

Related-Cipher Attacks

Hongjun Wu

Laboratories for Information Technology
21 Heng Mui Keng Terrace
Singapore 119613
hongjun@lit.a-star.edu.sg

Abstract. We formally introduce the concept of related-cipher attack. In this paper, we consider the related ciphers as block ciphers with the same round function but with different round numbers. If their key schedules do not depend on the total round number, then related-cipher attack could be applied if the same key is used. We applied this attack to block cipher SQUARE and show that SQUARE is vulnerable to this attack. We also show that a new AES key schedule proposed at ACISPO2 is weaker than the original one under this attack. We then classify the differential attacks into three categories: related-message attack (the original differential cryptanalysis), related-key attack and related-cipher attack. These attacks should be taken into consideration in cipher design.

1 Introduction

There have been a number of attacks on block ciphers. The most important two kinds of attacks are differential cryptanalysis [1] and linear cryptanalysis [11]. There are some variants or extensions of these two attacks such as the higher order differential cryptanalysis [7], truncated differential cryptanalysis [5], multiple linear approximations [9], non-linear approximations [6], partitioning cryptanalysis [4] and differential-linear cryptanalysis [8], etc. A common feature of these attacks is that both the cipher and the key are fixed. By analyzing some known (or chosen) plaintexts, information about the key could be revealed. The linear cryptanalysis can also be applied in the ciphertext only attack when there is sufficient redundancy in the plaintexts. All these attacks are very important in the design of ciphers. In [2], the related-key attack is introduced. For this attack, the cipher is fixed while the keys are related. This attack can be applied when some related keys and one common cipher are used to encrypt messages. Related key attack has important implication on the key schedule design of block ciphers.

In this paper, we introduce a new attack – related-cipher attack. For related-cipher attack, the key is fixed while the ciphers are related. It could be applied when someone uses the same key in related ciphers. In this paper, we consider the related ciphers as block ciphers with the same round function but different round number and their key schedules do not depend on the total round number. This attack can find the key easily when the difference between the round numbers is small. Related-cipher attack has important implication on the design of the key schedule of block ciphers with flexible round number.

This paper is organized as follows. The related-cipher attack is introduced in Section 2. Section 3 applies the related-cipher attack to some block ciphers with flexible round number. Section 4 suggests a way to resist related cipher attack by relating the key schedule to the total round number of the block cipher. Section 5 concludes this paper.

2 Related-Cipher Attack

Usually a secret key is associated with one particular cipher. However, the same key may be used in different ciphers in some cases. If those ciphers are related, the related-cipher attack may be applied. In this paper, we deal with the block ciphers with flexible round number.

Flexible round number is a feature in some block ciphers. It allows a user to choose greater security level. However, the key schedule of some of these block ciphers does not depend on the total round number. We denote these block ciphers as **related ciphers**. For this kind of cipher, if the same key is used in the ciphers with different round number, then the key can be found when the difference between the round numbers is small. The attack is outlined below.

Related-Cipher Attack on Block Ciphers. Consider two related block ciphers. Both of them have the same round function, but with different round numbers, r and $(r + \Delta r)$ respectively. If a key is used in these two ciphers to encrypt the same message, the attack can be carried out on the Δr -round cipher. For this Δr -round cipher, the plaintext is the ciphertext of the r -round cipher and the ciphertext is that of the $(r + \Delta r)$ -round cipher. The key can be determined easily for small Δr .

In the next section, we will apply related-cipher attack on some block ciphers with flexible round number.

3 Related-Cipher Attack on Some Block Ciphers

In this section related cipher attack is applied to two block ciphers with flexible round number. Block SQUARE [3] is vulnerable to this kind of attack. AES [13] can resist this kind of attack. But a new AES key schedule [12] is not that secure. Other block ciphers with flexible round number such as SAFER [10] are also vulnerable to the related cipher attack but we omit the attacks here. These results show that some of the block ciphers with flexible round number are really vulnerable to related cipher attack if their key schedules are not carefully designed. Care should be taken when we design block ciphers with flexible round number. In Subsection 3.1, we apply the attack to SQUARE. In Subsection 3.2, AES is shown to be able to resist the related-cipher attack. In Subsection 3.3, we show that a new AES key schedule presented at ACISP02 is not secure against the related-cipher attack.

3.1 Block Cipher SQUARE

SQUARE is a new block cipher designed by J. Daemen, L. Knudsen and V. Rijmen. The round number of SQUARE is set to eight while the designers also allow the con-

servative users to increase the number of rounds in a straight way. The key schedule of SQUARE does not depend on the total round number of the cipher and thus vulnerable to the related cipher attack.

3.1.1 Structure of SQUARE

The structure of SQUARE is outlined below. Interested readers may refer to [3] for the detail. SQUARE is an iterated block cipher with a block length and key length of 128 bits each. The basic building blocks of the cipher are five different invertible transformations that operate on a 4×4 array of bytes. The element of a state a in row i and column j is specified as $a_{i,j}$. Both indexes start from 0. These five transformations are outlined below.

A Linear Transformation θ .

$$\theta : b = \theta(a) \Leftrightarrow b_{i,j} = c_j a_{i,0} \oplus c_{j-1} a_{i,1} \oplus c_{j-2} a_{i,2} \oplus c_{j-3} a_{i,3}$$

where the multiplication in $\text{GF}(2^8)$ and the indices of c is taken modulo 4. If the rows of a state is denoted by polynomials

$$a_i(x) = \bigoplus_{j=0}^3 a_{i,j} x^j$$

Using this notation, and defining

$$c(x) = \bigoplus_{j=0}^3 c_j x^j$$

Then θ can be described as a modular polynomial multiplication:

$$b = \theta(a) \Leftrightarrow b_i(x) = c(x)a_i(x) \bmod(1+x^4) \text{ for } 0 \leq i < 4$$

In SQUARE, $c(x)$ is chosen to be

$$c(x) = 2_x \oplus 1_x \cdot x \oplus 1_x \cdot x^2 \oplus 3_x x^3$$

A Nonlinear Transformation γ

γ is a nonlinear byte substitution and is defined as

$$\gamma : b = \gamma(a) \Leftrightarrow b_{i,j} = S_\gamma(a_{i,j})$$

with S_γ an invertible 8-bit substitution table.

In SQUARE, the S-box is constructed by taking the mapping $x \rightarrow x^{-1}$ and applying an affine transformation to the output bits.

A Byte Permutation π .

$$\pi : b = \pi(a) \Leftrightarrow b_{i,j} = a_{j,i}$$

Bitwise Round Key Addition σ .

$\sigma[k^t]$ consists of the bitwise addition of a round key k^t .

$$\sigma[k^t] : b = \sigma[k^t](a) \Leftrightarrow b = a \oplus k^t$$

The Round Key Evolution ψ .

The round keys k^t are derived iteratively from the cipher key K in the following way.

$$\begin{aligned}k^0 &= K \\ k^t &= \psi(k^{t-1})\end{aligned}$$

where ψ is an invertible affine transformation and $k^{t+1} = \psi(k^t)$ is defined by

$$\begin{aligned}k_0^{t+1} &= k_0^t \oplus \text{rotl}(k_3^t) \oplus C_t \\ k_1^{t+1} &= k_1^t \oplus k_0^{t+1} \\ k_2^{t+1} &= k_2^t \oplus k_1^{t+1} \\ k_3^{t+1} &= k_3^t \oplus k_2^{t+1}\end{aligned}\tag{1}$$

where $\text{rotl}(a_i)$ is a left byte-rotation operation on a row as

$$\text{rotl}[a_{i,0}a_{i,1}a_{i,2}a_{i,3}] = [a_{i,1}a_{i,2}a_{i,3}a_{i,0}]$$

and the round constants C_t are also defined iteratively as

$$\begin{aligned}C_0 &= 1_x \\ C_t &= 2_x \cdot C_{t-1}\end{aligned}$$

We notice that the key schedule of SQUARE does not depend on the total round number.

The Cipher SQUARE

The t th round function is denoted by $\rho[k^t]$:

$$\rho[k^t] = \sigma[k^t] \circ \pi \circ \gamma \circ \theta$$

SQUARE is defined as eight rounds preceeded by a key addition $\sigma[k^0]$ and by θ^{-1} :

$$\begin{aligned}\text{SQUARE}[k] &= \rho[k^8] \circ \rho[k^7] \circ \rho[k^6] \circ \rho[k^5] \circ \\ &\rho[k^4] \circ \rho[k^3] \circ \rho[k^2] \circ \rho[k^1] \circ \sigma[k^0] \circ \theta^{-1}\end{aligned}$$

As a safety margin, the designers fixed the number of rounds to eight. However, the designers also allow conservative users to increase the number of rounds in a straight way.

3.1.2 Related Cipher Attack on SQUARE

From the description of SQUARE, it is noted that the key schedule of SQUARE does not depend on the total round number. So SQUARE ciphers with different round numbers are related. If the same key is used in SQUARE with different round number, then the related cipher attack can be applied.

Denote c^r as the ciphertext of r round SQUARE and $c^{r+\Delta r}$ as that of $r+\Delta r$ round SQUARE. If a c^r and a $c^{r+\Delta r}$ are related to the same plaintext, they are denoted as one right pair. We apply the related cipher attack to the situations where $\Delta r = 1$ and $\Delta r = 2$.

When $\Delta r = 1$, the cipher key can be determined from only one right pair. In this case, SQUARE is reduced to only one round and the following relation holds

$$c^{r+1} = \rho[k^{r+1}](c^r) \quad (2)$$

From equation (2), the round key k^{r+1} is derived as

$$k^{r+1} = (\pi \circ \gamma \circ \theta(c^r)) \oplus c^{r+1}$$

The cipher key K can be derived from this round key directly since the key evolution ψ is invertible. This cipher key K can be used to decrypt all the messages encrypted with it.

When $\Delta r = 2$, the cipher key can be determined from two right pairs easily. In this case, SQUARE is reduced to two rounds and the following relation holds

$$c^{r+2} = \rho[k^{r+2}] \circ \rho[k^{r+1}](c^r) \quad (3)$$

Let

$$c^{r'} = \pi \circ \gamma \circ \theta(c^r)$$

then equation (3) is simplified to

$$c^{r+2} = k^{r+2} \oplus (\pi \circ \gamma \circ \theta(c^{r'} \oplus k^{r+1})) \quad (4)$$

We note the fact that one row of $(c^{r'} \oplus k^{r+1})$ is related to one column of $(c^{r+2} \oplus k^{r+2})$. So equation (4) is decomposed into four block ciphers each with 32-bit block length. These four block ciphers have the common form as

$$c = k_2 \oplus (\gamma \circ \theta(c' \oplus k_1)) \quad (5)$$

The value of k_1 (or k_2) can be determined easily from 2 pairs of (c, c') . So the round key k^{r+1} (or k^{r+2}) is known and the cipher key can be determined.

3.2 Block Cipher AES

AES is also with flexible round number: 10 for AES-128, 12 for AES-192, and 14 for AES-256 (where AES-x indicates AES with x-bit secret key). However, AES is not vulnerable to the related-cipher attack.

3.2.1 Structure of AES

We introduce only the key schedule of AES here. Its pseudo code is given in Fig. 1.

In Fig. 1, the $key[]$ represents the cipher key, Nk is the length of the cipher key in 32-bit words, Nb is the block size in words, $w[]$ is the round keys, Nr is the round number. Subword, RotWord and Rcon are some functions we will omit their illustrations here.

```

KeyExpansion(byte key[4*Nk], word w[Nb*(Nr+1)], Nk)
begin
  word temp
  i = 0
  while (i < Nk)
    w[i] = word(key[4*i], key[4*i+1],
                key[4*i+2], key[4*i+3])
    i = i+1
  end while
  i = Nk
  while (i < Nb * (Nr+1))
    temp = w[i-1]
    if (i mod Nk = 0)
      temp = SubWord(RotWord(temp)) xor Rcon[i/Nk]
    else if (Nk > 6 and i mod Nk = 4)
      temp = SubWord(temp)
    end if
    w[i] = w[i-Nk] xor temp
    i = i + 1
  end while
end

```

Fig. 1. Pseudo code for AES key schedule

3.2.2 AES Is Able to Resist the Related-Cipher Attack

From the description of the AES key schedule, we see that the key schedule of AES depends on the key length Nk . It is thus impossible for the same key being used in the AES with different round numbers. Even if a 256-bit key is the repeat of a 128-bit key and both of them are used to encrypt the same message, the related-cipher attack could not be applied since the key schedule of AES-256 is slightly different from that of AES-128. We see that AES is able to resist the related cipher attack because the relationship between the key length and the round number is fixed. It is thus avoided that the same key being used in the related ciphers.

3.3 A New AES Key Schedule

At ACISP2002, a new AES key schedule [12] was proposed. However, we will show that this new key schedule is weaker than the original one under the related-cipher attack.

3.3.1 Description of the New AES Key Schedule

We introduce only the new key schedules for AES-192 and AES-256 here.

```

Let  $p = 8$ ,  $Nr = 12$  for AES-192
     $p = 16$ ,  $Nr = 14$  for AES-256
for  $r = 0$  to  $Nr$ 
    for  $j = 0$  to 15
         $a_j = Mk_j \oplus S[r \times 16 + j] \oplus S[MK_{j+p}]$ 
         $a_j = Mk_{j+p} \oplus S[r \times 16 + j] \oplus S[MK_j]$ 
    for  $i = 0$  to 2
        ByteSub( $a$ )
        ShiftRow( $a$ )
        MixColumn( $a$ )
        AddRoundKey( $a, b$ )
     $KR_r = a$ 

```

Fig. 2. Pseudo code for the new AES key schedule

In Fig. 2, each Mk_j represents one byte of the cipher key. ByteSub, ShiftRow, MixColumn and AddRoundKey are the components of the AES round function. $S[]$ is the S-box used in AES. Each KR_r represents a 128-bit round key.

3.3.2 Weakness in the New AES Key Schedule

We consider the following scenario. Consider that a 64-bit key being used in AES-192 and AES-256. And very likely the 64-bit key is concatenated to form the 192 and 256-bit key, respectively. Then the first 12 round keys for AES-192 and AES-256 would be identical. Now an attack could be applied to the last two rounds of AES-256.

4 Method to Resist the Related Cipher Attack

In Section 3, we applied the related-attack on SQUARE, AES and a new AES key schedule. AES is able to resist the attack. In this section, we introduce a general method to resist the related-cipher attack on block ciphers with flexible round number: relating the key schedule to the total round number. So when the same key is used to encrypt the same plaintext, the intermediate value after the i th round in the r round cipher should be quite different from that in the r' round cipher ($r \neq r'$).

The actual implementation that relates the key schedule to the total round number may vary from cipher to cipher. In the following example, we show how to relate the key schedule of SQUARE to the total round number. The original key schedule of SQUARE is maintained and additional modification is carried out on the subkeys.

After the original key schedule of SQUARE, we denote all the subkeys as k_1, \dots, k_n (each one is one byte). The additional modification is carried out in this way:

for $i = 1$ **to** n **do**
 $k_i = S_\gamma[k_i + S_\gamma[r]];$

where S_γ is the S -box used in SQUARE and r is the total round number. We expect that SQUARE with this modified key schedule could resist the related-cipher attack.

Since 8 round SQUARE is in use now, we suggest to keep the 8-round SQUARE the same as in [3], but those SQUARE with increased round number may adopt this strengthened key schedule.

5 Conclusion

In this paper, we introduced the related-cipher attack and applied this attack to some block ciphers with flexible round number. A Block cipher with flexible round number but with key schedule unrelated to the total round number is vulnerable to this attack. Care should be taken in designing ciphers with flexible features. A method to resist related cipher attack by relating the key schedule to the total round number is also suggested.

After introducing the related-cipher attack, we can classify the differential attack as related-message attack (the original differential cryptanalysis), related-key attack and related-cipher attack. Any combination of these attacks also gives a new attack. We believe that the cipher design should take all these attacks into consideration.

References

1. E. Biham and A. Shamir. Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.
2. E. Biham. New Types of Cryptanalytic Attacks Using Related Keys. In T. Helleseeth, editor, Advances in Cryptology: Proc. of Eurocrypt '93, LNCS 765, pages 398-409, Springer-Verlag, 1994.
3. J. Daemen, L. Knudsen and V. Rijmen. The Block Cipher SQUARE. In E. Biham, editor, Fast Software Encryption – Proc. Forth International Workshop, Haifa, Israel, January 1997, LNCS 1267, pages 13-27, Springer Verlag, 1997.
4. C. Harpes and J.L. Massey. Partitioning Cryptanalysis. In E. Biham, editor, Fast Software Encryption: Forth International Workshop, Haifa, Israel, January 1997, LNCS 1267, pages 13-27, Springer Verlag, 1997.
5. L.R. Knudsen. Truncated and higher order differentials. In B. Preneel, editor, Fast Software Encryption: Second International Workshop, Leuven, Belgium, 1994, LNCS 1008, pages 196-211, Springer Verlag, 1995.
6. L.R. Knudsen and M.J.B. Robshaw. Non-Linear Approximations in Linear Cryptanalysis. In U. Maurer, editor, Advances in Cryptology – Eurocrypt'96, LNCS 1070, pages 224-235. Springer Verlag, 1995.
7. X. Lai. Higher order derivatives and differential cryptanalysis. In Proc. "Symposium on Communication, Coding and Cryptography", in honor of James L. Massey on the occasion of his 60'th birthday, Feb. 10-13, 1994, Monte-Verita, Ascona, Switzerland, 1994.

8. S.K. Langford and M.E. Hellman. Differential-linear cryptanalysis. In Y. G. Desmedt, editor, *Advances in Cryptology – Proc. Crypto'94*, LNCS 839, pages 17-26. Springer Verlag, 1994.
9. B.S. Kaliski Jr. and M.J.B. Robshaw. Linear Cryptanalysis Using Multiple Approximations. In Y. G. Desmedt, editor, *Advances in Cryptology – Proc. Crypto'94*, LNCS 839, pages 27-39. Springer Verlag, 1994.
10. J. Massey. SAFER K-64: A Byte-Oriented Block-Ciphering Algorithm. In R. Anderson, editor, *Fast Software Encryption – Proc. Cambridge Security Workshop*, Cambridge, U.K., Dec. 9-11, 1993, LNCS 809, Springer-Verlag, pp.1-17. [See also: SAFER K-64: One Year Later. In B. Preneel, editor, *Fast Software Encryption-- Proceedings of the Second International Workshop on Fast Software Encryption*, Springer-Verlag, 1995, pp.212-241; and Strengthened Key Schedule for the Cipher SAFER, posted to the USENET newsgroup sci.crypt, September 9, 1995]
11. M. Matsui, Linear Cryptanalysis Method for DES Cipher. In T. Hellesest, editor, *Advances in Cryptology – Proc. of Eurocrypt '93*, LNCS 765, pages 386-397, Springer-Verlag, 1994.
12. L. May, M. Henricksen, W. Millan, G. Carter, and E. Dawson, Strengthening the Key Schedule of the AES. In *Information Security and Privacy – Proc. of ACISP 2002*, LNCS 2384, pages 226-240.
13. National Institute of Standards and Technology, Advanced Encryption Standard. Available at <http://csrc.nist.gov/encryption/aes/>