http://dx.doi.org/10.7840/kics.2016.41.4.479

양자키분배와 RSA 암호를 활용한 이중키 설정 키유도함수

박 호 중◆, 배 민 영*, 강 주 성**, 염 용 진°

Key Derivation Functions Using the Dual Key Agreement Based on QKD and RSA Cryptosystem

Hojoong Park◆, Minyoung Bae*, Ju-Sung Kang**, Yongjin Yeom°

요 약

안전한 통신 시스템을 갖추기 위해서는 안전한 암호 알고리즘의 사용과 안전한 암호키 사용이 필수적이다. 현대 암호에서는 표준화된 키유도함수(Key derivation function)를 통해 안전한 암호키를 생성한다. 최근에는 양자물리의 성질을 이용한 양자키분배(Quantum key distribution, 이하 QKD) 시스템에 대한 연구가 활발히 진행되고 있어, 현대 암호시스템의 안정성 향상에 기여할 수 있을 것으로 기대된다. 이러한 관점에서 양자 암호와 현대 암호를 결합한 이중키 설정에 대한 연구가 요구된다. 본 논문에서는 양자키분배(QKD)와 현대 암호시스템인 RSA를 조합하여 안전한 키를 생성하는 두 가지의 키유도함수를 제안한다. 또한, 시뮬레이션을 통하여 생성된 암호키의 엔트로피를 측정하는 방법으로 제안한 키유도함수의 유효성을 살펴본다.

Key Words : Key derivation function (KDF), Quantum key distribution (QKD), RSA, Dual key agreement, Entropy

ABSTRACT

For a secure communication system, it is necessary to use secure cryptographic algorithms and keys. Modern cryptographic system generates high entropy encryption key through standard key derivation functions. Using recent progress in quantum key distribution(QKD) based on quantum physics, it is expected that we can enhance the security of modern cryptosystem. In this respect, the study on the dual key agreement is required, which combines quantum and modern cryptography. In this paper, we propose two key derivation functions using dual key agreement based on QKD and RSA cryptographic system. Furthermore, we demonstrate several simulations that estimate entropy of derived key so as to support the design rationale of our key derivation functions.

Ⅰ. 서 론

안전한 통신 시스템 환경을 구축하기 위해서는 안전한 암호 알고리즘 사용과 함께 예측 불가능한 암호키 사용이 필수적이다. 정보이론에 기반을 둔 현대 암호에서는 엔트로피를 예측 불가능성의 측도로 하여,

※ This work was supported by ICT R&D program of MSIP/IITP.[10044559, 2014-044-014-002]
◆ First Author : Kookmin University Department of Financial Information Security, ruokay@kookmin.ac.kr, 학생회원
° Corresponding Author : Kookmin University Department of Math. / Financial Information Security, salt@kookmin.ac.kr, 종신회원
* Kookmin University Department of Financial Information Security, mypear@kookmin.ac.kr, 학생회원
** Kookmin University Department of Math. / Financial Information Security, jskang@kookmin.ac.kr, 정회원
논문번호 : KICS2016-01-024, Received January 31, 2016; Revised April 6, 2016; Accepted April 21, 2016

엔트로피가 높은 암호키를 생성하기 위한 연구를 활발히 진행하고 있다. 현대 암호에서 이를 위해 키유도함수(Key derivation function, 이하 KDF)를 사용한다. 현재 사용되고 있는 KDF의 대표적인 표준으로는 의사난수생성 알고리즘을 사용하여 키를 생성하는 NIST SP 800-108[1], 패스워드 기반 KDF인 NIST SP 800-132[2], HMAC 기반 KDF인 RFC-5869[3] 등이 있다.

한편, 예측 불가능한 양자물리의 특성을 이용하여 키를 생산하는 양자키분배(Quantum key distribution, 이하 QKD) 방법에 대한 연구가 활발히 진행되고 있다. 예를 들면, 양자 암호시스템인 QKD는 높은 엔트로피의 암호키를 출력하는 장점을 가지고 있지만, 출력속도가 느리기 때문에 고속 현대 암호와 결합하여 사용한다. 따라서 양자 암호의 안전성뿐만 아니라 결합방법과 적용하는 현대 암호시스템의 안전성을 함께 고려해야 한다.

이에 본 논문에서는 양자 암호와 현대 암호를 결합하는 이중키 설정 키유도함수 모델 두 가지를 제안한다. 이 키유도함수들은 상호 보완적인 구조를 가지고 있기 때문에, 한쪽 시스템이 불안정하여도 안전한 암호키를 생성할 수 있으며 입력 데이터의 낭비를 최소화할 수 있는 특징을 가진다.

1.1 이중키 설정에 대한 연구 배경

이중키 설정(Dual key agreement)이란 양자 암호시스템과 현대 암호시스템을 조합하여 엔트로피가 높은 암호키를 분배하는 시스템으로 두 채널의 키 요소로부터 가장 안전한 키를 얻어내는 Parallel key agreement으로 분류된다[4]. 이중키 설정에 대한 연구는 스위스 ID Quantique의 네트워크 장비인 CERBERIS[5]를 통해 진행되고 있었음을 확인할 수 있다. 하지만 CERBERIS의 이중키 설정에 대해 알려진 정보는 양자 암호시스템인 QKD와 현대 암호시스템인 RSA를 사용하고 있는 것만 명시되어 있을 뿐 세부적인 구조에 대해서는 알려져 있지 않다. 한편, 최근 양자 암호시스템이 적용된 Parallel key agreement에 대한 연구는 현대 암호시스템인 RSA, 디지털 서명구조 등을 적용하여 양자 암호시스템의 인증 문제를 보완하는 연구 방향으로 진행되고 있다[6,7]. 이에 본 논문에서는 현대 암호시스템의 역할을 인증에 한정하지 않고, 양자 암호시스템과 결합하여 안정적으로 엔트로피가 높은 키를 출력하는 키유도함수를 제안한다. 제안하는 키유도함수는 양자 채널 QKD와 현대 암호 채널(Classic channel) RSA-OAEP 2048[8]을 이용하여 NIST 표준 기반 키유도함수 모델과 확률론적 이론 기반 키유도함수 모델을 제안한다. 표준 기반 키유도함수(이하 HMAC KDF)는 미국 NIST SP 800-56C[9]를 바탕으로 HMAC을 키유도함수의 알고리즘으로 활용하여 설계하였고, 확률론적 이론 기반 키유도함수(이하 Hankel matrix KDF)는 Leftover Hash Lemma를 그 이론적 기반으로 Hankel matrix를 사용하여 설계하였다. 두 키유도함수는 서로 다른 특징을 가지고 있기 때문에 사용되는 환경에 따라 적합한 키유도함수를 선택할 수 있도록 전체 구조를 그림 1과 같이 설계하였다.

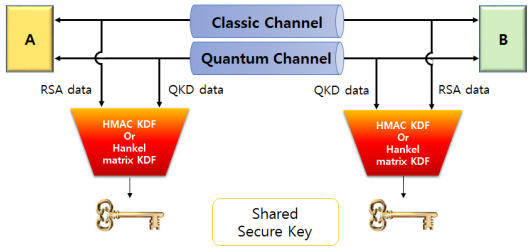

그림 1. 이중키 설정 키유도함수 구조
Fig. 1. Structure of dual key agreement KDF

현대 암호 채널에는 선택 암호문 공격(Chosen ciphertext attack)에 내성을 가지는 공개키 암호 알고리즘 RSA-OAEP 2048을 사용하여 키 요소를 공유하고, KDF에서는 이를 양자 채널인 QKD에서 생성한 데이터와 결합하여 암호키를 생성한다. 이때 사용되는 환경에 맞게 HMAC KDF 또는 Hankel matrix KDF를 선택하여 엔트로피가 높은 암호키를 생성하는 구조를 가지고 있다. 각각의 키유도함수에 대한 자세한 내용은 3장에서 다루겠다.

1.2 주요 결과

본 논문에서는 환경에 적합한 방식을 선택하여 구현하도록 다음과 같은 QKD와 RSA 기반 키유도함수 모델 두 가지를 제안한다.

○ HMAC KDF
- NIST의 SP 800-56B[10]와 SP 800-56C[9] 표준에 근거하여 암호키의 안전성을 보장받는다.
- 양자와 현대 암호시스템 중 하나의 정상동작만 확보되면 안전한 키를 생성할 수 있다.

○ Hankel matrix KDF
- Leftover Hash Lemma에 근거하여 출력한 암호키의 안전성을 보장받는다.
- Hankel matrix를 이용한 유니버설 해쉬 함수족을 구성함으로써 행렬에 사용되는 데이터양을

절약할 수 있다.

- 주기적으로 QKD 데이터의 엔트로피를 측정하여 압축 비율을 조절함으로써 QKD 데이터의 낭비를 최소화 할 수 있다.

사용 환경에 적합하도록 선택할 수 있는 두 키유도함수는 안전한 암호 통신을 위해 필수적인 비밀키 갱신 알고리즘으로 사용될 것으로 기대된다[11].

Ⅱ. KDF 설계를 위한 안전성 이론

이중키 설정 키유도함수 중 Hankel matrix KDF의 안전성에 대한 이론적 근거를 제공하는 수학적 사실은 Leftover Hash Lemma이다. 먼저, 이를 이해하는데 필요한 정의를 소개하고 Leftover Hash Lemma는 그 내용만을 언급하기로 한다. 또한, 두 키유도함수의 출력 엔트로피 측정에는 SP 800-90B에 정의된 IID (Independent and Identically Distributed) 데이터의 엔트로피 측정방식을 사용한다.

2.1 Leftover Hash Lemma

정의 1. 최소 엔트로피(Min-entropy)[12]

표본공간 U를 갖는 두 확률변수 X에 대하여, X의 최소 엔트로피(Min-entropy)를 다음과 같이 정의한다.

$$H_{\infty}(X) = -\log_2\left(\max_{u\in U} p(X=u)\right) .$$

정의 2. 통계적 거리(Statistical distance)[13]

표본공간 U를 공통으로 갖는 두 확률변수 X, Y에 대한 통계적 거리는

$$\Delta(X, Y) \equiv \frac{1}{2}\sum_{u\in U}|\Pr[X=u]-\Pr[Y=u]|$$

로 정의된다. 통계적 거리는 두 분포의 유사성을 비교하는 측도로 사용된다.

정의 3. (k,ϵ)-strong extractor[14]

정수 $d, k, m, n > 0$ 와 실수 $\epsilon > 0$에 대하여, U_d, U_m은 각각 d-비트와 m-비트 공간에서의 균등분포이다. 임의의 n-비트 확률변수 X가 $H_{\infty}(X) \geq k$를 만족하고 U_d와 X는 서로 독립이라 하자. 이때, 두 입력을 가진 Extractor $Ext: \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$이 통계적 거리 Δ에 대해

$$\Delta\big(\big(Ext(X, U_d),\ U_d\big), \big(U_m, U_d\big)\big) < \epsilon$$

을 만족하면, 이 Extractor는 (k,ϵ)-strong extractor라 한다. 단, $\big(Ext(X, U_d),\ U_d\big)$와 $\big(U_m, U_d\big)$에서 $(\cdot,\cdot)$는 결합분포(joint distribution)를 의미한다.

정의 4. 유니버설 해쉬 함수족(Universal hash family)[14,15]

정수 $d, m, n > 0$에 대하여, 원소의 개수가 2^d개인 함수족

$$H = \left\{h_i : \{0,1\}^n \rightarrow \{0,1\}^m \mid 0 \leq i \leq 2^d - 1\right\}$$

가 임의의 $x, y \in \{0,1\}^n$, $x \neq y$ 에 대하여

$$\Pr_{h\in H}[h(x) = h(y)] \leq 2^{-m}$$

을 만족하면, H를 유니버설 해쉬 함수족이라 한다. 이때 유니버설 해쉬 함수족은 일반적으로 출력의 균등성 보장을 통한 비밀성 증폭(Privacy amplification)에 사용된다[15,16].

정리 1. Leftover Hash Lemma[13,14]

임의의 n-비트 확률변수 X가 $H_{\infty}(X) \geq k$를 만족하고, $\epsilon > 0$이라 하자.

$$H = \left\{h_i : \{0,1\}^n \rightarrow \{0,1\}^m \mid i \in \{0,1\}^d\right\}$$

이 유니버설 해쉬 함수족이고, $m \leq k - 2\log(1/\epsilon)$을 만족할 때,

$$Ext(X, h_i) = h_i(X) \quad , \quad \forall h_i \in H$$

로 정의된 Extractor는 $(k, \epsilon/2)$-strong extractor가 된다.

2.2 SP 800-90B의 엔트로피 추정법[12]

NIST SP 800-90B는 잡음원의 엔트로피를 측정하기 위한 표준문서로 암호모듈의 검증제도(CMVP, Cryptographic Module Validation Program)[17]에서 사용되는 난수발생기의 안전성 평가기준이다. SP

800-90B는 2015년 Whitewood사에서 개발한 양자난수발생기 "Whitewood Entropy Engine"의 안전성 검증에도 사용되었다[18].

이 문서에 따르면, IID 데이터의 엔트로피 추정법은 다음과 같다.

샘플의 개수를 N, 가장 많이 나온 사건(event)의 개수를 C라 하고, 전체에서 C가 발생한 비율을 $pmax = C/N$라 하자. 이때 엔트로피를 추정하기 위해 C의 99% 상계(upper bound)를

$$C_{BOUND} = C + 2.3\sqrt{N \times pmax(1-pmax)}$$

로 정의하여 최소 엔트로피(Min-entropy)

$$H_{\infty} = -\log_2(C_{BOUND}/N)$$

으로 추정한다.

이 정의에 따르면, 샘플 공간이 $\{0,1\}$ 인 비트열에서 0과 1의 비율이 정확히 0.5인 이상적인 분포의 경우, 최소 엔트로피 추정 결과는 0.997 이상으로 판정한다.

Ⅲ. 이중키 설정 키유도함수의 구성 및 특징

3.1 이중키 설정 키유도함수

이중키 설정 키유도함수는 양자 암호시스템인 QKD와 현대 암호시스템인 RSA를 조합하여 안정적으로 엔트로피가 높은 키를 생성하는데 그 목적을 두고 있다. 우리가 제안하는 이중키 설정 키유도함수는 미국 NIST SP 800-56C와 SP 800-108 표준에 안전성 기반을 둔 HMAC KDF와 확률론적 이론인 Leftover Hash Lemma에 안전성 기반을 둔 Hankel matrix KDF 두 모델이다. HMAC KDF은 양자 시스템과 현대 암호시스템 모두가 어느 정도 불안정하더라도 입력 엔트로피에 따른 데이터 크기 조정을 통해 안전한 암호키를 출력할 수 있는 장점을 가지고 있다. 한편 Hankel matrix KDF는 입력되는 QKD 데이터의 엔트로피에 대응하도록 크기가 가변적인 행렬을 생성하여 데이터 요소의 낭비를 최소화할 수 있는 장점을 가지고 있다.

3.1.1 HMAC KDF

HMAC KDF는 NIST SP 800-56C와 NIST SP 800-108의 표준에 근거하여 설계되었다. NIST 표준

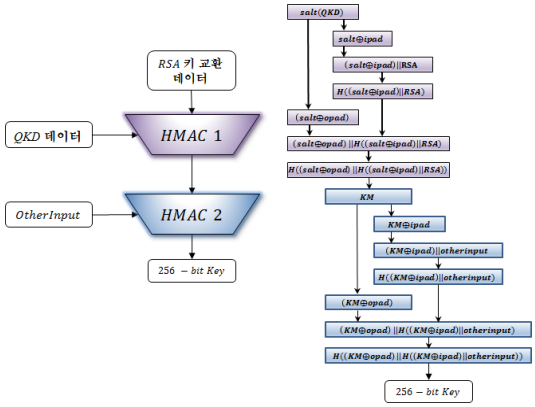

그림 2. HMAC KDF의 구조
Fig. 2. Structure of HMAC KDF

을 참조하여 설계하였기 때문에 HMAC KDF의 안전성 근거는 NIST 표준에서 획득할 수 있다. 표준을 바탕으로 키유도함수의 내부를 HMAC으로 선정하였고, HMAC을 구성하는 내부함수로 SHA-256[19]을 사용하였다. 기존 NIST SP 800-56C의 압축-확장(Extraction-then-expansion) 구조로 두 개의 HMAC을 사용할 수 있다. 하지만 제안하는 HMAC KDF는 확장함수 HMAC 2를 변형한 구조로 HMAC 2의 ctr 값을 고정하여 사용하는 구조이다. 설계한 HMAC KDF는 그림 2와 같다.

키유도함수 알고리즘에 사용되는 매개변수 중 암호키, 인증 데이터와 같이 변조 또는 노출되면 모듈의 안전성에 영향을 미치는 매개변수를 중요보안매개변수(Sensitive security parameter)라고 한다. 다음 표 1은 HMAC KDF에 사용되는 중요보안매개변수를 정리해놓은 것이다.

HMAC 2에 사용되는 중요보안매개변수 OtherInput은 ctr, Label, context, $[L_2]$로 구성되어있다. HMAC KDF의 HMAC 2는 확장하는 구조가 아니기 때문에 ctr을 0x00000001로 고정하고, Label과 context부분은 TTA 표준[20]에 근거하여 설계하였다.

표 1. HMAC KDF의 중요보안매개변수
Table 1. Sensitive security parameter of HMAC KDF

Parameter	Value
Salt	QKD data (512 bits or more)
Z	RSA key exchange data (512 bits or more)
KDK	Result of HMAC 1
OtherInput	ctr||Label||context||$[L_2]$

또한, [L_2]는 HMAC 1 결과인 K_{DK}의 길이 256 비트를 이진으로 표현한 값 0x00000100으로 사용한다.

한편, HMAC KDF에서 출력된 암호키가 Full-entropy로 주장되는 근거는 NIST SP 800-90B의 엔트로피 추정법에서 찾을 수 있다. NIST SP 800-90B에서는 미국 FIPS 표준으로 제정된 알고리즘을 후처리(conditioning) 함수로 사용하고 측정된 입력 엔트로피가 출력 길이의 2배 이상이면 출력의 엔트로피를 Full-entropy로 인정한다. HMAC KDF는 입력 엔트로피를 출력 길이의 2배 이상으로 설계를 하였기 때문에 이 KDF로부터 출력된 암호키는 Full-entropy를 갖는다고 할 수 있다.

또한, NIST SP 800-90B 엔트로피 추정법을 근거로 QKD 시스템과 RSA 시스템 중 어느 하나에 이상이 발생하더라도 Full-entropy를 얻을 수 있는 조건인

입력 엔트로피의 크기 ≥ 출력 길이×2

만 만족시켜주면, HMAC KDF는 안전한 암호키를 출력한다고 주장할 수 있다.

3.1.2 Hankel matrix KDF

Hankel matrix KDF는 정리 1의 Leftover Hash Lemma를 안전성의 근거로 두고 있다. Leftover Hash Lemma를 키유도함수에 적용하기 위해서는 다음 조건을 만족해야 한다. 첫째, 두 입력이 독립이어야 한다. 둘째, Extractor로 유니버설 해쉬 함수족을 사용해야한다. 마지막으로 $m \le k-2\log(1/\epsilon)$ 을 만족해야 한다. 이때 m은 출력의 길이, k는 입력의 최소 엔트로피, ϵ은 출력 분포와 균등분포와의 통계적 거리를 나타낸다. 제안하는 Hankel matrix KDF를 도식화하면 그림 3과 같다.

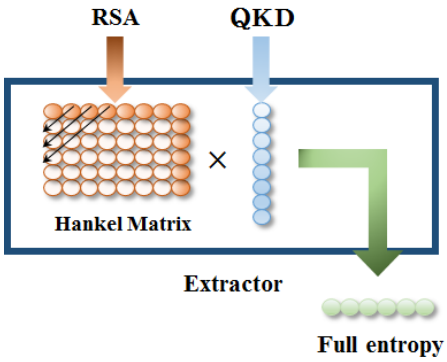

그림 3. Hankel matrix KDF의 구조
Fig. 3. Structure of Hankel matrix KDF

먼저, 논문에서 사용하는 이중키 설정은 QKD와 RSA의 독립적인 두 개의 채널을 사용했기 때문에 두 입력이 독립이어야 한다는 첫 번째 조건을 정확히 만족시킨다. 또한 유니버설 해쉬 함수족으로 사용할 수 있는 Hankel matrix를 적용하여 조건을 만족시켰다[15]. 랜덤 행렬을 이용한 해쉬 함수족과 달리, Hankel matrix는 그림 4와 같이 '┐' 만큼의 데이터만으로 행렬을 생성할 수 있기 때문에 행렬을 생성에 사용되는 데이터를 절약할 수 있다.

수식 $m \le k-2\log(1/\epsilon)$ 을 이용하여 입력되는 QKD 데이터의 엔트로피 밀도(Entropy density, s=k/n)에 따라 유동적으로 행렬 크기를 조절할 수 있도록 설계하였다. 표 2는 $m \le k-2\log(1/\epsilon)$ 수식을 이용하여, 키유도함수의 출력 분포와 균등분포 사이의 통계적 거리가 $\epsilon = 2^{-100}$ 이하, 출력된 암호키의 크기가 128 비트 또는 256 비트인 경우에 엔트로피 밀도에 대응하는 행렬 크기의 예시를 나타낸다.

만약 QKD 데이터의 엔트로피 밀도가 0.76인 경우 128 비트의 암호키를 얻기 위해서는 128×480 크기 이상의 행렬을 사용해야한다. 또한 구현의 편의를 위하여 행렬 크기는 32의 배수로 설정하였다.

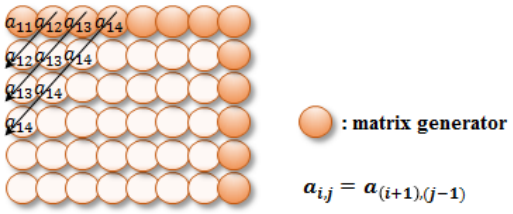

그림 4. Hankel matrix 생성
Fig. 4. Generation of Hankel matrix

표 2. 엔트로피 밀도 s에 대응하는 행렬 크기
Table 2. Matrix size corresponding entropy density s

s≥	Key size(m) 128	Key size(m) 256
0.9	128×384	256×512
0.8	128×416	256×576
0.7	128×480	256×672
0.6	128×576	256×768
0.5	128×672	256×928

3.2 제안하는 키유도함수의 특징

3.1절에서는 논문에서 제안한 이중키 설정 키유도함수 두 모델 HMAC KDF와 Hankel matrix KDF의 설계 사상을 다루었다. 본 절에서는 앞에서 다룬 키유도함수의 설계 사상을 바탕으로 두 키유도함수의 특징을 제시한다. 두 모델 가진 장점이 각각 다르기 때문에 키유도함수를 사용하는 환경에 적합한 함수를 선택적으로 적용할 수 있는 장점이 있다. 두 가지의 키유도함수의 장·단점을 요약하면 다음과 같다.

○ HMAC KDF

- 장점
  - 양자 암호 채널 QKD와 현대 암호 채널 RSA 중 하나의 정상동작만 확보되면 안전한 키를 생성.
  - 표준 현대 암호기술에 근거한 출력의 안전성.
- 단점
  - NIST SP 800-90B의 엔트로피 추정법에 근거하여 안전성을 보장받지만, 증명가능 안전성을 제공하지는 않음.

○ Hankel matrix KDF

- 장점
  - Leftover Hash Lemma가 적용됨으로써 출력의 안전성을 이론적으로 보장.
  - 데이터의 엔트로피에 대응하는 행렬 크기 조정으로 QKD 데이터 낭비 최소화.
- 단점
  - 이론적인 안전성을 보장받기 위하여 행렬 생성 데이터인 RSA 키 교환 데이터의 Full-entropy 조건이 만족되어야 함.

Ⅳ. 실험 및 결과

4.1 실험 목적

본 논문에서 제시한 두 가지 이중키 설정 키유도함수의 유효성과 효율성을 입증하기 위하여 실험을 진행하였다. 두 키유도함수의 유효성을 확인하기 위해 두 채널이 모두 정상 작동하는 경우, QKD 채널의 입력 엔트로피가 저하된 발생한 경우, 두 채널의 입력 엔트로피가 모두 저하된 경우의 세 가지 시나리오를 구상하고 각각에 대한 실험을 실시하였다. 위 시나리오에 적용시키기 위해 실험대상으로는 엔트로피 0.987, 0.977, 0.628, 0.610인 데이터를 선정하였다. 이때, 엔트로피가 0.628, 0.610인 데이터를 두 채널의 입력 엔트로피가 저하된 경우로 설정하였다. 그 이유는 첫째, QKD란 그 자체 출력을 키로 사용할 수 있는 시스템이기 때문에 CMVP 기준에 의해 엔트로피 밀도가 0.875이상을 만족해야한다는 것에 있다[21]. 둘째, HMAC KDF 설계에서 상수를 고정값으로 사용하였기 때문이다. 이는 키유도함수의 출력 엔트로피가 두 채널의 상태에만 영향 받음을 의미한다. 이때, 두 채널에 문제가 발생하여 데이터의 엔트로피가 낮은 경우에는 3.1.1에 작성한 NIST SP 800-90B 기준에 근거하면 Full-entropy의 키를 얻기 위해 요구되는 데이터량이 증가됨을 의미한다. 즉, 키유도함수의 출력을 저하시키는 결과를 가져온다.

두 키유도함수의 유효성을 측정하기 위해 2장에 작성한 NIST SP 800-90B의 IID 데이터 엔트로피 추정법을 사용하였다. 이를 측정하기 위하여 통계적 난수성 평가도구[22]를 이용하였다. 또한 HMAC KDF와 Hankel matrix KDF의 효율성을 비교하기 위한 방법으로 약 4,000번 반복하여 속도(cycles/bit)를 측정하여 그 평균값을 비교하는 방법을 선택하였다.

4.2 실험 환경 및 방법

두 키유도함수에 대한 유효성 및 효율성에 대한 실험은 다음과 같은 환경에서 진행되었다.

- 구현 프로그램 : Microsoft Visual Studio 2013
- Windows 버전 : Windows 7 Professional K
- 프로세서 : Intel(R) Core(TM) i7-4770K CPU @ 3.5GHz
- 시스템 RAM : 16.0GB
- 시스템 종류 : 64비트 운영체제

실험은 NIST 표준과 Leftover Hash Lemma을 바탕으로, 먼저 입력 데이터의 엔트로피에 대응하는 데이터의 최소 크기를 계산한다. NIST SP 800-90B 방법으로 엔트로피를 측정하기 위해서는 최소 1,000,000 비트가 필요하다. 1,000,000 비트의 출력을 얻기 위해 256 비트를 출력하는 KDF를 약 4,000번 반복하여 수집하였다. 통계적 난수성 평가도구로 데이터의 IID 여부를 확인하고 IID 엔트로피 추정을 통해 데이터의 엔트로피를 측정하게 된다. 또한 키유도함수를 실행하여 측정된 약 4,000개의 cycles/bit의 평균값을 저장한다.

앞에서 언급한 세 가지 시나리오로 실험을 하는데 있어서 편의를 위해, 두 채널이 모두 정상동작하는 경우를 시나리오 1, QKD 채널의 입력 엔트로피가 저하된 경우를 시나리오 2, 두 채널의 입력 엔트로피가 모두 저하된 경우를 시나리오 3으로 명명한다. 한편, 시

나리오 3에서 Hankel matrix KDF에 대한 실험은 행렬 생성에 Full-entropy가 사용되어야 한다는 Leftover Hash Lemma의 조건에 위배되기 때문에 진행하지 않았다.

○ 시나리오 1 : 두 채널 모두 정상인 경우

- QKD 데이터의 엔트로피 밀도 : 0.977
- RSA 키 교환 데이터의 엔트로피 밀도 : 0.987

① HMAC KDF

HMAC KDF는 내부함수를 SHA-256을 쓰고 있기 때문에 입력 데이터의 엔트로피가 512 비트 이상이 필요하다. 그림 2를 참고하면 Full-entropy 키를 얻기 위해서는 최소 256 비트의 엔트로피를 가진 QKD 데이터와 최소 512 비트의 엔트로피를 가진 RSA 키 교환 데이터가 요구된다. 이때 시나리오 1의 입력되는 RSA 키 교환 데이터와 QKD 데이터가 Full-entropy에 근접하기 때문에 각각 512 비트면 충분하다.

② Hankel matrix KDF

입력되는 QKD 데이터의 엔트로피가 0.977로 측정되었기 때문에 표 2를 참고하여 256×512 행렬을 생성한다. 이때 행렬 생성에 사용되는 RSA 키 교환 데이터는 767(=256+512-1) 비트이고 입력되는 QKD 데이터는 512 비트이다.

○ 시나리오 2 : QKD 채널의 입력 엔트로피가 저하된 경우

- QKD 데이터의 엔트로피 밀도 : 0.610
- RSA 키 교환 데이터의 엔트로피 밀도 : 0.987

① HMAC KDF

시나리오 2의 입력되는 QKD 데이터의 엔트로피가 0.610이므로 512 비트를 입력했을 때, 약 312 비트의 엔트로피를 갖는다. 따라서 Full-entropy 암호키를 출력하는데 각각 512 비트만 있어도 충분하다.

② Hankel matrix KDF

입력되는 QKD 데이터의 엔트로피가 0.610으로 측정되었기 때문에 표 2를 참고하여 256×768 행렬을 생성한다. 이때 행렬 생성에 사용되는 RSA 키 교환 데이터는 1,023(=256+768-1) 비트이고 입력되는 QKD 데이터는 768 비트이다.

○ 시나리오 3 : 두 채널의 입력 엔트로피가 모두 저하된 경우

- QKD 데이터의 엔트로피 밀도 : 0.610
- RSA 키 교환 데이터의 엔트로피 밀도 : 0.628

① HMAC KDF

RSA 키 교환 데이터의 엔트로피 밀도가 0.628이므로 512 비트의 엔트로피를 보유하기 위해서는 최소 812 비트가 필요하다. 또한, QKD 데이터는 512 비트이므로 Full-entropy의 암호키를 얻기 위한 요구조건을 만족시킨다.

② Hankel matrix KDF

설계사상을 적용할 수 없으므로 실행하지 않음.

표 3. 시나리오별 KDF 종류 및 실험 데이터 크기
Table 3. KDF type and input data for each test

Scenario	KDF Type	Input data Size (bit)		Entropy / bit
1	HMAC	QKD	512	0.977
		RSA	512	0.987
	Hankel matrix	QKD	512	0.977
		RSA	767	0.987
2	HMAC	QKD	512	0.610
		RSA	512	0.987
	Hankel matrix	QKD	768	0.610
		RSA	1,023	0.987
3	HMAC	QKD	512	0.610
		RSA	812	0.628
	Hankel matrix	N/A		

세 가지 시나리오를 실험하여 키유도함수에서 출력한 데이터의 엔트로피 측정을 통해 제안한 키유도함수의 유효성을 확인한다. 표 3은 Full-entropy 암호키를 얻기 위한 시나리오에 따른 입력 데이터의 크기를 정리한 것이다. 한편, 효율성을 측정하는 방법으로는 최신 해쉬 함수 KECCAK의 효율성을 측정하는데 사용한 Cycles per byte(cpb)를 적용하였다[23]. 이때 제안한 키유도함수는 정해진 크기의 출력을 얻는데 사용되므로 cycles/bit를 비교하는 것이 타당하다.

4.3 실험 결과

4.3.1 두 채널이 모두 정상동작하는 경우

시나리오 1은 두 채널이 모두 정상동작하는 경우 키유도함수에서 Full-Entropy의 키를 출력하는지 확인하는 실험이다. 먼저 Hankel matrix KDF에 0.977인 QKD 데이터 512 비트를 입력하여 출력된 1,000,000 비트 키에 대한 엔트로피 측정 결과, 키 데

이터는 IID로 판정되었고 이때 데이터의 엔트로피는 그림 5와 같이 0.990으로 측정되었다. 같은 방법으로 HMAC KDF에 0.977인 QKD 데이터 512 비트를 입력하여 출력된 1,000,000 비트 키에 대한 엔트로피 측정 결과, 키는 IID로 판정되었고 이때 데이터의 엔트로피는 0.985로 측정되었다.

한편, 알고리즘 효율성을 측정했을 때 Hankel matrix KDF가 평균 351.9 cycles/bit, HMAC KDF 평균 88.3 cycles/bit 로 측정되었다. 이를 통해 Hankel matrix KDF보다 HMAC KDF의 효율성이 더 높다고 할 수 있다.

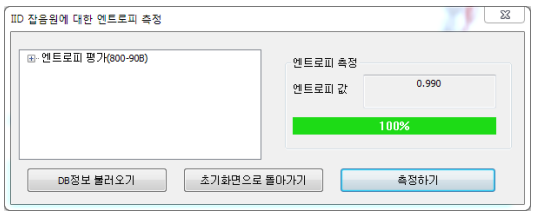

그림 5. 시나리오 1의 Hankel matrix KDF의 출력 엔트로피
Fig. 5. Output entropy of Hankel matrix KDF in scenario 1

4.3.2 QKD 채널의 입력 엔트로피가 저하된 경우

시나리오 2는 QKD 채널의 입력 엔트로피가 저하된 경우에서도 두 키유도함수가 Full-entropy 키를 출력하는지 확인하는 실험이다. 먼저, Hankel matrix KDF에 0.610인 QKD 데이터 768 비트를 입력하여 출력된 1,000,000 비트 키에 대한 엔트로피 측정 결과, 데이터는 IID로 판정되었고 이때의 엔트로피는 0.989로 측정되었다. 같은 방법으로 HMAC KDF에 0.610인 QKD 데이터 512 비트를 입력하여 출력된 1,000,000 비트 키에 대한 엔트로피 측정 결과, 키 데이터는 IID로 판정되었고 이때의 엔트로피는 0.988로 측정되었다.

한편, 알고리즘 효율성을 측정했을 때 Hankel matrix KDF가 평균 487.7 cycles/bit, HMAC KDF 평균 89.3 cycles/bit 로 측정되었다. 이를 통해 Hankel matrix KDF보다 HMAC KDF의 효율성이 더 높다고 할 수 있다.

4.3.3 두 채널의 입력 엔트로피가 모두 저하된 경우

시나리오 3은 두 채널의 입력 엔트로피가 모두 저하된 경우에도 HMAC KDF가 Full-entropy 키를 출력하는지 확인하는 실험이다. HMAC KDF에 0.628인 QKD 데이터를 입력하여 출력된 1,000,000 비트 키에 대한 엔트로피 측정 결과, 키 데이터는 IID로 판정되었으며 이때의 엔트로피는 0.986으로 측정되었다. 또한 HMAC KDF가 평균 90.8 cycles/bit로 측정되었다.

실험 결과를 통해 Hankel matrix KDF와 HMAC KDF는 입력되는 QKD 데이터의 엔트로피가 낮더라도 이론적 조건만 만족시켜주면 Full-entropy에 근접한 데이터를 출력하는 것을 확인할 수 있다. 또한 효율성 측면으로 보았을 때 Hankel matrix KDF보다는 HMAC KDF가 더 우수하다고 판단할 수 있다. 표 4는 시나리오에 따른 키유도함수의 결과를 정리한 것이다.

표 4. 시나리오에 따른 키유도함수의 출력 결과
Table 4. KDF output for corresponding to each test scenario

Scenario	KDF Type	Entropy of Output data (entropy/bit)	Efficiency (cycles/bit)
1	HMAC	0.985	88.3
	Hankel matrix	0.990	351.9
2	HMAC	0.988	89.3
	Hankel matrix	0.989	487.7
3	HMAC	0.986	90.8
	Hankel matrix	N/A	

V. 결 론

본 논문에서는 사용 환경에 따라 적합한 키유도함수를 선택할 수 있도록 두 가지 이중키 설정 키유도함수 모델을 제안하였다. 먼저 HMAC KDF의 경우 '입력 데이터의 엔트로피 ≥ 출력 길이×2'의 조건을 만족시키면 어떠한 환경에서라도 안전한 암호키를 생성할 수 있는 장점을 가진다. 또한 실험을 통해 알고리즘 효율성 측면에서도 Hankel matrix KDF보다 약 5배 정도 우수함을 알 수 있었다. 반면, Hanekel matrix KDF는 행렬 생성 데이터가 Full-entropy이어야 한다는 제약조건이 있지만, 안전성을 증명해주는 Leftover Hash Lemma라는 확실한 이론적 근거가 있다는 점과 QKD 데이터의 엔트로피에 따른 압축률 조정으로 데이터의 낭비를 줄일 수 있다는 장점을 가진다. 알고리즘 최적화 구현을 중심으로 두 키유도함수의 정확한 효율성 분석을 추후 연구과제로 남긴다.

References

[1] NIST, *Recommendation for Key Derivation Using Pseudorandom Functions*, SP 800-108, Oct. 2009.

[2] NIST, *Recommendation for Password-Based Key Derivation*, SP 800-132, Dec. 2010.

[3] H. Krawczyk and P. Eronen, *Hmac-based extract-and-expand key derivation function (hkdf)*, RFC 5869 (Proposed Standard), May 2010.

[4] ID Quantique, *KEY SERVER*, Retrieved Mar., 26 from http://swissquantum.idquantique.com/?Key-Server#Parallel_Key_Agreements.

[5] ID Quantique, *CERBERIS*, from http://www.idquantique.com/wordpress/wp-content/uploads/Cerberis-Datasheet.pdf.

[6] R. Sarath and A. Shajin Narguman, "Key distribution using dual channel technique for ultimate security," *Indian J. Sci. and Technol.*, vol. 8, no. 26, 2015.

[7] A. Odeh, K. Elleithy, M. Alshowkan, and E. Abdelfattah, "Quantum key distribution by using public key algorithm(RSA)," *IEEE INTECH 2013*, pp. 83-86, London, UK, Aug. 2013.

[8] ISO/IEC, *Information technology- Security technique –Encryption algorithms-Part 2: Asymmetric ciphers*, ISO/IEC 18033-2, May 2006.

[9] NIST, *Recommendation for Key Derivation through Extraction-then –expansion*, SP 800-56C, Nov. 2011.

[10] NIST, *Recommendation for Pair-Wise key establishment schemes using integer factorization cryptography*, SP 800-56B, Sept. 2014.

[11] Y. S. Kim, "Group key transfer protocol based on shamir's secret sharing," *J. KICS*, vol. 39B no. 9, pp. 555-560, 2014.

[12] NIST, *Recommendation for the entropy sources used for random bit generation*, SP 800-90B, Aug. 2012.

[13] T. Matthias and R. Renner, *A randomness extractor for the Quantis device*, vol. 31. Id Quantique Technical Report, 2012.

[14] B. Barak, Y. Dodis, H. Krawczyk, O. Pereira, K. Pietrzak, F. Standaert, and Y. Yu, *Leftover hash lemma, revisited*, Sept. 2011.

[15] G. V. Assche, *Quantum cryptography and secret-key Distillation*, CAMBRIDGE, 2012.

[16] S. Im, H. Jeon, and J. Ha, "A novel distributed secret key extraction technique for wireless network," *J. KICS*, vol. 39A, no. 12, pp. 708-717, 2014.

[17] K. J. Ha, C. H. Seo, and D. Y. Kim, "Design of validation system for a crypto-algorithm implementation," *J. KICS*, vol. 39B no. 04, pp. 242-250, 2014.

[18] Whitewood, *Whitewood Entropy Engine*, Retrieved Jan., 23 from http://www.whitewoodencryption.com/wp-content/uploads/2015/08/Whitewood_EE.pdf.

[19] NIST, *Secure Hash Standard(SHS)*, FIPS 180-4, Aug. 2015.

[20] TTA, *Key Derivation Functions Using ARIA/SEED*, TTAK.KO-12.0241, Jul. 2014.

[21] NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*, Jan. 2016.

[22] H. Kang, Y. Yeom, and J. S. Kang, "An implementation of integrated tool for statistical randomness tests and entropy estimations," in *Proc. KICS Winter Conf. 2016*, Jeongseon, Korea, Jan. 2016.

[23] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, *The KECCAK sponge function family*, Retrieved Jan., 25 from http://keccak.noekeon.org.

박 호 중 (Hojoong Park)

2015년 2월 : 국민대학교 수학과 학사

2015년 3월~현재 : 국민대학교 금융정보보안학과 석사

<관심분야> 암호이론, 정보보호 알고리즘 및 프로토콜, 난수성 분석

배 민 영 (Minyoung Bae)

2016년 2월 : 국민대학교 수학과 학사

2016년 3월~현재 : 국민대학교 금융정보보안학과 석사

<관심분야> 암호이론, 병렬구현, 정보보호 프로토콜

강 주 성 (Ju-Sung Kang)

1989년 2월 : 고려대학교 수학과 학사

1991년 2월 : 고려대학교 수학과 석사

1996년 2월 : 고려대학교 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)

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~현재 : 국민대학교 수학과 부교수

2013년~현재 : 국민대학교 BK21+ 미래 금융정보보안 인력양성사업단 교수

<관심분야> 암호구현 및 분석, 보안시스템 평가