순환 그래프에 기반한 다자간 양자 키 분배

Cycle graph-based multiparty quantum key distribution

권영완

한국과학기술원, 학부 20220043

Abstract | 본고에서는 양자 통신 채널이 직접 연결되지 않은 두 참가자 A_1 과 A_i 가 다른 참가자들을 경유해 양자 통신을 주고받는 다자간(multiparty) QKD를 다룬다. 이러한 상황에서 두 참가자가 포함된 순환 그래프(Cycle graph)에 기반한 QKD를 제안하였고, 간단한 공격에 대한 보안성을 증명하였다. 순환 그래프에 기반함으로써 본 프로토콜이 가지는 장단점 및 한계에 대해 논의하였고 예시를 통해 그 활용방안을 제시하였다.

I. Introduction

양자 암호(Quantum Cryptography, QC)란 양자역학의 원리에 기반한 보안성을 가지는 암호체계를 말한다. 예를 들어, '계를 섭동(perturbation)하지 않고 관측할 수 없다'는 양자역학적 원리는 곧 섭동의 유무를 통해 도청자가 존재하는지 확인할 수 있음을 시사한다. **양자 키 분배** (Quantum Key Distribution, **QKD**)는 양자 암호 통신의 대표적인 분야로서, 대칭키 암호 방식에 이용되는 암호키를 안전하게 공유하는 것을 목적으로 한다.

가장 대표적인 QKD 프로토콜은 1984년 Charles H. Bennett과 Gilles Brassard에 의해 고안된 BB84 프로토콜 [1] 이다. BB84 프로토콜은 직선 기저(basis)인 $\{|0\rangle, |1\rangle\}$ 과 대각선 기저

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

을 이용한다. 그 과정은 다음과 같다. 먼저 Alice가 4개의 상태 중 무작위로 하나를 선택해 해당 큐비트(qubit)를 Bob에게 전송한다. Bob은 두 개의 기저 중 하나를 무작위로 선택해 그 상태를 측정한다. 이를 반복한 후, Alice와 Bob은 공개 채널을 통해 그들이 사용한 기저 정보를 주고받는다. Alice와 Bob이 동일한 기저를 선택한 경우의 비트만을 남겨 sifted key를 얻는다. 만약 Eve가 Alice와 Bob 사이 도청을 시도한다고 가정할 때, 양자 상태의 복제 불가능성 원리(No-cloning theorem)에 의해 도청자는 새로운 큐비트를 Bob에게 송신해야 한다. 이 과정에서 error가 발생하게 되고, Alice와 Bob이 서로의 sifted key 일부를 비교하면 도청자의 존재를 파악할 수 있다. 그렇지 않은 경우 sifted key를 이용해 암호키(secret-key)를 생성한다 [2].

본고는 Alice와 Bob 뿐만 아니라 다수의 참가자들을 대상으로 하는 **다자간 QKD** 프로토콜을 다룬다. 여기서 말하는 **다자간**(**multi-party**) 암호체계란 [3,4]에서 제시된 것과 유사하게, Alice가 다른 참가자들인 Bob, Charlie, ...을 거쳐 목적지인 David와 양자 통신을 주고받는 상황을 상정한다. Alice가 경유하는 다른 참가자들이 부정직(dishonest)할 수 있으므로 이를 보완할 방법이 필요하다 [4].

이에 본 연구가 제안하는 프로토콜은 보안 그래프(graph)에 존재하는 **사이클**(**cycle**)을 이용하는 방법이다. 관련된 선행 연구 [5]에서는 최소 스패닝 트리(Minimum Spanning Tree, MST)를 이용한 다자간 QKD가

고안되었다. 본 연구가 [5] 프로토콜에 대해 가지는 차이점은 참가자들이 하나의 암호키를 공유하지 않는다는 것, 그리고 스패닝 트리가 아닌 Cycle에 기반한다는 것에서 기인하는 다양한 성질들이다.

본고는 다음과 같이 구성되어 있다: 제 II절은 고안한 프로토콜을 소개한다. 제 III절은 간단한 공격들에 대한 보안성을 보인다. 제 IV절에서 결론과 논의점을 서술한다 [6].

II. Protocol

N 명의 참가자들이 존재하는 네트워크에서, 각 참가자들을 꼭짓점으로 하고, 두 참가자 사이 양자 채널을 간선으로 가지는 무향 그래프를 생성하자. 이를 보안 그래프(security graph)라고 한다 [5]. 보안 그래프 G 내에서, 한 참가자 A_1 이 다른 참가자 A_i 와 키 분배를 하고자 한다.

이 때 우리가 필요한 것은 A_1 과 A_i 를 지나는 Cycle이 존재하는 것이다. 이를 전제로 하여, n 명의 참가자 $A_1, A_2, \cdots, A_i, \cdots, A_n$ 이 Cycle을 이룬다고 가정하자. 즉, Figure 1과 같은 G의 부분 그래프 C_n이 존재한다고 가정한다.

본 연구에서 제안하는 Cycle에 기반한 QKD는 Figure 1의 순환 그래프 C_n 에서 행해진다. 그 과정은 다음과 같다.

1. **A_1 이 A_i 와 경로 p_1 을 통한 양자 통신으로 키를 분배한다.**
2. **A_1 과 A_i 이, p_1 과 반대인 경로 p_2 을 통해 같은 방법으로 키를 분배한다.**
3. **경로 p_1 을 이용해 얻은 암호키를 k_1, p_2 을 이용해 얻은 암호키를 k_2 라 하자.**
4. **A_1과 A_i의 최종 암호키 k를**
$$k = k_1 \oplus k_2$$
로 설정한다. ($\oplus$는 $mod\,2$ 덧셈 연산)

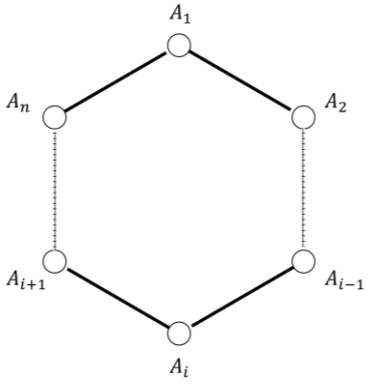

Figure 1. n개의 꼭짓점 $V = \{A_1, A_2, \cdots, A_n\}$에 대해 V로 구성된 순환 그래프 C_n의 모습. A_1과 A_i 사이에는 두 개의 경로

$$p_1 = A_1 A_2 \cdots A_{i-1} A_i$$
$$p_2 = A_1 A_n \cdots A_{i+1} A_i$$

가 존재함을 확인할 수 있다.

몇 가지 주의할 부분이 존재한다. 먼저, 과정 1, 2에서 '경로를 통한 양자 통신'을 정의해야 한다. 그 과정은 다음과 같다.

1. A_1 이 발신자, 목적지, 통하는 경로 정보 (A_1, A_i, p_1) 을 다른 참가자들에게 공개 채널로 알린다.
2. A_1 이 경로 내 첫번째 참가자인 A_2 에게 양자 채널로 큐비트를 전송한다.
3. A_2는 수신된 큐비트의 상태를 보존한 채 경로 내 다음 참가자인 A_3 에게 전송한다. 이는 양자 리피터(Quantum repeater)의 원리를 이용해 가능하다 [7].
4. 경로 내의 모든 참가자 A_j ($2 \le j \le i-1$)가 3을 반복한다. 결과적으로 목적지 A_i에게 큐비트가 수신된다.

두번째로, Cycle에 기반한 QKD의 과정 3에서 A_1 은 비트 오류율(QBER)을 계산해야 한다. 각각의 경로 p_1 , p_2 을 통한 양자 통신의 QBER을 구하고, 그 값이 둘 모두 기준치보다 충분히 작은 경우에만 과정 4로 넘어간다. 그렇지 않은 경우 과정 1,2를 반복하거나,

도청의 유무를 파악한다. (자세한 내용은 제 III절에서 서술)

세번째로, 과정 4에서 두 개의 암호키 k_1, k_2 문자열의 길이 $|k_1|$, $|k_2|$는 일반적으로 다르다. 따라서 최종 암호키 k 의 길이가 $|k| = min(k_1, k_2)$ 이 되도록 암호키를 슬라이싱할 필요가 있다.

III. Security Proof

제 III절에서는 본 프로토콜이 몇 가지 기본적인 공격 (도청, 부정직한 참가자, 스푸핑)에 대하여 가지는 무조건적 보안성을 보인다. 무조건적 보안성(unconditional security)은 공격자에게 어떠한 컴퓨팅 파워나 자원에 대한 제약이 존재하지 않는 상황을 가정한다.

A. 도청 (Eavesdropping)

Eve가 순환 그래프 C_n의 어떤 한 간선에서 도청을 시도한다고 가정하자. 본 프로토콜은 크게 두가지 이유로 보안성을 가진다.

먼저, BB84에서와 유사하게 도청은 비트 오류(bit error)를 발생시킨다 [2]. 이로 인해 발신자 A_1은 Eve의 존재를 파악할 수 있다. 게다가, A_1은 다음과 같은 이진 탐색(binary search) 알고리즘으로 Eve의 위치를 특정할 수 있다.

1. A_1과 A_i 사이 두 경로 p_1, p_2을 통한 양자 통신의 QBER 값을 각각 r_1, r_2라 하자. QBER 값의 기준치 λ에 대해, $r_1 \cong r_2 < \lambda$ 이면 도청자가 존재하지 않는다.
2. 만약 $r_2 \ll r_1$이면 경로
$$p_1 = A_1 A_2 \cdots A_{i-1} A_i$$
내에 도청자가 존재함을 알 수 있다. $i' = [i/2]$로 두고 두 경로
$$p'_1 = A_1 A_2 \cdots A_{i'-1} A_{i'}$$
$$p'_2 = A_1 A_n \cdots A_{i'+1} A_{i'}$$
에 대하여 다시 키 분배를 수행한다. 이 후 각각의 경로에 대해 QBER 값 r'_1, r'_2를 구한다. 두 값을 비교하면 마찬가지로 p'_1, p'_2 중 도청자가 존재하는 경로를 알 수 있다.
3. 과정 2를 반복하면 시간 복잡도 $O(\log n)$ 과정으로 도청자 Eve의 위치를 특정할 수 있다.

뿐만 아니라, 순환 그래프 내에 다수의 도청자가 존재하는 경우에도 위 과정을 이용하면 도청자들이 포함되는 최소의 경로 p을 찾을 수 있다. 이 때 경로 p 내부의 한 참가자에 대해서 위 과정을 반복하면, 이론적으로 다수의 도청자의 위치를 모두 특정할 수 있다.

두번째로, Eve가 순환 그래프 내의 두 개의 경로 p_1, p_2 중 p_1을 도청해 암호키 k_1을 완전히 알더라도 최종 암호키 $k = k_1 \oplus k_2$로 암호화된 암호문을 복호화 할 수 없다. 가령 평문 s가 $c = s \oplus k$로 OTP(One-time pad) 방식으로 암호화된 경우,

$$c \oplus k_1 = s \oplus (k_1 \oplus k_2) \oplus k_1 = s \oplus k_2$$

으로 k_2에 대한 정보 없이는 복호화가 불가능하다 [8].

B. 부정직한 참가자 (Dishonest participant)

순환 그래프 내부에서 정보를 얻는 부정직한 참가자에 대해서도 도청에 대한 보안성이 동일하게 적용된다. 마찬가지로 두 개의 경로 p_1, p_2를 이용해 이진 탐색을 하면 부정직한 참가자를 특정할 수 있다.

C. 스푸핑 (Spoofing)

Eve가 순환 그래프 내부의 참가자 A_1을 모방하여 양자 통신을 시도하는 경우를 가정하자. 양자 통신 과정에서 발신자, 목적지, 경로 정보를 그래프 내 모든 참가자들에게 알려야 하므로, A_1 또한 해당 사실을 알게 된다. 따라서 A_1이 Eve의 존재를 알려 스푸핑 시도를 저지한다.

IV. Conclusion and Discussion

본고에서는 양자 채널이 직접 연결되지 않은 두 참가자 A_1 과 A_i 가 암호키를 안전하게 분배하는 프로토콜을 제시하였다. 이에 대하여 몇 가지 논의점이 존재한다.

먼저 보안 그래프 G 에 A_1 과 A_i 을 지나는 Cycle이 존재한다고 가정하였다. 이는 일반적인 경우에 대하여 보다 수치적인 분석이 필요할 것으로 보인다. 허나 QKD의 실제 장거리(수십 km) 구현에서는 양자 채널을 나누어서 양자 리피터(Repeater; 신호 재생 중계장치)들을 설치하는 것이 필요하다 [2]. 따라서 적당한 위치의 노드 $A_1, A_2, \cdots, A_i, \cdots, A_n$ 에 리피터를 설치하고 이들이 Cycle을 이루도록 설계한다면 장거리 양자 채널 형성 및 본 프로토콜을 활용 가능할 것이다.

또한 주목할 점은 제 III절에서 볼 수 있듯 Cycle 외부의 공격자에 대하여 견고한 보안성을 가진다는 점이다. 뿐만 아니라, 순환 그래프 내부에 존재하는 모든 참가자 A_i 와 A_j 가 키 분배를 한다고 가정하자. 이 경우 순환그래프를 이루는 시스템에서, 분산(distributed)되고 탈중앙화(de-centralized)된 양자보안 모델 구축의 가능성을 시사한다. 탈중앙화 보안 모델의 장단점에 대해서는 여러 논의가 진행되어왔다 [9]. 이러한 논의를 받아들이고, 본 연구로 돌아와 대전광역시의 대덕연구개발특구에서 연구기관, 국가기관 및 교육기관에 대해 순환 그래프를 이루는 양자 네트워크를 생각해보자. 양자 암호에 기반하여 더욱 보안성이 높고 이상적으로 설계된 보안 통신 체계를 구축 가능하다는 기대를 가질 수 있다.

본 다자간 QKD 프로토콜의 효율과 실제 구현 가능성은 본고에서 다루어지지 않았는데, 이는 추후 연구와 다양한 논의가 필요할 것으로 보인다.

V. Reference

[1] C. H. Bennett, G. Brassard et al., “Quantum cryptography: Public key distribution and coin tossing,” in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, no. 0. New York, 1984.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Reviews of modern physics, vol. 74, no. 1, pp. 145-152, 2002.

[3] M. Hillery, V. Bu˘zek, and A. Berthiaume, Phys. Rev., vol. 59, p. 1829, (1999).

[4] K. Chen and H.-K. Lo, "Conference key agreement and quantum sharing of classical secrets with noisy GHZ states," *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*, pp. 1607-1611, 2005.

[5] S. K. Singh and R. Srikanth, e-print arXiv:quant-ph/0306118.

[6] R. Matsumoto, Phys. Rev. A., vol. 76, no. 6, p. 062316, (2007).

[7] Q. Ruihong and M. Ying, *J. Phys.: Conf. Ser.* **1237** 052032, (2019).

[8] C. E. Shannon, "Communication theory of secrecy systems," in *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, 1949.

[9] R. O. Sinnott *et al*., "Advanced Security for Virtual Organizations: The Pros and Cons of Centralized vs Decentralized Security Models," *2008 Eighth IEEE International Symposium on Cluster Computing and the Grid (CCGRID)*, pp. 106-113, 2008.