김일성종합대학학보
(자연과학)
주체103(2014)년 제60권 제12호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 60 No. 12 JUCHE103(2014).

내부상태예측공격에 안전한 통보문인증부호구성의 한가지 방법

박 진 국

위대한 령도자 **김정일**동지께서는 다음과 같이 교시하시였다.

《기초과학부문들을 발전시켜야 나라의 과학기술수준을 빨리 높일수 있고 인민경제 여러 분야에서 나서는 과학기술적문제들을 원만히 풀수 있으며 과학기술을 주체성있게 발전시켜나갈수 있습니다.》(《**김정일**선집》 증보판 제10권 485페지)

론문에서는 정보보안의 중요한 수단의 하나로 되고있는 통보문인증부호(MAC)의 한가지 구성방법을 연구하였다.

선행연구[1]에서는 통보문인증부호에 대한 내부상태예측공격방법과 그 효과성을 론의하였으나 그 공격에 안전한 통보문인증부호의 구성방안에 대하여 제기하지 못하였다.

론문에서는 선행연구[1]에서 제안된 공격방법에 견딜수 있는 한가지 새로운 통보문인증부호를 비밀열쇠암호 AES와 4단 AES를 리용하여 구성하고 그 효과성을 검증하였다.

1. 제안한 통보문인증부호(MAC)알고리듬

여기서 제기한 통보문인증부호는 임의의 길이의 통보문을 입력하면 128bit의 통보문을 출력한다. 만일 입력통보의 길이가 128bit의 배수로 되지 않는다면 통보문의 첫 비트는 1이고 128의 배수로 되는 최소의 비트수만큼 0을 붙여서 얻은 렬을 통보문에 보충하여 통보문을 확장한다. 이때 확장된 통보문을 $X_1, X_2, \cdots, X_m$으로 표시한다. 여기서 X_i는 128bit이다.

제안한 통보문인증부호알고리듬은 다음과 같다.

① $Y_0 = E_k(0) \oplus X_1$

여기서 E는 AES암호화함수이고 k는 비밀열쇠이며 $\oplus$는 XOR연산이다.

② $Y_0' = f(Y_0) \oplus X_2$로 하고 Y_1을 구한다. 즉

$$Y_1 = H_1(Y_0,\ Y_0') = G_{kk_1}(E_k(0) \oplus X_1 \oplus E_k(1+a)) \oplus (F(E_k(0) \oplus X_1) \oplus X_2).$$

여기서 $H(\alpha,\ \beta) = G_{kk_i}(\alpha \oplus E_k(i+a) \oplus \beta)$, $kk_i = E_k(i-1) \oplus E_k(i)$, $a = 1+2+\cdots+m$이며 F는 4-AES암호화함수이다.

③ $Y_i = H_i(Y_{i-1},\ Y_{i-1}') = G_{kk_i}(Y_{i-1} \oplus E_k(i+1)) \oplus (F(Y_{i-1}) \oplus X_i)$

④ $C = \mathrm{Trunc}(E_k(H_m))$

여기서 Trunc(·) 는 끝을 자르는 함수이다.

제기한 통보문인증부호구성도는 그림 1과 같다.

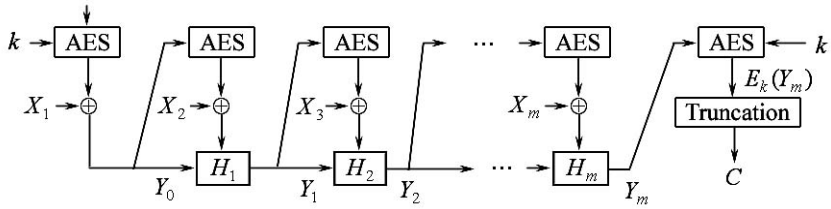

그림 1. 한가지 통보문인증부호구성도

2. 선행한 방법과 비교

선행연구[2]에서는 통보문의 2, 3, 4, 7, 8, 9, 13, 14번째 Byte들의 값들을 동일하게 취할 때 Y_1, Y_1'가 오직 1개의 B만큼 차이나는 통보문쌍의 존재성을 밝히고 그에 기초하여 충돌쌍을 생일공격을 리용하여 찾을수 있는 방법을 제기하였다. 여기서 제기한 MAC는 128bit통보문 X_1, X_1'가 주어진 경우로서 그 도식은 그림 2와 같다.

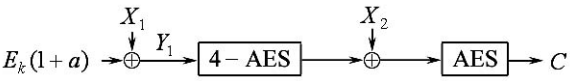

그림 2. 선행한 방법의 MAC구성도

론문에서 새롭게 제안한 MAC는 그림 3과 같다.

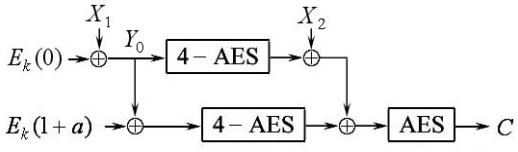

그림 3. 제기한 MAC구성도

그림 2와 3으로부터 알수 있는바와 같이 선행연구[2]에서는 MAC값 C에 대하여 어떤 Y_2, Y_2'가 있어서 충돌이 생기는 경우를 $Y_2 = \mathrm{AES}^{4r}(Y_1) \oplus X_2$인 Y_1, Y_1' 즉

$$\mathrm{AES}^{4r}(Y_1) \oplus \mathrm{AES}^{4r}(Y_1') = X_2 \oplus X_2',$$

$$\mathrm{AES}^{4r}(E_k(1+a) \oplus X_1) \oplus \mathrm{AES}^{4r}(E_k(1+a) \oplus X_1') = X_2 \oplus X_2'$$

를 만족시키는 그런 X_2, X_2'를 찾는 문제를 제기하고 $\Delta X_1 = Y_1 - Y_1'$를 리용하여 특수한 경우의 충돌통보문쌍을 얻을수 있다는것을 밝혔다.

그러나 론문에서 제안한 MAC도식에서는 다음과 같이 결정된다.

$$\mathrm{AES}^{4r}(Y_1) \oplus \mathrm{AES}^{4r}(Y_1') = X_2 \oplus X_2' \oplus E_k(Y_0),$$

$$\mathrm{AES}^{4r}(E_k(1+a) \oplus E_k(Y_0) \oplus X_1) \oplus \mathrm{AES}^{4r}(E_k(1+a) \oplus E_k(Y_0) \oplus X_1') = X_2 \oplus X_2' \oplus E_k(Y_0)$$

우의 식에서 보는바와 같이 론문에서 제기한 MAC는 선행연구[2]에서 리용한 공격방법에 비하여 안전하다. 특히 론문에서 리용한 $G(\cdot)$와 $F(\cdot)$에서의 열쇠값은 k와 kk로서 서로 다르다. 또한 론문에서는 kk의 생성을 $kk_i = E_k(i-1) \oplus E_k(i)$와 같이 구성함으로써 원문의 혼란과 확산을 크게 하였다.

맺 는 말

선행연구에서 주목한 내부상태공격에 대응하여 비밀열쇠를 보조적으로 생성하는 방법으로 극복하고 원문의 혼란과 확산을 크게 하였다.

참 고 문 헌

[1] K. Mimenmatsu et al.; Mathematics and Computer Science, 2, 2, 226, 2006.

[2] G. Yuval et al.; Cryptologia, 3, 187, 1999.

주체103(2014)년 8월 5일 원고접수

A Method on Secure Component of MAC for Internal State Recovery Attack

Pak Jin Guk

The previous study presented a method of internal state recovery for one MAC and proved its effectiveness. In this paper, internal state recovery attack observed in the previous study was overcome by making the sub-secret key from the main key, which enlarged confusion and expansion of the original message.

Key words: MAC, birthday attack, internal state recovery