

# 유한 키 환경에서의 Decoy-state QKD에 대한 Advantage Distillation 성능 분석

김범일, 허준\*

\*고려대학교

bik0118@korea.ac.kr, \*junheo@korea.ac.kr

## Performance Analysis of Advantage Distillation in Finite-Key Decoy-State QKD

Kim Bum Il, \*Heo Jun

\*Korea Univ.

### 요약

양자키분배기법(Quantum Key Distribution, QKD)은 양자역학의 특성을 활용하여 송신자와 수신자인 도청자가 있는 상황을 감지하면서 정보이론적으로 안전한 대칭 비밀키를 분배하는 기법이다. 양자키분배기법은 면 전송거리와 높은 secret key rate를 위해 고가의 장비나 특별한 광파이버를 이용하기도 한다. 하지만, Advantage Distillation(AD)이라는 기법을 통해 동일한 장비에서도 더 먼 거리를 전송할 수 있는 후처리 기법이 제시되었고 다양한 활용할 수 있을 것으로 전망된다. 본 논문은 Advantage distillation을 적용한 Decoy QKD 기법에 유한 키 효과를 반영하여 실제 환경에서 어떻게 반영되는지 시뮬레이션을 통해 확인한다.

### I. 서론

양자키분배기법은 양자 통신 기법들 중 가장 실용화되어 있는 기법이다. 양자키분배 기법은 이론상으로는 정보이론적으로 안전하지만 이론을 만족하지 못하는 장비 및 소자들 때문에 이후 다양한 연구들이 진행되어 왔다.

대표적으로 항상 순수한 단일 광자를 출력하는 광원이 존재하지 않으므로 다중 광자 발생에 의한 보안 문제를 극복하기 위해 decoy 기법이 제시되었고 [1] 구성되는 장비들 중 도청자가 외부에서 쉽게 검출결과에 영향을 줄 수 있어 측정장비에 독립적인 기법인 Measurement-Device-Independent QKD가 제안되었다 [2]. 최근에는 많은 기술적인 어려움이 있었던 Device-Independent QKD가 기술적 문제가 해소됨에 따라 구현이 진행되었다 [3].

장비를 통한 QKD 성능 개량에 대한 연구와 동시에 소프트웨어를 이용한 QKD 성능 개선도 연구가 진행되어 왔다. Advantage Distillation은 Alice와 Bob 사이 양방향 통신을 이용해 QKD의 성능을 증가시킨 방법 [4]으로 단일 광자에 대해 제안된 이후 근래에 단일 광자가 아닌 광원에 대해서도 적용이 가능함을 보여 많은 연구가 진행되고 있다 [5].

본 논문에서는 Advantage Distillation을 적용된 decoy QKD에 finite key effect를 반영하여 실작용 환경에 대해 분석을 진행하여 그 효과를 확인한다.

### II. 본론

#### A. Advantage Distillation

AD 기법은 Alice와 Bob 사이 Local Operation and Classical Communication 환경에서 양방향 통신을 통해 전체 sifting 키에서 손해는 발생하지만 error

correction 전에 채널환경에서 발생한 QBER의 크기를 감소시켜 key rates와 전송거리를 증가시킬 수 있다 [4].

전체 전개는 다음과 같이 전개된다. 이때, 키 생성 효율을 증가시키기 위해 Z basis는 키로 사용하고 X basis는 parameter 예측하는데 이용한다.

1. State preparation: Alice는 보내려는 광자에 대한 정해진 확률에 따라 전송하려는 세기, basis, bit 정보 세가지 상태를 결정하여 광자에 부호화한다.
2. Measurement: Bob은 정해진 확률 Basis를 결정하여 측정을 진행하고 이때, 하나의 검출기에서만 검출되면 성공적인 검출로 저장한다.
3. Basis reconciliation: Bob이 성공적인 검출로 표시한 것만 저장한 것만 이용하여 Alice와 Bob이 서로 검증된 고전 채널을 통해 통신하여 서로 사용한 Basis를 맞춰 본다. 이때, 같은 basis인 것만 모아서 집합을 만든다. 이 집합의 크기가 충분해질 때까지 앞 순서를 반복적으로 수행한다.
4. Parameter Estimation: reconciliation과정이 완료되면 Alice와 Bob은 raw key 쌍 ( $Z_A, Z_B$ ) 중 최종 키 생성에 필요한 parameter를 예측한다.
5. Advantage distillation: Alice와 Bob은 raw key 쌍을 가지고 b 크기의 block으로 나누고 Alice는 임의의 bit c를 정한다. ( $c \in \{0,1\}$ ), 그리고 나눠 놓은 block의 각 bit와 XOR 연산을 한다. 그후 결과를 Bob에게 전송한다. Bob은 Alice가 전송해준 비트열과 Bob이 가지고 있는 block에 XOR연산을 진행한다. 그 결과가

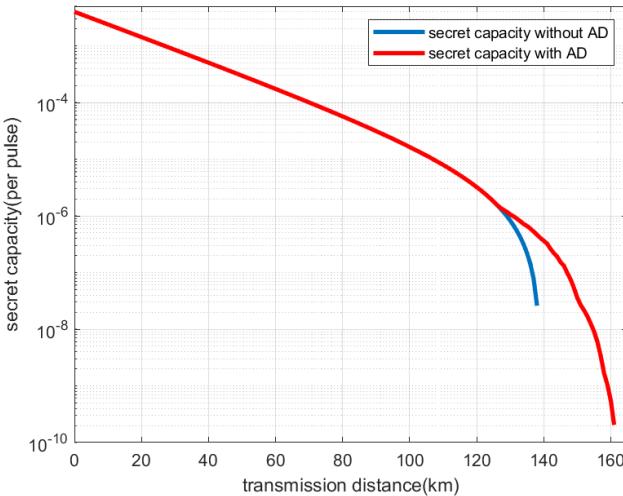


그림 1 전송거리별 pulse 당 비밀 키 생성률

$\{0,0,\dots,0\}$  이나  $\{1,1,\dots,1\}$ 라면 Bob은 Alice에게 “accept”을 보내고 아니라면 “reject”을 전송한다. Alice는 전송된 결과를 보고 “accept”이라면 Alice와 Bob은 block의 첫 비트만 남기고 아니라면 block을 구성하는 bit열을 제거한다.

- postprocessing: Alice 와 Bob은 오류정정을 진행하고 privacy amplification을 통해 노출되는 정보를 제거하여 최종 키를 나눠 갖게 된다.

### B. 유한 키 효과

유한 키 효과는 실제 QKD 가 전송될 때, 무한한 비트열을 전송하지 못한다는 점에서 발생하는 문제점이다. 실제 QKD 환경을 보안성을 확인하기 위해서는 이를 반영하여 분석을 진행하여야 한다. 본 논문에서는 다음의 과정을 통해 유한 키 효과를 분석한다[6].

측정값  $x$ 와 정의한 실패 확률  $\varepsilon$ 을 기준으로 측정값  $x$ 가 발생 가능한 최악의 경우의 예측값  $x^*$ 을 계산한다.

$$\bar{x}^* = x + \beta + \sqrt{2\beta x + \beta^2}, \underline{x}^* = x - \frac{\beta}{2} - \sqrt{2\beta x + \frac{\beta^2}{4}} \quad (1)$$

Where  $\beta = \ln \varepsilon^{-1}$ .

수식 (1)에서 구한 예측값  $x^*$ 을 가지고 보안성을 위해 보수적으로 발생가능한 측정값의 상한 값  $\bar{x}$ 과 하한 값  $\underline{x}$ 은 다음 수식을 통해 연산된다.

$$\bar{x} = x^* + \frac{\beta}{2} + \sqrt{2\beta x^* + \frac{\beta^2}{4}}, \underline{x} = x^* - \sqrt{2\beta x^*} \quad (2)$$

### C. Result

그림 1 은 전송비트열이  $10^{12}$  인 경우의 weak+ vacuum state 를 decoy state 로 이용한 BB84 의 전송거리별 pulse 당 secret key rates 를 계산한 결과이고 그림 2 는 AD 를 적용한 상황에서의 거리별 block 크기  $b$  를 나타낸 것이다.  $b$  가 1 인 경우, AD 의 효과를 볼 수 없으므로 AD 를 적용한 것과 아닌 것의 결과가 동일한 상황이다. 이때, AD 를 적용시 전송거리가 138km 에서 161km 로 증가하는 것을 확인할 수 있다. 또한, 129km 서부터 block 크기의 차이가 1 이 아니어서 AD 를 사용한 효과가 발생하고 이로 인해 발생하여 비밀 키 생성률을 증가된다. 최종적으로 block 의 크기가 4 일 때까지 진행한다.

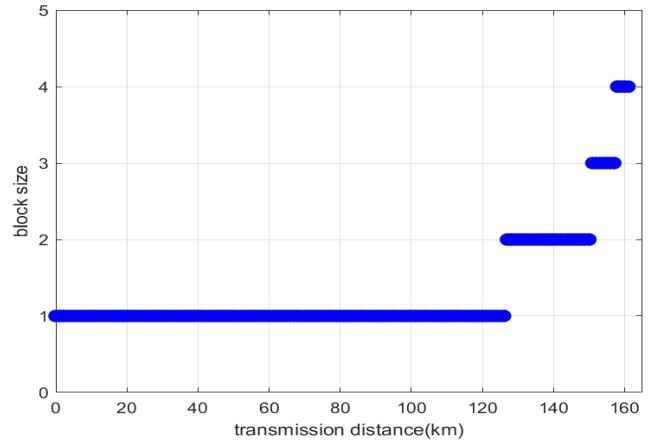


그림 2 전송거리별 block 크기

### III. 결론

본논문에서는 AD 를 적용한 Decoy QKD 기법에 유한 키 효과를 반영하여 실제 환경을 모사한 시뮬레이션 환경에서 키 생성률과 전송거리를 증가를 확인하였다. 주어진 환경에서 기준대비 전송거리가 약 16.7%의 전송거리가 증가되었다.

이를 통해 QKD 를 구현하는 데 필요한 하드웨어비용을 절약하거나 기준의 에러율이 높은 가혹한 통신환경을 극복하는데 많은 이용을 할 수 있을 것으로 예상된다.

### ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단 양자정보과학 인적기반 조성사업의 지원을 받아 수행된 연구임 (Grant No. 2022M3H3A1063074)또한, 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. RS-2023-00242396).

### 참 고 문 헌

- Won-Young Hwang. Quantum key distribution with high loss: toward global secure communication. *Physical Review Letters*, 91(5):057901 (2003)
- Lo Hoi-Kwong, Marcos Curty, and Bing Qi., “Measurement-device-independent quantum key distribution.” *Physical review letters* 108.13(2012)
- Kołodyński, Jan, et al. "Device-independent quantum key distribution with single-photon sources." *Quantum* 4 (2020): 260.
- Renner, Renato. "Security of quantum key distribution." *International Journal of Quantum Information* 6.01 (2008)
- Li, Hong-Wei, et al. "Improving the performance of practical decoy-state quantum key distribution with advantage distillation technology." *Communications Physics* 5.1 (2022): 53.
- Yin, Hua-Lei, et al. "Tight security bounds for decoy-state quantum key distribution." *Scientific Reports* 10.1 (2020): 14312.