The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 18, No. 4, pp.73-78, Aug. 31, 2018. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2018.18.4.73
JIIBC 2018-4-10

공개 채널을 통한 상관 키 분산 암호화의 프라이버시 증폭

Privacy Amplification of Correlated Key Decryption over Public Channels

이선의*, 김진영**

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

요 약 본 논문에서는 다중 소스가 분리 된 노드에서 암호화되고 각각의 공개 통신 채널을 통해 공동 싱크 노드로 전송되는 시스템을 고려한다. 우리는 상관 관계가 있는 암호화 키를 가진 것으로 알려진 기존 시스템의 보안 문제에 관심이 있다. 특히, 우리는 추가적인 비밀 키를 도입하지 않고 해결책을 찾는데 초점을 맞추고 비용을 최소화하고 이미 실행중인 시스템을 중단시키는 위험을 최소화하기 위해 최소한의 수정만으로. 우리는 도청자가 이용 가능한 공개 통신 채널에 액세스함으로써 모든 암호문, 즉 암호화 된 소스를 획득하는 보안 모델 하에서의 해결책을 제안한다. 우리의 주요 기술은 암호문을 공개 통신 채널에 보내기 전에 특정 선형 코드의 유니버셜 함수를 사용하여 암호문을 인코딩하는 것이다.

Abstract In this paper, we consider a system where multiple sources are encrypted in separated nodes and sent through their respective public communication channels into a joint sink node. We are interested at the problem on protecting the security of an already existing system such above, which is found out to have correlated encryption keys. In particular, we focus on finding a solution without introducing additional secret keys and with minimal modification to minimize the cost and the risk of bringing down an already running system. We propose a solution under a security model where an eavesdropper obtains all ciphertexts, i.e., encrypted sources, by accessing available public communication channels. Our main technique is to use encoders of universal function to encode the ciphertexts before sending them to public communication channels.

Key Words : Random privacy amplification, QKD(Quantum Key Distribution), hash functions, $universal_2$ hash functions, Random Number Generator (RNG).

Ⅰ. 서 론

암호화를 위해서 필요한 시드 키의 보안성 증폭을 위해서는 임의의 랜덤 변수를 통하여 생성된 $universal_2$ 해쉬 함수가 사용된다. 이 기술에 대한 연구는 랜덤 변수 추출 기술에 기반하여 많은 연구가 진행되어 왔다[1]. 랜덤 보안성 증폭 기술은 공용 통신, 인터넷 결제, 도청가능성이 있는 통신, 모바일 결제 등의 비밀키 생성(distillation)에 적용이 가능하다[2]. 최근에는 보안성의 기준을 구분 가능한 norm L_1이라 불리는 기술로 적용하고

*준회원, 광운대학교 전파공학과
**정회원, 광운대학교 전자융합공학과, 교신저자
접수일자 2018년 6월 27일, 수정완료 2018년 7월 27일
게재확정일자 2018년 8월 10일

Received: 27 June, 2018 / Revised: 27 July, 2018 /
Accepted: 10 August, 2018
*Corresponding Author: jinyoung@kw.ac.kr
Dept of Wireless Communications Engineering, Kwangwoon Univ, Korea.

있다. 이 기준은 보편적으로 구성 가능한 보안과 밀접한 관련이 있기 때문이다. 이 논문에서는 비밀성의 증폭의 기준으로 L_1 구별성을 채택하고 이를 양자 암호 증폭에 적용하여 임의의 보안성 증폭에 대한 성능을 평가한다. 독립적이고 동일하게 분포된 암호 비밀키의 경우에, 생성 된 난수의 비율이 원 정보 소스의 엔트로피보다 작으면, 균일한 난수에 대한 표준 거리가 0에 가깝게 접근하는 확률 변수를 생성하는 것이 가능하다.

논문에서 2장은 시스템 모델에 대하여 설명하고 기존 시스템과의 차별점과 제안하는 아이디어에 대해 서술한다. 3장에서는 공개 채널을 통과하는 키의 상관 관계에 따른 보안성 증폭에 대하여 설명하고 4장에서 결론은 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.

$$H(S_1,S_2|C_1,C_2)<H(S_1,S_2). \quad (1)$$

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 수있는 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

그림 1. 공개채널을 통한 상관 키 분배 시스템 모델.
Fig. 1. correlated key distribution system model through public channel.

것이다. 우리는 Slepian-Wolf를 사용하여 임의성 생성에 대한 Oohama[3]의 결과를 인용한다. 또한 Csiszár[4]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 제안된 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 제안된 접근법이 이미 실행중인 시스템의 경우 암호화의 입력 수정에 비해 더 실현 가능하다는 것을 보여준다. 암호 출력 대신 암호 입력에 대한 수정을 수행하여 제안된 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 상관 키로부터 도청자가 가져갈 수 있는 정보량을 이용하여 공개 키의 보안성을 높여 정보 유출 유무를 확인하는 것이다.

III. 양자 암호 키 생성 및 보안성 증가

랜덤 소스 정보와 키들은 랜덤 변수 $S_1\times S_2$의 유한 쌍 (S_1,S_2)으로 나타낼 수 있다. 이 유한 랜덤 변수 쌍 $\{(S_{1,t},S_{1,t})\}_{t=1}^{\infty}$ 이 고정 이산 비저장 소스라 놓고 여기서 $t=1,2,...$이고 $P_{S_1,S_2}=\{P_{S_1S_2}(s_1,s_2)\}_{(s_1,s_2)\in S_1\times S_2}$로 표시된$(S_1,S_2)$과 동일한 분포를 따른다. 또한 (K_1,K_2)는 2개의 개별 단말에서의 암호화에 사용 된 키 쌍을 나타내는 동일한 유한 집합 $S_1\times S_2$로부터 취한 랜덤 변수의 쌍이라고 한다[5]. 이와 유사하게 $\{(K_{1,t},K_{2,t})\}_{t=1}^{\infty}$은 각각의 $t=1,2,..,$ 쌍 $(K_{1,t},S_{K,t})$은 유한 집합 $S_1\times S_2$와

$P_{K_1K_2}=\{P_{K_1K_2}(k_1,k_2)\}_{(k_1,k_2)\in S_1\times S_2}$로 표시되는 (K_1,K_2)과 동일한 분포를 따른다. 랜덤 넘버 생성기를 이용하여 부분적으로 도청가능성이 있는 비밀 키를 생성하는 것을 고려한다. 도청을 고려한 랜덤 넘버 생성기를 이용하여 생성된 정보는 전송자와 수신자 그리고 도청자 모두가 랜덤 넘버 생성기 A와 연관성이 있다. 전송자와 수신자가 공유하는 공통 랜덤 넘버는 $\alpha\in A$, 도청자가 일부 도청을 해내서 α와 일부를 동일한 정보를 가지고 있는 다른 랜덤 넘버는 $e\in A$라 한다. 이 공통 랜덤 키에서 공통된 랜덤 넘버 중에 도청가능성이 큰 e와 가장 연관성이 없게 추출해 내는 것이 보안성 증폭이다. 이를 수식으로 나타내면

$$H_{1+s}(X|P^X):=\frac{\hat{H}_{1+s}(X|P^X)}{s}. \quad (2)$$

그리고 조건부 엔트로피 $1+s$ 차수에 대한 식은

$$H_{1+s}(X|Y|P^{X,Y}):=\frac{\hat{H}_{1+s}(X|Y|P^{X,Y})}{s}. \quad (3)$$

이제 우리는 stochastic 형태의 함수 f로 표현되어 생성된 랜덤 넘버 $A=\{1,\dots,M\}$의 모음 함수 f_X를 살펴본다. 이 함수 f_X는 다음 조건을 만족할 때 $universal_2$ 이라고 부른다.

조건 1: $\forall_{a_1}\neq\forall_{a_2}\in A$, 확률 $f_X(a_1)=f_X(a_2)$가 거의 $1/M$일 때.

조건 2:모든 X에 대하여, $f_X^{-1}\{i\}$의 집합원의 개수가 i에 의존하지 않을 경우일 때.

이 절에서는 QKD에 거의 모든 이중 유니버설 해시 함수 집합이 적용될 때 강력한 보안을 보인다. 이를 위해 QKD 보안 증거의 위상 오류 수정에 적용한다. QKD에서 Alice와 Bob은 Quantum 통신의 결과로 얻은 결정된 키에서 비밀 키를 생성하기 위해 키 추출 프로토콜을 수행해야 한다. 보안성 증폭을 위한 함수 집합을 사용하는 다음 유형의 BB84 프로토콜을 고려한다. 유니버셜 해시 함수 집합 $F=\{f_r:F_2^m\to F_2^l|r\in I\}$을 사용하는 BB84 프로토콜 :

1) Alice와 Bob은 sifted 키를 설정하고 BB84 프로토콜의 일반적인 절차에 따라 비트 오류율을 추정한다.

a. Alice는 임의로 선택된 Bob 큐 비트 상태 $\{|0_z>,|1_z>,|0_x>,|1_x>\}$를 보낸다.

b. Bob은 무작위로 선택한 $\{z,x\}$를 받아서 측정한다.

c. 인증 된 공개 채널을 사용함으로써 Bob은 모든 큐 비트에 대한 측정 기준을 발표하고 동일한 기준을 선택한 비트 만 유지한다.

d. 이들은 공개 채널을 통해 임의로 샘플링 된 비트를 공개하고 예상 된 비트 오류율을 계산하고 비율이 너무 높으면 프로토콜을 중단한다.

e. 결과적으로 Alice와 Bob은 각각 sifted key $\{k_A,k_B\}\in F_2^n$를 얻는다.

2) Alice는 난수$r_A=F_2^l$를 선택하고 $v=k_A\oplus G(C_l)r_A^T$과XOR 연산을 표시하여 발표한다.

3) Bob은 $R_B=k_B\oplus v$를 계산하고 C_1을 사용하여 오류를 수정함으로써 $R'_B\in C_1$ 얻는다. 그런 다음 Bob은 $R_B=G(C_1)r_B^T$ 을 만족하는 가공 안한 비트 $r_B\in F_2^l$ 를 계산한다. (그러므로, 높은 확률로 $r_A=r_B$ 에 근접한).

4) Alice는 선형 유니버셜$_2$ 함수 $f_r:F_2^m\to F_2^l$ 를 무작위로 선택하여 이를 Bob에게 알린다. 그런 다음 비밀 키 $s_A=f_r(r_A)$ 와 $s_B=f_r(r_B)$를 계산한다.

우리는 F가 δ-almost 이중 유니버셜$_2$인 약한 상태를 유지하는 Shor-Preskill 유형의 보안 증명을 제시한다. 이 절의 조건은 실제로 함수 집합이 δ-almost 이중 유니버셜$_2$의 제한된 경우이기 때문에 실제로 완화되어 있어 유의해야 한다. 이 방법은 [6]에서와 달리, Alice와 Bob이 sifted 키 비트의 무작위 치환을 수행 할 필요가 없다는 추가적인 이점을 가지고 있다. 반대로, 랜덤 치환이 이미 QKD 시스템에 구현되어 있거나 채널이 순열 불변 인 경우, 해쉬 함수는 결정론적인 코드를 사용하는 것으로 대체 될 수 있다. 이 코드 쌍의 치환된 코드는 (n+1)-almost 이중 유니버셜$_2$ 서브 코드 쌍을 형성하기 때문이다. 보안을 보여주기 위해 다음과 같이 고전적인 CSS 코드의 관점에서 프로토콜을 다시 작성하는 것이 편리하다.

코드 C_2 집합을 사용하는 BB84 프로토콜 :

1) Alice와 Bob은 전술 한 프로토콜과 동일한 절차에 의해 sifted key $k_A,k_B\in F_2^n$를 설정한다.

2) Alice가 임의로 $R_A\in C_1$ 선택하여 공개 채널을 통해 $v=k_A\oplus R_A$을 밥에게 보낸다.

3) Bob은 $R_B=v\oplus k_B$를 계산하고 C_1를 사용하여 오류를 수정함으로써 $R'_B\in C_1$ 얻는다. (그러므로, 높은

확률로 $R_A = R'_B$.)

4) Alice가 임의로 코드 $C_{2,r}$를 선택하여 Bob에게 알립니다. 그들은 둘 모두의 코셋 $C_{2,r}$, i.e., $S_A = R_A + C_{2,r}, S_B = R'_B + C_{2,r}$으로써 비밀 키를 얻는다.

간단한 계산을 위해서 이 절의 나머지 부분에서는 이 프로토콜로 제한한다. 우리는 몇 가지 알려진 결과를 검토하고 표기법을 명확히 하는 것으로 시작한다. Alice와 Bob 사이의 양자 채널은 임의의 양자 연산 $\wedge$에 의해 주어지므로, sifted 키는 $\wedge$에 의해 영향을 받는다. [7]에서 논의 된 바와 같이, BB84 프로토콜의 위 유형은 회전된 큐 비트의 하에서 일반적으로 손실없이 불변하므로, 원래 채널를 회전시켜 얻은 Pauli 채널 $\wedge_t$를 고려해 보자. Pauli 채널 $\wedge_t$는 일반적으로 위상 오류와 비트 오류의 공동 확률 분포 P^{XZ}로 설명 할 수 있다.

즉, $\wedge_t$는 $n-$ 큐 비트 상태 ρ로 변형하면

$$\wedge_t(\rho) = \sum_{x,z\in} P^{XZ}(x,z) Z^x X^z \rho (Z^x X^z)^\dagger, \qquad (4)$$

여기서 $Z^x := \sigma_z^{x_1} \otimes \cdots \otimes \sigma_z^{x_n}$ $X^z := \sigma_x^{z_1} \otimes \cdots \otimes \sigma_x^{z_n}$이고 σ_x와 σ_z는 Pauli 행렬이고 $x = (x_1, \cdots, x_n), z = (z_1, \cdots z_n) \in \{0,1\}^n$ 이다. 우리는 위상 오차의 한계 분포를 $P^X(x) = \sum_{z\in F_2^n} P^{XZ}(x,z)$로 나타낸다. $\hat{P}^X(k)$는 $P^X(x)$에 따른 x의 해밍 가중치 k의 분포를 나타낸다. 다음으로, 비밀 키를 고려하기 전에, sifted 키 k의 보안성을 예를 들어 평가한다. 여기에 나온 결과는 와이어 탭 채널 및 이후의 임의 추출을 위한 섹션에도 사용된다. 프로토콜의 첫 번째 단계가 완료되면 Alice와 Eve의 전체 시스템을 $\rho_{A,E}$로 한다(양자 통신부). 보편적인 구성 가능성을 고려한 보안 기준을 사용한다면, sifted 키의 보안은 $\rho_A := Tr_E \rho_{A,E}$와 $\rho_E := Tr_A \rho_{A,E}$[3]의 이브의 구별 가능성 $\| \rho_{A,E} - \rho_A \otimes \rho_E \|_1$로 평가할 수 있다. 또는 Eve의 Holevo정보 $X := Tr \rho_{A,E} (\log \rho_{A,E} - \log \rho_A \otimes \rho_E)$을 통해 보안을 평가할 수 있다. 이 값들은 다음 수식으로 묶여있는 것으로 알려져 있다.

$$\| \rho_{A,E} - \rho_A \otimes \rho_E \|_1 \le 2\sqrt{2}\sqrt{P_{ph}}, \qquad (5)$$

$$X \le \eta_n(P_{ph}), \qquad (6)$$

여기서 $P_{ph} := 1 - P^X(x = 0^n)$는 채널 $\wedge_t$의 위상 에러 확률이다. η_n은 다음과 같이 정의된다.

$$\eta_x(x) := \begin{cases} -x\log x - (1-x)\log(1-x) + nx, & \text{if } x \le 1/2 \\ 1 + nx, & \text{if } x > 1/2. \end{cases} \qquad (7)$$

이제 비밀 키의 보안을 살펴보면

이론 1: 함수 $\{f_X\}$의 집합의 모임이 $universal_2$ 일 경우 다음을 만족한다.

$$E_X H(f_X(A)|E|P^{A,E}) \ge \log M - \frac{M^s e^{-\hat{H}_{1+s}(A|E|P^{AE})}}{s} = \log M - \frac{e^{s(\log M - H_{1+s}(A|E|P^{AE}))}}{s}, \qquad (8)$$

여기서 $0 \le \forall_s \le 1$ 일 경우에 다음을 만족한다. 상호 연관 정보는 다음과 같다.

$$I(f_X(A): E|P^{A,E}) := H(f_X(A)|P^A) - H(f_X(A)|E|P^{A,E}), \qquad (9)$$

여기서 경계조건은 $\log M - H(f_X(A)|E|P^{A,E})$이고, 다음과 같이 나타낼 수 있다.

$$E_X I(f_X(A): E|P^{A,E}) \le \frac{M^s e^{-\hat{H}_{1+s}(A|E|P^{AE})}}{s}, 0 < s \le 1, \qquad (10)$$

이론 2: $\{1,..,M\}$으로부터 생성된 A로 이루어진 함수 f가 존재할 경우 다음을 만족한다.

$$I(f(A): E) \le \frac{M^s e^{-\hat{H}_{1+s}(A|E|P^{AE})}}{s} \quad \frac{e^{s(\log M - H_{1+s}(A|E|P^{AE}))}}{s}, 0 \le \forall_s \le 1, \qquad (11)$$

우리는 실질적으로 사용하는 기본함수는 $\tilde{H}_{1+s}(A|E|P^{A,E})$인데 그 이유는 좀 더 암호화의 보안성 강화를 지수적으로 증가하게 표현을 비교하기에 복잡도가 낮기 때문이다.

이제 우리는 $0 < s \le 1$일 경우의 두 가지 $\frac{e^{\psi(s|W^E,p)}}{L^s s}$과 $\frac{e^{\phi(s|W^E,p)}}{L^s s}$ 상위 경계조건을 비교할 것이다. 측정 공간 (χ, p) 내의 Holder inequality는 다음과 같이 주어진다.

$$\left| \sum_{x\in X} p(x) X(x) Y(x) \right| \le \left(\sum_{x\in X} p(x) |X(x)|^{\frac{1}{1-s}} \right)^{1-s} \left(\sum_{x\in X} p(x) |Y(x)|^{\frac{1}{s}} \right)^{s} . \qquad (12)$$

$$\sum_x p(x) (W_x(y))^{1+s} W_P(y)^{-s} \le \left(\sum_x p(x) (W_x(y))^{\frac{1}{1-s}} \right)^{1-s} . \qquad (13)$$

다음으로 우리가 보안성 증폭의 키 생성 속도 R이 주어진 상호정보량 $I(p: W)$에 극한으로 가는 경우 $s \to 0$이면 테일러 정리를 사용할 수 있다.

이 식을 테일러 정리를 풀어서 나타내면

$$\sum_x p(x)\left(W_x(y)\right)^{1+s} W_P(y)^{-s} \cong 1 + I(p:W)s + I_2(p:W)s^2 + \left(I_3(p:W) + \hat{I}_3(p:W)\right)s^3, \quad (14)$$

여기서

$$I_2(p:W) := \frac{1}{2}\sum_{x,y} p_x W_z(y)\left(\log W_x(y) - \log W_p(y)\right)^2$$

$$I_3(p:W) := \frac{1}{6}\sum_{x,y} p_x W_x(y)\left(\log W_x(y) - \log W_p(y)\right)^3$$

$$\hat{I}_3(p:W) := \frac{1}{2}\sum_y \left(\sum_x p_x W_x(y)\left(\log W_x(y)\right)^2 - \frac{\left(\sum_x p_x W_x(y)\log W_x(y)\right)^2}{W_p(y)}\right). \quad (15)$$

실제로 Schwarz 부등식을 적용하고 inner 곱 연산을 하면 다음을 얻을 수 있다.

$$\left(\sum_x p_x W_x(y)\left(\log W_x(y)\right)^2\right) \cdot \left(\sum_x p_x W_x(y)\right) \geq \left(\sum_x p_x W_x(y)\log W_x(y)\right)^2 \quad (16)$$

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

$$e^{\psi(s|W^Z,p_{\min})} = |\chi|^s e^{-\hat{H}_{1+s}(X|P)}. \quad (17)$$

$$e^{\phi(t|W^Z,p_{\min})} = |\chi|^t e^{-(1-t)\hat{H}_{1+\frac{t}{1-t}}(X|P)}. \quad (18)$$

이고 (17)은 제안한 보안성 증폭을 이용한 것이고 (18)은 기존의 $universal_2$ 해쉬 함수 이용한 양자 채널을 가정하였을 때 BB84 프로토콜의 보안성을 나타낸 것이다. 이를 다시 정리하면 다음 식을 얻을 수 있다.

$$e_\psi(R|W^E,p_{mix}) = \max s(R-\log|\chi|) + \hat{H}_{1+s}(X|P) \geq \max \frac{s(R-\log|\chi|) + \hat{H}_{1+s}(X|P)}{1+s} = e_\phi(R|W^E,p_{mix}). \quad (19)$$

여기서 $t = s/(s+1)$ 이다. 그림 2은 본 논문에서 제안한 $universal_2$ 기반의 부분 랜덤 보안성 증폭과 기존 $universal_2$ 해쉬함수를 이용했을 때의 성능을 비교한 것이다. 키 생성 속도에 따라 지수적으로 더 급격하게 제안한 방식이 증가하는 것으로 더 좋은 성능을 가지는 것을 보였다. 그림 3은 제시한 상관 키의 공개 채널을 통해 유출되는 정보량을 유니버셜 해쉬 함수를 이용하여 인코딩하였을 때 허용 가능한 프라이버시 증폭 영역을 그래프로 나타낸다. 그림 4는 평균 상관 노출 키의 비율에 따른 유한 비밀 키의 비율을 나타낸다. 그래프의 실선은 제안한 $universal_2$ 기반의 부분 랜덤 보안성 증폭이 동일한 키 노출 비율일 때 $universal_2$ 해쉬함수를 이용했을 때 보다 키 생성 성능이 우월한 것을 비교한 것이다.

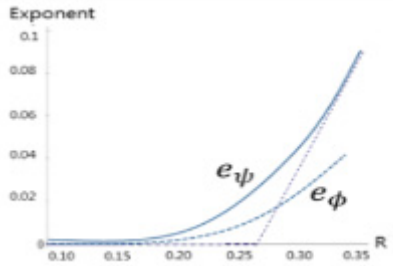

그림 2. 유니버셜 랜덤키 방식에 따른 키 레이트와 보안성의 exponent 증가.
Fig. 2. Increase exponent of key rate and security according to universal random key method.

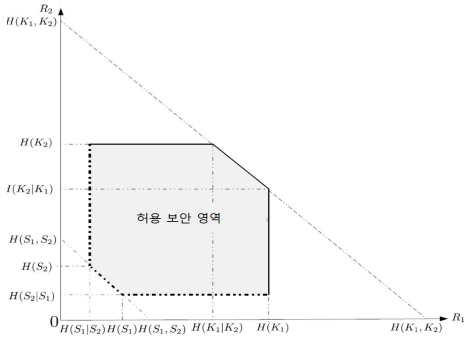

그림 3. 허용된 상관 키 분산의 프라이버시 증폭 영역.
Fig. 3. Privacy amplification region of allowed correlation key distribution.

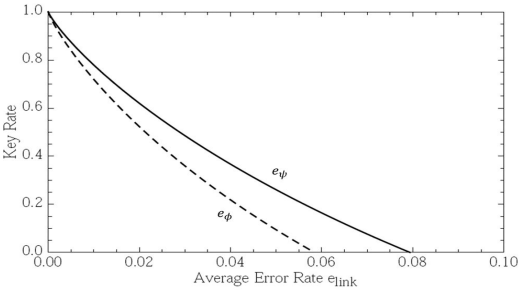

그림 4. 평균 상관 노출 키 비율에 따른 유한 비밀 키의 비율.
Fig. 4. The ratio of the finite secret key to the average correlation key ratio.

Ⅳ. 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 $universal_2$ 기반의 랜덤 보안성 증폭을 적용하여 실제 상위 경계조건에 도달하기 위한 키 생성 속도와의 관계를 나타내었다. 또한 기존 BB84 프로토콜을 적용하여 제안한 보안성 증폭 방식과 기존 $universal_2$ 해쉬 함수만을 적용한 방식의 보안성 증폭도가 지수적으로 먼저 도달하는 성능을 보였다. 그래서 우리는 양자 채널에서의 도청자가 있을 경우 도달하게 되는 키 생성 속도와 보안성의 지수 상한선을 산출하였다.

References

[1] A. De, C. Portmann, T. Vidick, and R. Renner, Trevisan's extractor in the presence of quantum side information [Online]. Available: arXiv:0912.5514
DOI: https://doi.org/10.1137/100813683

[2] 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

[3] I. Csiszar and J. Karner, "*Information Theory: Coding Theorem for Discrete Memoryless Systems,*" New York, NY, USA: Academic, 1981.

[4] 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

[5] 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: hhttps://doi.org/10.1109/isit.2004.1365172

[6] 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

[7] J. W. Wallace, "Secure physical layer key generation schemes: Performance and information theoretic limits," *in Proc. IEEE Int. Conf. Commun.*, Jun. 2009, pp. 1 - 5.
DOI: https://doi.org/10.1109/icc.2009.5199440

[8] 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.

[9] 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

<관심분야> : 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

<관심분야> : 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]