978-89-294-1160-2

양자암호 네트워크를 위한 양자키분배 프로토콜 기술보고서

2020. 11. 1.

국가슈퍼컴퓨팅본부
과학기술연구망센터
손일권

KiSTi www.kisti.re.kr
한국과학기술정보연구원
Korea Institute of Science and Technology Information

목 차

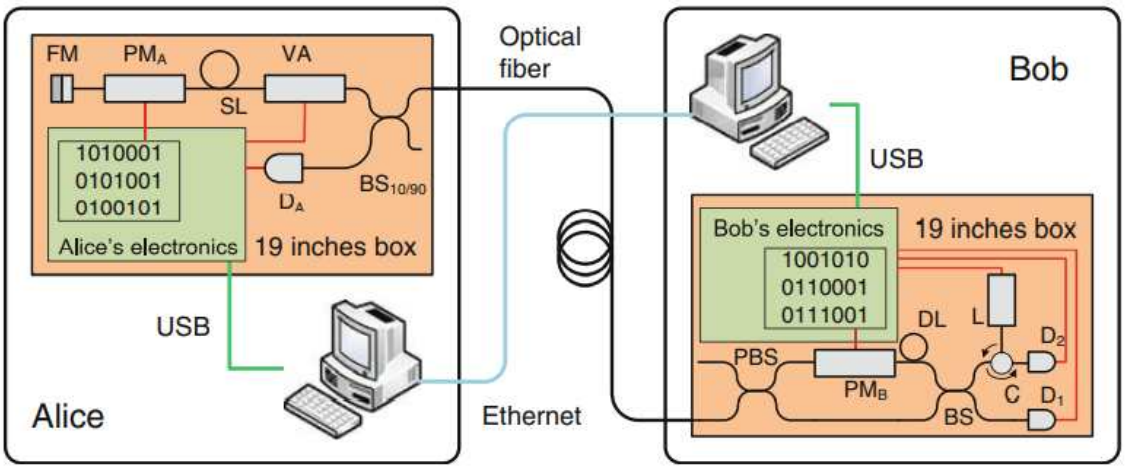
Ⅰ. 양자키 분배 프로토콜 분석

1. Plug&Play 2-Way BB84 프로토콜

가. 프로토콜 개요

- Bennett과 Brassard가 BB84 프로토콜을 도입하고 1992년에 처음으로 BB84 프로토콜이 실험적으로 구현 된 이후로, QKD와 관련된 많은 실험이 수행되었었음. 본 절에서는 Plug&Play system으로 2-way이기 때문에 위상 오류가 자동으로 보정되는 QKD 프로토콜에 대해 설명함. 해당 프로토콜은 약 70km 정도의 전송거리를 가지며, 1550nm 파장대의 신호를 사용함. 큐비트는 두 펄스 사이의 위상차를 통해 인코딩되며, 간섭계를 통해 검출함.

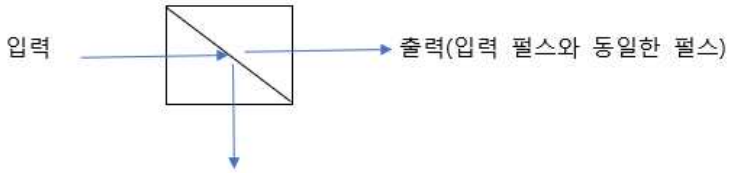
나. 프로토콜 동작



<그림 1.> Plug&Play 2-Way BB84 프로토콜 구성도

- 그림 1.은 Plug&Play 2-Way BB84 프로토콜 구성을 나타냄. ① Bob 쪽에서 방출되는 강한 레이저 펄스(1550nm)는 Beam splitter(BS)에 의해 50/50으로 분할됨 (BS의 역할: 레이저 펄스의 경로를 분리하는 역할을 하는데 이는 경로를 나누어서 뒤의 과정에서 광섬유를 통해 양자 키 분배를 할 때 발생하는 편광의 변화나 경로의 흔들림을 보정하는 소자 사용없이 패러데이 거울을 사용하여 자동 보상하는 과정에서 필요함)
- 분할기의 두 펄스는 각각 짧은 경로와 Phase modulator(PM_B)와 delay line(DL)을 갖는 긴 경로를 거침, Bob 쪽에서 Quantum Channel로 진행 할 때 PM_B는 동작하지 않음 (DL: 짧은 경로를 통과한 펄스와 긴 경로를 통과한 펄스가 동시에 겹치지 않도록 긴 경로를 짧은 경로에 비해 길게 만들어 주기 위해 일반적으로 20m 정도의 DL을 사용함)

- 짧은 경로와 긴경로를 지난 펄스는 Polarized Beam Splitter(PBS)를 통과하여 서로 수직한 편광 성분을 가짐. PBS로 출력된 펄스들은 서로 수직한 편광성분 가지며 경로의 지연으로 인해 시간 상으로 분리되어 있음
  - 두 경로를 통과한 pulse의 편광 변화
    - 짧은 경로를 통과한 pulse가 왼쪽에서 들어오면 통과하는 것은 입력 펄스와 동일한 펄스임



    - 긴 경로를 통과한 pulse가 위쪽에서 들어오면 통과하는 것은 입력 펄스와 수직인 펄스임

- PBS를 지나온 두 개의 펄스는 순서대로 quantum channel을 통과하여 Alice에게 전송되며 0.2dB/km의 채널 loss를 가짐음
- 채널을 통해 들어온 펄스는 Attenuator와 Phase modulator(PM_A)를 통과하는데 이때는 둘 다 아무런 동작을 하지 않음
- PM_A를 통과한 pulse는 Storage line(SL)을 지남
  - Storage line(SL)의 2가지 역할
    - Back scattering은 초반부에서 발생하며, 'backscattering으로 인해 검출기에서 검출되는 신호'와 '검출기에서 측정되는 key 정보'가 섞이는 것을 막아줌
    - PM_A에서 Bob에서 생성한 pulse가 들어오는 것과 Alice에서 FM를 지나서 돌아오는 펄스가 섞이지 않도록 구분하기 위한 역할
    - Back scattering은 레이저에서 발생된 펄스가 각 소자를 지나면서 일부 반사되는 것에 의해 키 정보가 아닌 것이 detector에 의해 측정됨으로써 발생함.
    - 양방향 통신을 할 때 광 펄스가 진행할 때 생기는 Rayleigh backscattering으로 인해 에러가 심각하게 발생하며 이는 양자 암호 통신의 성능을 저하시킴

- 따라서 필요한만큼의 키를 생성한 후 저장해 놓을만큼의 거리가 필요함, 예를 들어 펄스를 1MHz로 생성 ($10^{-6}s$), 유선 광섬유에서 빛의 전송속도 $2\times10^{8}m/s$, 한번에 발생하는 키의 개수가 125개면, 총 $2\times10^{8}\ m/s \times10^{-6}s\times125=25km$, 즉 25km의 Storage line이 필요함.
- 그런데 이때 Storage line은 왕복하면서 걸리므로 실제 길이는 25km의 절반인 12.5km이상이면 됨.

- FM(Faraday Mirror)에서 Bob쪽에서 마지막에 PBS를 통과하면서 나온 펄스의 편광을 입사 편광의 수직한 편광 성분으로 바꿈
- (Faraday Mirror의 역할: 입사 편광을 이와 수직한 편광으로 바꾸어서 Bob쪽으로 펄스가 다시 들어갈 때 짧은 경로로 나온 펄스는 PBS에 의해 긴 경로로 나가도록하고 긴 경로로 나온 펄스는 짧은 경로로 들어가도록 만들어 줌
- 따라서 진행할 때와 반사되어 돌아올 때 편광이 서로 수직이므로 광섬유상에서 광 펄스가 겪는 복굴절이 서로 상쇄되어 안정적인 시스템 구축이 가능함)
- FM에서 반사된 후 SL을 통과한 후 Phase modulator(PM_A)에서 광 펄스들의 위상 코딩을 함.(키 정보를 생성하는 과정)
- 즉, Alice측의 PM_A를 통과하는 두번째 펄스에 위의 그림에서와 같이 4가지 서로 다른 위상을 인가하여 위상 코딩 수행
- 광 신호기의 세기를 Attenuator를 사용하여 단일 광자 수준을 낮춘 후 Quantum channel로 펄스를 내보냄
- PBS에서 양자 채널로 나갈 때의 펄스와 양자 채널에서 PBS로 들어올 때의 펄스의 위상은 FM에 의해 편광이 서로 수직임
- 따라서 Bob에서 채널로 나갈 때 긴 경로와 짧은 경로를 지나는 두 펄스는 채널에서 Bob으로 되돌아올 때는 나갈 때와 다른 경로를 지나게 됨
- Bob에서 돌아오는 첫번째 펄스는 긴 경로를 지나며 PM_B에서 위 그림의 2가지 위상을 인가하여 측정 Basis를 결정함
- BS에서 Bob에서 돌아오는 첫번째 펄스(긴 경로 통과), 두 번째 펄스(짧은 경로)는 서로 중첩됨
- 중첩된 결과에 따라 detection 결과는 detector 1과 2 중 어떤 것에서 측정될지가 결정되며 그 결과는 아래 표와 같음

	0(+basis)	$\pi/2$(×basis)	π(+basis)	$3\pi/2$(×basis)
0(+basis)	SPD1 측정	랜덤 측정	SPD2 측정	랜덤 측정
$\pi/2$(×basis)	랜덤 측정	SPD1 측정	랜덤 측정	SPD3 측정

<표 1.> 위상 별 측정 결과

다. 프로토콜 특징

- 2-way Plug&play 방식은 1-way 방식과 비교하여 transmission rate가 낮다는 단점이 있지만, Bob에서 생성된 광자가 Alice에 전송되었다가 패러데이 거울에 반사되어 같은 경로로 돌아오기 때문에 편광이 보정되는 효과가 있기 때문에 구현이 보다 용이하다는 장점이 있음. 또한, 상대적을 Alice측 장비가 간단한 비대칭적 구조를 가지기 때문에 Alice측의 장비가 운용/관리하기 용이하다는 장점이 있음.

라. 참고문헌

[1] Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Rev. Mod. Phys. 74, 145 (2002) 97, 98, 100, 103, 105, 112

[2] Muller, A., Herzog, T., Huttner, B., Tittel, W., Zbinden, H., Gisin, N.: Appl. Phys. Lett. 70, 793 (1997) 98, 102

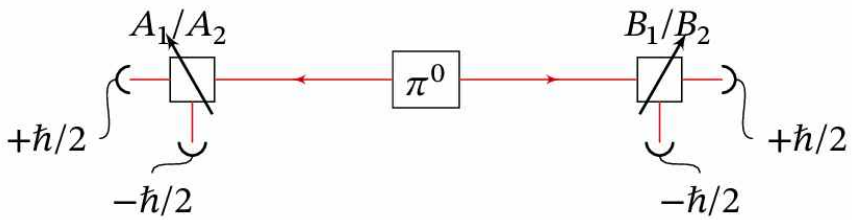
[3] Stucki, D., Gisin, N., Guinnard, O., Ribordy, G., Zbinden, H.: New. J. Phys. 4, 41.1 (2002) 98, 100

2. E91 프로토콜

가. 프로토콜 개요

- Oxford 대학의 Arther Ekert는 1991년도 논문에서 Bell 부등식을 이용하여 이 두-큐빗 프로토콜의 보안성을 입증하는 기초적인 방법을 제안함.
- Bell 부등식은 1864년 J. Bell이 제안한 부등식으로, 양자역학에 의해 예측된 특정 상관관계를 국소성 이론으로는 설명할 수 없다는 것을 증명하는 수단이 된 부등식임.
- 이 프토로콜을 수행하기 위해서는 Alice와 Bob이 세 번째 추가 기저를 사용해야함.
- 세 번째 추가 기저를 사용하면, 그들이 우연히 같은 기저를 선택할 확률은 1/2에서 2/9로 떨어지지만, Bell 부등식을 시험하기에는 충분한 데이터를 확보할 수 있음.
- 이후, 광원이 정말 얽힘 상태를 방출하는지 확인할 수 있음.

나. 프로토콜 동작



<그림 4.> E91 프로토콜 구성도

- Alice로부터 Bob에게 전달되는 큐빗을 운반하는 양자채널을 공통의 광원으로부터 한 큐빗은 Alice에게, 나머지는 Bob에게 전달해 주는 채널로 바꿔줌.
- 광원은 언제나 두 큐빗을 BB84 프로토콜의 4가지 상태 중에서 랜덤하게 골라 항상 같은 상태로 방출해줄 수 있음.
- Alice와 Bob은 그들이 가진 큐빗을 각자 두 기저 중 하나를 무작위적으로 골라서 측정함. 이후, 광원 쪽에서 기저를 발표하고, Alice와 Bob은 서로 같은 기저를 사용했을 때의 데이터만 남겨줌.
- 만약 광원을 신뢰할 수 있다면, 이 프로토콜은 BB84와 수학적으로 동일함이 증명되었음. 마치 큐빗이 Alice로부터 광원 쪽으로 시간 역순으로 전달된 다음에 Bob에게 전달되는 것처럼 보임.
- 하지만 E91 프로토콜에서는 이미 도청자의 손아귀에 있을 수도 있는 광원을 신뢰하기보다, 두 큐빗이 다음과 같은 최대 얽힘 상태로 방출된다고 가정함.

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle)$$

- 이 경우 Alice와 bob이 우연히 같은 기저를 사용했을 경우 그들의 측정결과는 동일함을 알 수 있음.

다. 프로토콜 특징

- E91 프로토콜의 경우 그 자체로는 현재 많이 사용되지 않는 프로토콜임. 그러나 E91 프로토콜로부터 시작된 얽힘 기반의 QKD 프로토콜들이 다수 존재함.
- 편광을 사용하여 얽힘 광자를 만들어낸 무선 장거리 QKD의 144km에서 성공적으로 시연된 바 있음[9].
- 광섬유 기반의 얽힘 광자 기반 QKD의 은행 송금을 처리하기 위해, 오스트리아의 대형 은행의 본사와 비엔나 시청 사이에 QKD 시스템을 설치하여 도시 환경에서 1.45km 유리 섬유를 통해 비밀 키를 성공적으로 배포 가능하다는 것을 입증함[8].
- 광원이 Eve의 통제하에 있거나 Alice와 Bob 사이의 중간에 있는 경우 더 높은 손실을 허용 할 수 있는 얽힘 광자 기반의 QKD 프로토콜에 대한 보안성이 증명된 바있음[10].

라. 참고문헌

[1] Dusek, M., Lutkenhaus, N., Hendrych, M.: Progress in Optics ¨ 49, 381 (2006) 97, 109

[2] Ribordy, G., Brendel, J., Gautier, J., Gisin, N., Zbinden, H.: Phys. Rev. A 63, 012,309 (2000) 110

[3] Pelton, M., Marsden, P., Ljunggren, D., Tenger, M., Karlsson, A., Fragemann, A., Canalias, C., Laurell, F.: Opt. Express 12, 3573 (2004) 110

[4] Konig, F., Mason, E., Wong, F., Albota, M.: Phys. Rev. A 71, 033,805 (2005) 110

[5] Bennett, C., Brassard, G., Mermin, N.: Phys. Rev. Lett. 68, 557 (1992) 110

[6] Marcikic, I., de Riedmatten, H., Tittel, W., Zbinden, H., Legre, M., Gisin, N.: Phys. Rev. Lett. ´93, 180,502 (2004) 111

[7] Takesue, H.: Opt. Express 14, 3453 (2006) 111

[8] Poppe, A., Fedrizzi, A., Ursin, R., Bohm, H., Lorunser, T., Maurhardt,

O., Peev, M., Suda, M., Kurtsiefer, C., Weinfurter, H., Jennewein, T., Zeilinger, A.: Opt. Express 12/16, 3865 (2004) 111

[9] Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., Weier, H., Scheidl, T., Lindenthal, M., Blauensteiner, B., Jennewein, T., Perdigues, J., Trojek, P., Omer, B., Furst, M., Meyenburg, M., Rarity, J., Sodnik, Z., Barbieri, C., Weinfurter, H., Zeilinger, A.: nature physics doi, 10.1038/nphys629 (2007) 111

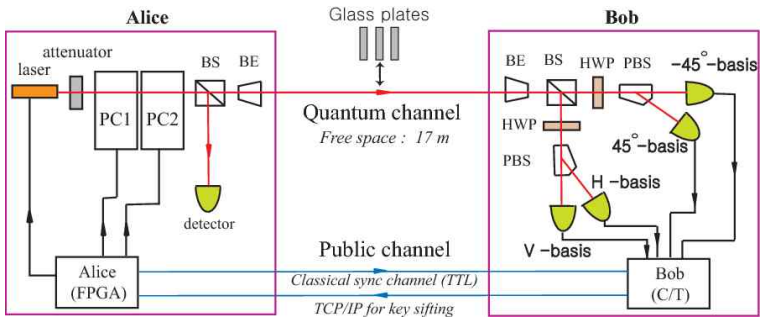
[10] Ma, X., Fung, C.H., Lo, H.K.: Phys. Rev. A 76, 012,307 (2007) 111

3. SARG04 프로토콜

가. 프로토콜 개요

- SARG04는 2004년 Physical Review Letters에 Valerio Scarani, Antonio Acin, Gregoire Ribordy, Nicolas Gisin이 발표한 프로토콜임.
- 해당 프로토콜은 prepare and measure 형태로, BB84 프로토콜이 PNS 공격에 취약하다는 점을 보완하기 위해서 단일 광자 생성원 대신 감쇠 된 레이저 펄스를 사용하였음. PNS 공격은 prepare and measure 프로토콜에서 사용된 기저와 관련된 정보를 탈취하게 되므로, 이 기저정보를 알 수 있는 요소를 삭제해야 보안성을 확보할 수 있다는 아이디어를 기반으로 설계되었음.

나. 프로토콜 동작



<그림 5.> SARG04 프로토콜 구성도

- SARG04 프로토콜의 첫 단계는 BB84 프로토콜과 동일함. Alice는 Z 혹은 X 기저의 4가지 상태중 하나를 무작위적으로 골라서 전송함.
- Bob은 두 기저를 이용하여 해당 펄스들을 측정함.
- Alice와 Bob이 같은 기저를 사용한 비트를 확인하는 두 번째 단계에서 Alice는 기저에 대해 직접적으로 발표하지 않고 서로 수직하지 않은 상태들로 구성된 하나의 세트를 공개함. 이 세트를 구성하는 두 요소 중 하나가 Alice의 비트를 암호화하는 데 쓰이게 됨.
- 복호화의 경우 B92 프로토콜과 유사하며, 예를 들어 Alice가 $|0\rangle$을 보내고 Bob이 그것을 X 기저로 측정했다고 가정 했을 때, Alice는 $\{|0\rangle,|+\rangle\}$이라는 세트를 발표함.
- 만약 Bob의 측정결과가 $|+\rangle$라면, Bob은 Alice의 상태를 확정적으로 유추할 수 없게 됨. 입력 상태가 두 가지 상태($|0\rangle,|+\rangle$) 중 어떤 경우라도 $|+\rangle$라는 측정결과를 도출할 수 있기 때문임. 이런 불확실한 경우의 비트는 제거하여 키 생성 과정에서 배제함.
- 만약 측정결과가 $|-\rangle$로 나타났다면, 입력 상태가 $|0\rangle$인 경우에만 생길 수

있는 측정결과이므로 제거하지 않고 남겨두어 암호키 생성에 사용함.

- 발표한 세트를 구성하는 두 상태가 수직하지 않으므로, 도청자가 PNS 공격으로 암호화된 비트에 대한 완벽한 정보를 알아낼 수 없게 되어 PNS 공격에 대한 내성을 가지게 됨.

다. 프로토콜 특징

- SARG04 프로토콜의 사용 용도는 Weak pulse를 생성하는 Poissonian source를 통해 정보를 인코딩하고 해당 정보들을 불완전한 검출기를 통해 측정하는 경우를 가정하였음. 이는 완벽한 단일 광자 생성원이 아닌 감쇠한 레이저를 사용하는 경우로 이러한 경우에 SARG04의 신뢰할 수 있는 전송거리는 10 km로 현재 사용하기에는 조악한 프로토콜이라 할 수 있음.
- Kiyoshi Tamaki와 Hoi-Kwong Lo에 의해 단일광자, 이중광자 펄스를 사용하는 SARG04 프로토콜에 대해서 보안성을 검증하였음. 단일광자를 사용할 경우 9.68 %, 이중광자 펄스를 사용할 경우 2.71 %의 QBER 값까지는 보안이 보장할 수 있음이 검증됨.
- SARG04는 일관성 없는 PNS 공격에 대해 BB84보다 안전하다는 것이 검증되었음.
- Incoherent 공격에 대해서는 단일광자 생성 $Q \geq 14.9\%$일 때 굉장히 취약하다는 점이 증명되었음.

라. 참고문헌

[1] Valerio Scarani, Antonio Acin, Gregoire Ribordy, and Nicolas Gisin (2004). Physical Review Letters. 92 (5): 057901.

[2] Chi-Hang Fred Fung, Kiyoshi Tamaki, and Hoi-Kwong Lo (2006). Physical Review A. 73 (1): 012337.

[3] Branciard, Cyril; Gisin, Nicolas; Kraus, Barbara; Scarani, Valerio (2005). Physical Review A. 72: 32301.

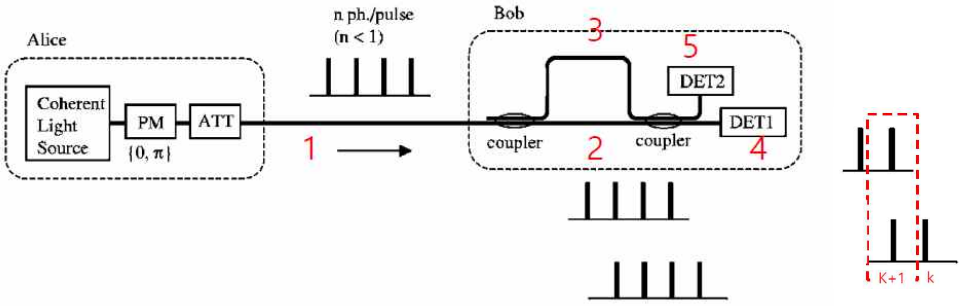
[4] Cyril Branciard, Nicolas Gisin, Barbara Kraus, Valerio Scarani (2005). Physical Review A. 72 (3): 032301.

4. Differetial Phase Shift(DPS)-QKD 프로토콜

가. 프로토콜 개요

- DPS QKD는 BB84 프로토콜과는 다르게 송신자인 Alice만 위상 정보 코딩을 하여 수신자 Bob과 비밀키를 나눠가짐. Alice는 매 전송마다 0 또는 π만큼의 위상을 펄스에 인코딩을 하면 Bob은 자동적으로 보강/상쇄 간섭의 결과로 검출기1, 검출기2 중 한 곳으로 검출 결과를 알 수 있음.

나. 프로토콜 동작



<그림 6.> DPS-QKD 구성도

- 앞서 서술한 내용을 수식으로 표현하면 위의 그림과 같은데 송수신자가 관심이 있는 $k+1$ 시간에 확률적으로 존재하는 상태를 보면 그림 우측의 빨간 상자친 부분에 해당함.

$$e^{i\theta_1}a_1^k \rightarrow coupler\ 1 \rightarrow \frac{1}{\sqrt{2}}e^{i\theta_1}\left(a_2^k + ia_3^{k+1}\right) \rightarrow coupler\ 2 \rightarrow \frac{1}{2}e^{i\theta_1}\left(a_4^k + ia_5^k - a_4^{k+1} + ia_5^{k+1}\right)$$

$$e^{i\theta_2}a_1^{k+1} \rightarrow coupler\ 1 \rightarrow \frac{1}{\sqrt{2}}e^{i\theta_2}\left(a_2^{k+1} + ia_3^{k+2}\right) \rightarrow coupler\ 2 \rightarrow \frac{1}{2}e^{i\theta_2}\left(a_4^{k+1} + ia_5^{k+1} - a_4^{k+2} + ia_5^{k+2}\right)$$

Detector1

$$\frac{1}{2}\left(e^{i\theta_1}a_4^k - e^{i\theta_1}a_4^{k+1} + e^{i\theta_2}a_4^{k+1} - e^{i\theta_2}a_4^{k+2}\right)$$

Detector2

$$\frac{1}{2}i\left(e^{i\theta_1}a_5^k + e^{i\theta_1}a_5^{k+1} + e^{i\theta_2}a_5^{k+1} + e^{i\theta_2}a_5^{k+2}\right)$$

- DPS QKD는 한 번의 전송마다 각각의 위상 정보는 중요하지 않음. 연속적으로 전송되는 펄스의 위상차이(differential phase)를 이용하기 때문에 위상차가 중요함. 위 수식에 있는 θ_1은 k 시간에 전송된 펄스의 위상이며, θ_2는 $k+1$ 시간에 전송된 펄스의 위상임. $\theta_1 = \theta_2$인 경우 $k+1$ 시간에 검출된 경우 검출기1에서는 검출될 확률이 0이며 검출기2에서 검출될 확률은 1임. 반면에 $\theta_1 \neq \theta_2$인 경우 $k+1$ 시간에 검출된 경우 검출기1에서는 검출될 확률이 1이고 검출기2에서 검출될 확률은 0임.
- 위에서 본 것과 같이 Alice가 코딩하는 위상 값의 차이에 따라 Bob은 확정적으로 검출결과를 갖게 되며, 이를 통해 Alice와 Bob은 동일한 비밀키를 확보할 수 있음.

- DPS-QKD 프로토콜의 동작 순서를 정리하면 다음과 같음.

1. Alice와 Bob은 아래 그림과 같이 비밀키를 나눠가질 수 있는데 검출기1에서 검출될 때는 Bob이 0, 검출기2에서 검출될 때는 Bob이 1을 비밀키로 갖는다고 약속함.

DET1에서 검출되면 key bit 0, DET2에서 검출되면 key bit 1

Time index	1	2	3	4
Bob detection	X	O (DET1)	O (DET2)	X
Bob key bit	-	0	1	-
Alice PM	0	π	π	0
Alice key bit	-	0	1	-

→ Bob은 Alice에게 검출의 성공 유무와 검출시점만 공개

→ Bob이 알린 검출시점과 바로 전 시점의 위상 값이 다르면 key bit 0, 같으면 key bit 1

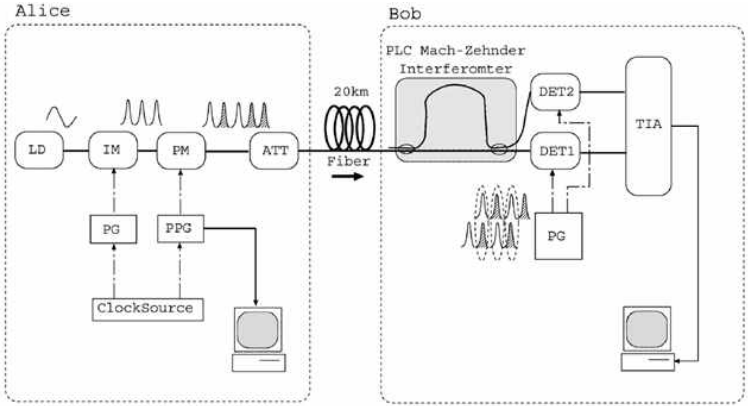
<그림 5.> DPS-QKD 프로토콜 동작 예시

2. Bob은 검출된 신호를 바탕으로 얻은 키의 값을 저장하면서 어느 시간에 검출신호가 발생했는지를 Alice에게 공개함. 예시 그림에서는 time index 2와 3에서 검출신호가 발생했다고 Alice에게 공개를 하였음.
3. Alice는 time index 1,2,3,4에서 어떤 값의 위상을 코딩했는지 알고 있기 때문에 time index 2에서 검출이 되었다는 사실을 통하여 Bob의 검출기1에 신호가 발생했을 것이라고 추측할 수 있고 결과적으로 Alice는 0을 비밀키로 갖음. 마찬가지로 time index 3에서 검출이 된 경우는 Alice가 time index 2,3에서 전송했던 위상정보를 바탕으로 검출기2에서 검출됐을 것으로 추측하고 1을 비밀키로 갖음.
4. 후처리를 통하여 Alice와 Bob은 동일한 비밀키를 확보함.

- DPS QKD는 BB84프로토콜과 다르게 송신자인 Alice만 위상정보를 코딩하고, 수신자인 Bob은 검출된 사실과, 그 검출신호가 발생한 시간 정보만 공개해도 송수신자가 서로 같은 키를 나눠가질 수 있음. BB84 프로토콜과 다르게 송수신자가 사용한 편광판 정보를 비교할 필요가 없기 때문에(Alice만 코딩을 함) 검출된 비밀키 정보는 모두 사용할 수 있는 결과값임. 따라서 BB84프로토콜에 비해 비밀키의 생성 효율이 높은 것을 확인할 수 있음.

- 이러한 DPS-QKD 프로토콜의 실제 실험은 다음과 같이 수행할 수 있음.

• DPS QKD는 서로 다른 연속된 두 개의 pulse의 간섭을 통해 Alice와 Bob이 비밀키를 나눠갖기 때문에 레이저 pulse를 전송하는 빈도가 간섭효과에 큰 영향을 미침. 따라서 Bob이 구성한 간섭계의 경로차이에 해당하는 시간이 Alice가 전송하는 pulse의 빈도가 됨.



<그림 6.> DPS-QKD 실험 배치도

- 예를 들어 Alice가 1GHz 간격으로 레이저 pulse를 생성하여 전송한다면 Bob은 간섭계의 경로차를 $\frac{1}{1GHz} \times 2 \times 10^8 m/s$로 설정하여 20cm의 경로차를 가지게 됨(광케이블에서 빛의 속도를 $2 \times 10^8 m/s$로 가정함.)

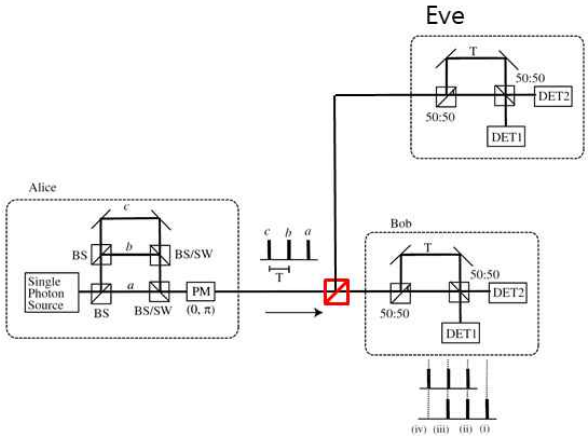
연도	2004 [1]	2007 [2]	2012 [3]
특징	DPS-QKD의 첫 구현	DPS-QKD 구현 표준	최대 전송거리 260km
레이저	1GHz	~10GHz	~10GHz
검출기	APD	SSPD	SSPD

- 위의 표에서 볼 수 있듯이 2004년에 처음 실험적으로 DPS QKD가 구현된 이후로 레이저 pulse의 주기가 빨라지고 detector 효율이 좋아지면서 비밀키 생성속도와 전송거리가 비약적으로 늘어나고 있음.

다. 프로토콜 특징

- DPS QKD의 보안성 이슈들은 다음과 같이 정리 할 수 있음.

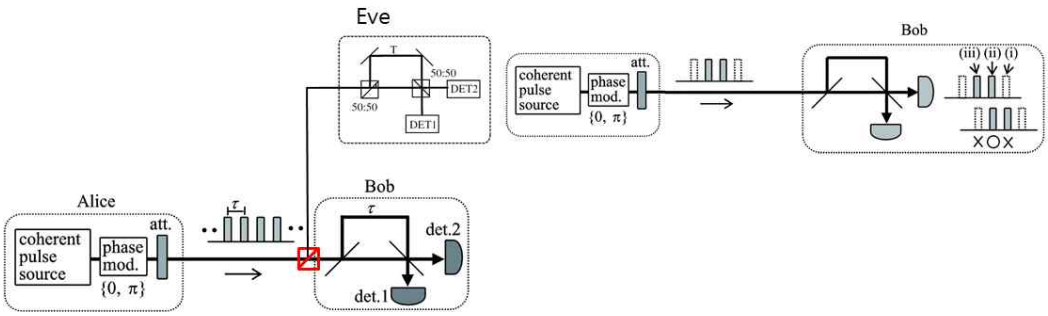
1. Beam splitting 공격



<그림 7.> DPS-QKD의 BS 공격도

- 도청자 Eve는 Alice와 Bob이 연결된 channel 사이에 r:1−r BS를 두어 Alice가 전송한 pulse를 일부 탈취함. (r : original transmission loss, 즉 channel 자체에서 생기는 loss)
- 이 경우 Eve가 정보를 탈취해가도 Alice와 Bob은 어차피 잃었을 정보를 탈취당하기 때문에 알아차릴 수 없음.
- Alice가 매 전송마다 평균 μ 개의 광자가 포함된 laser pulse를 전송하면(small mean photon number μ는 0.1~0.2) Eve는 매 전송마다 $r\mu$ 광자를 탈취할 수 있음.
- Bob이 검출 결과를 공개하는 시점에 Eve는 $2r\mu$개의(현재 시간과 바로 이 전의 시간에 도착한 광자) 광자를 평균적으로 가지고 있지만 이 정도로 매 번 정확한 정보를 얻기는 작은 정도이고, 후처리 과정으로 제거할 수 있음. 따라서 DPS-QKD 프로토콜은 BS 공격에 대해 안전함.

2. Intercept resend 공격



<그림 8.> DPS-QKD IR 공격도

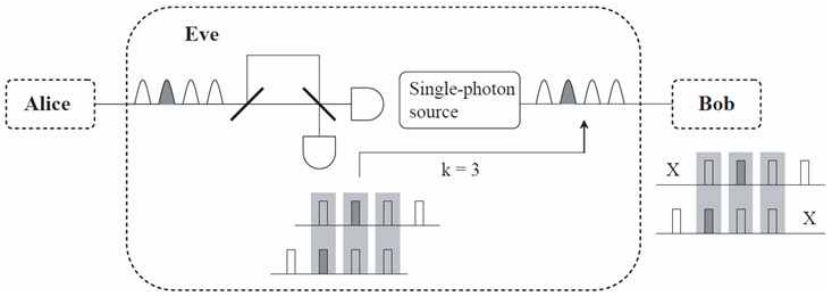
- 도청자 Eve는 Alice와 Bob 사이의 channel에 관여하여 모든 정보를 가져감.
- Bob이 DET1(DET2)에서 검출하는경우 Eve는 Bob에게 진공-π-0-진공(진공-π-π-진공) 혹은 진공-0-π-진공(진공-0-0-진공) 상태를 만들어서 전송함. 진공상태라 함은 해당 시간 레이저를 전송하지 않는 것을 의미하고 그렇게 함으

로 Eve가 보내고자 하는 정보를 온전히 Bob에게 보낼 수 있게함.

- (ii) slot에서 Alice와 Bob은 Eve의 존재를 알 수 없고, (i),(iii) slot에 임의의 검출기에서 검출이 되어 bit error rate은 ½가 됨((ii) slot과 (i),(iii) slot의 차이는 앞,뒤 펄스와의 간섭 유무임).
- (i),(iii) slot이 만들어질 확률이 ½이기 때문에 도청으로 인해 발생하는 bit error rate은 ¼임. (i),(iii) slot이 만들어질 확률이 ½인 이유는 앞의 1장에서 살펴본 수식에서 알 수 있듯이 해당 시간 인덱스에 존재하는 state의 개수와 연관이 있음. 그림 2에서 보면 총 8개의 state 중에 k 시간 state가 2개, $k+1$ state가 2개이기 때문에 (i),(iii) slot이 만들어질 확률이 ½임.
- 정상 상황에 비하여 bit error rate이 크게 높아지므로(0~10%를 보통 정상상황으로 간주함) 송수신자는 도청자의 존재를 감지할 수 있음. 따라서 DPS-QKD 프로토콜은 IR 공격에 대해 안전함을 알 수 있음.

3. Sequential 공격

- Sequential 공격이란 Intercept resend attack과 유사하지만 BER을 낮춘 개선된 공격 방법임.



<그림 9.> DPS-QKD Sequential 공격도

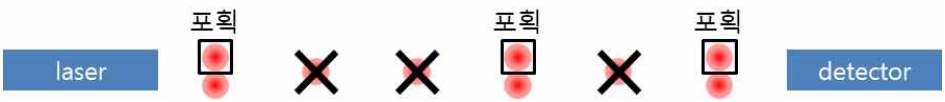
- Eve는 Alice로부터 탈취한 펄스가 연속적으로 검출된 경우 Bob에게 재전송함.
- 중첩이 이뤄지는 time slot 구간을 central, 중첩이 이뤄지지 않는 구간을 side라고 하면, Bob은 ¾ 확률로 central 구간에서 검출하고 ¼ 확률로 side 구간에서 검출함.
- Sequential attack을 수행하는 경우 송수신자가 갖는 BER은 다음과 같음.

$$\frac{3}{4}\times 0+\frac{1}{4}\times\frac{1}{2}=\frac{1}{8}$$

- 일반화 하면 k개의 연속검출 상황에서 BER은 $\frac{1}{2(k+1)}$임.
- 따라서 sequential attack을 수행하는 경우 intercept resend attack의 경우보다 송수신자가 Eve의 존재를 감지하기 더 어려움.
- 하지만 sequential attack을 수행하는 경우 Eve는 연속적인 검출사건을 기다

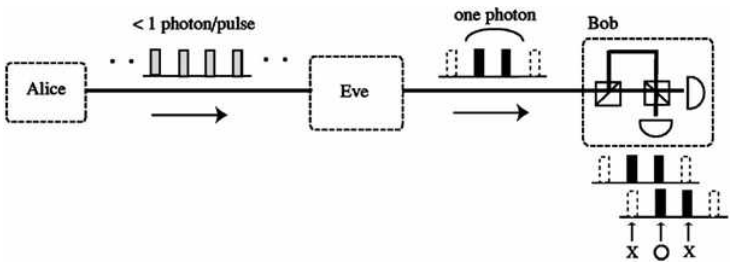
려야 하고 연속검출의 기준을 3개,4개로 늘릴수록 해당사건이 발생할 확률이 줄어드는 문제점이 있기 때문에 비교적 안전함을 알 수 있음.

4. Photon Number Splitting(PNS) 공격



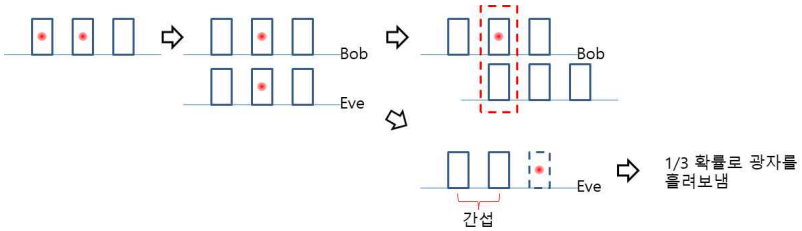
<그림 10.> PNS 공격 예시

- PNS 공격은 Eve가 Alice와 Bob 사이의 channel을 지켜보다가 지켜보는 pulse안에 광자가 2개 이상 포함된 경우 한 개를 탈취하여 보관하고 단일광자가 전송되는 경우는 전송을 모두 막아버리는 공격임.
- 단일광자를 사용하지 않고 weak coherent source를 사용하는 경우 일반적으로 막을 수 없는 공격으로 알려져 있음.



<그림 11.> DPS-QKD 프로토콜 PNS 공격도

- 위 그림은 DPS QKD에서 Eve가 수행하는 PNS attack을 나타낸 그림임. channel을 살피다가 2개의 pulse에서 2개 이상의 광자가 포함된 경우를 기다림. 해당 조건이 아닌 경우 Bob에게 전송되지 못하도록 다 막음.
- 두 개의 pulse에서 두 개 이상의 광자가 포함된 사건이 발생하면 Eve는 1개의 광자가 2개의 pulse에 포함되도록 하여 Bob에게 전송함. 이 경우 앞에서 본 intercept resend attack과 동일한 방법이 되므로 BER이 1/4가 되어 도청사실이 발각됨. 따라서 Eve는 BER을 낮추기 위해서 3개 혹은 그 이상의 sequential pulses에 광자 1개를 넣어서 Bob에게 전송할 수 있음. Eve가 3개의 sequential pulses로 정했다면, 앞에서 본 sequential attack과 마찬가지로 BER은 1/6로 낮아짐.



<그림 12.> Eve가 3개 이상의 sequential pulses에 광자 넣을 경우 예시도

- 하지만 위 그림에서 볼 수 있듯이, Bob이 검출시간을 공개하는 시간에 Eve가 보관하고 있던 pulse에서는 해당시간에 관측을 했을 때 관측되지 않을 확률이 생김. 따라서 필연적으로 잃어버리는 정보가 생기기 때문에 도청을 통해 모든 정보를 알아낼 수 없다는 문제가 발생함.

라. 참고문헌

[1] T. Honjo, K. Inoue, and H. Takahashi, "Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer," Opt. Lett. 29, 2797-2799 (2004)

[2] Takesue, H., Nam, S., Zhang, Q. et al. Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. Nature Photon 1, 343-348

[3] Shuang Wang, Wei Chen, Jun-Fu Guo, Zhen-Qiang Yin, Hong-Wei Li, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," Opt. Lett. 37, 1008-1010 (2012)

[4] IEEE Journal of selected topics in quantum electronics, vol. 21, No. 3, may/june 2015

[5] Diamanti, Eleni. (2006). Security and implementation of differential phase shift quantum key distribution systems.

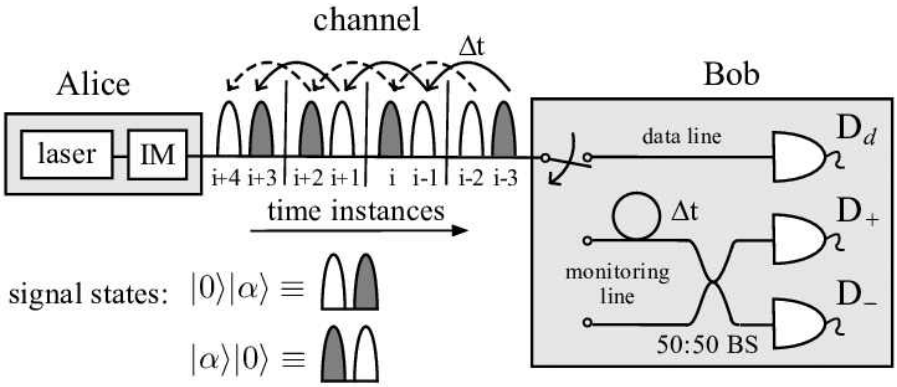
[6] Kyo Inoue and Toshimori Honjo. “Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack”. In:Phys. Rev. A71 (4 Apr. 2005),

5. Coherent One Way(COW)-QKD 프로토콜

가. 프로토콜 개요

- COW-QKD 프로토콜은 제네바 대학의 응용 물리학 그룹(Group of Applied Physics, University of Geneva)에 의해 개발되었음. COW-QKD의 경우 잘 알려진 BB84 프로토콜을 기반으로 개발되었으며, BB84에서 사용하던 서로 직교하는 두 개의 basis X, Y 외에도 Z인 세 번째 basis $\{|10\rangle,|01\rangle\}$를 사용하며, 이는 큐비트로 광자의 도착 시간을 사용하기 때문에 광학 에러에 대해 민감하지 않다는 장점이 있음. Y basis 대신 Z basis를 사용하며, X basis는 coherence를 확인하기 위해서 가끔 사용됨.

나. 프로토콜 동작



<그림 13.> COW-QKD 프로토콜 구성도

- Intensity modulator가 적용된 1550nm 대 Alice측의 CW 레이저는 평균 광자 수가 μ이거나 아예 차단된 형태(vacuum 신호)의 coherent state 신호를 준비함.
- Alice측에서 쏘아보내는 신호는 정보를 coherent state 형태로 인코딩하여 보냄. 해당 프로토콜에서는, 임의의 어떤 연속된 신호 쌍 사이에 coherence를 이용함. 두 연속된 신호로 인코딩 된 K번째 논리 비트 0과 1은 coherent state $|\sqrt{\mu}\rangle$와 $|0\rangle$의 곱으로 이루어져 있음.

$$|0_k\rangle = |\mu\rangle_{2k-1}|\sqrt{0}\rangle_{2k}, \quad |1_k\rangle = |0\rangle_{2k-1}|\sqrt{\mu}\rangle_{2k}$$

- 각 논리적 상태가 서로 직교하지 않는 것을 확인할 수 있음. time-of-arrival 측정은 비트 값에 대해 최적의 명확한 값을 제공함. Coherence를 확인하기 위해 $f \ll 1$인 $|\sqrt{\mu}\rangle_{2k-1}|\sqrt{\mu}\rangle_{2k}$ 형태의 decoy 시퀀스를 생성함. 매우 큰 coherence 길이를 가지는 굉장히 좁은 협대역을 가지는 CW 레이저로 인하여 어떤 임의의 두 non vacuum pulse 사이에서도 잘 정의된 위상이 존재함.
- 동일한 간격의 펄스가 생성되기 때문에 단일 간섭계로 디코이와 $(1-0)$-비트

열의 coherence을 확인할 수 있음.

- Eve는 오류없이 유한한 펄스 내에서 광자 수를 계산할 수 없기 때문에, 광자 수 분할(PNS) 공격을 감지 할 수 있음. 이것은 PNS 공격을 방어할 수 없는 BB84 프로토콜과 대비되는 점임.
- 신호는 transmission t인 양자 채널을 통해 Bob으로 송신되며, $[t_b:(1-t_b)]$인 빔 스플리터에 의해 분할 됨($t_b \lesssim 1$). 10% 정도의 신호만 quantum coherence를 체크하기 위한 Bob의 간섭계로 반사됨. 나머지 90%의 신호는 도착시간을 측정함으로써 raw key를 생성하기 위해 사용됨. 검출기 D_B의 검출율 R은 $R=1-e^{-\mu t t_B \eta} \approx \mu t t_B \eta$임. 이때 η는 광자 카운터의 양자 효율이며 $\mu \approx 0.1$임.
- COW-QKD 프로토콜의 동작 순서를 정리하면 다음과 같음.

  1. Alice는 각각 $\frac{1-f}{2}$ 확률로 많은 수의 논리적 비트 0과 1을 보내며 $f \ll 1$의 확률로 decoy 신호를 보냄.
  2. Bob은 신호를 받은 뒤, 모니터링 라인의 D_{M2}이 동작했을 때의 data line의 검출기인 D_B를 통해 얻은 bit와 공개함.
  3. Alice는 Bob에게 그의 raw key에서 제거해야하는 decoy로 쓰였던 bit를 알려줌.
  4. Alice는 Bob의 검출기 D_{M2} 검출을 분석함. Alice는 visibilities $V_{(1-0)}$와 V_d 통해 coherence의 깨짐을 추정하여 Eve가 획득한 정보량을 계산함. $V_{(1-0)}$와 V_d가 같지 않으면 Alice와 Bob은 도청자가 존재하는 것으로 간주하고 해당 프로세스를 포기함.
  5. Alice와 Bob은 후처리를 통해 최종적으로 암호키를 확보함.

다. 프로토콜 특징

- COW-QKD 프로토콜의 보안성은 아직 검증 중임. QKD 프로토콜의 보안성을 증명하는 표준적인 방법은 심볼을 하나씩 보내는 프로토콜, 예를들어 BB84, B92 등에 대한 방법들이 었음. 그러나 COW 프로토콜은 심볼 단위의 인코딩을 사용하지 않기 때문에 기존의 표준적인 보안성 증명 방법이 바로 적용될 수 없음. 대조적으로 DPS-QKD 등과 마찬가지로 Distributed-Phase-reference 프로토콜로 불리는 COW-QKD 프로토콜은 프로토콜의 보안성을 보장하는데 있어 전체 위상, 명확히는 연속적인 non-vacuum 신호 사이의 coherence에 의존함.
- 이러한 프로토콜 군을 위해서는 보안성 증명을 위해서 다양한 수준의 작업이 필요함. 현재까지 COW-QKD 프로토콜은 Beam-Splitting(BS) 공격, Intercept-Resend(IR) 공격과 같은 일부 공격에 대해 보안성이 검증되었음. 또한, Zero

-Error 공격과 같이 BS 공격을 일반화하는 공격에 대한 보안성도 검증되었음.

라. 참고문헌

[1] Stucki, D., Brunner, N., Gisin, N., Scarani, V., Zbinden, H.: Appl. Phys. Lett. 87, 194,108 (2005) 103, 105

[2] Stucki, D., Barreiro, C., Fasel, S., Gautier, J.D., Gay, O., Gisin, N., Thew, R., Thoma, Y., Trinkler, P., Vannel, F., H., Z.: arXiv:0809.5264 (2008) 103

[3] Gisin, N., Ribordy, G., Zbinden, H., Stucki, D., Brunner, N., Scarani, V.: arXiv:0411022 (2004) 103, 104, 105

[4] Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Rev. Mod. Phys. 74, 145 (2002) 97, 98, 100, 103, 105, 112

[5] Bennett, C., Brassard, G.: Conf. on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York) p. 175 (1984) 98, 100, 103, 112, 115

[6] Lo, H.K., Chau, H., Ardehali, M.: J. Cryptology 18, 133 (2005) 104

[7] Debuisschert, T., Boucher, W.: Phys. Rev. A 70, 1042,306 (2004) 104

[8] Hwang, W.Y.: Phys. Rev. Lett. 91, 057,901 (2003) 101, 103, 104

[9] Wang, X.B.: Phys. Rev. Lett. 94, 230,503 (2005) 100, 101, 104

[10] Lo, H.K., Ma, X., Chen, K.: Phys. Rev. Lett. 94, 230,504 (2005) 100, 101, 104

[11] Branciard, C., Gisin, N., Lutkenhaus, N., Scarani, V.: Quant. Inf. Comput. 7, 639 (2007) 105

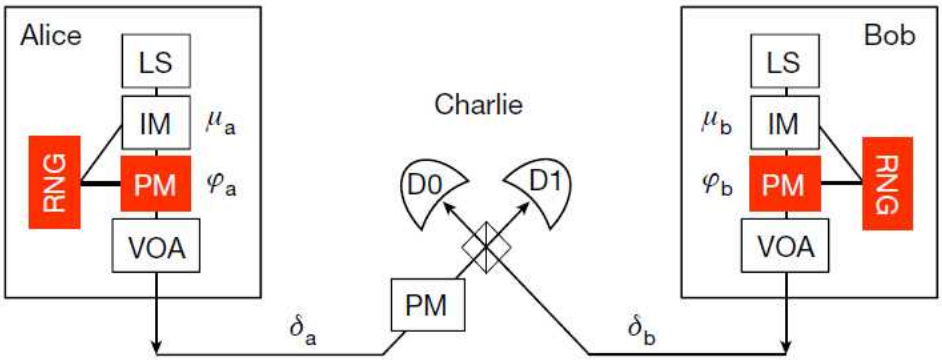
[12] Branciard, C., Gisin, N., Scarani, V.: New. J. Phys. 10, 013,031 (2008) 105

6. Twin field QKD

가. 프로토콜 개요

- 2018년에 새롭게 개발된 QKD 프로토콜이다. Measurement device independent(MDI) QKD 구조와 유사하고 그 특성을 갖고 있기 때문에 MDI QKD와 마찬가지로 측정부가 도청에 영향을 받지 않는 보안성을 지닌다. discrete variable(DV) QKD의 secret key rate와 key의 전송거리는 검출기의 dark count rate에 영향을 크게 받는데 TF QKD는 MDI QKD와 다른 방식으로 검출과정이 진행되기 때문에 검출 효율이 크게 개선된다(MDI QKD ~ η, TF QKD ~ $\sqrt{\eta}$, η는 channel transmittance).

나. 프로토콜 동작



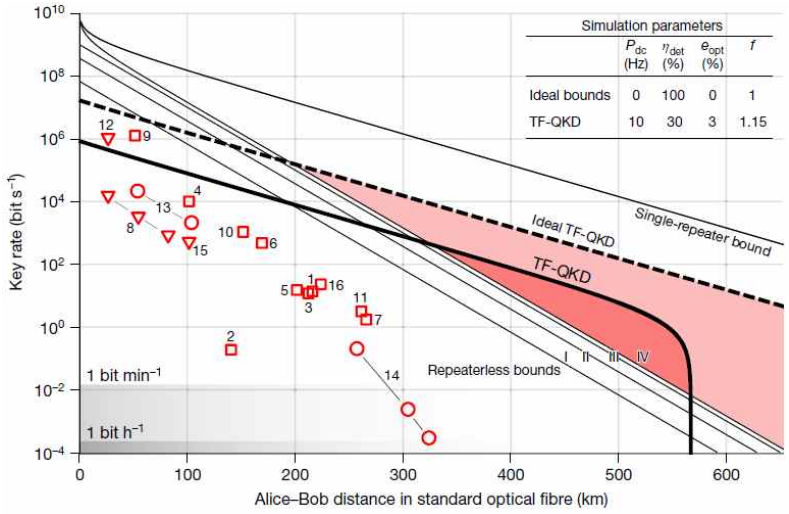
<그림 14.> TF-QKD 프로토콜 구성도

- 프로토콜의 진행과정은 다음과 같다

TF QKD의 진행과정
0. 위상 구간 $[0, 2\pi)$을 $M=16$으로 동등하게 나누는 구간을 준비함. $\Delta_k = 2\pi k/M$, $k=0,\ldots,M-1$
1. classcal stage - Alice와 Bob이 relay station, Charlie에게 강한 광펄스를 전송함. 이를 통하여 채널의 특성을 파악, $\delta_{ba}=\delta_b-\delta_a$로 표현되는 phase misalignment를 최소화
2. Quantum stage - Alice와 Bob은 광펄스를 단일광자 수준으로 감쇄시키고 위상과 세기를 변조함
3. Preparation - Alice와 Bob은 임의의 광펄스 세기를 $\mu_{a,b} \in \{\mu/2, \nu/2, \omega/2\}$ 중에서 고름. bit phase에 해당하는 $\alpha_{a,b} \in \{0,\pi\}$중 하나를 고르고(각각 bit 0, 1) phase에 해당하는 $\beta_{a,b} \in \{0,\pi/2\}$ 중 하나를 고름(각각 bases X, Y). global phase에 해당되는 $\rho_{a,b} \in [0,2\pi)$를 고른다. Alice와 Bob이 선택한 ρ_a, ρ_b가 어떤 slice $\Delta_{k(a)}, \Delta_{k(b)}$에 속하는지 기록함. Alice와 Bob은 광펄스 세기 $\mu_{a,b}$ 위상 $\varphi_{a,b}=(\alpha_{a,b}+\beta_{a,b}+\rho_{a,b})\oplus 2\pi$를 준비하고 Charlie에게 전송함

4. Charlie's measurement and announcement - Charlie는 Alice와 Bob에게서 전송된 펄스들을 간섭시켜서 검출 결과를 기록함. 양자채널을 사용한 전송이 끝나면 송신자들에게 검출결과를 공개함(언제 검출기0, 검출기1이 검출되었는지). Alice와 Bob은 검출사건이 발생하지 않거나 두 검출기에서 동시에 검출된 회차는 삭제함. Alice와 Bob은 새로운 변수 χ를 만들고 검출기0에 검출된 경우 0, 검출기1의 경우 π를 할당함.
5. User's announcement and sifting - Alice는 $\mu_a, \beta_a, \Delta_{a(k)}$를 공개하고 Bob은 같은 세기, 위상, slice를 선택한 회차를 공개함. Alice와 Bob은 서로 다른 parameter를 고른 회차를 삭제하고 남은 회차들의 bit 값을 공개하는데, 이 때 X basis를 고르고 μ 세기를 이용한 회차는 비밀키로 사용하는 경우기 때문에 공개하지 않음.
6. Raw key bit distillation and parameter estimation - X basis를 고르고 μ 세기를 이용한 회차에서 $\chi = \lvert\alpha_b - \alpha_a\rvert$인 관계를 이용하여 Bob은 α_a를 유추할 수 있고 그 값을 통해 해당 회차의 raw key bit 값이 0인지 1인지 판단할 수 있음. 나머지 회차의 결과를 이용하여 decoy-state parameter 추정을 하고 도청자가 존재하는지 유무를 파악하는데 사용함.
7. 오류정정과 privacy amplification 등의 후처리 과정을 통하여 final secret key를 공유한다

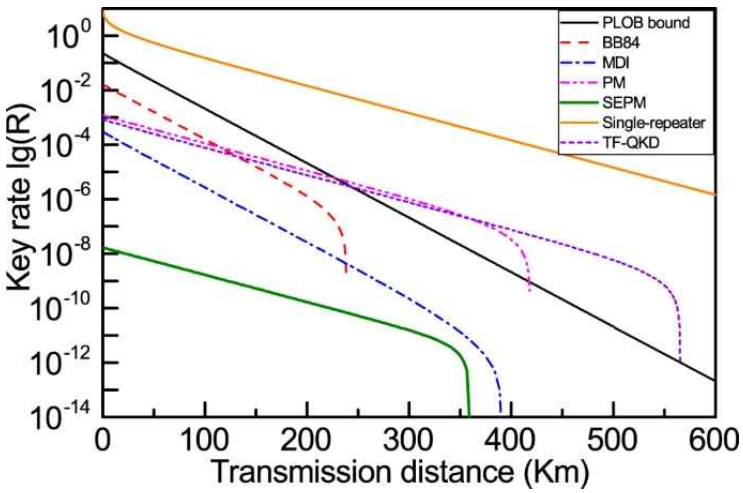
- 1. 과정을 거친 후 channel의 특성을 파악하면 Charlie는 Phase modulator (PM)을 이용하여 양 channel의 phase를 맞춰줌.
- Alice와 Bob은 bit phase와 basis phase를 임의로 고르고 global phase까지 임의로 고르기 때문에 검출사건 이후에 global phase를 공개하지 않으면, 다시 말하여 기준점을 맞추지 않으면 어떤 간섭사건이 생기는지 확신할 수 없기 때문에 global phase를 맞춰주는 과정이 필요함. 그렇기 때문에 phase slice를 나눠서 각 회차가 어떤 slice에 들어가는지를 확인함.
- phase slice를 무한대로 준비하여 나눈다면 완벽히 동일한 기준점을 갖게 되겠지만 그 경우 전체 key rate가 너무 떨어지는 문제가 생김(일치하지 않는 경우 모두 버리기 때문에). 따라서 [1]에서는 $M=16$으로 16 등분을 하여 구간을 준비하였고, 이 경우에 channel에는 오류가 없어도 발생하게 되는 QBER이 생기게 되는데 이를 intrinsic QBER이라고 부르고 $M=16$인 경우 intrinsic QBER은 1.275%임.



<그림 15.> TF-QKD의 전송거리에 따른 key rate

다. 프로토콜 특징

- 그림에서 볼 수 있듯이 TF QKD는 PLOB bound를 넘어서는 전송거리를 보여줌. 앞서 기술했듯이 MDI QKD의 특성을 가지면서 검출기는 1개만 검출사건이 발생할 때 성공적인 검출사건이 되기 때문에 갖는 특성으로 조건에 따라 500km 이상 비밀키를 전송할 수 있는 것으로 알려져있음.
- 보안성은 BB84 프로토콜과 같거나 그 이상임. BB84 프로토콜보다 보안성을 좋다고 얘기할 수 있는 이유는 BB84프로토콜은 검출 정보를 도청당하면 굉장히 큰 위험인데 반하여 TF QKD는 검출결과 자체만으로는 비밀키를 알 수 없기 때문임. 또한, Alice와 Bob이 어떤 값을 보냈는지도 비밀키의 생성에 영향을 미침. 즉, 검출기0에서 검출사건이 발생하는 경우 BB84 프로토콜에서 비밀키는 0 bit인 것에 반해, TF QKD에서는 Alice와 Bob의 bit phase의 차이를 통하여 Alice의 phase를 유추해야만 해당 비밀키가 0인지 1인지 알 수 있음.



<그림 16.> QKD 프로토콜 별 전송 거리 및 key rate

- 비밀키 전송거리가 대략 120km 부근까지는 BB84프로토콜에 비하여 secret

key rate가 떨어짐. phase slice를 맞추는 과정에서 slice가 다른 경우에 전송된 사건은 모두 버려지기 때문에 key rate 손실이 발생함.

- 짧은 전송거리에서 key rate가 떨어지는 단점이 있지만 BB84 프로토콜이 갖지 못하는 검출기에 무관한 안전성을 갖고 있기 때문에 짧은 거리에서도 의미가 있는 프로토콜이다.
- TF QKD가 갖는 단점인 낮은 key rate와 phase slice를 맞추는 복잡함을 개선하기 위하여 phase slice를 맞추는 과정이 없게 동작하게 개선한 sending or not sending(SNS) TF QKD, no-phase-postselected(NPP) TF QKD등이 발표됨.

라. 참고문헌

[1] Lucamarini M, Yuan ZL, Dynes JF, Shields AJ. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. Nature. 2018

[2] Li, W., Wang, L. & Zhao, S. Phase Matching Quantum Key Distribution based on Single-Photon Entanglement. Sci Rep 9, 15466 (2019).

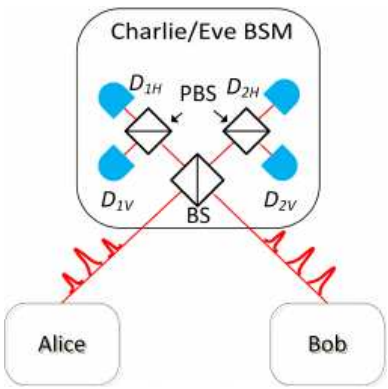
7. Measurement Device Independent(MDI)-QKD 프로토콜

가. 프로토콜 개요

- MDI-QKD의 아이디어는 EPR(얽힘)기반 양자키분배 프로토콜로부터 영감을 받음. 초기 EPR 기반 프로토콜(E91, BBM92)에서 Alice와 Bob은 각각 얽힌 입자쌍을 준비하고 각 광자쌍으로부터 하나의 광자를 중앙에 있는 릴레이인 Charlie에게 전송함. Charlie는 얽힘 교환(entanglement swapping)을 위해 받은 광자쌍에 Bell 상태 측정(BSM)을 수행함. 측정결과는 고전채널을 통해 공표하며, BSM이 완료되면, Alice와 Bob이 자기들이 가진 EPR 광자쌍의 나머지 광자에 대해 X와 Z 측정기저를 랜덤하게 선택하여 측정함. 그들의 측정 결과 중 일부를 비교하면 Alice와 Bob은 Charlie가 신뢰할 만한 인물인지 판단할 수 있게 되고, Alice와 Bob은 BBM92 프로토콜을 이용하여 비밀키를 생성할 수 있음.
- EPR 프로토콜은 시간을 역행해도 똑같이 동작할 수 있음. 즉, Alice와 Bob이 Charlie의 측정결과를 기다리지 않고 그들이 가진 광자에 대해 먼저 측정을 수행하여도 동일한 결과를 얻을 수 있음. 이러한 순서는 기존의 prepare-and-measurement QKD와 같음. Alice와 Bob이 각각 BB84 상태를 준비하고 Charlie에게 보내어 BSM을 수행하는 것을 뜻함. 이후, Alice와 Bob이 가진 키의 일부를 비교함으로써 Charlie의 신뢰성을 판단할 수 있음. Charlie의 BSM은 Alice와 Bob의 비트에 대한 parity를 비교하는 용도로만 사용되므로, 각 비트 값에 대한 그 어떤 정보도 유출하지 않게됨. 이 시간 역순 EPR 프로토콜이 MDI-QKD의 주요 아이디어로 발전하게 됨. 이러한 시간 역순 EPR 프로토콜은 1996년 Biham, Huttner, Mor가 처음으로 제안하였음.

나. 프로토콜 동작

- MDI-QKD 프로토콜의 동작 순서는 다음과 같음.



<그림 17.> MDI-QKD 프로토콜 구성도

1. Alice와 Bob이 4개의 BB84 상태 중에 하나를 각자 무작위적으로 준비함. 이 때 위상이 랜덤하게 조절되는 weak coherent pulse 광원과 decoy signal을 섞어줌. 이 양자상태들을 제3자인 Charlie에게 전송해 줌.
2. (신뢰할 수 있는) Charlie가 BSM을 수행하여 Alice와 Bob의 상태가 서로 간섭하여 Bell 상태가 만들어질 수 있게 함. 예를 들어 Charlie가 50:50 빔분할기(BS)에 입사되는 펄스들을 간섭시킨 후 각 출력부에 있는 편광 빔분할기(PBS)를 통해 각각의 광자를 수평이나 수직 편광으로 투영해줌. 검출기 D_{1H}와 D_{2V}, 혹은 D_{1V}와 D_{2H}에서 광자가 동시에 검출되면 BSM의 결과가 $|\Psi^-\rangle$상태가 된다. D_{1H}와 D_{1V}, 혹은 D_{2H}와 D_{2V}에서 광자가 동시에 검출될 경우에는 BSM의 결과가 $|\Psi^+\rangle$가 되고, 나머지 검출 형태는 BSM이 실패한 것으로 간주함.
3. Charlie는 고전 공개 채널을 이용하여 자신의 BSM이 성공했을 때의 결과를 공표함.
4. Alice와 Bob은 Charlie가 측정에 성공한 시행들에 대한 데이터만 남기고 나머지는 버림. 그 다음 BB84의 sifting 프로토콜과 비슷하게 Alice와 Bob이 그들이 선택한 기저를 발표함.
5. Charlie의 BSM 결과를 기반으로 Alice는 그가 가진 비트의 일부를 뒤집어서 Bob이 가진 비트와 올바른 상관관계를 가지도록 만들어 줌. 최종적으로 decoy-상태 프로토콜을 이용하여 단일광자상태의 이득과 QBER을 추정하여 도청 여부를 확인함.

다. 프로토콜 특징

- MDI-QKD 프로토콜에서 Alice와 Bob은 동시에 송신자이고, BSM을 수행할 제 3자에게 그들이 각자 인코딩한 광자를 전송함. BSM은 추후 얽힘상태를 골라내는 데에만 사용되므로 완벽한 블랙 박스처럼 다룰 수 있음. 따라서 MDI-QKD는 모든 검출기에 대한 부채널들을 제거할 수 있으므로 다른 프로토콜에 비해 높은 보안성을 갖게 됨.
- 2002년에 Inamori가 보안성 검증을 하였으나, 이 연구는 한정된 성능을 보여주었기 때문에 초기 QKD 커뮤니티에서 크게 주목을 받지 못하였음. Biham, Huttner, Mor의 연구의 경우 완벽한 단일광자광원과 저장시간이 긴 양자 메모리를 가정했기 때문에 현재의 기술력으로는 적용하기 어려우며, Inamori의 연구의 경우 실용화된 Weak Coherent Pulse(WCP)를 사용하기는 하지만 decoy 상태를 포함하지 않았음. 결정적으로 두 초기 연구들은 QKD에 존재할 수 있는 부채널 공격에 대해 특별히 고려하지 않아 한계가 있음. 그로부터 10

년 뒤인 2012년에 와서야 Braunsten과 Priandola가 시간 역행 EPR QKD에 대해 일반적인 보안성 검증을 수행하였고 검출기 부채널 공격은 원격전송을 통해 막을 수 있다는 것을 증명하였음.

라. 참고문헌

[1] Phys. Rev. Lett 108, 130503 (2012)

[2] REVIEW OF MODERN PHYSICS, VOLUME 92, APRIL-JUNE 2020

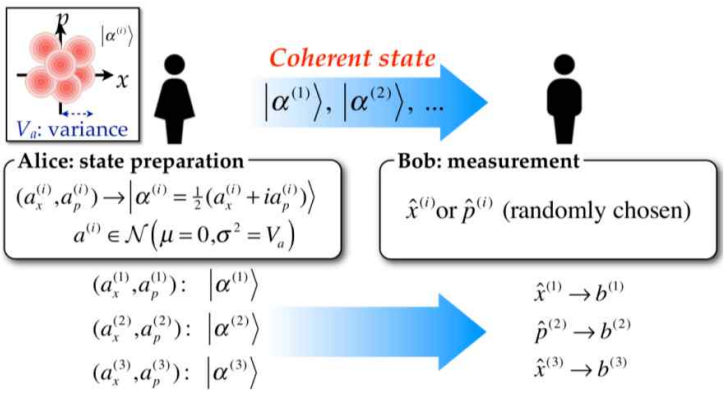
8. Continuous variable QKD

가. 프로토콜 개요

- CV-QKD는 coherent state의 두 quadrature를 모두 사용하는 프로토콜임. 프로토콜에서 사용되는 quadrature들은 position $\hat{x}(=\frac{1}{\sqrt{2}}(\hat{a}^{\dagger}+\hat{a}))$과 moment um $\hat{p}(=\frac{i}{\sqrt{2}}(\hat{a}^{\dagger}-\hat{a}))$임. $\hat{a}$와 $\hat{a}^{\dagger}$는 bosonic annihilation, creation operator이며, coherent state $|\alpha\rangle$의 eigenvalue 방정식 $\hat{a}|\alpha\rangle=\alpha|\alpha\rangle$을 이용함.

나. 프로토콜 동작

- CV-QKD를 위한 양자상태 생성은 레이저의 진폭 및 위상을 변조함으로써 이루어지며, 생성한 양자상태를 광섬유, 대기 또는 인공위성을 이용하여 원거리 전송할 수 있음.

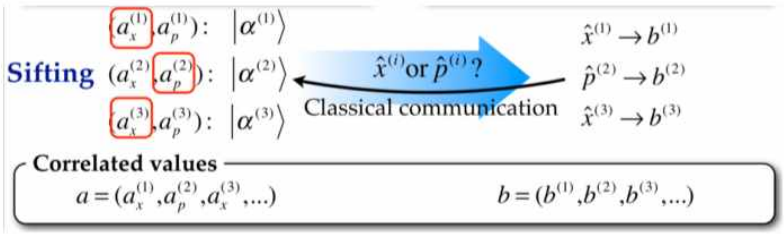


<그림 18.> 연속변수 양자상태 생성 및 측정

- Alice가 임의의 진폭 및 위상을 가진 coherent state를 준비하여 Bob에게 전송함. 이 때 진폭과 위상의 값은 평균이 0, 분산이 V_a인 가우시안 분포를 따르도록 함. 이 과정을 통해 생성한 i번째 coherent state는 다음과 같음.

$$|\alpha^{(i)}\rangle, \alpha^{(i)}=(a_x^{(i)}+ia_p^{(i)})/2$$

- Bob은 Alice로부터 이러한 양자상태를 전송받은 뒤 위치($\hat{x}$) 및 운동량($\hat{p}$)에 대한 양자측정을 임의로 수행하고, 측정한 물리량 정보와 그에 대한 결과 $b^{(i)}$를 기록함.



<그림 19> CV-QKD의 sifting 과정

- CV-QKD에서 key sifting 과정은 Alice가 준비한 진폭과 위상에 대한 정보를 Bob이 측정한 값과 비교하는 과정임. Bob은 고전 통신을 통해 매번 어떤 물리량(x, p)을 측정하였는지에 대한 정보를 Alice에게 전달함. Alice는 이 정보를 바탕으로 x를 측정하였으면 a_x, p를 측정하였으면 a_p 값을 선택함. 이 과정을 통해 Alice와 Bob은 각각 비밀키 $(a_x^{(1)}, a_p^{(2)}, a_x^{(3)}, \cdots)$, $(b^{(1)}, b^{(2)}, b^{(3)}, \cdots)$를 보유하게 되며, 이 둘은 서로 상관관계를 갖게 됨.
- 양자상태 전송 과정에서 생긴 잡음과 Eve가 도청을 한 정도를 예측하는 과정임. Alice와 Bob은 sifted key의 일부를 고전 채널을 통해 공개함으로써 양자상태의 특성을 분석하는 과정을 거침. 이 과정에서 가장 중요하게 분석하는 변수는 채널의 투과율(η)과 과잉잡음(δ)인데, 이 값에 대한 분석을 토대로 키 생성률을 예측하고, 오류정정에 필요한 변수를 결정할 수 있음.
- Alice와 Bob이 가진 key에 존재하는 오류를 보정하는 과정을 거침. 오류보정을 위해 고전통신을 이용하여 정보를 전송하며, 정보전송 방향에 따라 크게 두 가지로 나누어짐. Alice가 Bob에게 오류보정에 필요한 정보를 보내는 과정을 Direct Reconciliation 이라하고 Bob은 이에 따라 자신이 가진 key를 수정함. Direct Reconciliation은 채널의 투과율이 50 % 이하일 경우 Eve가 Bob보다 많은 의 정보를 가지게 되므로 비밀키를 획득하기 어려운 단점이 있음. Reverse Reconciliation은 Bob이 Alice에게 오류보정 정보를 전송하여 Alice의 key를 수정하는 방법임. 이 방법은 채널의 투과율이 50 %보다 낮더라도 Alice가 가진 정보가 Eve보다 크므로 전송거리를 멀리 늘릴 수 있음. 따라서 Reverse reconciliation 이 채택되고 있으며 오류보정을 위해 주로 사용되는 프로토콜은 slice reconciliation, multidimensional reconciliation이 있음. 이때 사용하는 코드 이론은 low-density parity-check (LDPC)와 높은 잡음에서 사용될 수 있는 multi-edge-type LDPC가 대표적임.
- 오류정정이 끝나면 높은 확률로 Alice와 Bob이 동일한 key를 나누어 갖지만 Eve 또한 키와 관련된 소량의 정보를 가지고 있을 수 있음. 이러한 확률을 용인할 수 있는 수준 이하로 낮추기 위하여 추가적으로 Privacy Amplification 과정을 거침. 이를 위해 Alice와 Bob이 나누어 가진 bits를 seed로 하여 rand

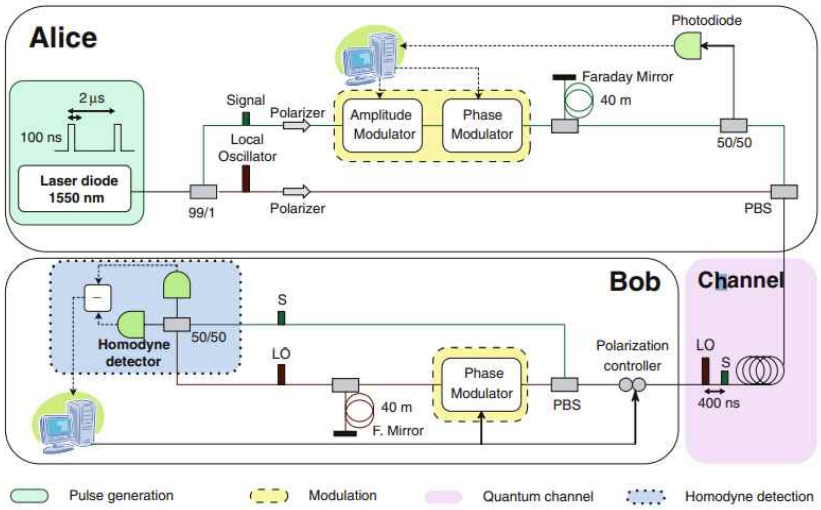
om number를 발생시키는데, 이때 universal hash functions이 사용됨.

- 비밀키 생성률: 위 과정들을 거쳐서 비밀키를 획득할 수 있으며 이때 비밀키 생성률은 다음과 같이 주어짐.

$$K = \beta I(A:B) - S(B:E)$$

- $I(A:B)$는 Alice와 Bob이 가진 mutual information이며, $S(B:E)$는 Holevo information으로 Eve가 가질 수 있는 Bob의 정보 최대량을 의미함. β는 오류 정정 효율을 의미하며 , SNR = 0.002의 큰 잡음이 섞인 신호에서도 β= 95.6 %의 높은 효율을 가질 수 있음이 보고되었음.
- CV-QKD를 단계별로 정리하면 다음과 같음.
  1. Alice는 두 개의 random variable을 뽑는데 이 때, random variable은 gaussian distribution을 따르는 임의의 실수임.
  2. Alice는 앞선 과정에서 얻은 두 개의 실수를 이용하여 phase와 amplitude를 정하여 원하는 모습으로 modulation함.
  3. 양자채널을 통하여 Bob에게 laser pulse를 전송하면 Bob은 두 개의 quadrature (X 또는 P) 중 임의의 하나로 laser를 측정함.
  4. 공개채널을 통하여 Alice에게 어떤 quadrature로 측정하였는지 공개하고 Alice는 사용되지 않은 quadrature의 정보는 버림.
  5. 서로 나눠가진 corelated gaussian random variable을 이진수로 나눠갖기 위하여 sliced reconciliation, multidimensional reconciliation 등의 reconciliation 과정을 거침.
  6. 비밀 키를 나눠갖는 과정에서 생긴 노출 정보는 privacy amplification을 이용하여 삭제함.

- 이러한 CV-QKD 프로토콜의 실제 실험은 다음과 같이 수행할 수 있음.



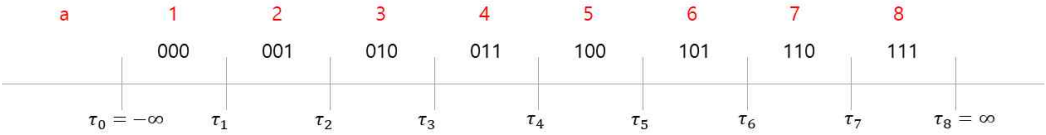
<그림 20.> CV-QKD 프로토콜 구성도

1. 광원: 저잡음, 좁은 선폭을 가진 연속파(CW) 레이저. Koheras ADJUSTIK (NKT photonics) - 선폭<1 kHz, 위상잡음 0.8 rad/Hz/m
2. Isolator: 레이저에서 나온 빛이 한쪽 방향으로만 전파할 수 있도록 해주는 장치. 빛이 되반사되어 광원으로 다시 들어가는 것을 방지할 수 있음.
3. Electro-optic Modulator (EOM): 결맞음 빛의 시간모드를 결정하기 위해 연속파인 빛을 사각 펄스 형태로 변조해줌. EOM에 사각파 형태의 라디오파 전압을 인가하여 1 MHz 주파수의 사각파 형태의 빛을 생성함.
4. 사각파 형태로 변조해준 빛을 편광 빔 분할기(PBS)를 통해 local oscillator (LO)와 signal 빛으로 나누어 주고 진폭 및 위상제어 과정을 거친 뒤 다시 빔 분할기 (BS)로 합쳐서 호모다인 측정을 수행함. 이 과정을 통해 raw key를 얻을 수 있으며, 앞서 설명한 고전정보 후처리 및 오류정정 과정을 통해 비밀키를 생성함.
5. Signal: 빛에 양자정보(x,p)를 기록하기 위하여 진폭 변조와 위상 변조 과정을 거치는데, 설정한 가우시안 분포의 확률변수로부터 랜덤하게 추출된 값을 이용함. 결과적으로 매 시간마다 나오는 펄스의 진폭과 위상이 무작위적으로 변하게 됨. 변조된 빛의 세기를 줄여주기 위해 ND 필터를 사용하여 평균 광자 수 레벨이 수십 개 정도가 될 정도로 조절함.
6. LO: 호모다인 측정을 수행하기 위한 것으로, x, p를 무작위로 바꿔서 측정하기 위해 EOM을 통해 위상을 0 또는 $\frac{\pi}{2}$로 변조해 줌. (여기서 측정데이터의 일부는 위상 드리프트를 모니터링하기 위해 쓰이며, 여기서 측정한 위상 드리프트는 EOM을 통해 보정해줌.)

- CV-QKD 프로토콜의 후처리 과정으로는 다음 두가지 프로토콜이 있음.

1. Slice reconciliation

  - Slice reconciliation은 Alice와 Bob이 서로 correlated gaussian variable을 나눠가진 상태에서 시작함. Alice와 Bob이 실수 구간을 정해진 개수로 나누는데 구간을 나누는 방법은 서로 약속이 되어있음. 편의를 위해 8개의 구간으로 나눈다고 가정함.



<그림 21.> Slice reconciliation 구간 분할 예시

  - Bob이 얻은 실수 값이 a3 구간 ($\tau_2 \sim \tau_3$)에 측정되었을 때 그 값이 Alice가 어떤 값을 보냈을 때 a3 구간으로 측정되었는지를 계산함.
  - Alice가 전송한 실수 값이 다음과 같이 4개의 실수 값을 보냈고 그 값이 그림과 같은 이진수로 할당된 상황을 가정함. k는 비밀키 행을 의미하고 각각의 비밀키를 쌓아서 오른쪽 bit부터 c1열~ c3열까지 나타냄.

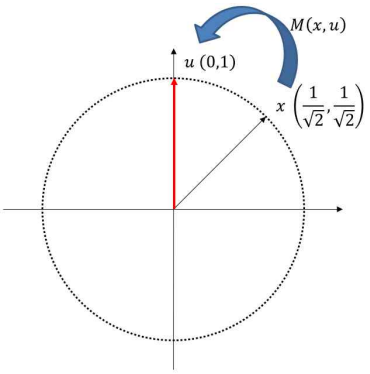
	c3	c2	c1
k1	0	0	1
k2	0	1	0
k3	1	0	0
k4	0	0	1

<그림 22.> bit 예시

  - Alice로부터 받은 실수 값을 유일한 정보로 사용하여 Bob은 첫 번째 열을 추측함. 첫 번째 열을 추정하고 해당 열을 대상으로 오류정정과정을 진행했다면 bob은 두 번째 열을 추정함. 이 때, 두 번째 열을 추정하는데 사용되는 정보는 Alice로부터 받은 실수 값과 완벽하게 Alice의 값과 동일해진 첫 번째 열임. 첫 번째 열의 정보를 이용할 수 있는 이유는 만약 k1행의 c1열의 값이 1로 결정이 되었다면 두 번째 열인 k1,c2 값이 될 수 있는 범위가 a2,a4,a6,a8로 줄어들기 때문임.
  - 두 번째 열도 완전히 Alice의 값과 똑같다면 세 번째 열인 c3열을 추정하는데는 alice의 실수값과 c1,c2열을 이용할 수 있음. 예를들어 k1열의 c2,c1 값이 01이라면 c3열의 값으로 추정되는 구간은 a2, a6 구간임. 위의 방식을 순차적으로 반복하여 Alice와 Bob은 나눠가진 실수값을 바탕으로 이진수 값을 나눠가질 수 있음.

2. Multidimensional reconciliation

- DV-QKD에서 uniform하게 정해지는 비밀키의 reconciliation 과정과 다르게 CV QKD에서 비밀키는 gaussian 분포를 가지기 때문에 reconciliation 과정에서 노출하는 부가정보가 비밀키에 대한 정보를 드러낼 수 있음. 따라서 Alice와 Bob이 나눠가진 실수 값을 normalize한 후에 spherical code를 이용하여 Alice와 Bob이 서로 이진수 값을 나눠갖고 오류를 고치는 과정을 사용함.
- 임의의 실수 값에서 얻은 임의 vector x를 임의의 binary bit u를 component로 갖는 vector로 보내는 함수를 $M(x,u)$이라고 할 때 아래 그림처럼 표현할 수 있음.



<그림 23.> vector 변환

- $M(x,u)x=u$를 만족하고 x^{-1}이 존재하기 때문에 $M(x,u)=ux^{-1}$을 통하여 rotation 함수를 구할 수 있음. $x=\frac{1}{\sqrt{2}}+i\frac{1}{\sqrt{2}}, u=0+i1$로 표현할 수 있고 임의의 vector x에 대하여 $x^{-1}=\frac{x^*}{|x|}$이기 때문에 (x^*은 x의 conjugate) $M(x,u)=ux^{-1}$은 다음과 같음.

$$M(x,u)=ux^{-1}=i\times(\frac{1}{\sqrt{2}}-i\frac{1}{\sqrt{2}})=\frac{1}{\sqrt{2}}+i\frac{1}{\sqrt{2}}$$

- 위에서 구한 $M(x,u)$를 이용하여 검산하면, 다음과 같음.

$$M(x,u)x=(\frac{1}{\sqrt{2}}+i\frac{1}{\sqrt{2}})\times(\frac{1}{\sqrt{2}}+i\frac{1}{\sqrt{2}})=i=u$$

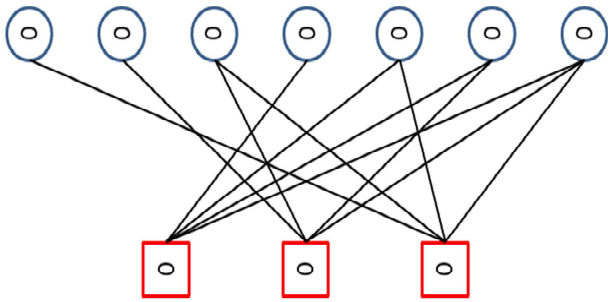
- 위의 예시는 R^n에서 dimension $n=2$인 경우의 예시이고, $n=1,2,4,8$인 경우에만 rotaion 함수가 존재한다는 제한이 있음. $n=4,8$인 경우 quaternion unit, octonion unit으로 정의됨.
- orthogonal matrices의 그룹을 $A_n=(A_1,\cdots,A_n)$으로 정의하고 $A_1=1_n$이고 $i,j>1$의 범위에서 $A_iA_j=-2\delta_{i,j}1_n$의 특성을 유지하는 matrices를 찾을 수 있음.

- 다음과 같은 lemma를 통해 reconciliation을 수행할 수 있음.
- $M(x,y)=\sum_{i=1}^{n}\alpha_i(x,y)A_i\ with\ \alpha_i(x,y)=(A_ix|y)$ is a continuous map from $S^{n-1}\times S^{n-1}$ to $O(n)$ such that $M(x,y)\cdot x=y$
- $M(x,u)=\sum_{i=1}^{2}\alpha_i(x,u)A_i=\frac{1}{\sqrt{2}}A_1+\frac{1}{\sqrt{2}}A_2$
- $M(x,u)x=(\frac{1}{\sqrt{2}}A_1+\frac{1}{\sqrt{2}}A_2)x=\frac{1}{\sqrt{2}}A_1x+\frac{1}{\sqrt{2}}A_2x=\begin{pmatrix}0\\1\end{pmatrix}=u$
- lemma 4를 통해 적절한 orthogonal matrices만 있으면 rotation 함수 $M(x,y)$를 쉽게 계산 가능함을 확인할 수 있음.

3. Low Density Parity Check codes (LDPC codes)
   - LDPC codes는 반복 복호를 통하여 높은 성능을 달성하는 선형부호이다
   - 다음의 parity check matrix를 예시로 들 수 있다

$$H=\begin{pmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{pmatrix}$$

   - 위의 parity check matrix는 다음과 같은 tanner graph를 통하여 나타낼 수 있음.



<그림 24.> H의 tanner graph

   - 파란색 원으로 표시된 node가 variable node로 수신한 값에 해당하는 node이고 빨간색 네모로 표시된 node가 check node로 variable node에 따른 syndrome을 확인하여 edge를 통해 주고 받는 정보를 제어하는 역할을 함.
   - 반복 복호를 통해 수신 값의 오류를 정정하고 Alice에게 받은 syndrome과 Bob이 매 복호마다 확인하는 syndrome이 일치할 때까지 복호를 계속함.

다. 프로토콜 특징

- CV-QKD는 Discrete variable(DV)-QKD와 다음과 같은 차이점을 가짐.
  - DV QKD는 이진수 0 또는 1을 송수신자인 Alice와 Bob이 나눠가지는 반면 CV QKD는 실수 값을 송수신자가 나누어 가짐.

- DV QKD는 양자채널을 BSC 표현하는데 비하여 CV QKD는 AWGN channel로 가정하고 reconciliation 과정에 따라 BSC 혹은 binary input AWGN (BI-AWGN) channel로 모델링이 가능함.
- DV QKD는 광원으로 단일광자 검출기를 가정하고 검출을 위하여 단일광자 검출기가 필요한 반면 CV QKD는 광원으로 coherent laser를 필요로 하고 검출을 위하여 homodyne 또는 heterodyne 검출기가 필요함.

- 이와 같은 차이점에 따라 CV QKD가 DV QKD에 비하여 구현 비용 매우 낮으며(단일광자 생성기와 단일광자 검출기는 모두 CV QKD의 필요장비에 비해 매우 비쌈), 구현의 용이함.

라. 참고문헌

[1] Leverrier, A., Alle´aume, R., Boutros, J., Ze´mor, G. & Grangier, P. Multi dimensional reconciliation for a continuous-variable quantum key distribution. Phys. Rev. A 77, 042325 (2008)

[2] Cerf, N., Iblisdir, S. & Van Assche, G. Cloning and cryptography with quantum continuous variables. Eur. Phys. J. D 18, 211-218 (2002)

[3] Ralph, T.: Phys. Rev. A 61, 010,303(R) (1999) 106

[4] Hillery, M.: Phys. Rev. A 61, 022,309 (2000) 106

[5] Cerf, N., Levy, M., Assche, G.: Phys. Rev. A ´ 63, 052,311 (2001) 106

[6] Grosshans, F., Grangier, P.: Phys. Rev. Lett. 88, 057,902 (2002) 106, 108

[7] Grosshans, F., Assche, G., Wenger, J., Brouri, R., Cerf, N., Grangier, P.: Nature 421, 238 (2003) 106, 108

[8] Lodewyck, J., Bloch, M., Garc´ıa-Patron, R., Fossier, S., Karpov, E., Diamanti, E., Debuisschert, T., Cerf, N., Tualle-Brouri, R., McLaughlin, S., Grangier, P.: Phys. Rev. A 76, 042,305 (2007) 106, 108, 109

[9] Gerry, C., Knight, P.: Introductory quantum optics. 1st edn. Cambridge University Press, Cambridge (2005) 102, 106

[10] Fossier, S., Diamanti, E., Debuisschert, T., Villing, A., Tualle-Brouri, R., Grangier, P.: arXiv:0812.3292 (2008) 106, 108

II. 과학기술연구망 적합 양자키분배 프로토콜 비교

1. QKD 프로토콜 과학기술연구망 적합도 평가 항목 설정

- QKD는 다양한 프로토콜이 존재하며 해당 프로토콜을 구현하는 방식들도 다양하게 존재함. 이러한 프로토콜과 구현방식에 따라 장단점이 매우 다르기 때문에 과학기술연구망에 적합한 프로토콜을 고르기 위한 기준을 세우는 것이 중요하다 할 수 있음. 과학기술연구망에 적합한 QKD 프로토콜을 선정하기 위한 기준들은 각각 다음과 같음.

  - 전송거리
  - 보안성
  - Star topology 적합도
  - 시스템 복잡도
  - 시스템 단가
  - 기존 광장비 활용성
  - Key rate
  - 개발/제작 난이도

- 전송거리 : 현재 상용 장비들의 전송거리가 70Km 내외로 과학기술연구망 백본에 적용하기에는 부족한 실정임. Trusted node를 통해 거리의 연장이 가능하지만, trusted node의 경우 보안성 측면에서 이슈가 제기되는 상황이며 끊어가는 구간이 많을수록 비용이 증가함. 따라서 과학기술연구망 내의 대전-서울, 대전-제주 구간 등의 장거리 백본망에 양자암호망을 효율적으로 적용하기 위해서 각 QKD 프로토콜의 전송거리에 대한 비교가 필요함.

- 보안성 : 각 프로토콜들이 모두 ITS(Information Theoretical Security)가 증명된 것이 아니며, 또한 각각이 취약하거나 강한 공격이 다름. 예를 들어 가장 초기에 제시된 BB84 프로토콜의 경우 단일광자가 아닌 것들을 갈라가져가는 Photon Number Splitting 공격에 매우 취약하다는 사실이 잘 알려져있음. 따라서, 양자암호 기반의 과학기술연구망에서 실제로 일어날 수 있는 공격에 강한 프로토콜을 선정하는 것이 중요함.

- Star topology 적합도 : 과학기술연구망의 경우 대전 본원, 서울 분원을 중심으로 각 지역망 센터가 연결되는 Star topology 형태를 가짐. Star topology의 경우 중앙에 각종 중앙 장비가 존재하는 중앙 집중형이기 때문에, 특정 구간의 문제가 전체 네트워크에 영향을 미치지는 않는 장점이 존재함. 과학기술연구망에 적용하려는 양자암호 장비들도 이러한 Star topology에 적합한 형태인 것이 운용 및 유지보수에 유리함. QKD 양단 장비가 서로 다른 비대칭형일 경우 복잡한

쪽을 중앙에 설치하고 상대적으로 간단한쪽을 사용자측에 설치하는 것이 사용자 측에서 장비 유지보수가 용이할 것으로 판단됨.

- 시스템 복잡도 : 본분원에 설치된 장비의 경우 유지보수가 용이하지만 지역망센터에 설치된 장비의 경우 유지보수가 쉽지 않기 때문에 송수신단의 복잡도가 다른 형태의 장비가 과학기술연구망에 더 적합할 수 있음.

- 시스템 단가 : 현재 상용 장비의 가격이 굉장히 높은 실정임. 이에 비교하여 비교적 저렴한 비용으로 구성할 수 있는 QKD 프로토콜이 있다면 백본뿐만 아니라 선별적으로 end-to-end까지 양자암호망 적용을 고려하고 있기 때문에 비용을 고려하는 것이 중요함.

- 기존 광장비 활용성 : 시스템 단가와 유사한 평가항목으로 현재 상용장비의 경우 단독 장비가 필요하며 노드를 추가할 때마다 Dark fiber로 연결이 필요함. QKD를 기존 광장비를 통해 할 수 있다면 비용 및 운영관리 측면에서 장점이 되기 때문에 중요한 평가항목임.

- Key rate : 현재 과학기술연구망은 100G망까지 지원하고 있기 때문에 사용자들이 대용량 데이터를 전송할 경우 암호키 교체주기가 매우 빠를 수 있음. 따라서 Key rate가 이를 지원할 수 있을 정도의 성능이 되어야함.

- 개발/제작 난이도 : 단일광자를 사용하는 프로토콜들의 경우 제작 난이도가 높으며, 얽힘을 사용하면 제작 난이도가 매우 높아짐. 이외에도 양단 기기 간 신호 싱크를 맞추는 것 등도 제작 난이도에 영향을 미침. 또한, 현재 상용장비화 되지 않은 프로토콜들은 개발 난이도 또한 높다 판단할 수 있음.

2. QKD 프로토콜 과학기술연구망 적합도 평가

프로토콜\ 평가항목	전송 거리	보안성	Star topology 적합도	시스템 복잡도	시스템 단가	기존 광장비 활용성	Key rate	개발/ 제작 난이도
Plug & Play 2-way BB84	약 70km	PNS, BS, MITM, DoS attack에 취약	중간	중간	높음	낮음	3×10^{-7} /pulse	중간
E91	-	BS, DoS attack에 취약	낮음	높음	높음	낮음	-	높음
SARG04	약	PNS, DoS	낮음	중간	높음	낮음	5×10^{-7}	중간

	90km	attack에 취약					/pulse	
DPS-QKD	260km	ITS 미증명	낮음	중간	중간	낮음	10^{-5} /pulse	중간
COW-QKD	125km	DoS attack에 취약 ITS 미증명	낮음	중간	높음	낮음	$10^{-3.8}$ /pulse	높음
TF-QKD	550km	측정 장비 보안성 극복 가능	낮음	높음	높음	낮음	$9\times10^{-}$ /pulse	높음
MDI-QKD	390km	측정 장비 보안성 극복 가능	낮음	높음	높음	낮음	2×10^{-6} /pulse	높음
CV-QKD	140km	ITS 미증명	높음	낮음	낮음	높음	5×10^{-6} /pulse	높음

<표 3> 과학기술연구망 적합 QKD 평가

III. 결론

○ 상기 평가표를 통해 각각의 프로토콜들을 비교분석 결과를 바탕으로 단기적으로는 Plug&Play 2-way BB84 프로토콜을, 중기적으로는 DPS-QKD를, 장기적으로는 TF-QKD, CV-QKD 연구개발 및 제작하는 것이 적합하다고 판단함.

○ Plug&Play 2-way BB84 프로토콜은 실험적으로 구현한 대학 연구실이 있으며, 협업을 통해 자체개발 가능할 것으로 판단되었음. 2-way 구조는 신호가 왕복 전송되기 때문에, 전송로를 통한 편광 오류가 자동보정되는 장점이 있음. 또한, 신호 동기화에 있어서 용이하기 때문에 1-way 프로토콜에 비해 제작 난이도가 낮을 것으로 판단됨. 또한 2-way 프로토콜이 Bob측의 장비에 비해 Alice측의 장비가 상대적으로 간단한 비대칭적 구조를 가지고 있어 Star topology에 적합하다고 판단됨. 이에따라 단기적으로 Plug&Play 2-way BB84 프로토콜을 제작하여 과학기술연구망에 양자암호망 운영/관리 시험용으로 사용하며, 자체제작 예정인 KMS 시험용 등으로 사용 가능할 것으로 판단함.

○ Plug&Play 2-way BB84 프로토콜의 경우 초기 시험용으로는 적합하나 전송거리의 한계 및 시스템의 단가가 높아 과학기술연구망 백본용으로는 부적합함. 따라서 장거리 전송이 가능한 QKD 프로토콜에 대한 연구개발이 필요하며, 프로토콜 비교분석에 따라 시스템 복잡도가 낮고 장거리 전송이 가능한 DPS-QKD를 중기적으로 연구개발해야함. DPS-QKD 프로토콜의 경우 260km 정도의 장거리 전송이 가능하며, 시스템 복잡도가 다른 단일광자를 사용하는 프로토콜에 비해 낮은 것으로 판단되어 중기적으로 개발하는 것을 목표로 함.

○ DV-QKD 프로토콜의 경우 단일광자를 사용해야하기 때문에 고가의 단일광자검출기가 필요함. 이러한 고가의 장비들이 부피가 매우 크며, 온습도에 매우 민감하여 이를 보정하기 위한 장비들까지 고려하면 시스템의 복잡도와 단가가 매우 높아짐. 또한 단일광자의 신호레벨이 매우 낮아 양자암호망 구축을 위해서 연결하려는 노드마다 dark fiber로 연결되어야하는 문제도 있음. 따라서 장기적으로 단대단 양자암호망 지원을 목표로하는 본 사업의 목표에 DV-QKD는 기능측면에서 부적합한 부분이 있음.

○ CV-QKD 프로토콜의 경우 단일광자가 아닌 광자다발을 사용하기 때문에 단일광자검출기가 필요하지 않으며 매우 간단하고 저비용인 호모다인 검출시스템을 갖추면 됨. 호모다인 검출시스템의 경우 상온에서도 고효율로 동작하기 때문에 시스템의 복잡도와 단가가 매우 낮음. 또한, 단일광자를 사용하지 않기 때문에 dark fiber가 필요없으며 기존의 데이터 통신 채널과

multiplexing도 가능하다는 큰 장점이 있음. 현재 프로토콜이 전송거리가 짧다는 단점이 존재하기 때문에, 장기적인 목표로 CV-QKD 프로토콜을 연구개발 하는 것이 적합하다고 판단함.

비매품/무료
93560
9 788929 411602
ISBN 978-89-294-1160-2