**Cycle에 기반한 다자간 양자 키 분배**

Cycle-based multiparty quantum key distribution

권영완

*한국과학기술원, 학부 20220043*

Abstract (초록) | (size 10) 보고서의 내용을 요약하여 초록을 작성한다. 연구의 배경, 연구의 동기, 연구 결과, 연구의 시사점이 명확히 드러나도록 작성한다. 초록은 6줄 이내로 쓴다. 보고서는 높임말을 사용하지 않는다.

1. **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 과 대각선 기저

를 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].

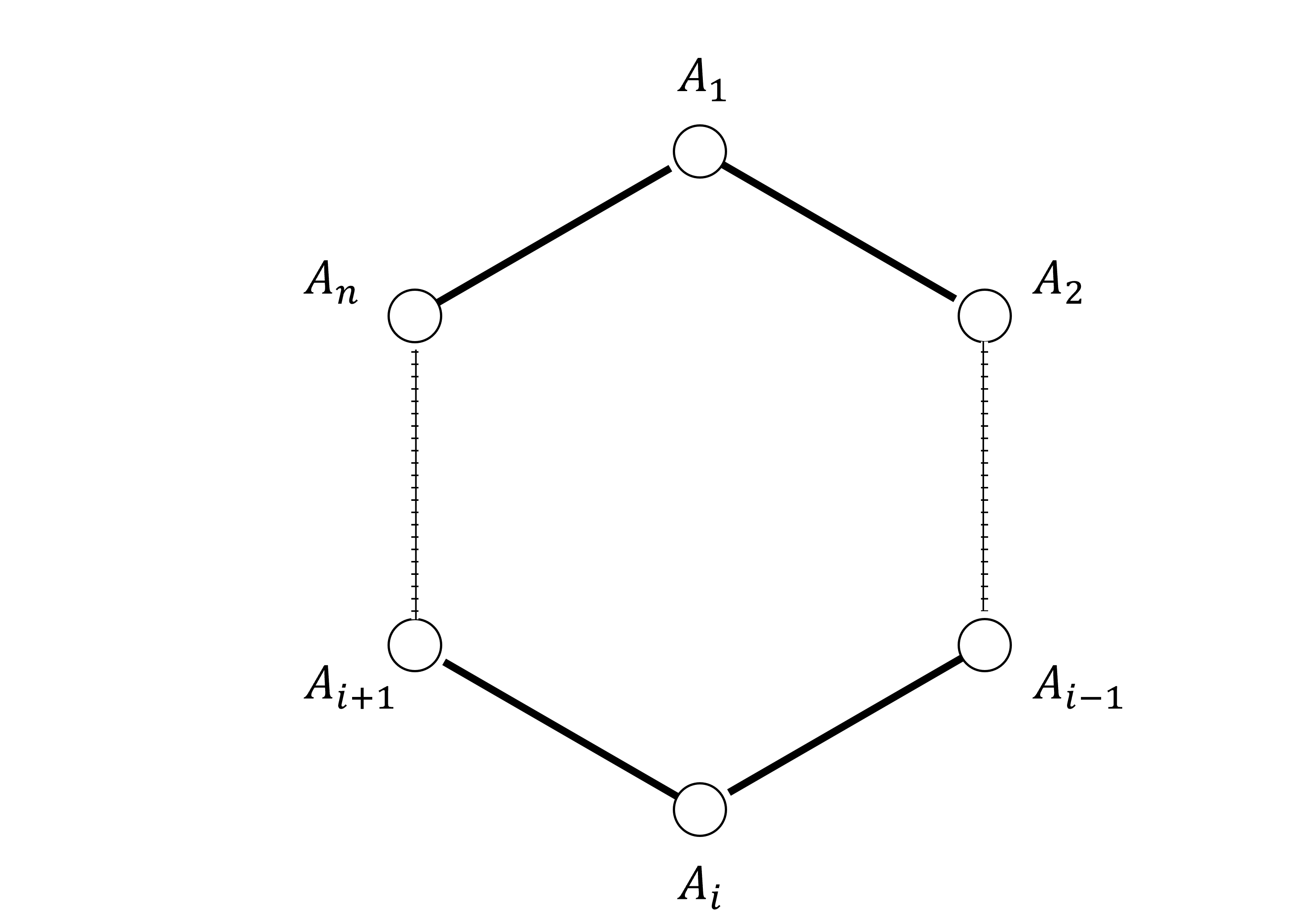
이에 본 연구가 제안하는 프로토콜은 보안 그래프(graph)에 존재하는 **사이클**(**cycle**)을 이용하는 방법이다. 관련된 선행 연구 [5]에서는 최소 스패닝 트리(Minimum Spanning Tree, MST)를 이용한 다자간 QKD가 고안되었다. 본 연구가 [5] 프로토콜에 대해 가지는 차이점은 참가자들이 하나의 암호키를 공유하지 않는다는 것, 그리고 스패닝 트리가 아닌 Cycle에 기반한다는 것에서 기인하는 다양한 성질들이다.

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

1. **Protocol**

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 내에서, 한 참가자 이 다른 참가자 와 키 분배를 하고자 한다.

이 때 우리가 필요한 것은 과 를 지나는 Cycle이 존재하는 것이다. 이를 전제로 하여, 명의 참가자 이 Cycle을 이룬다고 가정하자. 즉, Figure 1과 같은 의 부분 그래프 이 존재한다고 가정한다.

Figure 1. 개의 꼭짓점 에 대해 로 구성된 순환 그래프 의 모습. 과 사이에는 두 개의 경로

가 존재함을 확인할 수 있다.

본 연구에서 제안하는 Cycle에 기반한 QKD는 이러한 순환 그래프 에서 행해진다. 그 과정은 다음과 같다.

1. **이 와 경로 을 통한 양자 통신으로 키를 분배한다.**
2. **과 이, 과 반대인 경로 을 통해 같은 방법으로 키를 분배한다.**
3. **경로 을 이용해 얻은 암호키를 , 을 이용해 얻은 암호키를 라 하자.**
4. **과 의 최종 암호키 를**

**로 설정한다. (는 덧셈 연산)**

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

1. 이 발신자, 목적지, 통하는 경로 정보을 다른 참가자들에게 공개 채널로 알린다.
2. 이 경로 내 첫번째 참가자인 에게 양자 채널로 큐비트를 전송한다.
3. 는 발신된 큐비트의 상태를 보존한 채 경로 내 다음 참가자인 에게 전송한다. 이는 양자 리피터(Quantum repeater)의 원리를 이용해 가능하다 [7].
4. 경로 내의 참가자 는

각각의 암호키 ,에 대한 비트 오류율(QBER)을 구하고, 각각의 QBER이 모두 기준치보다 충분히 작은 경우 과정 4로 넘어간다. 그렇지 않으면,

K\_1 K\_2 길이 차이

1. **Security Proof**
2. **Conclusion and Discussion**

연구 결과를 정리하고 그 의미를 설명한다.

연구 내용을 정리하고, 연구가 가지는 의의와 한계를 서술힌다.

1. **Reference**

참고문헌을 작성한다. 논문의 경우 아래와 같이 저자/저널/권호수/페이지/년도 순서대로 작성하되, 권호수는 bold로 나타낸다.

[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. Buˇzek, 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).

**<추가 공지 내용>**

**기말보고서 제출기한: 6/10 (금) 오후 6시**

반드시 전체 5페이지 이하로 작성한다!!! .(길다고 좋은 보고서가 되는 것은 아니다. 간단하지만 핵심을 정확히 전달하는 것이 좋은 보고서다. 생각해보라. 평가하는 사람은 5 x 20 = 100 쪽의 보고서를 읽어야 한다. 짧지만 핵심을 전하는 보고서가 더 효과적일 수 있다.)

**평가기준**

format and structure (형식 및 가독성) - 20%

Logic and contents (논리성, 참신성, 독창성) - 30%

Impact (연구 수행의 깊이, 성실도, 연구결과의 중요성) - 50%

**1.**

(폰트크기10) 연구의 배경 및 필요성 등을 기술한다. 잘 모르는 사람도 이해될 수 있도록 쉽게 설명하고, 연구의 동기가 명확히 드러나도록 서술한다. 문헌을 인용할 때는 인용한 위치에 표시해주고, 보고서 마지막 reference에 추가한다. 아래 예시

“…이러한 이유로, 기존의 연구에서는 반강자성체 자체를 연구의 대상으로 삼지 못했고, 강자성체의 자화를 고정시키는 교환바이어스(exchange bias)를 주기 위한 수동적 소자 정도로만 사용되어 왔다 [1,2]. 그러나 최근에 들어 이러한 반강자성체 연구가 스핀트로닉스 연구의 주류로 떠오르고 있다…”

그림을 넣는 경우도 마찬가지로 본문 중에 해당하는 부분에 표시해주어야 함. 아래 예시

“[그림 1]에서 보는 것과 같이….”

“최근 보고된 결과에 의하면 [그림 1 참조], 통계적 분석의 중요성이 더욱 증가하고 있다”

연구 목표 및 내용을 기술함. 목차는 본인이 자유롭게 조절가능함 (research goal을 introduction에 써도 됨). 자신의 연구결과를 가장 잘 나타낼 수 있도록 목차나 content를 조절할 수 있음..

아래 내용을 명심해서 작성

“이 연구는 기존의 연구에 비해서 어떤 것이 다른가? 어떤 것이 새로운가?”

“왜 이 연구를 해야 하는가?”

“이 연구는 누구에게 혹은 어디에 도움이 되는가? (왜 사람들은 귀중한 시간을 들여서 이 보고서를 읽어야 하는가?”

**-글을 쓰는 요령 몇 가지-**

1. 요리를 만드는 요리사든, 글을 쓰는 작가든, 자신감이 있어야 한다.

그림 1. 그림 설명 (size 9, 삽입된 그림을 정확히 설명함. 그림에 나타나는 글자는 size 9에 맞춤 (글자가 작아서 보이지 않으면 곤란함)). 그림은 군더더기 없어야 하며, 본문에 설명하지 않는 그림은 넣을 필요가 없음. 즉, 그림을 넣으면 반드시 그림에 대한 설명을 해 주어야 함.

그림 2.

**2.** 연구추진 전략 및 방법을 서술한다.

**3.**

2. 나쁜 재료로 맛있는 음식을 만들기는 어렵다. 연구 내용자체가 좋아야 좋은 글로 이어진다.

3. 군더더기는 최대한 빼라. 전하고자 하는 핵심 내용을 정확히 전달할 수 있도록.

4. 글을 쓸 때는 문장과 문장이 논리적으로 잘 연결되는지 확인하면서 글을 쓴다. 의미없는 나열식의 문장은 최대한 자제하라.

5. 이 글을 읽는 사람은 “이 내용을 모르는 사람”이다. 상대가 모른다고 생각하고 설명해라. 용어를 설명해야 할 필요가 있다면 각주를 활용하는 것도 방법이다.

6. 결론을 낼 수 없다면, 질문을 던지는 것도 방법이 될 수 있다. 그것이 설득력있고, 상대를 자극할 수 있는 질문이라면.

7. 글의 목적을 분명히하라. 설득인가? 설명인가? 자랑인가? 감동인가?

8. intro에 다양한 문헌을 설명과 함께 인용하면 깊이 있어 보인다. 많이 조사하고 많이 인용하라. (그렇다고 관계없는 것까지 인용할 필요는 없다)

9. 한 문장에는 한 가지 내용만 전달하는 것이 좋다. 문장이 길어지면 읽는 사람도 집중력을 잃어버린다.

10. 문장이 다른 뜻으로 읽히지 않는지 항상 검토해보라. 모호한 표현은 자제하라.

11. 정말 중요하다고 생각되는 부분은 **bold로 쓰거나**, *기울여쓰거나* 밑줄을 그어주어도 좋다. 읽는 사람이 관심을 가질 수 있도록.

12. 전체 보고서 내용의 핵심을 단 한문장으로 나타낼 수 있는가? 그 한문장을 설명하기 위해 논리적으로 구성되어 있는가? 고민하면서 작성한다.