情報保護學會論文誌
第20卷 第4號, 2010. 8

블록암호 기반 키유도함수의 증명가능 안전성*

강 주 성†‡, 이 옥 연, 염 지 선
국민대학교 수학과

Provable Security of Key Derivation Functions Based on the Block Ciphers*

Ju-Sung Kang, Okyeon Yi, and Ji-Sun Youm
Department of Mathematics, Kookmin University

요 약

키유도함수는 고정된 길이의 키로부터 정보보호 알고리즘 수행을 위하여 필요로 하는 다양한 키들을 유도해내는 메커니즘으로 암호시스템의 필수적인 구성요소이다. 본 논문에서는 키유도함수에 대한 최신 연구 동향을 조사 분석하고 증명가능 안전성 관점에서 키유도함수 구조의 견고성에 대하여 논한다. 특히 NIST가 최근 제안한 의사난수함수(PRF) 기반 키유도함수 모드를 블록암호로 대표되는 의사난수치환(PRP) 기반 키유도함수로 변형할 경우의 증명 가능 안전성에 초점을 맞추어 Double-Pipeline Iteration 모드의 의사난수성을 규명한다.

ABSTRACT

Key derivation functions are used within many cryptographic systems in order to generate various keys from a fixed short key string. In this paper we survey a state-of-the-art in the key derivation functions and wish to examine the soundness of the functions on the view point of provable security. Especially we focus on the key derivation functions using pseudorandom functions which are recommended by NIST recently, and show that the variant of Double-Pipeline Iteration mode using pseudorandom permutations is a pseudorandom function. Block ciphers can be regarded as practical primitives of pseudorandom permutations.

Keywords: Key derivation function, Provable security, Pseudorandom function, Pseudorandom permutation, Modes of operation.

I. 서 론

키유도함수(key derivation function, 이하 KDF)는 마스터키나 패스워드 같은 비밀 정보로부터 각종 정보보호 알고리즘 실행을 위하여 필요로 하는 다양한 키들을 유도해내는 메커니즘이다. KDF는 마스터키가 암호통신을 위한 대칭키나 랜덤수 생성을 위한 시드(seed)처럼 직접적으로 사용되기를 원치 않을 때, 마스터키와 다른 데이터를 입력하여 직접 사용될 키들을 유도해내는 과정이다. 즉, KDF는 키 확장 기능을 제공하며, 단일키로부터 여러 개의 키를 생성하는 것을 가능하게 해준다. 대칭키 하나를 공유하고 있는 개체들이 키 설정 과정에서 이 대칭키로부터 추가적인 키들을 유도해내는 것이 필요한 경우가 일반적이다. 추가적으로 유도된 키들은 분리되어 서로 다른 암호적 기능을 위해서 사용된다. 암호화 키(encryption key)와 무결성 키(integrity key)를 서로 다르게 사용하는 것은 키 분리 정책의 좋은 예라 할 수 있다. 또한, 신뢰성을 갖는 중앙 서버에서 한 개의 마스터키로부터 각 사용자마다 개별화된 키들을 여러 개체들에게 배포할 경우에도 KDF는 사용된다.

* 접수일(2009년 12월 23일), 수정일(1차: 2010년 3월 25일), 게재확정일(2010년 4월 30일)
* 본 연구는 국민대학교 교내연구비 및 (주)유비즈코아 지원으로 수행하였음.
† 주저자, jskang@kookmin.ac.kr
‡ 교신저자, jskang@kookmin.ac.kr

정보보호시스템 내에 각종 암호 기능이 탑재될 경우 위에서 보는 바와 같이 KDF는 필수적인 구성 요소가 된다. KDF가 정보보호시스템에서 반드시 필요한 요소임에도 불구하고 이에 대한 연구 결과는 상대적으로 빈약하다. 대칭키 암호 알고리즘, 공개키 암호 알고리즘, 해쉬함수, 난수발생기 등의 암호시스템 구성 요소들에 대해서는 그동안 활발히 연구되어 왔고 여전히 많은 학자들의 연구 대상이 되고 있다. 이에 비하면 KDF에 대한 연구는 이제 걸음마 단계에 놓여 있다고 할 수 있다.

정보보호시스템의 필수 요소인 만큼 표준화 되어 있는 KDF의 종류도 다양하다. ISO-18033-2[1], IEEE P1363a[2], PKCS#1 v2.1[3], ANSI X9.42[4], NIST SP800-56A[5], IEEE 802.11i[6] 등에는 해쉬함수가 핵심함수로 사용되는 KDF가 나타나 있으며, PKCS#5[7]와 참고문헌 [8]에는 핵심함수가 해쉬함수인 패스워드 기반 KDF가 기술되어 있다. 한편, 3GPP TR 35.909[9]와 IEEE 802.15.1^{TM}[10]에서는 블록암호를 핵심함수로 사용하는 KDF를 표준으로 제안하고 있으며, NIST 표준문서 SP800-108[11]에는 PRF(pseudorandom function)를 핵심함수로 사용하는 KDF의 세 가지 유형을 추천하고 있다.

의사난수함수인 PRF는 입출력 공간의 크기가 동일한 경우에는 일대일 대응이 가능한 치환 형태의 의사난수치환인 PRP(pseudorandom permutation)로 특수화 가능하다. 실제 구현 시 키가 알려지지 않은 상태의 블록암호는 PRP의 대표적인 예로 간주되는 것이 일반적이므로 NIST SP800-108에 나타나 있는 세 가지 유형의 KDF들을 PRF 기반이 아닌 PRP 기반 KDF로 변형할 경우에는 블록암호 기반 KDF로 분류하는 것이 타당하다. 본 논문에서 우리는 NIST가 제안한 PRF 기반 KDF를 블록암호로 대표되는 PRP 기반 KDF로 변형한 유형에 대한 의사난수성 관점의 안전성 분석 결과를 제시하고자 한다.

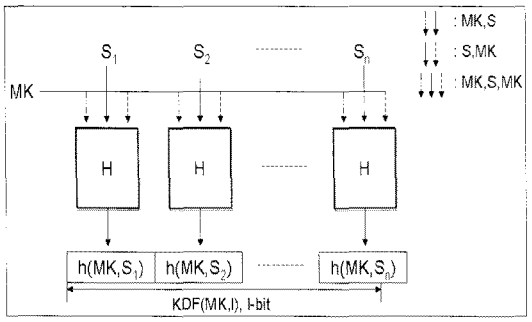
현재까지 KDF가 각종 정보보호시스템 표준에 필수적으로 나타나 있을 만큼 중요한 요소임에도 불구하고 이에 대한 안전성 분석 관련 연구 결과는 매우 빈약한 실정이다. KDF에 대한 안전성 문제를 본격적으로 다룬 연구 결과는 Adams 등[12]이 2004년에 발표한 논문이 처음이라고 할 수 있다. 이들은 해쉬함수 기반 KDF를 입출력 값의 유형에 따라 분류하고 각각의 안전성 분석을 실시하였으며, 여러 표준에서 사용되고 있는 KDF의 안전성을 높일 수 있는 방안을 제시하였다. 블록암호 기반 KDF의 경우는 의사난수성(pseudorandomness) 관점에서 여러 운영모드의 안전성을 분석한 Gilbert[13]의 논문이 대표적이다. Gilbert는 한 블록 길이의 입력으로부터 여러 블록 길이의 출력을 얻어내는 확장 함수 개념으로 KDF 구조를 인식하여 Counter 모드, OFB 모드, Milenage 모드 등의 안전성을 논하였다. Gilbert의 결과는 기본적으로 핵심함수를 PRP로 가정하여 KDF 구조의 의사난수성을 규명한 것이므로 본 논문의 안전성 분석 결과도 Gilbert의 논리전개 방식과 유사하다.

한편, NIST SP800-108[11]에 나타나 있는 세 가지 형태의 PRF 기반 KDF에 대한 안전성 분석 결과는 아직까지 알려진 연구 결과가 없다. NIST 문서에 나타나 있는 세 가지 형태의 KDF에서 PRF를 어떻게 구성할 것인가에 대한 구체적인 언급은 나타나 있지 않다. 마스터키 값을 포함한 여러 가지 부가적인 입력 값들이 모두 연접(concatenation) 되어 PRF에 입력된다는 사실만 언급되어 있다. 그러므로 의사난수성 관점의 안전성 분석을 실시하기 위해서는 기반이 되는 PRF에 대한 추가적인 정보가 필요하다. 본 논문에서는 NIST가 제안한 PRF 기반 KDF 구조를 실용성이 높을 것으로 예상되는 PRP 기반 KDF 고조로 변형한 형태에 대한 안전성 분석을 실시한다. NIST의 세 가지 형태를 PRP 기반으로 변형할 경우에 Counter 모드와 Feedback 모드로 표시된 두 가지 형태의 의사난수성은 Gilbert[13]의 연구 결과로부터 안전하지 않음을 쉽게 유추해낼 수 있다. 하지만 Double-Pipeline Iteration 모드에 대한 의사난수성은 PRP 기반으로 변형한 경우에도 기존 결과로부터 쉽게 유추되지 않는다. 우리는 의사난수성 관점에서 NIST의 Double-Pipeline Iteration 모드를 PRP 기반 KDF 구조로 변형한 형태의 안전성을 규명한다.

II. KDF 연구 동향

KDF는 중요한 정보보호 기술 표준에 필수 요소로 자주 등장하고 있지만, 이에 대한 학계의 연구 결과는 상대적으로 빈약한 실정이다. 본 절에서는 먼저 KDF의 구조를 살펴보기 위하여 표준에 나타나 있는 대표적인 KDF를 소개한다.

KDF는 사용하는 핵심함수의 종류에 따라 해쉬함수 기반 KDF와 블록암호 기반 KDF로 대별할 수 있다. 무선 LAN의 RSN 내 PRF는 해쉬함수 기반 KDF이고, 3GSM의 Milenage 함수와 Bluetooth



〔그림 1〕 해쉬함수 기반 KDF의 블록도

의 함수 $Ar(A'r)$은 블록암호 기반 KDF이다.

2.1 해쉬함수 기반 KDF

KDF의 핵심 함수로 SHA1이나 MD5같은 해쉬함수를 사용하는 구조로서 MK와 스트링 S의 입력을 통해, l-비트 키를 출력한다.

$$KDF(MK,l) = [h(MK,S_1)\| \cdots \|h(MK,S_n)]_l$$

여기에서 MK는 마스터키, l은 유도하고자 하는 키 길이, 스트링 S는 외부 입력값이다. S는 공개된 정보로 간주되며, 각각의 $i \neq j$에 대해, $S_i \neq S_j$이다. $h(\cdot)$는 해쉬함수, $n = \lceil l/hashlen \rceil$, $[x]_l$는 x의 상위 l-비트이다. $h(x,y) = h(x \| y)$, $hashlen$는 해쉬함수의 출력 길이다. KDF의 출력은 해쉬값을 연접한 후 원하는 길이만큼 절삭한 값이 되는 것이다. Adams 등〔12〕은 해쉬함수 기반 KDF를 입출력 값의 유형에 따라 분류하고 각각의 안전성 분석을 실시하였다. "〔그림 1〕"은 해쉬함수 기반 KDF의 블록도를 표현한 것이다.

해쉬함수 기반 KDF는 ISO-18033-2〔1〕, IEEE P1363a〔2〕, PKCS#1 v2.1〔3〕, ANSI X9.42〔4〕, NIST SP800-56A〔5〕, IEEE 802.11i〔6〕, PKCS #5〔7〕 등의 다양한 표준에 등장하며, Adams 등〔12〕은 해쉬함수 기반 KDF를 다음 네 가지 유형으로 분류하여 안전성을 분석하였다. 이들의 안전성 분석은 입력 데이터의 형태에 따라 공격량이 다를 수 있음을 밝힌 것으로 해쉬함수 기반 KDF의 안전성 분석을 처음으로 실시하였다는 데에 그 의의가 있다. 여기에서는 이들의 결과를 간략히 기술하기로 한다.

2.1.1 MK,S 입력 유형

가장 일반적인 구조로서 입력 값을 MK,S로 갖으며, KDF 함수는 다음과 같다.

$$KDF(MK,l) = [h(MK,S_1)\| \cdots \|h(MK,S_n)]_l$$

이 구조에서 MK의 결과를 올바르게 추정하기 위한 공격량은 $O(2^{hashlen})$로 분석된다.

2.1.2 S,MK 입력 유형

입력 값을 S,MK로 갖는 구조로 앞의 구조와 MK와 S의 입력 순서를 바꾼 것이다.

$$KDF(MK,l) = [h(S_1,MK)\| \cdots \|h(S_n,MK)]_l$$

이 구조는 먼저 공개된 정보인 서로 다른 S값만을 이용하여 충돌쌍을 찾을 경우, 이후의 미지의 동일한 MK에 대하여 동일한 KDF 출력값을 갖는 개체들을 알 수 있다. 그러므로 이 구조에 대한 공격량은 $O(2^{hashlen/2})$로 낮아진다.

2.1.3 MK,S,MK 입력 구조

MK,S,MK 순서로 입력되는 구조로 기존 MK,S에 MK를 한 번 더 입력 값에 추가한 것이다.

$$KDF(MK,l) = [h(MK,S_1,MK)\| \cdots \|h(MK,S_n,MK)]_l$$

이 구조는 안전성 관점에서 S,MK입력 유형을 개선한 것으로 충돌쌍을 찾기 이전에 MK출력값에 대한 정보를 가정해야 하므로 공격량이

$$O(2^{hashlen} \cdot 2^{hashlen/2}) = O(2^{3hashlen/2})$$

으로 증가한다.

2.1.4 $HMAC(MK,S)$ 유형

이 유형은 핵심 함수로 HMAC〔14〕을 사용하는 구조로 MK,S를 입력 값으로 갖는다. MK는 HMAC의 키로 사용되며, 입력 부분에 ipad와 출력직전에 opad를 추가적으로 사용하는 HMAC의 특성에 따라 공격량이 $O(2^{2\,hashlen})$으로 증가한다.

2.2 블록암호 기반 KDF

블록암호 기반 KDF는 핵심 함수로서 AES[15]나 SAFER+[16] 같은 블록암호를 사용하는 구조로, *MK*와 고정된 데이터 *S*의 입력을 통해 원하는 길이의 키를 생성한다. 일반적으로 *MK*는 KDF 내의 블록암호에 대한 암호화 키로 사용되고, 외부입력값으로 분류되는 *S*는 $Label \| 0x00 \| Context \| [l]_2$의 형태를 갖는다. *Label*은 KDF의 사용 목적, *Context*는 유도될 키의 정보를 각각 포함한다. $[l]_2$는 유도될 키의 길이를 2진수로 표현한 것이다.

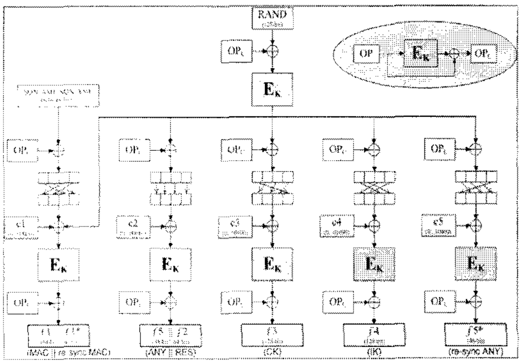
블록암호 기반 KDF는 주로 무선 환경의 표준인 3GPP TR 35.909[9]와 IEEE 802.15.1^{TM}[10] 등에서 나타난다. 유럽의 비동기식 제3세대 무선통신 규격을 정하고 있는 3GSM에서는 블록암호 AES를 사용하는 Milenage[9]라는 명칭의 KDF를 추천하고 있으며, 근거리 무선통신 규격인 Bluetooth[10]에서는 SAFER+를 기반 함수로 하는 KDF를 표준으로 채택하고 있다.

미국의 NIST에서는 PRF 기반 KDF 함수를 세 가지 모드로 분류하였다[11]. PRF에 대한 구체적인 언급은 없으므로 PRF의 특수한 형태인 PRP 기반 KDF도 NIST가 제안한 범주에 속하는 것이며, PRP는 실제 응용에서 블록암호로 대체될 수 있다. NIST는 PRF 기반 KDF로 Counter 모드, Feed-back 모드, Double-Pipeline Iteration 모드를 추천하고 있지만 이들에 대한 구체적 안전성 분석 결과는 아직까지 발표되지 않고 있다.

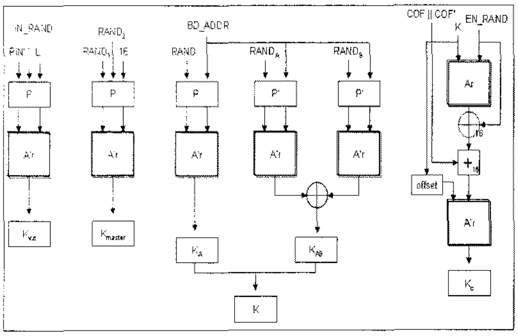
2.2.1 3GSM의 KDF Milenage

3GSM은 3세대 이동통신으로 기존의 2세대 이동통신에 연결성, 무선 네트워크상의 자유로운 데이터 송수신, 로밍 및 부가 서비스가 더해져 획기적으로 발전된 기술이다. 3GSM 시스템을 위한 보안 메커니즘에는 인증과 키일치, 단말과 RNC(radio network controller) 사이의 무선구간을 지나는 데이터의 암호화를 위한 키들이 필요하며, 이러한 키들의 생성을 위한 KDF로 Milenage[9]가 표준안으로 권고되어 있다.

"[그림 2]"에 나타나 있는 Milenage는, 네트워크 인증을 위한 MAC값을 생성하는 f1, 사용자 인증을 위한 RES(response) 값을 생성하는 f2, 인증 후 데이터 암호화를 위한 키 CK(cipher key)를 생성하는



[그림 2] Milenage의 블록도



[그림 3] Bluetooth의 KDF 블록도

f3, 데이터 무결성 확인을 위한 키 IK(integrity key)를 생성하는 f4, SQN(sequence number)의 익명성을 위한 키 AK(anonymity key)를 생성하는 f5로 이루어져 있다. Milenage의 내부 함수 E_K는 대칭키 K를 사용하는 블록암호를 의미하고, 이 K는 KDF 관점에서 마스터키 역할을 한다. 표준에서는 블록암호로 AES 사용을 권장하고 있다. "[그림 2]"에서 OP, SQN, AMF, RAND 등은 KDF 관점에서 외부입력값에 해당하는 것으로 안전성 분석 시에는 비밀이 아닌 데이터로 인식된다.

2.2.2 Bluetooth의 KDF

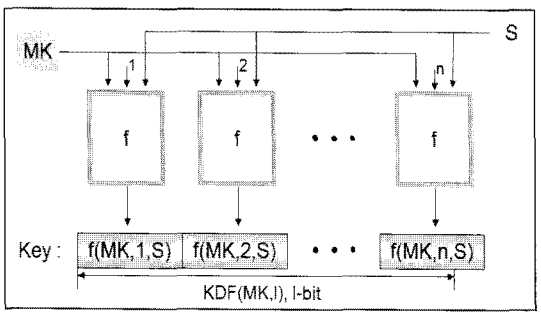
Bluetooth 표준은 휴대폰, 컴퓨터, PDA 등의 모바일 장치 간 근거리 무선 채널을 설립하기 위한 것이다. IEEE 802.15.1^{TM}[10]을 살펴보면 인증과 데이터 암호에 사용되는 비밀키로 링크키 K와 암호화키 K_c가 있다. 링크키에는 초기 키 K_{init}, 장치 A의 키 K_A, A와 B의 결합 키 K_{AB}, 마스터 키 K_{master}까지 4가지 종류가 있고, K_c와 함께 초기화 단계에서 KDF를 통

해 생성된다. 단, K_A는 초기화 단계가 아닌 최초 장치 설치 시 생성된다.

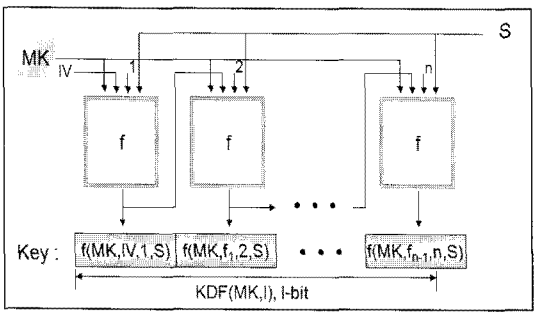
Bluetooth의 KDF는 블록암호인 SAFER+인 함수 Ar과 SAFER+에서 1라운드의 입력을 3라운드의 입력에 더해 약간의 변형을 가한 함수 $A'r$을 핵심 함수로 사용한다. "[그림 3]"은 Bluetooth의 KDF를 나타낸 것이다. Bluetooth의 키유도 과정은 크게 2단계로 분류할 수 있다. 제 1단계에서는 KDF의 마스터키 역할을 하는 RAND와 외부 입력값인 PIN과 BD_ADDR을 입력으로 하여 $A'r$을 사용하는 KDF 수행 결과 K_{init}, K_A, K_{AB}, K_{master} 등 4가지 종류의 링크키를 생성한다. 제 2단계는 링크키 중 K_A나 K_{AB}를 Ar과 $A'r$을 사용한 KDF의 마스터키 K로 설정하여 K_c를 생성하는 과정이다.

2.2.3 NIST의 KDF Counter 모드

의사난수함수로 불리는 PRF는 완전랜덤함수와 계산적으로 구별불능한 함수로 설명될 수 있다. 완전한 이론적 정의는 여기에서 생략한다. NIST의 Counter 모드는 블록암호 운영모드 중 Counter 모드와 흡사한 KDF 구조로 PRF 출력이 카운터 값과 함께 계산된다. PRF를 $f(\cdot)$로 표현할 경우 KDF는



[그림 4] NIST의 Counter 모드 블록도



[그림 4] NIST의 Feedback 모드 블록도

$$KDF(MK,l) = [f(MK,1,S) \| \cdots \| f(MK,n,S)]_l$$

이다. 즉, PRF 각각의 출력을 연접시켜 원하는 l-비트 길이의 키를 생성한다. Counter 모드는 "[그림 4]"에 나타나 있다.

2.2.4 NIST KDF Feedback 모드

NIST의 PRF 기반 Feedback 모드 KDF 구조는 블록암호 운영모드 중 CBC 모드와 Counter 모드를 합성한 것과 유사한 형태로 볼 수 있으며, "[그림 5]"에 그 블록도가 나타나 있다. 수식으로는 PRF를 $f(\cdot)$로 놓을 경우 다음과 같이 표현 가능하다.

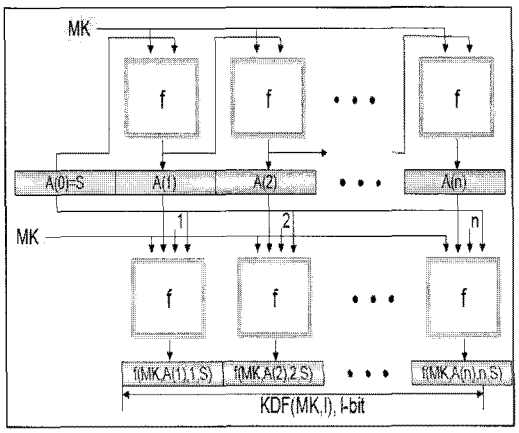
$$f_i = f(MK, f_{i-1}, i, S),\ f_0 = IV$$
$$KDF(MK,l) = [f(MK,f_0,1,S) \| \cdots \| f(MK,f_{n-1},n,S)]_l$$

2.2.5 NIST KDF Double-Pipeline Iteration 모드

NIST가 제안한 PRF 기반 Double-Pipeline Iteration 모드 KDF의 구조는 2단계로 구성되고, 블록암호의 CBC 운영모드와 Counter 운영모드를 단계적으로 합성한 형태와 유사한 것으로 "[그림 6]"에 나타나 있다. 수식으로는 PRF를 $f(\cdot)$로 놓을 경우 다음과 같이 표현될 수 있다.

$$A(i) = f(MK, A(i-1)),\ A(0) = S$$
$$KDF(MK,l) = [f(MK,A(1),1,S) \| \cdots \| f(MK,A(n),n,S)]_l$$

우리는 이후로 이 모드를 간단히 DPI 모드로 부르기로 한다.



[그림 6] Double-Pipeline Iteration Mode의 블록도

한편, 블록암호 기반 KDF의 안전성 분석은 해쉬 함수 기반 KDF와 달리 의사랜덤성 관점의 이론적 분석이 주류를 이루고 있다. 이러한 이론적 안전성 분석은 이상적인 랜덤비트생성기와 블록암호의 구별불능성(indistinguishability)을 분석하는 것으로 구조의 견고성(soundness)을 논하는 것이므로 매우 중요한 안전성 분석 방법이다.

III. 의사난수성(Pseudorandomness) 개념

블록암호나 이들의 운영모드(modes of operation)와 같이 비밀키가 내재되어 있는 암호적 함수는 랜덤하게 선택된 키에 의해서 결정되는 랜덤함수(random function)로 볼 수 있다. KDF도 블록암호를 핵심함수로 사용할 경우 운영모드의 한 예로 생각할 수 있으므로 랜덤함수로 볼 수 있다. 의사난수성 개념은 이러한 랜덤함수를 확률론적으로 엄밀히 정의하는 것으로부터 출발한다.

3.1 랜덤함수의 정의 및 기호

의사난수성 개념의 출발점이 되는 랜덤함수를 수학적으로 정의하기 위하여 다음과 같은 몇 가지 기호를 약속한다.

- $I_n = \{0,1\}^n$
- $\Omega_{n,m} = \{f : I_n \to I_m \mid f$는 함수$\}$
- $\wp_n = \{f : I_n \to I_n \mid f$는 치환$\}$

이와 같이 정의하면 각 집합의 원소의 개수는 각각 $|I_n| = 2^n$, $|\Omega_{n,m}| = 2^{m \cdot 2^n}$, $|\wp_n| = 2^n!$이 됨을 알 수 있다.

$\Omega_{n,m}$의 랜덤함수는 $\Omega_{n,m}$을 표본공간으로 하여 추출된 함수 F로 정의된다. 즉, 랜덤함수 F는 확률공간 $\Omega_{n,m}$ 위의 확률변수(random variable)이다. 랜덤치환도 유사하게 정의된다. $\Omega_{n,m}$과 $\wp_n$의 확률분포가 균일분포(uniform distribution)일 때, 랜덤함수는 완전랜덤함수(perfect random function), 랜덤치환은 완전랜덤치환이라 각각 부른다.

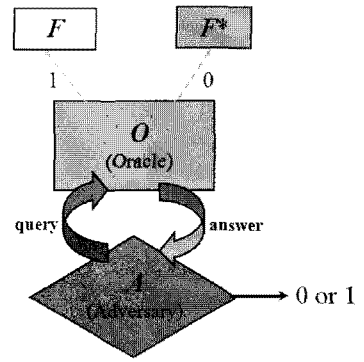
정의 3.1. $\Omega_{n,m}$의 확률분포가 균일분포일 때, $\Omega_{n,m}$을 표본공간으로 하여 추출된 함수 F를 완전랜덤함수라 하고, $\wp_n$의 확률분포가 균일분포일 때, $\wp_n$을 표본공간으로 하여 추출된 함수 F를 완전랜덤치환이라 한다.

한편, 블록암호와 같이 비밀키 K에 의하여 함수가 결정되는 경우는 키공간 $\mathcal{J}$의 분포가 균일분포라 생각하고 키를 추출한 후 $\Omega_{n,m}$의 한 원소인 어떤 함수가 대응되는 것으로 보는 것이 합리적이다. 그러므로 이 경우에는 랜덤함수를 $F = (f_K)_{K \in \mathcal{J}}$로 표현한다. 키 길이가 m비트이고, 입출력 길이가 n비트인 블록암호를 $\wp_n$의 한 원소로 보는 경우의 랜덤치환은 $\wp_n$ 내의 임의의 한 치환이 $1/(2^n!)$의 확률로 나타나는 균일분포가 아니라 키에 의해서만 결정되는 2^m개의 치환만이 균일하게 분포하고 다른 치환은 확률 0을 갖는 분포이다.

3.2 의사난수성에서의 공격 모델

무한한 계산 능력을 소유한 공격자(adversary) A가 있고, A는 오라클 O에 유한개의 질의(query)를 입력할 수 있다고 하자. 오라클 O는 특정한 암호적 함수 F 또는 완전랜덤함수 F^*를 정확히 1/2의 확률로 한 번 선택한다. 공격자 A는 오라클 O가 둘 중에 어떤 것을 선택하였는지 알 수 없고, 질의가 계속되는 동안 O의 선택은 변하지 않는다고 가정한다. 오라클 O는 입력된 질의에 대한 응답(response)을 A에게 출력해준다. 공격자 A가 질의와 응답의 결과만을 가지고 오라클 O가 어떤 함수를 선택했는지 구별할 수 있는 확률이 1/2에서 크게 벗어나지 못할 때 F는 의사난수성을 만족한다고 정의한다. 이러한 공격자 모델을 도식화 한 것이 "[그림 7]"이며, 엄밀한 정의는 다음과 같다.

정의 3.2 함수 F를 동일한 입출력 공간을 가진 완전랜덤함수 F^*로부터 구별하기 위한 공격자 A의



[그림 7] 의사난수성 공격자 모델

이점(advantage) $Adv_A(F, F^*)$는 다음과 같이 정의된다.

$$Adv_A(F,F^*) = |\Pr(A\text{의출력}=1 \mid O \leftarrow F^*) - \Pr(A\text{의출력}=1 \mid O \leftarrow F)|$$

여기에서 $O \leftarrow F^*$와 $O \leftarrow F$는 각각 오라클이 F^*와 F를 선택하여 질의에 대한 응답을 출력한 것임을 의미한다.

정의 3.3 정의역이 자연수이고 공역이 실수인 임의의 함수 $h: N \rightarrow R$가 무시가능(negligible)이라 함은 임의의 상수 $c>0$와 충분히 큰 자연수 n에 대하여

$$h(n) < \frac{1}{n^c}$$

이 성립한다는 것이다.

정의 3.4 함수 F를 동일한 입출력 공간을 가진 완전랜덤함수 F^*로부터 구별하기 위한 임의의 공격자 A의 $Adv_A(F, F^*)$가 무시가능(negligible)할 정도로 작을 때, 함수 F는 의사난수성을 만족한다고 정의한다.

위 정의에서 F와 F^*는 단순히 고정된 어떤 함수들이 아닌 확률변수들로 이해되어야만 한다. 예를 들어 블록암호의 의사난수성을 조사하는 경우라면 F는 m 비트 키를 선택함으로써 $1/(2^m)$의 확률로 결정되는 블록암호 함수이고, F^*는 공간 $\wp_n$으로부터 $1/(2^n!)$의 확률로 선택된 함수인 것이다.

한편, 공격자 A가 오라클 O에게 입력할 질의를 선택할 때, 이전의 질의-응답 쌍에 대한 정보를 알고 있는 상태에서 새로운 질의를 선택할 경우라면 A를 능동적(adaptive) 공격자라 한다. 그렇지 않고 사전에 일정한 개수의 질의를 선택하고, 이들 각각에 대한 응답을 얻는 경우에는 A를 수동적(non-adaptive) 공격자라 부른다.

우리는 어떤 랜덤함수의 의사난수성을 증명하기 위하여 매우 유용한 정리를 사용한다. Patarin[17]에 의하여 처음 제시되고, Vaudenay[18]와 Gilbert[13]의 논문에도 나타나 있는 이 정리의 내용은 다음과 같다.

정리 3.1 F는 함수공간 $\Omega_{n,m}$ 내의 랜덤함수이고, F^*는 $\Omega_{n,m}$ 내의 완전랜덤함수라 하자. q는 자연수이고, ${I_n}^q$의 부분집합 X는 $x^i (1 \le i \le q)$들이 서로 다른 I_n의 원소들일 때의 $\xi = (x^1, \cdots, x^q)$들을 모두 포함하고 있는 집합이라 하자. 즉,

$$X = \{\xi = (x^1, \cdots, x^q) \in {I_n}^q \mid x^i \neq x^j \text{ for } i \neq j\}$$

이다. 만일 다음 두 가지 조건

$$(i)\ |Y| \ge (1-\epsilon_1) \cdot 2^{mq}$$

$$(ii)\ \forall \xi \in X,\ \forall \zeta \in Y,\ \Pr\left(\xi \xrightarrow{F} \zeta\right) \ge \frac{(1-\epsilon_2)}{2^{mq}}$$

를 만족하는 집합 $Y \subset {I_m}^q$와 양수 ϵ_1, ϵ_2가 존재한다면, q개의 질의로 F를 F^*로부터 구별하기 위한 공격자 A의 이점은 다음을 만족한다.

$$Adv_A(F, F^*) \le \epsilon_1 + \epsilon_2 .$$

정리 3.1의 내용은 공격자의 이점 $Adv_A(F, F^*)$는 함수 F에 의한 전환확률(transition probability) $\Pr\left(\xi \xrightarrow{F} \zeta\right)$에 의해서 전적으로 결정된다는 사실을 말해주고 있다. 우리는 정리 3.1을 이용하여 공격자의 이점에 대한 상계(upper bound)를 계산함으로써 랜덤함수의 의사난수성을 밝히고자 한다.

IV. PRP 기반 NIST KDF의 의사난수성

NIST의 표준문서 SP800-108[11]에서는 PRF를 핵심함수로 사용하는 KDF의 세 가지 유형을 추천하고 있다. 하지만 의사난수함수인 PRF에 대한 구체적인 언급은 나타나 있지 않다. 우리는 PRF의 특수한 부류인 의사난수치환으로 불리는 PRP(Pseudorandom permutation) 기반 KDF로 변형할 경우의 안전성 분석을 실시하고자 한다. 실제 구현 환경에서 PRP는 의사난수성을 만족하는 블록암호로 생각할 수 있으므로 NIST가 제안한 세 가지 유형도 블록암호 기반 KDF로 변형하여 안전성을 분석해보는 것은 블록암호의 사용 빈도가 높기 때문에 실용성 면에서 의미있는 연구로 볼 수 있다.

NIST의 PRF 기반 KDF 중에서 PRP 기반으로 변형할 경우에 Counter 모드와 Feedback 모드는 의사난수성을 만족하지 않는다. 이는 PRP 기반 KDF 모드로 변형할 경우 Counter 값이 다른 입력 값과 XOR 연산된다는 기본 전제 하에서 얻을 수 있는 결과이다. PRP의 입력값들이 XOR 연산 형태가 아닌 연

접이나 다른 선계산(pre-computation)에 의한 가공이 이루어질 경우의 안전성 분석은 또 다른 관점의 안전성 분석이 이루어져야함을 밝혀둔다. PRP 기반 Counter 모드가 의사난수성을 만족하지 않는다는 사실은 Gilbert[13]의 연구 결과에 이미 언급되어 있다. 우리는 NIST의 변형 PRP 기반 Feedback 모드의 의사난수성 관점의 안전성도 유사한 논리로 분석될 수 있음을 보인다. 또한, 세 번째 모드인 DPI 모드에 대해서는 PRF 기반에서 PRP 기반 모드로 변형할 경우의 적절한 형태를 제시하고, 이에 대하여 Milenage 모드의 의사난수성과 유사한 안전성 분석 결과를 입증한다.

4.1 변형 PRP 기반 Feedback 모드의 비의사난수성

NIST의 PRF 기반 Feedback 모드를 의사랜덤치환인 PRP 기반 모드로 변형한 형태의 의사난수성 분석을 위하여 정의 4.1에서와 같은 수식으로 표현하고, "[그림 8]"에 나타나 있는 기호들을 사용하기로 한다.

정의 4.1 임의의 랜덤치환 $f \in \wp_n$, t개의 상수 $c_1, c_2, \cdots, c_t \in \{0,1\}^n$이 주어졌을 때, PRP 기반 Feedback 모드는 랜덤함수 $F_{Feedback} \in \Omega_{n,nt}$로 다음과 같이 정의 된다.

$$\begin{aligned} F_{Feedback}(f)\colon \{0,1\}^n &\rightarrow \{0,1\}^{nt} \\ x &\mapsto (z_1, z_2, \cdots, z_t) \\ z_1 &= f(x \oplus c_1), \\ z_k &= f(x \oplus z_{k-1} \oplus c_k),\ 2 \le k \le t. \end{aligned}$$

정리 4.1 완전랜덤치환 $f^* \in \wp_n$을 핵심함수로 사용하는 $F_{Feedback}(f^*) \in \Omega_{n,nt}$는 의사난수성을 만족하지 않는다.

증명) 임의의 순서쌍 (i,j)에 대하여 $1 \le i \ne j \le q$일 때, 각각의 질의 x^i와 x^j를

$$x^j = x^i \oplus c_1 \oplus c_2 \oplus z_1^i$$

가 만족되도록 선택한다. 그러면 이 경우

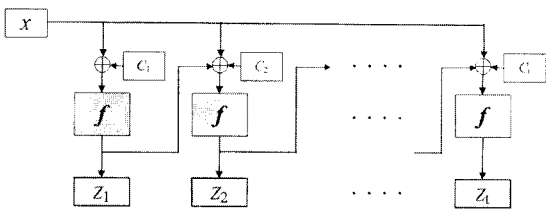
$$\begin{aligned} z_1^j &= f^*(x^j \oplus c_1) \\ &= f^*((x^i \oplus c_1 \oplus c_2 \oplus z_1^i) \oplus c_1) \\ &= f^*(x^i \oplus c_2 \oplus z_1^i) \\ &= z_2^i \end{aligned}$$

라는 관계가 항상 성립하므로 능동적 공격자 A는 위와 같은 관계를 만족하는 두 개의 질의 x^i와 x^j를 선택하여 각각의 응답으로부터 $z_2^j = z_1^j$의 등식이 성립하는지를 확인함으로써 $F_{Feedback}$을 완전랜덤함수 $F^* \in \Omega_{n,nt}$로부터 구별할 수 있다. 랜덤한 경우에 등식 $z_2^i = z_1^j$이 성립할 확률은 $1/2^n$로 아주 작기 때문에 공격자 A의 성공확률은 거의 1에 가깝다는 사실을 알 수 있다.

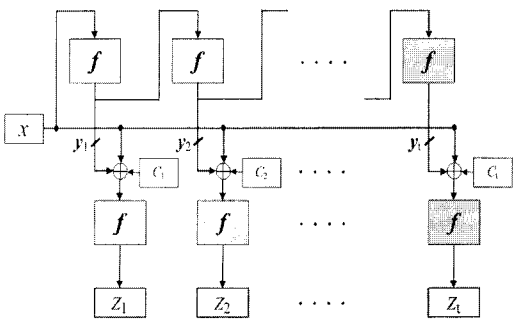
4.2 변형 PRP 기반 DPI 모드의 의사난수성

NIST의 PRF 기반 DPI 모드는 블록암호 운영모드 중 암호화 기법으로 가장 널리 사용되고 있는 CBC 모드와 Counter 모드를 단계적으로 합성한 구조이다. PRF 기반 DPI 모드를 의사랜덤치환인 PRP 기반 DPI 모드로 변형한 형태의 의사난수성 증명을 위하여 정의 4.2에서와 같은 수식으로 표현된 모드를 제시하고, "[그림 9]"에 나타나 있는 기호들을 사용한다.

정의 4.2 임의의 랜덤치환 $f \in \wp_n$, t개의 상수 $c_1, c_2, \cdots, c_t \in \{0,1\}^n$이 주어졌을 때, PRP 기반 DPI 모드는 랜덤함수 $F_{DPI} \in \Omega_{n,nt}$로 다음과 같이 정의 된다.



[그림 8] NIST의 변형 PRP 기반 Feedback 모드



[그림 9] NIST의 변형 PRP 기반 DPI 모드

$$F_{DPI}(f)\colon \{0,1\}^n \to \{0,1\}^{nt}$$
$$x \mapsto (z_1, z_2, \cdots, z_t)$$
$$z_k = f(x \oplus f^k(x) \oplus c_k), \forall 1 \le k \le t.$$

정리 4.2 완전랜덤치환 $f^* \in \wp_n$을 핵심함수로 사용하는 변형 DPI 모드를 $F = F_{DPI}(f^*) \in \Omega_{n,nt}$로 놓고, F^*는 $\Omega_{n,nt}$ 내의 완전랜덤함수라 하자. 그러면 $t \ge 2$인 경우에

$$\frac{t^2q^2}{2^n} \le \frac{2}{3}$$

를 만족하는 q개의 질의를 사용하는 임의의 공격자 A가 F와 F^*를 구별하는 이점 $Adv_A(F, F^*)$는 다음을 만족한다.

$$Adv_A(F, F^*) \le \frac{13t^2q^2}{2^{n+1}}.$$

증명) X는 I_n의 서로 다른 원소들로 구성된 q-순서쌍들을 개별적인 원소로 갖는 집합

$$X = \{\mathbf{x} = (x^1, \cdots, x^q) \in {I_n}^q \mid x^i \ne x^j\} \subset {I_n}^q$$

이고, 집합 Z는 I_n 내의 서로 다른 tq개 원소들로 이루어진 순서쌍을 개별적인 원소로 갖는 집합

$$Z = \{\mathbf{z} = ((z_1^1, \cdots, z_t^1), \cdots, (z_1^q, \cdots, z_t^q)) \in {I_{nt}}^q \mid z_k^i \ne z_l^j\}$$

이라 하자. 정리 3.1을 적용시키기 위해 다음을 만족하는 양의 실수 ϵ_1과 ϵ_2가 존재한다는 것을 보인다.

$$|Z| \ge (1-\epsilon_1) \cdot |I_{nt}|^q$$

$$\forall \mathbf{x} \in X,\ \forall \mathbf{z} \in Z,\ \Pr[\mathbf{x} \xrightarrow{F} \mathbf{z}] \ge (1-\epsilon_2) \cdot \frac{1}{|I_{nt}|^q}.$$

먼저 $|Z| > (1-\epsilon_1) \cdot |I_{nt}|^q$ $(\epsilon_1 > 0)$을 살펴보면,

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

이 성립하므로

$$\epsilon_1 = \frac{q^2t^2}{2^{n+1}} > 0$$

으로 놓으면 첫 번째 조건이 만족된다.

다음으로 두 번째 조건을 위해 $\mathbf{x} \in X$와 $\mathbf{z} \in Z$를 임의의 고정된 값이라 생각하고, 전이 확률 $\Pr[\mathbf{x} \xrightarrow{F} \mathbf{y}]$를 고려하자. 전이확률은 $\mathbf{x}$에서 $\mathbf{z}$로 전이되는 과정 중의 중간값 $\mathbf{y} = (\mathrm{y}^1, \cdots, \mathrm{y}^q)$들의 집합 Y에 의해 다음과 같이 정의된다.

$$\Pr[\mathbf{x} \xrightarrow{F} \mathbf{z}]$$
$$= \sum_{\mathbf{y} \in Y} \Pr[\mathbf{x} \xrightarrow{f^*} \mathbf{y},\ y_k^i \oplus c_k \oplus x^i \xrightarrow{f^*} z_k^i\ (1 \le i,k \le t)].$$

여기에서 집합 $Y \subset {I_{nt}}^q$는

$$Y = \{\mathbf{y} = ((y_1^1, \cdots, y_t^1), \cdots, (y_1^q, \cdots, y_t^q)) \mid y_k^i \ne y_k^j\}$$

이며,

$$y_1^1 = f^*(x^1),\ y_2^1 = (f^*)^2(x^1) \cdots, y_t^1 = (f^*)^t(x^1),$$
$$\cdots$$
$$y_1^q = f^*(x^q),\ y_2^q = (f^*)^2(x^q) \cdots, y_t^q = (f^*)^t(x^q)$$

이다. 집합 Y의 크기는

$$|Y| = 2^{nt} \cdot (2^n-1)^t \cdot \cdots \cdot (2^n-q+1)^t$$
$$= (2^n \cdot (2^n-1) \cdot \cdots \cdot (2^n-q+1))^t$$
$$= \left(\frac{2^n!}{(2^n-q)!}\right)^t \quad (1)$$

이다.

계산의 편이성을 위하여 다음 조건을 만족하는 $\mathbf{y} = \{\mathrm{y}^1, \cdots, \mathrm{y}^q\}$들의 집합인 Y의 부분집합 Y'을 고려하자.

1) $\forall i_1, i_2 \in \{1, \cdots, q\},\ \forall k_1, k_2 \in \{0, \cdots, t-1\},$
$y_{k_1}^{i_1} \ne y_{k_2}^{i_2}$

2) $\forall i_1, i_2 \in \{1, \cdots, q\}, \forall k_1 \in \{0, \cdots, t\}, \forall k_2 \in \{1, \cdots, t\},$
$y_{k_1}^{i_1} \ne y_{k_2}^{i_2} \oplus c_{k_2} \oplus x^{i_2}$

3) $\forall i_1, i_2 \in \{1, \cdots, q\},\ \forall k_1, k_2 \in \{1, \cdots, t-1\},$
$y_{k_1}^{i_1} \ne z_{k_2}^{i_2}$

1)과 2)의 조건은 f^*들의 입력값들을 각각 개별적인 값으로 가정하기 위한 것이고 3)의 조건은 f^*들의 출력값들을 각각 개별적인 값으로 가정하기 위한 조건이다.

전이확률은 Y'에 의해 다음을 만족하며 Y'는 1), 2), 3) 모든 조건을 만족하도록 가정했기 때문에 f^*의 모든 입출력은 각각 개별적인 값들이다. 입출력들은 총 $2tq$개가 존재하므로 다음 수식이 성립한다.

$$\begin{aligned}&\Pr[\mathbf{x}\xrightarrow{F}\mathbf{z}]\\&\geq \textstyle\sum_{\mathbf{y}\in Y'}\Pr[\mathbf{x}\xrightarrow{f^*}\mathbf{y}\wedge y_k^i\oplus c_k\oplus x_k\xrightarrow{f^*}z_k^i]\\&=|Y'|\cdot\frac{(|I_n|-2tq)!}{|I_n|!}\\&=|Y'|\cdot\frac{(2^n-2tq)!}{2^n!}.\end{aligned}\tag{2}$$

$|Y'|$의 상한을 구하기 위해 Y의 원소들 중 Y'의 조건을 만족하지 않는 것들을 생각해보자. 집합의 성질에 의해 $|Y-Y'|$은 Y'의 조건 1), 2), 3)을 각각 만족하지 않는 원소 개수들의 합보다는 작다. 즉, 조건 1), 2), 3)을 만족하는 각각의 집합을 A, B, C로 나타내면

$$\begin{aligned}|Y-Y'|&=|Y\cap(A\cap B\cap C)^c|\\&\leq|A^c\cup B^c\cup C^c|\\&\leq|A^c|+|B^c|+|C^c|\end{aligned}$$

이 성립한다. 각 조건을 만족하지 않는 Y의 원소 $\mathbf{y}=(y^1,\cdots,y^q)$들의 가능한 개수를 계산해 보자. 조건 1), 2), 3)의 부정을 각각 1'), 2'), 3')으로 표기한다.

1') $k_1=0, k_1\neq k_2$일 때,

$$\begin{aligned}y_{k_1}^{i_1}=y_{k_2}^{i_2}&\Rightarrow y_0^{i_1}=y_{k_2}^{i_2}\\&\Rightarrow x^{i_1}=y_{k_2}^{i_2}\end{aligned}$$

이고, x^{i_1}이 고정이라면 위 식을 만족하는 원소의 개수는

$$\frac{|Y|}{2^n}\cdot q\cdot q\cdot(t-1)=\frac{q^2(t-1)}{2^n}|Y|$$

이다.

$i_1=i_2, k_1\neq k_2\neq 0$일 때,

$$y_{k_1}^{i_1}=y_{k_2}^{i_2}\Rightarrow y_{k_1}^{i_1}=y_{k_2}^{i_1}$$

이고, 이를 만족하는 원소의 개수는

$$\frac{|Y|}{2^n}\cdot q\cdot\binom{t}{2}=\frac{q(t-1)(t-2)}{2\cdot 2^n}|Y|$$

이다.

$i_1\neq i_2, k_1\neq k_2\neq 0$ 일 때, $y_{k_1}^{i_1}=y_{k_2}^{i_2}$를 만족하는 원소의 개수는

$$\frac{|Y|}{2^n-1}\cdot\binom{q}{2}\cdot\binom{t}{2}=\frac{q(q-1)(t-1)(t-2)}{4(2^n-1)}|Y|$$

이다.

2') $k_1=0, k_1\neq k_2, i_1=i_2$ 일 때,

$$\begin{aligned}y_{k_1}^{i_1}=y_{k_2}^{i_2}\oplus c_{k_2}\oplus x^{i_2}&\Rightarrow x^{i_1}=y_{k_2}^{i_2}\oplus c_{k_2}\oplus x^{i_1}\\&\Rightarrow c_{k_2}=y_{k_2}^{i_2}\end{aligned}$$

이고, c_{k_2}는 고정이므로 이를 만족하는 원소의 개수는

$$\frac{|Y|}{2^n}\cdot q\cdot t=\frac{qt}{2^n}|Y|$$

이다.

$k_1=0, k_1\neq k_2, i_1\neq i_2$ 일 때,

$$\begin{aligned}y_{k_1}^{i_1}=y_{k_2}^{i_2}\oplus c_{k_2}\oplus x^{i_2}&\Rightarrow y_0^{i_1}=y_{k_2}^{i_2}\oplus c_{k_2}\oplus x^{i_2}\\&\Rightarrow x^{i_1}\oplus x^{i_2}\oplus c_{k_2}=y_{k_2}^{i_2}\end{aligned}$$

이고, x^{i_1}가 고정된 값이므로 위 식을 만족하는 원소의 개수는

$$\frac{|Y|}{2^n}\cdot q\cdot(q-1)\cdot t=\frac{q(q-1)t}{2^n}|Y|$$

이다.

$i_1\neq i_2, k_1=k_2\neq 0$ 일 때,

$$\begin{aligned}y_{k_1}^{i_1}=y_{k_2}^{i_2}\oplus c_{k_2}\oplus x^{i_2}&\Rightarrow y_{k_1}^{i_1}=y_{k_1}^{i_2}\oplus c_{k_1}\oplus x^{i_2}\\&\Rightarrow x^{i_2}\oplus c_{k_1}=y_{k_1}^{i_1}\oplus y_{k_1}^{i_2}\end{aligned}$$

이고, 위 식을 만족하는 원소의 개수는

$$\frac{|Y|}{2^n-1}\cdot q\cdot(q-1)\cdot(t-1)=\frac{q(q-1)t}{2^n-1}|Y|$$

이다.

$i_1=i_2, k_1\neq k_2\neq 0$ 일 때,

$$\begin{aligned}y_{k_1}^{i_1}=y_{k_2}^{i_2}\oplus c_{k_2}\oplus x^{i_2}&\Rightarrow y_{k_1}^{i_1}=y_{k_2}^{i_1}\oplus c_{k_2}\oplus x^{i_1}\\&\Rightarrow x^{i_1}\oplus c_{k_2}=y_{k_1}^{i_1}\oplus y_{k_2}^{i_1}\end{aligned}$$

이고, 위 식을 만족하는 원소의 개수는

$$\frac{|Y|}{2^n} \cdot q \cdot t \cdot (t-1) = \frac{qt(t-1)}{2^n}|Y|$$

이다.

$i_1 \neq i_2, k_1 \neq k_2 \neq 0$ 일 때,

$$y_{k_1}^{i_1} = y_{k_2}^{i_2} \oplus c_{k_2} \oplus x^{i_2} \Rightarrow y_{k_1}^{i_1} = y_{k_2}^{i_2} \oplus c_{k_2} \oplus x^{i_2}$$
$$\Rightarrow x^{i_2} \oplus c_{k_2} = y_{k_1}^{i_1} \oplus y_{k_2}^{i_2}$$

이고, 위 식을 만족하는 원소의 개수는

$$\frac{|Y|}{2^n-1} \cdot q \cdot (q-1) \cdot (t-1) \cdot (t-2) = \frac{q(q-1)t(t-1)}{2^n-1}|Y|$$

이다.

3') 임의의 i_1, i_2, k_1, k_2에 대하여 $y_{k_1}^{i_1} = z_{k_2}^{i_2}$를 만족하는 원소의 개수는

$$\frac{|Y|}{2^n} \cdot q^2 \cdot t^2 = \frac{q^2 \cdot t^2}{2^n} \cdot |Y|$$

이다.

결과적으로

$$|Y| - |Y'| \leq \left(\frac{q^2(t-1)}{2} + \frac{q(t-1)(t-2)}{2 \cdot 2^n} + \frac{q^2 t}{2^n} + \frac{q(q-1)t}{2^n-1} + \frac{qt(t-1)}{2^n} + \frac{q(q-1)t(t-1)}{2^n-1} + \frac{q(q-1)(t-1)(t-2)}{4(2^n-1)} + \frac{q^2 t^2}{2^n} \right) \cdot |Y| .$$

$$|Y'| \geq \left(1 - \left(\frac{q^2(t-1)}{2} + \frac{q(t-1)(t-2)}{2 \cdot 2^n} + \frac{q^2 t}{2^n} + \frac{q^2 t^2}{2^n} + \frac{q(q-1)t}{2^n-1} + \frac{qt(t-1)}{2^n} + \frac{q(q-1)t(t-1)}{2^n-1} + \frac{q(q-1)(t-1)(t-2)}{4(2^n-1)} \right) \right) \cdot |Y| \quad (3)$$

이 성립하고, 수식 (1), (2), (3)으로부터 다음 식을 얻을 수 있다.

$$\Pr[\mathbf{x} \xrightarrow{F} \mathbf{z}] \geq \left(1 - \left(\frac{q^2(t-1)}{2} + \frac{q(t-1)(t-2)}{2 \cdot 2^n} + \frac{q^2 t}{2^n} + \frac{q^2 t^2}{2^n} + \frac{q(q-1)t}{2^n-1} + \frac{qt(t-1)}{2^n} + \frac{q(q-1)(t-1)(t-2)}{4(2^n-1)} + \frac{q(q-1)t(t-1)}{2^n-1} \right) \right) \cdot \frac{(2^n-2qt)!}{2^n!} \cdot \left(\frac{2^n!}{(2^n-q)!} \right)^t .$$

위 식을 간단히 하면 다음과 같다.

$$\begin{aligned} &\Pr[\mathbf{x} \xrightarrow{F} \mathbf{z}] \\ &\geq \frac{1}{2^{ntq}} \left(1 - \frac{q}{2^{n+1}} (7qt^2 + qt - 2t^2 - 2t) \right) \cdot \left(1 + \frac{3q^2t^2 - qt}{2^{n+1}} \right) \\ &= \frac{1}{2^{ntq}} (1-\epsilon)(1+\epsilon'), \end{aligned}$$

$$\epsilon = \frac{q}{2^{n+1}} (7qt^2 + qt - 2t^2 - 2t),$$
$$\epsilon' = \frac{3q^2t^2 - qt}{2^{n+1}} .$$

가정에 의해 $\frac{t^2q^2}{2^n} \leq \frac{2}{3}$이므로, $\epsilon' \leq 1$이며, 다음 식이 성립하는 것을 보일 수 있다.

$$\begin{aligned} (1-\epsilon)(1+\epsilon') &= 1 - \epsilon + \epsilon' - \epsilon\epsilon' \\ &\geq 1 - \epsilon + \epsilon' - \epsilon \\ &= 1 - 2\epsilon + \epsilon' \\ &\geq 1 - \frac{1}{2^{n+1}} \cdot 12q^2t^2 . \end{aligned}$$

그러므로

$$\Pr[\mathbf{x} \xrightarrow{F} \mathbf{z}] \geq \left(1 - \frac{12q^2t^2}{2^{n+1}} \right) \cdot \frac{1}{2^{ntq}}$$

이 성립한다. $\epsilon_2 = \frac{12q^2t^2}{2^{n+1}}$라 놓으면, $\epsilon_1 = \frac{q^2t^2}{2^{n+1}}$이므로 정리 3.1에 의해

$$Adv_A(F, F^*) \leq \frac{13t^2q^2}{2^{n+1}}$$

을 얻는다.

정리 4.2가 의미하는 바는 NIST가 제안한 키유도 함수 중 PRF 기반 DPI 모드를 PRP 기반 DPI 모드로 변형한 형태의 KDF 구조가 의사난수성을 만족한다는 것이다. 정리 4.2의 결과는 NIST 변형 PRP 기반 DPI 모드를 완전랜덤함수로부터 구별해내기 위

한 공격자의 이점이 n이 증가함에 따라 지수적으로 (exponentially) 감소하여 0에 가까워진다는 것을 보여준 것이므로 정의 3.3에 의하여 그 이점이 무시할 정도로 작다는 것을 의미한다.

V. 결 론

본 논문에서 우리는 정보보호 시스템에서 필수적인 요소라 할 수 있는 키유도함수의 안전성을 분석하였다. 키유도함수의 최신 연구 동향을 간단히 조사 분석하였으며, 특히 블록암호에 기반한 키유도함수의 의사난수성 관점의 안전성 분석에 초점을 맞추었다. 최근 NIST에서 제안한 PRF 기반 Counter 모드, Feedback 모드, DPI 모드를 블록암호로 대표되는 PRP 기반 모드로 변형할 경우의 안전성을 의사난수성 관점에서 분석하였다. 블록암호와 같은 PRP를 핵심함수로 사용하는 KDF 구조에서는 Counter 값이 다른 입력값들과 XOR 연산되는 형태가 일반적이므로 이러한 형태로 변형된 NIST의 PRP 기반 KDF 구조를 제시하고 안전성을 논하였다. 그 결과 PRP 기반 Counter 모드와 Feedback 모드는 의사난수성 관점에서 취약하며, PRP 기반 DPI 모드는 의사난수성을 만족한다는 사실을 입증하였다.

키유도함수는 정보보호 관점에서 매우 중요한 역할을 하지만, 그 중요성에 비해 상대적으로 활발한 연구가 진행되고 있지 않은 실정이다. 따라서 본 논문은 아직 안전성 분석 관점에서 자세한 연구가 진행되지 않은 NIST의 PRF 기반 키유도함수에 대한 증명가능 안전성을 PRP 기반 모드로 변형한 특수한 형태에 대하여 의사난수성 관점에서 분석했다는 것에 그 의미를 둘 수 있다. 앞으로도 기존에 있던 키유도함수에 대한 안전성 분석 방법을 지속적으로 연구하여 개선하고 발전시킬 필요가 있다.

참고문헌

[1] ISO/IEC 18033-2:2006, Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers, Ed. Victor Shoup, 2006. The final committee draft version FCD 18033-2, Dec. 2004.

[2] IEEE P1363 Standard Specifications for Public Key Cryptography, IEEE, Nov. 1993.

[3] RSA Laboratories. PKCS #1 v2.1: RSA Encryption Standard. Jun. 2002, 〈download〉.

[4] ANSI X9.42-2003 Agreement of Symmetric Keys Using Discrete Logarithm Cryptography, American National Standards Institute, 19 Nov. 2003.

[5] NIST Special Publication 800-56A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, National Institute of Standards and Technology, Mar. 2007.

[6] IEEE 802.11i : "IEEE Standard for Information technology-Telecommunications and information exchange between systems -Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements," Jul. 2004.

[7] RSA Laboratories. PKCS #5 v2.1: Password-Based Cryptography Standard, 5 Oct. 2006.

[8] Bruce Schneier, Applied Cryptography - Protocols, Algorithms and Source Code in C, second edition, John Wiley, Nov. 1995.

[9] 3GPP TR 35.909 v8.0.0 : "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; 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*; Document 5: Summary and results of design and evaluation," Dec. 2008.

[10] IEEE 802.15.1TM : "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 15.1: Wireless medium access control (MAC)

and physical layer (PHY) specifications for wireless personal area networks (WPANs)," Jun. 2002.

[11] NIST Special Publication 800-108, "Recommendation for Key Derivation Using Pseudorandom Functions (Revised)," SP 800-108, Oct. 2009.

[12] C. Adams, G. Kramer, S. Mister, and R. Zuccherato, "On the security of key derivation functions," LNCS 3225, Springer-Verlag, pp 134-145, 2004.

[13] H. Gilbert, "The security of One-Block-to-Many modes of operation," FSE 2003, LNCS 2887, pp. 376-395, 2003.

[14] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," RFC2104, Feb. 1997.

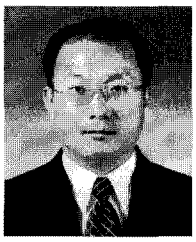
[15] Federal Information Processing Standards Publication 197, "Specification for the ADVANCED ENCRYPTION STANDARD (AES)," Non. 2001.

[16] J. Massey, G. Khachatrian, and M. Kuregian, "Nomination of SAFER+ as Candidate Algorithm for the Advanced Encryption Standard (AES)," NIST AES Proposal, 1998.

[17] J. Patarin, "New results on pseudorandom permutation generators based on the DES scheme," Advances in Cryptology - CRYPTO'91, LNCS 576, pp. 301-316, 1992.

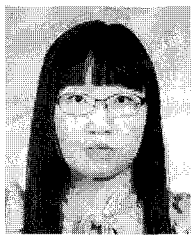
[18] S. Vaudenay, "On Provable Security for Conventional Cryptography," Proc. ICISC '99, invited lecture, LNCS 1787, pp. 1-16, 2000.

〈著者紹介〉



강 주 성 (Ju-Sung Kang)
1989년 고려대학교 수학과(학사)
1991년 고려대학교 일반대학원 수학과 (이학석사)
1996년 고려대학교 일반대학원 수학과 (이학박사)
1997년~ 2004년 한국전자통신연구원 선임연구원
2001년 ~ 2002년 벨기에 루벤대학 COSIC 방문연구원
2004년~ 현재 국민대학교 수학과 부교수
〈관심분야〉 암호이론, 정보보호이론, 응용확률론 등

이 옥 연 (Okyeon Yi)
e-mail : oyyi@kookmin.ac.kr
1988년 고려대학교 수학과 졸업
1990년 고려대학교 일반대학원 수학과 (이학석사)
1996년 University of Kentucky 수학과 (이학박사)
1999년~2001년 한국전자통신연구원 선임연구원, 팀장
2001년~현재 국민대학교 수학과 부교수
〈관심분야〉 정보보호, 이동통신, 암호론 등



염 지 선 (Ji-Sun Youm)
e-mail : bohun86@hanmail.net
2008년 국민대학교 수학과(학사)
2010년 국민대학교 일반대학원 수학과 (이학석사)
〈관심분야〉 암호이론, 정보보호이론 등