Advantage Distillation 기법을 적용한 QKD 비밀 키 용량 분석

김범일, 허준*
*고려대학교

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

Analysis of QKD secret capacity using Advantage distillation

Kim Bum Il, *Heo Jun
*Korea Univ.

요 약

양자키분배기법(Quantum Key Distribution,QKD)는 양자의 물리적 특성을 이용하여 비밀키를 나눠 갖는 기법이다. 양자키분배는 BB84 가 제안된 이래로 많은 연구와 구현이 되어 왔다. 그러나, 먼 거리를 전송하기 위해서는 고가의 장비나 광파이버를 이용해야 되어 높은 비용이 발생한다. 본 논문은 QKD 에 Advantage Distillation 기법을 적용하는 경우 하드웨어의 변화 없이 전송거리가 증가하는 것을 시뮬레이션을 통해 확인하였다.

Ⅰ. 서 론

양자키분배기법은 1984 년 BB84 이후로 다양한 연구와 구현이 진행되어 왔다[1,2,3]. QKD 의 구현에는 비밀키 생성 성능과 보안성이 중요한 요소이다. QKD 구현에는 세가지 부분이 보안성 검토가 필요하다. 광원과 채널의 경우 간단하거나 잘 분석되어 있기 때문에 문제가 되지 않는다. 그러나 측정장치의 경우 복잡하고 도청자가 외부에서 검출결과를 바꿀 수 있어 측정장비에 독립적인 기법인 Measurement-Device-Independent QKD 가 제안되었다[4]. 또한, 양자 리피터가 없는 환경에서 제한되는 전송거리의 한계를 극복하기 위해 TF QKD 기법이 제안되었다[5]. 또는 단일광자를 이용하는 이산변수 양자키분배 기법의 경우 구현 장비의 비용이 높기 때문에 기존의 광통신 장비를 이용하여 양자키분배를 진행하는 연속변수 양자키분배 기법도 제안되어 구현되었다[6]. 양자키분배의 전송거리를 증가시키기 위해 장비에 대한 연구도 많이 진행되었지만, 추가적인 후처리과정을 통해 보다 높은 오류환경에서도 양자키분배가 가능하게 해주는 방법인 Advantage distillation 기법도 제안되었다[7].

본논문에서는 QKD 에 advantage distillation 을 적용하여 secret rate 비교를 통해 advantage distillation 을 이용한 성능 향상을 확인한다.

Ⅱ. 본론

A. Secret Key Capacity

상용적으로 많이 구현되는 BB84 protocol 의 경우, prepare and measure 방식을 통해 구현된다. Pre pare and measure 방식의 BB84 는 얽힘을 이용한 QKD 프로토콜로 환원할 수 있다. 이를 기반으로 BB84 에서의 secret key capacity 는 얽힘쌍을 나눠 갖는 상황에서 도청자가 Pauli attack 을 하는 상황을 반영하면 다음과 같이 최종키는 구성된다.

$$R = \min H(X|E) - H(X|Y)$$

$$\begin{aligned} H(X|E) &= H(X,E) - H(E) \\ &= 1 - (\lambda_0+\lambda_1)h\left(\frac{\lambda_0}{\lambda_0+\lambda_1}\right) \\ &\quad - (\lambda_2+\lambda_3)h\left(\frac{\lambda_2}{\lambda_2+\lambda_3}\right) \end{aligned}$$

$$H(X|Y) = H(X,Y) - H(Y) = h(\lambda_0+\lambda_1) \quad (1)$$

수식 (1)에 (2), (3)을 대입하면 최종수식은 다음과 같이 결정된다.

$$\begin{aligned} R \geq\ & 1 - (\lambda_0+\lambda_1)h\left(\frac{\lambda_0}{\lambda_0+\lambda_1}\right) \\ & -(\lambda_2+\lambda_3)h\left(\frac{\lambda_2}{\lambda_2+\lambda_3}\right) - h(\lambda_0+\lambda_1) \end{aligned} \quad (2)$$

B. Advantage distillation

Advantage distillation 기법은 Alice 와 Bob 사이 양방향 통신을 통해 약한 상관관계를 갖는 비트쌍에서 강한 상관관계를 갖는 비트쌍을 추출하는 방법이다. 이 과정을 통해 기존 보다 더 먼거리에 전송이 가능하게 해준다. Advantage distillation 기법은 다음과 같이 구성된다.

1) QKD 과정에서 basis sifiting 과정을 종료한 후 송신자인 Alice 는 sifted key sequence 를 b 크기의 블록으로 나눈다.
2) 임의의 bit $c \in \{0,1\}$를 결정하여 비트열 C 를 구한다.

$$C = \{c_1, c_2, \dots, c_b\} = \{x_1 \oplus c, x_2 \oplus c, \dots, x_b \oplus c\}$$

3) 비트열 C 를 Bob 에게 전송한다.

4) 수신자인 Bob 은 sifted key sequence 를 b 크기의 블록으로 나누어 전송받은 C 와 비트연산을 진행한다.

$$C' = C \oplus Y_B$$

C' 의 결과가 모두 $\{0,0,\dots,0\}$ 이거나 $\{1,1,\dots,1\}$이면 남기고 Alice 에게 accept 신호를 보내고 첫번째 비트만 남기고 아니면 블록안에 있는 비트를 파기하고 reject 를 보낸다.

5) Alice 는 답장을 보고 accept 이면 첫번째 비트만 남기고 아니면 블록 전체를 파기한다.

이 과정에서 Advantage distillation 을 통과하는 경우는 block 내 Bob 의 비트값이 Alice 와 모두 같거나 Alice 와 모두 반전되어 있는 경우이다. 이에 대한 확률은 다음과 같이 계산된다.

$$p_{succ} = E_\mu^b + (1 - E_\mu)^b \qquad (3)$$

이때, Block 안에는 비트 에러와 별개로 위상 에러가 발생한 경우가 남아있다. 따라서, Advantage distillation 이후 위상 에러가 발생하기 위해서는 하나의 블록안에서 위상 에러가 발생한 홀수개의 얽힘 쌍이 있어야 한다. 이를 반영하여 Secret key capacity 는 다음과 같이 결정된다.

$$R = \max_b \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{1}{b} p_{succ} [\{1 - (\tilde{\lambda}_0 + \tilde{\lambda}_1) h\left(\frac{\tilde{\lambda}_0}{\tilde{\lambda}_0 + \tilde{\lambda}_1}\right) - (\tilde{\lambda}_2 + \tilde{\lambda}_3) h\left(\frac{\tilde{\lambda}_2}{\tilde{\lambda}_2 + \tilde{\lambda}_3}\right)\} - h(\lambda_0 + \lambda_1)] \qquad (4)$$

$$\tilde{\lambda_0} = \frac{(\lambda_0 + \lambda_1)^b + (\lambda_0 - \lambda_1)^b}{2p_{succ}}, \tilde{\lambda_1} = \frac{(\lambda_0 + \lambda_1)^b - (\lambda_0 - \lambda_1)^b}{2p_{succ}}$$

$$\tilde{\lambda_2} = \frac{(\lambda_2 + \lambda_3)^b + (\lambda_2 - \lambda_3)^b}{2p_{succ}}, \tilde{\lambda_3} = \frac{(\lambda_2 + \lambda_3)^b - (\lambda_2 - \lambda_3)^b}{2p_{succ}} \qquad (5)$$

C. Result

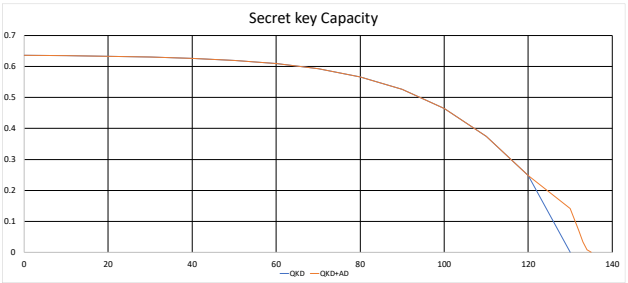

그림 1 AD 기법 적용 결과

μ	e_0	e_{det}	η_D	Y_0	α
0.1	*0.5*	*0.033*	*0.045*	$1.7 * 10^{-6}$	*0.21dB/km*

표 1 QKD 구현 환경 파라미터

그림 1 은 QKD 만의 secret key capacity 인 수식(2)와 Advantage distillation 을 적용한 secret key capacity 인 수식(4)를 거리에 따라 얻어지는 결과를 보인 것이다. Advantage distillation 기법은 근본적으로 전송되는 광자의 검출에 영향을 주는 것이 아니기 때문에 QBER 이 낮은 구간에서는 효과를 보이지 않아 비밀 키 생성률에 변화를 주지 못한다. 거리가 증가하여 QBER 이 증가하면서 QKD 만 이용한 경우에는 120km 가 넘어가면 QBER 이 threshold 에 도달하여 더 이상 비밀키를 생성할 수 없다. 그러나, Advantage distillation 기법을 적용하게 되면 기존에는 전송되지 못했던 135km 까지 비밀키를 전송할 수 있는 것을 확인할 수 있다.

Ⅲ. 결론

본논문에서는 통계적 분석을 반영한 QKD 기법에 Advantage distillation 기법을 이용하여 secret key capacity 를 확인해보았다. 기법을 사용하지 않은 기존 QKD 의 secret key capacity 대비 약 15km 전송거리가 증가하는 것을 확인할 수 있었다. 이를 통해 Advantage distillation 기법은 하드웨어비용을 절약하거나 에러율이 높은 가혹한 통신환경에서 Decoy 기법과 결합하여 QKD 구현에 많은 도움이 될 수 있을 것으로 기대된다.

ACKNOWLEDGMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No. RS-2023-00242396)과 ETRI 부설연구소의 위탁연구과제[2023-117]로 수행한 연구결과입니다.

참 고 문 헌

[1Bennett, C. H. & Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. in Proc. IEEE International Conference on Computers, Systems and Signal Processing. pp. 175-179 (IEEE Press, New York, 1984).

[2] Ekert, A. K. Quantum cryptography based on bell's theorem. Phys. Rev. Lett. 67, 661 (1991)

[3] Koashi, M. Simple security proof of quantum key distribution based on complementarity. N. J. Phys.11, 045018 (2007)

[4] Lo Hoi-Kwong, Marcos Curty, and Bing Qi,, "Measurement-device-independent quantum key distribution." Physical review letters 108.13(2012)

[5] Lucamarini, Marco, et al. "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters." *Nature* 557.7705 (2018)

[6] Grosshans, Frédéric, and Philippe Grangier. "Continuous variable quantum cryptography using coherent states." *Physical review letters* 88.5 (2002)

[7] Renner, Renato. "Security of quantum key distribution." *International Journal of Quantum Information* 6.01 (2008)