Related-Cipher Attacks on Block Ciphers with Flexible Number of Rounds *

Jaechul Sung[1], Jongsung Kim[2]†, Changhoon Lee[3] and Seokhie Hong[3]

[1]Department of Mathematics, University of Seoul,
Cheonnong-Dong, Dongdaemun-Gu, Seoul, KOREA
jcsung@uos.ac.kr
[2]Katholieke Universiteit Leuven, ESAT/SCD-COSIC,
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
Kim.Jongsung@esat.kuleuven.ac.be
[3]Center for Information Security Technologies(CIST), Korea University,
Anam-Dong 5-ga, Sungbuk-Gu, Seoul, KOREA
{crypto77, hsh}@cist.korea.ac.kr

Abstract: Related-cipher attack was introduced by Hongjun Wu in 2002 [25]. We can consider related ciphers as block ciphers with the same round function but different number of rounds. This attack can be applied to related ciphers by using the fact that their key schedules do not depend on the total number of rounds. In this paper we introduce differential related-cipher attack on block ciphers, which combine related-cipher attack with differential cryptanalysis. We apply this attack to the block ciphers ARIA [15] and SC2000 [24]. Furthermore, related-cipher attack can be combined with other block cipher attacks such as linear cryptanalysis, higher-order differential cryptanalysis, and so on. With these combined attacks we also analyze some other block ciphers which use flexible number of rounds, SAFER++, CAST-128 and DEAL.

Keywords : Block Cipher, Related-Cipher Attack, Related-Key Attack, Slide Attack, Differential Cryptanalysis, ARIA, SC2000, SAFER++, CAST-128, DEAL.

C. Wolf, S. Lucks, P.-W. Yau (Eds.): WEWoRC 2005, LNI P-74, pp. 64–75, 2005.

*This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment).

†The second author was financed by Ph.D. grants of the Katholieke Universiteit Leuven and of CIST, Korea University and supported by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government and by the European Commission through the IST Programme under Contract IST2002507932 ECRYPT.

1 Introduction

Related-key attack [4] allows the cryptanalyst to obtain plaintext and ciphertext pairs by using different but related keys. For this attack, the cipher is fixed while the keys are related. For related-cipher attack [25], the key is fixed while the ciphers are related. In [25] the author considered related ciphers as block ciphers with the same round function but different number of rounds. In related ciphers their key schedules do not depend on the total number of rounds. Related-cipher attack can be applied to block ciphers with flexible number of rounds, which have some weaknesses on key schedules. This attack has great affect on protocols, where changing the cipher might introduce weaknesses. As an example of its applications, this kind of attack can be applied to WinZIP's encryption mechanism [23].

In this paper we introduce differential related-cipher attack on block ciphers. This attack combines related-cipher attack with differential cryptanalysis by exploiting a weakness of key schedule. With this method we analyze the block ciphers ARIA [15] and SC2000 [24]. We also combine related-cipher attack with other block cipher attacks such as linear cryptanalysis and higher-order differential cryptanalysis. With these methods we analyze some other block ciphers with flexible number of rounds, SAFER++ [18], CAST-128 [1] and DEAL [13]. Finally, we summarize our results.

2 Key-Schedule Cryptanalysis

There are some attacks which use some weaknesses of key schedules of block ciphers, such as weak-key attack [10, 11], slide attack [8, 9], related-key attack [12, 4], and related-cipher attack [25].

In weak key attack, weak keys can be defined as the keys which are more vulnerable to block cipher cryptanalysis such as differential cryptanalysis, linear cryptanalysis, and so on. Due to the simple design of the key schedule of IDEA, various weak-key attacks on IDEA [16] were introduced in [10, 11, 7]. Since IDEA uses multiplication in modular $2^{16} + 1$, the round keys such as 0 and 1, which can be used in the multiplication, have a weakness against differential or linear cryptanalysis. For details, see [10].

Slide attack exploits the degree of self-similarity of a block cipher. The attack is applicable to iterative block ciphers with a periodic key schedule and does not depend on the number of rounds. It also uses a weakness of the key schedule of block ciphers.

Related-key attack uses relationships between keys which are different but related. For this attack the cipher is fixed while the keys are related.

Related-cipher attack can be applied to the ciphers with flexible number of rounds. In [25] they applied the attack to the block cipher SQUARE and the AES variant [19] which was proposed at ACISP 2002. An interesting feature of the related-cipher attacks is that they are independent of the number of rounds. They only depend on the difference of the number of rounds. While the related-key attack uses different but related keys for

the fixed number of rounds, the related cipher attack uses related ciphers with flexible number of rounds. If the difference of round numbers between related ciphers is small, it is more vulnerable to the related-cipher attack. However typical related-cipher attack is more difficult to apply as the difference of round numbers becomes bigger. In order to overcome this problem we combine related-cipher attack with differential cryptanalysis, which we call differential related-cipher attack (or, related-cipher differential attack). Moreover we can also extend related-cipher attack by combining other block cipher attacks, such as linear cryptanalysis, higher-order differential cryptanalysis and so on.

3 Differential Related-Cipher Attack on ARIA

3.1 The Block Cipher ARIA

ARIA is the 128-bit block cipher with an involution SPN structure. ARIA has 10/12/14 rounds for 128-/192-/256-bit keys, respectively.

Inverse of involution Ciphers such as Khazad [2] and Anubis [3] differs from the forward operation in the key scheduling only. This property can reduce the required chip areas in a hardware implementation as well as the code and table size. However, there were found some flaws caused by the totally involution structure [6]. In this point of view, ARIA was not designed to be a totally involutional block cipher. More precisely, the substitution layer is not an involution.

Each of round of the cipher consists of three layers ; Round key addition layer, Substitution layer, and Diffusion layer. The substitution layer uses four S-boxes such that S_1, S_2, S_1^{-1}, and S_2^{-1}, where S_1 and S_2 are defined as an affine transformation of the inverse function over $GF(2^8)$. The diffusion layer uses a 16×16 binary matrix A.

The two substitution layers, type 1 and 2, are arranged for ARIA to be an involution even though each of two substitution layers is not an involution. Let $SL1 : GF(2^8)^{16} \rightarrow GF(2^8)^{16}$ be the S-box layer type 1 and $SL2 : GF(2^8)^{16} \rightarrow GF(2^8)^{16}$ be the S-box layer type 2. Then

$$SL1 = (\ S_1\ ,\ S_2\ , S_1^{-1}, S_2^{-1},\ S_1\ ,\ S_2\ , S_1^{-1}, S_2^{-1},\ S_1\ ,\ S_2\ , S_1^{-1}, S_2^{-1},\ S_1\ ,\ S_2\ , S_1^{-1}, S_2^{-1})$$

$$SL2 = (S_1^{-1}, S_2^{-1},\ S_1\ ,\ S_2\ , S_1^{-1}, S_2^{-1},\ S_1\ ,\ S_2\ , S_1^{-1}, S_2^{-1},\ S_1\ ,\ S_2\ , S_1^{-1}, S_2^{-1},\ S_1\ ,\ S_2\ )$$

It follows that $SL2 \circ SL1$ and $SL1 \circ SL2$ be the identity transformation.

The matrix $A : GF(2^8)^{16} \rightarrow GF(2^8)^{16}$ used in the diffusion layer is an involution, *i.e.*, $A^2 = I$. In [14] they gave how to construct an involution binary 16×16 matrix with a branch number 8. They indicated that the maximum branch number of invertible 16×16 binary matrices is 8 while the maximum branch number of invertible 16×16 matrices over $GF(2^8)$ is 17.

They also showed that ARIA has the cryptanalytic properties such as the resistance to differential, linear, impossible differential, and truncated differential cryptanalyses in [14].

The Cipher ARIA: Let $\sigma[ek_i]$ be the i-th round key addition layer with encryption key ek_i and A be the diffusion layer. Define γ_i be the substitution layer such that γ_i is $SL1$ if i is odd and $SL2$ if i is even. Then the i-th round of ARIA is denoted by $\phi[ek_i] = A \circ \gamma_i \circ \sigma[ek_i]$.

We can denote t-round ARIA with respect to 128-/192-/256-bit key sizes as the following ($t = 10, 12, 14$);

$$ARIA^t(MK) = \sigma[ek_{t+1}] \circ \gamma_t \circ \sigma[ek_t] \circ \phi[ek_{t-1}] \circ \cdots \circ \phi[ek_2] \circ \phi[ek_1].$$

Key Schedule of ARIA: ARIA uses different key sizes (128/192/256 bits) with different number of rounds, respectively. The key schedule of ARIA consists of two parts, the initialization and round key generation.

In the initialization part, four 128-bit values W_0, W_1, W_2, and W_3 are generated from the master key MK by using a 3-round Feistel cipher. The MK can be of 128, 192, or 256 bits. First, we fill out the 128-bit value KL with bits from MK and use what is left in MK on the 128-bit value KR. The remaining on KR is filled with zeroes as follows.

$$(KL||KR) \;=\; MK||00\cdots0.$$

After we obtain the values W_i's from the expanding key $(KL||KR)$ (W_i depends only on $(KL||KR)$), we obtain the round key ek_i in the round key generation part as the following, where $\ll a$ and $\gg a$ denote the a-bit left and right rotations, respectively;

$$\begin{array}{rclrcl}
ek_1 &=& (W_0^{\gg 7}) \oplus (W_1^{\ll 11}), & ek_2 &=& (W_1^{\ll 22}) \oplus (W_2), \\
ek_3 &=& (W_2^{\gg 17}) \oplus (W_3^{\ll 16}), & ek_4 &=& (W_0^{\gg 14}) \oplus (W_3^{\ll 32}), \\
ek_5 &=& (W_0^{\gg 21}) \oplus (W_2^{\gg 34}), & ek_6 &=& (W_1^{\ll 33}) \oplus (W_3^{\ll 48}), \\
ek_7 &=& (W_1^{\ll 44}) \oplus (W_2^{\gg 51}), & ek_8 &=& (W_0^{\gg 28}) \oplus (W_3^{\ll 64}), \\
ek_9 &=& (W_1^{\ll 55}) \oplus (W_3^{\ll 80}), & ek_{10} &=& (W_0^{\gg 35}) \oplus (W_2^{\gg 68}), \\
ek_{11} &=& (W_0^{\gg 42}) \oplus (W_1^{\ll 66}), & ek_{12} &=& (W_1^{\ll 77}) \oplus (W_2^{\ll 85}) \oplus (W_3^{\ll 96}), \\
ek_{13} &=& (W_0^{\gg 49}) \oplus (W_2^{\gg 102}), & ek_{14} &=& (W_2^{\ll 119}) \oplus (W_3^{\gg 112}) \oplus (KR^{\ll 64}), \\
ek_{15} &=& (W_0^{\gg 56}) \oplus (W_1^{\ll 88}) \oplus (KR). & & &
\end{array}$$

Note that the number of rounds ARIA uses is 10, 12, or 14 which depends on the size 128, 192, or 256 bits of master key. Since there is one more key addition layer in the last round, we need 11, 13, or 15 round keys depending on the sizes of master key.

3.2 Attack on ARIA

ARIA has different number of rounds with respect to the sizes of key bits. However, since the key schedule does not depend on the size of key bits and has relatively simple, we

can construct semi-equivalent keys which we can use in differential related-cipher attack (semi-equivalent keys will be defined in the below).

From a master key MK, we construct the 256-bit value $(KL||KR)$, which is equal to $MK||00\cdots0$. As mentioned before, we exploit the 256-bit value $(KL||KR)$ which construct each round key ek_i.

Let K be an arbitrary 128-bit key value. If the size of the master key is 128 such that $MK = K$, $(KL||KR)$ equals to $K||0^{128}$. Furthermore, if the MK has 192-bit size with $MK = K||0^{64}$, the $(KL||KR)$ equals to $K||0^{128}(= (K||0^{64})||0^{64})$. Similarly, if the MK has 256-bit size with $MK = K||0^{128}$, $(KL\ ||KR)$ has the same value just like the 128 and 192 bit cases. We define the keys which have the same $(KL||KR)$ as semi-equivalent keys.

Let us consider the case that 128-bit and 192-bit keys are semi-equivalent. Let K be the 128-bit key value and P be a plaintext and C and C' be the corresponding ciphertexts with respect to the key size. Then we have the following;

$$\begin{aligned} C &= ARIA^{10}(K)(P) \\ &= \sigma[ek_{11}] \circ \gamma_{10} \circ \sigma[ek_{10}] \circ \phi[ek_9] \circ \cdots \circ \phi[ek_2] \circ \phi[ek_1]\ (P) \\ C' &= ARIA^{12}(K||0^{64})(P) \\ &= \sigma[ek_{13}] \circ \gamma_{12} \circ \sigma[ek_{12}] \circ \phi[ek_{11}] \circ \cdots \circ \phi[ek_2] \circ \phi[ek_1]\ (P) \\ &= \sigma[ek_{13}] \circ \gamma_{12} \circ \sigma[ek_{12}] \circ \phi[ek_{11}] \circ A \circ \sigma[ek_{11}]\ (C) \end{aligned}$$

Since A is linear and involutional, we have the following relation between C and C' (See Fig. 3).

$$\begin{aligned} & C' = \sigma[ek_{13}] \circ SL2 \circ A \circ \sigma[A(ek_{12})] \circ SL1 \circ \sigma[ek_{11} \oplus A(ek_{11})]\ (A(C)) \\ \Leftrightarrow\ & A(C) = \sigma[ek_{11} \oplus A(ek_{11})] \circ SL1^{-1} \circ \sigma[A(ek_{12})] \circ A \circ SL2^{-1} \circ \sigma[ek_{13}]\ (C') \end{aligned}$$

Note that the inverse transformation of $SL2$ is $SL1$ and vice versa. The above equation is same as 2.5-round ARIA relation between C and C'. Analysis of this type appeared in [21] by using algebraic equations. In this paper, we find the round keys, ek_{11}, ek_{12}, and ek_{13} directly by using the technique in differential cryptanalysis. Let us see the details.

Let $X = (X^1, X^2, \cdots, X^{16})$ be an 128-bit value, where X_i be an 8-bit value for each. Let (C_1, C_1') and (C_2, C_2') be two ciphertext pairs of related-cipher corresponding to plaintexts P_1 and P_2, respectively.

Note that, in differential cryptanalysis, if we know the two right values of S-box inputs and output difference, then we can obtain the right key value using the difference table of S-box.

In order to get ek_{13} and ek_{12}, we first guess the seven 8-bit values of ek_{13} (ek_{13}^4, ek_{13}^5, ek_{13}^7, ek_{13}^9, ek_{13}^{10}, ek_{13}^{14}, ek_{13}^{15}) and the one 8-bit value of $A(ek_{12})$ ($A(ek_{12})^1$) which affect

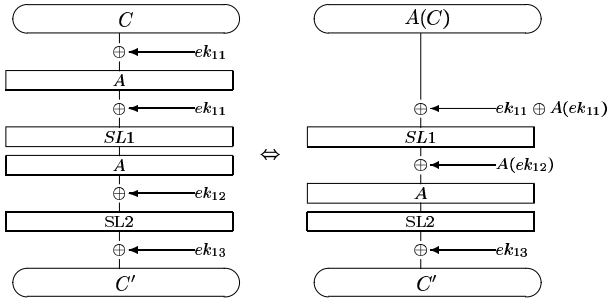

Figure 1: Related Ciphers between the 10- and 12-round ARIA

to the first S-box input of $SL1^{-1}$, then we can determine whether the guessing key is right or not, using the difference tables of S-boxes. Since the probability that a random key passes the test is about 2^{-8}, we can obtain the right key values with about 9 pairs since $2^{64} \times 2^{-8 \cdot 9}$ is less than 1.

By observing the second S-box in the $SL1^{-1}$, we can obtain 5 more 8-bit keys of ek_{13} and one 8-bit key $A(ek_{12})^2$. We can also get the remaining four 8-bit values of ek_{13} in the similar way. So we can find the right key values of ek_{13} and 4 bytes of $A(ek_{12})$. After finding ek_{13}, we can find the right $A(ek_{12})$ values using the difference tables of S-boxes.

If we find ek_{13} and $A(ek_{12})$, then we can know the input value of $SL1$. Let us assume the value as X. Therefore we have the following equation ;

$$A(C) \oplus (ek_{11} \oplus A(ek_{11})) = X \Leftrightarrow (A + I)(ek_{11}) = A(C) \oplus X,$$

where I be the 16×16 identity matrix. Since the rank of $A + I$ is 14, there exist about 2^{16} equivalent round keys in the eleventh round. However we can not determine the right key in the equivalent keys. Other methods such as exhaustive key search are need to determine exactly.

This attack needs about 2^{64} S-box table up operations with some memories. Our attack can be successful with only about 9 related-cipher pairs.

We can also attack on the related-ciphers between the 12 and 14 round ARIA if the keys are semi-equivalent in a similar way. Our attack is possible because ARIA uses flexible rounds with respect to different key sizes and the key schedule of ARIA is independent of the number of rounds.

4 Differential Related-Cipher Attack on SC2000

This section briefly describes the block cipher SC2000[24] and then presents differential related-cipher attack on SC2000.

SC2000 is a 128-bit block cipher with 128, 192 and 256-bit key sizes and it has the number

of 6.5/7.5/7.5 rounds for 128-/192-/256-bit keys, respectively.

One round of SC2000 is divided into two half rounds; The first half round is defined by $I \circ B \circ I$ where the I is a bit-wise key XOR function and the B is a nonlinear function which consists of 32 4-bit S-box S_4. The last half round is defined by $R \times R$ where the R is a data randomizing function and $\times$ represents a cross connection $(a_0, a_1, a_2, a_3) \rightarrow (a_2, a_3, a_0, a_1)$, ($a_i$: 32-bit string). Thus one round function of SC2000 consists of $(R \times R) \circ I \circ B \circ I$. Note that each round requires two 128-bit keys (*i.e.*, the first one is used in the I part before the B function and the second one is used in the I part after the B function) and the last round of 6.5- and 7.5-round SC2000 consists of $I \circ B \circ I \circ (R \times R)$.

The key schedule of SC2000 is independent of the key size. This fact enables us to construct semi-equivalent keys for 128-bit key and 192-bit key or 128-bit key and 256-bit key. That is, we can find a number of weak keys which allow us to construct related-ciphers for SC2000.

Before the key is inserted into the key schedule algorithm, the master key is expanded to eight 32-bit user keys as follows;

$$\begin{aligned}
K_1 = (K_1^1, K_1^2, K_1^3, K_1^4) &\longrightarrow (K_1^1, K_1^2, K_1^3, K_1^4, K_1^1, K_1^2, K_1^3, K_1^4) \\
K_2 = (K_2^1, K_2^2, \ \ldots, K_2^6) &\longrightarrow (K_2^1, K_2^2, K_2^3, K_2^4, K_2^5, K_2^6, K_2^1, K_2^2) \\
K_3 = (K_3^1, K_3^2, \ \ldots, K_3^8) &\longrightarrow (K_3^1, K_3^2, K_3^3, K_3^4, K_3^5, K_3^6, K_3^7, K_3^8)
\end{aligned}$$

where K_1, K_2, and K_3 are 128-/192-/256-bit keys, respectively and each of K_i^js is a 32-bit key string.

If the 128-bit master key is of the form $K_1 = (K_1^1, K_1^2, K_1^1, K_1^2)$ and the 192-bit master key is of the form $K_2 = (K_1^1, K_1^2, K_1^1, K_1^2, K_1^1, K_1^2)$ where K_1^1 and K_1^2 are arbitrary 32-bit key strings, then these two keys generate the same round keys for the first 6.5 rounds of SC2000. Similarly, if the 128-bit master key is of the form $K_1 = (K_1^1, K_1^2, K_1^3, K_1^4)$ and the 256-bit master key is of the form $K_3 = (K_1^1, K_1^2, K_1^3, K_1^4, K_1^1, K_1^2, K_1^3, K_1^4)$ where K_1^1, K_1^2, K_1^3 and K_1^4 are arbitrary 32-bit key strings, then these two keys also generate the same round keys for the first 6.5 rounds of SC2000. So these keys are semi-equivalent keys which we can use for our attack.

We now exploit the above semi-equivalent keys (K_1, K_2) or (K_1, K_3) to retrieve the last half round key of 7.5-round SC2000. Let P be a plaintext and C and C' be the corresponding ciphertexts with respect to the key size. Then we have the following relation between C and C':

$$\begin{aligned}
C = \ & SC2000^{6.5}(P, K_1) \\
C' = \ & SC2000^{7.5}(P, K_i) && = I \circ B \circ I \circ (R \times R) \circ SC2000^{6.5}(P, K_i) \\
& && = I \circ B \circ I \circ (R \times R) \circ SC2000^{6.5}(P, K_1) \\
& && = I \circ B \circ I \circ (R \times R)(C) \\
& && = I \circ B \circ I(D)
\end{aligned}$$

where i is 2 or 3 and $D = (R \times R)(C)$.

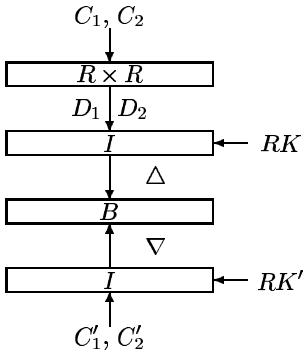

Figure 2: Attack on related ciphers between the 6.5- and 7.5-round SC2000

Using the technique of the differential related-cipher attack described in the previous Section we can find the 128-bit round keys RK and RK' (See Fig. 2). Let (C_1, C'_1) and (C_2, C'_2) be two ciphertext pairs of related-cipher corresponding to plaintexts P_1 and P_2, respectively. Then we can get the values $D_1 = (R \times R)(C_1)$, $D_2 = (R \times R)(C_2)$, and the input/output differences of the B function, $\Delta = D_1 \oplus D_2$, $\nabla = C'_1 \oplus C'_2$. Thus we can find the round key RK by using the difference table of the 4 bit S-box, S_4. For one pair of related-cipher, the difference table suggests on average two candidates of each 4-bit right key. So we exploit two related-cipher pairs to find the round key RK. Once we find RK, we can easily find another round key RK'. This attack requires about $2^6 (= 2 \cdot 32)$ difference table of S_4 look up operations.

5 Related-Cipher Attacks on SAFER++, CAST-128 and DEAL

In this section we devise related-cipher attacks on SAFER++ [18] and CAST-128 [1] using the techniques in linear cryptanalysis and higher-order differential cryptanalysis, respectively.

SAFER++ is a 128-bit block cipher and it has the number of 7/10 rounds for 128-/256-bit keys, respectively. The key schedule of SAFER++ does not depend on the key size. So we can construct semi-equivalent keys as follows; If the 128-bit key is K and the 256-bit key is of the form $K' = (K, K)$ where K is a arbitrary 128-bit key string, then these two keys generate the same round keys for the first 7 rounds of SAFER++.

Let us consider the case that 128-bit and 256-bit keys are semi-equivalent, *i.e.*, (K, K'). Assume that P is a plaintext and C and C' are the corresponding ciphertexts with respect to the key size. Then we have the following relation between C and C';

$$
\begin{aligned}
C = SAFER++^{7}(P,K) &= \sigma(k_{15}) \circ E(k_{14},k_{13}) \circ \cdots \circ E(k_2,k_1) \\
C = SAFER++^{10}(P,K') &= \sigma(k_{21}) \circ E(k_{20},k_{19}) \circ \cdots \circ E(k_2,k_1) \\
&= \sigma(k_{21}) \circ E(k_{20},k_{19}) \circ E(k_{18},k_{17}) \\
&\quad \circ A \circ \sigma(k_{16}) \circ XL(C),
\end{aligned}
$$

where $E(k_{2i}, k_{2i-1})$(=$A \circ \sigma(k_{2i}) \circ XL \circ \sigma(k_{2i-1})$) is the i-th round encryption. The σ is a function of the key addition and the XL is a nonlinear function and A is a linear function. For details, see the paper [18].

From the above equation we obtain a relation of the incomplete 3 round SAFER++ between C and C' and apply it to the technique of the linear cryptanalysis on 3-round SAFER++ presented in [22], which requires about 2^{81} known plaintexts and 2^{101} encryptions. Therefore we can succeed in attacking the incomplete 3 round SAFER++ with the complexity which is not larger than the complexity presented in [22].

We now describe a related-cipher attack on CAST-128. CAST-128 is a 128-bit block cipher and it has the number of 12/16 rounds for the keys between 40 and 80 bits/the keys between 80 and 128 bits, respectively. If the key between 40 and 80 bits is K and the key between 81 and 128 bits is of the form $K' = K||0 \cdots 0$, then these two keys generate the same round keys for the first 12 rounds of CAST-128. Similarly, we obtain a relation of 4-round CAST-128 by using the above semi-equivalent key and apply it to the higher order differential cryptanalysis on 5-round CAST-128 presented in [20], which needs about 2^{17} texts and 2^{40} encryptions and thus we can succeed in attacking 4-round CAST-128 with the complexity which is not larger than the complexity presented in [20]. Note that this attack is a chosen ciphertext and adaptive chosen plaintext attack for the related ciphers.

Furthermore, we can perform a related cipher attack on DEAL [13], which complexity requires less than it presented in [13]. But, since the attack method is almost same as the previous case, we omit a detail description for this attack.

6 Conclusion

It is difficult to apply related-cipher attack as the difference of numbers of rounds between related ciphers grows bigger. In order to overcome this problem we have combined related-cipher attack with differential cryptanalysis, linear cryptanalysis, and higher order differential cryptanalysis. With these combined attacks we have analyzed the block ciphers, ARIA, SC2000, SAFER++, CAST-128, and DEAL. Table 1 summarizes our results of related-cipher attacks.

Finally, we summarize what kinds of block ciphers may be vulnerable to the combined related-cipher attacks, and we suggest a simple design method for avoiding these kinds of attacks. The combined related-cipher attacks can be applied to a block cipher that has the following three properties:

Table 1: Summary of Related-Cipher Attacks

Related-Cipher[1] (Cipher(a)/Cipher(b))	Combined Attack	# Rounds[2] (c/d)	# Semi-Equi. Keys	Complexity[3] (Data/Time)	Type[4] (Cipher(a)/Cipher(b))
ARIA(128)/ARIA(192)	Differential	10/12	2^{64}	9RC/2^{64}T	KP/CP
ARIA(192)/ARIA(256)	Differential	12/14	2^{64}	9RC/2^{64}T	KP/CP
SC2000(128)/SC2000(192)	Differential	6.5/7.5	2^{64}	2RC/2^{33}T	KP/CP
SC2000(128)/SC2000(256)	Differential	6.5/7.5	2^{128}	2RC/2^{33}T	KP/CP
DEAL(128)/DEAL(256)	Differential	6/8	2^{128}	$\leq 2^{70}$RC/$\leq 2^{121}$E	KP/CP
DEAL(192)/DEAL(256)	Differential	6/8	2^{64}	$\leq 2^{70}$RC/$\leq 2^{121}$E	KP/CP
SAFER++(128)/SAFER++(256)	Linear	7/10	2^{128}	$\leq 2^{81}$RC/$\leq 2^{101}$E	KP/CP
CAST-128(m)/CAST-128(n)	Higher-Order	12/16	2^{m}	$\leq 2^{17}$RC/$\leq 2^{40}$E	CC/ACP

[1] a,b : The size of key , m , n : $40 \leq m < 80, 80 \leq n \leq 128$.

[2] c,d : Each number of rounds for Cipher(a) and Cipher(b)

[3] RC : Related Cipher pairs, T : Table look-up operations, E : Encryption units

[4] KP : Known Plaintext, (A)CP : (Adaptive) Chosen Plaintext, CC : Chosen Ciphertext

- The block cipher supports different key lengths (e.g., key sizes S(short) and L(large), $S < L$).
- For large keys, the block cipher runs through more rounds than for short keys (e.g., X rounds for key size S and Y rounds for key size L, and $X < Y$).
- Semi-equivalent keys exist (e.g., an S-bit key KS and an L-bit key KL are semi-equivalent, if the round keys used in the first X rounds of an encryption under KL are the same as the round keys of an encryption under KS (which runs through X rounds).

If the difference $Y - X$ is small, it may be feasible to attack the cipher, i.e., to find the round keys used in these $Y - X$ rounds. Therefore, if one would design a block cipher with flexible number of rounds, in order to avoid these kinds of attacks one should avoid a key schedule that create semi-equivalent keys. The simple way to achieve this is to design a key schedule to depend on the total number of rounds.

References

[1] C. M. Adams, *The CAST-128 Encryption Algorithm*, Request for Comments(RFC) 2144, Network Working Group, Internet Engineering Task Force, May, 1997.

[2] P. S. L. M. Barreto and V. Rijmen, *The Khazad Legacy-level Block Cipher*, Primitive submitted to NESSIE, 2000.

[3] P. S. L. M. Barreto and V. Rijmen, *Anubis Block Cipher*, Primitive submitted to NESSIE, 2000.

[4] E. Biham, *New Types of Cryptanalytic Attack Using Related Keys*, Journal of Cryptology, Vol. 7, No. 4, pp. 156–171, 1994.

[5] E. Biham and A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, Advances in Cryptology - CRYPTO'90, LNCS 537, Springer-Verlag, pp. 2–21, 1991.

[6] A. Biryukov, *Analysis of Involutional Ciphers : Khazad and Anubis*, The 10th Fast Software Encryption Workshop(FSE 2003), LNCS 2887, Springer-Verlag, pp. 45–53, 2003.

[7] A. Biryukov, J. Nakahara Jr, B. Preneel, and J. Vandewalle, *New Weak-Key Classes of IDEA*, Information and Communications Security: 4th International Conference(ICICS 2002), LNCS 2513, Springer-Verlag, pp. 315–326, 2002

[8] A. Biryukov and D. Wagner, *Side Attacks*, The 6th Fast Software Encrytion Workshop(FSE 1999), LNCS 1636, Springer-Verlag, pp. 245–259, 1999.

[9] A. Biryukov and D. Wagner, *Advanced Side Attacks*, Advances in Cryptology - EUROCRYPT 2000, LNCS 1807, Springer-Verlag, pp. 589–606, 2000.

[10] J. Daemen, R. Govaerts, and J. Vandewalle, *Weak Keys for IDEA*, Advances in Cryptology - CRYPTO'93, LNCS 773, Springer-Verlag, pp. 224–231, 1994.

[11] P. Hawkes, *Differential-Linear Weak Key Classes of IDEA*, Advances in Cryptology - EUROCRYPT'98, LNCS 1403, Springer-Verlag, pp. 112–126, 1998.

[12] J. Kelsey, B. Schneier, and D. Wagner, *Key-schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES*, Advances in Cryptology - CRYPTO'96, LNCS 1109, Springer-Verlag, pp. 237–251, 1996.

[13] L. Knudsen, *DEAL - A 128-bit Block Cipher*, February 21, 1998, revised May 15, 1998; Available at http://www.mat.dtu.dk/people/Lars.R.Knudsen/new block.html.

[14] B. W. Koo, H. S. Jang, and J. H. Song, *Constructing and Cryptanalysis of a* 16×16 *Binary Matrix as a Diffusion Layer*, The 4th International Workshop on Information Security Applications(WISA 2003), LNCS 2908, Springer-Verlag, pp. 489–503, 2003.

[15] D. Kwon, J. Kim, S. Park, S. Sung, Y. Sohn, J. Song, Y. Yeom, E. Yoon, S. Lee, J. Lee, S. Chee, D. Han, and J. Hong, *New Block Cipher : ARIA*, The 6th International Conference on Information Security and Cryptography(ICISC 2003), LNCS 2971, Springer-Verlag, pp. 432–445, 2004.

[16] X. Lai, J. Massey, and S. Murphy, *Markov Ciphers and Differential Cryptanalysis*, Advances in Cryptology - EUROCRYPT'91, LNCS 547, Springer-Verlag, pp. 17–38, 1991.

[17] S. Lucks, *On Security of the 128-bit Block Cipher DEAL*, The 6th Fast Software Encrytion Workshop(FSE 1999), LNCS 1636, Springer-Verlag, pp. 112–123, 1999.

[18] J. L. Massey, G. H. Khachatrian, and M. K. Kuregian, *Nomination of SAFER++ as candidate algorithm for the NESSIE*, Primitive submitted to NESSIE by Cylink Corp., 2000.

[19] L. May, M. Henricksen, W. Millan, G. Carter, and E. Dawson, *Strengthening the Key Schedule of the AES*, The 7th Australasian Conference on Information Seucurity and Privacy(ACISP 2002), LNCS 2384, Springer-Verlag, pp. 226–240, 2002.

[20] S. Moriai, T. Shimoyama, and T. Kaneko, *Higher Order Differential Attack of a CAST Cipher*, The 5th Fast Software Encryption Workshop(FSE 1998), LNCS 1372, Springer-Verlag, pp. 17–31, 1998.

[21] F. Muller, *A New Attack against Khazad*, Advances in Cryptology - ASIACRYPT 2003, LNCS 2894, Springer-Verlag, pp. 387–358, 2003.

[22] J. Nakahara Jr, *Cryptanalysis and Design of Block Ciphers*. PhD thesis, Katholieke Universiteit, Leuven, June 2003.

[23] T. Kohno, *Analysis of the WinZip encryption method*, ePrint, 2004.

[24] T. Shimoyama, H. Yanami, K. Yokoyama, M. Takenaka, K. Ioth, J. Yajima, N. Toril, and H. Tanaka, *The Block Cipher SC2000*, The 8th Fast Software Encryption Workshop(FSE 2001), LNCS 2355, Springer-Verlag, pp. 312–327, 2001.

[25] H. Wu, *Related-Cipher Attacks*, Information and Communications Security : 4th International Conference(ICICS 2002), LNCS 2513, Springer-Verlag, pp. 447–455, 2002.