feistel with an ultra-light (non-existent) key schedule. We also investigate whether our optimization works for three-round key-alternating Feistel. We show a distinguishing attack on three-round key-alternating Feistel without key schedule, and prove that with a suitable key schedule three-round key-alternating Feistel is a PRP.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61602302, 61472250, 61672347, 61802255, 61702331, 61472251, U1536101), Natural Science Foundation of Shanghai (Grant No. 16ZR1416400), Shanghai Excellent Academic Leader Funds (Grant No. 16XD1401300), the 13th Five-year National Development Fund of Cryptography (Grant Nos. MMJJ20170114, MMJJ20170105), Sichuan Science and Technolog Program (Grant No. 2017GZDZX0002), Science and Technology on Communication Security Laboratory, China Scholarship Council (Grant No. 201806230107).

Supporting information Appendixes A–C. 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 Daemen J, Rijmen V. The Design of Rijndael: AES-the Advanced Encryption Standard. Berlin: Springer, 2013

2 Chen S, Lampe R, Lee J, et al. Minimizing the two-round Even-Mansour cipher. In: Proceedings of Annual Cryptology Conference, 2014. 39–56

3 Guo C, Wang L. Revisiting key-alternating Feistel ciphers for shorter keys and multi-user security. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, 2018. 213–243

4 Bogdanov A, Knudsen L R, Leander G, et al. PRESENT: an ultra-lightweight block cipher. In: Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems, 2007. 450–466

5 Wu W L, Zhang L. LBlock: a lightweight block cipher. In: Proceedings of International Conference on Applied Cryptography and Network Security, 2011. 327–344

6 Hong D, Sung J, Hong S, et al. HIGHT: a new block cipher suitable for low-resource device. In: Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems, 2006. 46–59

7 Guo J, Peyrin T, Poschmann A, et al. The LED block cipher. In: Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems, 2011. 326–341

8 Knudsen L, Leander G, Poschmann A, et al. PRINTcipher: a block cipher for IC-printing. In: Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems, 2010. 16–32

9 Nandi M. The characterization of Luby-Rackoff and its optimum single-key variants. In: Proceedings of International Conference on Cryptology in India, 2010. 82–97