듀얼 유니버셜 해쉬 함수를 이용한 양자 키 분배 시스템의 보안성 증폭

이선의*, 김진영*

Privacy Amplification of Quantum Key Distribution Systems Using Dual Universal Hush Function

Sun Yui Lee*, Jin Young Kim*

요 약

초록 – 본 논문은 양자 키 분배 시스템에서의 보안성을 증폭시키기 위한 이중 해시 함수의 개념을 소개한다. 양자 오류 정정과 보안 사이의 관계를 이용하여 보안성 증폭을 제공하는 것을 보인다. 또한 보안성 증폭 측면에서 접근 방식이 위상 오차 보정 방식이 더 보다 나은 보안성을 제시한다는 것을 보인다. QKD의 대표적인 예인 BB84 프로토콜을 이용하여 유니버셜 해시 함수가 보안성을 강화하는 과정을 설명한다. 마지막으로 결정적인 유니버셜 해시 함수가 메시지의 길이에 의존하지 않고 양자 Pauli 채널에서 보안성을 평가 받는 것을 유도한다.

Key Words : Calderbank – Shor – Steane (CSS) code, QKD(Quantum Key Distribution), hash functions, ϵ-almost $universal_2$ hash functions, Random Number Generator (RNG).

ABSTRACT

This paper introduces the concept of a dual hash function to amplify security in a quantum key distribution system. We show the use of the relationship between quantum error correction and security to provide security amplification. Also, in terms of security amplification, the approach shows that phase error correction offers better security. We describe the process of enhancing security using the universal hash function using the BB84 protocol, which is a typical example of QKD. Finally, the deterministic universal hash function induces the security to be evaluated in the quantum Pauli channel without depending on the length of the message.

I. 서 론

암호화를 위해서 필요한 시드 키가 부분적으로 도청 자에게 유출 된 경우에도 랜덤 해시 기능을 적용하면 보안성을 증폭시킬 수 있다. 이 과정을 보안성 증폭이라고 한다. 이 과정에서 비밀 증폭은 다른 보조 랜덤 키의 도움으로 구체화고 이 키는 공개되어 있으며 랜덤 시드 키라 한다. 이 목적으로 사용되는 랜덤 해시 함수는 흔히 추출기라고 불리는데, 보조 무작위 소스가 공개되지 않는 두 개의 소스 추출기라고 불리는 유사하지만 별개의 프로세스도 있다[1].

이러한 보안성 증폭 목적을 위한 가장 일반적인 랜덤 해시 함수는 유니버셜$_2$ 해시 함수이다[2][3].

유니버셜$_2$ 해시 함수를 사용한다고 가정하는 많은 보안 정리가 있는데 특히, 잔여 해싱 보조 정리 [4], [5]은 고전 및 양자 환경에서 다양한 확장과 응용을 가진다.

따라서 보안성 증폭 증폭은 이제 양자 키 분배 (QKD)의 보안을 보장하는 데 필수 불가결하게 되었다[4][8].

지금까지 가장 실용적인 추출기는 보편적인 해시 함수로 알려져 있으며, 그 중 가장 널리 사용되는 것은 Toeplitz 행렬이다. 이는 주로 입력 길이 n 에 대해 복잡도 $0(n\log n)$ 로 효율적으로 구현할 수 있기 때문이다.

여기서, 효율성의 통상적인 개념인 알고리즘이 다항식 시

※ 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음. [1711042435, 양자암호통신망 구축을 통한 신뢰성 검증기술 및 QKD 고도화를 위한 핵심요소기술 개발]

*광운대학교 전파공학과 소속 유비쿼터스 통신 연구실(sunyuil22@naver.com), (jinyoung@kw.ac.kr)

접수일자: 2017년 01월 15일, 최종게재확정일자: 2017년 02월 01일

간에서 완료가 되는 것은 충분하지 않지만, $0(n\log n)$인 복잡성의 엄격한 기준은 양자 키 분배 (QKD)에 대해 바람직하다는 것을 알 수 있다. 이는 일반적인 QKD 시스템의 경우 유한한 크기 효과가 입력 길이 n이 $n \geq 10^6$ [9], [10], [11] 이므로 일반적인 의미에서 효율적인 알고리즘인 $0(n^2)$은 쓸모가 없다.

실질적인 해시 함수에 대한 또 다른 중요한 기준은 임의의 시드에 얼마나 많은 난수를 필요로 하는 가이다. 이는 두 가지 방법, 즉 균일하게 랜덤 한 시드의 요구되는 길이 및 시드의 엔트로피에 의해 측정 될 수 있다.

전자를 최소화하는 것의 중요성은 확실하지만 후자는 실제 암호화 시스템을 위한 완벽한 난수 생성기를 준비하는 것이 매우 어렵 기 때문에 두 가지 방법 모두 똑같이 중요하다.

Trevisan의 추출기는 이러한 기준 [7, 11]의 관점에서 예외적으로 우수한 성능을 구현하는 것으로 알려져 있지만 계산 복잡도가 Toeplitz 사례의 $0(n\log n)$보다 크다는 단점이 있다 [11].

이 논문의 주된 목표는 이전 문헌에서보다 더 적은 랜덤 시드 길이를 필요로 하는 보안성 증폭을 위한 명쾌하게 무작위 해시 함수를 구성하는 것이며 입력 길이 n 에 대해 복잡성 $0(n\log n)$을 갖는 효율적인 구현을 허용하는 것이다.

이것은 물론 실제 암호화 시스템에 포함 된 실제 난수 생성기의 구현 비용을 줄이는 데 목적이 있다. 이 목표를 달성하기 위해 우리는 δ-almost dual universal2 해시 함수의 개념을 사용한다. 또한 우리는 δ-almost dual universal2 해시 함수와 기존 추출기를 연결하여 추출기를 구성하는 새로운 방법을 사용한다. 시드 길이를 최소화하는 것 외에도 불균일한 랜덤 시드를 사용할 수 있는 일반적인 방법을 제시한다. 이러한 방법은 일반적인 유니버셜$_2$ 해시 함수뿐 아니라 이중 유니버셜$_2$ 해시 함수를 포함하여 다양한 클래스의 추출기에 적용될 수 있다는 점에서 일반적이다. 여기서 최소 엔트로피는 불균일한 랜덤 시드의 무작위성을 설명하는 척도로 사용된다. 이 방법은 난수 생성기 (RNG)의 구현 비용을 줄이기 위한 합리적인 트릭을 의미하는 것이 아니라 보안성 증폭 이론과 실제구현간의 차이를 채우기 위한 중요한 기술이다. 즉, 실제적으로 랜덤 시드을 출력하는 난수 생성기는 없지만 불완전한 난수 생성기를 랜덤 시드로 사용하여 실제 보안성 증폭 모듈로부터 엄격한 보안 출력을 추출하기 위해 이와 같은 대안을 선택 할 수 있다. 특히, QKD의 맥락에서 그러한 난수 생서기의 불균일성은 최근 광범위하게 연구 된 실용적인 시스템의 불완전성의 새로운 사례로 간주 될 수 있으며 [12], δ-almost 이중 유니버셜$_2$ 해시 함수는 실용시스템의 불완전성에 대한 대책으로 활용가능하다.

δ-almost 이중 유니버셜$_2$ 해시 함수의 개념과 이를 위한 확장된 남은 해싱 보조 정리는 참고 문헌에서 제안되었다 [12], [13]. 참고 문헌 [13]에서는 전통적인 유니버셜$_2$ 해시 함수와의 명시적인 포함 관계를 제시했다. 예를 들어, 임의의 선형 및 사상 적 해시 함수가 유니버셜$_2$ (δ = 1 인 경우)이면, 그것은 자동적으로 δ'-almost 이중 유니버셜$_2$ 이며, 여기서 δ'은 2보다 작은 또 다른 상수이다. 이러한 의미에서, δ-almost 이중 유니버셜$_2$ 함수는 전통적인 유니버셜$_2$ 함수의 확장으로 간주 될 수 있다. 이 새로운 클래스의 해시 함수를 기반으로 여러 클래식 및 양자 보안 평가가 수행되었다 [14], [15]. 특히 유한 길이 보안 분석에 대해서 이 새로운 클래스로 수행되었다.

본 논문은 기존 및 이중 유니버셜$_2$ 해시 함수의 특성, 해당 보안 기준 및 해당하는 나머지 해싱 보조 정리를 검토하여 시작한다. 그런 다음 임의의 해시 함수를 연결하여 임의의 해시 함수를 생성하는 새로운 방법을 제안한다. 2 개의 기존 δ-almost 유니버셜$_2$ 해시 함수 [11]를 연결하는 방법이 이미 알려져 있지만, 여기서는 δ-almost 이중 유니버셜$_2$ 해시 함수를 포함한 다른 조합에 중점을 둔다. 이러한 결과를 이용하여 이전 방법보다 적은 랜덤 시드 길이 h를 요구하는 보안 해시 함수를 제시하고 복잡도 $0(n\log n)$로 구현할 수 있다. 다음 장에서는 δ-almost 이중 유니버셜$_2$ 해시 함수를 이용한 QKD의 보안성 증폭을 적용한 것을 설명하고 복잡성을 낮춤을 보인다.

Ⅱ. 본론

이 섹션에서는 QKD에 거의 모든 이중 유니버설 해시 함수 집합이 적용될 때 강력한 보안을 보인다. 이를 위해 QKD 보안 증거의 위상 오류 수정에 적용한다. 따라서 이 접근 방식을 위상 오류 수정 접근 방식이라고 부른다. 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 $\mathcal{F} = \{f_r : \mathbb{F}_2^m \to \mathbb{F}_2^l | r \in I\}$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 $v = k_A \oplus G(C_l) r_A^T$ 과 XOR 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 가장 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 $f_r : F_2^m \rightarrow F_2^l$ 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.

Shor and Preskill [8], [14], [15]에 의해 널리 사용되는 증명 기법을 사용함으로써, 이 프로토콜의 완전 보안성을 $\mathcal{F}$가 완전 랜덤인 선형 함수 [3], [15]일 때 보였다. 다른 한편, 양자 Finneti 표현 정리를 사용함으로써 Renner는 보안성 증폭을 위해 유니버셜$_2$ 해시 함수를 사용하여 BB84 프로토콜의 무조건 보안을 증명했다 [5]. 이 섹션에서 우리는 $\mathcal{F}$가 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 [10]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 섹션의 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]과 [8]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

$$\wedge_t(\rho) = \sum_{x,z \in} P^{XZ}(x,z) Z^x X^z \rho (Z^x X^z)^\dagger, \qquad (1)$$

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(즉, 양자 통신부).

보편적인 구성 가능성 [3]을 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 Holevo 정보 $X := Tr \rho_{A,E} (\log \rho_{A,E} - \log \rho_A \otimes \rho_E)$을 통해 보안을 평가할 수 있다. 이 값들은 다음 수식으로 묶여있는 것으로 알려져 있다.

$$\| \rho_{A,E} - \rho_A \otimes \rho_E \|_1 \leq 2\sqrt{2} \sqrt{P_{ph}}, \qquad (2)$$
$$X \leq \eta_n(P_{ph}), \qquad (3)$$

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

$$\eta_x(x) := \begin{cases} -x \log x - (1-x)\log(1-x) + nx, & \text{if } x \leq 1/2 \\ 1 + nx, & \text{if } x > 1/2. \end{cases} \qquad (4)$$

이제 비밀 키의 보안을 살펴보면 유일한 차이점은 키가 효과적으로 기존 CSS 코드 C_1, C_2에 해당하는 퀀텀 CSS 코드에 의해 오류가 수정 된 퀀텀 채널을 통해 전송된다는 것이다. 그러므로 위와 같은 주장을 본질적으로 사용함으로써, 보안은 양자 에러 정정 이후에 남아있는 위상 에러 확률에 의해 평가 될 수 있다. 사람이 이것을 단계별로 볼 때(즉, x 기준), 이 확률은 $P_{ph}(C_2^\perp / C_1^\perp)$로 표시되는 고전적인 CSS 코드 $C_2^\perp / C_1^\perp$의 디코딩 오류 확률에 의해 주어진다. 그런

다음, 비밀 키의 보안은 다음과 같이 계산될 수 있다.

$$\| \rho_{A,E} - \rho_A \otimes \rho_E \|_1 \leq 2\sqrt{2}\sqrt{P_{ph}\left(C_2^{\perp}/C_1^{\perp}\right)} \quad (5)$$

$$X \leq \eta_l\left(P_{ph}\left(C_2^{\perp}/C_1^{\perp}\right)\right). \quad (6)$$

Renes [34, Th.5.1]는 (4)와 동일한 평가를 수행했다. $C_1 = \mathbb{F}_2^n$의 경우, 코아시 (Koashi) 와 미야 데라 (Miyadera)는 본질적으로 동일한 관계를 발견했다.

그 다음, 우리는 $P_{ph}\left(C_2^{\perp}/C_1^{\perp}\right)$을 평가하기 위해 정리 8을 적용한다. 우리의 BB84 프로토콜에서, 서브 코드 $C_2 \subset C_1$은 고정 코드 C_1의 최소 차원 $m-l$을 갖는 ϵ-almost 유니버셜 서브 코드 집합 로부터 무작위로 선택된다. 이는 최대 차원 $n-m+l$ 인 고정 코드 $C_1^{\perp}$의 ϵ-almost 유비너셜$_2$ 확장 코드 집합에서 이중 코드 $C_2^{\perp}$가 선택되는 경우에 해당한다. 따라서, 다음 부등식

$$E_{C_1 \in C} P_e\left(C_1/C_2\right) \leq \epsilon \sum_{k=0}^{n} \hat{P}^X(k) 2^{-n\left[1-h\left(\{k/n,1/2\}\right)-R\right]_+}. \quad (7)$$

을 이용하여 식 (8)을 얻을 수 있다.

$$\mathrm{E}_{C_2 \in \mathcal{C}} P_{\mathrm{ph}}\left(C_2^{\perp}/C_1^{\perp}\right) \leq \varepsilon \sum_{k=0}^{n} \hat{P}^X(k) 2^{-n[S-h(\min\{k/n,1/2\})]_+}. \quad (8)$$

여기서, $S=(m-l)/n$은 희생 된 비트 레이트, 즉, 보안성 증폭에 의해 감소 된 비트의 비율이다. 따라서, (2), (3) 및 $x \mapsto \sqrt{x}$, $x \mapsto \eta_l$ 으로부터 다음 수식을 얻을 수 있다.

$$\begin{aligned} &\mathrm{E}_{C_2 \in \mathcal{C}} \|\rho_{A,E} - \rho_A \otimes \rho_E\| \\ &\leq 2\sqrt{2}\sqrt{\varepsilon \sum_{k=0}^{n} \hat{P}^X(k) 2^{-n[S-h(\min\{k/n,1/2\})]_+}} \\ &\mathrm{E}_{C_2 \in \mathcal{C}} \chi \\ &\leq \eta_l\left(\varepsilon \sum_{k=0}^{n} \hat{P}^X(k) 2^{-n[S-h(\min\{k/n,1/2\})]_+}\right). \end{aligned} \quad (9)$$

실용적인 QKD 시스템에서, 가중치 분포 $\hat{P}^X$은 샘플링 된 비트의 비트 오류율로부터 추정 될 필요가 있다. 무시할 수 있는 작은 확률을 제외하고 위상 오류율 $p_{ph}=k/n$가 특정 값 $\hat{p}_{ph}$ 미만으로 추정되고 $S > h\left(\hat{p}_{ph}\right)$ 인 경우 인수 $\epsilon 2^{-n[S-h(\min\{k/n,1/2\})]_+}$는 $n \to \infty$에 대해 0으로 수렴한다. 점근 적으로, 보안성 증폭에 의해 임의의 $\delta > 0$ 비트로 $n\left[h\left(\hat{p}_{ph}\right)+\delta\right]$ 비트를 희생하는 것으로 충분하다.

위에서 언급 한 논증을 통해 우리는 QKD의 보안을 위해 C_1의 ϵ-almost 유비너셜$_2$ 서브 코드 집합에서 코드 C_2을 선택하는 것으로 충분하지만 기존 결과는 코드 C_2이 C_1의 유비너셜$_2$ 서브 코드 그룹에서 임의로 선택된 경우에만 보안을 보장한다. C_1의 서브 코드 집합은 C_1의 2-almost 유비너셜$_2$ 서브 코드 집합이므로 조건은 [9]에 의한 것보다 상당히 약하다.

또한 $C_1 = \mathbb{F}_2^n$를 설정함으로써 우리의 논리가 Koashi의 증명 기법 [6]에도 적용된다는 점에 유의해야한다. 즉, Koash's의 프로토콜에 나타나는 무작위 행렬은 almost 이중 유비너셜$_2$ 코드 집합으로 대체 될 수 있다. 더욱이, 전술 한 논의는 $\{C_2 \subset C_1\}$의 ϵ-almost 이중 유비너셜$_2$ 서브 코드 쌍으로 확장 될 수 있다. 이제 우리는 이중 코드 $C_2^{\perp}$가 정리 6 [18]의 조건을 만족하도록 C_1의 $m-l$ 차원 서브 코드 C_2를 선택한다. 파울리 채널이 순열 불변 인 경우, 이 코드는 (8)과 (9)를 $\epsilon = n+1$로 만족시킨다.

Ⅲ. 결정적 유니버셜 해시 함수

사실, 앞서 언급 한 내용은 ϵ-almost 이중 유비너셜$_2$ 코드 쌍 집합에 대해서도 유효하다. 우리의 설정은 순열이 불변하므로, 결정론적인 코드 쌍을 사용할 수 있다. 즉, 코드 C_1이 주어지면 $C_1^{\perp} \subset C_2^{\perp}$과 $\epsilon\left(C_2^{\perp}/C_1^{\perp}\right) \leq n+1$와 같은 또 다른 t-차원의 서브 코드 C_2를 선택할 수 있다. 그런 다음 (5), (6) 및 (9)를 결합하여 C_1, C_2의 보안이 다음과 같이 평가할 수 있다.

$$P_e(C_1/C_2) \leq (n+1)2^{-nE(R,p)}. \quad (9)$$

$$\|\rho_{AE} - \rho_A \otimes \rho_E\|_1 \leq \sqrt{n+1}\, 2^{-\frac{1}{2}nE(1-S,p_{\mathrm{ph}})+\frac{3}{2}}$$

$$\chi \leq \eta_l\left((n+1)2^{-nE(1-S,p_{\mathrm{ph}})}\right). \quad (10)$$

여기서 메시지 길이는 $l = \dim C_1 - t$ 이고 코드 C_2의 생성은 p_{ph}의 값에 의존하지 않는다는 점에서 보편적이다. 따라서, $C_1 \to C_1/C_2$에 의해 정의 된 선형 맵은 임의로 주어진 양자 Pauli 채널의 독립적이고 동일한 애플리케이션에 대해 안전한 결정적인 유니버셜 해시 함수의 유형으로 간주 될 수 있다.

Ⅳ. 결론

본 논문은 양자 키 분배 시스템에서의 보안성을 증폭시키기 위한 이중 해시 함수의 개념을 소개하였다. 우리는 almost 이중 해시 함수 집합의 클래스가 해시 함수 집합에 포함하는 것을 보였다. 양자 오류 정정과 보안 사이의 관계를 이용하여, 우리는 ϵ-almost 이중 유비너셜$_2$ 집합이 적용되면 보안성 증폭을 제공하는 것을 보였다. 또한 보안성 증폭 측면에서 접근 방식이 위상 오차 보정 방식이 더 보다 나은 보안성을 제시한다는 것을 보였다. QKD의 대표적인 예인 BB84 프로토콜을 이용하여 유니버셜 해시 함수가 보안성을 강화하는 과정을 설명하였다. 이와 관련하여 완전한 무작위성을 보장하는 시드를 이용하여 어떻게 보안성이 강화되는 지를 BB84 프로토콜이 양자 키를 주고받는 과정을 통하여 보였다. 마지막으로 결정적인 유니버셜 해시 함수로 메시

지의 길이에 의존하지 않고 양자 Pauli 채널에서 보안성을 평가하였다.

참 고 문 헌

[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

[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.

[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.

[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.

[5] J. L. Carter and M. N.Wegman, "Universal classes of hash functions," *J. Comput. Syst. Sci.*, vol. 18, pp. 143 - 154, 1979.

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

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

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

[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.

[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.

[11] M. Hamada, "Reliability of Calderbank - Shor - Steane codes and security of quantum key distribution," *J. Phys. A: Math. Gen.*, vol. 37, no. 34, pp. 8303 - 8328, 2004.

[12] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441 - 444, 2000.

[13] D. R. Stinson, J. Feigenbaum, Ed., "Universal hashing and authentication codes," *in Proc. Adv. Cryptol.—CRYPTO*, 1992, vol. 576, LNCS, pp. 62 - 73.

[14] D. R. Stinson, "Universal hash families and the leftover hash lemma, and applications to cryptography and computing," *J. Combin. Math. Combin. Comput.*, vol. 42, pp. 3 - 31, 2002.

[15] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover hashing against quantum side information," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5524 - 5535, Aug. 2011.

저자

이 선 의(Sun Yui Lee) **학생회원**

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

<관심분야> : 가시광 통신, 협력통신, 인지무선통신, 양자통신

김 진 영(Jin Young Kim) **종신회원**

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

<관심분야> : 다지털통신, 가시광통신, UWB, 부호화, 인지무선통신, 4G 이동통신