Related-key Attacks on Triple-DES and DESX Variants

Raphael C.-W. Phan

Department of Engineering, Swinburne Sarawak Institute of Technology,
1st Floor, State Complex, 93576 Kuching, Malaysia
rphan@swinburne.edu.my

Abstract. In this paper, we present related-key slide attacks on 2-key and 3-key triple DES, and related-key differential and slide attacks on two variants of DESX. First, we show that 2-key and 3-key triple-DES are susceptible to related-key *slide* attacks. The only previously known such attacks are related-key *differential* attacks on 3-key triple-DES. Second, we present a related-key differential attack on DESX+, a variant of the DESX with its pre- and post-whitening XOR operations replaced with addition modulo 2^{64}. Our attack shows a counter-intuitive result, that DESX+ is weaker than DESX against a related-key attack. Third, we present the first known attacks on DES-EXE, another variant of DESX where the XOR operations and DES encryptions are interchanged. Further, our attacks show that DES-EXE is also weaker than DESX against a related-key attack. This work suggests that extreme care has to be taken when proposing variants of popular block ciphers, that it is not always newer variants that are more resistant to attacks.

1 Introduction

Due to the DES' small key size of 56 bits, variants of the DES under multiple encryption have been considered, including double-DES under one or two 56-bit key(s), and triple-DES under two or three 56-bit keys. Another variant based on the DES is the DESX [9].

In this paper, we consider the security of 2-key and 3-key triple-DES against *related-key slide attacks*, and the security of DESX variants against both *related-key slide and related-key differential attacks*. We point out that our results on the DESX variants do not invalidate the security proofs of [9, 10], but serve to illustrate the limitations of their model. In particular, we argue that one should also consider a more flexible model that incorporates related-key queries [1, 7, 8].

1.1 Our model

Related-key attacks are those where the cryptanalyst is able to obtain the encryptions of certain plaintexts under both the unknown secret key, K, as well as an unknown related key, K' whose relationship to K is known, or can even

be chosen [1, 7, 8]. Most researchers consider related-key attacks as strictly theoretical and which involves a strong and restricted attack model. However, as has been demonstrated by several researchers such as [7, 8], some of the current real-world cryptographic implementations may allow for practical related-key attacks. Examples of such instances include key-exchange protocols and hash functions, details of which we refer the reader to [7, 8].

1.2 Outline of the paper

We briefly recall previous attacks on variants of triple-DES and DESX in Section 2. In Section 3, we present our related-key slide attacks on 2-key and 3-key triple-DES. We then present in Section 4 related-key attacks on DESX+ [9], a variant of DESX that replaces the pre- and post-whitening XOR operations with additions modulo 2^{64}; and DES-EXE [6], a DESX variant with its outer XOR operations interchanged with the inner DES encryption. We show that these variants are weaker than the original DESX against related-key attacks. We conclude in Section 5.

2 Previous Work

We review in this section, previous attacks on variants of triple-DES and of DESX.

Two-key triple-DES can be broken with a meet-in-the-middle (MITM) attack requiring 2^{56} *chosen-plaintexts* (*CP*s), 2^{56} memory and 2^{56} single DES encryptions [12]. There is also an attack by van Oorschot and Wiener [13] that requires m *known-plaintexts* (*KP*s), m words of memory and approximately $2^{120-log_2\ m}$ single DES encryptions. For $m = 2^{56}$, the number of encryptions is roughly 2^{114}.

Meanwhile, the most basic attack on three-key triple-DES is the MITM attack which requires 3 chosen plaintexts, 2^{56} memory and 2^{112} single DES encryptions. In [11], Lucks proposed an attack that requires 2^{32} known plaintexts, 2^{88} memory and roughly 2^{106} single DES encryptions. There is also a related-key differential attack by Kelsey et. al [7] that works with one known plaintext, one related-key chosen ciphertext (*RK-CC*), and 2^{56} single DES encryptions. [1]

As for DESX, Daemen proposed an attack [5] requiring 2^{32} chosen plaintexts and 2^{88} single DES encryptions, or 2 known plaintexts and 2^{120} single DES encryptions. Meanwhile, another attack by Kilian and Rogaway [9, 10] requires m known plaintexts and $2^{118-log_2\ m}$ single DES encryptions. For $m = 2^{32}$, the number of encryptions is roughly 2^{113}. By making use of related-key queries, Kelsey et. al [8] demonstrated an attack that requires 2^6 related-key known plaintexts (*RK-KP*s) and 2^{120} single DES encryptions. Recently, Biryukov and

[1] As pointed out by an anonymous referee, our estimates are independent of the memory access time in contrast to the approach taken in [14], and hence we assume no difference between memory with slow access and memory with intensive access. Such a general approach has been adopted in this paper to maintain uniformity with other previous results.

Wagner [4] presented a more efficient attack requiring $2^{32.5}$ known plaintexts, $2^{32.5}$ memory and $2^{87.5}$ single DES encryptions.

3 Related-Key Slide Attacks on Triple-DES

3.1 Attacking 3-key Triple-DES

We first consider the three-key triple-DES, which was attacked by a related-key differential attack in [7]. We denote such an encryption of P under key $K = (K_1, K_2, K_3)$ by:

$$C = E_{K_3}(E^{-1}_{K_2}(E_{K_1}(P))). \tag{1}$$

If we also obtain the three-key triple-DES decryption of another plaintext, $P' = E_{K_1}(P)$ under a related key $K' = (K_1, K_3, K_2)$, we will get the situation as shown in Fig. 1.

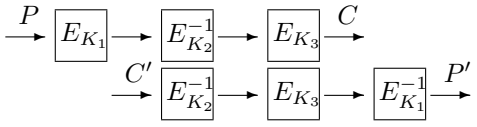

Fig.1. Sliding-with-a-twist on 3-key triple-DES of the form $E_{K_1}E^{-1}_{K_2}E_{K_3}$

We have in essence aligned the encryption, E_{K_1} *o* $E^{-1}_{K_2}$ *o* E_{K_3} under key K, with the decryption, $E^{-1}_{K_2}$ *o* E_{K_3} *o* $E^{-1}_{K_1}$ under key K' in a *sliding with a twist* [4] style. The plaintexts, P and P', and the ciphertexts, C and C' are hence related by the following slid equations:

$$C' = E_{K_1}(P) \tag{2}$$

$$P' = E^{-1}_{K_1}(C) \tag{3}$$

Our related-key slide attack works as follows:
1. Obtain 2^{32} known plaintexts, P encrypted with three-key triple-DES under the key, $K = (K_1, K_2, K_3)$
2. Obtain another 2^{32} known ciphertexts, C' decrypted with three-key triple-DES under the key, $K' = (K_1, K_3, K_2)$. Store the values of (C', P') in a table, $T1$. By the birthday paradox, we would expect one slid pair (P, C) and (P', C') such that the slid equations (2) and (3) are satisfied.
3. Guess all 2^{56} values of K_1 and do:
(i) Partially encrypt all $2^{32}P$ under the key, K_1.
(ii) Search through $T1$ for a collision of the 1st element with the result of (i). Such a collision satisfies the slid equation in (2).
(iii) For such a collision, partially decrypt C under K_1 and check for a collision of this result with the 2nd element of $T1$. The latter collision satisfies the slid

equation in (3).

The first step requires 2^{32} known plaintexts while Step 2 requires 2^{32} related-key known ciphertexts and $2^{32} \times 2 = 2^{33}$ words of memory. Step 3 requires $2^{56} \times 2^{32} = 2^{88}$ single DES encryptions, and no memory. To summarize, we have an attack on three-key triple-DES that requires 2^{32} known plaintexts, 2^{32} related-key known ciphertexts (*RK-KC*s), 2^{33} words of memory and 2^{88} single DES encryptions.

We note that a similar attack also applies to the case of three-key triple-DES of the form:

$$C = E_{K_3}(E_{K_2}(E_{K_1}(P))). \tag{4}$$

In this case, instead of sliding an encryption with a decryption, we slide two encryptions, one under the key $K = (K_1, K_2, K_3)$ and the other under $K' = (K_2, K_3, K_1)$, and obtain the situation as shown in Fig. 2.

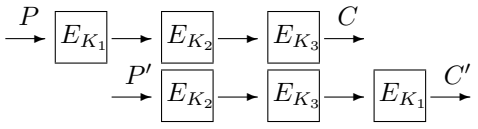

Fig.2. Sliding 3-key triple-DES of the form $E_{K_1}E_{K_2}E_{K_3}$

3.2 Attacking 2-key Triple-DES

Two-key triple-DES is also vulnerable to a related-key slide attack. We slide an encryption under the key $K = (K_1, K_2)$, with a decryption under the key $K = (K_2, K_1)$. We then have the situation in Fig. 3.

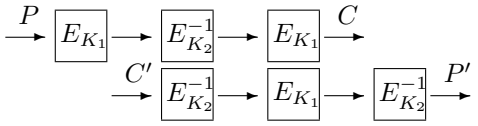

Fig.3. Sliding-with-a-twist on 2-key triple-DES of the form $E_{K_1}E_{K_2}^{-1}E_{K_1}$

We thus obtain the slid equations:

$$C' = E_{K_1}(P) \tag{5}$$

$$P' = E_{K_2}^{-1}(C) \tag{6}$$

The attack follows:

1. Obtain 2^{32} known plaintexts, P encrypted with two-key triple-DES under the key, $K = (K_1, K_2)$.
2. Obtain another 2^{32} known ciphertexts, C' decrypted with two-key triple-DES under the key, $K' = (K_2, K_1)$. Store the values of (C', P') in a table, $T1$. By the birthday paradox, we would expect one slid pair (P, C) and (P', C') such that the slid equations (5) and (6) are satisfied.
3. Guess all 2^{56} values of K_1 and do:
(i) Partially encrypt all $2^{32}P$ under the key, K_1.
(ii) Store $(E_{K_1}(P), C, K_1)$ in another table, $T2$.
4. Search through $T1$ and $T2$ for collisions in the first element, which immediately reveals the corresponding key, K_1. With $2^{56} \times 2^{32} = 2^{88}$ entries in $T2$, and a probability of 2^{-64} for a collision to occur, we expect $2^{88} \times 2^{-64} = 2^{24}$ values of K_1 to be suggested, and 2^{24} $(E_{K_1}(P), C, K_1)$ entries in $T2$ to survive this filtering.
5. For all 2^{24} remaining values of K_1, guess all 2^{56} values of K_2 and do:
(i) Partially decrypt $E_{K_1}(P)$ under the guessed key, K_2.
(ii) Further encrypt the result under K_1, and verify if the result is equal to C. The correct $K = (K_1, K_2)$ should satisfy this due to (5). Repeat with another plaintext-ciphertext pair if necessary.

The first step requires 2^{32} known plaintexts while Step 2 requires 2^{32} related-key known ciphertexts. Step 3 requires $2^{56} \times 2^{32} = 2^{88}$ single DES encryptions, and $2^{88} \times 3 \approx 2^{89.5}$ words of memory. Step 4 is negligible while Step 5 requires $2^{24} \times 2^{56} \times 2 = 2^{81}$ single DES encryptions, and no memory. To summarize, we have an attack on two-key triple-DES that requires 2^{32} known plaintexts, 2^{32} related-key known ciphertexts, $2^{89.5}$ words of memory and 2^{88} single DES encryptions.

4 Related-Key Attacks on DESX Variants

DESX encryption is denoted by:

$$C = K_b \oplus E_K(P \oplus K_a). \tag{7}$$

In this section, we will present related-key attacks on two DESX variants, namely the DESX+ [9] and the DES-EXE [6].

4.1 An Attack on DESX+

It was suggested in [9] to replace the XOR pre- and post-whitening steps in DESX by addition modulo 2^{64}, to obtain the DESX variant which we call DESX+, denoted by:

$$C = K_b + E_K(P + K_a) \tag{8}$$

where + denotes addition modulo 2^{64}. We show here that this variant can be attacked by a related-key attack. The key observation is that if we obtain the DESX+ encryption of P under key, $K = (K_a, K, K_b)$, and also obtain the DESX+ encryption of P under key $K' = (K_a, K, K'_b) = (K_a, K, K_b \oplus \triangle)$, where $K_b \oplus K'_b = \triangle$ is any arbitrary known difference, then the two encryptions are related pictorially as in Fig. 4.

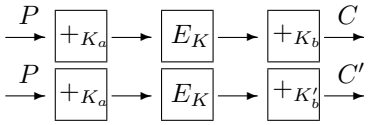

Fig.4. Related-key differential attack on DESX+

Here, $+_{K_a}$ denotes addition modulo 2^{64} with K_a. Notice that we started off with the same plaintext, P, and the similarity between the two encryptions remains until just before $+_{K_b}$.
Based on this observation, our related-key differential attack is given by:
1. Obtain the DESX+ encryption of P under key, $K = (K_a, K, K_b)$, and denote that as C.
2. Obtain the DESX+ encryption of P under key $K' = (K_a, K, K'_b) = (K_a, K, K_b \oplus \triangle)$, and denote that as C'.
3. Guess all 2^{64} values of K_b, and do:
(i) Compute $X = C - K_b$.
(ii) Compute $X' = C' - K'_b$.
(iii) If $X = X'$, then the guessed K_b could be the right key value. The right key value would always satisfy this condition, whereas a wrong key value would satisfy this only with some probability, hence the number of possible values of K_b is reduced. Wrong key values can be easily checked against a trial encryption in the second analysis phase.

We have implemented this attack on a scaled-down generalization of DESX+, which we call FX32+, whose ciphertext, C is defined as:

$$C = K_b + F_K(P + K_a) \tag{9}$$

Here, F denotes a random function, and P, C, K_a, K_b, and K are all 32 bits instead of 64. The execution takes just less than 1 minute on a Pentium 4, 1.8GHz machine with 256MB RAM, running on Windows XP. The correct K_b value is always suggested, while the number of wrong key values suggested ranges from $O(1)$ to $O(2^{31})$, depending on the hamming weight of the key difference, $\triangle$. The higher the hamming weight, the more efficient the filtering of wrong key values. An anonymous referee remarked that as the only difference between XOR and modulo addition lies in the carries, and that if the addition with K_b generates no carries, the attack on DESX+ would not work since in that case

modulo addition would be the same as XOR. This possible complication can be overcome by using a $\triangle$ with a large hamming weight, or by repeating the attack with different plaintext-ciphertext pairs.

Once K_b is obtained in this way, the remaining keys K_a and K can be obtained from exhaustive search of 2^{120} single DES encryptions. But we can do better than that. We use K_b to peel off the $+_{K_b}$ operation, and apply a basic MITM attack on the remaining cipher that requires 2^{56} words of memory and 2^{56} DES encryptions [12]. Alternatively, we could reverse the roles of the plaintexts and ciphertexts, and repeat our attack to recover K_a in a similar way. What remains is then a single DES which can be attacked by exhaustive key search of 2^{56} values.

The main bulk of this attack is step 3, requiring $2^{64} \times 2 = 2^{65}$ modulo subtractions, which is negligible, so most of the work needed lies in the exhaustive key search of the remaining keys or an MITM attack on the remaining double-DES.

In summary, we have a related-key differential attack on DESX+ that requires 1 known plaintext, P encrypted under the secret key, K and related key, K', and 2^{120} single DES encryptions. The work complexity is similar to the attack on DESX in [8], but the text complexity is much less. Alternatively, our attack could work with the same text complexity but with 2^{56} words of memory and 2^{56} single DES encryptions. In this case, when memory is available, then both the text and work complexities are much less than those in [8].

Ironically, the original DESX with XOR for pre- and post-whitening is resistant to this attack. Therefore, this is the first attack for which the original DESX is stronger than the DESX+. This is counter-intuitive since the common belief is that the XOR operation is weaker than modulo addition. [2]

4.2 Attacks on DES-EXE

In [6], the authors posed the question of whether, DES-EXE, a DES variant of the form:

$$C = E_{K_b}(K \oplus E_{K_a}(P))) \tag{10}$$

would be stronger or weaker than DESX. Note that the DES-EXE is simply the DESX with its XOR operations in the pre- and post-whitening stage interchanged with the DES encryption in the middle.

Consider a key, $K = (K_a, K, K_b)$, and a related key, $K' = (K_b, K, K_a)$. Then, the encryptions under these two related keys could be slid as shown in Fig. 5.

[2] Except in the work by Biham and Shamir [2, 3] that showed how replacing XOR with addition in certain locations in the DES can significantly weaken the DES.

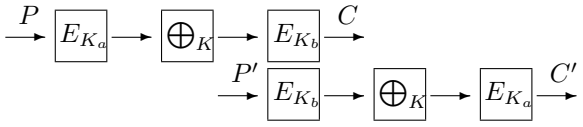

Fig.5. Sliding DESX-EXE

Therefore, we have the slid equations:

$$P' = E_{K_a}(P) \oplus K, \tag{11}$$

$$E^{-1}_{K_a}(C') = C \oplus K. \tag{12}$$

XORing (10) and (11), we obtain:

$$P' \oplus E^{-1}_{K_a}(C') = E_{K_a}(P) \oplus C. \tag{13}$$

A related-key slide attack proceeds as follows:
1. Obtain 2^{32} known plaintexts, P encrypted with DES-EXE under the key, $K = (K_a, K, K_b)$.
2. Obtain another 2^{32} known plaintexts, P' encrypted with DES-EXE under the key, $K = (K_b, K, K_a)$. Store the values of (P', C') in a table, $T1$. By the birthday paradox, we would expect one slid pair (P, C) and (P', C') such that the slid equations (10) and (11), and hence (12) are satisfied.
3. Guess all 2^{56} values of K_a, and do:
(i) Compute $E_{K_a}(P) \oplus C$ for all (P, C) and store $(E_{K_a}(P) \oplus C, K_a)$ in a table, $T1$.
(ii) Compute $P' \oplus E^{-1}_{K_a}(C')$ for all (P', C') and store $(P' \oplus E^{-1}_{K_a}(C'), K_a)$ in a table, $T2$.
4. Search through $T1$ and $T2$ for a collision in the first entry, which immediately reveals the key, K_a.

The remaining keys can be obtained via exhaustive search, or we could use K_a to peel off one layer and apply an MITM attack on the remaining two layers requiring 2^{56} words of memory and 2^{56} DES encryptions.

Step 1 requires 2^{32} known plaintexts while Step 2 requires 2^{32} related-key known plaintexts. Step 3 requires $2^{56} \times 2^{32} \times 2 = 2^{89}$ single DES encryptions, and $2^{88} \times 3 \times 2 \approx 2^{90.5}$ words of memory. Step 4 is negligible. Meanwhile, exhaustive search of the remaining keys requires $2^{56} \times 2^{64} = 2^{120}$ single DES encryptions, or an alternative MITM attack requires 2^{56} memory and 2^{56} DES encryptions. To summarize, we have an attack on DES-EXE that requires 2^{32} known plaintexts, 2^{32} related-key known plaintexts, $2^{90.5}$ words of memory and 2^{89} single DES encryptions.

A better attack works by observing that if we obtain the encryption, C of a plaintext, P under the key $K = (K_a, K, K_b)$, and subsequently obtain the

decryption of C under the key $K' = (K'_a, K, K_b) = (K_a \oplus \triangle, K, K_b)$ where $\triangle$ is any arbitrary known difference, then we get the situation as indicated in Fig. 6.

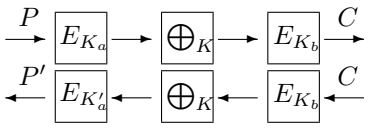

Fig.6. Related-key differential attack on DESX-EXE

Here, $\oplus_K$ denotes an XOR operation with the key, K. The following relation then applies:

$$P' = E^{-1}_{K_{a'}}(E_{K_a}(P)). \tag{14}$$

For all 2^{56} values of K_a, check that (13) satisfies, and K_a can be recovered with 2^{56} encryptions. Use this to peel of the first layer, and apply an MITM attack on the remaining two layers, requiring 2^{56} memory and 2^{56} encryptions [12]. In summary, we require one known plaintext, one related-key chosen ciphertext, 2^{56} words of memory and 2^{56} single DES encryptions. This shows that DES-EXE is much weaker than the original DESX against a related-key differential attack.

5 Conclusions

We have presented related-key slide attacks on 2-key and 3-key triple-DES. Our attacks are the first known related-key slide attacks on these triple-DES variants.

We have also presented attacks on DESX variants. In particular, we showed that contrary to popular belief, the DESX+, a DESX variant that uses addition modulo 2^{64} for its pre- and post-whitening, is weaker than DESX against a related-key differential attack. Our attacks on DES-EXE, another DESX variant with the outer XOR operations interchanged with the middle DES encryption, also show that DES-EXE is much weaker than the original DESX against related-key attacks. In Tables 1 and 2, we present a comparison of our attacks with previous attacks on variants of triple-DES and DESX.

6 Acknowledgement

We would like to thank David Naccache for his interest and comments on our attacks on triple-DES. We are grateful to the anonymous referees whose numerous suggestions helped to improve this paper. We also thank God for His many blessings (Ps. 33).

Table 1. Comparison of Attacks on Triple-DES Variants

Block Cipher	Texts	Memory	DES Encryptions	Source
2-key Triple-DES	2^{56} CP	2^{56}	2^{56}	[12]
2-key Triple-DES	2^{56} KP	2^{56}	2^{114}	[13, 14]
2-key Triple-DES	2^{32} KP, 2^{32} RK-KC	$2^{89.5}$	2^{88}	This paper
3-key Triple-DES	3 CP	2^{56}	2^{112}	[12]
3-key Triple-DES	1 KP, 1 RK-CC	2^{56}	2^{56}	[7]
3-key Triple-DES	2^{32} KP	2^{88}	2^{106}	[11]
3-key Triple-DES	2^{32} KP, 2^{32} RK-KC	2^{33}	2^{88}	This paper

Table 2. Comparison of Attacks on DESX Variants

Block Cipher	Texts	Memory	DES Encryptions	Source
DESX	2^{32} CP	-	2^{88}	[5]
DESX	2 KP	-	2^{120}	[5]
DESX	2^{32} KP	-	2^{113}	[9, 10]
DESX	2^{6} RK-KP	-	2^{120}	[8]
DESX	$2^{32.5}$ KP	$2^{32.5}$	$2^{87.5}$	[4]
DESX+	1 RK, 1 RK-KP	-	2^{120}	This paper
DESX+	1 RK, 1 RK-KP	2^{56}	2^{56}	This paper
DES-EXE	2^{32} KP, 2^{32} RK-KP	$2^{90.5}$	2^{89}	This paper
DES-EXE	1 KP, 1 RK-CC	2^{56}	2^{56}	This paper

References

1. E. Biham, "New Types of Cryptanalytic Attacks Using Related Keys", Advances in Cryptology - Eurocrypt'93, Lecture Notes in Computer Science, Vol. 765, pp. 398–409, Springer-Verlag, 1994.
2. E. Biham and A. Shamir, "Differential Cryptanalysis of the Full 16-round DES", Advances in Cryptology - CRYPTO'92, Lecture Notes in Computer Science, Vol. 740, pp. 487–496, Springer-Verlag, 1993.
3. E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", Journal of Cryptology, Vol. 4, No.1, pp. 3–72, 1991.
4. A. Biryukov and D. Wagner, "Advanced Slide Attacks", Advances in Cryptology - Eurocrypt'00, Lecture Notes in Computer Science, Vol. 1807, pp. 589–606, Springer-Verlag, 2000.
5. J. Daemen, "Limitations of the Even-Mansour Construction", Advances in Cryptology - Asiacrypt'91, Lecture Notes in Computer Science, Vol. 739, pp. 495–498, Springer-Verlag, 1992.
6. B. S. Kaliski and M. J. B. Robshaw, "Multiple Encryption: Weighing Security and Performance", Dr. Dobb's Journal, 1996.
7. J. Kelsey, B. Schneier and D. Wagner, "Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER and Triple-DES", Advances in Cryptology - Crypto'96, Lecture Notes in Computer Science, Vol. 1109, pp. 237–251, Springer-Verlag, 1996.

8. J. Kelsey, B. Schneier and D. Wagner, "Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA", ICICS'97, Lecture Notes in Computer Science, Vol. 1334, pp. 233–246, Springer-Verlag, 1997.
9. J. Kilian and P. Rogaway, "How to Protect DES Against Exhaustive Key Search", Advances in Cryptology - Crypto'96, Lecture Notes in Computer Science, Vol. 1109, pp. 252–267, Springer-Verlag, 1996.
10. J. Kilian and P. Rogaway, "How to Protect DES Against Exhaustive Key Search (an Analysis of DESX)", Journal of Cryptology, Vol. 14, No.1, pp. 17–35, 2001.
11. S. Lucks, "Attacking Triple Encryption", Advances in Cryptology - FSE'98, Lecture Notes in Computer Science, Vol. 1372, pp. 239–253, Springer-Verlag, 1998.
12. R. C. Merkle and M. E. Hellman, "On the Security of Multiple Encryption", Communications of the ACM, Vol. 24, No.7, 1981.
13. P. C. van Oorschot and M. J. Wiener, "A Known-plaintext Attack on Two-Key Triple Encryption", Advances in Cryptology - Eurocrypt'90, Lecture Notes in Computer Science, Vol. 473, pp. 318–325, Springer-Verlag, 1990.
14. P. C. van Oorschot and M. J. Wiener, "Parallel Collision Search with Cryptanalytic Applications", Journal of Cryptology, Vol. 12, No.1, pp. 1–28, 1999.