Improved Related-key Attacks on DESX and DESX+

Raphael C.-W. Phan[1] and Adi Shamir[3]

[1] Laboratoire de sécurité et de cryptographie (LASEC),
Ecole Polytechnique Fédérale de Lausanne (EPFL), CH-1015 Lausanne, Switzerland
Raphael.Phan@epfl.ch
[2] Faculty of Mathematics & Computer Science,
The Weizmann Institute of Science, Rehovot 76100, Israel
Adi.Shamir@weizmann.ac.il

Abstract. In this paper, we present improved related-key attacks on the original DESX, and DESX+, a variant of the DESX with its pre- and post-whitening XOR operations replaced with addition modulo 2^{64}. Compared to previous results, our attack on DESX has reduced text complexity, while our best attack on DESX+ eliminates the memory requirements at the same processing complexity.

Keywords: DESX, DESX+, related-key attack, fault attack.

1 Introduction

Due to the DES' small key length 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 popular variant based on the DES is the DESX [15], where the basic keylength of single DES is extended to 120 bits by wrapping this DES with two outer pre- and post-whitening keys of 64 bits each. Also, the endorsement of single DES had been officially withdrawn by NIST in the summer of 2004 [19], due to its insecurity against exhaustive search. Future use of single DES is recommended only as a component of the triple-DES. This makes it more important to study the security of variants of single DES which increase the key length to avoid this attack.

In this paper[3], we present improved related-key attacks on DESX and DESX+. This work extends the results in [20]. Note that such attacks are applicable to any cryptosystem that uses pre/post-whitening with additional keys, rather than just to DES-based schemes. Previous related-key attacks on DESX and DESX+ have been reported in [14] and [20]

[3] A summary of prelim results were presented in [22].

respectively. We remark here that our results on the DESX variants do not invalidate the security proofs of [15, 16], 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 [2, 13, 14].

1.1 Our model

Related-key attacks [25, 2, 13, 14] are those where the cryptanalyst is able to obtain the encryptions of plaintexts under both the unknown secret key, K, as well as an unknown related key, K' whose relationship to K is known, or can be chosen [25, 2, 13, 14]. Natural generalizations consider several more related keys e.g. 2^2 [3], 2^8 [12] or up to 2^{16} [13]. Most related-key attacks use related keys with a chosen key difference. For instance, the related-key attacks in [2] require two related keys such that some round key bits match, the recent attack on full SHACAL-1 [4] requires 2 to 2^3 related keys satisfying specific relations on all key bits; the attacks on full KASUMI [4] require 2^2 related keys that differ in only one bit between each related key pair; and the recent [17] best known related-key attacks on AES-192 and AES-256 require 2^6 related keys satisfying strict relationships between them.

The first variant of our attack on DESX in Section 3 uses related keys that differ by some known difference in the pre- or post-whitening key, while the second requires related keys where the pre- or post-whitening keys are negations of each other. While our basic attack on DESX+ in Section 4.1 requires 2^6 related keys with specific chosen bit differences, our more efficient attack in Section 4.2 requires just 2 related keys where the pre- or post-whitening keys are complements of each other.

Some 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 [25, 13, 14, 10, 21, 23], some of the current real-world cryptographic implementations may allow for practical related-key attacks. Examples of such instances include key-exchange protocols, hash functions and cryptoprocessors, details of which we refer the reader to [25, 13, 14, 10, 21, 23]. In a different direction, the security against related-key attacks has been considered in the theoretical provable security setting [1, 18, 24] as well.

1.2 Outline of the paper

We briefly recall previous attacks on DESX and DESX+ in Section 2. In Sections 3 and 4, we present our improved related-key attacks on DESX and DESX+ respectively. We also discuss in Section 5 how to apply our analysis as part of a fault attack. We conclude in Section 6.

2 Previous Work

We review in this section all previously known attacks on DESX and DESX+.

In the non-related key setting, Daemen [11] presented an attack on DESX that requires 2^{32} chosen plaintexts (CPs) and 2^{88} single DES encryptions, or 2 known plaintexts (KPs) and 2^{120} single DES encryptions; Kilian and Rogaway [15, 16] gave an attack requiring m known plaintexts and $2^{118-log_2\ m}$ single DES encryptions, i.e. for $m = 2^{32}$, the number of encryptions is approximately 2^{113}; and Biryukov and Wagner [9] gave an attack requiring $2^{32.5}$ known plaintexts, $2^{32.5}$ memory and $2^{87.5}$ single DES encryptions.

Kelsey et. al [14] presented a related-key attack on DESX that requires 2^7 related-key known plaintexts (RK-KPs) and 2^{56} single DES encryptions.

Meanwhile, Phan [20] presented two related-key attacks on DESX+ requiring 2 related-key known plaintexts, 2^{120} single DES encryptions and no memory, or similar texts, 2^{56} single DES encryptions and 2^{56} memory. These are the only known attacks on DESX+.

Comparing these previous results, it appears that DESX is stronger than DESX+. Our results in the next few sections will further strengthen this fact.

3 Related-Key Attacks on DESX

In this section, we will present two variants of improved related-key attacks on DESX. First, we define DESX encryption, denoted by:

$$C = K_b \oplus E_K(P \oplus K_a), \tag{1}$$

where $E_K(\cdot)$ denotes DES encryption under key K. Note that DESX is basically single DES encryption with pre- and post-whitening via exclusive-OR (XOR).

The intuition used in our attack is that if we obtain the encryptions of a plaintext P under K_b and K_b' where $K_b' = (K_b \pm D) \bmod 2^n$, to get the ciphertexts C and C' respectively, then:

$$E_K(P \oplus K_a) \oplus K_b = X \oplus K_b = C \tag{2}$$

$$E_K(P \oplus K_a) \oplus K_b' = X \oplus K_b' = C'. \tag{3}$$

XORing both equations, we obtain:

$$C \oplus C' = K_b \oplus K_b' = K_b \oplus (K_b \pm D) \bmod 2^n. \tag{4}$$

This is illustrated in Fig. 1, where $\bigoplus_{K_a}$ denotes XORing with K_a. Notice that we started off with the same plaintext, P, and the similarity between the two encryptions remains until just before $\bigoplus_{K_b}$.

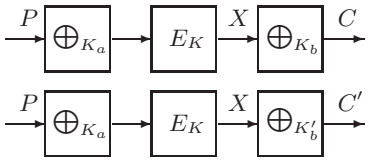

Fig. 1. Related-key differential attack on DESX

Since the Left Hand Side (LHS) of equation (4) is known, and the difference, D between the keys is also known, we can try all possible values of K_b and verify if the RHS equals to the LHS. Each verification requires 2 XOR operations and 1 modulo addition, which is negligible. With the correct choice of D, this reduces the keyspace of K_b considerably, and so repeating the attack up to 3 times with different plaintexts, Ps or key difference, Ds will leave only two possible choices of K_b, one of which is the correct key.

In total, we need 3 pairs of related-key known plaintexts (6 RK-KPs), neglibile effort and memory. Once K_b is obtained, use it to peel off the last key XOR, and simply do a meet-in-the-middle attack requiring 2^{56} single DES encryptions and 2^{64} memory. Alternatively, repeat the attack in the reverse direction with related-key known ciphertexts to obtain K_a with similar complexities. We are then left with the single DES encryption which can be brute-forced with 2^{56} single DES encryptions.

Alternatively, we let $K_b' = -K_b \bmod 2^n$. Then XORing equations (2) and (3):

$$C \oplus C' = K_b \oplus K_b' = K_b \oplus (-K_b) \bmod 2^n = K_b \oplus (\overline{K_b} + 1) \bmod 2^n. \tag{5}$$

Trying all possible keys K_b and checking for equality with the LHS allows to reduce the keyspace after repeating a few times. With K_b recovered, the attack is repeated in reverse to obtain K_a.

In summary, we can attack DESX with $6 \times 2 \approx 2^{3.5}$ related-key known plaintexts/ciphertexts (RK-KPs), and 2^{56} single DES encryptions. The amount of required texts is less than Kelsey et. al's attack.

4 Related-Key Attacks on DESX+

We now discuss two related-key differential attacks on DESX+. First, we define DESX+ as

$$C = K_b + E_K(P + K_a). \tag{6}$$

4.1 A Basic Attack

Let ΔK_b denote the difference betweeen K_b and K_b' with respect to XOR, X denote the intermediate state just before modulo addition with K_b or K_b', $C[i]$ denote the ith bit (for $i = \{0, \ldots, 63\}$), and bit i means the bit that is set in the value 2^i. Our related-key differential attack is as follows:

1. Choose $\Delta K_b = \epsilon[i]$ which denotes a '1' in bit i and 0 elsewhere.
2. Obtain the DESX+ encryption of P under both $K = (K_a, K, K_b)$ and $K' = (K_a, K, K_b') = (K_a, K, K_b \oplus \triangle K)$, and denote them as C and C' respectively. Refer to Fig. 2.
3. Compare between $C[i+1]$ and $C'[i+1]$, and between $C[i]$ and $C'[i]$.

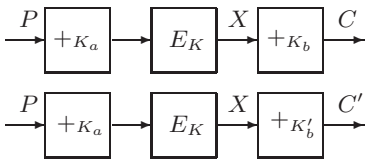

Fig. 2. Attack 1: Related-key differential attack on DESX+

Note that the only difference between K_b and K_b' is in the ith bit. $C[i+1]$ and $C'[i+1]$ might be different due to a carry over from bit i, caused by the addition of $X[i]$ and $K_b[i]$ (resp. $K_b'[i]$), and a possible carry over from bit i-1 (denoted as $CY[i-1]$).

Possible values of $X[i]$, $K_b[i]$ (resp. $K_b[i]'$) and $CY[i-1]$ that cause a carry over from bit i into $C[i+1]$ (resp. $C[i+1]'$), are given in Table 1 (resp. Table 2).

Table 1. Values of $X[i]$, $K_b[i]$, and $CY[i-1]$ causing a carry from bit i

$X[i]$	$K_b[i]$	$CY[i-1]$	Carry into $C[i+1]$?	Value of $C[i]$
0	0	0	No	0
0	0	1	No	1
0	1	0	No	1
0	1	1	Yes	0
1	0	0	No	1
1	0	1	Yes	0
1	1	0	Yes	0
1	1	1	Yes	1

Table 2. Values of $X[i]$, $K_b'[i]$, and $CY[i-1]$ causing a carry from bit i

$X[i]$	$K_b'[i]$	$CY[i-1]$	Carry into $C'[i+1]$?	Value of $C'[i]$
0	1	0	No	1
0	1	1	Yes	0
0	0	0	No	0
0	0	1	No	1
1	1	0	Yes	0
1	1	1	Yes	1
1	0	0	No	1
1	0	1	Yes	0

From the above observations, we see that for the cases where $C[i+1] = C'[i+1]$ (either with or without carries into *both* $C[i+1]$ and $C'[i+1]$), then we have the following:

$$K_b[i] = C[i] \tag{7}$$

and

$$K_b'[i] = C'[i]. \tag{8}$$

Meanwhile, for the cases where $C[i+1] \neq C'[i+1]$ (one has a carry into bit i +1 while the other does not), then we have the following:

$$K_b[i] = \overline{C[i]} \tag{9}$$

and

$$K'_b[i] = \overline{C'[i]} \tag{10}$$

where $\overline{C[i]}$ denotes the complement operation. This gives us 1 bit of K_b (as well as K'_b). We can repeat this for all bits, i (0 to 62) of K_b with corresponding $\Delta K_b = e[i]$ (for $i = 0$ to 62). This leaves us to determine the MSB of K_b via exhaustive search.

This requires 1 plaintext encrypted under K and also under 63 other different K's corresponding to $\Delta K_b = e[i]$ (for $i = 0$ to 62). The processing complexity involves the exhaustive search of the MSB which typically takes up to 2 trial encryptions. Meanwhile, memory is negligible.

After obtaining K_b, repeat the attack (see Fig. 3) but in reverse direction to obtain K_a with similar complexities. In more detail, this involves 1 ciphertext decrypted under K and under 63 other different K' corresponding to $\Delta K_b = e[i]$ (for $i = 0$ to 62).

We are then left with the single DES encryption which can be brute-forced with 2^{56} single DES encryptions, thus the overall attack complexity is reduced to that of attacking the inner single DES encryption.

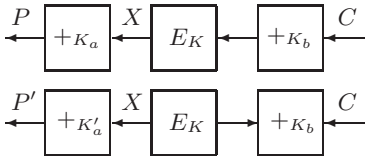

Fig. 3. Repeat the attack in reverse i.e. under decryption

Note that although this attack requires more texts than previous results [20], the gain is the reduction in the number of encryptions and the fact that no memory is required.

4.2 A More Efficient Attack

There is a more efficient related-key attack on DESX+. Let's start with an intuition. Consider if we numerically add D to the final key, K_b, then

the value of the ciphertext, C is numerically increased by D mod 2^n, and similarly if we subtract D from K_b we see the same effect on the output ciphertext, C.

Now if we complement bit i in K_b, then if K_b had a 0 the effect on both K_b and C is to add 2^i to them, and if the key had a 1 in that bit position the effect is to subtract 2^i. Since the ciphertext, C is known, we can easily determine whether we added or subtracted 2^i, except in the MSB. If the length of the key is k, we can find all its bits (except the MSB) in $k-1$ complementation tests. By using the decryption process we can similarly determine the first key, K_a which is added to the plaintext, and thus reduce the scheme to single DES which can be attacked with an exhaustive key search of 2^{56} single DES encryptions.

At first glance, this attack appears to require 63 related-key chosen plaintext queries, and 63 bit comparisons to obtain K_b, and similar complexities to obtain K_a. However, we can enhance this considerably by simultaneous attacking all bits of K_b and find K_b by using a single pair!

Let C and C' be the ciphertexts from encrypting plaintext, P (even an unknown one!) under $K = (K_a, K, K_b)$ and $K' = (K_a, K, K'_b) = (K_a, K, \overline{K}_b)$ respectively.

This simultaneously adds or subtracts 2^i to each bit position i, and as explained previously, it adds to the ciphertext a known quantity D which is the sum of all the 2^i with signs which are either $+$ or $-$. In other words, we have:

$$C' = (C + D) \texttt{ mod } 2^n, \tag{11}$$

where

$$D = \sum_{i=0}^{n-1} \pm 2^i = \pm\{1, 3, 5, \ldots, 2^n - 1\}.$$

It is easy to show that these sums are all different, and there is a very simple algorithm for recovering all the signs from D. In more detail, it is clear that

$$C - C' = (K_b - \overline{K}_b) \texttt{ mod } 2^n. \tag{12}$$

Since $-K_b = (\overline{K}_b + 1) \texttt{ mod } 2^n$, we have that

$$C - C' = (2K_b + 1) \texttt{ mod } 2^n. \tag{13}$$

By just looking at the difference of $C - C'$, we can determine all but the MSB of K_b.

In total, we need only a pair of related-key chosen plaintexts, and one comparison (subtraction) which is negligible.

After obtaining K_b, use it to peel off the last key addition, and repeat the attack in reverse direction on the first key addition to obtain K_a with similar complexities. We are then left with the single DES encryption which can be brute-forced with 2^{56} single DES encryptions.

Consequently, DESX+ is extremely weak against related key attacks - with one complementation of the final key, K_b you can recover it. Similarly for the first key, K_a. And overall the attack complexity reduces to that of attacking the inner single DES encryption.

5 Applying our Analyses as Part of a Fault Attack

We comment on how to apply our analyses of DESX and DESX+ as part of a fault attack [8] rather than a related-key attack. Fault attacks are considered weaker (and thus more realistic) than related-key differential attacks since the attacker does not choose or know the changed bits in the middle of the encryption, except that they affect a small number of internal bits (a low hamming-weight change vector). If the change affects a few bits at the output of the single DES, we can again see a numeric difference which is the sum of some $\pm 2^i$ values. Since we do not know which bits are affected, there are in principle 3^n possibilities (each bit position can contribute 0, $+2^i$, and -2^i to the sum) and a simple counting argument shows that we cannot uniquely identify the case based on the sum $\texttt{mod}\ 2^n$. In more detail, we get 3^n possible combinations of 2^0 to $2^n - 1$. On the other hand, the biggest possible value is the sum of all these powers, or $2^n - 1$, and the smallest possible value is $-(2^n - 1)$ so the range is about 2^{n+1}, which is much smaller than the number of possible partial combinations (3^n). Consequently, many combinations should be equal, and one cannot hope to uniquely determine the combination from the final value. Just to give an example, 2 can be obtained either as $(2^1 + 0 + 0 + 0 \dots)$ or as $(2^2 - 2^1 + 0 + 0 + 0 \dots)$. However, if the change pattern has low hamming weight we expect to identify the values in the sum uniquely. Note that if we are allowed to use fault attacks, then Biham and Shamir showed how to use a very small number of faults in the last few rounds of DES to find its key, requiring less than 200 faulty ciphertexts [8]. In our attack we can use the same faults used in [8], use the fact that they create a small hamming-weight change in the output of DES, and then simultaneously find the pre- and post-whitening keys K_a, K_b by our technique and the inner DES key K by the Biham-Shamir attack in [8]. The bottom line is that one needs less than 200 faulty ciphertexts (where a single bit fault is distributed uniformly over

all the steps of DESX or DESX+) and negligible additional computation to completely break these schemes (including the extraction of the inner DES key K) by fault analysis.

6 Concluding Remarks

We have presented improved related-key attacks on both the original DESX and its variant, DESX+. Our results further support the claim in [20] that the DESX+ is weaker than DESX against related-key attacks. We present a comparison of our attacks with previous attacks on DESX and DESX+ in Tables 3 and 4.

Our related-key attacks exploit the fact that differences between two encryptions are induced halfway in the middle of a cipher due to the difference between two related keys [13]. This is then used to attack that remaining half of the cipher. Our attacks also exploit the non-commutativity between the XOR and modulo addition operations. In particular, the difference operation between two related keys is chosen to be non-commutative to the whitening key mixing operation. This ensures that the difference observed between the corresponding two ciphertexts would be dependent on the key difference. Interestingly, we note as a side remark that the reason differential cryptanalysis [6, 7] works on ciphers is that there exists non-linear components within them. If all components within the ciphers were linear, then differential cryptanalysis would be ineffective against them.

Table 3. Comparison of Attacks on DESX

Block Cipher	Texts	Memory	DES Encryptions	Source
DESX	$2^{32}CP$	-	2^{88}	[11]
DESX	$2\ KP$	-	2^{120}	[11]
DESX	$2^{32}KP$	-	2^{113}	[15, 16]
DESX	$2^{r}RK\text{-}KP$	-	2^{56}	[14]
DESX	$2^{32.5}KP$	$2^{32.5}$	$2^{87.5}$	[9]
DESX	$2^{3.5}RK\text{-}KP$	-	2^{56}	This paper

References

1. M. Bellare and T. Kohno, "A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications", Advances in Cryptology - Eurocrypt

Table 4. Comparison of Related-key Attacks on DESX+

Block Cipher	Texts	Memory	DES Encryptions	Source
DESX+	2 RK-KP	-	2^{120}	[20]
DESX+	2 RK-KP	2^{56}	2^{56}	[20]
DESX+	2^7 RK-KP	-	2^{56}	This paper
DESX+	2 RK-KP	-	2^{56}	This paper

'03, Lecture Notes in Computer Science, Vol. 2656, pp. 491–506, Springer-Verlag, 2003.

2. 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.
3. E. Biham, O. Dunkelman and N. Keller, "Related-Key Boomerang and Rectangle Attacks", Advances in Cryptology - Eurocrypt '05, Lecture Notes in Computer Science, Vol. 3494, pp. 507–525, Springer-Verlag, 2005.
4. E. Biham, O. Dunkelman and N. Keller, "A Related-Key Rectangle Attack on the Full KASUMI", Advances in Cryptology - Asiacrypt '05, Lecture Notes in Computer Science, Vol. 3788, pp. 443–461, Springer-Verlag, 2005.
5. E. Biham, O. Dunkelman and N. Keller, "A Simple Related-Key Attack on the Full SHACAL-1", Topics in Cryptology - CT-RSA '07, Lecture Notes in Computer Science, Vol. 4377, pp. 20–30, Springer-Verlag, 2007.
6. 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.
7. E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", Journal of Cryptology, Vol. 4, No.1, pp. 3–72, 1991.
8. E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems", Advances in Cryptology - Crypto '97, Lecture Notes in Computer Science, Vol. 1294, pp. 513–525, Springer-Verlag, 1997.
9. 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.
10. M. Bond, "Attacks on Cryptoprocessor Transaction Sets", Proceedings of Cryptographic Hardware and Embedded Systems (CHES '01), Lecture Notes in Computer Science, Vol. 2162, pp. 220–234, Springer-Verlag, 2001.
11. 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.
12. N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner and D. Whiting, "Improved Cryptanalysis of Rijndael", Proceedings of Fast Software Encryption (FSE '00), Lecture Notes in Computer Science, Vol. 1978, pp. 213–230, Springer-Verlag, 2000.
13. 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.

14. J. Kelsey, B. Schneier and D. Wagner, "Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA", Proceedings of Information and Communications Security (ICICS '97), Lecture Notes in Computer Science, Vol. 1334, pp. 233–246, Springer-Verlag, 1997.
15. 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.
16. 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.
17. J. Kim, S. Hong and B. Preneel, "Related-Key Rectangle Attacks on Reduced AES-192 and AES-256", Proceedings of Fast Software Encryption (FSE '07), Lecture Notes in Computer Science, Vol. 4593, pp. 225-241, Springer-Verlag, 2007.
18. S. Lucks, "Ciphers Secure against Related-Key Attacks", Proceedings of Fast Software Encryption (FSE '04), Lecture Notes in Computer Science, Vol. 3017, pp. 359-370, Springer-Verlag, 2004.
19. NIST, "Announcing Proposed Withdrawal of Federal Information Processing Standard (FIPS) for Data Encryption Standard (DES) and Request for Comments", 26 July 2004. [Online] Available at: `http://csrc.nist.gov/Federal-register/July26-2004-FR-DES-Notice.pdf`
20. R.C.-W. Phan, "Related-Key Attacks on Triple-DES and DESX Variants", Topics in Cryptology - CT-RSA '04, Lecture Notes in Computer Science, Vol. 2964, pp. 15-24, Springer-Verlag, 2004.
21. R.C.-W. Phan and H. Handschuh, "On Related-Key and Collision Attacks: The Case for the IBM 4758 Cryptoprocessor", Proceedings of Information Security Conference (ISC '04), Lecture Notes in Computer Science, Vol. 3225, pp. 111–122, Springer-Verlag, 2004.
22. R.C.-W. Phan and A. Shamir, "Improved Related-Key Attacks on DESX and DESX+", Presented at the rump session of Asiacrypt '04, Jeju Island, Korea, 7 December 2004. Slides available online at `http://www.iris.re.kr/ac04/presentation.htm`
23. E. Razali and R.C.-W. Phan, "On the Existence of Related-Key Oracles in Cryptosystems based on Block Ciphers", Proceedings of Information Security (IS '06), OTM 2006 Confederated Conferences, Lecture Notes in Computer Science, Vol. 4277, pp. 425–438, Springer-Verlag, 2006.
24. E. Razali, R.C.-W. Phan and M. Joye, "On the Notions of PRP-RKA, KR and KR-RKA for Block Ciphers", Proceedings of Provable Security (ProvSec '07), Lecture Notes in Computer Science, Vol. 4784, pp. 188–197, Springer-Verlag, 2007.
25. R. Winternitz and M. Hellman, "Chosen-Key Attacks on a Block Cipher", Cryptologia, Vol. 11, No.1, pp. 16–20, 1987.