

양자 키 분배 프로토콜 BB84 와 B92 에서 도청률과 기저의 수에 따른 error rate 비교

이선아, 문봉교
동국대학교 컴퓨터공학과
cosmos1526@dgu.edu, bkmoon@dgu.edu

Comparisons of error rate according to eavesdropping rate and basis number in quantum key distribution protocols BB84 and B92

Sun-Ah Lee, Bong-Kyo Moon
Dept. of Computer Science Engineering, Dongguk University

요 약

양자 암호통신에서는 키를 실시간으로 안전하게 분배하는 양자 키 분배방식이 핵심이다. 본 논문에서는 양자 키 분배 방식인 BB84 protocol 과 B92 protocol 을 python 으로 구현(이를 Lee' s code 라 명명)한다. 기존에 존재하는 양자 simulator 와 LEE' s code 를 이용해 error rate 의 차이를 두 가지 관점(기저에 따른 차이, 도청률에 따른 차이)에서 비교한다. 이를 바탕으로 어떤 protocol 이 도청자로부터 더 취약한지 알아본 결과, B92 protocol 의 QBER 이 항상 높으므로 도청자를 잡아내기는 쉽지만, 기저가 두 가지 밖에 없으므로 도청자의 공격에는 취약함을 알 수 있다.

1. 서론

일반적으로 사용되는 암호화 방법에는 비밀키 암호화(대칭 키 암호화)와 공개키 암호화 (비대칭 키 암호화)가 있다. 비밀키 암호화에서는 하나의 키를 둘이서 나눠가져 암호화, 복호화 할 때 같은 키가 사용되는데 이를 대칭 키 암호화라고도 한다. 하지만 비밀키 암호화는 키로 암호화 한 뒤 키 전달과정에서 누군가가 키를 획득한다면 쉽게 복호화해서 정보를 탈취할 수 있다. 이를 보완하기 위한 것이 공개키 암호화이다. 공개키 암호화는 암호화와 복호화 할 때 사용되는 키가 서로 달라 비 대칭 키 암호화라고도 한다. 공개키 암호화 알고리즘의 대표적인 예로는 RSA 가 있다. RSA 는 소인수분해를 사용하는데 두 개의 큰 소수의 곱과 추가연산을 통해 하나는 공개키로 다른 하나는 개인키로 만든다.

하지만 양자컴퓨터를 이용한 소인수분해 알고리즘이 개발되면서 매우 큰 숫자도 소인수분해가 가능해져 도청자가 키를 탈취할 수가 있게 되었다. 이를 해결하기 위해 양자 암호통신이 등장하였다. 양자 암호통신에서 양자 키 분배는 비밀 키 방식을 사용한다. 비밀 키를 만들기 위한 과정이 양자 상태에서 이루어진다.

본 논문에서는 양자 키 분배 방식인 BB84 와 B92 protocol 을 구현하고 두 가지 관점에서 QBER (Quantum Bit Error Rate)를 비교한다.

2. 양자 암호 프로토콜

가. 양자의 3가지 특성

양자암호는 중첩, 얽힘, 불확정성의 양자의 3 가지 특성을 이용한다. 중첩은 양자가 두 가지 성질을 동시에 가질 수 있음을 의미한다. 따라서 측정하기 전까지는 정확한 양자 상태를 알 수 없다. 하지만 한번 측정하면 하나의 성질만 갖게 되기 때문에 복제가 불가능하다. 얽힘은 하나의 근원에서 발생된 두 양자가 서로 관계를 갖고 있음을 의미한다. 한쪽을 측정하는 순간 그 양자의 상태가 정해지고, 나머지 양자도 상태가 정해진다. 불확정성은 양자의 위치와 속도라는 서로 다른 물리량을 동시에 정확하게 측정할 수 없음을 의미한다. 따라서 양자의 상태를 정확하게 복제하는 것이 불가능하다. 양자암호는 이 3 가지 특성으로 키 분배의 안정성을 보장할 수 있다.

나. 양자 암호 프로토콜 소개

(1) BB84 protocol

BB84 protocol 은 Charles Bennet 과 Gilles Brassard 가 1984 년에 제안한 프로토콜로 최초의 양자 키 분배 방식이다. 송신자(Alice)와 수신자(Bob)사이에서 One - Time Password (일회성 암호)를 생성한다. bit 는 0 과 1 을 사용하고, basis (편광필터)로는 수직수평기저(+)와 대각 기저(x)를 사용한다. 광자에 신호를 실어서 보내는 양자채널과 고전채널인 퍼블릭 채널을 사용한다.

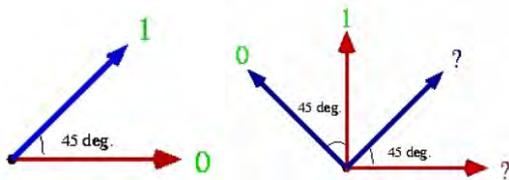
Basis	0	1
+	↑	→
×	↗	↘

[그림 1] bit와 편광 필터에 따른 편광 신호[1]
BB84 protocol 의 과정은 다음과 같다.

- 1) 송신자가 임의의 bit 와 편광필터를 생성한다.
- 2) 필터에 대응되는 편광신호를 생성해 양자채널로 전송한다.
- 3) 수신자는 측정을 위해 편광필터를 bit 의 개수만큼 선택한다.
- 4) 선택한 편광 필터로 값을 측정한다.
- 5) 송신자와 수신자는 퍼블릭 채널로 동일한 필터 사용 여부를 확인한다.
- 6) 다른 필터를 사용한 비트는 제외하고 동일한 필터를 사용한 비트만 저장한다.
- 7) 송신자와 수신자가 저장한 데이터를 비밀키로 사용한다.

(2) B92 protocol

B92 protocol 은 Charles Bennet 이 1992 년에 제안한 프로토콜이다. BB84 protocol 과 비슷하지만 더 사용하기 쉽게 만들어졌다. 송신자와 수신자는 각각 두 개의 비 직교기저를 사용한다.



[그림 2] 비직교 기저의 예시 참고[2]

B92 protocol 의 과정은 다음과 같다

- 1) 송신자가 0° 와 45° 중 하나를 선택한다. 0° 면 bit 0, 45° 면 bit 1을 선택한다.
- 2) 수신자가 90° 와 135° 중 하나를 선택한다. 90° 면 bit 1, 135° 면 bit 0을 선택한다.
- 3) 송신자와 수신자가 선택한 기저의 차이가 45° 가 아니면 100%의 확률로 통과하지 못하고, 45° 이면 50%의 확률로 통과하지 못한다.

4) 통과된 비트는 비밀키로 사용한다.

3. 연구 목적 및 제안 모델

본 논문에서는 파이썬 코드를 이용하여 양자 키 분배 방식인 BB84 protocol 과 B92 protocol 을 직접 구현(이를 LEE' s code 로 명명) 한다. 기존에 존재하는 양자 simulator 와 LEE' s code 를 이용해 error rate 의 차이를 두 가지 관점에서 비교한다.

우선, BB84 와 B92 는 기저의 개수에 차이가 있으므로 기존에 존재하는 양자 simulator 에 동일한 시뮬레이션을 수행한 후 기저에 따른 error rate 를 각각 비교한다. 다음으로 [2]의 결과(도청률에 따른 QBER)를 바탕으로 도청률에 따른 error rate 를 각각 비교한다. 이를 바탕으로 어떤 protocol 이 도청자로부터 더 취약한지 확인하는 것이 본 연구의 목적이다.

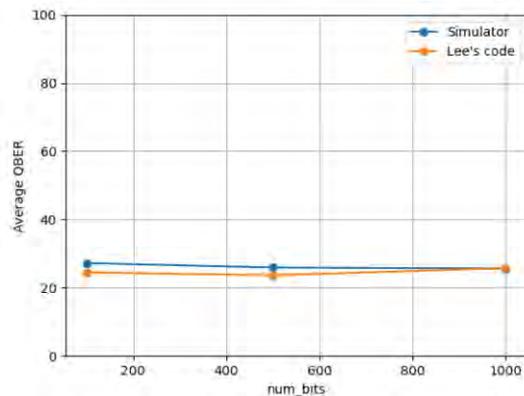
가. 실험방법

첫 번째로 기저가 QBER 에 어떤 영향을 미치는지 알기 위해 BB84 protocol 과 B92 protocol 의 QBER 을 각각 비교한다. 이 때 QBER 은 (오류가 생긴 bit 수)/(검사한 bit 수)로 한다[3]. 이 때 송신자가 생성한 총 bit 의 개수를 100 개 500 개 1000 개로 늘려가면서 QBER 을 체크한다. 각 경우를 10 번씩 반복해 평균을 구한다. bit 의 개수에 따른 평균 QBER 을 산점도 형태로 나타내기 위해 python 의 pandas, matplotlib 를 사용했다. 또한 simulator 와의 비교를 위해 [4],[5] 두 개의 simulator 를 사용했다.

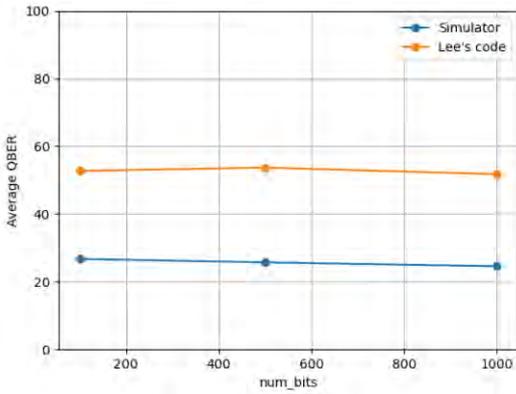
두 번째로 도청률을 다르게 설정하여 error rate 를 비교하기 위해 [2]의 결과와 Lee' s code 를 비교했다. 이 때 도청률은 0%~100%까지 골고루 설정했다.

4. 결과 및 분석

가. 기저에 따른 QBER 차이



[그림 3] Simulator 와 Lee' s code 의 BB84protocol QBER 비교



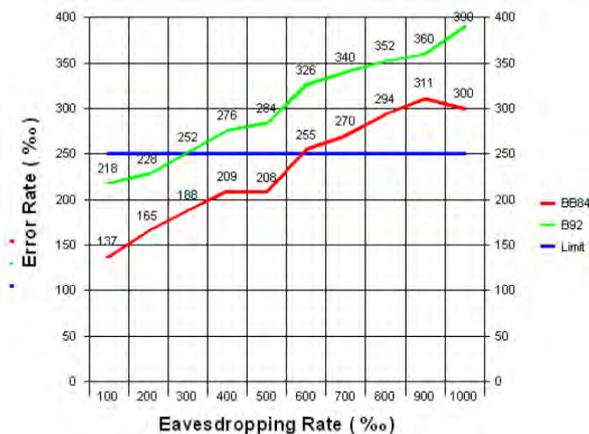
[그림 4] Simulator 와 Lee' s code 의 B92protocol QBER 비교

먼저 기저에 따른 차이를 보자. BB84 protocol[그림 3]에서는 Lee' s code 와 simulator 의 평균 QBER 이 거의 일치했다. 하지만 B92 protocol [그림 4]에서는 Lee' s code 의 평균 QBER 이 훨씬 높게 나왔다.

BB84 protocol 은 서로 직교하는 수직수평기저와 대각기저를 사용하고, B92 protocol 은 두 개의 비직교 기저를 사용한다. BB84 에서 도청자가 기저를 예측 할 때, 송신자와 다른 기저를 예측해(1/2) 신호가 바뀌는 경우(1/2) 중간에 신호가 손상이 될 확률은 1/4 이 된다. 하지만 B92 protocol 에서는 송신자와 도청자가 선택한 기저의 차이가 45° 일 확률이 1/2 이고 그 때 통과하지 못할 확률이 1/2 이므로 이 때의 확률은 1/4 이고, 기저의 차이가 45° 가 아닐 확률이 1/2 이고 그 때는 100% 통과하지 못하기 때문에 이 경우의 확률은 1/2 이어서 총 확률은 3/4 이 된다. 따라서 B92 protocol 의 평균 QBER 이 훨씬 높게 나온 것이라고 예측된다.

나. 도청률에 따른 QBER 차이

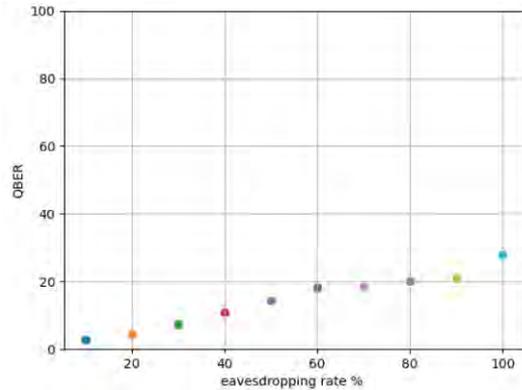
(1) [2]의 결과



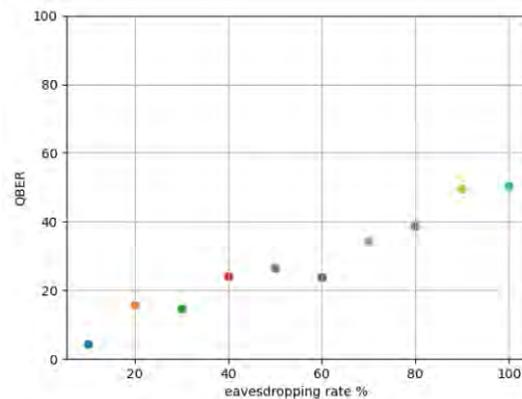
[그림 5] 도청률에 따른 QBER 차이 참고[2]

첫 번째로 [그림 5]의 도청률에 따른 QBER 의 차이를 보자. 도청률은 도청자가 전체 비트의 개수 중에 몇 %를 도청한 것인지 나타낸 비율이다. 따라서 도청률이 올라갈수록 도청자가 많이 간섭했다는 의미이므로 도청률이 증가할 수록 error rate 도 증가하는 것을 볼 수 있다. 또한 앞서 말한 기저에 따른 QBER 차이에서와 마찬가지로 BB84 protocol 보다 B92 protocol 의 error rate 가 항상 높게 나왔다.

(2) LEE's code



[그림 6] BB84protocol 에서 도청률에 따른 QBER 차이



[그림 7] B92protocol 에서 도청률에 따른 QBER 차이

두 번째로 LEE' s code 의 도청률에 따른 QBER 의 차이를 보자. (1)의 결과처럼 BB84 와 B92 둘 다 도청률이 증가할수록 error rate 가 증가하는 경향이 나타난다. 또한 항상 B92 protocol 의 QBER 이 BB84 protocol 의 QBER 보다 높다는 것도 알 수 있다.

5. 결론

첫 번째로 기저에 따른 QBER 의 차이를 보자. simulator 와 Lee' s code 둘 다 BB84 protocol 의 QBER 은 비슷했지만 B92 protocol 은 Lee' s code 의 결과가 더 높았다. B92 가 두 개의 비 직교기저를 사용하기 때문에 도청자가 올바른 기저를 선택하기 쉽고, bit 를 사용할 수 있는지 알아보기 위해

각도의 차이(45°)를 이용하기 때문에 Lee's code 에서 B92 의 error rate 가 더 높게 나온 것으로 예상된다.

두 번째로 도청률에 따른 QBER 차이를 보면 BB84 와 B92 둘다 도청률이 높아질수록 QBER 은 커진다. 이는 도청자가 간섭할 수록 올바른 bit 를 공유할 확률이 적어지므로 당연한 결과이다. 또한 앞서 말한 기저에 따른 QBER 의 차이의 결과처럼 BB84 보다 B92 의 QBER 이 항상 높게 나왔다.

따라서 B92 protocol 의 QBER 이 항상 높으므로 도청자를 잡아내기 쉬움을 알 수 있다. 하지만 기저가 두 가지 밖에 없으므로 도청자의 공격에는 취약하다.

참고문헌

- [1] Rupesh Kumar Sinha, Dr. Mrinal Mishra, Dr. S.S. Sahu, "Quantum Key Distribution: Simulation of BB84 Protocol in C", Conference Proceeding of 2nd International Conference on Engineering Technology, Science and Management Innovation (ICETSMI-2017) at National Institute of Technical Teachers Training & Research (NITTTR),MHRD, Govt of India, Chandigarh, India, 15th January 2017 ,p72-73
- [2] Ergün GÜMÜŞ, G.Zeynep AYDIN, M.Ali AYDIN, "QUANTUM CRYPTOGRAPHY AND COMPARISON OF QUANTUM KEY DISTRIBUTION PROTOCOLS" ,ISTANBUL UNIVERSITY-Journal of electrical&electronics engineering, 8, 1, p509, 2008
- [3] Logan O. Mailloux, Michael R. Grimaldi, Douglas D. Hodson , Gerald Baumgartner , Colin McLaughlin, "Performance Evaluations of Quantum Key Distribution System Architectures", Copublished by the IEEE Computer and Reliability Societies, p32, January/February 2015
- [4] https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/cryptography-bb84/Quantum_Cryptography.html, University of St Andrews, QuVis
- [5] https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/cryptography-b92/B92_photons.html, University of St Andrews, QuVis