Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.3, Jun. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.3.547

PRF-기반 키유도함수에서 카운터 입력 형태에 따른 증명가능 안전성*

김 나 영,† 강 주 성,‡ 염 용 진
국민대학교 수학과 / 금융정보보안학과

Provable Security of PRF-based Key Derivation Functions according to Input Types of Counters*

Nayoung Kim,† Ju-Sung Kang,‡ Yongjin Yeom
Dept. of Math. / Financial Information Security, Kookmin University

요 약

암호 알고리즘과 암호 프로토콜은 사용되는 키들의 기밀성이 유지된다는 가정 하에서 안전성을 보장받을 수 있다. 대부분의 암호시스템에는 전반적으로 사용되는 키들을 안전하게 관리하는 키관리 메커니즘이 필수 요소로 구현되어 있으며, 키관리 메커니즘의 내부에는 하나의 마스터키로부터 더 많은 종류의 키들을 생성하는 키유도함수(KDF)가 존재한다. NIST SP 800-108에서는 PRF-기반 KDF를 표준안으로 제안하고 있다. 본 논문에서는 KDF와 암호화 운영모드에 대한 증명가능 안전성 관점의 차이를 분석하고, PRF-기반 KDF 중 Counter 모드와 Feedback 모드에 대하여 핵심함수인 PRF의 입력값으로 카운터 값이 XOR과 연접 연산 형태로 입력되는 경우를 비교하여 안전성을 규명한다. 증명가능 안전성 관점에서 카운터 값이 XOR 형태로 입력되는 경우의 KDF는 안전하지 않은 반면, 연접 연산 형태로 삽입되는 경우의 KDF는 안전함을 증명한다.

ABSTRACT

The security of all cryptographic algorithms and protocols is based on the confidentiality of secret keys. Key management mechanism is an indispensable part of the cryptographic system and this deals with the generation, exchange, storage, use, and replacement of keys. Within the key management mechanism there are key derivation functions (KDFs) which derive one or more keys from a master key. NIST specifies three families of PRF-based KDFs in SP 800-108. In this paper, we examine the difference of security models between the KDFs and the encryption modes of operations. Moreover we focus on the provable security of PRF-based KDFs according to input types of counters, and show that the counter and feedback modes of KDFs using XOR of counters are insecure, while these modes using concatenation of counters are secure.

Keywords: Key Derivation Functions, KDF, Provable Security, PRF, Encryption modes of operation.

I. 서 론

암호 알고리즘과 암호 프로토콜은 사용되는 키들의 기밀성이 유지된다는 가정 하에서 그 안전성을 보장받을 수 있다. 암호시스템 안에는 전반적으로 사용되는 키들을 안전하게 관리하는 키관리 메커니즘이 필수

접수일(2015년 3월 4일), 게재확정일(2015년 4월 27일)
* 본 연구는 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단-차세대정보 · 컴퓨팅기술개발사업의 지원을 받아 수행된 연구임(No. 2014M3C4A7030648).
† 주저자, izerotwo@kookmin.ac.kr
‡ 교신저자, jskang@kookmin.ac.kr(Corresponding author)

요소로 구현되어 있으며, 키관리 메커니즘의 내부에는 하나의 마스터키로부터 더 많은 종류의 키를 생성하는 키유도함수(key derivation function, 이하 KDF)가 존재한다. NIST SP 800-108[1]에서는 KDF에 대한 표준안으로 Counter 모드, Feedback 모드, Double‐Pipe line Iteration 모드라 불리는 세 가지 형태의 PRF-기반 KDF를 표준안으로 제안하고 있다. 이 표준안에는 KDF의 핵심 함수로 HMAC이나 CMAC과 같은 알고리즘을 PRF로 사용할 것을 권고하고 있다. 한편, NIST SP 800-108[1]이 발표된 지 여러 해가 지났음에도 불구하고 이에 대한 안전성 분석 관련 연구 결과는 매우 드문 실정이다.

본 논문에서는 먼저 KDF의 증명가능 안전성을 규명하기 위해 KDF와 암호화 운영모드의 안전성 분석 관점의 차이를 분석한다. 의사랜덤성을 기반으로 한 증명가능 안전성 분석에서 기존의 암호화 운영모드의 안전성 모델을 KDF에 동일하게 적용하는 것은 적절하지 않기 때문이다.

최근 저자들은 [2]에서 NIST가 제시한 PRF-기반 KDF를 변형한 형태인 카운터 값이 XOR 연산으로 입력되는 PRP-기반 KDF의 안전성을 분석하였다. 여기에서는 [2]에 제시된 사실보다 진전된 연구 결과로 NIST 표준안에서 권고하고 있는 형태인 카운터 값이 연접 연산으로 입력되는 PRF-기반 KDF의 안전성을 분석한다. 카운터 값의 입력 형태를 연접 연산으로 고려한 점과 핵심함수를 PRP에서 PRF로 확장했다는 점이 [2]에서 고려한 조건과 다르고, 이는 NIST의 표준안에서 권고된 사항을 충실히 따른 것이라 할 수 있다.

본 논문의 주요 연구 결과는 크게 다음 두 가지로 요약할 수 있다. 첫째, 카운터 값이 XOR 연산으로 입력되는 PRF-기반 KDF 중 Counter 모드와 Feedback 모드는 PRP-기반 하에서 분석한 [2]에서와 유사한 맥락으로 공격하였을 때, 확장된 랜덤함수족과 구별 가능하여 안전하지 않음을 밝힌다. 둘째, 카운터 값이 연접 연산으로 입력되는 PRF-기반 KDF의 Counter 모드와 Feedback 모드는 확장된 랜덤함수족과 구별 불가능함을 보임으로써 안전한 방식이라는 사실을 얻는다. 결과적으로 PRF-기반 KDF에서는 사소하게 생각할 수 있는 카운터 값의 입력 형태가 증명가능 안전성을 좌우하게 됨을 알 수 있다. 즉, PRF-기반 KDF인 Counter와 Feedback 모드는 카운터 값이 연접 연산 형태로 입력되면 안전한 반면, XOR 연산 형태로 입력되면 안전하지 않다는 사실을 얻게 된다.

II. KDF와 암호화 운영모드

카운터 값은 다중 블록의 식별 요소로 KDF와 암호화 운영모드(modes of operation)에서 자주 사용된다. KDF와 암호화 운영모드에서 카운터 값이 모두 사용되지만 카운터 값의 입력 형태에 따른 차이점은 존재한다. 핵심 함수가 블록암호와 같이 입·출력 길이가 동일한 PRP로 간주할 수 있는 환경에서는 카운터 값이 XOR 연산 형태로 삽입되는 것이 일반적이다. 암호화 운영모드 중 CTR-모드[6]와 KDF 중 Millenage[7]가 대표적인 경우이다.

한편, 핵심함수를 NIST SP 800-108[1]에서 권고하고 있는 것과 같이 입·출력 길이가 다른 PRF로 사용하는 KDF인 경우에는 카운터 값이 연접 연산 형태로 삽입된다. PRP는 PRF의 특별한 경우이므로 PRF-기반 KDF에 PRP가 적용되어도 무방하다. 하지만 PRP-기반 KDF로 한정해서 안전성을 분석할 경우 카운터 값의 입력 형태가 안전성을 좌우할 수도 있음을 본 논문의 결과로부터 알 수 있게 된다. 암호화 운영모드의 안전성 모델 하에서는 안전하다고 알려진 방식이 KDF의 안전성 모델에서는 안전하지 않을 수도 있는 것이다. 그러므로 먼저 KDF와 암호화 운영모드의 안전성 모델에 대한 정립이 필요하다.

2.1 KDF와 암호화 운영모드의 안전성 모델

KDF의 주된 목적은 객체들에 의해 서로 공유된 마스터키로부터 사용자 인증, 기밀성, 디지털 서명, 부인방지 등과 같이 다양한 기능의 보안 서비스를 위해 필요로 하는 여러 개의 키들을 유도해 내는 것이다. KDF의 안전성은 마스터키의 기밀성에 기반 하므로, 키 복구 공격에서 공격자의 이점으로 설명할 수 있다. 이 경우 공격자가 마스터키 값을 알아내기 위한 공격 시나리오를 생각할 수 있다. 3GPP의 보안 서비스를 위해 필요한 KDF인 Millenage[7]에서 보는 바와 같이 적용 환경이 결정되면 마스터키로부터 유도해내는 키들의 개수는 정해지는 것이 일반적이다. 그러므로 KDF의 안전성 분석은 PRF를 사용하는 하나의 확장된 함수족으로 KDF를 간주하고, 이를 확장된 랜덤함수족과 비교하였을 때의 구별가능성을 분석하는 것이 타당하다. 또한, 키 복구 공격의 이점은 이 구

별가능 공격의 이점으로 상계를 정할 수 있으므로 우리는 KDF의 안전성을 확장된 랜덤함수족과 비교하였을 때의 구별가능성 관점에서 탐구하고자 한다.

한편, 블록암호의 운영모드와 같은 암호화 운영모드의 목적은 가변적인 길이의 평문을 고정된 비밀키를 사용하여 암호화 하는 것이다. 암호화 운영모드의 증명가능 안전성은 비밀키를 복구하는 키 복구 공격에 안전해야 한다. 운영모드가 키 복구 공격에만 안전하다고 해서 증명가능 안전성을 보장하는 것은 아니다. 키는 모르지만 공격자가 암호문으로부터 평문에 대한 정보의 일부분을 알아낼 수 있는 경우도 있다. 암호문으로부터 평문을 알아내기 힘들게 하기 위해 운영모드의 입력에 현재 상태에 해당하는 카운터 값이나 랜덤한 초기 벡터와 같은 값을 사용한다. 카운터 값이나 초기벡터 값으로 인해 같은 입력값에 대응되는 출력값이 다르게 되고, 이는 암호화 운영모드의 안전성 목적에 부합하는 것이다.

암호화 운영모드의 증명가능 안전성은 운영모드의 입력값의 길이가 가변적이므로 KDF의 안전성 모델과는 다르다고 할 수 있다. 공격 시나리오 상에서 공격자가 오라클에게 보낼 수 있는 질의(query)의 형식이 본질적으로 다르기 때문에 KDF와 암호화 운영모드의 안전성 모델을 동일하게 적용할 수 없는 것이다. Bellare-Rogaway[3]에서 보는 바와 같이 암호화 운영모드의 안전성은 다양한 길이의 평문 쌍들로 구성된 질의(query)를 오라클에게 보낼 수 있는 공격 모델인 IND-CPA 공격 관점에서 안전성을 규명하는 것이 일반적이다.

2.2 암호화 운영모드의 증명가능 안전성

암호학계에서 KDF에 관한 연구가 상대적으로 활발히 이루어지지 않고 있는 반면, 블록암호 관련 연구 결과는 대단히 많은 편이다. KDF의 안전성 분석을 위해 참고할만한 암호화 운영모드의 증명가능 안전성 관련 연구 결과로는 Bellare-Rogaway[3]가 대표적이다. 이들은 블록암호를 핵심함수로 사용하는 암호화 운영모드에 관한 증명가능 안전성을 규명하기 위해 CTR과 CBC 운영모드를 입력되는 카운터 값의 랜덤성 유무에 따라 각각 CTRC, CTR$, CBCC, CBC$ 모드로 구분하였다. 그리고 IND-CPA 안전성 모델 하에서 CTRC, CTR$, CBC$ 모드는 안전한 반면, CBCC 모드는 안전하지 않다는 사실을 입증하였다.

III. PRF(pseudorandom function) 개념과 구별가능 안전성

KDF 구조의 견고성을 분석하기 위해서는 의사난수성 개념이 필요하다. 임의의 함수족과 그 함수족과 같은 정의역 및 치역을 가지는 랜덤함수족을 비교하였을 때, 두 함수족이 구별 불가능하다면 임의의 함수족이 의사난수성을 만족한다고 하고 이를 간단히 PRF(pseudorandom function)라고 정의한다. 일반적으로 블록암호 또는 해쉬함수 등과 같은 암호시스템의 핵심 알고리즘은 키공간의 균등한 분포에 의해 유도된 함수족으로 생각하여 PRF로 간주되는 것이 일반적이다. 본 논문에서 논할 KDF의 경우 핵심함수로 랜덤함수 또는 PRF를 사용하는 하나의 확장된 함수족으로 간주할 수 있다. 여기에서는 이 KDF 함수족을 확장된 랜덤함수족과 비교하였을 때의 구별가능성을 분석함으로써 KDF의 안전성을 논하고자 한다.

3.1 함수족(function family)

함수족은 키공간 $Keys$, 정의역 D, 치역 R로 하는 하나의 사상 $\mathfrak{I}: Keys \times D \rightarrow R$ 으로 키 $K \in Keys$와 임의의 $x \in D$를 입력값으로 하여, $y \in R$ 를 출력값으로 하는 이변수 함수로 생각할 수 있다. 임의의 키 $K \in Keys$에 대하여 $\mathfrak{I}_K: D \rightarrow R$ 는 $\mathfrak{I}_K(x) = \mathfrak{I}(K, x)$ 로 정의하며 $\mathfrak{I}_K$를 함수족 $\mathfrak{I}$의 인스턴스(instance)라고 한다. 그러면 키공간 $Keys$에서 키를 추출한 후 함수족 $\mathfrak{I}$의 한 원소인 하나의 함수가 대응되는 것으로 볼 수 있다. 함수족의 확률분포는 키공간의 확률분포에 기인한다. 본 논문에서는 특별한 언급이 없으면 키공간이 균등분포(uniform distribution)를 이루고 있다고 가정한다.

또한, 본 논문에서는 키공간, 정의역, 치역에 대한 특별한 언급이 없는 한 임의의 양의 정수 k, m, n에 대하여, $Keys = \{0,1\}^k$, $D = \{0,1\}^m$, $R = \{0,1\}^n$ 으로 나타낸다. 키공간 $Keys$로부터 임의의 K를 추출하는 것을 $K \leftarrow Keys$ 로 나타내고, 함수족 $\mathfrak{I}$에서 인스턴스 하나를 선택한다는 것은 $f \leftarrow \mathfrak{I}$ 로 표현하며, 이는 $K \leftarrow Keys$ 와 $f = \mathfrak{I}_K$ 를 의미한다.

3.2 PRF와 PRP 개념

PRF와 PRP(pseudorandom permutation)

개념을 정의하기 위해 특별한 두 개의 함수족을 고려하자. 하나는 D에서 R로 가는 모든 함수를 모아놓은 $Func(D,R)$이고, 다른 하나는 D에서 D로 가는 모든 치환을 모아놓은 $Perm(D)$이다. 균등분포를 이루고 있는 $Func(D,R)$에서 추출한 하나의 함수를 랜덤함수(random function)라 하고, 균등분포를 이루고 있는 $Perm(D)$에서 추출한 하나의 치환을 랜덤치환(random permutation)이라 정의한다. 참고로 랜덤함수족 $Func(D,R)$과 랜덤치환족 $Perm(D)$의 원소의 개수는 각각 $2^{n \cdot 2^m}$과 $2^m!$이다.

정의역과 치역이 고정된 랜덤함수족과 특정 함수족을 비교하였을 때, 계산적으로 구별 불가능한 성질을 만족하는 특정 함수족을 PRF라 하고, 이와 유사하게 랜덤치환족과 계산적으로 구별 불가능한 특정 치환족을 PRP라고 한다.

3.3 구별가능 안전성

구별가능 안전성을 분석하기 위하여 다음과 같은 안전성 모델을 설정하자. 공격자(adversary) A를 정의역과 치역이 고정된 랜덤함수족과 특정 함수족을 구별하는 알고리즘이라고 하자. 오라클은 랜덤함수 또는 특정 함수족의 인스턴스를 정확히 1/2의 확률로 한 번 선택하고, A는 오라클이 선택한 함수에 접근하여 유한개의 질의(query)를 입력할 수 있다. 오라클이 선택 가능한 함수 g를 형식적으로 표현하기 위하여 다음과 같이 두 가지 "World"를 고려하자.

World 0 : 오라클이 랜덤함수족 $Func(D,R)$에서 임의의 함수를 선택한다. 즉, $g \leftarrow Func(D,R)$을 통해서 함수 g가 결정된다.

World 1 : 오라클이 함수족 $\mathfrak{I}$에서 임의의 함수를 선택한다. 즉, $g \leftarrow \mathfrak{I}$를 통해서 함수 g가 결정된다.

공격자 A는 오라클이 둘 중에 어떤 것을 선택하였는지 알 수 없고, 질의가 계속되는 동안 오라클의 선택은 변하지 않는다. 오라클은 입력된 질의에 대해 선택한 함수 g의 출력을 A에게 응답(response)해준다. 공격자 A는 유한개의 질의와 응답의 결과를 바탕으로 g가 어떤 World로 부터 결정되었는지를 나타내는 한 비트 값 $b \in \{0,1\}$를 공격의 결과물로 출력한다. 이러한 안전성 모델은 다음과 같은 형식으로 정의할 수 있다.

정의 1. $\mathfrak{I}: Keys \times D \rightarrow R$ 를 하나의 주어진 함수족이라고 하자. 오라클은 World 0과 World 1 중에서 함수 $g: D \rightarrow R$ 를 선택한다. 공격자 A가 오라클이 선택한 g에 접근할 수 있고 한 비트 b를 출력하는 알고리즘일 때, 두 가지 실험(experiment)을 다음과 같이 나타낸다.

$Experiment\ \mathrm{Exp}_{\mathfrak{I}}^{prf-1}(A)$	$Experiment\ \mathrm{Exp}_{\mathfrak{I}}^{prf-0}(A)$
$K \leftarrow Keys$	$g \leftarrow Func(D,R)$
$b \leftarrow A^{\mathfrak{I}_K}$	$b \leftarrow A^{g}$
$Return\ b$	$Return\ b$

공격자 A의 이점(advantage) $Adv_{\mathfrak{I}}^{prf}(A)$는 다음과 같이 정의된다.

$$\begin{aligned} Adv_{\mathfrak{I}}^{prf}(A) &= \Pr\left[\mathrm{Exp}_{\mathfrak{I}}^{prf-1}(A)=1\right] \\ &\quad - \Pr\left[\mathrm{Exp}_{\mathfrak{I}}^{prf-0}(A)=1\right] \\ &= \Pr\left[A^{g}=1 | g \leftarrow \mathfrak{I}\right] \\ &\quad - \Pr\left[A^{g}=1 | g \leftarrow Func(D,R)\right]. \end{aligned}$$

정의 1에서 묘사한 안전성 모델을 도식화 한 것이 Fig.1이다.

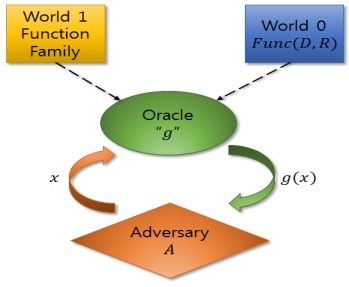

Fig. 1. prf-security model

IV. 카운터 값 입력 형태에 따른 PRF-기반 KDF

NIST는 SP 800-108[1]에서 특별한 내부 구조에 대한 설명 없이 PRF를 사용하는 세 가지의 KDF를 명시하고 있다. KDF의 핵심함수로 PRF의 특별한 경우인 PRP를 사용할 경우 카운터 값이 XOR 연산 형태로 입력되는 것이 일반적이다. 블록암호의 암호화

운영모드 중 CTR-모드[6]와 KDF 중 Millenage[7]가 카운터 값이 XOR 연산 형태로 입력되는 대표적인 경우이다. PRP-기반 KDF의 안전성을 분석한 결과는 [2]에 나타나 있다. 한편, 핵심함수로 PRF가 사용되는 경우에는 카운터 값이 XOR이나 연접 연산 형태로 입력되는 경우를 모두 고려해볼 수 있다. 그러므로 카운터 값이 XOR 또는 연접 연산으로 입력되는 경우 각각에 대한 안전성 분석 관점의 차이를 탐구해 볼 필요가 있다. 이를 위하여 먼저 카운터 값 입력 형태 차이에 대한 두 가지 모드를 엄밀하게 정의한다.

4.1 카운터 값 입력 형태에 따른 Counter 모드

카운터 값이 XOR 연산으로 입력되는 Counter 모드는 *CNT-X*, 카운터 값이 연접 연산으로 입력되는 Counter 모드는 *CNT-C*로 명명하자. 각각을 엄밀하게 정의하면 다음과 같다. 두 정수 m과 n에 대하여, G를 정의역이 $\{0,1\}^m$이고 공역이 $\{0,1\}^n$인 함수공간이라 한다.

정의 2. [*CNT-X* 모드] 임의의 함수 $g \in G$, 정수 $t \geq 2$, $c_1, c_2, \ldots, c_t \in \{0,1\}^m$에 대하여, *CNT-X* 모드는 다음과 같이 정의하고, 블록도는 Fig.2에 나타나 있다.

$$CNT-X[g]: \{0,1\}^m \rightarrow \{0,1\}^{nt},$$
$$CNT-X[g](x) = (g(x \oplus c_1), g(x \oplus c_2), \ldots, g(x \oplus c_t)).$$

정의 3. [*CNT-C* 모드] 임의의 함수 $g \in G$, 정수 $t \geq 2$, $\alpha(0 < \alpha < m)$, $c_1, c_2, \ldots, c_t \in \{0,1\}^\alpha$에 대하여, *CNT-C* 모드는 다음과 같이 정의하고, 블록도는 Fig.3에 나타나 있다.

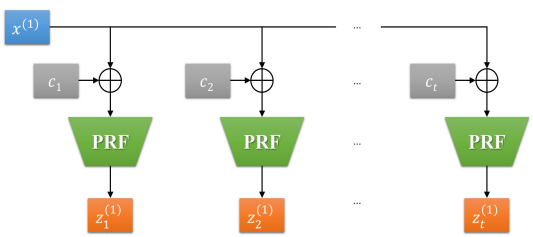

Fig. 2. *CNT-X* mode

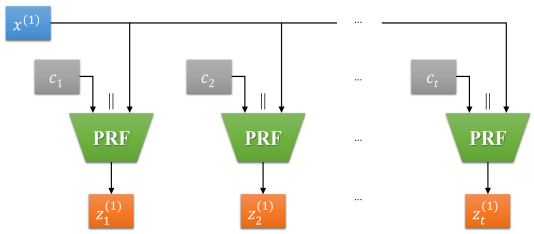

Fig. 3. *CNT-C* mode

$$CNT-C[g]: \{0,1\}^{m-\alpha} \rightarrow \{0,1\}^{nt},$$
$$CNT-C[g](x) = (g(c_1 \| x), g(c_2 \| x), \ldots, g(c_t \| x)).$$

4.2 카운터 값 입력 형태에 따른 Feedback 모드

카운터 값이 XOR 연산으로 입력되는 Feedback 모드는 *FB-X*, 카운터 값이 연접 연산으로 입력되는 Feedback 모드는 *FB-C*로 명명하고 다음과 같이 정의된다.

정의 4. [*FB-X* 모드] 임의의 함수 $g \in G$, 정수 $t \geq 2$, $c_1, c_2, \ldots, c_t \in \{0,1\}^m$에 대하여, *FB-X* 모드는 다음과 같이 정의하고, 블록도는 Fig.4에 나타나 있다.

$$FB-X[g]: \{0,1\}^m \rightarrow \{0,1\}^{nt},$$
$$FB-X[g](x) = (g(x \oplus c_1), g(x \oplus c_2 \oplus z_1), \ldots, g(x \oplus c_t \oplus z_{t-1})).$$

정의 5. [*FB-C* 모드] 임의의 함수 $g \in G$, 정수 $t \geq 2$, $\alpha(0 < \alpha < m-n)$, $c_1, c_2, \ldots, c_t \in \{0,1\}^\alpha$, $z_0 \in \{0,1\}^n$에 대하여, *FB-C* 모드는 다음과 같이 정의하고, 블록도는 Fig.5에 나타나 있다.

$$FB-C[g]: \{0,1\}^{m-\alpha-n} \rightarrow \{0,1\}^{nt},$$
$$FB-C[g](x) = (g(z_0 \| c_1 \| x), g(z_1 \| c_2 \| x), \ldots, g(z_{t-1} \| c_t \| x)).$$

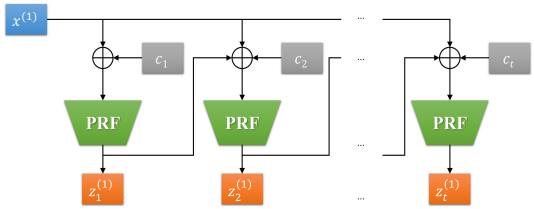

Fig. 4. *FB-X* mode

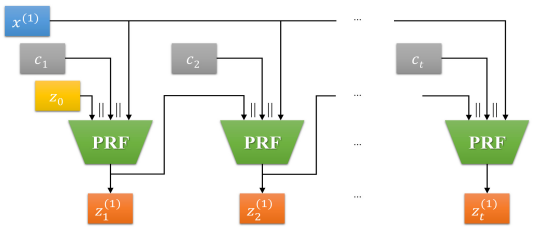

Fig.5. *FB-C* mode

V. 카운터 값 입력 형태에 따른 PRF-기반 KDF의 안전성

NIST SP 800-108[1]에서 KDF의 핵심함수로 권고하고 있는 HMAC이나 CMAC과 같은 해쉬함수는 PRF로 간주되는 것이 일반적이다. 카운터 값의 입력 형태에 따른 PRF-기반 KDF의 안전성을 규명하기 위해 4장에서 정의한 *CNT-X*, *CNT-C*, *FB-X*, *FB-C*로 구분하여 확장된 랜덤함수족과의 구별 가능성을 분석한다. 안전성 증명을 위하여 Patarin[5]에 의해 처음 제시된 매우 유용한 정리를 인용한다. 이 장에서는 정의역 $D=\{0,1\}^m$, 치역 $R=\{0,1\}^n$ 임을 다시 한 번 상기하자.

정리 1.[5] 함수족 $\mathfrak{I}$의 한 인스턴스를 $E: D \rightarrow R$ 라 하자. 랜덤함수 F에 대하여 E와 F를 구별하는 임의의 공격자를 A라 하자. $X \subset (\{0,1\}^m)^q$가 서로 다른 $\mathbf{x}=(x^{(1)}, x^{(2)}, \ldots, x^{(q)})$의 집합이라 하고, 다음 두 가지 조건

$$|Y| \geq (1-\epsilon_1) \cdot 2^{nq} \quad , \tag{1}$$

$$\forall \mathbf{x} \in X, \forall \mathbf{y} \in Y, \ \Pr[\mathbf{x} \xrightarrow{E} \mathbf{y}] \geq \frac{(1-\epsilon_2)}{2^{nq}} \tag{2}$$

를 만족하는 집합 $Y \subseteq (\{0,1\}^n)^q$와 양의 실수 ϵ_1, ϵ_2가 존재한다면, q개의 질의를 가지는 임의의 공격자 A에 대하여 다음을 만족한다.

$$\begin{aligned} Adv_{\mathfrak{I}}^{prf}(A) = &\Pr[A^E=1 | E \leftarrow \mathfrak{I}] \\ &- \Pr[A^F=1 | F \leftarrow Func(D,R)] \\ \leq &\ \epsilon_1 + \epsilon_2 \ . \end{aligned}$$

5.1 *CNT-X*와 *FB-X*의 비의사난수성

PRF의 입력값으로 카운터 값이 XOR 연산으로 입력되는 *CNT-X*와 *FB-X* 모드는 PRP-기반 KDF에 대한 연구 결과인 참고문헌 [4]와 [2]의 공격방법과 유사하게 PRF-기반 KDF의 경우라도 안전하지 않음을 밝힐 수 있다.

정리 2. [*CNT-X*의 비의사난수성] 임의의 랜덤함수 $\rho \in Func(D,R)$에 대하여 *CNT-X*[ρ]는 확장된 랜덤함수족과 구별가능하다.

증명. *CNT-X*가 확장된 랜덤함수족과 구별 가능함을 보이기 위하여 임의의 랜덤함수 ρ를 이용한 *CNT-X*[ρ]를 공격하는 특정한 공격자 하나를 구체적으로 명시하자. 정의 1의 안전성 모델에 의해 오라클은 함수 World 0과 1에서 확률 1/2로 함수 G를 선택하고 공격자 A는 오라클이 선택한 함수 G에 접근하여 구동한다. World 0에서는 G에 확장된 랜덤함수가 선택되고 World 1에서는 랜덤함수 ρ를 사용하는 *CNT-X*[ρ]가 G에 선택된다. 이 때 공격자 A를 다음과 같이 구성한다.

Adversary A^G

$(z_1^{(1)}, \ldots, z_t^{(1)}) \leftarrow G(x^{(1)})$
$(z_1^{(2)}, \ldots, z_t^{(2)}) \leftarrow G(x^{(2)} = x^{(1)} \oplus c_1 \oplus c_2)$
if $z_1^{(1)} = z_2^{(2)}$ and $z_2^{(1)} = z_1^{(2)}$
then return 1
else return 0

만일 임의의 ρ에 대하여 $G = CNT\text{-}X[\rho]$이면 $z_1^{(1)} = z_2^{(2)}$와 $z_2^{(1)} = z_1^{(2)}$는 항상 성립한다. 반면에 만약 G가 확장된 랜덤 함수이면 $z_1^{(1)} = z_2^{(2)}$와 $z_2^{(1)} = z_1^{(2)}$이 성립할 확률은 2^{-2n}이다. 그러므로 공격자 A의 이점은 다음과 같다.

$$Adv_{CNT-X}^{prf}(A) = 1 - 2^{-2n} \ .$$

위와 같이 *CNT-X*에 대한 공격자의 이점이 거의 1에 가까운 효과적인 공격자 하나를 직접 구성할 수 있으므로 *CNT-X*는 확장된 랜덤함수족과 구별가능하다. □

정리 3. [*FB-X*의 비의사난수성] 임의의 랜덤함수 $\rho \in Func(D,R)$에 대하여 *FB-X*[ρ]는 확장된 랜

덤함수족과 구별가능하다.

증명. $FB\text{-}X$가 확장된 랜덤함수족과 구별 가능함을 보이기 위해 임의의 랜덤함수 ρ에 대하여 $FB\text{-}X[\rho]$를 공격하는 특정한 공격자를 구성하자. 정의 1의 안전성 모델에 의해 오라클은 함수 World 0과 1에서 확률 1/2로 함수 G를 선택하고 공격자 A는 오라클이 선택한 함수 G에 접근하여 구동한다. World 0에서는 G에 확장된 랜덤함수가 선택되고 World 1에서는 랜덤함수 ρ를 사용하는 $FB\text{-}X[\rho]$가 G에 선택된다. 이 때 공격자 A를 다음과 같이 구성한다.

$Adversary\ A^{G}$

$\left(z_1^{(1)},\dots,z_t^{(1)}\right) \leftarrow G\left(x^{(1)}\right)$
$\left(z_1^{(2)},\dots,z_t^{(2)}\right) \leftarrow G\left(x^{(2)}=x^{(1)}\oplus c_1\oplus c_2\oplus z_1^{(1)}\right)$
if $z_1^{(2)}=z_2^{(1)}$ **then return** 1
else return 0

두 번째 질의 $x^{(2)}$를 선택할 때 $z_1^{(1)}$의 값은 m-비트로 패딩이 되어 있는 값을 선택하여 XOR 연산을 하여야 한다. 이것은 첫 번째 질의 $x^{(1)}$에서 $t=2$일 때 $z_1^{(1)}$값이 랜덤함수 ρ의 패딩규칙에 따라 m-비트로 패딩되고 이 값이 다시 c_2와 $x^{(1)}$과 XOR 연산되는 것과 동일하다. 만일 위의 과정으로 질의를 선택하여 공격할 때 ρ에 대하여 $G=FB\text{-}X[\rho]$이면 $z_1^{(2)}=\rho\left(x^{(1)}\oplus c_2\oplus z_1^{(1)}\right)=z_2^{(1)}$ 이다. 반면에 G가 확장된 랜덤함수이면 $z_1^{(2)}=z_2^{(1)}$ 이 성립할 확률은 2^{-n} 이다. 그러므로 공격자 A의 이점은 다음과 같다.

$$Adv_{FB-X}^{prf}(A)=1-2^{-n}\ .$$

위와 같이 $FB\text{-}X$에 대한 공격자 이점이 거의 1에 가까운 공격자 하나를 구성하였으므로 $FB\text{-}X$는 확장된 랜덤함수족과 구별가능하다. □

5.2 $CNT\text{-}C$와 $FB\text{-}C$의 의사난수성

구별가능 안전성 분석에 적용한 정리 1을 이용하여 $CNT\text{-}C$와 $FB\text{-}C$가 확장된 랜덤함수족과 구별 불가능함을 보이자. 실제적으로 HMAC이나 CMAC은 키공간에서 랜덤하게 키 K를 추출하는 암호적 함수 $\mathfrak{I}_K$로 간주할 수 있으며 이와 같은 암호적 함수는 PRF라 가정할 수 있다. 구별가능 안전성 관점에서 PRF-기반 KDF의 안전성을 증명하기 위해서는 먼저 핵심함수로 랜덤함수가 사용되는 KDF를 확장된 랜덤함수족과 구별하는 공격자 A의 이점을 구한다. 이를 이용하여 KDF의 핵심함수로 사용되는 $\mathfrak{I}_K$를 랜덤함수와 구별하는 공격자 B의 존재성을 밝히고, B의 이점을 구하면 된다.

정리 4. 〔$CNT\text{-}C[\rho]$의 의사난수성〕 임의의 랜덤함수 $\rho\in Func(D,R)$를 이용한 $CNT\text{-}C[\rho]$에 대하여, q개의 질의를 사용하는 임의의 공격자 A의 이점은 다음을 만족한다.

$$Adv_{CNT-C[\rho]}^{prf}(A)\le\frac{t^2q^2}{2^{n+1}}\ .$$

증명. $x^{(i)}\neq x^{(j)}\,(1\le i\neq j\le q)$ 를 만족하는 $\mathbf{x}=(x^{(1)},x^{(2)},\dots,x^{(q)})$들의 집합을 $X\subset\left(\{0,1\}^{m-\alpha}\right)^q$ 라 하고, $Z\subset\left(\{0,1\}^{nt}\right)^q$ 는 서로 다른 tq개의 $\{0,1\}^n$ 상의 원소들인 $z_k^{(i)}(1\le i\le q,1\le k\le t)$들로 구성된 $\mathbf{z}=\left((z_1^{(1)},z_2^{(1)},\dots,z_t^{(1)}),\ \dots\ ,(z_1^{(q)},z_2^{(q)},\dots,z_t^{(q)})\right)$들 의 집합이라 하자. 정리 1을 적용하기 위하여 위의 집합 Z에 대하여 다음을 만족하는 양의 실수 ϵ_1과 ϵ_2가 존재함을 보이자.

$$|Z|\ge(1-\epsilon_1)\cdot 2^{ntq}\ ,$$
$$\forall\,\mathbf{x}\in X,\ \forall\,\mathbf{z}\in Z,$$
$$\Pr[\mathbf{x}\xrightarrow{CNT-C[\rho]}\mathbf{z}]\ge\frac{(1-\epsilon_2)}{2^{ntq}}.$$

우선 $|Z|\ge(1-\epsilon_1)\cdot 2^{ntq}$ 를 살펴보면,

$$\begin{aligned}\frac{|Z|}{2^{ntq}}&=\frac{2^n\cdot(2^n-1)\cdots(2^n-tq+1)}{2^{ntq}}\\&=1\cdot\left(1-\frac{1}{2^n}\right)\cdots\left(1-\frac{1}{2^n}\right)\\&\ge 1-\frac{1}{2^n}(1+2+\cdots+(tq-1))\\&=1-\frac{1}{2^n}\left(\frac{(tq-1)tq}{2}\right)\\&\ge 1-\frac{t^2q^2}{2^{n+1}}\end{aligned}$$

이 성립하므로 $\epsilon_1=\frac{t^2q^2}{2^{n+1}}$ 이라 놓으면 첫 번째 조건을 만족한다.

두 번째 조건이 성립함을 보이기 위해 $\mathbf{x}\in X$와 $\mathbf{z}\in Z$을 고정하자. 고정된 $\mathbf{x}$, $\mathbf{z}$에 대하여 전환확률 $\Pr[\mathbf{x}\xrightarrow{CNT-C[\rho]}\mathbf{z}]$을 고려하기 위해 PRF의 입력값의 중간 값 $\mathbf{y}$를 정의하자. 임의의 i와 k에 대하여 $y_k^{(i)}=c_k\|x^{(i)}$라 두면 $y_k^{(i)}$는 m-비트이고 랜덤함수 ρ의 입력값이 된다. 또한 임의의 서로 다른 i,j에 대하여 $x^{(i)}\neq x^{(j)}$이므로 $y_k^{(i)}\neq y_k^{(j)}$이며, 서로 다른 k,l에 대하여 $c_k\neq c_l$ 이므로 $y_k^{(i)}\neq y_l^{(i)}$이다. 그러므로 임의의 i와 k에 대하여 $y_k^{(i)}$는 모두 다른 값이다. $\mathbf{y}=\left((y_1^{(1)},y_2^{(1)},\dots,y_t^{(1)}),\dots,(y_1^{(q)},y_2^{(q)},\dots,y_t^{(q)})\right)$라 두면 고정된 $\mathbf{x}$, $\mathbf{z}$에 대하여 $\mathbf{y}$ 역시 고정된 값이다. 따라서 임의의 i와 k에 대하여 랜덤함수 ρ의 고정된 tq개의 입력값이 고정된 tq개의 출력값으로 가는 함수 이므로 전환확률은 다음과 같다.

$$\begin{aligned}\Pr[\mathbf{x}\xrightarrow{CNT-C[\rho]}\mathbf{z}]&=\Pr[\mathbf{y}\xrightarrow{CNT-C[\rho]}\mathbf{z}]\\&=\Pr[y_k^{(i)}\xrightarrow{\rho}z_k^{(i)}]\\&=\frac{\left(2^n\right)^{2^m-tq}}{\left(2^n\right)^{2^m}}=\frac{1}{2^{ntq}}\ .\end{aligned}$$

그러므로 $\epsilon_2=0$으로 놓으면, 두 번째 조건을 만족한다. 따라서 정리 1에 의해

$$Adv^{prf}_{CNT-C[\rho]}(A)\le\epsilon_1+\epsilon_2=\frac{t^2q^2}{2^{n+1}}$$

을 얻는다. □

정리 5. 〔FB-$C[\rho]$의 의사난수성〕 임의의 랜덤함수 $\rho\in Func(D,R)$일 때, FB-$C[\rho]$에 대하여 q개의 질의를 사용하는 임의의 공격자를 A라 하면 다음을 만족한다.

$$Adv^{prf}_{FB-C[\rho]}(A)\le\frac{t^2q^2}{2^{n+1}}\ .$$

증명. $x^{(i)}\neq x^{(j)}(1\le i\neq j\le q)$ 를 만족하는 $\mathbf{x}=(x^{(1)},x^{(2)},\dots,x^{(q)})$들의 집합을 $X\subset\left(\{0,1\}^{m-\alpha-n}\right)^q$라 하고, $Z\subset\left(\{0,1\}^{nt}\right)^q$ 는 서로 다른 tq개의 $\{0,1\}^n$ 상의 원소들인 $z_k^{(i)}(1\le i\le q,1\le k\le t)$들로 구성된 $\mathbf{z}=\left((z_1^{(1)},z_2^{(1)},\dots,z_t^{(1)}),\ \dots\ ,(z_1^{(q)},z_2^{(q)},\dots,z_t^{(q)})\right)$들의 집합이라 하자. 정리 1을 적용하기 위하여 위의 집합 Z에 대하여 다음을 만족하는 양의 실수 ϵ_1과 ϵ_2가 존재함을 보이자.

$$|Z|\ge(1-\epsilon_1)\bullet 2^{ntq}\ ,$$
$$\forall\,\mathbf{x}\in X,\forall\,\mathbf{z}\in Z,\quad \Pr[\mathbf{x}\xrightarrow{FB-C[\rho]}\mathbf{z}]\ge\frac{(1-\epsilon_2)}{2^{ntq}}.$$

우선 $|Z|\ge(1-\epsilon_1)\bullet 2^{ntq}$ 를 살펴보면,

$$\begin{aligned}\frac{|Z|}{2^{ntq}}&=\frac{2^n\bullet(2^n-1)\cdots(2^n-tq+1)}{2^{ntq}}\\&=1\bullet\left(1-\frac{1}{2^n}\right)\cdots\left(1-\frac{1}{2^n}\right)\\&\ge 1-\frac{1}{2^n}(1+2+\cdots+(tq-1))\\&=1-\frac{1}{2^n}\left(\frac{(tq-1)tq}{2}\right)\ge 1-\frac{t^2q^2}{2^{n+1}}\end{aligned}$$

이 성립하므로 $\epsilon_1=\frac{t^2q^2}{2^{n+1}}$이라 놓으면 첫 번째 조건을 만족한다.

두 번째 조건이 성립함을 보이기 위해 $\mathbf{x}\in X$, $\mathbf{z}\in Z$ 을 고정하자. 고정된 $\mathbf{x}$, $\mathbf{z}$에 대하여 전환확률 $\Pr[\mathbf{x}\xrightarrow{FB-C[\rho]}\mathbf{z}]$를 고려하기 위해 PRF의 입력값의 중간 값 $\mathbf{y}$를 정의하자. 임의의 i,j에 대하여 $z_0^{(i)}=z_0^{(j)}=z_0$ 라 두고 임의의 i와 k에 대하여 $y_k^{(i)}=z_{k-1}^{(i)}\|c_k\|x^{(i)}$라 두면 $y_k^{(i)}$는 m-비트이고 랜덤함수 ρ의 입력값이 된다. 또한 임의의 서로 다른 i,j에 대하여 $x^{(i)}\neq x^{(j)}$ 이므로 $y_k^{(i)}\neq y_k^{(j)}$ 이며 서로 다른 k,l에 대하여 $c_k\neq c_l$ 이므로 $y_k^{(i)}\neq y_l^{(i)}$ 이다. 그러므로 임의의 i,k에 대하여 $y_k^{(i)}$는 모두 다른 값이다. $\mathbf{y}=\left((y_1^{(1)},\dots,y_t^{(1)}),\dots,(y_1^{(q)},\dots,y_t^{(q)})\right)$라 두면 고정된 $\mathbf{x}$, $\mathbf{z}$에 대하여 $\mathbf{y}$ 역시 고정된 값이다. 따라서 임의의 i와 k에 대하여 랜덤함수 ρ의 고정된 tq개의 입력값이 고정된 tq개의 출력값으로 가는 함수이므로 전환확률은 다음과 같다.

$$\begin{aligned}\Pr[\mathbf{x}\xrightarrow{FB-C[\rho]}\mathbf{z}]&=\Pr[\mathbf{y}\xrightarrow{FB-C[\rho]}\mathbf{z}]\\&=\Pr[y_k^{(i)}\xrightarrow{\rho}z_k^{(i)}]\\&=\frac{\left(2^n\right)^{2^m-tq}}{\left(2^n\right)^{2^m}}=\frac{1}{2^{ntq}}\ .\end{aligned}$$

그러므로 $\epsilon_2 = 0$으로 놓으면, 두 번째 조건을 만족한다. 따라서 정리 1에 의해

$$Adv^{prf}_{FB-C[\rho]}(A) \le \epsilon_1 + \epsilon_2 = \frac{t^2q^2}{2^{n+1}}$$

을 얻는다. □

핵심함수로 $\mathfrak{I}_K$를 사용한 KDF와 확장된 랜덤함수족이 구별 불가능함을 보이기 위해서는 $\mathfrak{I}_K$를 랜덤함수 ρ와 구별하는 공격자 B의 존재성을 밝히면 된다.

정리 6. 〔CNT-$C[\mathfrak{I}_K]$의 의사난수성〕 q개의 질의를 이용하여 CNT-$C[\mathfrak{I}_K]$를 확장된 랜덤함수족과 구별하는 임의의 공격자를 A라고 하면, tq개의 질의를 이용하여 함수족 $\mathfrak{I}$의 인스턴스 $\mathfrak{I}_K$와 랜덤함수 $\rho \in Func(D,R)$를 구별할 수 있는 공격자 B가 존재해서 다음을 만족한다.

$$Adv^{prf}_{CNT-C[\mathfrak{I}_K]}(A) \le Adv^{prf}_{\mathfrak{I}}(B) + \frac{t^2q^2}{2^{n+1}} .$$

증명. $\mathfrak{I}_K$를 공격하는 특정한 공격자 B를 구체적으로 명시하자. B에 대응되는 오라클은 World 0과 1에서 확률 1/2로 함수 g를 선택하고, B는 오라클이 선택한 함수 g에 접근하여 구동한다. World 0에서는 g에 랜덤함수 ρ가 선택되고, World 1에서는 키공간에서 랜덤하게 선택한 K에 의해 유도된 $\mathfrak{I}_K$가 선택된다. 공격자 B는 공격자 A를 서브루틴으로 이용한 시나리오에 의하여 공격한다. 이 때 A 역시 A에 대응되는 오라클이 필요하므로 공격자 B가 A의 오라클 역할을 시뮬레이션 한다.

Adversary B^g
Run adversary A,
replying to its oracle queries as follows:
  For $i = 1, \dots, q$ do
  When A makes an oracle query $x^{(i)}$
    $\mathbf{z}^{(i)} = \left(z_1^{(i)}, \dots, z_t^{(i)}\right) \hookleftarrow CNT-C[g(x^{(i)})]$
    Return $\mathbf{z}^{(i)}$ to A as the answer
  Until A stops and outputs a bit, b
Return b

위에서 구성한 시나리오에서 A가 질의 $x^{(i)}$를 자신의 오라클에게 보낼 때, 공격자 B가 관여하여 A의 오라클처럼 행동한다. 여기에서 B는 A로부터 받은 $x^{(i)}$를 CNT-C 모드의 입력 서식에 맞게 카운터 값을 연접한 후 B의 오라클에 t개의 질의를 보낸다. 그러면 B의 오라클은 선택된 g로부터 계산된 $g(c_1 \| x^{(i)})$, …, $g(c_t \| x^{(i)})$를 응답하게 되고, 이 출력값으로부터 B는

$$CNT\text{-}C[g](x^{(i)}) = (g(c_1 \| x^{(i)}), \dots, g(c_t \| x^{(i)}))$$

를 A의 오라클 응답처럼 출력한다. 정의 1에 의해 B의 이점은 다음과 같다.

$$Adv^{prf}_{\mathfrak{I}}(B) = \Pr[B^g = 1 | g \leftarrow \mathfrak{I}] - \Pr[B^g = 1 | g \leftarrow Func(D,R)] .$$

한편, B^g가 마지막에 출력하는 b는 A가 출력하는 비트 값과 일치하므로 "$B^g = 1$"인 사건과 "$A^G = 1$"인 사건은 동일하다. 더욱이 공격 시나리오에 의하여 B의 오라클이 g를 $\mathfrak{I}$에서 선택하는 경우는 A의 오라클 입장에서는 G가 CNT-$C[\mathfrak{I}_K]$로부터 선택된 것과 같고, B의 오라클이 g를 $Func(D,R)$에서 선택하는 경우는 A의 오라클 입장에서는 CNT-$C[\rho]$로부터 G가 선택된 것과 같으므로,

$$\Pr[B^g = 1 | g \leftarrow \mathfrak{I}] = \Pr[A^G = 1 | G \leftarrow CNT-C[\mathfrak{I}_K]]$$
$$\Pr[B^g = 1 | g \leftarrow Func(D,R)] = \Pr[A^G = 1 | G \leftarrow CNT-C[\rho]]$$

이 성립한다. 따라서 확장된 랜덤함수족을 $\overline{Func}$로 표시하면,

$$\begin{aligned} Adv^{prf}_{\mathfrak{I}}(B) &= \Pr[B^g = 1 | g \leftarrow \mathfrak{I}] - \Pr[B^g = 1 | g \leftarrow Func(D,R)] \\ &= \Pr[A^G = 1 | G \leftarrow CNT-C[\mathfrak{I}_K]] - \Pr[A^G = 1 | G \leftarrow CNT-C[\rho]] \\ &= \Pr[A^G = 1 | G \leftarrow CNT-C[\mathfrak{I}_K]] - \Pr[A^G = 1 | G \leftarrow \overline{Func}] + \Pr[A^G = 1 | G \leftarrow \overline{Func}] - \Pr[A^G = 1 | G \leftarrow CNT-C[\rho]] \\ &= Adv^{prf}_{CNT-C[\mathfrak{I}_K]}(A) - Adv^{prf}_{CNT-C[\rho]}(A) . \end{aligned}$$

결과적으로 정리 4에 의해서

$$Adv^{prf}_{CNT-C[\mathfrak{I}_K]}(A) = Adv^{prf}_{\mathfrak{I}}(B) + Adv^{prf}_{CNT-C[\rho]}(A) \le Adv^{prf}_{\mathfrak{I}}(B) + \frac{t^2q^2}{2^{n+1}}$$

을 얻는다. □

정리 7. 〔*FB-C*[$\mathfrak{I}_K$]의 의사난수성〕 q개의 질의를 이용하여 *FB-C*[$\mathfrak{I}_K$]를 확장된 랜덤함수족과 구별하는 임의의 공격자를 A라고 하면, tq개의 질의를 이용하여 함수족 $\mathfrak{I}$의 인스턴스 $\mathfrak{I}_K$와 랜덤함수 $\rho \in Func(D,R)$를 구별할 수 있는 공격자 B가 존재해서 다음을 만족한다.

$$Adv^{prf}_{FB-C[\mathfrak{I}_K]}(A) \le Adv^{prf}_{\mathfrak{I}}(B) + \frac{t^2q^2}{2^{n+1}}.$$

정리 7의 증명은 정리 6의 증명 과정과 매우 유사하므로 생략한다.

VI. 결 론

본 논문에서는 KDF의 증명가능 안전성을 규명하기 위해 KDF와 암호화 운영모드의 안전성 관점의 차이를 밝히고, 최근 발표된 사실보다 진전된 연구 결과로 NIST 표준안에서 권고하고 있는 형태인 카운터 값이 연접 연산으로 입력되는 PRF-기반 KDF의 안전성을 분석하였다. 본 논문의 주요 연구 결과는 크게 두 가지로 요약할 수 있다. 첫째, 카운터 값이 XOR 연산으로 입력되는 PRF-기반 KDF 중 Counter 모드와 Feedback 모드는 PRP-기반 하에서 분석한 〔2〕에서와 유사한 맥락으로 공격하였을 때 확장된 랜덤함수족과 구별 가능함을 보였다. 둘째, 카운터 값이 연접 연산으로 입력되는 PRF-기반 KDF의 Counter 모드와 Feedback 모드는 확장된 랜덤함수족과 구별 불가능함을 보임으로써 의사난수성을 만족한다는 사실을 얻었다. 이에 따라 PRF-기반 KDF에서는 사소하게 생각할 수 있는 카운터 값의 입력 형태가 증명가능 안전성을 좌우하게 된다는 사실을 알 수 있었다. 즉, PRF-기반 KDF인 Counter와 Feedback 모드는 카운터 값이 연접 연산 형태로 입력되면 안전한 반면, XOR 연산 형태로 입력되면 안전하지 않다는 사실을 밝힌 것이다.

한편, NIST 표준안에 제시되어 있는 나머지 다른 하나인 Double-Pipe line Iteration 모드는 〔2〕에서 PRP-기반으로 카운터 값이 XOR 형태로 입력되는 변형된 모드에 대해서 안전성이 입증되었다. 그러므로 이 변형된 모드의 경우 핵심함수를 PRF로 확장하여도 안전할 것이라 예상된다. 하지만 구조의 복잡성 때문에 안전성 규명이 단순하지는 않을 것으로 보인다. 후속 연구를 통하여 이것 역시 규명되어야 할 것이라 생각된다.

References

〔1〕 L. Chen, "Recommendation for key derivation using pseudorandom functions," NIST Special Publication 800-108, Oct. 2009.

〔2〕 Ju-Sung Kang, Nayoung Kim, Wangho Ju and Ok-Yeon Yi, "A security analysis of key expansion functions using pseudorandom permutations," Workshop in Information Security Theory and Practice 2014, LNCS 8501, pp. 10-23, June 2014.

〔3〕 M. Bellare and P. Rogaway, "Introduction to Mordern Cryptography," Available at http://cseweb.ucsd.edu/mihir/cse207/classnotes.html.

〔4〕 H. Gilbert, "The security of one-block-to-many modes of operation," Fast Software Encryption 2003, LNCS 2887, pp. 376-395, Feb. 2003.

〔5〕 J. Patarin, "How to construct pseudorandom and super pseudorandom permutations from one single pseudorandom function," Advances in Cryptology - EUROCRYPT 1992, LNCS 658, pp. 256-266, May 1992.

〔6〕 M. Dworkin, "Recommendation for block cipher modes of operation," NIST Special Publication 800-38A, Dec. 2001.

〔7〕 3rd Generation Partnership Project, "Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1,f1*,f2,f3,f4,f5 and f5*," 3GPP TS 35.206 v9.0.0, Dec. 2009.

〈저자소개〉

김 나 영 (Nayoung Kim) 학생회원
2005년 2월: 국민대학교 수학과 학사
2012년 2월: 국민대학교 수학교육학과 석사
2012년 9월~현재: 국민대학교 일반대학원 금융정보보안학과 박사과정
〈관심분야〉 정보보호론, 안전성 분석 및 평가

강 주 성 (Ju-Sung Kang) 종신회원
1989년 2월: 고려대학교 수학과 학사
1991년 2월: 고려대학교 일반대학원 수학과 석사
1996년 2월: 고려대학교 일반대학원 수학과 박사
1997년~2004년: 한국전자통신연구원 선임연구원/팀장
2001년~2002년, 2010년 벨기에 루벤대학 COSIC 방문 연구원
2004년~현재: 국민대학교 수학과 교수
2013년~현재: 국민대학교 BK21+ 미래 금융정보보안 인력양성사업단 교수
〈관심분야〉 암호이론, 정보보안 프로토콜, 안전성 분석 및 평가

염 용 진 (Yongjin Yeom) 종신회원
1991년 2월: 서울대학교 수학과 학사
1994년 2월: 서울대학교 수학과 석사
1999년 2월: 서울대학교 수학과 박사
2000년 4월~2012년 2월: ETRI 부설연구소 책임연구원/팀장
2006년 12월~2007년 12월: Columbia 대학교 방문 연구원
2012년 3월~현재: 국민대학교 수학과 부교수
2013년~현재: 국민대학교 BK21+ 미래 금융정보보안 인력양성사업단 교수
〈관심분야〉 암호구현 및 분석, 보안시스템 평가