A Survey on Cryptanalysis with Three Different Ways, DES-X, CAST, Biham - DES Encryption Algorithm Using Related Key

Vinod Singh Kharsan
Asst. Prof, Dept of CSE
CEC, Bilaspur (C.G.)

Vivek Singh Rathore
Asst. Prof., Dept of CSE
CEC, Bilaspur (C.G.)

Bharat Choudhary
Asst. Prof., Dept of CSE
CEC, Bilaspur (C.G.)

Abstract: Cryptanalysis is process to get the original message from the cipher text without any knowledge of key. In general we can say this is an attack. We present new related-key attacks on the block ciphers 3- WAY, Biham-DES, CAST and DES-X encryption algorithm. Differential related-key attacks allow both keys and plaintexts to be chosen with specific differences. In this paper we also suggest that how we can protect from related key attack we give specific design principles to protect against these attacks.

Keywords: 3- way, Biham – DES, CAST and DES-X

1. Introduction

Related-key cryptanalysis assumes that the attacker learns the encryption of certain plaintexts not only under the original (unknown) key *K*, but also under some derived keys $K0 = f(K)$. In a selected-related-key attack, the attacker specifies how the key is to be commute known-related-key attacks are those where the key difference is well known, but can't be chosen by the attacker. User emphasize that the attacker knows or he chooses a relationship between keys, not the actual key values. Related-key cryptanalysis is a practical attack on key-commute protocols that do not guarantee key-integrity an offender may be able to flip bits in the key without knowing the key and key-update protocols that update keys using a known function: e.g., $K, K + 1, K + 2$ [1]

New Differential Related-Key Attacks 3-WAY Cipher

3-WAY is an 11-round cipher on 96-bit blocks. Ignoring trivialities such as the input and output transformations, the 3-WAY round function $F(x)$ has an equivalent representation as:

$$y = N(x); \quad z = L(y);$$
$$F(x) = z \oplus K \oplus Ci \qquad (1)$$

Where *N* is a fixed nonlinear layer built out of 32 parallel 3-bit permutation S boxes, *L* is a fixed linear function, *K* is the 96-bit master key, and *Ci* is a fixed, round-dependent public constant. [1]

3-WAY is vulnerable to a simple related-key differential attack. It is trivial to find a differential characteristic for one S-box with the probability of 1/4, so that we can construct a characteristic $\Delta x \rightarrow \Delta y$ with the probability of 1/4 for the non-linear layer *N* by using only one active S-box. By the linearity we can see that $\Delta y \rightarrow \ \Delta z = L(\Delta y)$ with the probability 1 under the linear layer *L*. If we pick $\Delta K = \Delta x \oplus \Delta z$, then $\Delta x \rightarrow \Delta x$ by *F* with the probability of 1/4, which is a one-round iterative differential characteristic. In that way we can obtain the 9-round characteristic with the probability 2^{18} to cover rounds 1-9, and apply a 2R analysis to the last two rounds. This breaks 3-WAY with one related-key query and about 2^{22} chosen plaintexts.[2]

2. DES-X Cipher

DES-X is a DES variant proposed by Rivest to strengthen DES against exhaustive attacks. The DES-X encryption of *P* with key (K_1, K_2, K_3) is simply

$$C = K_1 \oplus \mathrm{DES}_{K2}(K_3 \oplus P) \qquad (2)$$

Where *K*3 is the pre-whitening key and *K*1 is the post-whitening key. DES-X has many complementation properties. Furthermore, every DES-X key (*K*1,*K*2,*K*3) has another equivalent key (*K*1,*K*2,*K*3). Therefore, DES-X cannot be used in a Davies-Meyer-like hash function construction. This complementation property leads to an attack which requires roughly $2^{56+64-n}$ trial encryptions when 2^n chosen plaintexts are available. Note that Kilian and Rogaway have proven that this attack is theoretically approximately optimal when DES is viewed as a black box, so any better (nonrelated- key) attack would have to take advantage of the internal structure of DES. However, their proof doesn't deal with related-key attacks. We give a related-key differential attack on the DES-X, using the key differences modulo 2^{64} and the plaintext differences modulo 2. The attack is requires 64 chosen key relations to recover the key, with one plaintext encrypted under each new key.[3]

We start with a simple intuition. Suppose we have some unknown number *Z*. We are allowed to add any number we like modulo 2^{64}, and then XOR it with 2 another number of choosing. We are informed whether or not they obtained result of our calculations is equal to *Z*. There for, we select *T* and *U*, and we test whether

$$(Z + T \bmod 2^{64}) \oplus U = Z \quad (3)$$

It is clear that we can learn the value of *Z* with enough queries. This is essentially the position we are in with DES-X. We can add *T* to K_1**,** and XOR *U* into our plaintext block. If the resulting ciphertext block is resulting as the ciphertext those outcomes from encrypting the unaltered plaintext block under the unaltered DES-X key, then we can put restrictions on the list of possible values for *K*1.[4] With enough such restrictions, we retrieve all of *K*1 except for its high-order bit. This then allows attacks against the remainder of DES-X.

The simplest version of this attack uses *T* and *U* values each with same single bit on. For each bit leave out the high-order bit, we try a *T*,*U* pair with the same bit on. If this results in the same ciphertext as resulted when $T = U = 0$, then we learn that bit in K_1 is a zero. If it results in a different ciphertext, then we learn that that bit in K_1 was a one.

Many have suggested in using a DES-X variant which replaces the XOR pre- and post-whitening steps by addition modulo 2^{64}:

$$C = K_1 + \mathrm{DES}_{K2} (K_3 + P) \quad (4)$$

From the discussions done above, it is clear that this would be vulnerable to a related-key attack very similar to the one that works against regular DES-X.

3. CAST Cipher

CAST is a Feistel cipher whose key schedule uses nonlinear S-boxes. The key schedule for 8 rounds CAST with a 64 bit master key is as follows:

$$(k_1,\ k_2 \ldots\ldots\ldots\ k_8) = \text{Master Key}$$

$$(k'_1,k_2',k_3',k_4') = (k_1, k_2, k_3, k_4) \oplus s5\ [k_5] \oplus s6\ [k_7] \quad (5)$$

$$(k'_5,k'_6,k'_7,k'_8) = (k_5, k_6, k_7, k_8) \oplus s5\ [k'_2] \oplus s6\ [k'_4] \quad (6)$$

$$K_1 = (k_1, k_2) \quad K_2 = (k_3, k_4) \qquad K_3 = (k_5, k_6) \qquad K_4 = (k_7, k_8)$$

$$K_5 = (k'_4, k'_3) \quad K_6 = (k'_2 , k'_1) \quad K_7 = (k'_8 , k'_7) \qquad K_8 = (k'_6 , k'_5)$$

$$(Kr,_1, Kr,_2) = Kr \qquad\qquad r = 1\ldots\ldots\ldots\ldots 8$$

$$skr = S5\ [Kr,_1] \oplus S6\ [Kr,_2] \qquad\qquad r = 1\ldots\ldots\ldots\ldots 8$$

Where the *S*5 and *S*6 are different 8-bit to 32-bit S-boxes. The *r*-th round sub key,*skr*, is XORed into the input of F function as it is conventional for Feistel ciphers.[5] The variance of CAST analyzed here is in an older version of CAST, and not the CAST-128 that is used by confides products and described in Internet RFC 2144

CAST is an interesting example of a cipher designed to resist Biham's rotational related-key cryptanalysis, but not the differential key-related to cryptanalysis. We apply a key-difference to the master key which changes only the byte *k*1; this will lead to a difference only in round subkeys *sk*1 and *sk*6. When *Δk*1 is known, there are only 256 possible differences for *Δsk*1; by encrypting 2^{16} chosen plaintexts are under individualeach key, we can make sure that the 1st round is bypassed for some of the pairs. Cover rounds 2-5 with the trivial differential characteristic of probability 1, and use a 2R attack. Note that *sk*7 and *sk*8 have only 32 bits of entropy in total, so we can try all 2^{32} possibilities for them, decrypt the last two rounds, and recognize correct guesses by 32 zero bits in the block difference. We recover the rest of the key with 2^{16} offline guesses by auxiliary techniques.[5] In the end, we can recover the entire CAST master key with a total of about 2^{17} chosen plaintexts, one related-key query, and 2^{48} offline computations.

4. Biham-DES Cipher

Biham and Biryukov have suggested strengthening DES against exhaustive attacks by using extra key bits to modify the F-function slightly. One of their modifications uses 5 key bits to select from 32 possible reordering of the 8 DES S-boxes.[6] We regard related keys which differ only in those 5 bits, and we apply related-key differential cryptanalysis. Specifically, suppose one key uses ordering 15642738 and another uses ordering 75642138 (both are from the 32 suggested reordering. The only difference between the two F-functions is that S-boxes 1 and 7 have been locomote. Observe that:

$$\Pr_x (S1[x] \oplus S7 [x \oplus 2] = 0) = 14/64 \ (7)$$

The input differential 2 appears only in the middle input bits of the S-box, and will not spread to neighboring S-boxes. Hence, we can construct a one-round characteristic with probability (14 /64)2.[7]

This leads to a 13-round iterative characteristic with probability (14/64)12 = 2-26. The differential techniques of Biham and Shamir will break Biham- DES with 227 chosen plaintexts when this special related-key pair is available. If two related keys allow the above attack (i.e. differ only in the key orderings as defined above), we call them partners. There is a 1 /16 chances that a randomly chosen key will have a partner; if it does, this can be detected with one related key probe. Furthermore, we can always obtain one useful pair of related-key partners from any starting key after 32 related-key queries.[8] Therefore, when using Biham-DES with the 32 recommended DES S-box reorderings, we have a 1/16 probability of success when 227 chosen plaintexts and one related-key query are available; success is nearly guaranteed with 231 chosen plaintexts and 32 related-key queries.

Biham and Biryukov also mention the possibility of using 215 reorderings of the s3-DES S-boxes. They don't present the recommended reorderings, so it is impossible to present any specific results. Still, in general, increasing the 4 number of reordering gives the cryptanalyst more degrees of freedom to find more effective attacks. So, using this variant is not expected to increase security against our attacks.

5. Protection against the known related-key attacks

Avoid the “sub key rotation" attacks, round sub keys should be generated differently, so that each key bit affects nearly every round, but not always in the same way. Key schedule should be designed to protest derivative related-key attacks.[9] And, when related-key queries are cheap, the master key should be long enough to avoid generic black box attacks, as the key length is effectively halved under these attacks.

Avoid dead spots; ensure that every key bit is about equally powerful in terms of its effect on the round keys. Beware of equivalent representations, for they can expose new avenues of attack to an adversary. Our analysis of 3-WAY bears witness to this recommendation.[10]

Avoid the independent round sub key. It has commonly been assumed that a cipher's key length (and strength) can be increased by allowing round keys to be specified independently, but we have shown that this dramatically lowers the cipher's resistance to related-key attacks. In general, when independent 10 round sub keys are in use, the strength of a cipher against related-key attacks will be approximately proportional to the strength of one round standing on its own.

Avoid multiple encryptions with independent keys. And finally, protocol designers should be aware of related-key attacks. Key exchange protocols should exchange a short master key rather than exchanging expanded keys.[11] Design tamper-resistant devices so that it is not possible to change the sub keys without such changes being detected.

6. Conclusion

Thus, using cryptanalysis we can get the original message from the cipher text without any knowledge of key, so we can say this is a attack.. Related-key cryptanalysis is a practical attack on key-exchange protocols that do not guarantee key-integrity an attacker may be able to flip bits in the key without knowing the key and key-update protocols that update keys using a known function: e.g., K, $K + 1$, $K + 2$, etc. We present new related-key attacks on the block ciphers 3-WAY, Biham-DES, CAST & DES-X encryption algorithm.

Differential related-key attacks allow both keys and plaintexts to be chosen with specific differences. The protection from related key attack has also been suggested. Specific design principles for protecting against these attacks have been presented.

References

[1]. C. Adams, “Simple and Effective Key Scheduling for Symmetric Ciphers". SAC '94, 1994 “Workshop on Selected Areas in Cryptography” (Page 129-133)

[2]. C. Adams, “Constructing Symmetric Ciphers Using the CAST Design” Ben-Aroya and E. Biham“Differential Cryptanalysis of Lucifer” Springer-Verlag, 1994”Advances in Cryptology “(Page 187-199)

[3]. E. Biham “New Types of Cryptanalytic Attacks Using Related Keys" Springer-Verlag, 1994”Advances in Cryptology” (Page 398-409)

[4]. Alex Biryukov and David Wagner. Fast Software Encryption: 6th International Workshop, FSE’99 Rome, Italy, March 24–26, 1999 Proceedings, chapter Slide Attacks, pages 245–259. Springer Berlin Heidelberg, Berlin, Heidelberg, 1999.

[5]. Daniel J Bernstein. ChaCha, a variant of Salsa20. In Workshop Record of SASC, volume 8, 2008.

[6]. Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and Raphael C.-W. Phan. SHA-3 Proposal BLAKE. https://131002.net/blake/blake.pdf, 2010.

[7]. S. Moriai, T. Shimoyama, and T. Kaneko, “Higher Order Differential Attack of a CAST Cipher”, Proceedings of the Fifth International Workshop on Fast Software Encryption, Paris, France, March 1998, LNCS 1372, Springer, pp.17- 31.

[8]. B. Schneier and J. Kelsey, “Unbalanced Feistel Networks and Block Cipher Design”, in Proceedings of the Third International Workshop on Fast Software Encryption, Cambridge, UK, February 1996, Springer, LNCS 1039, pp.121-144.

[9]. Joan Daemen, Michaël Peeters, Gilles Van Assche, and Vincent Rijmen. Nessie proposal: NOEKEON. In First Open NESSIE Workshop, pages 213–230, 2000.

[10]. Ferguson Niels, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. The Skein hash function family. Submission to NIST, (round 3), 2010.

[11]. BIHAM, E., KNUDSEN, L., "Cryptanalysis of the ANSI X9.52 CBCM Mode, Journal of Cryptology, to appear, 2001.

[12]. Yosuke Todo. Advances in Cryptology – EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I, chapter Structural Evaluation by Generalized Integral Property, pages 287–314. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[13]. Deukjo Hong, Jung-Keun Lee, Dong-Chan Kim, Daesung Kwon, Kwon Ho Ryu, and Dong-Geon Lee. LEA: A 128-bit block cipher for fast encryption on common processors. In Information Security Applications, pages 3–27. Springer, 2013.

[14]. S. Moriai, T. Shimoyama, and T. Kaneko, “Higher Order Differential Attack of a CAST Cipher”, Proceedings of the Fifth International Workshop on Fast Software Encryption, Paris, France, March 1998, LNCS 1372, Springer, pp.17- 31.