새로운 인증-암호화 모드 NAE에 대한 위조 공격*

정기태**, 이창훈**, 성재철***, 홍석희**, 이상진**

**고려대학교 정보보호기술연구센터, ***서울시립대 수학과

Forgery attack against New Authenticated Encryption

Kitae Jeong**, Changhoon Lee**, Jaechul Sung***,

Seokhie Hong**, Sangjin Lee**

**Center for Information Security Technologies, Korea University
***Department of Mathematics, University of Seoul

요 약

신상욱 등은 JCCI 2003에서 새로운 인증-암호화 모드 NAE를 제안하였다[1]. NAE는 CFB 모드와 CTR 모드를 결합시킨 변형된 형태로, 하나의 기반이 되는 블록 암호 키를 가지고 최소한으로 블록 암호를 호출하여 기밀성과 무결성을 모두 제공한다. 이 모드는 CBC 암호화 모드와 CBC-MAC이 결합된 CCM 인증-암호화 모드보다 효율적이며, 기제안된 다른 인증-암호화 기법들과 유사한 성능을 가진다. 그러나 본 논문에서는 단순 암호문 조작으로 유효한 암호문-태그 쌍을 생성할 수 있음을 보인다.

I. 서론

신상욱 등은 JCCI 2003에서 새로운 인증-암호화 모드 NAE를 제안하였다[1]. 기존에 제안된 대부분의 기법들이 CBC (Cipher Block Chaining) 모드, ECB (Electronic Code Book) 모드의 변형된 형태이지만, 이 모드는 CFB (Cipher FeedBack) 모드와 CTR (Counter) 모드를 결합시킨 변형된 형태로, 하나의 기반이 되는 블록 암호 키를 가지고 최소한으로 블록 암호를 호출하는 인증-암호화 기법이다. NAE는 기제안된 인증-암호화 기법들과 유사한 성능을 가지며, CBC 암호화 모드와 CBC-MAC이 결합된 CCM 인증-암호화 모드보다 효율적이다.

본 논문에서는 [1]에서 제안된 새로운 인증-암호화 모드 NAE에 대하여 단순 암호문 조작으로 유효한 암호문-태그 쌍을 생성할 수 있음을 보인다.

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성지원 사업의 연구결과로 수행되었음

먼저 2절에서는 새로운 인증-암호화 모드 NAE에 대하여 살펴보고, 3절에서는 한 블록 메시지를 갖는 NAE와 여러 개의 블록 메시지를 갖는 NAE에 대해 각각 위조 공격을 수행한다. 그리고 마지막 4절에서는 본 논문의 결과를 요약한다.

II. 새로운 인증-암호화 모드 NAE

2.1 표기

스트링은 0과 1 중의 한 값을 가지는 기호들의 유한 수열이다. $\{0,1\}^*$는 모든 스트링의 집합을 나타내며, $\{0,1\}^n$는 길이 n의 모든 스트링의 집합을 나타낸다. $A \in \{0,1\}^*$이면, $|A|$는 스트링 A의 비트 길이를 나타내고, $\|A\|_n = \max\{1, \lceil |A|/n \rceil\}$은 A의 n-비트 블록 개수를 나타낸다. $A, B \in \{0,1\}^*$이면 $A\|B$는 두 스트링의 연결(concatenation)을 의미한다. 0^i와 1^i는 각각 i개의 0과 1의 스트링을 나타낸다.

$A, B \in \{0,1\}^*$이면, $A \oplus B$는 두 스트링의 비트 단위 XOR이다. 만약 두 스트링의 길이가 다

른 경우에 $A \oplus B$는 A의 처음 l비트와 B의 처음 l비트의 비트 단위 XOR를 나타낸다. 이때 $l = \min\{|A|,|B|\}$이다.

블록 암호는 어떤 정수 n에 대한 함수 E: $K \times \{0,1\}^n \rightarrow \{0,1\}^n$이다. 각 $E(K, \cdot) = E_K(\cdot)$는 $\{0,1\}^n$에서의 순열(permutation)이다. 여기서 K는 가능한 키들의 집합이고 n은 블록 길이이다. 태그 길이는 정수 $\tau \in [0, \cdots, n]$ 이다.

NAE는 n-비트 nonce R을 필요로 한다. 카운터 값 또는 랜덤한 값이 nonce로 사용될 수 있다. 현재의 암호화키가 사용되는 동안 nonce가 반복되지 않는다면, 공격자가 nonce를 제어할 수 있더라도 안전성은 유지되어야 한다. 제안된 기법에서 nonce는 랜덤이거나 예측할 수 없거나 비밀일 필요가 없다. nonce는 암호화와 복호화 모두에 사용된다. 보통 암호문과 함께 전달된다.

2.2 새로운 인증된 암호화 기법

본 절에서는 새로운 인증된 암호화 기법 NAE (New Authenticated Encryption)을 구체적으로 기술한다. [그림 1]은 제안된 기법의 암호화 알고리즘을 보여준다.

(1) 키 생성 및 세션 셋업

블록 암호를 위한 키 집합 K를 랜덤하게 선택한다. 키 K는 송신자와 수신자 모두에게 제공된다. 송신자와 수신자는 각각 블록 암호 암호화와 복호화에 관련된 키 셋업을 수행한다.

(2) 암호화 알고리즘 : $NAE_E(R, K, P)$

$P = P[1] \| \cdots \| P[m]$

$L \leftarrow E_K(R)$

$C[1] \leftarrow E_K(R \oplus (L+1)) \oplus P[1]$

for $i \leftarrow 2$ **to** m **do**

$C[i] \leftarrow E_K((L+i) \oplus C[i-1]) \oplus P[i]$

$C \leftarrow C[1] \| \cdots \| C[m]$

$l \leftarrow |P[m]|$

$Checksum \leftarrow P[1] \oplus \cdots \oplus P[m-1] \oplus P[m]0^{n-l}$

$T \leftarrow E_K(\text{Checksum} \oplus \text{C[m]}0^{n-1} \oplus (\text{L+m+1})) \oplus (L+m+1+l)\,[\text{first } \tau \text{ bits}]$

return $AC \leftarrow C \| T$

(3) 복호화 알고리즘 : $NAE_D(R, K, AC)$

$AC = C[1] \| \cdots \| C[m] \| T$

$L \leftarrow E_K(R)$

$P[1] \leftarrow E_K(R \oplus (L+1)) \oplus C[1]$

for $i \leftarrow 2$ **to** m **do**

$P[i] \leftarrow E_K((L+i) \oplus C[i-1]) \oplus C[i]$

$P \leftarrow P[1] \| \cdots \| P[m]$

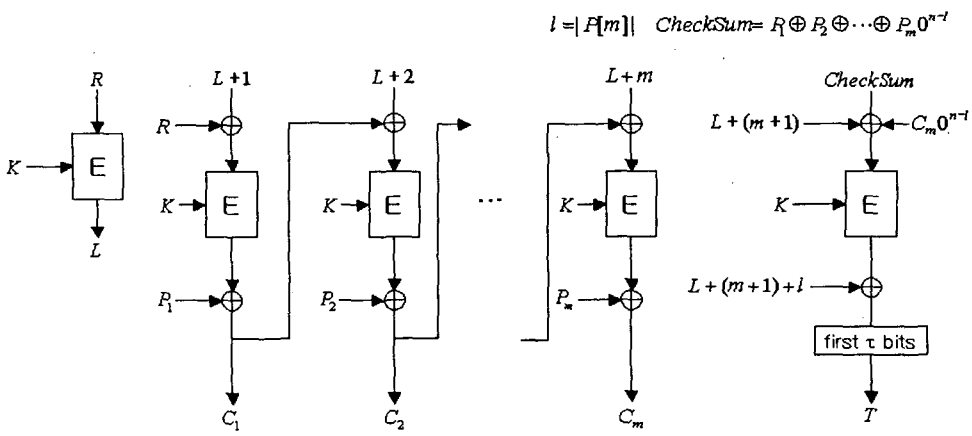
$l \leftarrow |C[m]|$

$CheckSum \leftarrow P[1] \oplus \cdots \oplus P[m-1] \oplus P[m]0^{n-l}$

$T' \leftarrow E_K(\text{CheckSum} \oplus \text{C[m]}0^{n-1} \oplus (\text{L+m+1})) \oplus (L+m+1+l)\,[\text{first } \tau \text{ bits}]$

if $T = T'$ **then return** P

else return INVALID



[그림 1] NAE의 암호화

III. NAE에 대한 위조 공격

본 절에서는 새로운 인증-암호화 모드 NAE에 대하여 단순한 암호문 조작으로 유효한 암호문-태그 쌍을 생성할 수 있음을 보인다. 위조 공격은 한 블록 메시지와 $m(>1)$개 블록 메시지에 대하여 각각 수행된다.

3.1 한 블록 메시지에 대한 위조 공격

공격자에게 1개 블록을 가지는 n 비트 메시지 P에 대한 유효한 암호문-태그 쌍 $C\|T$가 주어진다고 가정한다. 이때, 공격자는 임의의 n 비트 값 α에 대하여 암호문 C를 $C\oplus\alpha$로 단순 조작하여 새로운 암호문-태그 쌍 $C\oplus\alpha\|T^*$를 수신자에게 보낸다. 여기서 $C\oplus\alpha$는 n 비트 메시지 $P\oplus\alpha$에 대한 암호문을 의미한다. 그러면 다음과 같은 이유로 수신자는 $C\oplus\alpha\|T^*$를 유효한 암호문-태그 쌍으로 받아들인다.

T는 다음과 같은 식으로 표현된다.

$$T = E_K(\text{Checksum} \oplus \text{C} \oplus (\text{L}+2)) \oplus (L+2+n)[\text{first } \tau \text{ bits}]$$

그리고 새로운 태그 T^*는 다음과 같은 식으로 표현된다.

$$T^* = E_K(\text{Checksum}^* \oplus \text{C} \oplus \alpha \oplus (\text{L}+2)) \oplus (L+2+n)[\text{first } \tau \text{ bits}]$$

여기서, $CheckSum = P$이고 $CheckSum^* = P \oplus \alpha$이다. 따라서 T^*는 다음과 같이 표현된다.

$$\begin{aligned} T^* &= E_K(\text{Checksum}^* \oplus \text{C} \oplus \alpha \oplus (\text{L}+2)) \oplus (L+2+n)[\text{first } \tau \text{ bits}] \\ &= E_K(P \oplus \alpha \oplus C \oplus \alpha \oplus (L+2)) \oplus (L+2+n)[\text{first } \tau \text{ bits}] \\ &= E_K(P \oplus C \oplus (L+2)) \oplus (L+2+n)[\text{first } \tau \text{ bits}] \\ &= T \end{aligned}$$

이는 새로운 암호문-태그 쌍 $C\oplus\alpha\|T^*$가 유효함을 의미하고 수신자는 $C\oplus\alpha\|T^*$를 유효한 암호문-태그 쌍으로 받아들이게 된다. 따라서 공격자는 단순한 암호문 조작으로 유효한 암호문-태그 쌍을 생성할 수 있다.

3.2 $m(>1)$개 블록 메시지에 대한 위조 공격

m개 블록 메시지에 대한 위조 공격은 한 블록 메시지에 대한 위조 공격과 유사하다.

공격자에게 m개 블록을 가지는 $(n\times m)$ 비트 메시지 $P = P_1\|P_2\|\cdots\|P_m$에 대하여 유효한 암호문-태그 쌍 $C_1\|C_2\|\cdots C_m\|T$가 주어진다고 가정한다. 이때, 공격자는 임의의 n 비트 값 α에 대하여 암호문 $C_1\|C_2\|\cdots\|C_m$을 $C_1\|C_2\|\cdots\|C_m\oplus\alpha$로 단순 조작하여 새로운 암호문-태그 쌍 $C_1\|C_2\|\cdots\|C_m\oplus\alpha\|T^*$를 수신자에게 보낸다. 여기서 $C_1\|C_2\|\cdots\|C_m\oplus\alpha$는 $(n\times m)$ 비트 메시지 $P_1\|P_2\|\cdots\|P_m\oplus\alpha$에 대한 암호문을 의미하게 된다. 그러면 다음과 같은 이유로 수신자는 $C_1\|C_2\|\cdots\|C_m\oplus\alpha\|T^*$를 유효한 암호문-태그 쌍으로 받아들인다.

T는 다음과 같은 식으로 표현된다.

$$T = E_K(\text{Checksum} \oplus \text{C}_\text{m} \oplus (\text{L}+\text{m}+1)) \oplus (L+m+1+n)[\text{first}\tau\text{bits}]$$

그리고 새로운 태그 T^*는 다음과 같은 식으로 표현된다.

$$T^* = E_K(\text{Checksum}^* \oplus \text{C}_\text{m} \oplus \alpha \oplus (\text{L}+\text{m}+1)) \oplus (L+m+1+n)[\text{first}\tau\text{bits}]$$

여기서, $CheckSum = P_1 \oplus \cdots \oplus P_m$이고 $CheckSum^* = P_1 \oplus P_2 \oplus \cdots \oplus P_m \oplus \alpha$이다. 따라서 T^*는 다음과 같이 표현된다.

$$\begin{aligned} T^* &= E_K(\text{Checksum}^* \oplus \text{C}_\text{m} \oplus \alpha \oplus (\text{L}+\text{m}+1)) \oplus (L+m+1+n)[\text{first}\tau\text{bits}] \\ &= E_K(P_1 \oplus \cdots \oplus P_m \oplus \alpha \oplus C_m \oplus \alpha \oplus (L+m+1)) \oplus (L+m+1+n)[\text{first}\tau\text{bits}] \\ &= E_K(P_1 \oplus \cdots \oplus P_m \oplus C_m \oplus (L+m+1)) \oplus (L+m+1+n)[\text{first}\tau\text{bits}] \\ &= T \end{aligned}$$

이는 새로운 암호문-태그 쌍 $C_1\|C_2\|\cdots\|C_m\oplus\alpha\|T^*$가 유효함을 의미하고 수신자는 $C_1\|C_2\|\cdots\|C_m\oplus\alpha\|T^*$를 유효한 암호문-태그 쌍으로 받아들인다. 따라서 공격자는 단순한 암호문 조작으로 유효한 암호문-태그 쌍을 생성할 수 있다.

IV. 결론

신상욱 등은 JCCI 2003에서 새로운 인증-암호화 모드 NAE를 제안하였다[1]. NAE는 CFB 모드와 CTR 모드를 결합시킨 변형된 형태로, 하나의 기반이 되는 블록 암호 키를 가지고 최소한으로 블록 암호를 호출하여 기밀성과 무결성을 모두 제공한다. 이 모드는 CBC 암호화 모드와 CBC-MAC이 결합된 CCM 인증-암호화 모드보다 효율적이며, 기제안된 인증-암호화 기법들과 유사한 성능을 가진다. 그러나 본 논문

에서는 단순한 암호문 조작으로 유효한 암호문-태그 쌍을 생성할 수 있음을 보였다. 이는 NAE가 위조 공격에 매우 취약함을 의미하므로 실생활에 절대 사용되어서는 안 된다.

[참고문헌]

[1] 신상욱, 류희수. 새로운 인증된 암호화 기법. JCCI 2003 [S9-692], April, 2003.

[2] M. Bellare and C. Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. Advances in Cryptology ASIACRYPT 2000. LNCS 1976, Springer-Verlag, 2000.

[3] M. Bellare, J. Kilian, and P. Rogaway. The security of the cipher block chaining message authentication code. Journal of Computer and System Sciences, vol. 61, no. 3, Dec 2000.

[4] J. Black and P. Rogaway. CBC-MACs for arbitrary-length messages: The three key construction. Advances in Cryptology-Crypto 2000, LNCS 1880, pp.197-215, Springer-Verlag, 2000.

[5] D. McGrew and J. Viega. The Galois/Counter mode of operation (GCM). Submission to NIST. Available at http://csrc.nist.gov/CryptoToolkit/modes/, 2004.

[6] D. Whiting, R. Housley and N. Ferguson. Counter with CBC-MAC (CCM). Submission to NIST. Available at http://csrc.nist.gov/CryptoToolkit/modes/, 2002.

[7] ISO/IEC 9797-1. Information technology-Security techniques-Message Authentication Codes 35: 1626-1627, 1999.

[8] K. Kurosawa and T. Iwata. TMAC: Two-Key CBC-MAC. Topics in Cryptology-CT-RSA 2003. LNCS 2612. pp. 33-49, Springer-Verlag, 2003.

[9] J. Sung, D. Hong and S. Lee. Key Recovery Attacks on the RMAC, TMAC and IACBC. ACISP 2003. LNCS 2727. pp. 265-273, Springer-Verlag, 2003.

[10] C. J. Mitchell. On the Security of XCBC, TMAC and OMAC. Technical Report RUHL-MA-2003-4. 19. August, 2003.