情報保護學會論文誌
第11券 第4號, 2001. 8

OFB 모드와 3GPP f8 암호화 모드의 안전성

신 상 욱*, 홍 도 원*, 강 주 성*, 이 옥 연*

Security of OFB mode and 3GPP f8 encryption mode

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

요 약

본 논문에서는 블록 암호의 기본적인 동작 모드 중의 하나인 OFB 암호화 모드와 비동기식 IMT-2000의 무선 구간 메시지 암호화를 위해 사용되는 3GPP f8 암호화 모드의 안전성을 분석한다. Left-or-right 안전성 개념을 적용하여 각각 랜덤 함수 모델과 랜덤 치환 모델에서의 안전성에 대한 하한과 상한을 증명하고, 또한 유사랜덤 함수 모델과 유사 랜덤 치환 모델에서의 안전성을 각각 증명한다.

ABSTRACT

In this paper, we analyze the security of OFB encryption mode which is one of the basic modes of operation for the block cipher and the security of 3GPP f8 encryption mode used to provide the data confidentiality over a radio access link of W-CDMA IMT-2000. We provide the lower bound and the upper bound on security of both modes in random function model and random permutation model, respectively, by means of the left-or-right security notion, and prove the security of both modes using a pseudorandom function and a pseudorandom permutation, respectively.

keyword : *mode of operation, OFB, 3GPP f8, Left-or-right security*

Ⅰ. 서 론

대칭키 블록 암호는 암호 시스템에서 가장 빈번하게 사용되는 암호 프리미티브 중의 하나이다. 기본적으로 블록 암호는 통신로 상에서 허가되지 않은 제3자에 의해 메시지 내용이 도청되는 것을 방지하기 위해 사용된다. 블록 암호는 스트림 암호, 메시지 인증 코드(message authentication code : MAC), 해쉬 함수 등과 같은 다양한 암호 프리미티브들을 구성하기 위해 사용될 수도 있다. 블록 암호는 l-비트 평문 블록을 l-비트 암호문 블록으로 사상시키는 함수이고, 특정한 길이의 키 k를 파라메터로 가진다. 한 블록 이상의 평문을 암호화하고 다양한 응용 환경을 만족시키기 위해 블록 암호에 대한 여러 가지 동작 모드(mode of operation)가 제안되어졌다. 현재 표준화된 동작 모드로 ECB(electronic codebook), CBC(cipher block chaining), CFB(cipher feedback), OFB(output feedback) 모드가 알려져 있다[6]. 또한 비동기식(W-CDMA) 3세대 이동통신 진영의 3GPP(3rd generation partnership project)에서도 무선 구간의 메시지 기밀성을 보장하기 위해 블록 암호 KASUMI에 기반한 f8 암호화 기법을 제안하였는데, 이는 OFB 모드의 변형된 형태로 볼 수 있다[1].

동작 모드의 안전성 증명은 1994년 Bellare-Kilian-Rogaway에 의해 CBC MAC 모드의 안전성 분석으로부터 시작되었고[4], 1997년 Bellare-Desai-Jokipii-Rogaway가 처음으로 암호화 모드의 안전성

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

개념을 소개하고 CTR(counter) 모드와 CBC 암호화 모드의 안전성을 증명하였다[3]. 최근에 Alkassar-Geralay-Pfitzmann-Sadeghi은 CFB 모드의 안전성을 분석하고 CFB 모드의 성능을 개선한 OCFB (optimized cipher feedback) 모드를 제안하고 그 안전성을 분석하였다[2]. 블록 암호에 기반한 동작 모드에 관한 최근의 연구는 MAC 모드에 관한 안전성[5,11] 및 무결성과 기밀성을 결합한 모드의 안전성[7,9,12]에 관해 주로 진행되고 있다.

본 논문에서는 기반이 되는 블록 암호가 안전하다면 OFB 암호화 모드와 3GPP f8 암호화 모드가 안전하다는 것을 보인다. 먼저 암호화 모드의 안전성 개념을 간단히 기술한 후, 블록 암호의 기본적인 동작 모드 중의 하나인 OFB 암호화 모드와 비동기식 IMT-2000의 무선 구간 메시지 암호화를 위해 사용되는 3GPP f8 암호화 모드의 안전성을 분석한다. Bellare-Desai-Jokipii-Regaway[3]이 처음 사용한 left-or-right 안전성 개념을 적용하여 두 가지 암호화 모드의 안전성에 대한 하한과 상한을 각각 랜덤 함수 모델과 랜덤 치환 모델에서 증명하고, 또한 유사랜덤 함수 모델과 유사랜덤 치환 모델에서의 안전성을 각각 증명한다.

Ⅱ. 암호화 모드의 안전성 개념

2.1 표기

$A(\cdot,\cdot,\cdots)$가 확률적 알고리즘이면, $a \leftarrow A(x_1, x_2, \cdots)$는 입력 $x_1, x_2, \cdots$에 대해 A를 수행하여 a를 출력하는 실행을 나타낸다. 만약 A가 집합이면, $a \xleftarrow{R} A$는 A로부터 균등하게 한 점을 선택하여 결과를 a에 할당하는 실험을 나타낸다.

먼저 엄밀하게 대칭 암호 기법(symmetric encryption scheme)을 다음과 같이 정의한다.

[정의 1]

대칭 암호 기법은 아래와 같은 $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ 세 알고리즘으로 구성된다.

- 키 생성 알고리즘 $\mathcal{K}$: 키를 출력하는 확률적 알고리즘:
  $K \xleftarrow{R} \mathcal{K}$
- 암호화 알고리즘 $\mathcal{E}$: 키 K와 평문 M을 입력하여 암호문 C를 출력하는 확률적 알고리즘:
  $C \xleftarrow{R} \mathcal{E}\mathrm{K}(M)$
- 복호화 알고리즘 $\mathcal{D}$: 키 K와 암호문 C를 입력하여 대응하는 평문 M을 출력하는 결정적 알고리즘:
  $M \leftarrow \mathrm{DK}(C)$

여기서 메시지 M은 메시지 집합 $MS \subseteq \{0,1\}^*$에서 선택된다.

대칭 암호 기법의 안전성을 분석하기 위해서는 Goldreich-Goldwasser-Micali[8]에 의해 소개되어 Bellare-Kilian-Rogaway[4]이 CBC MAC의 안전성 증명에 이용한 유사랜덤 함수라는 개념이 필요하다. 함수 패밀리(function family)는 사상 $F: K(F) \times D(F) \rightarrow R(F)$이다. 여기서 $K(F)$는 F의 키 공간, $D(F)$는 F의 정의역, $R(F)$는 F의 치역이다. 각 키 $k \in K(F)$에 대해 사상 $F_k: D(F) \rightarrow R(F)$은 $F_k(x) = F(k, x)$, $\forall x \in D(F)$로 정의한다. 따라서 F는 $D(F)$에서 $R(F)$로 가는 함수들의 집합이다. $f \xleftarrow{R} F$는 랜덤한 $a \xleftarrow{R} K(F)$를 뽑아 $f \leftarrow F_a$를 할당하는 연산을 나타낸다. $R_{l,L}$을 l-비트 스트링의 집합에서 L-비트 스트링의 집합으로 가는 모든 함수들의 집합을 나타내고, $f \xleftarrow{R} R_{l,L}$는 l-비트에서 L-비트로의 함수를 랜덤하게 선택하는 연산이다. 유사하게, P_l을 l-비트 스트링에서 모든 치환(permutation)들로 구성된 함수 패밀리라고 하면, $f \xleftarrow{R} P_l$는 l-비트 스트링의 치환을 랜덤하게 선택하는 연산을 나타낸다.

F와 G를 같은 길이의 입력과 출력을 가진 함수 패밀리라고 하자. F와 G의 구별자(distinguisher)는 오라클(oracle) h에 접근하여 한 비트를 출력하는 공격자 A이다. 구별자의 목적은 오라클 h가 F로부터 랜덤하게 선택되었는지 또는 G에서 랜덤하게 선택되었는지 두 가지 경우를 구별하는 것이다. G로부터 F를 구별할 때 A의 이점(advantage)는 $Adv_A(F, G) = |\Pr_{k,R_F}[A=1] - \Pr_{k,R_G}[A=1]|$로 정의된다. 여기서 $\Pr_{k,R_F}[A=1]$ (또는 $\Pr_{k,R_G}[A=1]$)은 오라클 h가 함수 패밀리 F(또는 G)에서 랜덤하게 선택될 때 A가 1을 출력할 확률이다.

유사랜덤 함수(pseudorandom function : PRF) 패밀리는 키 a를 알지 못하는 사람에게 F_a가 "랜덤"하게 보이는 것이다. 직관적으로 어떤 공격자 A에게도 F와 $R_{l,L}$을 구별할 이점 $Adv_A(F, R_{l,L})$이 충

분히 작으면 함수 패밀리 F를 유사랜덤 함수 패밀리라고 한다. 유사하게 임의의 공격자 A에 대해 $Adv_A(F, P_f)$가 충분히 작으면 함수 패밀리 F를 유사랜덤 치환(pseudorandom permutation : PRP) 패밀리라고 한다.

[정의 2]

$F \subseteq R_{l,l}$ (또는 $F \subseteq P_l$)은 함수 패밀리라고 하자. 기껏해야 q개의 질의(query)를 하고 기껏해야 t 시간동안 수행하는 임의의 구별자 A에 대해 $Adv_A(F, R_{l,l}) \leq \varepsilon$ (또는 $Adv_A(F, P_l) \leq \varepsilon$)이면, 함수 패밀리 F는 $(t, q : \varepsilon)$-안전한(secure) 유사랜덤 함수 패밀리(또는 유사랜덤 치환 패밀리)라고 한다. 그리고, 기껏해야 q개의 질의(query)를 하고 기껏해야 t 시간동안 수행하는 어떤 구별자 A에 대해 $Adv_A(F, R_{l,l}) > \varepsilon$ (또는 $Adv_A(F, P_l) > \varepsilon$) 이면, 함수 패밀리 F는 $(t, q : \varepsilon)$-해독(break)되는 유사랜덤 함수 패밀리(또는 유사랜덤 치환 패밀리)라고 한다.

2.2 암호화 모드의 안전성 개념(security notion)

Bellare-Desai-Jokipii-Rogaway는 대칭키 암호 기법에 대한 안전성으로 4가지 개념을 고려하였다[3]. "Real-or-random indistinguishability"와 그 변형인 "left-or-right indistinguishability"를 새롭게 제안하였고, 비대칭 암호 기법의 개념인 "find-then-guess security"와 "semantic security"를 대칭키 암호화 기법에 적용하였다.

Real-or-random indistinguishability은 다음과 같은 두 가지 다른 게임을 고려한다. 게임 1은 질의된 메시지 x의 암호문을 응답하는 오라클이 주어지고, 게임 2는 질의된 메시지가 아닌 랜덤한 스트링(길이는 질의된 메시지의 길이와 동일하다)의 암호문을 응답하는 오라클이 주어진다. 공격자가 게임 1과 게임 2를 구별할 수 있는 의미있는 이점을 얻을 수 없다면 암호 기법은 real-or-random 개념으로 안전하다.

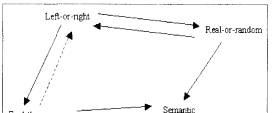
Left-or-right indistinguishability은 뒤의 정의 3에서 기술한다.

Find-then-guess 안전성은 비대칭키 기법의 polynomial security를 대칭키 기법에 적용한 것이다. 공격자는 두 단계(stage)를 가진다. 공격자는 find 단계에서 같은 길이의 메시지 쌍 (x_0, x_1)을 선택하고 상태 정보 s를 유지한다. Guess 단계에서 평문 x_0와 x_1 중의 하나에 대한 랜덤한 암호문 y가 공격자에게 주어진다. 공격자가 y가 어느 평문의 암호문인지를 정확히 구별하는데 의미있는 이점을 얻을 수 없다면 암호 기법은 안전하다.

Semantic security 역시 비대칭키 기법에서의 개념을 대칭키 상황으로 가지온 것이다. 공격자는 select 단계에서 메시지 공간에서 이점이 있는 확률 분포를 선택한다. predict 단계에서 그 분포에 의해 선택된 평문 x의 암호문 y가 공격자에게 주어지면, 공격자는 평문 x에 관한 어떤 함수 $I(x)$를 추측하기 원한다. 공격자가 선택된 분포 상에서 최대 확률보다 더 좋은 확률로 $I(x)$를 추측할 수 없다면, 암호 기법은 함수 I와 확률 분포에 대하여 semantically secure하다고 한다.

Bellare-Desai-Jokipii-Rogaway은 또한 4가지 개념들간의 관계를 보였다[3]. Real-or-random indistinguishability와 left-or-right indistinguishability 각각의 이점들은 서로 작은 상수배 정도 차이가 난다. 즉, 둘 사이에는 안전성이 보존된다. 또한 이 두 가지 개념은 find-then-guess 개념으로 안전성이 보존된다. 하지만 find-then-guess 개념에서 이 두 가지 개념으로는 안전성이 보존되지 않는다. Real-or-random과 semantic 개념은 서로 같은 안전성을 제공한다. [그림 1]은 Bellare 등에 의해 증명된 대칭키 암호 기법의 안전성 개념들간의 내포 관계를 보인다. 그림 1에서 $\rightarrow$은 안전성이 보존되는 관계를 나타내고, $\not\rightarrow$은 안전성이 보존되지 않는 관계를 나타낸다.

본 논문에서는 left-or-right 안전성 개념을 적용하여 OFB 암호화 모드와 3GPP 암호화 알고리즘 f8의 안전성을 분석한다. 앞에서 살펴본 바와 같이 left-or-right 관점에서 안전성 증명은 다른 3가지 개념에서의 안전성을 내포하기 때문이다. left-or-right



[그림 1] 대칭키 암호 기법의 안전성 개념들간의 관계

안전성 관점에서 공격자는 능동적 선택 평문 공격(adaptive chosen plaintext attack)을 수행한다. 공격은 두 가지 다른 게임을 고려한다. 어느 게임이든지 질의(query)는 메시지 공간 MS로부터 같은 길이의 스트링 (x_1, x_2) 쌍으로 이루어진다. 어느 게임이든지 키 공간 KS에서 랜덤한 키 $a \xleftarrow{R} KS$를 선택하고 이 키는 고정된다. 게임 1에서 (x_1, x_2)을 수신한 오라클(oracle)은 $\mathcal{E}_a(x_1)$을 반환하고, 게임 2에서 오라클은 $\mathcal{E}_a(x_2)$을 반환한다. 따라서 게임 1은 왼쪽 오라클을 제공하고 게임 2는 오른쪽 오라클을 제공한다. 공격자가 게임 1과 게임 2를 구별하는데 의미있는 이점을 얻을 수 없다면 암호화 모드는 left-or-right 의미에서 안전하다고 한다.

다음은 left-or-right 의미에서의 안전성 개념에 대한 정의이다.

[정의 3] (left-or-right 안전성)[3]

기껏해야 t의 시간동안 수행하고 많아야 q개의 질의를 하고 질의의 총 길이는 기껏해야 μ 비트인 임의의 공격자 A에 대해 다음의 이점(advantage)을 가진다면, 암호화 기법 $(\mathcal{E}, \mathcal{D}, \mathcal{K})$는 left-or-right 의미에서 $(t, q, \mu; \varepsilon)$-안전하다고 말한다.

$$Adv_A^{lr} \stackrel{\text{def}}{=} \left| \Pr_{a \xleftarrow{R} KS}[A^{\mathcal{E}_a(O(1,(\cdot,\cdot)))} = 1] - \Pr_{a \xleftarrow{R} KS}[A^{\mathcal{E}_a(O(2,(\cdot,\cdot)))} = 1] \right| \leq \varepsilon.$$

그리고, 기껏해야 t의 시간동안 수행하고 많아야 q개의 질의를 하고 질의의 총 길이는 기껏해야 μ 비트인 어떤 공격자 A에 대해, $Adv_A^{lr} > \varepsilon$ 이면, 암호화 기법 $(\mathcal{E}, \mathcal{D}, \mathcal{K})$는 left-or-right 의미에서 $(t, q, \mu; \varepsilon)$-해독된다고 말한다.

여기서, $A^{\mathcal{E}_a(O(1,(\cdot,\cdot)))}$는 질의 (x_1, x_2)에 대한 응답으로 $y \xleftarrow{R} \mathcal{E}_a(x_1)$을 반환하는 오라클 $O(1, (\cdot, \cdot))$을 가진 A를 나타내고, $A^{\mathcal{E}_a(O(2,(\cdot,\cdot)))}$는 질의 (x_1, x_2)에 대한 응답으로 $y \xleftarrow{R} \mathcal{E}_a(x_2)$을 반환하는 오라클 $O(2, (\cdot, \cdot))$을 가진 A를 나타낸다. 그리고 $\Pr_{a \xleftarrow{R} KS}[A^{\mathcal{E}_a(O(i,(\cdot,\cdot)))} = 1]$ $(i = 1, 2)$는 키 a가 키 공간 KS에서 랜덤하게 선택될 때 오라클 $O(i, (\cdot, \cdot))$ $(i = 1, 2)$을 가진 공격자 A가 1을 출력할 확률이다.

Ⅲ. OFB 암호화 모드와 3GPP f8 암호화 모드의 안전성

이 장에서는 위에서 정의한 left-or-right 안전성 개념을 적용하여 OFB 암호화 모드와 3GPP f8 암호화 알고리즘의 안전성을 증명한다. 암호화 모드의 기반이 되는 함수는 입력 길이 l, 출력 길이 l, 키 길이 k을 가진 유사랜덤 함수(pseudo random function : PRF) 패밀리 F로 고정한다. 앞으로 이 논문에서는 유사랜덤 함수 f는 송수신자간에 공유된 비밀키 a가 고정될 때 $f \leftarrow F_a$ 연산을 나타낸다. 먼저 랜덤 함수 모델하에서 left-or-right 의미로 두 암호화 모드를 해독하려고 시도하는 공격자의 성공 확률에 관한 하한과 상한을 유도한 후, 유사랜덤 함수 모델에서 안전성을 증명한다.

3.1 OFB 암호화 모드

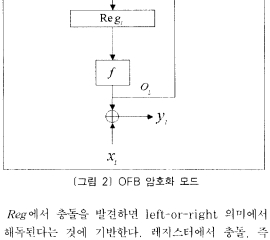
OFB 암호화 모드는 블록 암호를 스트림 암호로 동작시키는 방법으로, l-비트 레지스터 Reg을 사용한다. 기반이 되는 유사랜덤 함수는 $f: \{0,1\}^l \rightarrow \{0,1\}^l$이고, 암호화될 입력 메시지 x는 l-비트 블록들의 연결, 즉 $x = x_1 x_2 \cdots x_n$ (x_i는 l-비트 블록)이라 가정하자. 암호화 기법 $\mathcal{E}$- $OFB^f(x)$는 다음과 같이 동작한다([그림 2] 참조).

Function $\mathcal{E}$- $OFB^f(x)$
  $IV \xleftarrow{R} \{0,1\}^l$
  $Reg_1 = IV$
  for $i = 1, \cdots, n$ do
    $o_i = f(Reg_i)$
    $y_i = o_i \oplus x_i$
    $Reg_{i+1} = o_i$
  return $(IV\, y_1 \cdots y_n)$

여기서, IV는 nonce로서 초기 벡터(initial vector)이다.

OFB 암호화 모드와 관련하여 다음과 같은 두 개의 함수 패밀리를 고려한다. 패밀리 $OFB^{R_{l,l}}$은 $\mathcal{E}$- $OFB^f(x)$, $\forall f \in R_{l,l}$ 함수들의 집합이고, OFB^F은 $\mathcal{E}$- $OFB^f(x)$, $\forall f \in F$ 함수들의 집합이다.

OFB 모드의 안전성 증명은 공격자가 레지스터



(그림 2) OFB 암호화 모드

Reg에서 충돌을 발견하면 left-or-right 의미에서 해독된다는 것에 기반한다. 레지스터에서 충돌, 즉 $Reg_i = Reg_j, i \neq j$이 발생하면, $o_i = o_j$이고 따라서 $y_i \oplus y_j = x_i^b \oplus x_j^b (b=1,2)$이다. 그러므로 $x_i^1 \oplus x_j^1 \neq x_i^2 \oplus x_j^2$이면 b가 노출된다.

먼저 OFB 암호화 모드의 기반이 되는 함수 f를 랜덤 함수(random function)로 가정했을 때, left-or-right 의미에서 안전성의 하한(lower bound)을 보인다.

[보조 정리 4]

[랜덤 함수 모델에서 OFB 모드 안전성의 하한]

기껏해야 총 μ 비트인 q개의 질의를 하고 다음의 이점을 가지는 left-or-right 의미에서 OFB^{R_0}을 공격하는 공격자 E가 존재한다($(\mu/l)^2 \leq 2^l$라고 가정한다).

$$Adv_E^{lr} \geq 0.316 \cdot \frac{(\mu/l)\cdot(\mu/l-1)}{2^l}.$$

(증명)

주어진 안전성 파라메터를 달성하는 공격자가 존재한다는 것을 보임으로써 정리를 증명한다. left-or-right 의미에서 공격자는 메시지의 쌍으로 구성된 오라클 질의를 한다. 공격자 E는 기법의 기반이 되는 랜덤 함수 f의 입력에서 충돌을 발견한다. 다음과 같이 공격자 E를 구성하자.

알고리즘 $E^{O(\cdot,\cdot)}$

(1) $n = \frac{\mu}{lq}$ (각 질의의 평균 블록 개수)

(2) 각각 n-블록 길이인 q개의 질의 메시지 $N_1, \cdots, N_q$를 선택한다.
$N_i[k] \neq N_i[k']$, $(i,k) \neq (j,k')$,
$1 \leq i, j \leq q,\ k, k' = 1, \cdots, n$

(3) for $i = 1, \cdots, q$
$(IV_i \| y_i[1] \cdots y_i[n]) \leftarrow O(0^{nl}, N_i)$
$IV_i \in \{0,1\}^l$은 i번째 질의의 초기값이다.

(4) $Reg_i[k] = Reg_j[k']$인 (i,k)와 (j,k') $((i,k) \neq (j,k'), 1 \leq i, j \leq q,\ k, k' = 1, \cdots, n)$이 존재하는 경우, $y_i[k] \oplus y_i[k'] = 0$이면 1을 출력하고, $y_i[k] \oplus y_i[k'] = N_i[k] \oplus N_i[k']$이면 2를 출력한다.

(5) (4)에서 (i,k)와 (j,k')가 존재하지 않으면, coin flip을 출력한다.

Col을 $Reg_1[k] = Reg_2[k']$인 사건이라고 하자. 공격자의 이점은 단지 이 사건의 확률이다. 이를 보이기 위해, 먼저 이 사건 Col의 확률은 두 게임에서 랜덤한 값만을 수반한다는 것을 관찰한다. $\Pr_b[E=1]$은 게임 $b \in \{0,1\}$에서 동작 중일 때 E가 게임 1에서 동작 중이라고 추정하는 확률이라고 하자. 그러고 p를 Col의 확률이라고 하자. 그러면

$$\begin{aligned} Adv_E^{lr} &= |\Pr_1[E=1] - \Pr_2[E=1]| \\ &= \left| (p\cdot 1 + (1-p)\cdot\frac{1}{2}) \right. \\ &\quad \left. - (p\cdot 0 + (1-p)\cdot\frac{1}{2}) \right| \\ &= p \end{aligned}$$

이다. p의 하한을 계산하기 위해 스트링 B를 다음과 같이 정의한다.

$$\begin{aligned} B = &IV_1\, o_1[1] \cdots o_1[n-1] \\ &IV_2\, o_2[1] \cdots o_2[n-1] \\ &\cdots \\ &IV_q\, o_q[1] \cdots o_q[n-1] \end{aligned}$$

즉, 마지막 q번째 질의의 n번째 블록의 암호화까지 Reg을 통과하는 값들이다. B의 길이는 $Q = nq = \mu/l$ 블록이다. 레지스터 $Reg_i[k]$의 내용은 $Reg_i[k] = B[(i-1)nl + k]$이다($|B[i]| = l$).

C_i를 B에서 i번째 블록까지 충돌이 발생하지 않은 사건이라고 하고, D_i를 $B[i]$가 이전 블록들

$B[1], \cdots, B[i-1]$와 충돌하지 않는 사건이라고 하자. Bayes's rule과 $\Pr[C_i]=1$이라는 사실을 이용하면 마지막 블록까지 충돌하지 않을 확률 $\Pr[C_{n_q}]$은 다음과 같이 계산된다.

$$\begin{aligned}&\Pr[C_{n_q}]\\&=\Pr[D_{n_q}|C_{n_q-1}]\Pr[C_{n_q-1}]\\&=\Pr[D_{n_q}|C_{n_q-1}]\cdots\Pr[D_2|C_1]\Pr[C_1]\\&=\prod_{j=1}^{n_q}\Pr[D_j|C_{j-1}]\end{aligned}$$

여기서,

$$\begin{aligned}\Pr[D_j|C_{j-1}]&=\frac{2^l-(j-1)}{2^l}\\&=1-\frac{j-1}{2^l}.\end{aligned}$$

따라서,

$$\begin{aligned}\Pr[C_{n_q}]&=\prod_{j=2}^{n_q}\Pr[D_j|C_{j-1}]\\&=\prod_{j=1}^{n_q-1}\left(1-\frac{j}{2^l}\right)\le\prod_{j=1}^{n_q-1}e^{-\frac{j}{2^l}}\\&=e^{-\frac{n_q(n_q-1)}{2^{l+1}}}.\end{aligned}$$

그러므로,

$$\begin{aligned}p&=1-\Pr[C_{n_q}]\ge 1-e^{-\frac{n_q(n_q-1)}{2^{l+1}}}\\&=1-e^{-\frac{1}{2}\cdot\frac{\mu l(\mu l-1)}{2^l}}\\&\ge(1-e^{-1})\cdot\frac{1}{2}\cdot\frac{\mu l(\mu l-1)}{2^l}.\end{aligned}$$

여기서, $\left(\frac{\mu}{l}\right)^2\le 2^l$이라는 가정을 이용하였다. ■

랜덤 함수 모델에서 OFB 모드의 안전성의 상한은 보조 정리 5와 같다.

[보조 정리 5]

[랜덤 함수 모델에서 OFB 모드의 안전성에 관한 상한(upper bound)]

A를 기껏해야 총 μ 비트인 q개의 질의(query)를 하는, left-or-right 의미에서 $OFB^{R_{IV}}$을 공격하는 임의의 공격자라고 하자. 그러면 A의 이점(advantage)은 다음과 같다.

$$Adv_A^{b}\le\delta_{(RF)^*}=\frac{(\mu l)(\mu l-1)}{2^{l-1}}.$$

(증명)

$(x_1^1, x_1^2)\cdots(x_q^1, x_q^2)$를 같은 길이의 메시지 쌍으로 구성된 공격자 A의 오라클 질의라고 하자. 질의들은 A의 coin tossing과 이전 질의에 대한 오라클의 응답에 의존하는 확률 변수(random variable)이다. $IV_i\in\{0,1\}^l(\ i=1,\cdots,q\ )$은 오라클에 의해 랜덤하게 선택되는 i번째 질의 (x_i^1, x_i^2)에서 초기 벡터이다. $n_i(\ i=1,\cdots,q\ )$를 i번째 질의에서 블록의 수라고 하자. $x_i^b=x_i^b[1]\cdots x_i^b[n_i]\ (\ b\in\{1,2\})$은 i번째 질의 메시지를 나타내고, $y_i=y_i[1]\cdots y_i[n_i]$는 i번째 질의 메시지에 대한 오라클의 응답(response)를 나타낸다. $Reg_i=Reg_i[1]\cdots Reg_i[n_i]$는 i번째 질의에서 레지스터의 내용을 나타내고, $Reg_i[j]\ (\ j=1,\cdots,n_i)$는 i번째 질의에서 j번째 블록에 해당하는 레지스터를 나타낸다. $o_i[j]$는 $Reg_i[j]$를 함수 f에 입력하여 계산한 값을 나타낸다. $\Pr_1[\ \cdot\ ]$는 공격자 A에게 회적 오라클이 제공되는 게임 1에서의 확률을 나타내고, $\Pr_2[\ \cdot\ ]$는 공격자 A에게 오른쪽 오라클이 제공되는 게임 2에서의 확률을 나타낸다.

공격자 A는 초기 벡터 IV_i, 질의 메시지 x_i, 대응하는 응답 y_i를 알기 때문에 f의 출력 o_i를 안다. 따라서 공격자는 랜덤 함수 f의 입력인 Reg_i의 값을 안다. 공격을 위해 Reg_i에서의 충돌을 발견하려고 한다.

D를 충돌 사건(event), 즉 임의의 $(i,k)\neq(j,k')\ 1\le i,\ j\le q,\ k=1,\cdots,n_i,\ k'=1,\cdots,n_j$에 대해, $Reg_i[k]=Reg_j[k']$이 발생하는 사건이라고 하자.

충돌이 발생하지 않는다면, f가 랜덤 함수이므로 각 $o_i[k]$는 랜덤하고 독립적으로 선택된(randomly and independently chosen) 값들이다. 따라서 $y_i[k]$는 랜덤이고 $y_i[k']\ (1\le j\le i-1,\ 1\le k'\le n_j)$, $y_i[1],\cdots,y_i[k-1]$, $y_i[k+1],\cdots,y_i[n_i-1]$과 $x_j^b[k']\ (1\le j\le i,\ 1\le k'\le n_j)$에 독립이다. 따라서 충돌이 발생하지 않을 확률은 b에 의존하지 않고 다음처럼 쓸 수 있다.

$$\Pr_1[\overline{D}]=\Pr_2[\overline{D}]\qquad(3.1)$$

같은 이유로, 충돌이 발생하지 않는다면, 공격자에게 주어진 각 암호문 블록은 이전 암호문과 평문 블록에 독립이므로, 공격자는 게임 $1(b=1)$과 게임 $2(b=2)$에 대해 같은 확률로 $A=1$을 출력한다. 즉, 다음이 성립한다.

$$\Pr_1[A=1|\overline{D}] = \Pr_2[A=1|\overline{D}] \qquad (3.2)$$

식 (3.1)과 (3.2)를 이용하여 공격자의 이점은 다음과 같이 계산된다.

$$\begin{aligned} Adv_A^{\varepsilon} &= |\Pr_1[A=1]-\Pr_2[A=1]| \\ &= |\Pr_1[A=1|D]\Pr_1[D] \\ &\quad + \Pr_1[A=1|\overline{D}]\Pr_1[\overline{D}] \\ &\quad - \Pr_2[A=1|D]\Pr_2[D] \\ &\quad - \Pr_2[A=1|\overline{D}]\Pr_2[\overline{D}]| \\ &= |(\Pr_1[A=1|D]-\Pr_2[A=1|D])\Pr_1[D]| \\ &\le \Pr_1[D] \end{aligned}$$

식 (3.1)에 의해 어떤 게임인지 상관없이 충돌 확률을 계산하면 되므로, $\Pr_1[D]$를 $\Pr[D]$라 두고 확률을 계산하자. 스트링 B를 다음과 같이 정의한다.

$$\begin{aligned} B = IV_1\ o_1[1] &\quad \cdots\ o_1[n_1-1] \\ IV_2\ o_2[1] &\quad \cdots\ o_2[n_2-1] \\ &\quad \cdots \\ IV_q\ o_q[1] &\quad \cdots\ o_q[n_q-1] \end{aligned}$$

즉, 마지막 q번째 질의의 n_q번째 블록의 암호화까지 레지스터 Reg을 통과하는 값들이다. B의 길이는 $Q=l\cdot\sum_{i=1}^{q} n_i \le \mu$ 비트이다. $B[i]\,(1\le i\le Q/l)$은 B의 i번째 블록으로 l-비트 길이이다. 레지스터 $Reg_i[k]$의 내용은 $Reg_i[k]=B[l\cdot\sum_{j=1}^{i-1} n_j + k]$이다.

모든 가능한 쌍 $(i,k)\neq(j,k')\,(1\le i,j\le q,\ k=1,\cdots,n_i,\ k'=1,\cdots,n_j)$에 대해 충돌 $Reg_i[k]=Reg_j[k']$을 가질 수 있는 스트링 B의 개수를 계산하자. $Reg_i[k]=Reg_j[k']$이기 때문에 두 레지스터의 내용에 대해 2^l개의 가능한 값이 존재한다. 나머지 $Q-2l$ 비트는 $2^{\mu-2l}$개의 가능성을 가진다. 따라서 충돌을 가진 스트링의 개수 $2^{\mu-l}$이다.

모든 가능한 $(i,k)\neq(j,k')$에 대해 $(\mu/l)(\mu/l-1)/2$개의 가능한 $(i,k)\neq(j,k')$ 쌍이 존재한다. 따라서 적어도 하나의 충돌을 가진 스트링 B의 개수 C는 기껏해야 $(\mu/l)(\mu/l-1)2^{\mu-l-1}$이다.

스트링 B가 가질 수 있는 총 가지 수는 2^{μ}이다. 따라서,

$$\begin{aligned} \Pr[\overline{D}] &= (2^{\mu}-C)/2^{\mu} \\ &> 1-(\mu/l)(\mu/l-1)2^{-l-1} \end{aligned}$$

이다. 이것은 다음을 함축한다.

$$\Pr[D] \le \frac{(\mu/l)(\mu/l-1)}{2^{l+1}} \ . \blacksquare$$

블록 암호가 유사랜덤이기 때문에 실제 상황에서는 유사랜덤 함수 모델에서 OFB 모드의 안전성을 증명해야 한다. 이것은 보조 정리 5로부터 유도될 수 있다.

[정리 6] (유사랜덤 함수 모델에서 OFB의 안전성)
F를 입력 길이 l과 출력 길이 t을 가진 (t',q',ε')-안전한 유사랜덤 함수 패밀리라고 가정하자. 그러면 OFB^F 기반은 left-or-right 의미에서 $(t,q,\mu;\varepsilon)$-안전하다라고 한다. 여기서 $q=q'$, $\mu=q'l$이고 $t=t'-c\frac{\mu}{l}(l+1)$이며, $\varepsilon=2\varepsilon'+\delta_{OFB^F}$이다. 그리고 $c>0$는 임의의 작은 상수이고 $\delta_{OFB^F}=(\mu/l)(\mu/l-1)/2^{l+1}$이다.

(증명)

보조 정리 5에서 OFB^R가 안전하다는 것을 보였다. 이를 이용하여 만약 OFB^F가 안전하지 않다면, 이것은 F가 유사랜덤 함수 패밀리가 아니라는 것을 의미함을 보일 수 있다. 즉, 공격자 D가 OFB^F를 $(t,q,\mu;\varepsilon)$-해독한다라고 가정한다. $Adv_D^{\varepsilon}(F)$를 left-or-right 의미에서 OFB^F에 대한 D의 이점이라고 하고, $Adv_D^{\varepsilon}(R_{l,l})$를 left-or-right 의미에서 OFB^R에 대한 D의 이점이라고 하자. 그러면, t' 동안 수행하고 기껏해야 q' 질의를 할 수 있지만 $Adv_A(F,R_{l,l})>\varepsilon'$인 구별자 A를 구성할 수 있다. 이것은 유사랜덤 함수 패밀리로서 F의 안전성에 모순된다.

다음과 같이 공격자 A를 구성한다. A는 서브루틴으로 D를 수행하여 D가 암호화 모드를 해독하는지 관찰한다. D가 암호화 모드를 해독한다면, f는 F로부터 추출되었고, 그렇지 않다면 f는 $R_{l,l}$로부터

추출되었다. A가 D를 수행하기 위해 자신의 오라클 f에게 질의하는 것으로 D의 오라클 $O(b,(\cdot,\cdot))$을 흉내낸다.

알고리즘 A^f

(1) $b \xleftarrow{R} \{1,2\}$

(2) 다음처럼 오라클 질의에 응답을 얻는 D를 수행한다. D가 오라클 질의 (M_1, M_2)를 할 때, 오라클 질의에 대한 응답으로 $z \leftarrow \mathcal{E}\text{-}OFB^f(M_b)$를 D에게 반환한다.

(3) 모든 질의가 완료된 후 D는 left 오라클인지 또는 right 오라클인지를 나타내는 $d(\in\{1,2\})$를 출력한다. $d=b$이면 1을 출력하고, 그렇지 않으면 0을 출력한다.

공격자 A는 구별자 D를 서브루틴으로 가지므로 기껏해야 $q'=\mu l$개의 오라클 질의를 한다고 하자. 그러면 A의 수행 시간 t'은 $t+c(\mu l)(+l)$이다. 여기서 $c>0$는 임의의 작은 상수이다.

A의 이점 $Adv_A(F,R_{l,l})$을 계산하기 위해 먼저 다음 식을 계산하자. 임의의 $G \in \{F,R_{l,l}\}$에 대해

$$\begin{aligned}
&\Pr_{f,R_{l,l},G}[A=1] \\
&= \frac{1}{2}\sum_{b\in\{1,2\}} \Pr_{f,R_{l,l},G}[D^{O(b,(\cdot,\cdot))}=b] \\
&= \frac{1}{2}\Big(\Pr_{f,R_{l,l},G}[D^{O(1,(\cdot,\cdot))}=1] \\
&\quad + \Pr_{f,R_{l,l},G}[D^{O(2,(\cdot,\cdot))}=2]\Big) \\
&= \frac{1}{2}\Big(\Pr_{f,R_{l,l},G}[D^{O(1,(\cdot,\cdot))}=1]+1 \\
&\quad - \Pr_{f,R_{l,l},G}[D^{O(2,(\cdot,\cdot))}=1]\Big)
\end{aligned}$$

따라서, A의 이점은 다음과 같이 계산된다.

$$\begin{aligned}
&Adv_A(F,R_{l,l}) \\
&= |\Pr_{f,R_{l,l},F}[A=1] - \Pr_{f,R_{l,l},R_{l,l}}[A=1]| \\
&= \Big|\frac{1}{2}\Big\{\Pr_{f,R_{l,l},F}[D^{O(1,(\cdot,\cdot))}=1] \\
&\quad - \Pr_{f,R_{l,l},F}[D^{O(2,(\cdot,\cdot))}=1]\Big\} \\
&\quad \frac{1}{2}\Big\{\Pr_{f,R_{l,l},R_{l,l}}[D^{O(1,(\cdot,\cdot))}=1] \\
&\quad - \Pr_{f,R_{l,l},R_{l,l}}[D^{O(2,(\cdot,\cdot))}=1]\Big\}\Big| \\
&\geq \frac{1}{2}\left(Adv_D^{f_l}(F) - Adv_D^{f_l}(R_{l,l})\right)
\end{aligned}$$

보조 정리 5에서

$$Adv_D^{f_l}(R_{l,l}) \leq \delta_{OFB^{l_*}} = \frac{(\mu l)(\mu l-1)}{2^{l+1}}$$

라는 것을 보였고 $Adv_D^{f_l}(F) > \varepsilon$라고 가정했다. 따라서,

$$Adv_A(F,R_{l,l}) > \frac{\varepsilon}{2} - \frac{\delta_{OFB^*}}{2} = \varepsilon'$$

이다. 이것은 F가 (t', q', ε')-안전한 유사랜덤 함수 패밀리라는 가정에 모순이다. ■

3.2 3GPP $f8$ 암호화 모드

비동기식(W-CDMA) 3세대 이동 통신 진영의 3GPP (3rd generation partnership project)에서는 무선 구간의 메시지 기밀성을 보장하기 위해 블록 암호 KASUMI에 기반한 암호화 모드를 제안하였는데, 이것은 OFB 모드의 변형된 형태이다[1]. Kang-Yi-Hong-Cho[10]가 3GPP f8 암호화 모드의 기반이 되는 함수인 KASUMI가 유사랜덤 치환이라는 것을 보였기 때문에, 우리는 기반이 되는 함수를 l-비트 스트링에서의 유사랜덤 치환 패밀리 B_l로 고정한다. 그리고 암호화될 입력 메시지 x는 l-비트 블록들의 연결, $x=x_1\cdots x_n$이라고 하자. 3GPP f8 암호화 모드 역시 l-비트 레지스터 Reg을 사용한다. f8 암호화 모드와 관련하여 다음과 같은 두 개의 함수 패밀리를 고려한다. 패밀리 $f8^{B_l}$은 $\mathcal{E}\text{-}f8^f(x)$, $\forall f \in P_l$ 함수들의 집합이고, $f8^{B_l}$은 $\mathcal{E}\text{-}f8^f(x)$, $\forall f \in B_l$ 함수들의 집합이다. 암호화 알고리즘 $\mathcal{E}\text{-}f8^f(x)$는 다음과 같이 동작한다([그림 3] 참조).

Function $\mathcal{E}\text{-}f8^f(x)$

$IV \leftarrow f(Count||Direction||Bearer||0\cdots0)$

$Reg_1 = IV$

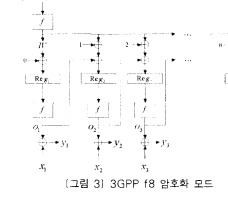
for $i=1,\cdots,n$ do

$o_i = f(Reg_i)$

$y_i = o_i \oplus x_i$

$Reg_{i+1} = IV \oplus i \oplus o_i$

return $(y_1\cdots y_n)$



〔그림 3〕 3GPP f8 암호화 모드

여기서, *Count*는 시간에 의존하는 32-비트 길이의 암호화 순서 번호이고, *Bearer*는 5-비트의 베어러 식별자(bearer identifier)이다. *Direction*은 1-비트의 방향 식별자(direction identifier)이다. 0…0은 입력이 *l*-비트(KASUMI의 경우, 64-비트)가 되도록 맞추어주는 패딩(padding) 부분이다.

OFB 모드와의 차이점은 초기 nonce $ctr = (Count||Direction||Bearer||0\ldots0)$는 수신측에게 전달하지 않으며, 또한 레지스터의 값으로 ctr 대신 $f(ctr)$을 사용한다는 것이다.

먼저 3GPP f8 암호화 모드의 기반이 되는 함수 f를 랜덤 치환으로 가정했을 때, left-or-right 의미에서 안전성의 하한을 보조 정리 7에서, 상한을 보조 정리 8에서 보인다. 정리 9에서는 유사랜덤 치환 모델에서의 안전성을 증명한다.

[보조 정리 7]

〔랜덤 치환 모델에서 f8 암호화 모드 안전성의 하한〕

기껏해야 총 μ 비트인 q개의 질의를 하고 다음의 이점을 가지는 left-or-right 의미에서 f8^{P}을 공격하는 공격자 E가 존재한다($(\mu/l)^2 \le 2^l$라고 가정한다).

$$Adv_E^{f8} \ge 0.316 \cdot \frac{(\mu/l)\cdot(\mu/l-1)}{2^l}.$$

(증명)

증명 과정은 보조 정리 4에서의 증명과 유사하다. 하지만 OFB 모드와 달리 공격자는 f8 모드의 레지스터 Reg의 값을 알지 못하므로 $Reg_i[k] = Reg_j[k']$ ($i \neq j, 1 \le i,j \le q, k, k' = 1, \cdots, n$)는 식별할 수 없다. 그렇지만 공격자는 질의된 메시지 블록 $x_i[k]$와 응답된 암호문 블록 $y_i[k]$를 알기 때문에 $o_i[k]$ 값을 알고 따라서 $o_i[k] = o_j[k']$는 식별할 수 있다. f가 치환(permutation)이기 때문에 f의 출력 값에서의 충돌 $o_i[k] = o_j[k']$은 다음을 함축한다.

$$\begin{aligned} & o_i[k] = o_j[k'] \\ \Leftrightarrow\ & f(Reg_i[k]) = f(Reg_j[k']) \\ \Leftrightarrow\ & Reg_i[k] = Reg_j[k'] \end{aligned}$$

따라서 공격자는 랜덤 치환 f의 출력에서 충돌을 발견한다. 공격자 E를 다음과 같이 구성하자.

알고리즘 $E^{O(\cdot,\cdot)}$

(1) $n = \frac{\mu}{lq}$ (각 질의의 평균 블록 개수)

(2) 각각 n-블록 길이인 q개의 질의 메시지 $N_1, \cdots, N_q$를 선택한다.
$N_i[k] \neq N_j[k']$, $(i,k) \neq (j,k')$,
$1 \le i,j \le q,\ k,k' = 1, \cdots, n$

(3) for $i = 1, \cdots, q$
$(y_i[1] \cdots y_i[n]) \leftarrow O(0^{nl}, N_i)$

(4) $o_i[k] = o_j[k']$인 $(i,k), (j,k')$ $((i,k) \neq (j,k'), 1 \le i,j \le q,\ k,k' = 1, \cdots, n)$가 존재하는 경우, $y_i[k] \oplus y_j[k'] = 0$이면 1을 출력하고, $y_i[k] \oplus y_j[k'] = N_i[k] \oplus N_j[k']$이면 2를 출력한다.

(5) 그러한 $(i,k), (j,k')$가 존재하지 않으면, coin flip을 출력한다.

Col을 $o_i[k] = o_j[k']$인 사건이라고 하면, Col의 확률의 하한을 구하기 위하여 스트림 B를 다음과 같이 정의한다.

$$\begin{aligned} B = o_1[1] \cdots o_1[n]\, o_2[1] \cdots o_2[n] \\ \cdots o_q[1] \cdots o_q[n] \end{aligned}$$

즉, 마지막 q번째 질의의 n번째 블록의 암호화까지 랜덤 치환 f의 출력들이다. B의 길이는 $Q = nq = \mu/l$ 블록이다.

증명의 나머지 부분은 보조 정리 4에서와 동일한 방법으로 계산되므로 생략한다. ■

[보조 정리 8]

[랜덤 치환 모델에서 $f8$의 안전성에 관한 상한]

E를 기껏해야 총 μ 비트인 q개의 질의를 하는, left-or-right 의미에서 $f8^{IV}$을 공격하는 임의의 공격자라고 하자. 그러면 E의 이점은 다음과 같다.

$$Adv_E^{ir} \le \delta_{f8^{IV}} = \frac{\mu/l \cdot (\mu/l-1)}{2^{l+1}}.$$

(증명)

$(x_1^1, x_1^2) \cdots (x_q^1, x_q^2)$를 같은 길이의 메시지 쌍으로 구성된 공격자 A의 오라클 질의라고 하자. 질의들은 A의 coin tossing과 이전 질의에 대한 오라클의 응답에 의존하는 확률 변수(random variable)이다.

$ctr_i = (Count_i \| Direction_i \| Bearer_i \| 0 \cdots 0)$는 i번째 질의 (x_i^1, x_i^2)에서 오라클에 의해 선택되고 $IV_i = f(ctr_i) \in \{0,1\}^l$가 계산된다. $n_i (i = 1, \cdots, q)$를 i번째 질의에서 블록의 수라고 하자. $x_i^b = x_i^b[1] \cdots x_i^b[n_i]$ $(b \in \{1,2\})$은 i번째 질의 메시지를 나타내고, $y_i = y_i[1] \cdots y_i[n_i]$는 i번째 질의 메시지에 대한 오라클의 응답(response)를 나타낸다. $Reg_i = Reg_i[1] \cdots Reg_i[n_i]$는 i번째 질의에서 레지스터의 내용을 나타내고, $Reg_i[j]$ $(j = 1, \cdots, n_i)$는 i번째 질의에서 j번째 블록에 해당하는 레지스터를 나타낸다. $o_i[j]$는 $Reg_i[j]$를 함수 f에 입력하여 계산한 값을 나타낸다. $\Pr_1[\cdot]$는 공격자 A에게 왼쪽 오라클이 제공되는 게임 1에서의 확률을 나타내고, $\Pr_2[\cdot]$는 공격자 A에게 오른쪽 오라클이 제공되는 게임 2에서의 확률을 나타낸다.

C를 충돌 사건(event). 즉 임의의 $(i,k) \neq (j,k')$, $1 \le i, j \le q$, $k = 1, \cdots, n_i$, $k' = 1, \cdots, n_j$에 대해, $Reg_i[k] = Reg_j[k']$이 발생하는 사건이라고 하자. 보조 정리 5와 유사한 방법으로 공격자의 이점은 다음과 같이 계산된다.

$$Adv_A^{ir} \le \Pr[C]$$

하지만 공격자는 $f8$ 모드의 레지스터 Reg에서 충돌을 발견하는데 있어 레지스터 Reg의 값을 알지 못하고, 따라서 공격자는 $Reg_i[k] = Reg_j[k']$ $(i \neq j, 1 \le i, j \le q, k = 1, \cdots, n_i, k' = 1, \cdots, n_j)$는 식별할 수 없다. 그렇지만 공격자는 질의된 메시지 블록 $x_i[k]$와 응답된 암호문 블록 $y_i[k]$를 알기 때문에 $o_i[k]$ 값을 알고 따라서 $o_i[k] = o_j[k']$는 식별할 수 있다. f가 치환(permutation)이기 때문에 f의 출력 값에서의 충돌 $o_i[k] = o_j[k']$은 다음을 함축한다.

$$\begin{aligned} & o_i[k] = o_j[k'] \\ \Leftrightarrow\ & f(Reg_i[k]) = f(Reg_j[k']) \\ \Leftrightarrow\ & Reg_i[k] = Reg_j[k'] \end{aligned}$$

따라서 $\Pr[C]$의 상한을 계산하기 위해, f의 출력 값에서의 충돌 사건 D, 즉 $o_i[k] = o_j[k']$ $((i,k) \neq (j,k'))$ $1 \le i, j \le q$, $k = 1, \cdots, n_i$, $k' = 1, \cdots, n_j$)의 확률을 계산한다. 스트림 S를 다음과 같이 정의한다.

$$S = o_1[1] \cdots o_1[n_1]\, o_2[1] \cdots o_2[n_2] \cdots o_q[1] \cdots o_q[n_q]$$

즉, 마지막 q번째 질의의 n_q번째 블록의 암호화까지 f의 출력 값들이다. S의 길이는 $Q = l \cdot \sum_{i=1}^{q} n_i \le \mu$ 비트이다. 먼저 모든 가능한 쌍 (i,k), (j,k') $((i,k) \neq (j,k'))$, $1 \le i, j \le q$, $k = 1, \cdots, n_i$, $k' = 1, \cdots, n_j$)에 대해 충돌 $o_i[k] = o_j[k']$을 가질 수 있는 스트림 S의 개수를 계산하자. $o_i[k] = o_j[k']$이기 때문에 두 값에 대해 2^l개의 가능한 값들이 존재한다. 나머지 $Q - 2l$ 비트는 2^{Q-2l}개의 가능성을 가진다. 따라서 충돌을 가진 스트림의 개수 2^{Q-l}이다. 모든 가능한 $(i,k) \neq (j,k')$에 대해 $(\mu/l)(\mu/l-1)/2$개의 가능한 (i,k), (j,k') 쌍이 존재한다. 따라서 적어도 하나의 충돌을 가진 스트림 S의 개수 η는 기껏해야 $(\mu/l)(\mu/l-1)2^{Q-l-1}$이다. 스트림 S가 가질 수 있는 총 가지 수는 2^Q이다. 따라서,

$$\begin{aligned} \Pr[D] &= (2^Q - \eta)/2^Q \\ &> 1 - (\mu/l)(\mu/l-1)2^{-l-1} \end{aligned}$$

이다. 이것은 다음을 함축한다.

$$\Pr[C] \le \frac{(\mu/l)(\mu/l-1)}{2^{l+1}}. \quad \blacksquare$$

[정리 9] [유사랜덤 치환 모델에서 f8의 안전성]

B_l를 l-비트 입력과 출력을 가진 $(t', q'; \varepsilon')$-안전한 유사랜덤 치환 패밀리라고 가정하자. 그러면 $f8^{B_l}$ 키없은 left-or-right 의미에서 $(t, q, \mu; \varepsilon)$-안전하다라고 한다. 여기서 $q = q'$, $\mu = q'l$이고 $t = t' - c\frac{q}{l}(l+l)$이며, $\varepsilon = 2\varepsilon' + \delta_{B^{l'}}$이다. 그리고, $c > 0$는 임의의 작은 상수이고, $\delta_{B^{l'}} = (\mu/l \cdot (\mu/l - 1))/2^{l+1}$이다.

(증명)

증명의 상세한 사항은 정리 6의 증명에서 유사랜덤 함수를 유사랜덤 치환으로 대치한 것과 거의 동일하기 때문에 생략한다. ■

Ⅳ. 결 론

본 논문에서는 블록 암호의 기본적인 동작 모드 중의 하나인 OFB 암호화 모드와 비동기식 IMT-2000의 무선 구간 메시지 암호화를 위해 사용되는 3GPP f8 암호화 모드의 안전성을 분석하였다. Left-or-right 안전성 개념을 적용하여 각각 랜덤 함수 모델과 랜덤 치환 모델에서의 안전성에 대한 하한과 상한을 증명하였으며, 또한 유사랜덤 함수 모델과 유사랜덤 치환 모델에서의 안전성을 각각 증명하였다. 이것은 기반이 되는 블록 암호 KASUMI가 유사랜덤 치환이라면, 3GPP f8 암호화 모드는 능동적 선택 평문 공격하에서 안전하다는 것을 의미한다.

참 고 문 헌

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

[2] A. Alkassar, A. Geraldy, B. Pfitzmann, A.hmad-reza Sadeghi, "Optimized Self-Synchronizing Mode of Operation," *Pre-proceedings of 8th Fast Software Encryption Workshop*, April 2, 2001, pp. 82~96.

[3] M. Bellare, A. Desai, E. Jokipii, P. Rogaway, "A Concrete Security Treatment of Symmetric Encryption : Analysis of the DES Modes of Operation," *38th Symposium on Foundations of Computer Science(FOCS)*, IEEE Computer Society, 1997, pp. 394~403.

[4] M. Bellare, J. Kilian, P. Rogaway, "The security of cipher block chaining," *Crypto '94*, LNCS Vol. 839, Springer-Verlag, 1994, pp. 341~358.

[5] J. Black, P. Rogaway, "CBC macs for arbitrary-length message : the three key constructions," *Crypto '2000*, LNCS Vol. 1880, Springer-Verlag, 2000, pp. 197~215.

[6] DES Modes of Operation, Federal Information Processing Standards Publication 81(FIPS PUB 81), December 2, 1980.

[7] V. Gligor, P. Donescu, "Fast Encryption and Authentication : XCBC Encryption and XECB Authentication Modes," *Pre-proceedings of 8th Fast Software Encryption Workshop*, April 2, 2001, pp. 97~111.

[8] O. Goldreich, S. Goldwasser, S. Micali, "How to construct random functions," *Journal of the ACM*, Vol. 33, No. 4, 1986, pp. 210~217.

[9] C.S. Jutla, "Encryption Modes with Almost Free Message Integrity," *NIST Workshop Symmetric Key Block Cipher Modes of Operation*, October 2000, http://csrc.nist.gov/encryption/modes/.

[10] J.S. Kang, O.Y. Yi, D.W. Hong, H.S. Cho, "Pseudorandomness of MISTY-type transformations and the block cipher KASUMI," *ACISP 2001*, LNCS Vol. 2119, Springer-Verlag, 2001, pp. 60~73.

[11] E. Petrank, C. Rackoff, "CBC MAC for Real-Time Data Source," *Journal of Cryptology*, Vol. 13, No. 3, 2000, pp. 315~338.

[12] P. Rogaway, "OCB Mode: Parallelizable Authentication Encryption," *NIST Workshop Symmetric Key Block Cipher Modes of Operation*, October 2000, http://csrc.nist.gov/encryption/modes/.

〈著者紹介〉

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 : 암호 이론, 이동통신 정보보호

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

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