Meet-in-the-Middle Attacks on 3-Line Generalized Feistel Networks

Le Dong[a,b], Yongxia Mao[a]

[a] *School of Mathematics and Information Sciences, Henan Normal University, Henan Province, China*
[b] *Henan Engineering Laboratory for Big Data Statistical Analysis and Optimal Control, Henan Normal University, Henan Province, China*

Abstract

In the paper, we study the security of 3-line generalized Feistel network, which is a considerate choice for some special needs, such as designing a 96-bit cipher based on a 32-bit round function. We show key recovery attacks on 3-line generic balanced Feistel-2 and Feistel-3 based on the meet-in-the-middle technique in the chosen ciphertext scenario. In our attacks, we consider the key size is as large as one-third of the block size. For the first network, we construct a 9-round distinguisher and launch a 10-round key-recovery attack. For the second network, we show a 13-round distinguisher and give a 17-round attack based on some common assumptions.

Keywords:
3-line Feistel, Meet-in-the-middle attack, Key recovery

1. Introduction

With the widely applications of intelligent devices, how to design security lightweight symmetric ciphers is an important subject for cryptographers. Substitution-permutation network (SPN) [1, 2, 3] and Feistel network [4, 5] are two common choices as the structures, but some ciphers use the generalized Feistel network (GFN) [6]. Most of GFN applications adopt the state with four branches (GFN_4), but 3-line GFN (GFN_3) is also an interesting choice to design block ciphers with 48- or 96-bit block size. In 2010, Bogdanov

Email address: dongle127@163.com (Le Dong)
URL: http://www.htu.cn/math/2014/0110/c1348a24713/page.htm (Le Dong)

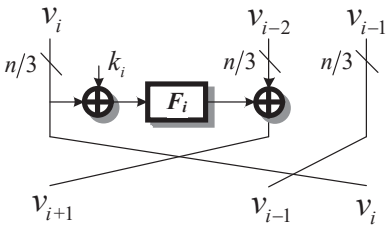

Figure 1: 3-line Feistel-2

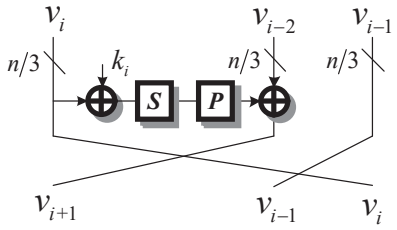

Figure 2: 3-line Feistel-3

showed the upper bounds on the differential and linear trail probabilities for 3-line contracting unbalanced Feistel networks [7]. The next year Bogdanov et al. gave an 8-round impossible differential distinguisher for 3-line GFNs with bijective functions [8]. To the best of our knowledge, no block cipher uses GFN_3 as the structure so far. The reason may be that people have not yet clear about its security bounds for common attacks, which is the right meaning of our work.

Meet-in-the-middle attack was proposed from cryptanalysis of block ciphers [9]. In recent years, a series of results about the attack are emerging, e.g. in the block cipher IDEA [10], in AES [11, 12, 13], and in GOST [14]. For the two-branch generic Feistel construction, Guo et al. gave a 6-round attack for single-key size on Feistel-2 and a 14-round attack on Feistel-3 in 2014 with the meet-in-the-middle technique [15]. Lin et al. presented an effective searching algorithm to obtain the best improved meet-in-the-middle distinguisher, and utilize it on GFN_4 [16] and other GFNs [17]. In 2017, Guo attacked 4-branch contracting Feistels and expanding Feistels [18].

Our Contributions. In this paper, we show key-recovery attacks on GFN_3 ciphers in the chosen-ciphertext scenario by the meet-in-the-middle technique.

In the case of 3-line Feistel-2, we give a 10-round attack based on a 9-round distinguisher. It is a general Feistel structure with three branches, and thus can be applicable broadly. For 3-line Feistel-3, we can attack more rounds because of the special properties of the structure. With the common assumption that the branch number of the P-layer reaches maximum, we give a 17-round attack based on a 13-round distinguisher. We launch the chosen-ciphertext attack because the internal state value of the branch we find is not in consecutive rounds.

Table 1: Comparison of previous results and ours

Target	Round functions	Rounds	Data	Time	Attack	Reference
Feistel-2	Bijective	8	-	-	distinguisher	[8]
	-	9	-	-	distinguisher	Section3
	-	10	$2^{2n/3}$	$2^{2n/3}$	key-recovery	Section3
Feistel-3	-	13	-	-	distinguisher	Section4
	-	17	2^{n-c}	$2^{n-c} + 2^{n/3+5c}$	key-recovery	Section4

2. Preliminaries

In this paper, we assume that the block size and the key length are n bits, the size of each branch is $n/3$ bits. The subkey length is equal to the size of each branch. The value of each branch is denoted by v_i and the n-bit plaintext and ciphertext are denoted by $m_0 \| m_1 \| m_2$ and $c_0 \| c_1 \| c_2$, respectively.

The networks of 3-line Feistel-2 and Feistel-3 are described in Figure 1 and Figure 2. The 3-line Feistel-2 network is a structure in which the round functions are composed of an XOR of a subkey followed by an application of a public function or permutation [19]. The round function of a 3-line Feistel-3 consists of a subkey XOR, an S-layer, and a P-layer. We recover the subkey by choosing ciphertexts based on the properties of GFN_3.

A b-δ-set is a set that b active bits are all different and other bits are fixed [15]. We define some notations as follows: F_i is the round function of round i, and $F_i^{\mathcal{I}}$ and $F_i^{\mathcal{O}}$ are its input and output. We use $\Delta\alpha$ to represent the difference of α.

3. Key-Recovery Attacks on 3-Line Feistel-2

In this section, we present a 9-round distinguisher of the 3-line generalized Feistel-2 structure using the meet-in-the-middle technique, and then to launch a 10-round key-recovery attack based on it. We do not give the restriction that round functions are bijective, while we assume that given a large set of fixed input and output differences of F_i there is one value pair match them on average.

3.1. The 9-Round Differential Characteristic

We consider a construction of GFN_3 with 9 rounds. Let a pair of ciphertexts (c, c') with the difference $0 \| X' \| 0$ corresponding to a pair of plaintexts (m, m') with the difference $0 \| 0 \| X$, where both X and X' are

non-zero, described in Figure 3. Based on the structure we can deduce that $\Delta v_{i+3} = X$ and $\Delta v_{i+4} = \Delta v_{i+7} = X'$, and then we have $\Delta F^{\mathcal{O}}_{i+3} = X'$, and $\Delta F^{\mathcal{O}}_{i+5} = X$. Let $\Delta F^{\mathcal{O}}_{i+4} = \Delta$, thus we get $\Delta v_{i+5} = \Delta F^{\mathcal{O}}_{i+7} = \Delta$. The input and output differences of F functions at round $i+3$, $i+4$, $i+5$, and $i+7$ are determined when Δ is fixed. As a result, there exists one state pair satisfying the input-output difference in each of the four rounds. We use bold lines to denote the states whose values are fixed.

Note that $n/3$-bit round key is added in each round, thus there are $2^{n/3}$ possible internal state pairs through the F function in each round. As a result, there are $2^{4n/3}$ possible state pairs for round $i+3$, $i+4$, $i+5$, and $i+7$. However, the state pairs in these rounds have $2^{n/3}$ possibilities on average as Δ have $2^{n/3}$ different values.

3.2. The Construction of the Differential Sequence

If we find a plaintext pair (m, m') with the difference $0 \parallel 0 \parallel X$ and the corresponding ciphertext difference $c \oplus c' = 0 \parallel X' \parallel 0$, a chosen ciphertext distinguisher can be constructed beginning with a b-δ-set shown in Figure 4. Note that selecting a value of Δ, we can obtain the fixed state pairs of $F^{\mathcal{I}}_{i+7}$, $F^{\mathcal{I}}_{i+5}$, $F^{\mathcal{I}}_{i+4}$, and $F^{\mathcal{I}}_{i+3}$. Denote the values corresponding the ciphertext c at the above four states by t_{i+7}, t_{i+5}, t_{i+4}, and t_{i+3}.

Modify the difference of the ciphertext to be $0 \parallel \delta_j \parallel 0 = c \oplus c''$, and we have $\Delta v_{i+7} = \Delta F^{\mathcal{I}}_{i+7} = \delta_j$. Since the value corresponding c at $F^{\mathcal{I}}_{i+7}$ is t_{i+7}, we can get the value of $\Delta F^{\mathcal{O}}_{i+7}$ by $\Delta F^{\mathcal{O}}_{i+7} \leftarrow F_{i+7}(t_{i+7}) \bigoplus F_{i+7}(t_{i+7} \bigoplus \delta_j)$, and denote it by $*$($*$ represent a state difference whose value is computable, and we do not distinguish them in the following analysis), so that $\Delta v_{i+5} = *$. Similarly, $\Delta F^{\mathcal{O}}_{i+5}$ can be obtained by $\Delta F^{\mathcal{O}}_{i+5} \leftarrow F_{i+5}(t_{i+5}) \bigoplus F_{i+5}(t_{i+5} \bigoplus *)$, and then we have $\Delta v_{i+3} = *$. With the knowledge of $\Delta v_{i+4} = \delta_j$, we can get $\Delta F^{\mathcal{O}}_{i+4}$ by $\Delta F^{\mathcal{O}}_{i+4} \leftarrow F_{i+4}(t_{i+4}) \bigoplus F_{i+4}(t_{i+4} \bigoplus \delta_j)$. Hence, the value of Δv_{i+2} can be computed by the equation $\Delta v_{i+2} = \Delta F^{\mathcal{O}}_{i+4} \bigoplus \Delta v_{i+5}$. Likewise, Δv_{i+1} can be calculated by $\Delta v_{i+1} = \Delta F^{\mathcal{O}}_{i+3} \bigoplus \delta_j$, which we also denote by $*$. When we traverse all the values of δ_j, where $j = 1, 2, 3, \cdots, 2^b - 1$, we get a special sequence of b-δ-set corresponding to a fixed Δ. Since Δ has $2^{n/3}$ different values, we can obtain at most $2^{n/3}$ different differential sequences. Whereas, there are $(2^{n/3})^{2^b} = 2^{2^b n/3}$ differential sequences if we modify the 9-round 3-line Feistel-2 to be an ideal function.

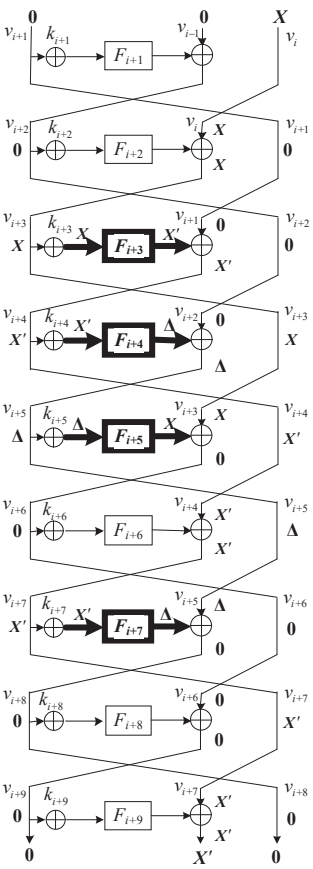

Figure 3: 9-round differential characteristic

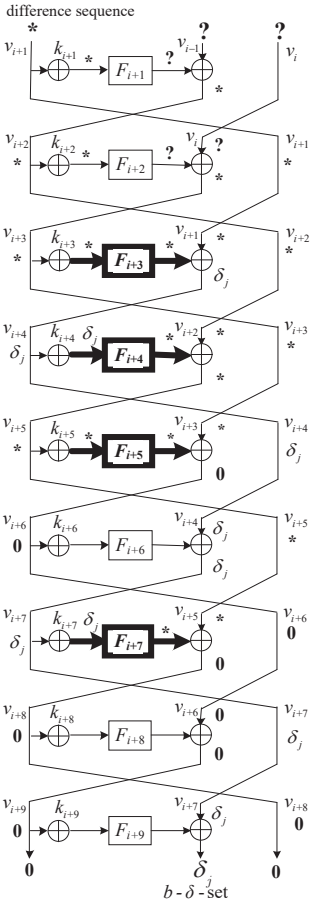

Figure 4: b-δ-set construction

3.3. 10-Round Key-Recovery Attack

Based on the above 9-round distinguisher, we add one round after it to launch a 10-round chosen-ciphertext key-recovery attack illustrated in Figure 5. It includes the precomputation and online part.

In precomputation part, we choose many pairs based on X and X', where X' is fixed and the last x bits of X are relaxed to be any possible nonzero value while other bits are zero. The value of x will be determined in the sequel to reach the best time/data/memory complexities. The tables $T_7, T_5, T_4, T_3, T_{10}$ and T_δ can be computed according to the method in the reference [15], where T_δ stores all of the output differential sequences of Δm_0 (plaintext $m = m_0 \| m_1 \| m_2$).

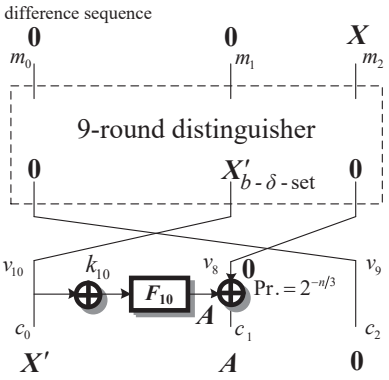

Figure 5: 10-round key-recovery

In online part, first of all, in order to collect enough data to ensure one of them can meet the 9-round differential characteristic, we construct a structure of $2^{n/3+1}$ ciphertexts with two lists and query the decryption oracle to get corresponding plaintexts. Denote c by $c_0\|c_1\|c_2$, and c_0 and c_2 are fixed while c_1 are pairwise distinct. Then compute the other list by $(c_0 \oplus X')\|c_1\|c_2$. We obtain about $2^{2n/3}$ pairs of (c, c') in total with the difference value $X' \parallel A \parallel 0$ in the above structure, where A is a nonzero difference. We want to pick up the ciphertext pairs of (c, c') which correspond to the plaintext differences $0 \parallel 0 \parallel X$ whose last x bits can be arbitrary. Therefore the ciphertext structure provides about $2^{2n/3} \cdot 2^{-(n-x)} = 2^{x-n/3}$ pairs conforming to the plaintext difference requirements. Furthermore, we need to cancel the differences of $F^{\mathcal{O}}_{i+10}$ and c_1 holding with probability $2^{n/3}$. Hence we construct $2^{2n/3-x}$ structures by repeating the above steps for different values of c_0 and c_2. As a result, we expect $2^{2n/3-x} \cdot 2^{x-n/3} \cdot 2^{-n/3} = 1$ pair to follow the whole characteristic.

Secondly, we recover the subkey K_{10}. Now we have $2^{2n/3-x} \cdot 2^{x-n/3} = 2^{n/3}$ candidate pairs with a ciphertext difference $X'\|\Delta c_1\|0$ and an appropriate plaintext difference. We match against the precomputed table T_{10} to find the corresponding value of $F^{\mathcal{I}}_{10}$, and compute the subkey candidate by $K_{10} \leftarrow F^{\mathcal{I}}_{10} \oplus c_0$. Then we construct a b-δ-set for c_0 to find the correct k_{10} from $2^{n/3}$ candidates. When we modify c_0, compute $F^{\mathcal{O}}_{10}$ with the knowledge of K_{10} and modify c_1 to make the value of v_8 unchanged. Query the ciphertext to get the corresponding plaintext, and calculate the differential sequence of m_0. If the sequence is included in T_δ, the guess of K_{10} is right with a high probability, otherwise it is wrong.

The data complexity is about $2^{n/3+1} \cdot 2^{2n/3-x} = 2^{n-x+1}$ chosen ciphertext, the time complexity is $2^x \cdot 2^b \cdot 2^{n/3} = 2^{n/3+x+b}$ encryptions to construct T_δ and 2^{n-x+1} memory access to query the decryption oracle. The memory complexity is $2^{n/3+x+b}$ $n/3$-bit blocks for storing T_δ. When $x = n/3$, the data complexity become about $2^{2n/3}$ chosen ciphertext, the time complexity becomes about $2^{2n/3}$ encryptions, and the memory complexity is about $2^{2n/3}$ $n/3$-bit blocks, i.e. the time and memory reach tradeoff.

4. Key-Recovery Attacks against Feistel-3 Construction

In this section, we present a 17-round chosen ciphertext key-recovery attack on the 3-line Feistel-3 structure based on a 13-round non-ideal behavior. We assume that the S-boxes in the network have good differential uniformity and each P-layer has the maximum of the branch number. In other words, there is one value matching the fixed input and output differences on average for an S-box, and the minimum of the sum of the active words at the input and output of a P-layer.

The block size of 3-line Feistel-3 is n bits, and each branch has $n/3$ bits. An S-box consists of c bits and there are r parallel S-boxes in an S-layer so that $rc = n/3$. For the branch-wise difference, $\mathbf{1}$ represents that only one word in the branch is active, and $\mathbf{0}$ represents a branch in which there is no active bit. Without loss of generality, we all take the first word active for $\mathbf{1}$. We assume the branch number of P-layer reach the maximum $r + 1$. Namely, the state with an active word becomes the state in which all bits are active after passing through the P-layer, and we denote the latter one by $\mathbf{P}$. Similarly, the state after an inverse transformation of the P-layer from an active word state is denoted by $\mathbf{P}^{-1}$.

As described in the previous section, $F_i^{\mathcal{I}}$ and $\Delta F_i^{\mathcal{I}}$ denote the input value and input difference of the round function in the round i, respectively, and $F_i^{\mathcal{I}}$ is also the input of the S-layer in F_i. Similarly, $F_i^{\mathcal{M}}$ and $\Delta F_i^{\mathcal{M}}$ denote the input value and input difference to the P-layer in F_i , and $F_i^{\mathcal{O}}$ and $\Delta F_i^{\mathcal{O}}$ denote the output value and output difference of the P-layer in F_i, respectively.

4.1. The construction of 13-round differential characteristic

The chosen ciphertext difference is $(\mathbf{0}, \mathbf{1}, \mathbf{0})$ and the corresponding plaintext difference is $(\mathbf{0}, \mathbf{0}, \mathbf{1})$. Afterwards, we select a set of parameters which include six nonzero differences in six c-bit words (marked by colored circles in Figure 7) and the values of $n/3 - c$ inactive bits of $F_{i+7}^{\mathcal{I}}$ (marked by a blue

star $'\star'$ in Figure 7), in total $n/3 + 5c$ bits. Hence, we can construct a 13-round differential characteristic as shown in Figure 7, in which the P-layer of the third round is removed and replaced with an equivalent form. The detail is described as follows.

Fixed a set of values of the parameters, we can obtain the internal state values in the round 4, 5, 6, 7, and 9, marked by the red lines in Figure 7. We also get the one-word values in the round 3, 8, and 11, marked by the blue lines in Figure 7. Specifically, if the 1-word differences of $F^{\mathcal{I}}_{i+3}$ and $F^{\mathcal{M}}_{i+3}$ are fixed, we expect the values for the corresponding words are determined. Use the same method to obtain the one-word values of $F^{\mathcal{I}}_{i+8}$, $F^{\mathcal{M}}_{i+8}$, $F^{\mathcal{I}}_{i+11}$, and $F^{\mathcal{M}}_{i+11}$. $\Delta F^{\mathcal{M}}_{i+3}$ passes through the inverse P-layer and a full-active branch can be obtained. For the full-active $F^{\mathcal{I}}_{i+4}$ and $F^{\mathcal{O}}_{i+4}$, we expect one value on average to be matched. The values of $F^{\mathcal{I}}_{i+5}$, $F^{\mathcal{I}}_{i+6}$, and $F^{\mathcal{I}}_{i+9}$ can be also determined in the same way. Besides, it seems that we can only get one-word value of $F^{\mathcal{I}}_{i+7}$, but the full state value is determined since the values of $n/3-c$ inactive bits are also fixed before. As a result, when we fix a set of values of $n/3+5c$ bits, we can determine a set of values of the (part of) internal state values in the round 3, 4, 5, 6, 7, 8, 9, and 11.

Note that it needs some conditions about our differential path, for instance, $\mathbf{1} \oplus \mathbf{P}$ should be a full active difference in round $i+7$. It leads to a minor reduction of the probability of the truncated difference path from one, but this do not affect our attack.

Then we can determine a sequence of the 1-word difference denoted by *[1] in Figure 8 based on the b-δ-set for the ciphertexts. If we change the difference of the active word of the ciphertext, the one-word difference of $F^{\mathcal{I}}_{i+11}$ is also changed. We can get the one-word difference of $F^{\mathcal{M}}_{i+11}$ based on the one-word value of $F^{\mathcal{I}}_{i+11}$ we obtained before. Hence, the difference of $F^{\mathcal{I}}_{i+9}$ is fixed. Utilize its value we can compute the difference of $F^{\mathcal{O}}_{i+9}$. The steps of determining differences can be launched until the round $i+3$. Since the P-layer is removed, the difference of the first word in the leftmost branch in the round $i+1$ can be computed. For some selecting rule of the differences of the b-δ-set, we can determine a difference sequence of $v'_{i+2}[1]$, which denotes the first word of v'_{i+2} in Figure 8. Therefore, we can obtain at most $2^{n/3+5c}$ difference sequences here.

4.2. The key-recovery of 17-round

Based on the 13-round distinguisher, we consider the 17-round chosen ciphertext attack extended by three rounds at the beginning and one round

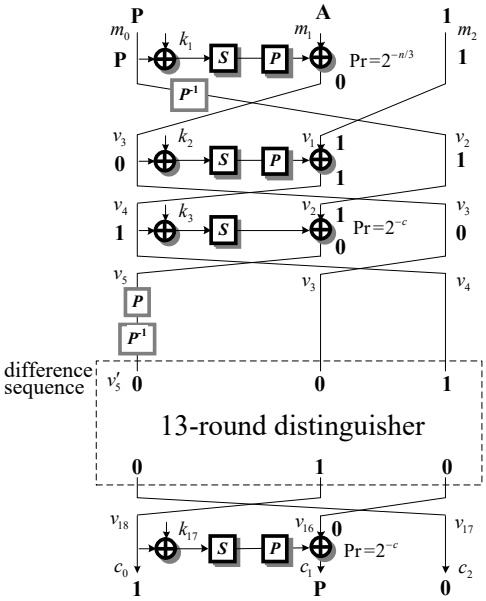

Figure 6: 17-round key-recovery

at the end as shown in Figure 6. The attack is composed of precomputation, collecting pairs, and detecting subkeys.

Precomputation. The primary workload for precomputation is the construction of the internal meet tables T_δ which include all the sequences of $\Delta v'_6[1]$ generated by traversing δ_j, $j = 1, 2, \cdots, 2^b - 1$. For each of the $2^{n/3+5c}$ values of the parameters, hence the precomputation costs about $2^{n/3+5c}$ encryptions as the parameter b is relatively small and we consider only a small fraction of all the rounds. Storing T_δ requires $3c/n \times 2^{n/3+5c+b}$ blocks of $n/3$ bits, as the sequences contains 2^b elements of c bits.

Collecting pairs. To launch the attack, we need a pair of ciphertexts whose difference satisfies the 13-round differential characteristic in Figure 7 at least. Then, the ciphertext difference (**1**,**P**,**0**) should propagate to the plaintext difference (**P**,**A**,**1**), where **A** is a truncated difference. The probability that the ciphertext difference (**1**,**P**,**0**) after inversion of the last round becomes (**0**,**1**,**0**) is 2^{-c}. The probability that the plaintext difference (**P**,**A**,**1**) after the first round becomes (**0**,**1**,**1**) is $2^{-n/3}$, and the probability that the difference (**1**,**1**,**0**) after the third round becomes (**0**,**0**,**1**) is 2^{-c}. Therefore, we need to collect $2^{n/3+2c}$ pairs of ciphertexts conforming the differential (**P**,**A**,**1**)$\xleftarrow{17R}$(**1**,**P**,**0**).

We choose a structure of ciphertexts $c \oplus c' = (\mathbf{1},\mathbf{P},\mathbf{0})$ consisting of 2^{4c} ciphertexts when we fix the inactive bits, and expect about $2^{4c} \times 2^{-2n/3+2c} = 2^{-2n/3+6c}$ corresponding plaintexts satisfying the difference $(\mathbf{P},\mathbf{A},\mathbf{1})$. Constructing 2^{n-4c} structures by releasing the inactive bits, there are $2^{n-4c} \times 2^{-2n/3+6c} = 2^{n/3+2c}$ pairs conforming the difference $(\mathbf{P},\mathbf{A},\mathbf{1}) \xleftarrow{17R} (\mathbf{1},\mathbf{P},\mathbf{0})$. The data complexity is approximately $2^{n-4c+2c} = 2^{n-2c}$ chosen ciphertexts. We also cost 2^{n-2c} times decryption, and the memory is about $2^{n/3+2c}$ blocks of $n/3$ bits.

Detecting subkeys. We first guess 1-branch value of $F_2^{\mathcal{I}}$ and assume that they all satisfy the 17-round differential, i.e. $\Delta v_3 = \mathbf{0}$, $\Delta v'_5 = \mathbf{0}$, and $\Delta v_{16} = \mathbf{0}$. Since we know the difference of plaintexts, we can determine the value of all the bits of $F_1^{\mathcal{I}}$ and $F_1^{\mathcal{O}}$ and then the value of k_1 can be obtained as $m_0 \oplus F_1^{\mathcal{I}}$. Compute $v_3 = F_1^{\mathcal{O}} \oplus m_1$ and then we get the value of k_2 based on the guessed value of $F_2^{\mathcal{I}}$ as $v_3 \oplus F_2^{\mathcal{I}}$. Besides, we can compute $k_3[1]$ and $k_{17}[1]$ by the 1-word matched differences at the S-boxes of the third and seventeenth rounds. As a result, based on the guessed value of $F_2^{\mathcal{M}}$ we derive $2^{n/3}$ candidates of k_1, k_2, $k_3[1]$, and $k_{17}[1]$.

In final, we construct the difference sequence of $\Delta v'_5[1]$ by modifying v_{18}, and remain v_{16} unchanged by modifying c_1. With the knowledge of k_1, k_2, and $k_3[1]$, we can calculate 2^b difference values of $\Delta v'_5[1]$. If they match with one of sequences in the middle meet table T_δ, then the guessed subkeys k_1, k_2, $k_3[1]$, and $k_{17}[1]$ are correct with a high probability, otherwise they are wrong.

The key-recovery phase costs $2^{n/3+2c} \times 2^{n/3} \times 2^b = 2^{2n/3+2c+b}$ for computing $\Delta v'_5[1]$, which is upper bounded by $2^{2n/3+3c}$ decryptions.

Complexity Analysis. As a result, the data complexity requires 2^{n-2c} chosen ciphertexts, the memory complexity is $2^{n/3+6c}$ blocks of $n/3$ bits and the time cost is $2^{n-2c}+2^{n/3+6c}+2^{2n/3+3c}$ encryptions, which is balanced for $n/3c = 2, 4$, or 5 S-Boxes per branch. Note that in order to make the attack effective, a branch must have at least 4 S-Boxes so that $n/3+6c < n$ and $2n/3+3c < n$, it is coincident with most block ciphers.

5. Conclusion

We have shown the 10 rounds chosen ciphertext attack on 3-line generic Feistel-2 structure and the 17 rounds chosen ciphertext attack on 3-line

generic Feistel-3 structure for the case of $k = n$, with the meet in the middle technique. In our analysis, we have just small constrain on the round function and its property, so the attack is applicable to any 3-line Feistel structure. Interested readers can use this method to analyze the structure of a larger key size.

References

[1] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, C. Vikkelsoe, Present: An ultra-lightweight block cipher, in: CHES, Vol. 4727, Springer, 2007, pp. 450–466.

[2] J. Guo, T. Peyrin, A. Poschmann, M. J. B. Robshaw, The led block cipher, in: Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings, 2011, pp. 326–341.

[3] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, et al., Prince–a low-latency block cipher for pervasive computing applications, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2012, pp. 208–225.

[4] G. Leander, C. Paar, A. Poschmann, K. Schramm, New lightweight des variants, in: International Workshop on Fast Software Encryption, Springer, 2007, pp. 196–210.

[5] W. Wu, L. Zhang, Lblock: a lightweight block cipher, in: Applied Cryptography and Network Security, Springer, 2011, pp. 327–344.

[6] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, T. Shirai, Piccolo: An ultra-lightweight blockcipher., in: CHES, Vol. 6917, Springer, 2011, pp. 342–357.

[7] A. Bogdanov, On unbalanced feistel networks with contracting mds diffusion, Designs, Codes and Cryptography 59 (1) (2011) 35–58.

[8] A. Bogdanov, K. Shibutani, Analysis of 3-line generalized feistel networks with double sd-functions, Information Processing Letters 111 (13) (2011) 656–660.

[9] W. Diffie, M. E. Hellman, Special feature exhaustive cryptanalysis of the nbs data encryption standard, Computer 10 (6) (1977) 74–84.

[10] H. Demirci, A. A. Selçuk, E. Türe, A new meet-in-the-middle attack on the idea block cipher, in: International Workshop on Selected Areas in Cryptography, Springer, 2003, pp. 117–129.

[11] O. Dunkelman, N. Keller, A. Shamir, Improved single-key attacks on 8-round aes-192 and aes-256, Advances in Cryptology-ASIACRYPT 2010 (2010) 158–176.

[12] O. Dunkelman, N. Keller, A. Shamir, Improved single-key attacks on 8-round aes-192 and aes-256, Journal of Cryptology 28 (3) (2015) 397–422.

[13] P. Derbez, P.-A. Fouque, J. Jean, Improved key recovery attacks on reduced-round aes in the single-key setting, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2013, pp. 371–387.

[14] T. Isobe, A single-key attack on the full gost block cipher, in: International Workshop on Fast Software Encryption, Springer, 2011, pp. 290–305.

[15] J. Guo, J. Jean, I. Nikolić, Y. Sasaki, Meet-in-the-middle attacks on generic feistel constructions, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2014, pp. 458–477.

[16] L. Lin, W. Wu, Y. Zheng, Improved meet-in-the-middle distinguisher on feistel schemes, in: International Conference on Selected Areas in Cryptography, Springer, 2015, pp. 122–142.

[17] L. Lin, W. Wu, Y. Zheng, Automatic search for key-bridging technique: Applications to lblock and TWINE, in: Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers, 2016, pp. 247–267.

[18] J. Guo, J. Jean, I. Nikolic, Y. Sasaki, Meet-in-the-middle attacks on classes of contracting and expanding feistel constructions, IACR Trans. Symmetric Cryptol. 2016 (2) (2016) 307–337.

[19] T. Isobe, K. Shibutani, Generic key recovery attack on feistel scheme, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2013, pp. 464–485.

Appendices

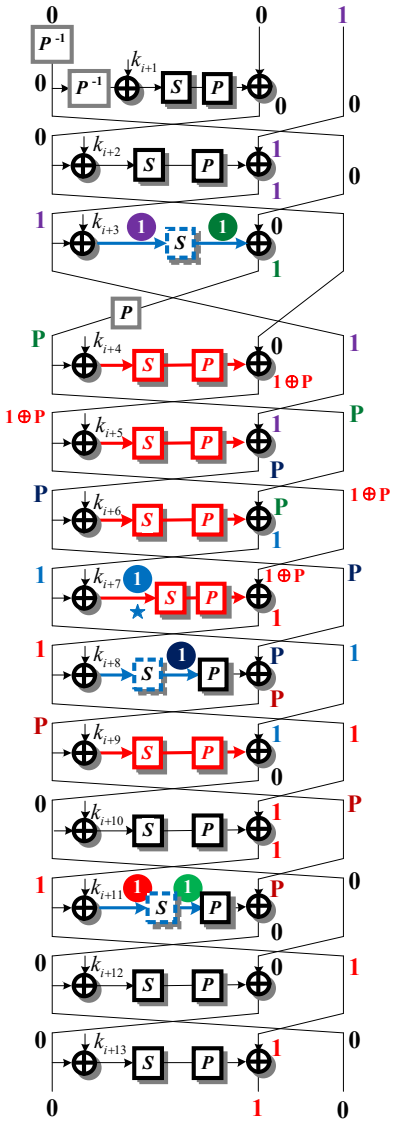

Figure 7: 13-round differential

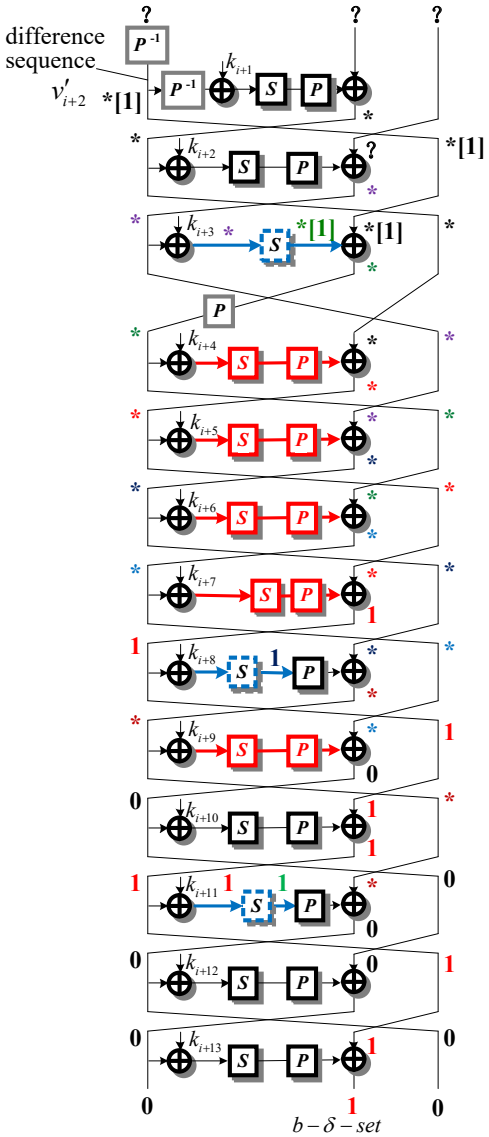

Figure 8: b-δ-set construction