3GPP-MAC 알고리즘에 대한 Concrete Security

성재철*, 이상진*, 임종인*, 홍도원**

*고려대학교, 정보보호기술연구센터

*한국전자통신연구원, 정보보호기술연구본부

Concrete Security of the 3GPP-MAC Algorithm

Jaechul Sung*, Sangjin Lee*, Jongin Lim*, and Dowon Hong**

*Center for Information Security Technologies, Korea Univ.

**Information Security Technology Division, ETRI

요 약

블록 암호 알고리즘과 블록 암호의 운영모드 및 메시지 인증 알고리즘에 대한 의사 난수성의 증명은 근래의 암호 분석에서 구조적인 안전성을 증명을 위한 기법으로 커다란 안전성의 평가 방법으로 자리 매김하고 있다. 본 논문에서는 비동기식(W-CDMA) 3세대 이동통신 3GPP에서의 MAC 알고리즘의 안전성을 의사 난수성에 기반한 concrete security 관점에서의 안전성에 대해 알아본다. 즉, 3GPP-MAC 알고리즘의 구조적인 안전성에 대한 증명을 다룬다.

I. 서론

블록 암호 알고리즘을 이용하여 메시지 인증 코드(MAC)를 설계하는 여러 가지의 방법이 제기되어 왔다. 이 중 Cipher Block Chaining(CBC) 모드를 이용한 CBC-MAC이 가장 널리 상용되어 지고 있다. 국제 표준 ISO/IEC 9797-1에서도 CBC-MAC과 그 변형된 형태로 6 가지의 알고리즘이 제시되어 있다. 3GPP-MAC 알고리즘으로 제시된 f_9 함수는 CBC-MAC을 약간 변형시켜 사용하고 있다[6, 9].

의사 난수성을 이용한 concrete security 관점에서의 안전성에 대한 평가는 최근 블록 암호를 이용한 대칭 키 암호 알고리즘에서 중요한 안전성 평가 방법으로 여겨지고 있다[1, 3, 7]. 블록 암호 자체에 대한 의사 난수성의 증명 뿐 아니라 블록 암호를 이용한 모드에 대한 안전성과 MAC에 대한 의사 난수성을 증명하는 것은 그 알고리즘의 전체적인 구조에 대한 안전성을 제시할 수 있다는 데 큰 의미가 있다.

CBC-MAC은 가변 길이에 대한 안전성을 제시하지는 못한다. 즉, 길이를 변화하는 메시지에 대한 위장 공격에 취약하다. Bellare et al.은 고정된 길이에 대한 CBC-MAC에 대한 의사 난수성을 증명하였다[2]. 그들의 논문에서는 가변 길이에 대한 안전성을 제시하지는 못하였다. 그 후 E.Petrank와 C.Rackoff는 CBC-MAC을 약간 변형시킨 EMAC 알고리즘에서 가변 길이에 대한 의사 난수성을 증명하였다[8].

MAC 알고리즘의 안전성의 평가 방법으로는 위장 공격 및 키 탐색 공격에 대한 안전성과 의사 난수성에 기반한 안전성으로 나뉠 수 있다. 3GPP-MAC에 대한 위장 공격 및 키 탐색 공격에 대한 안전성은 이미 분석되었다[5]. 본 논문에서는 3GPP-MAC 알고리즘에 대해 가변 길이에 대한 concrete security 관점에서의 의사 난수성을 증명한다. 우선 3GPP-MAC 알고리즘에 대해 소개한 후 concrete security 관점에서의 의사 난수성의 개념을 소개한다. 다음으로 3GPP-MAC 알고리즘의 의사 난수성을 증명한다.

II. 3GPP-MAC 알고리즘

CBC-MAC 알고리즘은 하나의 키를 이용하여 Cipher Block Chaining 모드에서의 마지막 출력의 값을 메시지에 대한 인증 코드로 사용한다. 여기서 마지막 출력의 값 중 특정 비트 부분만을 잘라내어 사용하기도 한다. 메시지의 블록 길이가 t 개라고 가정하면 t 번의 블록 암호를 이용한 암호화 과정으로 MAC 값을 얻을 수 있다.

3GPP-MAC 알고리즘은 CBC-MAC 알고리즘을 변형하여 만든 것이다. 우선 사용자는 하나의 키 K를 이용하여 고정된 상수 C를 이용하여 $K' = K \oplus C$의 값을 얻는다. 이 두 개의 키 중 K를 이용하여 CBC-MAC 값을 계산하고, 이 계산 과정에서 피드백 되는 중간 출력의 값을 모두 exclusive-or한 값을 K로부터 유도된 키 K'를 이용하여 한 번 더 암호화하여 값 중 왼쪽 m-비트를 최종 MAC 값으로 사용한다. 그림 1은 3GPP-MAC 알고리즘을 도식화 한 것이다.

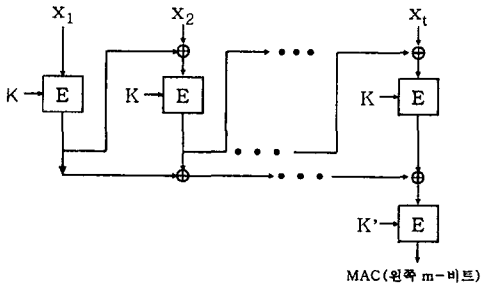

그림 1 : 3GPP-MAC 알고리즘

CBC-MAC 알고리즘은 고정된 길이, 다시 말해 평문의 길이가 s개로만 이루어 졌을 때의 안전성은 Bellare et al.에 의해 증명되었다[2]. 하지만 가변 길이에 대해서는 쉽게 위장 공격이 가능하다. 우선 공격자는 평문 0에 대한 MAC 값 α를 획득한다. 그러면 다음 평문을 $(0, \alpha)$로 놓으면 이 것에 대한 MAC 값은 α가 됨을 쉽게 알 수 있다. 이는 CBC-MAC은 가변 길이에 대해서는 안전성을 제시하지 못함을 의미한다.

가변 길이에 대한 CBC-MAC 알고리즘의 불안전성을 극복하고자 만들어 진 것이 CBC-MAC을 약간 변형시킨 EMAC 알고리즘이다[8]. 이 알고리즘은 우리가 다루고자 하는 3GPP-MAC 알고리즘은 비슷한 구조를 지니고 있다. 하지만 차이점은 피드 백 되는 모든 H_i의 값들을 XOR하여 한 번 더 암호화하는 것이 3GPP-MAC이고, EMAC 알고리즘에서는 CBC-MAC의 출력 값만을 가지고 한 번 더 암호화하는 것이다.

III. Concrete Security의 개념 정의

블록 암호 알고리즘에 대한 의사 난수성의 증명은 Luby와 Rackoff에 의해 시작되었다[7]. 그들은 Feistel 구조에서 각 라운드 함수가 의사 난수 함수라면 3 라운드 이상의 Feistel 구조의 블록 암호 알고리즘은 의사 난수 순열임을 증명함으로써 대칭 키 암호 알고리즘의 안전성의 증명에 큰 업적을 이룩하였다. 이 후 블록 암호 알고리즘에 대한 의사 난수성의 연구가 활발히 진행되어 졌고, 1994년 Bellare et al.은 블록 암호 알고리즘을 의사 난수성을 가정하여 고정 길이의 CBC-MAC의 의사 난수성을 증명하였다.

1997년 Bellare et al.은 4 가지의 안전성의 모델을 제시하여 이를 이용하여 XOR, CTR, CBC 모드에 대한 구체적인 안전성의 상한을 제시한다[1]. 이 방법을 그들은 의사 난수성에 기반한 concrete security라고 하였다. 본 절에서는 이 Bellare의 방법으로 가변 길이의 3GPP-MAC 알고리즘에 대한 안전성을 information-theoretical 관점에서 증명한다.

3GPP-MAC 알고리즘에서 기반이 되는 블록 암호 알고리즘으로 64-비트 암호 알고리즘인 KASUMI를 사용한다. KASUMI에 대한 의산 난수성은 J.S.Kang et al.에 의해 이미 증명되었다[4]. 따라서 우리는 기반이 되는 블록 암호 알고리즘의 의사 난수성을 자연스럽게 가정할 수 있다. 하지만 보다 일반적인 3GPP-MAC 알고리즘에 대한 concrete security 관점에서의 안전성을 증명하고자 한다. 이를 위해 우선 기반이 되는 블록 암호 알고리즘을 l-비트에서 l-비트로 가는 함수들의 모임을 F로 놓는다. 또한 $R^{l \to l}$을 l-비트에서 l-비트로 가는 모든 함수의 집합으로 하고 $R^{l^* \to l}$를 임의의 길이의 $\{0,1\}^{l^*}$에서 l-비트로 가는 모든 함수의 집합이라고 한다.

3CBC-MAC에서 키를 선택하는 것은 기반이 되는 블록 암호 알고리즘의 키가 되는 것이다. 이 과정은 l-비트에서 l-비트로 가는 하나의 함수를 선택하는 과정으로 볼 수 있다. 마찬가지로 3GPP-MAC 알고리즘에서도 하나의 키 K를 선택하고 이를 이용하여 K'를 생성한다. 이는 l-

비트에서 l-비트로 가는 두 개의 함수를 선택하는 것으로 볼 수 있다. 본 논문에서는 두 개의 키가 서로 독립이라는 가정 하에 이론을 전개한다. 또한 마지막 MAC의 값을 m-비트($l \le m$) 만을 취하는 것이 아닌 모든 l-비트를 MAC 값으로 선택하였을 때의 의사 난수성을 살펴본다. 모든 l-비트에 대한 의사 난수성을 증명하면 m-비트를 취하는 MAC에 대한 의사 난수성은 자연히 유도된다.

함수 $f_1^{(t)}(x_1 x_2 \cdots x_t)$를 다음과 같이 정의한다.

$$f_1^{(t)} = f_1(f_1(\cdots f_1(f_1(x_1) \oplus x_2) \oplus \cdots x_{t-1}) \oplus x_t).$$

또한 $f_1^{*}(x_1 x_2 \cdots x_t)$를 다음과 같이 정의한다.

$$f_1^{*} = f_1^{(1)}(x_1) \oplus \cdots \oplus f_1^{(m)}(x_1 x_2 \cdots x_t).$$

다음은 CBC-MAC과 3GPP-MAC을 수식화하여 나타낸 것이다.

- $CBC-MAC_{f_1}(x_1 \cdots x_t) = f_1^{(t)}(x_1 \cdots x_t)$
- $3GPP-MAC_{f_1,f_2}(x_1 \cdots x_t) = f_2(f_1^{*}(x_1 \cdots x_t))$

함수의 집합 F에서 임의의 함수를 랜덤 하게 선택됨을 $f \leftarrow F$로 표시하고 , 두 함수의 집합 F와 F'에 대한 거리의 개념을 다음과 같이 정의한다.

[정의 1] 두 함수의 집합 F와 F'를 임의의 정의역 D에서 치역 R로 가는 함수들의 집합이라고 하고 A를 두 함수들의 집합을 구분하는 임의의 distinguisher(공격자)라 하자. 그러면 A에 대한 advantage는 다음과 같이 정의한다.

$$Adv_{F,F'}^{dist} = \Pr[f \leftarrow F : A^f = 1] - \Pr[f \leftarrow F' : A^f = 1].$$

A의 오라클 query의 수가 최대한 q개일 때 두 함수들의 집합에 대한 advantage는 다음과 같이 정의한다.

$$Adv_{F,F'}^{dist}(q) = \max_A \{Adv_{F,F'}^{dist}(A)\}.$$

위의 정의를 이용하면 l-비트에서 L-비트로 가는 함수들의 집합 F와 $R^{l \mapsto L}$과의 advantage는 다음과 같이 정의할 수 있다.

[정의 2] 두 l-비트에서 L-비트로 가는 함수들의 집합 F와 $R^{l \mapsto L}$에 대한 거리를 prf로 놓고 임의의 distinguisher A에 대한 advantage는 다음과 같이 정의한다.

$$Adv_{F,F'}^{prf} = \Pr[f \leftarrow F : A^f = 1] - \Pr[f \leftarrow F' : A^f = 1].$$

A의 오라클 query의 수가 최대한 q개일 때 두 함수들의 집합에 대한 advantage는 다음과 같이 정의한다.

$$Adv_{F,F'}^{prf}(q) = \max_A \{Adv_{F,F'}^{prf}(A)\}.$$

의사 난수 순열에 대한 advantage의 값은 $R^{l \mapsto L}$을 랜덤 순열 $P^{l \mapsto l}$로 대치하고, prf를 prp로 대치하면 쉽게 위의 정의와 같게 정의할 수 있다. 블록 암호 알고리즘을 이용한 모드 기법에 대한 의사 난수성의 증명은 랜덤 함수와의 거리를 재는 Adv^{prf}의 상한 값을 제시하는 것이다.

MAC 알고리즘에 대한 의사 난수성의 증명을 위해서는 mac 관점에서의 안전성의 정의가 필요하다. MAC 알고리즘의 기본적인 안전성은 위장 공격에 대한 안전성이다. 이에 대한 정의는 다음과 같다.

[정의 3] 임의의 메시지 인증 코드 알고리즘을 MAC이라고 하고 A를 임의의 위장 공격자하고 하고 MAC 알고리즘에 대한 위장 공격(forgery attack)이 성공하였을 때 1의 값을 낸다고 가정하자. 그러면 A에 대한 성공 확률은 다음과 같이 정의한다.

$$Adv_{MAC}^{mac}(A) = \Pr[Forge(MAC, A) = 1].$$

A의 오라클 query의 수가 최대한 q개일 때 advantage는 다음과 같이 정의한다.

$$Adv_{MAC}^{mac}(q) = \max_A \{Adv_{MAC}^{mac}(A)\}.$$

MAC 알고리즘에 대한 안전성을 직접 mac에 대한 advantage를 이용하여 concrete security 관점에서 정확히 측정하는 것은 어려운 문제이다. 하지만 prf 관점에서의 안전성과의 관계식을 나타내는 다음의 정리를 이용하여 mac 관점에서의 안전성 증명을 prf 관점에서의 안전성의 증명으로 바꿀 수 있게 된다.

[보조 정리 1] MAC을 l-비트 길이의 내는 임의의 메시지 인증 코드 알고리즘이라고 하고, q를 오라클 query의 수라고 가정하면 다음의 식이 성립한다.

$$Adv_{MAC}^{mac}(q) \le Adv_{MAC}^{prf}(q) + \frac{1}{2^l}.$$

위의 증명은 논문 [2]에 나타나 있다. 위의 정리는 mac의 안전성의 증명을 prf에서의 안전성의 증명으로 전환할 수 있음을 의미한다. 따라서 우리는 3GPP-MAC 알고리즘의 mac에 대한 안전성을 prf 관점에서의 의사 난수성에 대한 안전성으로 전환할 수 있게 된다. 그러므로 다음 장에서는 3GPP-MAC 알고리즘의 의사 난수성을 prf 관점에서의 concrete security의 증명을 살펴본다.

IV. 3GPP-MAC의 의사 난수성

우리는 3GPP-MAC 알고리즘에 대한 mac 관점에서의 안전성을 살펴보기 위해 거리의 개념을 도입하였다. 그리고 mac 관점에서의 안전성의 증명은 prf 관점에서의 안전성의 증명을 이용하여 그 상한을 얻을 수 있음을 알아냈다. 본 절에서는 3GPP-MAC에 대한 안전성의 상한을 증명하여 본다.

우선 3GPP-MAC 알고리즘에서 근간이 되는 블록 암호 알고리즘을 함수들의 집합 F라 가정하고 이 함수들의 집합 F가 의사 난수성을 만족한다고 한다고 가정하자. 그러면 본 논문의 핵심이 되는 다음의 정리가 성립한다.

[정리 1] (3GPP-MAC의 안전성) F를 $R^{l\mapsto l}$의 부분 집합이라고 하고 임의의 q개의 오라클 query를 $X_1,\cdots,X_q$ 라 하자. 그러면 3GPP-MAC 알고리즘은 mac 관점에서의 의사 난수성을 만족하고, 이에 대한 concrete security는 다음과 같다. 여기서 $p=\sum_{i=1}^{q}|X_i|$이다.

$$Adv^{MAC}_{3GPP-MAC}(q) \le 2\cdot Adv^{prf}_{F}(p)+\frac{2p^2+1}{2^l}.$$

우선 3GPP-MAC 알고리즘의 정의를 다시 한번 살펴보자.

$$3GPP-MAC_{f_1,f_2}(x_1\cdots x_t)=f_2(f_1^*(x_1\cdots x_t)).$$

여기서 함수 f_1과 f_2는 함수들의 집합 F에서 임의로 선택되어 진다. 먼저, 우리는 함수 f_1과 f_2가 랜덤 함수의 집합 $R^{l\mapsto l}$에서 선택되어 졌을 때의 advantage 값을 살펴보자. 이 advantage의 값의 상한을 이용하면 3GPP-MAC의 알고리즘은 쉽게 증명이 된다. 다음의 정리는 f_1과 f_2가 $R^{l\mapsto l}$에서 선택되었을 때 prf 관점에서의 concrete security의 상한을 나타낸 것이다.

[정리 2] (랜덤 함수 모델에서의 3GPP-MAC의 안전성) A를 $3GPP-MAC^{R^{l\mapsto l},R^{l\mapsto l}}$또는 $R^{l\to l}$에 대하여 임의의 q개의 오라클 query $X_1,\cdots,X_q$를 만드는 확률론적 오라클 튜링 머시인 이라고 가정하자. 그러면 A에 대한 advantage는 다음과 같다. 여기서 $p=\sum_{i=1}^{q}|X_i|$이다.

$$Adv^{dist}_{3GPP-MAC^{R^{l\mapsto l},R^{l\mapsto l}},\ R^{l\to l}}(q) \le \frac{2p^2}{2^l}.$$

(증명) 다음에 나오는 보조 정리 4를 이용하면 쉽게 증명된다. ■

우리는 정리 1의 증명을 위해서 몇 가지의 정의를 도입하고, 이를 이용하여 필요한 보조 정리들을 증명할 것이다. 우리의 증명은 information-theoretical 모델에서의 안전성을 고려하므로, 공격자 A의 계산 능력은 무한하다고 가정한다.

공격자 A가 어떤 메시지 $X=(x_1,x_2,\cdots,x_t)$에 대한 query를 생성할 때, A는 X에 대한 MAC 값 뿐 아니라 이 메시지에 대한 모든 non-empty prefix들에 대한 query(이것을 subquery라 정의한다)들에 대한 값을 모두 획득할 수 있다고 가정한다. 다시 말해 $f_2(f_1^*(x_1)), f_2(f_1^*(x_1x_2)),\cdots, f_2(f_1^*(x_1x_2\cdots x_t))$에 대한 값을 획득함을 의미한다. 또한 q개의 메시지 $X_1,\cdots,X_q$에 대한 모든 가능한 서로 다른 subquery들을 distinct subquery라 정의한다. 이들 이용하여 collision을 다음과 같이 정의한다.

[정의 4] $X_1,\cdots,X_q$를 $\{0,1\}^{l^*}$에서의 q개의 메시지라고 가정하고 함수 f_1과 f_2를 랜덤 함수의 집합 $R^{l\mapsto l}$에 속하는 임의의 두 함수라고 가정하자. 그러면 이 중 임의의 서로 다른 메시지 X_i와 X_j에 대한 3GPP-MAC 값이 같을 때 collision이 발생하였다고 정의하고, 이 중 f_2 함수의 입력 전의 값들, $f_1^*(X_i)(1\le i\le q)$의 값에 대해 같은 값이 발생하였을 때를 inner-collision이라 정의한다. 또한 collision(inner collision)이 발생하지 않았을 경우를 collision-free(inner collision-free)라 정의한다.

q개의 query들 $X_1,\cdots,X_q$에 대한 distinct subquery를 $Y_1,\cdots,Y_m$이라고 놓고, $\beta_1,\cdots,\beta_m$을 서로 다른 l-비트라고 놓자. 그리고 다음의 서로 다른 MAC의 값이 발생하는 경우를 D라고 정의하자.

$$D\equiv\{3GPP-MAC_{f_1,f_2}(Y_j)=\beta_i,\forall\, j=1,\cdots,m\}$$

그러면 임의의 함수 $g(\in R^{l\mapsto l})$에 대해, 다음의 확률 분포는 균일하게 된다.

$$\Pr_{f_1,f_2}[f_1=g \mid D].$$

이를 이용하면 다음의 결과를 쉽게 얻을 수 있다.

[보조 정리 2] $X_1,\cdots,X_q(\in\{0,1\}^{l^*})$에 대한 서로 다른 subquery들을 $Y_1,\cdots,Y_m$라 놓고, $\beta_1,\cdots,\beta_m$을 서로 다른 l-비트라고 가정하자. 그리고 f_1과 f_2는 $\{0,1\}^l$에서 균등하게 선택되도록 분포되어 있다고 가정한다. 그러면 $m^2/4+m-1\le 2^{l/2}$을 만족하는 임의의 m, l-비트의 값 α와 임의의 서로 다른 i와 k $(1\le i,k\le m)$에 대해 다음의 두 식이 성립한다.

$$\Pr_{f_1,f_2}[f_1^*(Y_i)=\alpha\,|\,D]\le 2\cdot 2^{-l} \quad (1)$$

$$\Pr_{f_1,f_2}[f_1^*(Y_i)\oplus f_1^*(Y_k)=\alpha|D]\le 2\cdot 2^{-l} \quad (2)$$

임의의 query들에 대한 서로 다른 subquery들에 대한 collision이 발생하지 않았을 때, 다음의 정리는 새로운 query들에 대한 collision 발생 확률이 아주 작은 값으로 분포되어 있음을 보인다. 이것은 기존 query들에 대한 값에서 충돌이 발생하지 않는다면 새로운 query가 inner-collision이 발생하는 확률은 거의 균등함을 의미한다. 물론 subquery들의 수가 $O(2^{l/2})$보다 작을 때에만 성립한다. 그리고 메시지가 없는 empty string ε에 대한 $f_1^*(\varepsilon)$ 값은 0^l이라고 가정한다.

[보조 정리 3] $X_1,\cdots,X_q(\in\{0,1\}^{l^*})$에 대한 서로 다른 subquery들을 $Y_1,\cdots,Y_m$라 놓고, $\beta_1,\cdots,\beta_m$을 서로 다른 l-비트라고 가정하자. 그리고 f_1과 f_2는 $\{0,1\}^l$에서 균등하게 선택되도록 분포되어 있다고 가정한다. 그러면 $m^2/4+m-1\le 2^{l/2}$을 만족하는 임의의 m, l-비트의 값 w에 대해 다음의 4 가지의 성질이 성립한다.

1. 임의의 서로 다른 j와 $k(1\le j,k\le m)$에 대해, $Y_j\ne Y_k\omega$이면, 다음이 식이 성립한다.

$$\Pr_{f_1,f_2}[f_1^*(Y_j)=f_1^*(Y_k w)|D]\le 3\cdot 2^{-l} \quad (3)$$

2. 임의의 $j(1\le j\le m)$에 대해, $Y_j\ne\omega$이면, 다음이 식이 성립한다.

$$\Pr_{f_1,f_2}[f_1^*(Y_j)=f_1^*(w)|D]\le 3\cdot 2^{-l} \quad (4)$$

3. 모든 $j(1\le j\le m)$에 대해 $f_1^*(Y_j)\ne 0^l$이면, 다음이 식이 성립한다.

$$\Pr_{f_1,f_2}[f_1^*(Y_j)=0^l\,|\,D]\le 2^{-l} \quad (5)$$

4. 모든 $j(1\le j\le m)$에 대해 $f_1^*(Y_j)\ne 0^l$이면, 임의의 다음이 $k(1\le k\le m)$에 대해 다음의 식이 성립한다.

$$\Pr_{f_1,f_2}[f_1^*(Y_k w)=0^l\,|\,D]\le 2^{-l} \quad (6)$$

(증명) 증명 생략. ■

위의 보조 정리 3은 inner collision-free의 경우 랜덤 함수와 차이가 거의 없음을 의미한다. 다음의 결과는 위의 보조 정리 3과 생일 역설을 이용하여 얻은 정리이다.

[보조 정리 4] $X_1,\cdots,X_q(\in\{0,1\}^{l^*})$에 대한 서로 다른 subquery들을 $Y_1,\cdots,Y_m$라 놓고, f_1과 f_2는 $\{0,1\}^l$에서 균등하게 선택되도록 분포되어 있다고 가정한다. 또한 m이 $m^2/4+m-1\le 2^{l/2}$을 만족한다고 가정하자. 그러면 $3GPP-MAC_{f_1,f_2}$에 대한 subquery가 collision이 발생할 확률은 기껏해야 $(\sum_{i=1}^{q}|X_i|)^2\cdot 2\cdot 2^{-l}$이다.

(증명) 우선 i번 째 query에서, subquery $Y_j(j\le i)$를 선택하여 새로운 subquery $Y_i=Y_j w$를 생성할 경우를 살펴보자. X_i들의 값들 중 empty query ε이 없는 경우에는 처음 $i-1$개의 query가 collision이 발생하지 않았을 때, i번 째 query에서 inner-collision이 발생할 확률은 $(i-1)\cdot 3\cdot 2^{-l}$이 된다. X_i들의 값들 중 empty query가 있는 경우에는 i번 째 query에서 inner-collision이 발생할 확률은 $(i-1)\cdot 2^{-l}$ 보다 작거나 같다. 마찬가지로 i번 째 query에서, subquery $Y_j(j\ge i)$를 선택하여 새로운 subquery $Y_i=Y_j w$를 생성할 경우에도 i번 째 inner-collision이 발생할 확률은 $(i-1)\cdot 3\cdot 2^{-l}$ 보다 작거나 같다

MAC 값에 충돌이 발생하는 경우는 f_2 함수 이전에 충돌이 발생하는 inner collision의 발생 이외에 f_2의 입력이 다르더라도 충돌이 발생하는 경우가 존재한다. 이 경우의 i번 째 충돌 발생 확률은 $(i-1)\cdot 2^{-l}$ 보다 작거나 같게 된다.

따라서 위의 inner-collision 확률의 상한 값과 inner-collision이 아니고도 collision 발생 확률의 상한 값을 더하면 $(i-1)\cdot 4\cdot 2^{-l}$의 값을 얻는다. 따라서 이 값을 1부터 m 까지 모두 더하면 다음과 같은 상한 값을 얻는다.

$$\sum_{i=1}^{m}(i-1)\cdot 4\cdot 2^{-l} = 2\cdot m(m-1)\cdot 2^{-l}$$

여기서 $m \le \sum_{i=1}^{m}|X_i|$ 임으로, collision 발생 확률은 $(\sum_{i=1}^{q}|X_i|)^2\cdot 2\cdot 2^{-l}$ 보다 작거나 같게 된다. ■

보조 정리 4를 이용하면 쉽게 정리 2를 증명할 수 있다. 정리 2의 랜덤 함수 모델에서의 3GPP-MAC의 의사 난수성의 정리를 이용하여 3GPP-MAC의 안전성을 다음과 같이 증명한다.

(정리 1의 증명)

$Adv^{MAC}_{3GPP-MAC}(q)$ 의 값은 f_1과 f_2를 $\{0,1\}^l$에서 균등하게 선택된 것이 아닌 함수의 집합 F에서 선택된 함수들이다. 따라서 $Adv^{MAC}_{3GPP-MAC}(q)$를 자세히 표현하면 $Adv^{MAC}_{3GPP-MAC^{F,F}}(q)$ 이다. 이를 우선 보조 정리 1을 이용하여 mac의 advantage를 prf의 advantage로 전환하면 다음의 식을 얻는다.

$$Adv^{MAC}_{3GPP-MAC}(q) \le Adv^{dist}_{3GPP-MAC^{F,F},R^{l\to l}}(p) + \frac{1}{2^l}$$

이를 삼각 부등식과 정리 2를 순차적으로 정리하면 다음과 같이 정리 1의 증명이 완성된다.

$$\begin{aligned} Adv^{MAC}_{3GPP-MAC}(q) &\le Adv^{dist}_{3GPP-MAC^{F,F},R^{l\to l}}(p) + \frac{1}{2^l} \\ &\le Adv^{dist}_{3GPP-MAC^{F,F},3GPP-MAC^{F,R'^{\to}}}(p) \\ &+ Adv^{dist}_{3GPP-MAC^{F,R'^{\to}},3GPP-MAC^{R'^{\to},R'^{\to}}}(p) \\ &+ Adv^{dist}_{3GPP-MAC^{R'^{\to},R'^{\to}},R^{l\to l}}(p) + \frac{1}{2^l} \\ &\le 2\cdot Adv^{prf}_{F}(p) + \frac{2p^2}{2^l} + \frac{1}{2^l}\ . \ ■ \end{aligned}$$

지금까지 우리는 3GPP-MAC 알고리즘의 concrete security 관점에서의 안전성을 살펴보았다. CBC-MAC 알고리즘보다 한 번의 암호화 연산을 더하는 3GPP-MAC 알고리즘은 가변길이에 대해서 안전성을 제공하지 못하는 CBC-MAC과 달리, 가변 길이에 대한 의사 난수성을 제공하고 있다. 이는 3GPP-MAC 알고리즘에 대한 구조적인 취약성이 없음을 의미하고, 3GPP-MAC 알고리즘에 사용되는 KASUMI 알고리즘의 의사 난수성도 이미 증명되었으므로, 3GPP-MAC 또한 안전하게 사용될 수 있음을 의미한다.

V. 결론

의사 난수성에 대한 안전성의 증명 방법은 다른 어떠한 공격 방법에 대한 안전성의 증명 방법보다 뛰어나다. 이는 어떠한 알고리즘에 대해 의사 난수성을 증명한다면 다른 어떠한 실제적인 공격에 대한 안전성을 제시할 수 있다.

본 논문에는 3GPP-MAC 알고리즘에 대한 concrete security 관점에서의 안전성을 증명하였다. 이는 3GPP-MAC 알고리즘의 구조적인 안전성을 제시할 뿐 아니라 선택 평문 공격에서의 어떠한 실제적인 공격(예 : 위장 공격)들에 대해서도 안전함을 동시에 내포하고 있는 것이다.

참고문헌

[1] M. Bellare, A. Desai, E. JokiPii, and P. Rogaway, "A Concrete Security Treatment of Symmetric Encryption : Analysis of the DES Modes of Operation", Proceedings of the 38th Symposium on Foundations of Computer Science, IEEE, 1997.

[2] M. Bellare, J. Kilian, and P. Rogaway, "The Security of the Cipher Block Chaining Message Authentication Code", Advanced in Cryptology - CRYPTO'94, LNCS 839, pp. 341-358, Springer-Verlag, 1994.

[3] S. Goldwasser and S. Micali, "Probabilistic Encryption", Journal of Computer and System Sciences, Vol.28, pp. 270-279, April 1984.

[4] J. S. Kang, O. Y. Yi, D. W. Hong, and H. S. Cho, "Pseudorandomness of MISTY-type transformations and the block cipher KASUMI", ACISP 2001, LNCS 2119, pp. 205-318, Springer-Verlag, 2001.

[5] L. R. Knudsen and C. J. Mitchell, "An analysis of the 3gpp-MAC scheme", WCC 2001, pp. 319-328, 2001.

[6] ISO/IEC 9797-1, "Information technology-Security techniques-Message Authentication Codes (MACs)-Part I : Mechanisms using a block cipher", International Organization for Standardization, Genève, Swizerland, 1999.

[7] M. Luby and C. Rackoff, "How to construct pseudorandom permutations from pseudorandom functions", SIAM J. Comput., vol. 17, pp. 373-386, 1988.

[8] E. Petrank and C. Rackoff, "CBC-MAC for Real-Time Data Sources", Journal of Cryptology, Vol. 13, pp. 315-338, 2000.

[9] 3G TS 35.201, "Specification of the 3GPP confidentiality and integrity algorihm : Document 1 : f8 and f9 specification".