通信情報保護學會論文誌
第 11 券 第 2 號, 2001. 4

3GPP MAC 알고리즘 안전성 분석

홍 도 원*, 신 상 욱*, 강 주 성*, 이 옥 연*

An analysis on the security of the 3GPP MAC algorithm

Dowon Hong*, Sang Uk Shin*, Ju-Sung Kang*, Okyeon Yi*

요 약

비동기식(W-CDMA) 3세대 이동통신의 3GPP에서는 무선 구간의 메시지 무결성을 보장하기 위하여 블록 암호 KASUMI에 기반한 CBC-MAC의 변형된 형태를 제안하고 있다. 본 논문에서는 최근 발표된 Knudsen-Mitchell의 공격법을 심층 분석하여 구체적인 공격 수행 알고리즘을 제안하고, 이 알고리즘의 성공 확률 및 수행 복잡도를 계산한다. 또한, 3GPP-MAC에 대한 안전성을 기존 CBC-MAC 방식과 비교하여 분석한다.

ABSTRACT

3GPP proposed a variant CBC-MAC based on the block cipher KASUMI to provide the data integrity over a radio access link. We have studied deeply the Knudsen and Mitchell's attack. In this paper we proposed a definite performing algorithm of the Knudsen and Mitchell's attack and compute the success probability and complexity of that algorithm. Moreover We also analyze a security of 3GPP-MAC comparing with the original CBC-MAC.

keyword : *3GPP-MAC, CBC-MAC, forgery attack, key recovery attack*

Ⅰ. 서 론

메시지 인증 코드(Message Authentication Code :MAC)는 전송되는 메시지의 무결성과 출처 인증을 위해 광범위하게 사용된다. MAC은 송신자와 수신자가 같은 비밀키 K를 가지고 있는 시스템 환경에 적용된다. 메시지 x를 보호하기 위하여 송신자는 K와 x의 함수인 $MAC_K(x)$를 계산하여 메시지 x에 부가하여 보낸다. 메시지 x를 받은 수신자는 공유하고 있는 비밀키 K를 이용하여 $MAC_K(x)$를 계산한 후 전송된 MAC 값과 비교함으로써 메시지 x가 변조되지 않고 정당한 사용자로부터 온 것임을 검증한다.

MAC의 주요한 안전성 요인은 위장 공격이 불가능해야 한다는 것이다. 즉, 비밀키 K를 알지 못하는 공격자가 임의의 새로운 메시지 x와 대응되는 $MAC_K(x)$를 계산하는 것이 계산량적으로 불가능해야 한다. MAC에 대한 두 번째 공격은 키 탐색 공격이다. 공격자가 비밀키 K를 얻을 수 있다면 임의의 메시지와 대응하는 MAC 쌍을 위장할 수 있다.

비동기식(W-CDMA) 3세대 이동 통신 진영의 3GPP (3rd Generation Partnership Project)에서도 무선 구간의 메시지 무결성을 보장하기 위하여 블록 암호 KASUMI에 기반한 CBC-MAC의 변형된 형태를 제안하고 있다.[1] 블록 암호 동작 모드의 한 형태인 CBC(Cipher Block Chaining) 모드를 이용한 CBC-MAC은 국제 표준 ISO/IEC 9797-1[2]에 기본적인 CBC-MAC과 그 변형된 형태로 6종류의 CBC-MAC 알고리즘들이 제시되어 있다. 이들은 세 가지 메시지 패딩 방법 중 한 가지를 사용하고, 두 가지 입력 변환과 세 가지 출력 변환으로

* 한국전자통신연구원 정보보호기술연구본부 ({dwhong, shinsu, jskang, oyyi}@etri.re.kr)

구성된다. 이들 CBC-MAC 알고리즘의 안전성 분석은 ISO/IEC 9797-1[2] 문서와 Preneel-Oorschot[3], Knudsen[4], Brincat-Mitchell[5] 등에 의해 이루어졌다. 또한, ANSI X9.19[6] retail MAC으로 명명된 CBC-MAC 형태는 Preneel-Oorschot,[7] Knudsen-Preneel[8]에 의해 자세히 분석되었다.

3GPP-MAC에 대한 안전성 분석은 최근에 Knudsen-Mitchell[9]에 의해 이루어졌다. 그들은 위장 공격과 키 탐색 공격 관점에서 3GPP-MAC의 안전성을 분석하였다.

본 논문에서는 먼저 Knudsen과 Mitchell의 공격법을 심층 분석하여 구체적인 공격 수행 알고리즘을 제안하고 이 알고리즘의 성공 확률 및 수행 복잡도를 계산한다. 다음으로 기존의 CBC-MAC 방식과 변형된 형태인 3GPP-MAC 방식의 안전성을 비교 분석한다.

II. 3GPP-MAC의 공격법 분석

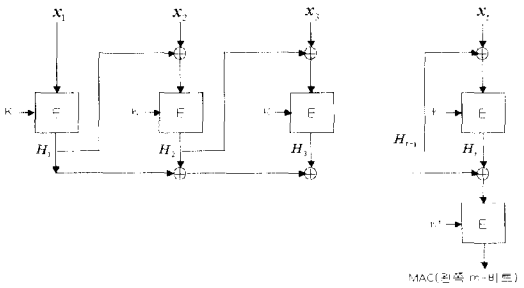
2.1 3GPP-MAC 알고리즘

3GPP 무결성 알고리즘 f9로 사용되는 3GPP-MAC 알고리즘의 경우는 ISO/IEC 9797-1에서 정의한 6가지 형태의 CBC-MAC과는 다른 형태의 변형된 CBC-MAC을 이용한다. 기존 CBC-MAC과의 가장 큰 차이점은 최종 출력 변환의 입력 값으로 이전의 블록 암호 출력 값으로 나온 모든 연쇄 변수를 XOR한다는 것이다.

3GPP-MAC은 아래와 같이 동작한다. 기본 블록 암호는 n-비트 블록들을 가지고 k-비트의 비밀키를 이용한다고 가정하자. 만약 X가 n-비트 블록을 가진다면 비밀키 K를 사용한 X의 암호화를 $E_K(X)$로 표기한다. 메시지 x는 먼저 n의 배수가 되도록 메시지의 끝에 하나의 1과 나머지 0를 이용하여 패딩되고 t 개의 n-비트 블록들 $x_1\|x_2\|\cdots\|x_t$로 분할된다. 여기에서 기호 $\|$는 연결을 뜻한다. 앞으로 우리는 패딩된 메시지만 고려할 것이다. 3GPP-MAC은 키 쌍 K, K'을 사용하며, K'은 K로부터 다음과 같이 유도될 수 있다.

$$K' = K \oplus C,$$

여기서 $C = 0101\cdots01$ (128비트)인 이진 상수이다. MAC 값의 계산은 다음과 같다([그림 1] 참조):



[그림 1] 3GPP-MAC 알고리즘

$$H_1 = E_K(x_1),$$
$$H_i = E_K(x_i \oplus H_{i-1}), \quad (2 \le i \le t),$$
$$MAC = E_{K'}(H_1 \oplus H_2 \oplus \cdots \oplus H_t).$$

여기에서 H_i는 연쇄 변수라 불리우며 3GPP-MAC에서 사용되는 MAC 값은 위의 마지막 식에서 주어진 MAC의 최상위 m-비트 ($m \le n$)만을 이용한다. 3GPP 기술 문서[1]에 제시된 무결성 알고리즘 f9는 기본 블록 암호로 128-비트 키와 64-비트 블록을 가진 KASUMI 알고리즘을 이용하며, MAC 값의 길이는 32-비트를 사용한다.

일반적으로 블록 암호에 기반한 CBC-MAC인 경우 블록 암호가 랜덤한 순열이라는 가정이 필요하다. 본 논문에서도 블록 암호 KASUMI의 랜덤성은 가정하고, 아래 보조 정리에서 KASUMI가 순열임을 보인다.

보조 정리 1.
블록 암호 KASUMI는 순열이다.

증명) 3GPP 기술 문서[10]에 나타난 KASUMI 알고리즘의 블록 구조는 다음과 같이

$$K(L, R) = (R \oplus f(L), L)$$

이고, K의 역은

$$K^{-1}(L, R) = (R, L \oplus f(R))$$

이다. 여기서 L, R은 임의의 32-비트 이진 벡터이다. 그러면

$$\begin{aligned} K^{-1}(K(L, R)) &= K^{-1}(R \oplus f(L), L) \\ &= (L, R \oplus f(L) \oplus f(L)) \\ &= (L, R), \end{aligned}$$

이고 비슷한 방법으로

$$K(K^{-1}(L, R))=(L, R)$$

이다. 따라서 KASUMI는 순열이다. □

Preneel-Oorshot[3]에 의하면 대부분의 공격은 두 메시지가 같은 MAC 값을 가지는 충돌 쌍에 기반한다. 따라서 본 논문에서도 두 메시지가 같은 MAC 값과 같은 마지막 연쇄 변수를 가질 때 내부 충돌(internal collision) 쌍이라 부르고, 내부 충돌 쌍이 아닌 충돌 쌍을 외부 충돌(external collision) 쌍이라 부른다.

ISO/IEC 9797-1[2]에서 사용된 표현 방법에 따라 공격자에게 필요한 자원을 명확하게 규정하기 위해 $[a, b, c, d]$ 표기를 사용한다. 여기서 a는 오프라인 블록 암호 암호화 횟수, b는 알려진 메시지/MAC 쌍의 수, c는 선택 메시지/MAC 쌍의 수, d는 온라인 MAC 검증 횟수를 나타낸다.

2.2 Knudsen-Mitchell 위장 공격법의 분석

본 절에서는 3GPP-MAC의 알려진 공격법 중 가장 효율적인 Knudsen과 Mitchell[9]의 위장 공격법을 고찰한다. 먼저 그들의 공격을 심층적으로 분석하고 구체적인 공격 수행 알고리즘의 복잡도를 계산하기 위해 필요한 몇 가지 정리들을 알아보자.

다음 두 보조 정리는 '생일 역설'로 잘 알려진 내용이다.

보조정리 2.

1에서 n까지의 번호가 적힌 n개의 공을 가진 한 개의 단지가 있다고 하자. 한 번 시행에 한 개씩 복원 추출을 통해 단지에서 r개의 공을 꺼내어 그 번호를 기록한다고 하자. n이 충분히 크고, $r=O(\sqrt{n})$일 때, 적어도 한 쌍의 충돌이 발생할 확률은 대략

$$1-\exp\left(-\frac{r(r-1)}{2n}\right)\approx 1-\exp\left(-\frac{r^2}{2n}\right)$$

이다.

보조정리 3.

1에서 n까지의 번호가 적힌 n개의 흰 공을 가진 단지와 1에서 n까지의 번호가 적힌 n개의 빨간 공을 가진 단지가 있다고 하자. 한 번 시행에 한 개씩 복원 추출을 통해 두 단지에서 각각 r_1개와 r_2개의 공을 꺼내어 그 번호를 기록한다고 하자. n이 충분히 크고, $r_1=r_2=r$, $r=O(\sqrt{n})$이면, 적어도 한 쌍의 충돌이 발생할 확률은 대략

$$1-\exp\left(-\frac{r^2}{n}\right)$$

이다.

Knudsen-Mitchell의 위장 공격법은 다음과 같다.

공격자가 $2^{\frac{n+m}{2}}$개의 알려진 메시지/MAC 쌍을 가지고 있다고 가정하자. $2^{\frac{n+m}{2}}$개의 알려진 MAC 값들을 MAC 값에 따라 2^m개의 집합으로 분할하자. 적어도 한개의 집합은 모두 MAC 값이 같은 $2^{(n-m)/2}$개 이상의 메시지를 포함할 것이고 그 집합을 선택한다. 이들 메시지 중에서 2개는 버려진 $(n-m)$-비트에서도 충돌할 것으로 기대된다. 선택한 집합의 모든 메시지 $x=x_1\|x_2\|\cdots\|x_t$에 대해, $2^{n/2}$개의 랜덤하게 선택한 $y(i)$로 만든 $x\|y(i)$ 메시지들과 대응하는 MAC 값들을 얻는다. 선택한 메시지/MAC 쌍의 총 개수는 $2^{(n-m)/2}\cdot 2^{n/2}=2^{n-m/2}$이므로 생일 역설에 의하여 좋은 확률로 같은 MAC 값을 가지면서 $H_t\oplus y=H'_s\oplus y'$가 되는 메시지들 $x_1\|\cdots\|x_t\|y$와 $x'_1\|\cdots\|x'_s\|y'$가 존재한다. 즉, $2^{n-m/2}$개의 선택 메시지/MAC 쌍의 집합에서 내부 충돌 쌍이 존재한다. $2^{n-m/2}$개의 메시지 중에서 충돌이 발생할 메시지는 $2^{n-m/2}$보다 작으므로 이들 메시지 중에서 내부 충돌 쌍을 찾기 위해서는 $2^{n-m/2}$개의 메시지의 끝에 고정된 n-비트 블록을 더한 새로운 메시지의 MAC 값이 필요하다. 이것은 $2^{n-m/2}$과 비교하여 무시할 수 있는 수이다.

x와 x'의 연쇄변수들에 대해 $H_1\oplus H_2\oplus\cdots\oplus H_t=H'_1\oplus H'_2\oplus\cdots\oplus H'_s$이 성립하고 $x\|y$와 $x'\|y'$이 내부 충돌 쌍이면 $H_t\oplus y=H'_s\oplus y'$이고

$$\triangle=y\oplus y'=H_t\oplus H'_s$$

이다. 그러면 임의의 n-비트 블록 z에 대하여

$$H_1 \oplus H_2 \oplus \cdots \oplus H_t \oplus E_K(H_t \oplus z)$$
$$= H'_1 \oplus H'_2 \oplus \cdots \oplus H'_s \oplus E_K(H_t \oplus H'_s \oplus H'_s \oplus z)$$
$$= H'_1 \oplus H'_2 \oplus \cdots \oplus H'_s \oplus E_K(H'_s \oplus z \oplus \triangle)$$

이므로 $x\|z$와 $x'\|(z \oplus \triangle)$는 같은 MAC 값을 가진다. 그러므로 공격자가 $x\|z$의 MAC 값을 관찰하거나 요청함으로써 $x'\|(z \oplus \triangle)$의 MAC 값을 위조할 수 있다. 이 공격의 총 복잡도는

$$[0,\ 2^{(n+m)/2},\ 2^{n-m/2},\ 0]$$

이다.

$n=64$, $m=32$를 사용하는 3GPP-MAC의 경우 2^{48}개의 선택 메시지/MAC 쌍과 2^{48}개의 알려진 메시지/MAC 쌍을 가진 공격자에 의해 위장 공격이 가능하다. 하지만 그들의 증명에서 구체적으로 위장 공격에 성공하기 위한 공격 수행 시나리오와 위장 공격에 성공하기 위한 실제적인 공격 복잡도를 정확하게 알 수는 없다.

2.3 위장 공격 수행 알고리즘

본 절에서는 Knudsen-Mitchell의 위장 공격법에 기반하여 실제적으로 공격을 성공하기 위해서 필요한 위장 공격 수행 알고리즘을 제안하고 그 성공 확률 및 수행 복잡도를 계산한다.

〔단계 1〕

$2^{\frac{n+m}{2}}$개의 알려진 메시지/MAC 쌍을 수집한다.

〔단계 2〕

수집된 $2^{\frac{n+m}{2}}$개의 메시지/MAC 쌍들을 MAC 값에 따라 분류할 때 처음으로 분류된 같은 MAC 값을 가진 $2^{(n-m)/2}$개의 메시지 집합을 선택한다.(단계 2가 다시 반복될 때에는 그 다음으로 분류된 메시지 집합을 택한다.)

〔단계 3〕

단계 2에서 선택한 집합의 모든 메시지 $x=x_1\|x_2\|x_t\|\cdots$에 대해, $2^{m/2}$개의 랜덤하게 선택한 $y(i)$로 만든 $x\|y(i)$ 메시지들과 대응하는 MAC 값들로 이루어진 전체 $2^{(n-m)/2} \cdot 2^{m/2} = 2^{n-m/2}$개의 메시지/MAC 집합을 구한다.

〔단계 4〕

단계 3에서 선택한 $2^{n-m/2}$개의 메시지/MAC 쌍을 같은 MAC 값을 가지는 메시지 집합들로 정렬한다.

〔단계 5〕

남아있는 메시지 집합들을 $\{X_i\}$라 할 때, 고정된 n-비트 블록 y를 첨가하여 새로운 메시지 집합들 $\{X_i\|y\}$를 구하고 대응하는 $\{MAC(X_i\|y)\}$ 집합들을 조사하여 충돌이 없으면 대응하는 메시지 X_i들을 각각의 집합에서 버린다.

〔단계 6〕

단계 5를 수행한 후 원래 메시지 집합들 $\{X_i\}$에서 버려진 메시지들을 제외하고 남아있는 메시지 집합들 중 메시지의 개수가 한 개인 집합은 버리고 남아있는 메시지 집합들을 구한다.

〔단계 7〕

단계 5와 단계 6을 $\lceil \frac{n}{m} \rceil$번 반복한다.

〔단계 8〕

단계 7을 수행한 후 두 개의 메시지를 가진 집합이 한 개 이상 존재한다면 이 메시지 쌍들을 내부 충돌쌍으로 출력한다. 남아있는 집합이 없다면 단계 2로 돌아간다.

〔단계 9〕

단계 8에서 구한 메시지 쌍을 $x=x_1\|\cdots\|x_t\|y$와 $x=x'_1\|\cdots\|x'_s\|y'$, 그리고 $\triangle = y \oplus y'$라고 할 때 임의의 n-비트 블록 z에 대하여 $x\|z$의 MAC 값을 관찰하거나 요청함으로써 $x'\|(z \oplus \triangle)$의 MAC 값을 위조한다.

이 공격 수행 알고리즘의 성공 확률과 공격 복잡도를 알아보자. 먼저 단계 2에서 단계 7까지의 수행을 통하여 단계 8에서 내부 충돌 쌍을 발견할 확률을 구해보자. 먼저 단계 2에서 버려진 $(n-m)$-비트에서도 충돌하는 메시지들이 있을 확률은 보조정리 2에 의해 대략 $1-e^{-1/2} \approx 0.39$이다. 단계 3에서 선택

한 $2^{n-m/2}$개의 메시지 중에서 $H_t \oplus y = H'_s \oplus y'$을 만족하는 내부 충돌 쌍 $x_1 \| \cdots \| x_t \| y$와 $x'_1 \| \cdots \| x'_s \| y'$을 발견할 확률은 다음과 같이 계산된다. 먼저

$$H_1 \oplus \cdots \oplus H_t \oplus E_K(H_t \oplus y)$$
$$= H'_1 \oplus \cdots \oplus H'_s \oplus E_K(H'_s \oplus y')$$

인 메시지 $x_1 \| \cdots \| x_t \| y$와 $x'_1 \| \cdots \| x'_s \| y'$가 존재할 확률은 보조정리 3에 의해 대략 $1-e^{-1} \approx 0.63$이고 동시에 $H_1 \oplus \cdots \oplus H_t = H'_1 \oplus \cdots \oplus H'_s$이 성립할 확률은 $0.63 \times 0.39 \approx 0.25$이다. 따라서 단계 8에서 내부 충돌 쌍을 출력하기 위해서는 단계 2에서 단계 7까지 평균 4번 반복 수행이 필요하다.

이제 이 공격 알고리즘의 복잡도를 계산해 보자. 단계 5, 6, 7을 수행하는 데에 필요한 선택 메시지의 개수는 대략 $2^{n-m/2} + 2^{n-3m/2} + 2^{n-5m/2} + \cdots \approx \frac{2^{n-m/2}}{1-2^{-m}} \approx 2^{n-m/2}$이다. 따라서 이 공격 알고리즘을 수행하기 위해 필요한 선택 메시지의 개수는 대략 $4 \cdot 2^{n-m/2+1} = 2^{n-m/2+3}$이다. 따라서 총 공격 복잡도는 $[0, 2^{(n+m)/2}, 2^{n-m/2+3}, 0]$이다. $n=64$, $m=32$인 경우 $[0, 2^{48}, 2^{51}, 0]$의 공격 복잡도를 가지고 항상 위장 공격에 성공할 수 있다.

단계 8에서 내부 충돌 쌍을 발견하는 성공 확률을 높이기 위해서는 단계 1의 알려진 메시지/MAC 쌍의 개수를 $2^{\frac{n+m}{2}+1}$로 증가시키면 단계 2에서 버려진 $(n-m)$-비트에서 충돌하는 메시지들이 있을 확률은 대략 $1-e^{-2} \approx 0.86$으로 증가한다. 따라서 단계 8에서 내부 충돌쌍이 있을 성공 확률은 0.54로 증가하고 전체 선택 메시지/MAC 쌍의 개수는 2^{50}으로 감소한다. 하지만 증가 시킬 수 있는 성공 확률이 0.63으로 제한되므로 알려진 메시지/MAC 쌍의 개수는 제한적이다. [표 1]은 성공 확률과 공격 수행 복잡도의 관계를 나타낸 것이다.

[표 1] 성공 확률과 알려진 메시지/MAC, 선택 메시지/MAC 쌍의 관계 ($n=64$, $m=32$ 인 경우)

복잡도 / 성공확률	알려진 메시지/MAC 쌍	선택 메시지/MAC 쌍	공격 수행 복잡도
0.02	2^{46}	1.6×2^{54}	$[0, 2^{46}, 1.6 \times 2^{54}, 0]$
0.12	2^{47}	1.7×2^{52}	$[0, 2^{47}, 1.7 \times 2^{52}, 0]$
0.25	2^{48}	2^{51}	$[0, 2^{48}, 2^{51}, 0]$
0.54	2^{49}	2^{50}	$[0, 2^{49}, 2^{50}, 0]$
0.63	2^{50}	1.6×2^{49}	$[0, 2^{50}, 1.6 \times 2^{49}, 0]$
0.63	2^{51}	1.6×2^{49}	$[0, 2^{51}, 1.6 \times 2^{49}, 0]$

Ⅲ. 3GPP-MAC과 기존 CBC-MAC 방식의 안전성 비교

먼저 CBC-MAC에 대한 다른 공격 형태인 키 탐색 공격의 경우를 살펴 보자. 키 쌍 K, K'이 서로 독립적으로 선택된 경우에는 Preneel-Oorschot[7]에서 사용된 분할과 정복(divide and conquer) 키 탐색 공격법을 이용한 결과들이 Knudsen-Mitchell[9]의 논문에 나타나 있다. 하지만 실제로 3GPP 기술문서[1]에 나타난 3GPP f9 함수의 경우 키 K'은 원래의 무결성 키 K로부터 유도되므로 우리는 간단한 전수 조사를 통하여 그 공격량을 알 수 있다.

정리 3.

3GPP-MAC에 대해 키 K'이 다른 키 K로부터 유도되는 경우, 메시지 길이가 기껏해야 t개 블록인 $\lceil \frac{k+1}{m} \rceil$개의 알려진 메시지/MAC 쌍과 $(t+1) \cdot 2^k$번의 암호화 연산으로 키 쌍 K, K'을 찾을 수 있다. 즉, 이 공격의 공격량은

$$[(t+1) \cdot 2^k, \lceil \frac{k+1}{m} \rceil, 0, 0]$$

이다.

따라서 키 K'의 사용은 안전성 측면에서는 키 K를 사용하는 것과 별 차이가 없으며 MAC 값의 길이 m이 작을수록 이 공격의 복잡도는 증가한다는 사실을 알 수 있다. 3GPP f9 함수의 경우 $k=128$, $m=32$이므로 키 탐색 공격은 현실적으로 불가능하다.

일반적인 CBC-MAC의 경우 생일 공격법을 이용하면 $\sqrt{2} \cdot 2^{n/2}$개의 알려진 메시지/MAC 쌍과 $\lceil \frac{n}{m} \rceil \cdot 2^{n-m}$개의 선택 메시지/MAC 쌍이 있으면 위장 공격이 가능하다. 가장 효율적인 Knudsen[4]의 공격법을 적용하면 $2^{\lceil \frac{n-m}{2} \rceil + 1}$개의 선택 메시지/MAC 쌍과 2개의 알려진 메시지/MAC 쌍이 필요하다. 즉, $n=64$, $m=32$인 경우 대략 2^{17}개의 선택 메시지/MAC 쌍을 가지면 일반적인 CBC-MAC에 대한

〔표 2〕 CBC-MAC과 3GPP-MAC의 공격 복잡도 비교 ($k=128$, $n=64$, $m=32$인 경우)

구분 \ 공격방식	위장 공격	키 탐색 공격
CBC-MAC	$[0,2,2^{17},0]$	$[t2^{128},5,0,0]$
3GPP-MAC	$[0,2^{48},2^{51},0]$	$[(t+1)2^{128},5,0,0]$

공격이 가능하다. 하지만 3GPP-MAC에서는 최종 출력 변환의 입력 값으로 모든 연쇄 변수를 XOR하여 사용함으로써 필요한 공격량을 2^{51}으로 증가시킬 수 있었다. 〔표 2〕는 $k=128$, $n=64$, $m=32$인 경우 CBC-MAC과 3GPP-MAC에 대한 현재까지 알려진 가장 효율적인 위장 공격과 키 탐색 공격의 복잡도를 비교 정리한 것이다. 3GPP-MAC의 경우 m이 작을수록 위장 공격이나 키 탐색 공격의 복잡도는 증가하지만 추측 공격을 고려하여 $m=n/2$를 사용하고 있으며, 이 경우 현실적인 공격은 불가능하다.

Ⅳ. 결 론

본 논문에서는 비동기식 3세대 이동통신의 무선 구간 무결성을 보장하기 위해 사용되는 3GPP-MAC의 안전성을 분석하였다. Knudsen-Mitchell의 공격법을 심층 분석하여 구체적인 공격 수행 알고리즘을 제안하고 이 알고리즘의 성공 확률 및 수행 복잡도를 계산하였다. 또한, 일반적인 CBC-MAC과의 안전성 비교를 통하여 3GPP-MAC에서 사용된 최종 출력 변환의 입력 값으로 연쇄 변수들의 XOR한 값을 이용하는 것이 위장 공격 관점에서 안전성을 높이는 효과가 있다는 것을 보였다.

3GPP-MAC의 안전성 분석과 관련된 것으로 아직까지 발표되지 않은 연구 과제는 Bellare 등[11]과 Petrank-Rackoff[12] 등에 의해 연구되어 온 안전성에 대한 이론적인 검증이다. 블록 암호 KASUMI의 유사 랜덤성에 기반한 3GPP-MAC의 유사 랜덤성에 대한 연구가 안전성 요인 중의 하나로 반드시 규명되어야 할 문제라 생각된다.

참 고 문 헌

〔1〕 3G TS 35.201 "Specification of the 3GPP confidentiality and integrity algorithm: Document 1: f8 and f9 specifications".

〔2〕 ISO/IEC 9797-1, Information technology - Security techniques-Message Authentication Codes(MACs)-Part 1: Mechanism using a block cipher, 1999.

〔3〕 B. Preneel and P.V. van Oorschot, "On the security of iterated Message Authentication Codes", IEEE Transactions on Information Theory, 45, pp. 71~82, 1999.

〔4〕 L.R. Knudsen, "Chosen-text attack on CBC-MAC", Electronics Letters, 33, pp. 48~49, 1997.

〔5〕 K. Brincat and C.J. Mitchell, "New CBC-MAC forgery attacks", preprint.

〔6〕 American Bankers Association, Washington, DC. ANSI X9.19, "Financial institution retail message authenticaion", August 1986.

〔7〕 B. Preneel and P.V. van Oorschot, "A key recovery attack on the ANSI X9.19 retail MAC", Electronics Letters, 32(17), pp. 1568~1569, 1996.

〔8〕 L.R. Knudsen and B. Preneel, "MacDES: MAC algorithm based on DES", Electronics Letters, 34, pp. 871~873, 1998.

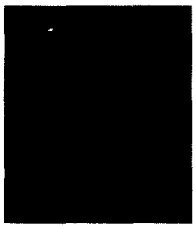
〔9〕 L.R. Knudsen and C.J. Mitchell, "An analysis of the 3gpp-MAC scheme", WCC 2001, pp. 319~328, January 2001.

〔10〕 3G TS 35.202 "Specification of the 3GPP confidentiality and integrity algorithm: Document 2: Kasumi algorithm specifications".

〔11〕 M. Bellare, J. Kilian, and P. R. Rogaway, "The security of cipher block chaining", in Advances in Cryptology, Proc. Crypto '94, Lecture Notes in Computer Science, 839, New York: Springer-Verlag, pp. 341~358, 1994.

〔12〕 E. Petrank and C. Rackoff, "CBC MAC for Real-Time Data Sources", J. Cryptology, pp. 315~338, 2000.

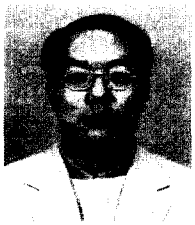
〈著者紹介〉



홍 도 원(Dowon Hong)
1994년 2월 : 고려대학교 이과대학 수학과(학사)
1996년 2월 : 고려대학교 수학과(석사)
2000년 2월 : 고려대학교 수학과(박사)
2000년 4월~현재 : 한국전자통신연구원 선임연구원
관심분야: 정보보호 이론, 이동통신 정보보호

신 상 욱(Sang Uk Shin)
1995년 2월 : 부산수산대학교(현 부경대학교) 전자계산학과 (학사)
1997년 2월 : 부경대학교 전자계산학과(석사)
2000년 2월 : 부경대학교 전자계산학과(박사)
2000년 4월~현재 : 한국전자통신연구원 선임연구원
관심분야 : 정보보호론, 컴퓨터 보안

강 주 성(Ju-Sung Kang)
1989년 2월 : 고려대학교 이과대학 수학과(학사)
1991년 2월 : 고려대학교 수학과(석사)
1996년 2월 : 고려대학교 수학과(박사)
1997년 12월~현재 : 한국전자통신연구원 선임연구원
관심분야: 암호 이론



이 옥 연(Okyeon Yi)
1988년 2월 : 고려대학교 이과대학 수학과(학사)
1990년 2월 : 고려대학교 수학과(석사)
1996년 8월 : University of Kentucky(박사)
1999년 7월~현재 : 한국전자통신연구원 선임연구원
관심분야: 이동통신 정보보호, 컴퓨터 보안