편광을 이용한 비용효율적인 4 차원 QSDC 구현 방안

김범일, 허준*
*고려대학교

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

Cost-effective 4Dimensional QSDC Implementation Method Using Polarization

Kim Bum Il, *Heo Jun
*Korea Univ.

요 약

양자직접통신(Quantum Secure Direct Communication, QSDC)은 양자적 특성을 이용하여 비밀키를 사용하지 않아도 보안성을 갖춰 데이터를 전송하는 기법이다. 하지만, QSDC 기법의 전송률은 단일광자검출율에 영향을 받게 된다. 전송률을 높이기 위해 본 논문은 양자직접통신기법중 하나인 DL04-QSDC 를 기반으로 편광을 이용한 4 차원 QSDC 기법의 구현 방법을 제안한다.

Ⅰ. 서 론

QSDC 기법은 비밀키를 이용하여 암호화하는 기존의 고전통신과 달리 물리적 특성을 이용하여 보안성을 갖춰 정보를 전달하는 기법이다. QSDC 는 2002 년 Long 과 Liu 가 개념을 제안한 이래로 다양한 이론적 연구와 실험적 구현이 진행되었다[1-6].

QSDC 는 임의의 비트정보를 전송하여 비밀키를 나눠 갖는 QKD 기법과 달리 정해진 정보를 전달하기 때문에 전송률에 중요하다. 단일광자검출에 이용되는 SPAD 나 SNSPD 의 dead time 에 의해 전송률이 감소된다. 이를 극복하기 위해 한번 전송시에 많은 정보를 보낼 수 있는 High dimensional QSDC 기법이 제안되었다[7]. 2 차원 방식의 경우, 단순한 보강, 상쇄 간섭의 결과를 얻었던 것과 달리 여러 단계의 위상을 이용하기 때문에 여러 번의 간섭을 통해 정보를 얻어야 하고 여러 위상을 측정하기 위해 비교적 많은 검출기가 요구된다. 이는 많은 비용을 야기한다.

본논문에서는 편광을 이용한 4D QKD 구현방안의 아이디어[8]를 통해 QSDC 기법중 하나인 DL04-QSDC 기법을 변형하여 하나의 광자에 2bit 정보를 부호화하는 4dimensional QSDC 기법에 편광을 이용하여 보다 효율적인 구현 방법을 제안한다.

Ⅱ. 본론

A. DL04 QSDC 프로토콜

DL04 QSDC 프로토콜은 Z basis 와 X basis 에 0 과 1 비트를 부호화하여 정보를 전달한다. 프로토콜의 진행방식은 다음과 같이 진행된다.

1) 수신자인 Bob 이 Z, X basis 와 비트를 정하여 광자에 부호화하여 송신자인 Alice 에게 전송한다.
2) Alice 는 전송받은 광자중 도청여부를 파악하기 위해 일부 광자를 측정하고 송수신자간 basis 와 비트 정보를 공유하여 측정 비트 오류율(Detection Bit Error rate, DBER)이 허용가능범위인지 확인하여 채널환경을 파악한다.
3) DBER 이 문제가 없다면 Alice 는 전송하고자 하는 정보에 따라 0 비트를 보내고자 한다면 I operator 를, 1 비트를 보내고자 하면 Y operator 를 취하여 Bob 에게 다시 전송하게 된다.
4) Bob 은 정해진 basis 에 따라 복호화를 진행하고 생성당시 state 와 동일하다면 0, 다르다면 1 로 저장한다. 마지막으로 양자 비트 오류율(Quantum Bit Error Rate, QBER)을 확인하여 도청여부를 확인하고 허용범위 이내인 경우 통신을 종료한다.

B. 4D-DL04 QSDC

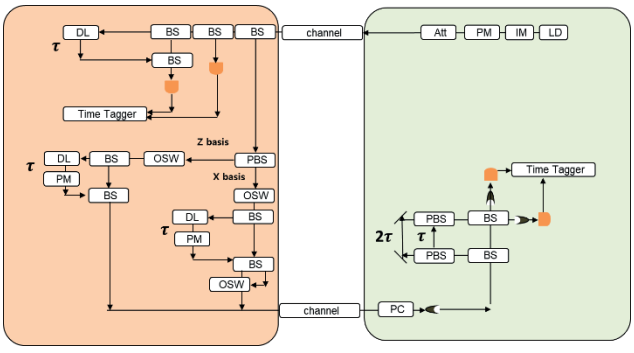

그림 1 제안하는 4D QSDC scheme

그림 1 은 제안하는 4D-DL04 QSDC 구성도를 나타낸다. 기존의 4D-DL04 QSDC 의 구현방식의 경우 위상정보를 다음과 같은 상태로 표현된다.

$$|p_k\rangle = \frac{1}{2}\sum_{j=0}^{3} \exp\left(\frac{2\pi ijk}{4}\right)|t_j\rangle$$

위와 같은 상태에서 위상정보를 얻기 위해서는 3 개의 간섭계와 4 개의 단일광자검출기를 필요로 한다. 제안하는 방식의 경우 편광을 이용하여 basis 정보를 부호화하기 때문에 위상정보는 $0, \pi$ 만 고려하게 되고. 프로토콜 구성은 다음과 같이 구성된다.

1') 수신자인 Bob 이 Z, X basis 와 비트 정보를 정하여 광자 정보를 전송한다. 이때 준비되는 상태는 그림 2 와 같이 준비한다.

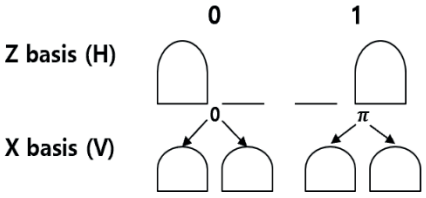

그림 2 각 basis 별 생성 state

2') Alice 는 전송된 광자의 일부를 통해 도청여부 판단하기 위해 측정하고 송수신자간 정보를 공유하여 DBER 이 허용범위인지 확인한다. 구현에서는 광자의 일부를 분리하기 위해 Beam Splitter 를 이용하여 검출한다.

3') DBER 이 허용범위안이라면 Alice 는 전송하고자 하는 정보를 그림 3 과 같이 위상과 시간을 이용하여 부호화하고 Bob 에게 다시 전송하게 된다.

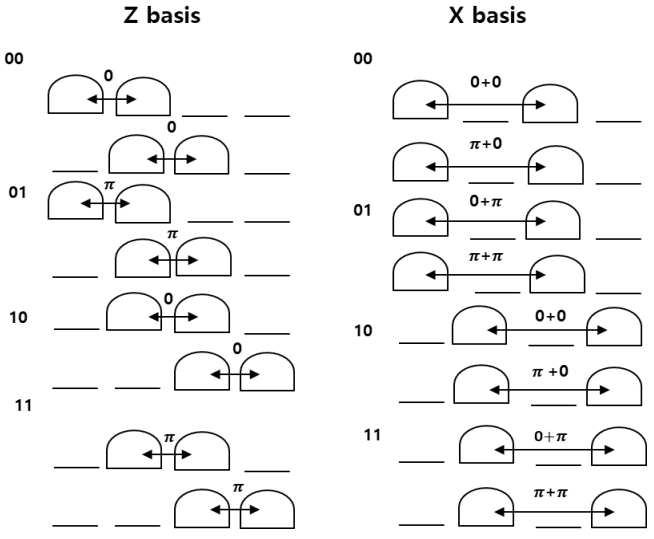

그림 3 Basis 별 Alice 부호화 state

4') Bob 은 Alice 로부터 전송된 광자를 basis 에 맞게 편광을 맞춰 준다. 전송되는 광자의 basis 정보를 가지고 있는 편광이 채널등을 통과하면서 기존과 달라지더라도 Bob 이 basis 를 알고 있기 때문에 이를 바탕으로 전송광자에 basis 를 맞춰준다.

5') Bob 은 검출 시간과 간섭의 결과를 통해 Alice 가 전송한 정보를 저장한다.

Ⅲ. 결론

본 논문은 시간과 위상을 이용한 4 차원 DL04 QSDC 를 구현할 때, 편광을 활용하여 고가의 장비인 단일광자검출기의 개수를 줄여 비용효율적인 구현방안에 대해 제안하였다. 단, 제안한 방식에서는 X basis 전송 상태를 부호화하는데 효율성 낮다는 단점이 있다. QKD 기법중 basis 의 전송비율을 동일하게 하는 것이 이닌 특정 basis 에 편향되어 구성하는 방식이 있다[9]. 추후에는 전송하고자 하는 비트 정보는 Z basis 를 통해 얻고 X basis 는 채널환경을 파악하는 데에만 이용하는 방식으로 성능개선이 이루어질 수 있을 것으로 생각된다.

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

[1] Long, G. L. & Liu, X. S. "Theoretically efficient high-capacity quantum-key-distribution scheme". Phys. Rev. A 65, 032302(2002).

[2] Zhang, W. et al. "Quantum secure direct communication with quantum memory". Phys. Rev. Lett. 118, 220501(2017).

[3] Zhou, Z., Sheng, Y., Niu, P. *et al.* "Measurement-device-independent quantum secure direct communication". *Sci. China Phys. Mech. Astron.* 63, 230362 (2020).

[4] Yu-Bo Sheng, Lan Zhou, Gui-Lu Long, "One-step quantum secure direct communication",Science Bulletin,Volume 67, Issue 4,(2022).

[5] Qi, R., Sun, Z., Lin, Z. *et al.* "Implementation and security analysis of practical quantum secure direct communication". *Light Sci Appl* **8**, 22 (2019).

[6] Liu, X. et al. "Fiber-based quantum secure direct communication without active polarization compensation". Sci. China Phys. Mech. Astron. 65, 120311 (2022).

[7] Ahn, B., Park, J., Lee, J. et al. "High-dimensional single photon based quantum secure direct communication using time and phase mode degrees". Sci Rep 14, 888 (2024).

[8] I. Vagniluca et al., "Efficient Time-Bin Encoding for Practical HighDimensional Quantum Key Distribution," Phys Rev Appl, vol. 14, no. 1, Jul. (2020),

[9] Lo, H.-K, Chau, H.F., Ardehali, M."Efficient quantum key distribution scheme and a proof of its unconditional security".J.Cryptol.18,133(2005).