The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 18, No. 5, pp.111-116, Oct. 31, 2018. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2018.18.5.111
JIIBC 2018-5-14

양자 키 분배 시스템에서 보안성 증폭의 성능 분석

Performance of privacy Amplification in Quantum Key Distribution Systems

이선의*, 김진영**

Sun-Yui Lee*, Jin-Young Kim**

요 약 본 논문은 양자 키 분배 시스템에서의 보안성을 증폭시키기 위한 유니버셜 랜덤 해쉬 함수의 개념을 소개하고 양자 오류 정정과 보안 사이의 관계를 이용하여 보안성 증폭을 제공하는 것을 보인다. 또한, 보안성 증폭 측면에서 접근 방식이 위상 오차 보정 방식을 소개하며 위상 오차 방식이 다른 방식보다 더 나은 보안성을 제시한다는 것을 보인다. 양자 키 분배의 대표적인 예인 BB84 프로토콜을 이용하여 유니버셜 해시 함수가 보안성을 강화하는 과정을 설명한다. 마지막으로 랜덤 프라이버시 증폭을 사용하는 BB84 프로토콜이 동일한 오류율을 가지는 Mayers의 성능보다 높은 키 레이트를 가지는 것을 보여 보안성이 강화된 것을 확인한다.

Abstract This paper introduces the concept of a random universal hash function to amplify security in a quantum key distribution system. It seems to provide security amplification using the relationship between quantum error correction and security. In addition, the approach in terms of security amplification shows that phase error correction offers better security. We explain how the universal hash function enhances security using the BB84 protocol, which is a typical example of QKD(Quantum Key Distribution). Finally, we show that the BB84 protocol using random privacy amplification is safe at higher key rates than Mayers' performance at the same error rate.

Key Words : Random privacy amplification, QKD, hash functions, universal2 hash functions, Random Number Generator(RNG)

Ⅰ. 서 론

양자 키 분배(QKD)는 양자 물리학의 절대적인 법칙으로 안전함을 제공하는 것으로 두 통신 당사자 간의 통신이 기본이다[1]. 불완전한 장치가 사용 되더라도 불완전 QKD 시스템에서 사용되는 광자 수를 측정하는 장비는 다중 광자 펄스를 방출하는 광원 쪼개지는 해킹 방법에 취약하다. 양자 역학에 기반한 영리한 솔루션 은 그러한 측정장비의 불완전성을 극복하기 사용된다. 디코이 상태 방법에서보다 효율적으로 불완전한 광자 소스의 사용보다 구체적으로는 약한 응집성 QKD에 대해 적당한 다중 광자 확률을 갖는 상태가 최근에 중요한 포인트로 인정되었다. QKD 시스템, 특히 단일 광자 검출기 (SPD)를 포함하는 일부 물리적 장치에서 개방 될 수 있다. 결함은 사이드 채널 공격에 대한 도청자 (Eve)의 도청으로 볼 수 있다. 이는 프로토콜의 보안을 위태롭게 할 수 있다. 이러

*준회원, 광운대학교 전파공학과
**정회원, 광운대학교 전자융합공학과, 교신저자
접수일자 : 2018년 8월 15일, 수정완료 : 2018년 9월 15일
게재확정일자 : 2018년 10월 5일

Received: 15 August, 2018 / Revised: 15 September, 2018 / Accepted: 5 October, 2018
**Corresponding Author: jinyoung@kw.ac.kr
Dept of Wireless Communications Engineering, Kwangwoon Univ, Seoul, Korea

한 양자 해킹 공격은 도청에 의한 간섭입니다. 수신자의 방송국 바깥에서 탐지를 높임으로써 어떤 정도의 응답을 예측할 수 있는 장치 심지어 조작할 수 있다. 모든 경우에 있어 공격으로 인해 눈치 채지 않고 정보를 얻는 것을 즉, 달성하기 위한 도청자와 송신자 간의 수신자의 매우 높은 상호 정보 양자 비트 오류율의 상한 임계 값 초과(QBER)를 가져야 한다. 해킹 계획은 기본적으로 다음 두 가지 핵심 사항을 목표로 한다. 불일치한 SPD(Single Photon Detector)과 미스 매치 효율성의 기반이다[2].

기본적인 양자 키 분배 시스템인 BB84는 두 개의 양자 암호문 (C_1, C_2)을 비밀 키로 공유한다. 각각 에러 보정 및 보안성 증폭을 위한 것인데, 보안성 증폭의 경우 짧은 길이의 키만을 사용한다. 다만 각각의 에러 보정 및 보안성 키들은 서로의 서브 코드를 공유하여 연관성을 가지게 된다. 따라서 우리는 두 키 사이에 사용되는 서브 코드를 유니버셜 함수를 사용하여 랜덤성을 증폭시켜 전체 양자 키 분배 시스템의 성능을 높이는 것을 제안한다. 불완전한 양자 측정 장비를 공략하는 해킹 방법을 시스템이 인식 하기 위한 에러율은 낮은 오류율을 가져 전체 보안성 증폭에 더 많은 비용이 소요된다. 또한 양방향 클래식 통신을 사용하는 QKD 프로토콜은 단방향 클래식 통신을 사용하는 QKD 프로토콜보다 높은 오류율을 허용 할 수 있음이 알려져 있다. 허용 가능한 오류율은 [3]에서 18.9 %, [4]에서 20 %, [5]에서 26 %이다. 유니버셜 랜덤 프라이버시 증폭에 대한 우리의 결과는 두 프로토콜을 사용하여 오류율을 줄인 후 오류 정정 및 프라이버시 증폭을 수행하기 때문에 이러한 프로토콜에도 적용 할 수 있다.

본 논문에서는 2장에서 시스템 모델에 대하여 설명하고 3장에서 양자 암호 키 생성 방식을 설명하고 4장 시뮬레이션 결과로 랜덤 유니버설 해쉬 함수를 이용한 키 생성 비율과 에러 비율을 기존 방식과 비교한다. 마지막으로 5장에서 결론을 맺는다.

II. 시스템 모델

본 논문의 시스템 모델은 암호문 쌍(C_1, C_2)이 (S_1, S_2)에 대한 추가 정보를 제공하지 않으므로 더 나은 성공 확률로 (C_1, C_2)를 사용하여 (S_1, S_2) 만 ((C_1, C_2)을 알지 못함) 분포에 기초하여 임의로 추측하는 것보다 좋다. 그러나 실제로는 키가 항상 이상적으로 생성된다는 보장이 없으며 시스템의 암호화 키가 상호 연관 될 수 있다. K_1과 K_2가 서로 관련되어있는 경우 즉, $H(K_1|K_2) < H(K_1)$이면 다음과 같이 유지된다.

$$H(S_1, S_2|C_1, C_2) < H(S_1, S_2). \tag{1}$$

따라서 (1)은 더 이상 쌍 (S_1, S_2)에 대한 추가 정보를 도청 자에게 제공하지 않는다는 것을 직접 보장 할 수 없으므로 보안 문제가 제기된다. K_1과 K_2는 임의의 단일 분리 된 암호문이 대응하는 소스 데이터, 즉 $i = 1,2$에 대해 $H(S_i|C_i) = H(S_i)$에 대한 추가 정보를 나타내지 않도록 그들의 각 영역에 걸쳐 균일 한 분포로부터 무작위로 생성된다. 따라서 보안을 보장하기 위해서는 기존의 시스템에 적용 할 수 있는 방법을 찾아야한다. 따라서 (1)의 조건에서도 도청자는 (C_1, C_2)에서 (S_1, S_2)를 추출할 수 없다. 우리의 주요 아이디어는 적절하게 선택된 선형 코드를 사용하여 각 노드의 암호문을 부호화하는 것이다. 이 아이디어의 핵심은 선형 코드의 동형 속성 덕분에 선형 코드를 사용하여 암호화 된 소스의 구조를 보존하는 동시에 키 간의 상관 효과를 크게 줄일 수 있다는 것이다. 우리는 Slepian-Wolf를 사용하여 임의성 생성에 대한 Oohama[6]의 결과를 인용한다. 부호화 된 암호문 내에 숨겨진 부호화 된 키의 공동 분포가 키들 사이의 상관 효과가 무시할 수 있게 되는 균일 한 분포에 가깝게 만들어 질 수 있음을 보여주기 위한 부호화이다. 또한 Csiszár [7]의 결과를 빌려 조인트 싱크 노드에서 원본 소스 데이터가 무시할 수 있는 오류 확률로 검색 될 수 있도록 좋은 선형 인코더와 디코더를 얻을 수 있음을 보여준다. 특히 제안 된 솔루션의 한 가지 장점은 숨겨진 임의성을 추가 할 필요가 없다는 것이다. 증폭된 비밀을 잃지 않고 공개 할 수 있다. 이제 우리는 암호화 된 출력을 수정하는 제안 된 접근법이 다른 접근법, 즉 이미 실행중인 시스템의 경우 암호화의 입력 수정에 비해 더 실현 가능하다는 것을 보여준다. 암호 출력 대신 암호 입력에 대한 수정을 수행하여 제안 된 접근법과 동일한 효과를 얻으려면 제안 된 접근 방식의 비용 중 두 배가 필요하다는 점에 유의해야 한다. 단순한 이유는 암호화에 대한 두 가지 입력 지점이 있어서다. 그림 1은 본 논문의 시스템 모델로 양자 암호 키 분배 시스템의 전송자와 송신자의 상

관 키로부터 도청자가 가져갈 수 있는 정보량을 이용하여 공개 키의 보안성을 높여 정보 유출 유무를 확인하는 것이다. 각각의 노드, 즉 소스 및 키가 존재하지만,

각 노드의 암호화로부터 오직 하나의 단일 출력 포인트가 존재한다 [9]. 또한 실제 환경에서는 노드의 장치가 전자 회로에 연결된 키를 가지고 있기 때문에 암호화하기 전에 키를 수정하면 이미 실행중인 시스템을 중지하지 않고도 하드웨어 침입을 수행해야 한다.

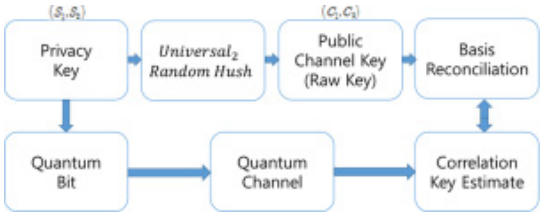

그림 1. 유니버설 랜덤 해쉬를 이용한 양자 암호 키 분배 시스템 모델.

Fig. 1. QKD system model using universal random hash.

Ⅲ. 유니버설 랜덤 해쉬 보안성 증폭

BB84 프로토콜을 구현하기 위해서는, 유니버설 해쉬를 거친 선형 코드 C_1 이 에러 정정을 위해 효율적으로 디코딩 가능해야한다. C_1 이 효율적으로 디코딩 가능한 한 쌍의 선형 코드 C_1 과 C_2 를 찾는 것은 어렵다. 반면에, 우리는 BB84 프로토콜에서 유니버셜 해쉬를 이용하기 때문에 임의의 디코딩 방법으로 보안성을 평가할 수 있다. 따라서 먼저 C_1 코드의 랜덤 유니버셜 해쉬를 선택하고 효율적으로 디코딩 할 수 있다. 코드의 조건은 $C_2 \subset C_1$을 만족하며 BSC(Binary Symmetric Channel)의 첫 번째 비트의 크로스 오버 확률이 p_0 보다 작거나 같고 후반 $\frac{n}{2}$ 비트의 크로스 오버 확률이 p_1 보다 작거나 같아야 한다. 두 번째로CSS(Cascading Style Sheets) 코드의 일부인 C_1 의 오류 확률이 작거나 같다. BSC의 첫 번째 $\frac{n}{2}$ 비트의 크로스 오버 확률이 p_1 보다 작거나 같고 후반 $\frac{n}{2}$ 비트의 크로스 오버 확률이 p_0 보다 작거나 같으면 $C_2^{\perp}$ 의 디코딩 오류 확률 BSC를 통한 CSS 코드의 일부가 작거나 같아야 한다.

그런 다음 조건을 만족하는 코드 C_1를 찾는다. 주어진 코드 C_1 이 조건을 만족하는 값을 갖는 코드 C_2 를 선택하는 것은 (a) $C_1^{\perp} \subset C_2^{\perp}$ 를 만족하는 코드 $C_2^{\perp}$ 를 선택하는 것과 동일하다. 위 조건에 대해 비율 R을 $1-H(p_0+p_1)$보다 낮게 고정하고 비율 R의 부호 $C_2^{\perp}$ 를 무작위로 선택하면 조건이 만족 될 확률이 높다. 이 절에서 우리는 $1-\frac{H(p_0)+H(p_1)}{2}$ 보다 낮은 비율 R을 고정하고 조건에서 비율 R의 코드 $C_2^{\perp}$ 를 무작위로 선택하면 높은 확률 조건이 만족된다.

실용적인 QKD 시스템에서, 우리는 앞에서 예로든 도청 가능한 와이어 채널을 사용한 BB84 프로토콜의 채널을 통하여 부분 신뢰성을 갖는 $universal_2$ 기반의 랜덤 보안성 증폭의 성능을 비교할 수 있다. 키 생성률에 따라서 시스템이 지수적으로 보안성이 증가하는 것을 보이고 이를 통하여 도청자가 존재하는 상황일 때 양자 암호 시스템의 에러율이 더 빨리 낮아져 실제 도청자의 유무를 더 빠르게 판단할 수 있다. 이를 나타내면

$$e^{\psi(s|W^Z,p_{\min})} = |\chi|^s e^{-\hat{H}_{1+s}(X|P)}. \tag{2}$$

$$e^{\phi(t|W^Z,p_{\min})} = |\chi|^t e^{-(1-t)\hat{H}_{1+\frac{t}{1-t}}(X|P)}. \tag{3}$$

랜덤 해쉬 함수의 보안성 증폭을 위한차원 r 의 코드 $C_1^{\perp}$ 이 주어진다면, 우리는 코드 $C_2^{\perp}$ 를 선택하는 방법을 고려한다.

$R=\frac{r+m}{n}<1-\frac{H(p_0)+H(p_1)}{2}$의 비율로 고정시키고, 다음으로 나타내면

$$A_m = C_2^{\perp} \subset F_2^n | C_2^{\perp}, \quad \dim C_2^{\perp} = r+m,\ C_1^{\perp} \subset C_2^{\perp}. \tag{4}$$

우리가 코드 $C_2^{\perp}$ 를 선택하는 집합을 A_m 이라 한다. 최소 조건부 엔트로피 복호화 : 복호 오류 확률을 평가하기 위해 최소 조건부 엔트로피 복호화를 사용한다. e 를 n 비트 바이너리 벡터에서 에러라고 하고, P_ζ를 e의 처음 $\frac{n}{2}$비트의 타입이라하고, P_η 을 e의 후반 $\frac{n}{2}$ 비트의

타입이라고 한다. 그런 다음, e의 조건부 엔트로피를 다음과 같이 정의한다.

$$H_c(e) = H_c(P_\zeta, P_\eta) = \frac{H(P_\zeta) + H(P_\eta)}{2}. \quad (5)$$

최소 조건부 엔트로피 복호화에서, 우리는 $H_c(\hat{e})$를 최소화하고 동일한 신드롬, 즉 $e\hat{H}_2^T = eH_2^T$ 를 갖는 추정 된 오차 e 를 발견하고, 여기서H_2 는 $C_2^\perp$ 의 패리티 검사 행렬이다[8]. 유니버셜 랜덤 해쉬를 적용하기 위한 디코딩 과정은 CSS 코드의 디코딩 과정 $C_2^\perp$ 에 의한 디코딩 과정을 고려한다. 때문에 위상 오류 만 발생한다고 가정한다. 코드 워드 $|v + C_2>$가 보내지고 $\sigma_z^{[e]}|v + C_2>$가 수신된다고 가정한다[9].

$$|v + C_2> = \frac{1}{|C_2|^{1/2}} \sum_{w \in C_2} |v + w> \; v \in C_1, \quad (6)$$

여기서 $\sigma_z^{[e]} = \sigma_z^{e_1} \otimes \cdots \otimes \sigma_z^{e_n}$, 이고 $e = (e_1, \cdots, e_n)$ 이다. 그리고 $e\overline{H}_2^T$ 신드롬을 계산하고 추정 된 오류 e 를 찾는다. 그런 다음 단위 연산자 $\sigma_z^{[\hat{e}]}$를 $\sigma_z^{[e]}|v + C_2>$ 에 적용하여 오류를 수정한다. 만약 $\sigma_z^{[e+\hat{e}]}|v + C_2> \neq |v + C_2>$ 이면 디코딩 오류가 발생한다. 디코딩 오류가 발생하는 조건을 고려해야 한다. 조건 $\hat{e}H_2^T = eH_2^T$ 는 $e + \hat{e} \in C_2^\perp$ 와 동일하다는 것을 주목한다. 선형 코드 $C_2^\perp$ 의 경우, $e + \hat{e} \in C_2^\perp$ 와 $H_c(\hat{e}) \le H_c(e)$ 가 되는 벡터 $\hat{e}$ 가 존재하면, 추정 된 오차는 $\hat{e}$ 대신 e 이다. 단일 연산자 $\sigma_z^{[e+\hat{e}]}$ 가 CSS 코드 $|v + C_2>$ 의 코드 워드에 적용되면, 다음을 얻을 수 있다.

$$\sigma_z^{[e+\hat{e}]}|v + C_2> = \frac{1}{|C_2|^{1/2}} \sum_{w \in C_2} (-1)^{(v+w)\cdot(e+\hat{e})}|v + w>. \quad (7)$$

모든 $v + w \in C_1$ 에 대해 $(v + w) \cdot (e + \hat{e}) = 0$ 이면, 코드 워드는 $\sigma_z^{[e+\hat{e}]}$ 의 곱셈에 의해 변하지 않는다. $v \in C_1$, $w \in C_2$ $C_2 \subset C_1$, 이므로 $e + \hat{e} \in C_1^\perp$ 이면 $(v + w) \cdot (e + \hat{e}) = 0$ 이다. 따라서, $e + \hat{e} \in C_1^\perp$ 이라면 오류는 정확하게 추정되지 않지만 수신 된 상태는 원래 상태로 수정되고 이러한 오류는 디코딩 오류를 발생시키지 않는다. CSS 코드를 디코딩하는 경우, 디코딩 오류를 일으키는 각 $C_2^\perp$ 에 대한 오류 집합을 다음과 같이 정의한다.

$$\varepsilon(C_2^\perp) = \left\{ e \in F_2^n | \exists\, \hat{e} H_c(\hat{e}) \le H_c(e), \; e + \hat{e} \in C_2^\perp / C_1^\perp \right\}. \quad (8)$$

우리는 첫 번째 $\frac{n}{2}$ 비트의 교차 확률이 p_1' 이고 후반 $\frac{n}{2}$ 비트의 교차 확률이 p_0' 인 BSC를 통해 CSS 코드의 일부로 수식 (1)에서 정의한 유니버셜 랜덤 해쉬를 적용하여 $C_2^\perp$ 의 디코딩 오류 확률을 정의한다.

$$P_{err}(C_2^\perp, p_0', p_1') = \sum_{e \in \varepsilon(C_2^\perp)} Q(e), \quad (9)$$

여기서 $Q(e)$ 는 첫 번째 $\frac{n}{2}$ 비트의 교차 확률이 p_1' 이고 두 번째 $\frac{n}{2}$ 비트의 확률이 p_0' 인 BSC에서 e 가 발생할 확률이다. CSS 코드의 일부인 C_1 의 디코딩 오류 확률은 CSS 코드의 비트 플립 오류 디코딩 프로세스를 고려하여 같은 방식으로 정의된다 [10]. 임의의 $\mu > 0$ 에 대해 A_m 에서 임의로 $C_2^\perp$ 코드를 선택하면

$$\Pr\left\{ \begin{array}{l} P_{err}(C_2^\perp, p_0', p_1') \le \\ \left(\frac{n}{2}+1\right)^4 2^{-n(E(R, p_0, p_1) - \mu)} \\ \qquad \forall\, p_0' \le p_0, p_1' \le p_1 \end{array} \right\} \ge 1 - \left(\frac{n}{2}+1\right)^2 2^{\mu n}, \quad (10)$$

여기서

$$E(R, p_0, p_1, \psi, \phi) = \min_{p_0, p_1, e^\psi, e^\phi} \left[\frac{\overline{D}(q_1|p_1) + \overline{D}(q_0|p_0)}{2} + \left|1 - \overline{R} - \overline{H}_c(q_1, q_0)\right|^+ \right] \times e^{\psi(s|W^Z, p_{\min})} e^{\phi(t|W^Z, p_{\min})}, \quad (11)$$

및 $|x|^+ = \max\{x,0\}$, $\min_{p_1, p_0, e^{\psi}, e^{\phi}}$ 은 $0 \le p_0, p_1, e^{\psi}, e^{\phi} \le 0$ 을 취한다. $q_1 = p_1$, $q_0 = p_0$, 그리고 $R < 1 - \frac{H(p_0)+H(p_1)}{2}$ 인 경우에만 $\frac{\overline{D}(q_1|p_1)+\overline{D}(q_0|p_0)}{2} = 0$ 이다. 따라서 A_m 에서 임의로 코드를 선택함으로써 높은 확률로 조건을 만족하는 코드 $C_2^{\perp}$ 를 얻을 수 있다.

Ⅳ. 실험결과

이 장에서는 제안한 시스템의 성능을 기존 시스템과 비교한다. 일률적으로 에러율을 추정 할 경우, $H\left(\frac{p_0+p_1}{2}\right)$ 보다 높은 비율의 코드 C_2 로 랜덤 프라이버시 증폭을 수행 할 수 있다. 생성 속도가 $1-H\left(\frac{p_0+p_1}{2}\right)$에 매우 가깝고 디코딩 오류 확률이 작은 효율적인 복호화 가능 코드가 존재하므로 $1-2H\left(\frac{p_0+p_1}{2}\right)$ 보다 낮은 비율로 안전하게 키를 공유 할 수 있다. 기존 Mayers 시스템은 [5]에서 $C_2^{\perp}/C_1^{\perp}$ 의 최소 해밍 가중치를 계산할 때, 우리는 $1-H\left(\frac{p_0+p_1}{2}\right)-H(p_0+p_1)$ 보다 낮은 비율로 키를 안전하게 공유 할 수 있다. 여기서 $1-H\left(\frac{p_0+p_1}{2}\right)$는 에러 정정을 위한 C_1의 비율이고, $H(p_0+p_1)$ 는 프라이버시 증폭을 위한 C_2 의 비율이다. 그림 1은 평균 상관 노출 키의 비율에 따른 유한 비밀 키의 비율을 나타낸다.

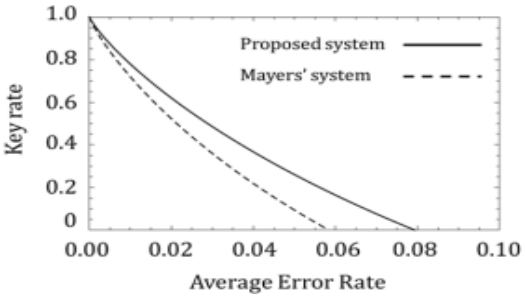

그림 2. 평균 상관 노출 키 비율에 따른 유한 비밀 키의 비율
Fig. 2. The ratio of the finite secret key to the average correlation key ratio.

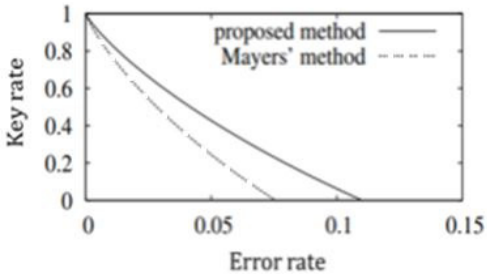

그림 3. 제안된 시스템의 달성 가능 키 생성 비율의 성능비교.
Fig. 3. Comparison of achievable key rates.

그래프의 실선은 제안한 $universal_2$ 기반의 랜덤 보안성 증폭이 동일한 키 노출 비율일 때 Mayers 방식을 이용했을 때 보다 키 생성 성능이 우월한 것을 비교한 것이다. 디코딩 에러 확률의 평가에 따르면, 허용 가능한 에러율은 7.5 %에서 11 %로 증가 할 수 있음을 보여 주었다. 그림 2은 보안 키비율과 Mayers의 오류율을 보여 주며 핵심 비율은 각각 7.5 %와 11 % 지점에서 0으로 떨어져 제안된 시스템이 보안성 증폭성능이 더 뛰어난 것을 보여준다.

Ⅴ. 결 론

본 논문은 양자 키 분배 시스템에서의 보안성을 증폭시키기 위한 이중 해시 함수의 개념을 소개하였다. 우리는 랜덤 키 생성 방식을 통하여 기존 도청 가능한 양자 채널의 보안성을 높이기 위해서 랜덤 $universal_2$ 해쉬 기반의 랜덤 보안성 증폭을 적용하여 실제 상위 경계조건에 도달하기 위한 키 생성 속도와의 관계를 나타내었다. 고정 코드 C_1 의 경우 BB84 프로토콜을 안전하게 유지하면서 무작위로 선택한 코드 C_2 의 비율을 줄일 수 있음을 보였다. 결과적으로, 우리는 랜덤 프라이버시 증폭을 사용하는 BB84 프로토콜이 심각한 잡음을 견딜 수 있고 더 긴 키를 공유 할 수 있음을 증명했다. 그래서 우리는 양자 채널에서의 도청자가 있을 경우 도달하게 되는 키 생성 속도와 보안성의 상한선을 산출하였다.

References

[1] M. Tope and J. McEachen, “Unconditionally

secure communications over fading channels," in *Proc. IEEE MILCOM,* Oct. 2001, pp. 54 - 58.
DOI: https://doi.org/10.1109/milcom.2001.985763

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, Bangalore, India, Dec. 1984, pp. 175 - 179.
DOI: https://doi.org/10.1016/j.tcs.2011.08.039

[3] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory,* vol. 41, no. 6, pp. 1915 - 1923, Nov. 1995.
DOI: https://doi.org/10.1109/18.476316

[4] G. Brassard and L. Salvail, T. Helleseth, Ed., "Secret-key reconciliation by public discussion," in *Proc. Adv. Cryptol.—Eurocrypt,* 1994, vol. 765, LNCS, pp. 410 - 423.
DOI: https://doi.org/10.1007/3-540-48285-7_35

[5] J. L. Carter and M. N.Wegman, "Universal classes of hash functions,"J. *Comput. Syst. Sci.*, vol. 18, pp. 143 - 154, 1979.
DOI: https://doi.org/10.1007/springerreference_550

[6] I. Csiszar, "Almost independence and secrecy capacity," *Probl. Inf. Transmiss.*, vol. 32, no. 1, pp. 40 - 47, 1996.

[7] C. Chen and M. A. Jensen, "Improved channel quantization for secret key establishment in wireless systems," in *Proc. IEEE ICWITS, Aug.* 2010, pp. 1 - 4.
DOI: https://doi.org/10.1109/icwits.2010.5611930

[8] Y. Dodis and A. Smith, "Correcting errors without leaking partial information,"in *Proc. 37th Annu. ACM Symp. Theory Comput.*, 2005, pp. 654 - 663.
DOI: https://doi.org/10.1145/1060590.1060688

[9] S. Fehr and C. Schaffner, "Randomness extraction via delta-biased masking in the presence of a quantum attacker," in *Proc. Theory Cryptogr. Conf.,* 2008, pp. 465 - 481.
DOI: https://doi.org/10.1007/978-3-540-78524-8_26

[10] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *J. Quant. Inf. Comput.*, vol. 5, pp. 325 - 360, 2004.
DOI: https://doi.org/10.1109/isit.2004.1365172

[11] H. D. Kim, "A study on the secure double pipe hash function," *The Journal of The Institute of Internet, Broadcasting and Communication (JIIBC)*, vol. 10, no. 6, pp. 201 - 208, Dec. 2010.

[12] J. S. Choi, S. S. Shin and G. H. Han, "Three-party key exchange protocol providing user anonymity based on smartcards," *Journal of the Korea Academia-Industrial cooperation Society (JKAIS),* vol. 10, no. 2, pp. 388 - 395, Feb. 2009.
DOI: https://doi.org/10.5762/KAIS.2009.10.2.388

저자 소개

이 선 의(준회원)

- 2013년 2월 : 광운대학교 전파공학과 졸업
- 2013년 2월 ~ 현재 : 광운대학교 전파공학과 석박사통합과정

<주관심분야 : 가시광 통신, 협력통신, 인지무선통신, 양자통신>

김 진 영(정회원)

- 1998년 2월 : 서울대학교 전자공학과 공학박사
- 2001년 2월 : SK텔레콤 네트웍연구소 책임연구원
- 2001년 3월 ~ 현재 : 광운대학교 전자융합공학과 교수

<주관심분야 : 차세대이동통신, 가시광통신, 전력선통신, 인공지능>

※ 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신 · 방송 연구개발사업의 일환으로 수행하였음. [1711073835 양자암호통신망 구축을 통한 신뢰성 검증기술 및 QKD 고도화를 위한 핵심요소기술 개발]