Related-Mode Attacks on CTR Encryption Mode

Dayin Wang, Dongdai Lin, and Wenling Wu
(Corresponding author: Dayin Wang)

Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences
Beijing 100080, China. (Email: {wdy, ddlin, wwl}@is.iscas.ac.cn)

(Received Dec. 9, 2005; revised and accepted Jan. 3, 2006)

Abstract

In this paper, we discuss using CTR mode, another standard encryption mode, to attack other standard encryption modes and using other standard encryption modes to attack CTR mode under the related-mode attack model. In particular, we point out that when the adversary has access to an oracle under one proper mode, then almost all other related-cipher modes, whether they are encryption modes or authentication modes or authenticated encryption modes, can be attacked with ease under the related-mode attack model.

Keywords: Block cipher, modes of operation, related-cipher attack, related-mode attack

1 Introduction

Block ciphers are often proposed with several variants, in terms of a different secret key size and corresponding number of rounds. Wu [9] presented the related-cipher attack model applicable to related ciphers in the sense that they are exactly identical to each other, differing only in the key size and most often also in the total number of rounds. In [7], the authors generalize the concept of the related-cipher attack model to apply to a larger class of related model, in particular cipher encryptions with different block cipher modes of operation, but with the underlying block cipher being identical. They called it related mode attack and further show that when the adversary has access to an oracle for any one mode of operation of ECB, CBC, OFB, CFB, then almost all other related cipher modes can be easily attacked. But they didn't study another standard encryption mode CTR. In this paper, we will discuss how to use CTR mode to attack other modes and how to use other modes to attack CTR mode under the *related-mode attack* model.

In Section 2, we briefly describe the standard block cipher modes of operation. In Section 3 and 4, we discuss how to use CTR mode to attack other modes and how to use other modes to attack CTR mode under the *related-mode attack* model. We conclude in Section 5.

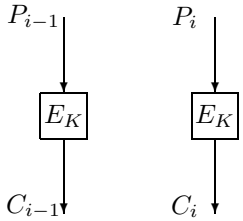

Figure 1: ECB mode encryption

2 Standard Block Cipher Encryption Modes

When encrypting a plaintext P, which is longer than the block size, n of the underlying block cipher, this plaintext is divided into m number of n-bit blocks P_i, and each one is encrypted at a time using a block cipher mode of operation that includes the Electronic Code Book (ECB), the Cipher Block Chaining (CBC), the Cipher FeedBack (CFB), the Output FeedBack (OFB) [4, 5] and Counter Mode (CTR) [1].

The ECB mode is the simplest, where each plaintext block P_i is independently encrypted to a corresponding ciphertext block C_i via the underlying block cipher E_K keyed by secret key K:

$$C_i = E_K(P_i).$$

Figure 1 illustrates the ECB mode encryption on two consecutive plaintext blocks P_{i-1} and P_i.

Meanwhile, the CBC mode uses the previous ciphertext block C_{i-1} as the feedback component that is exclusive-ORed (XORed) to the current plaintext block P_i, before the resulting XOR is encrypted to obtain the current ciphertext block C_i. In particular:

$$C_i = E_K(P_i \oplus C_{i-1})$$

where C_0 = initialization vector (IV). Figure 2 illustrates the CBC mode encryption on two consecutive plaintext blocks P_{i-1} and P_i.

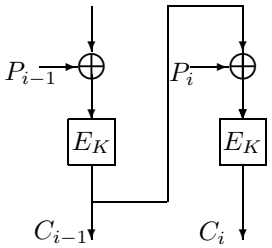

Figure 2: CBC mode encryption

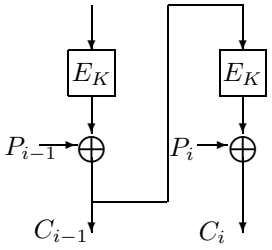

Figure 3: CFB mode encryption

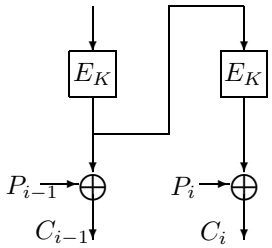

Figure 4: OFB mode encryption

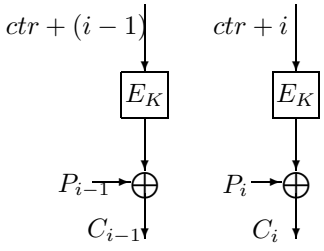

Figure 5: CTR mode encryption

The CFB mode also uses the previous ciphertext block C_{i-1} as feedback, which is first encrypted and then XORed to the current plaintext block P_i to obtain the current ciphertext block C_i:

$$C_i = P_i \oplus E_K(C_{i-1})$$

where C_0 = initialisation vector (IV). The CFB mode can also be viewed as a stream cipher mode by treating $X_i = E_K(C_{i-1})$ as a keystream that is XORed to the plaintext P_i to obtain the ciphertext C_i. Figure 3 shows the CFB mode.

The OFB mode is similar to the CFB in that a keystream is also generated to be XORed to the current plaintext block P_i to obtain the current ciphertext block C_i. The difference is that the keystream is not a function of the previous ciphertext block C_{i-1}, but is the previously encrypted feedback component X_i:

$$\begin{aligned} X_i &= E_K(X_{i-1}) \\ C_i &= P_i \oplus E_K(X_i) \end{aligned}$$

where X_0= initialisation vector (IV). Note that the keystream is independent of previous plaintext and ciphertext blocks. Figure 4 illustrates the OFB mode.

The CTR mode is similar to the CFB in that a keystream is also generated to be XORed to the current plaintext block P_i to obtain the current ciphertext block C_i. The difference is that the keystream is a function of a counter, *ctr*, which can also be looked on as an initialisation vector. Figure 5 illustrates the CTR mode.

$$C_i = P_i \oplus E_K(ctr + i).$$

There are two variants of the mode, one random and the other stateful. No matter which variant is used, the initialisation vector, *ctr*, is included in the ciphertext as the first block C_0 in order to enable decryption. The counter is not allowed to wrap around. Thus the decryption algorithm first chops off the first n bits C_0 and uses it as *ctr*, and then divides the rest of the string into n-bit blocks and decrypt ciphertext using the same method of encryption.

3 Using other Standard Modes to Attack CTR

Throughout this paper, we consider the case where the adversary has access to an oracle that is able to perform either encryption or decryption for some fixed mode. This is similar to having access to known or chosen plaintext/ ciphertext queries under that mode. We show that this oracle allows the adversary to attack other related-cipher modes, where the underlying block cipher is the same. P_i' and C_i' respectively denote the current plaintext and ciphertext block used in the interaction with the oracle being exploited, while P_i and C_i respectively denote the current plaintext and ciphertext blocks of the related-cipher mode being attacked.

For the mode being attacked, only the corresponding ciphertext blocks, C_i $(i = 0, 1, \cdots, m)$ are known, where $C_0 = IV$ is the initialization vector. It is the adversary's objective to directly recover these unknown plaintext blocks, P_i $(i = 0, 1, \cdots, m)$, i.e. we assume a ciphertext-only scenario for the mode being attacked.

For the mode being exploited, access to its oracle

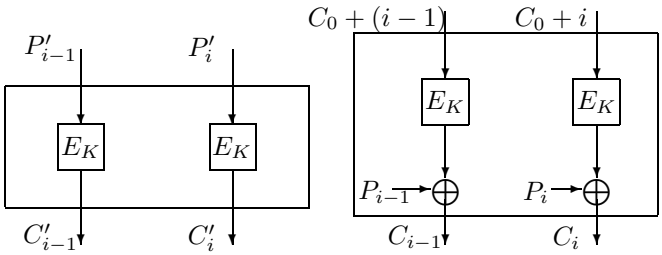

Figure 6: Exploiting ECB to attack CTR

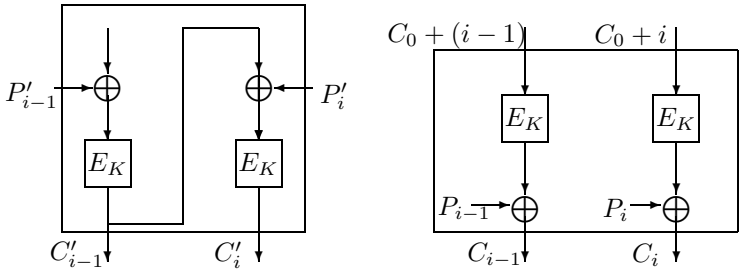

Figure 7: Exploiting CBC to attack CTR

allows the adversary to obtain known or chosen plaintext/ciphertext queries, and as necessary known or chosen IV queries - though we assume for more concrete and interesting results that he can only access either a mode encryption or mode decryption oracle, and not both at the same time. Having said this, note that a standard mode of operation is expected to be secure against attacks where both encryption and decryption oracles are possible [2].

3.1 Exploiting an ECB Oracle

Consider that the adversary has access to either an encryption or decryption oracle under ECB mode. We will show how this oracle can be exploited to obtain the unknown plaintext blocks encrypted under the CTR mode.

In our current case, the adversary has access to the ECB encryption oracle, and is exploiting it to attack another related cipher in the CTR mode. In particular, given that he desires to know the unknown plaintext block P_i corresponding to an intercepted ciphertext block C_i of the CTR mode, he chooses $P'_i = C_0 + i$ to feed to the ECB encryption oracle and hence obtains the corresponding ciphertext C'_i. Since $C_i = E_K(C_0 + i) \oplus P_i$, we can get $P_i = C_i \oplus C'_i$. This is illustrated in Figure 6, where the exploited oracle and the mode being attacked are on the left and right, respectively, and where the rectangular boxes delimit the parts inaccessible to the adversary. In summary, we require just one chosen plaintext(CP) query encrypted under ECB to obtain the plaintext block corresponding to any ciphertext block encrypted under CTR.

3.2 Exploiting a CBC Oracle

When the adversary has access to a CBC oracle, he can similarly use this to attack CTR mode.

Attacking this requires a CBC encryption oracle. First the adversary queries the encryption oracle and get the ciphertext C'_{i-1} of plaintext P'_{i-1}, then he chooses $P'_i = C'_{i-1} \oplus (C_0 + i)$ and queries the oracle to obtain the corresponding ciphertext C'_i. Since $C'_i = E_K(P'_i \oplus C'_{i-1}) = E_K(C_0 + i)$ is directly related to an intermediate state in CTR, namely that $C_i = P_i \oplus C'_i$. Therefore, we can computer $P_i = C'_i \oplus C_i$. This is illustrated in Figure 7. In summary, we require two chosen plaintext(CP) queries encrypted under CBC to obtain the plaintext block corresponding to any ciphertext block encrypted under CTR.

3.3 Exploiting a CFB Oracle

The adversary accesses a CFB decryption oracle and chooses $C'_{i-1} = C_0 + i$, and hence $E_K(C'_{i-1}) = E_K(C_0 + i) = X'_i$ can be directly related to a similar intermediate state within CTR, namely $X'_i = P'_i \oplus C'_i$. He then computes $P_i = X'_i \oplus C_i$. See Figure 8. Repeating this attack will allow him to other plaintext blocks of the CTR. In summary, we require just one chosen ciphertext (CC) query encrypted under CFB to obtain the plaintext block corresponding to any ciphertext block encrypted under CTR.

3.4 Exploiting an OFB Oracle

In this section, We will discuss how to exploit OFB oracle to attack the CTR mode.

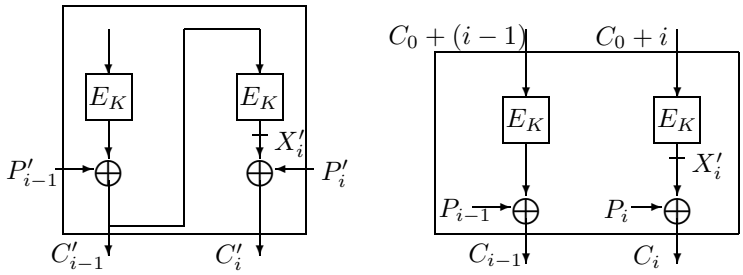

Figure 8: Exploiting CFB to attack CTR

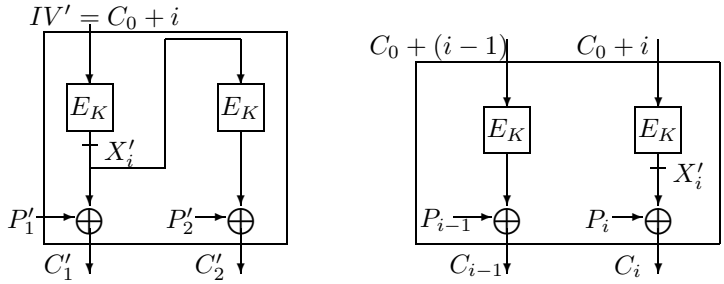

Figure 9: Exploiting OFB to attack CTR

This is so far the hardest attack to mount, and requires a chosen-$IV(CIV)$ scenario [8]. In particular, the adversary chooses $IV' = C_0 + i$, and hence $E_K(IV') = E_K(C_0+i) = X'_i$. This intermediate state relates between the two modes, OFB and CTR, namely $X'_i = P'_1 \oplus C'_1$, and so he can compute $P_i = X'_i \oplus C_i = P'_1 \oplus C'_1 \oplus C_i$. This is shown in Figure 9. Note that in this case the plaintext and ciphertext blocks of the exploited oracle do not need to be chosen but are merely known.

4 Exploiting a CTR Oracle

In this case, the adversary has access to a CTR oracle, and uses this to attack other related-cipher modes.

The CTR, CFB and OFB modes are sometimes called stream-cipher modes since despite starting with an underlying block cipher, E_K, using it in these modes essentially results in a stream cipher. A stream-cipher mode uses the underlying E_K in both its mode encryption and decryption, in contrast to other non-stream-cipher modes such as the ECB and CBC that use E_K for mode encryption and correspondingly E_K^{-1} for mode decryption. Because of this, it appears that stream-cipher mode oracles can only be used to construct encryption oracles for other non-stream-cipher modes. This means that it will not be possible to exploit a stream-cipher mode oracle (such as CTR CFB and OFB) to attack non-stream-cipher modes (such as ECB and CBC). Instead, we consider only how stream-cipher modes can be exploited to attack other stream-cipher modes.

Attacking CFB: The adversary accesses CTR decryption oracle and chooses $C'_0 = C_{i-1} - 1$, since $C'_1 = E_K(C'_0 + 1) \oplus P'_1 = E_K(C_{i-1}) \oplus P'_1$, and hence $E_K(C_{i-1}) = C'_1 \oplus P'_1 = X'_i$ can be directly related to a similar intermediate state within CFB, namely $X'_i = P'_1 \oplus C'_1 = C_i \oplus P_i$. He then computes $P_i = X'_i \oplus C_i$. See Figure 10. Repeating this attack will allow him to obtain other plaintext blocks of the CFB.

Attacking OFB: The adversary accesses a CTR decryption oracle and chooses $C'_0 = IV - 1$, since $C'_1 = E_K(C'_0+1) \oplus P'_1 = E_K(IV) \oplus P'_1$, and hence $E_K(IV) = X'_i$ can be directly related to a similar intermediate state within OFB, namely $X'_i = P'_1 \oplus C'_1 = P_1 \oplus C_1$. He then computes $P_1 = X'_i \oplus C_1$. This is illustrated in Figure 11. Repeating this attack will allow him to iteratively obtain the next plaintext blocks of the OFB.

5 Conclusions

In this paper we discuss how access to chosen plaintexts/ciphertexts in other standard encryption modes allows related-cipher CTR mode to be attacked and how access to chosen ciphertexts in the CTR mode allows almost all other related-cipher standard encryption modes to be attacked. In Table 1, we list our attacks and the corresponding text complexities, while computational complexity is negligible.

The five modes discussed above are all standard encryption modes. There are a lot of standard authentication modes and authenticated encryption modes using

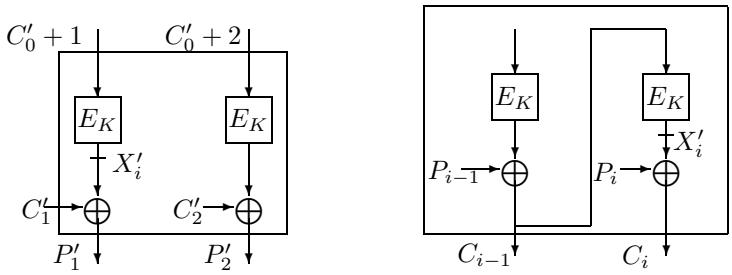

Figure 10: Exploiting CTR to attack CFB

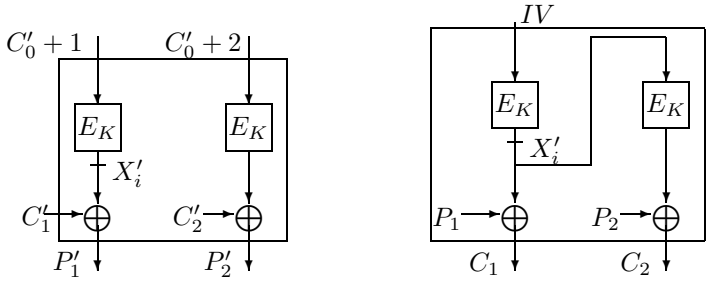

Figure 11: Exploiting CTR to attack OFB

Table 1: Related-mode attacks on standard encryption modes

Oracle Exploited	Cipher Mode Attacked	Text Complexity
ECB	CTR	1 CP
CBC	CTR	2 CP
CFB	CTR	1 CC
OFB	CTR	1 CP, 1 CIV
CTR	CFB	1 CC
	OFB	1 CC

block ciphers, such as authentication mode CMAC [6], authenticated encryption mode GCM [3]. We further study the security of those modes of operation under related-mode attack model and find they all are insecure if the adversary can access to an oracle under one proper mode. So when we have the same cipher being used as the underlying component in different block cipher modes of operation, we should avoid using the same key in those modes in practical applications.

Acknowledge

This research is supported by the National Natural Science Foundation of China under Grant No.60373047 and No.90204016; the National Basic Research 973 Program of China under Grant No.2004CB318004.

References

[1] http://csrc.nist.gov/encryption/modes/proposedmodes/ctr/

[2] A. Joux, "Cryptanalysis of the EMD mode of operation," *Advances in Cryptology-Eurocrypt'03*, LNCS 2656, pp. 1-16, Springer-Verlag, 2003.

[3] D. McGrew and J. Viega, *The Galois/Counter Mode of Operation (GCM)*, Submission to NIST Modes of Operation Process, 2004, Available at http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/

[4] National Institute of Standards and Technology (NIST), *Federal Information Processing Standards Publication 81 (FIPS PUB 81): DES Modes of Operation*, Dec. 1980.

[5] National Institute of Standards and Technology (NIST), *NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, Dec. 2001.

[6] National Institute of Standards and Technology (NIST), *NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005.

[7] R. C. W. Phan and M. U. Siddiqi, "Related-mode attacks on block cipher modes of operation," *ICCSA 2005*, LNCS 3482, pp. 661-671, Springer-Verlag, 2005.

[8] D. Wagner, "Cryptanalysis of some recently-proposed multiple modes of operation," *FSE'98*, LNCS 1372, pp. 254-269, Springer-Verlag, 1998.

[9] H. Wu, "Related-Cipher attacks," *ICICS'02*, LNCS 2513, pp. 447-455, Springer-Verlag, 2002.

Dayin Wang is now a Ph.D candidate at the State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences. His research interests include Message Authentication codes and mode of operation. E-mail address: wdy@is.iscas.ac.cn.

Dongdai Lin is now a full time research professor and deputy director of State Key Labortory of Information Security, Institute of Software of the Chinese Academy of Sciences. He received his B.S. degree in mathematics from Shandong University in 1984, and the M.S. degree and Ph. D degree in coding theory and cryptology at Institute of Systems Science of the Chinese Academy of Sciences in 1987 and 1990 respectively. His current research interests include cryptology, information security, grid computing, mathematics mechanization and symbolic computations.

Wenling Wu is now a professor at the State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences. She received her B.S. degree and M.S. degree inMaths from Northwest University in 1987 and 1990, respectively. She received her Ph.D degree in Cryptography from Xidian University in 1997. From 1998 to 1999 she was a postdoctoral fellow in the Institute of Software, Chinese Academy of Science. Her current research interests include theory of cryptography, mode of operation, block cipher, stream cipher and hash function.