Randomizing encryption mode

Yi-Shiung Yeh [1,*]

I-Te Chen [1,†]

Chan-Chi Wang [2,‡]

[1] *Department of Computer Science and Information Engineering*
National Chiao-Tung University
1001 Ta Hsueh Road
Hsinchu 30050
Taiwan
R.O.C.

[2] *Department of Computer Science and Information Engineering*
Ching-Yun University
Jung-Li, Taiwan
R.O.C.

Abstract

We investigate the mode of block cipher encryption which a random number is added into the process of an encryption. Many manners to add a random number are examined for the capabilities to defeat brute-force, differential and linear attacks. Then, we claim that if the underlying block cipher withstand brute-force attack, some manners will be secure even though the underlying block cipher is vulnerable to differential and linear attacks.

Keywords : *Block cipher, random number, ECB, RECB, PRECB.*

1. Introduction

There are four common encryption modes (ECB, CBC, CFB and OFB) [6] for block ciphers. Each encryption modes have different features for

[*] *E-mail*: ysyeh@csie.nctu.edu.tw

[†] *E-mail*: itchen@csie.nctu.edu.tw

[‡] *E-mail*: wcc@mail.cyu.edu.tw

Journal of Discrete Mathematical Sciences & Cryptography
Vol. ( ), No. , pp. 1–10

security [4]. However, they do not withstand the known/chosen-text attacks such as differential attack [5] and linear attack [7] by disclosing large amount of plaintext-ciphertext pairs of the underlying block cipher for the same key. To dispel the weakness, several new non-standard modes were suggested. The Efficient Error-Propagating Block Chaining (EPBC) mode [1] using both plaintext and ciphertext feedback claims that it is not vulnerable to any known-plaintext attacks. The All-or-nothing mode [8] has the property that one must decrypt the entire ciphertext before one can determine even one message block provides protection against chosen-plaintext attacks.

In this paper, we propose the methods of adding a random number [3] into the process of an encryption. There are many possible manners. The possible capability of defeating brute-force, differential and linear attacks for each manner are examined. Simplicity, the explorations base on ECB mode encryption can be applied to other encryption modes.

2. Randomizing encryption mode

The randomizing encryption mode processes by first selecting a random number, encrypted it to be the first ciphertext block, then using the random number to confuse the succeeding encryptions. Let a plain message be $P_1\|\ldots\|P_n$. The notation $\|$ denotes concatenation. Given a block cipher E and a secret key K, the corresponding ECB mode ciphertext is $C_1\|\ldots\|C_n$ where $C_i = E_K(P_i)$. The corresponding randomizing ECB mode ciphertext will be $C_0\|C_1\|\ldots\|C_n$ where $C_0 = E_K(r)$, r is a random number and $C_i = r_i \oplus EK_i(I_i)$ for $i = 1,\ldots,n$ so that r_i is either 0 or r, K_i is either K or $K \oplus r$ and I_i is either P_i or $P_i \oplus r$. The model of the randomizing ECB mode, abbreviated as RECB, is shown in Figure 1. There is a criterion that $|r|$ should be not less than $\text{Max}\{|K|, |P_i|, |C_i|\}$ where $|x|$ means the bit length of x. If necessary, r can be encrypted into multiple ciphertext blocks. Obviously, there is seven distinct manners of RECB mode encryption. Their security against brute-force, differential and linear attacks are discussed in the next section.

3. Security analysis for RECB

Let the underlying block cipher be E and the corresponding decrypting algorithm be D. K is the secret key in length of k bits. For a

plain message $P_1\|\ldots\|P_n$, the corresponding RECB mode ciphertext is $C_0\|C_1\|\ldots\|C_n$ where $C_0 = E_K(r)$, r is a random number, $O_i = EK_i(I_i)$ and $C_i = r_i \oplus O_i$ for $i = 1,\ldots,n$ as shown in Figure 1. According to the different assignments of K_i, I_i and C_i, using the notations in Figure 1, the seven possible cases are listed and analyzed as follows: [9] [10] (There are four assumptions: All elements in the plaintext space are used randomly and uniformly; The adversary knows E, D, P_i, C_0 and C_i where $i = 1,\ldots,n$; The operation of the differential and linear attacks is XOR, notated as $\oplus$; Both the differential and linear attacks need more than 2^b known plaintext-ciphertext pairs to break the pure underlying block cipher.)

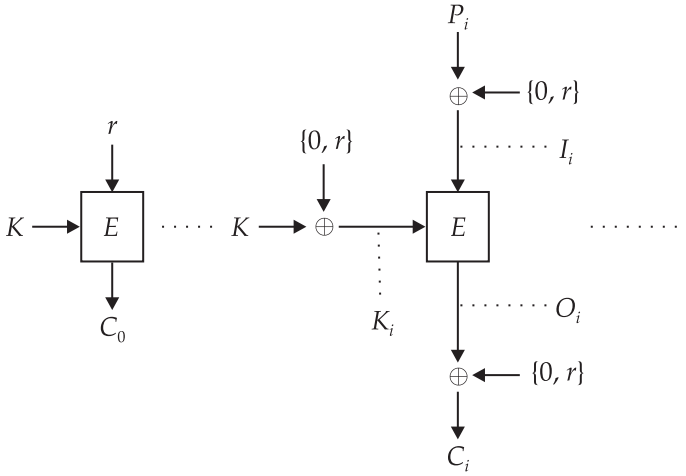

Figure 1
General Model of Randomizing ECB Mode Encryption

Case 1. $K_i = K \oplus r$, $I_i = P_i$ and $C_i = O_i$.

Brute-force attack: needs 2^{k+1} encryptions to derive out K.

Exhaustively search all possible key K'. Compute $r' = D_{K'}(C_0)$ and then check that if $E_{K'\oplus r'}(P_1) = C_1$ then it is very possible that $K = K'$. The needed computation is about 2^{k+1} encryptions.

Differential attack: needs 1 differential breaking and 2^k encryptions to derive out K.

For $K_i = K_1$, the adversary can collect necessary plaintext-ciphertext

pairs for K_1 by possibly one query. K_1 can be derived out by one differential breaking to the underlying block cipher. Then, the adversary exhaustively searches all possible key K'. Check that if $D_{K'}(C_0) \oplus K' = K_1$ then it is very possible that $K = K'$. The total necessary computation is about 1 differential breaking to the underlying block cipher and 2^k encryptions.

Linear attack: needs 1 linear breaking and 2^k encryptions to derive out K.

By applying the similar manner as the above differential attack, one linear breaking can derive K_1 out to the underlying block cipher. Then, the secret K can be exhaustively searched out. The total necessary computation is about 1 linear breaking to the underlying block cipher and 2^k encryptions.

Case 2. $K_i = K$, $I_i = P_i \oplus r$ and $C_i = O_i$.

Brute-force attack: needs 2^{k+1} encryptions to derive out K.

Exhaustively search all possible key K'. Compute $r' = D_{K'}(C_0)$ and then check that if $E_{K'}(P_1 \oplus r') = C_1$ then it is very possible that $K = K'$. The needed computation is about 2^{k+1} encryptions.

Differential attack: needs 1 differential breaking to derive out K.

For $K_i = K$ and $I_i \oplus I_j = P_i \oplus P_j$, the adversary can collect necessary specific difference plaintext pairs (he/she knows only the difference) and the corresponding ciphertexts for K by possibly one query. Thus, K can be derived out by one differential breaking to the underlying block cipher.

Linear attack: needs 1 linear breaking and 2^k encryptions to derive out K.

Let $I_i[s] \oplus K_i[t] \oplus O_i[u] = 0$ be a linear approximation of the underlying block cipher where $X[s]$ denotes the s^{th} bit in left of X. In the case, $I_i[s] \oplus K_i[t] \oplus O_i[u] = P_i[s] \oplus r[s] \oplus K[t] \oplus C_i[u]$. The value of $K[t] \oplus r[s]$ can be determined by a linear attack. If the adversary can collect enough values of $K[t] \oplus r[s]$ for some t and s, he/she can exhaustively search all possible key K' and check that whether $D_{K'}(C_0)[s] \oplus K'[t]$ corresponds with all of the collect conditions to determine the exact value of K. In the extreme case, let $t = s$ in all linear approximations, the total necessary computation is the same as that of case 1: about 1 linear breaking to the underlying block cipher and 2^k encryptions.

Case 3. $K_i = K$, $I_i = P_i$ and $C_i = O_i \oplus r$.

Brute-force attack: needs 2^{k+1} encryptions to derive out K.

Exhaustively search all possible key K'. Compute $r' = D_{K'}(C_0)$ and then check that if $E_{K'}(P_1) = C_1 \oplus r'$ then it is very possible that $K = K'$. The needed computation is about 2^{k+1} encryptions.

Differential attack: needs 1 differential breaking to derive out K.

For $K_i = K$ and $O_i \oplus O_j = C_i \oplus C_j$, the adversary can collect necessary specific difference ciphertext pairs (he/she knows only the difference) and the corresponding plaintexts for K by possibly one query. Thus, K can be derived out by one differential breaking to the underlying block cipher.

Linear attack: needs 1 linear breaking and 2^k encryptions to derive out K.

The attack manner is similar to case 2.

Case 4. $K_i = K \oplus r$, $I_i = P_i \oplus r$ and $C_i = O_i$.

Brute-force attack: needs 2^{k+1} encryptions to derive out K.

Exhaustively search all possible key K'. Compute $r' = D_{K'}(C_0)$ and then check that if $E_{K' \oplus r'}(P_1 \oplus r') = C_1$ then it is very possible that $K = K'$. The needed computation is about 2^{k+1} encryptions.

Differential attack: needs $2^b + 1$ differential breakings or 1 differential breaking and 2^k encryptions to derive out K.

For $K_i = K \oplus r$ and $I_i \oplus I_i \oplus I_j = P_i \oplus P_j$, the adversary can collect necessary specific difference plaintext pairs (he/she knows only the difference) and the corresponding ciphertexts for K_1 by possibly one query. Then, like the situation in case 1, K can be derived from C_0 and K_1. The total necessary computation is about 1 differential breaking to the underlying block cipher and 2^k encryptions. Alternatively, while K_1 has gotten, r can be derived out by formula $r = D_{K1}(C_1) \oplus P_1$. By this way, collecting enough distinct (r, C_0) pairs, a differential attack can be applied again to break the secret key K. We have assumed that an successful differential attack needs at least 2^b known plaintext-ciphertext pairs. Thus, the total computation is at least $2^b + 1$ differential breakings.

Linear attack: needs 1 linear breaking to derive out K.

Let $I_i[s] \oplus K_i[t] \oplus O_i[u] = 0$ be a linear approximation of the underlying block cipher where $X[s]$ denotes the s^{th} bit in left of X. In the case, $I_i[s] \oplus K_i[t] \oplus O_i[u] = P_i[s] \oplus r[s] \oplus K[t] \oplus r[t] \oplus C_i[u]$. The value of $K[t] \oplus r[s] \oplus r[t]$ can be determined by a linear attack. The attack is similar to the case 2. However, in the extreme case, let $t = s$ in all linear approximations, the value of K can be directly derived out, the total necessary computation reduces to one linear breaking to the underlying block cipher.

Case 5. $K_i = K \oplus r$, $I_i = P_i$ and $C_i = O_i \oplus r$.

Brute-force attack: needs 2^{k+1} encryptions to derive out K.

Exhaustively search all possible key K'. Compute $r' = D_{K'}(C_0)$ and then check that if $E_{K' \oplus r'}(P_1) = C_1 \oplus r'$ then it is very possible that $K = K'$. The needed computation is about 2^{k+1} encryptions.

Differential attack: needs $2^b + 1$ differential breakings or 1 differential breaking and 2^k encryptions to derive out K.

For $K_i = K \oplus r$ and $O_i \oplus O_j = C_i \oplus C_j$, the adversary can collect necessary specific difference ciphertext pairs (he/she knows only the difference) and the corresponding plaintexts for K_1 by possibly one query. Then, like the situation in the case 4, the total necessary computation to derive out K is at least $2^b + 1$ differential breakings or 1 differential breaking and 2^k encryptions.

Linear attack: needs 1 linear breaking to derive out K.

The, attack manner is similar to the case 4.

Case 6. $K_i = K$, $I_i = P_i \oplus r$ and $C_i = O_i \oplus r$.

Brute-force attack: needs 2^{k+1} encryptions to derive out K.

Exhaustively search all possible key K'. Compute $r' = D_{K'}(C_0)$ and then check that if $E_{K'}(P_1 \oplus r') = C_1 \oplus r'$ then it is very possible that $K = K'$. The needed computation is about 2^{k+1} encryptions.

Differential attack: is infeasible to the case.

Although $I_i \oplus I_j = P_i \oplus P_j$ and $O_i \oplus O_j = C_i \oplus C_j$. However the

adversary knows neither the exact value of plaintexts nor ciphertexts. Thus, a differential attack is difficult to work on this case [20].

Linear attack: needs 1 linear breaking to derive out K.

The attack manner is similar to the case 4.

Case 7. $K_i = K \oplus r$, $I_i = P_i \oplus r$ and $C_i = O_i \oplus r$.

Brute-force attack: needs 2^{k+1} encryptions to derive out K.

Exhaustively search all possible key K'. Compute $r' = D_{K'}(C_0)$ and then check that if $E_{K' \oplus r'}(P_1 \oplus r') = C_1 \oplus r'$ then it is very possible that $K = K'$. The needed computation is about 2^{k+1} encryptions.

Differential attack: is infeasible to the case. For the same reason of the case 6, a differential attack is difficult to work on this case.

Linear attack: needs 1 linear breaking to derive out K.

Let $I_i[s] \oplus K_i[t] \oplus O_i[u] \oplus O_i[v] = 0$ be a linear approximation of the underlying block cipher where $X[s]$ denotes the s^{th} bit in left of X. In the case, $I_i[s] \oplus K_i[t] \oplus O_i[u] \oplus O_i[v] = P_i[s] \oplus r[s] \oplus K[t] \oplus r[t] \oplus C_i[u] \oplus r[u] \oplus C_i[v] \oplus r[v]$. The value of $K[t] \oplus r[s] \oplus r[t] \oplus r[u] \oplus r[v]$ can be determined by a linear attack. In the extreme case, let $s = u$ and $t = v$ in all linear approximations, the cryptanalysis complexity reduces to the same as case 4. That is, the total necessary computation is about 1 linear breaking to the underlying block cipher.

4. Applying pseudo random numbers

The random number used in the above randomizing encryption mode can be replaced by a sequence of pseudo random number [2] [3] which is generated by the random number r (as the notation in the above section) through a pseudo random number generator R [11]. The generated pseudo random numbers are applied in order to a position wherein a random number is needed. Let $R(r)$ generate a sequence of $r_1, r_2, \ldots$. The new RECB, notated as PRECB, mode encryption is shown in Figure 2. The used pseudo random numbers are assumed to have length not less than the secret key K, and deriving out r_i from r_{i+1} is computationally infeasible.

The situations of brute-force, differential and linear cryptanalysis to attack the seven cases, as in the above section, of PRECB mode encryption are discussed as follows: (The attacker knows details of the pseudo random number generator.)

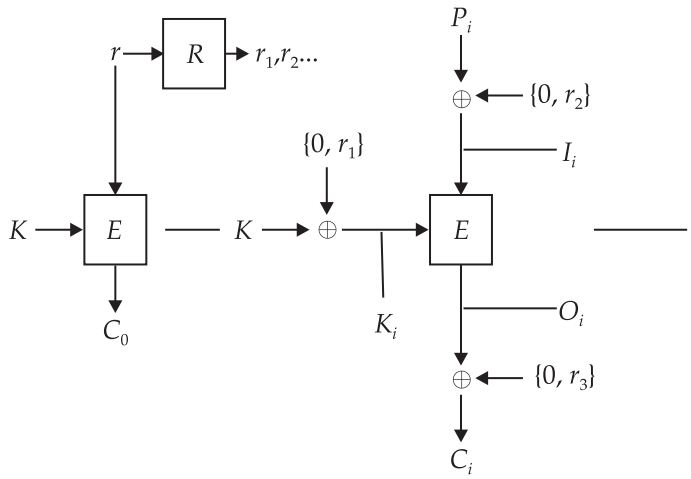

Figure 2
PRECB mode encryption

Brute-force cryptanalysis

The attacks of brute-force cryptanalysis to the seven cases of PRECB mode encryption have almost the same complexity with the attacks to RECB. Illustrating by the case 1, the scenario now is changed to as below. Exhaustively search all possible key K'. Compute $r' = D_{K'}(C_0)$ and $r'_1 = R(r')$ then check that if $E_{K' \oplus r'_1}(P_1) = C_1$ then it is very possible that $K = K'$. The needed computation just increases about 2^k random number computation to the case in RECB, that is 2^{k+1} encryptions and 2^k random number computation. Other cases have the similar situations.

Differential cryptanalysis

In PRECB, a random number is ideally not reused. Thus, for a differential attack, the necessary information is difficult to be collected from an encrypted message, that is, from just one query. However, by the manner of chosen-ciphertext, the pseudo random numbers can

be reconstructed by given a constant C_0. By this way, the necessary information for a differential cryptanalysis can still be obtained although by masses of queues.

In fact, the attacks of differential cryptanalysis to the case $1, 2, 3, 6$ and 7 of PRECB mode encryption have almost the same complexity to the cases of RECB, increasing about 2^k random number computation as the brute-force attack does. In the case 4 and 5 of PRECB, r is difficult to be gotten even K_1 is leaked. Thus, the second attack alternation in the case 4 and 5 of RECB is not workable here. In the two cases, the breaking time of K is about 1 differential breaking and 2^k encryptions and 2^k random number computation

Linear cryptanalysis

Like the situation of differential cryptanalysis, the adversary now should applied the manner of chosen-ciphertext to collect the necessary information of linear cryptanalysis by given a constant C_0 through masses of queries. The attacks of linear cryptanalysis to the case $1, 2$ and 3 of PRECB mode encryption have almost the same complexity to the cases of RECB, increasing about 2^k random number computations. For the case $4, 5, 6$ and 7 of RECB, a linear attack can extremely derive out K by a single linear breaking. However, in the cases of PRECB, the effects of random numbers are difficult to be eliminated. The necessary computation is changed to about 1 linear breaking and 2^k encryptions and 2^{k+1} random number computation for each of the four cases.

5. Discussions and conclusions

From the above analyses, we know that neither RECB nor PRECB are secure if the underlying block cipher is vulnerable to brute-force cryptanalysis. On the other hand, if the underlying block cipher can defeat brute-force attack, that is, 2^k encryptions of the underlying block cipher are computationally infeasible. Even though the underlying block cipher is vulnerable to differential and linear attacks. With the assumptions and criterion listed in the paper, the case 1 of RECB is secure for protecting the secret key K. The case 1, 4, 5, 6 and 7 of PRECB are also secure. It should be noted that the security mentioned above is limited to brute-force, linear and differential attacks, not including other attacks.

Acknowledgements. This work was supported in part by the Bestwise International Co.

References

[1] A. Zuquete and P. Guedes, Efficient error-propagating block chaining, *Cryptography and Coding – 6^{th} IMA International Conference Proceedings*, Springer-Verlag, 1997, pp. 323–324.

[2] A. Rukhin et al., A statistical test suite for the validation of random and pseudo *Random Number Generators for Cryptographic Applications*, NIST Special Publication (under preparation), Spring 2000.

[3] V. Becher, S. Daicz and G. Chaitin, A highly random number, Combinatorics, Computability and Logic, in *Proceedings of DMTCS'01*, C. S. Calude, M. I. Dinneen and S. Sburlan (eds.), Springer-Verlag, London, 2001, pp. 55–68.

[4] W. Stalling, *Cryptography and Network Security: Principle and Practice*, 3rd edn., Prentice Hall, 2003.

[5] E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag New York, Inc., 1993.

[6] Federal Information Processing Standard Publication 81, *DES Modes of Operation*, December 1980.

[7] M. Matsui, Linear cryptanalyis method for DES cipher, *Advances in Cryptology-EUROCRYPT'93 Proceedings*, Springer-Verlag, 1994, pp. 74–87.

[8] R. L. Rivest, All-or-nothing encryption and the package transform, *Fast Software Encryption – 4^{th} International Workshop FSE'97 Proceedings*, Springer-Verlag, 1997, pp. 210-218.

[9] T. Iwata and K. Kurosawa, Probabilistic higher order differential attack and higher order bent functions, *Advances in cryptology – ASIACRYPT'99 Proceedings*, Springer-Verlag, 1999, pp. 62–74.

[10] T. Jakobsen, Cryptanalysis of block ciphers with probabilistic non-linear relations of low degree, in *Advances in cryptology Advances in Cryptology-CRYPT'98 Proceedings*, Vol. 1462 of *Lecture Notes in Computer Science*, Springer-Verlag, 1998, pp. 212–222.

[11] T. S. Han and O. Uchida, Source code with cost as a non-uniform random number generator, *IEEE Transactions on Information Theory*, March 2000, pp. 712–717.

Received July, 2004