1. 서론

정보 보안은 오래 전부터 중요한 이슈로 여겨졌지만 정보화 시대를 맞이한 현대 사회에서는 다른 어느 때보다 그 중요성이 부각되고 있다. 컴퓨터와 스마트폰을 통해 어디에서든 인터넷을 이용한 정보 검색, 금융, 인터넷 상거래가 가능한 정보화 시대의 이면에는 도청이나 해킹, 스미싱 등에 의한 정보 보안의 위협이 항상 존재한다.

도청이나 해킹 등의 위협으로부터 안전한 정보통신을 구현하기 위해 다양한 현대암호 기법이 이용되는데, 특히 공개키 암호가 널리 이용되고 있다. 공개키 암호의 안전성은 계산의 복잡성에 기반한다. 공인인증 체계에서 널리 쓰이고 있는 RSA 암호는 두 개의 큰 수의 곱은 쉽게 계산할 수 있지만, 그 반대 과정인 소인수분해는 알고리즘에 비해 지수함수적으로 단축시킨다. 따라서 쇼어 알고리즘을 효과적으로 구현하는 양자컴퓨터의 개발은 RSA 암호체계의 붕괴를 가져올 것으로 판단된다 [1].

이러한 공개키 암호의 안전성에 대한 위협은 공개키 암호와 함께 현대암호의 한 축을 이루는 비밀키 암호를 이용함으로써 피할 수 있다. 비밀키 암호에서 송 · 수신자는 동일한 비밀키를 나누어 가지고 이를 이용하여 암호통신을 수행한다. 비밀키 암호의 대표적인 예로는 일회용 난수(One-Time-Pad, OTP) 방식이 있다. OTP 방식은 보내고자 하는 메시지의 길이와 같은 길이의 난수표를 이용하여 메시지를 암호화하는 방식으로, 비밀키를 도청자가 알 수 없을 경우 절대적인 안전성을 보장한다. 하지만 멀리 떨어진 송수신자가 제 3자의 도청 위협으로부터 안전하게 비밀키를 나누어

특집 ■ 양자정보

단일광자 생성, 검출 및 양자암호 통신 응용

김용수, 최유준, 이민수, 권오성, 한상욱, 문성욱*

무척 어려운 연산이라는 사실을 이용하여 만든 암호다. 이처럼 수학적 연산의 어려움에 기반한 공개키 암호의 안전성은 새로운 연산 알고리즘이나 컴퓨팅 파워의 증가에 위협을 받는다. 특히 컴퓨팅 파워의 증가는 RSA 암호의 현실적인 위협이 되며, 이에 따라 RSA 암호에서 이용하는 소수의 크기가 점점 커지고 있다. 또한, 양자컴퓨터의 쇼어 알고리즘(Shor algorithm)은 소인수분해를 하는 데 걸리는 시간을 기존 컴퓨터의 가지는 것은 매우 어려운 일이다.

1984년 IBM 사의 C.H. Bennet과 G. Brassard는 단일광자를 이용하여 멀리 떨어진 송 · 수신자가 비밀키를 안전하게 나누어가지는 방법을 제안하였는데, 이를 BB84 프로토콜이라 한다. BB84 프로토콜에서 비밀키 분배의 안전성은 단일광자가 가지는 양자측정에 의한 상태 변화, 복제 불가능성과 같은 양자(量子, Quantum)특성에 기반한다. 이처럼 양자특성을

* 한국과학기술연구원 나노양자정보연구센터

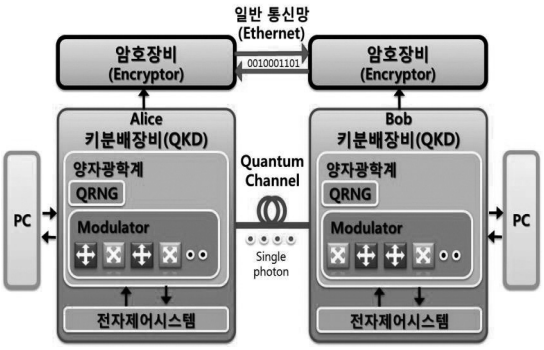


그림 1. 양자암호통신의 구성. '양자키분배(QKD)'와 분배된 비밀키를 이용한 현대암호통신을 수행하는 '암호장비'로 구성되어 있다. QKD 장비는 양자난수발생기, Modulator 등을 포함하는 양자광학계와 이를 제어하는 전자제어시스템으로 구성된다.

이용하여 비밀키를 안전하게 나누어가지는 것을 양자키분배(Quantum Key Distribution, QKD)라고 한다. 이렇게 안전하게 분배된 비밀키를 현대암호통신에 적용하여 실제 암호통신을 수행하는데, 이러한 일련의 과정을 양자암호통신이라고 부른다. 즉, 양자암호는 '양자키분배(QKD)'와 분배된 비밀키를 이용한 '현대암호통신'의 합으로 나타낼 수 있다.

본 고에서는 양자암호통신을 구성하는 한 축으로, 양자정보통신의 최초 활용 사례인 QKD의 원리에 대하여 소개하고 이를 구성하기 위한 단일광자 생성과 검출에 대해 이야기할 것이다. 특히 한국과학기술연구원(KIST)에서 개발한 QKD 시스템과 이 시스템에서 실제로 사용된 단일광자 생성 및 검출 기술을 소개할 것이다. 거기에 덧붙여 QKD 시스템 장비(Device)의 결함을 이용하여 도청을 시도하는 일련의 양자 공격에 대해서도 간략하게 소개할 것이다.

2. 양자키분배(QKD) 시스템

최초의 QKD 프로토콜인 BB84 프로토콜이 제안된 이후 Ekert 프로토콜, B92 프로토콜, Six State 프로토콜, SARG04 프로토콜 등 다양한 QKD 프로토콜이 제안되었으나 안전성 및 신뢰성이 수많은 이론 · 실험 연구를 통해 증명되었고, 구현이 비교적 간단한 BB84 프로토콜이 가장 널리 이용되고 있다. BB84 프로토콜은 두 기저(Basis)를 이루는 네 개의 편광상태(수평(0°), 수직(90°), 45° 그리고 −45°)를 이용하여 비밀키를 인코딩한다. 여기에서는 수평 편광과 45° 편광은 비밀키 Bit 값 0으로, 수직 편광과 −45° 편광은 비밀키 Bit 값 1로 약속한다. 송신자는 기저를 랜덤(Random)하게 선택하고, 선택한 기저의 두 편광상태 중 임의의 편광상태를 가지는 광자를 수신자에게 보낸다. 수신자는 임의로 선택한 기저를 이용하여 송신자로부터 받은 광자의 편광상태를 측정하고 이를 기록한다. 수신자의 측정과 기록이 끝나면, 송 · 수신자는 각자 자신이 선택한 기저를 공개하고, 서로 같은 기저를 이용한 경우에만 비밀키를 생성한다. 만약 제 3자에 의한 도청 시도가 있다면, 양자가 가지는 독특한 특성으로 인하여 송 · 수신자가 같은 기저를 사용하더라도 서로 다른 비밀키를 가지게 될 확률이 존재한다. 이러한 비밀키 오류율(Quantum Bit Error Rate, QBER)을 계산하여 도청 여부를 판단할 수 있다. 양자암호 시스템 측정 장비의 불확실성으로 인한 검출기 효율, 광전송 손실, 광학계 손실 등이 QBER에 영향을 미친다. 하지만, 이론적으로 QBER이 11%를 넘지 않으면 도청으로부터 자유로운 안전한 비밀키를 나누어 가질 수 있다. 그림 2는 BB84 프로토콜과 도청에 의한 비밀키 오류 발생 원리를 도식적으로 나타낸 것이다.

KIST에서는 외부 환경변화에 강인한 Plug & Play

송신자	기저	✕	+	+	✕	+	✕	✕	+
	편광	↗	↕	↕	↘	↔	↘	↗	↕
	비밀키	0	1	1	·	·	1	·	·
도청자	기저	·	+	✕	·	·	+	·	·
	측정된 편광	·	↕	↘	·	·	↔	·	·
수신자	기저	✕	+	+	+	✕	✕	+	✕
	편광	↗	↕	↔	↕	↗	↗	↕	↗
	비밀키	0	1	0	·	·	0	·	·
비밀키 일치 여부		o	o	x	·	·	x	·	·

그림 2. BB84 프로토콜과 도청에 의한 오류 발생 원리

그림 3. KIST에서 개발한 QKD 시스템

방식이 적용된 QKD 시스템(그림 3)을 개발하고 25km 양자키분배에 성공하였으며, 그 결과를 해외 양자암호학회(QCrypt 2013)에 전시 및 시연하였다. KIST에서 개발한 QKD 시스템의 비밀키 생성율은 약 1kbps, QBER은 3% 이하로 유지하였다. 현재 KIST에서는 KIST QKD 시스템의 안전성 및 신뢰성을 검증하고 있으며, 시스템의 성능을 올리기 위한 연구도 동시에 수행하고 있다.

3. 양자광원생성

QKD의 안전성은 단일광자의 양자특성에 기반한다. 단일광자가 아닌 다광자 펄스를 이용하여 QKD를 구현하면, 도청자는 펄스 중 일부의 광자를 가로채어 이를 도청에 활용할 수 있는데, 이를 광자개수 가르기(Photon-Number-Splitting, PNS)공격이라 한다 [4]. 따라서 QKD 시스템의 안전성을 보장하기 위해서는 단일광자 상태를 이용해야 한다.

단일광자를 생성하기 위한 다양한 방법이 연구되고 있지만 낮은 생성 효율, 안정적 동작의 어려움, 생성 장치의 복잡함 등 기술적 한계로 아직 실제 양자암호통신에는 거의 활용되지 못하고 있다. 이를 대신하여 대부분의 양자암호통신은 약하게 감쇄한 레이저 펄스를 이용하여 만든 유사 단일광자 상태를 이용한다.

유사 단일광자 상태란 레이저 펄스를 아주 약하게 감쇄시켜 하나의 펄스에 두 개 이상의 광자가 존재할 확률이 작은 상태를 말한다. 이러한 유사 단일광자 상태의 통계적 특성은 식 (1)과 같은 포아송(Poisson) 분포를 따른다.

$$P(x)=\frac{e^{-\mu}\cdot\mu^{x}}{x!} \quad (1)$$

여기서 x는 하나의 펄스에서 존재하는 광자수, μ는 펄스당 평균 광자수를 나타낸다. 표 1은 하나의 펄스에 존재하는 광자의 개수 확률분포를 펄스당 평균 광자수에 따라 정리한 것이다. 예를 들어 펄스당 평균 광자수가 0.5이라면, 하나의 레이저 펄스에 광자가 존재하지 않을 확률은 61%, 하나의 광자가 존재할 확률은 30%, 두 개의 광자가 존재할 확률은 7.6% 이다. QKD 시스템에서는 펄스당 평균 광자수를 줄임으로써 하나의 레이저 펄스에 두 개 이상의 광자가 존재하는 경우를 줄임으로써 다광자 상태에 의한 도청 가능성을 최소화 하고 있다.

현재 KIST에서 개발한 QKD시스템에서는 평균 광자수가 0.1개인 유사 단일광자 상태를 사용하고 있다. 아래 그림 4는 평균광자수가 0.1개일 때의 그래프로, x축은 하나의 펄스에 존재하는 광자수, y축은 광자수에 해당하는 확률을 나타낸다. 그림과 같이 하나의 펄스에 두 개 이상의 광자가 존재할 확률은 매우 작음을 알 수 있다. 이때 사용된 레이저는 2MHz로 동작하며 펄스폭은 3ns이다.

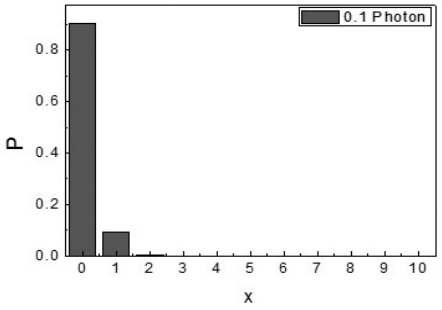


그림 4. 평균 광자수가 0.1일 경우 유사 단일광자 상태의 확률분포

표 1. 유사 단일광자 상태의 펄스당 발견된 광자수의 확률

	μ=0.01	μ=0.05	μ=0.1	μ=0.5	μ=1	μ=2	μ=5	μ=10
P(x=0)	0.990	0.951	0.905	0.607	0.368	0.135	0.007	4.54e-5
P(x=1)	0.010	0.048	0.090	0.303	0.368	0.271	0.034	4.54e-4
P(x=2)	4.95e-5	0.001	0.005	0.076	0.184	0.271	0.084	0.002
P(x=3)	1.65e-7	1.98e-5	1.51e-4	0.013	0.061	0.180	0.140	0.007
P(x=4)	4.13e-10	2.48e-7	3.77e-6	0.002	0.015	0.090	0.175	0.019
P(x=5)	8.25e-13	2.48e-9	7.54e-8	1.58e-4	0.003	0.036	0.175	0.038

하지만 펄스당 평균 광자수가 줄어들면 수신자가 성공적으로 광신호를 받을 확률이 낮아져 비밀키 분배 속도가 감소한다. 더욱이 펄스당 평균 광자수를 아무리 줄여도 두 개 이상의 광자가 하나의 펄스에 존재할 확률은 항상 존재하며, 이는 PNS 공격에 이용될 수 있다. 이러한 유사 단일광자 상태를 이용한 QKD의 안전성이 가지는 본질적인 한계는 미끼상태(Decoy state)를 이용함으로써 극복할 수 있다.

미끼상태는 QKD에 이용되는 광신호의 평균 광자수와 다른 수의 평균 광자수를 가지는 레이저 펄스로, PNS 공격을 효과적으로 막을 수 있는 방식이다. 즉, 미끼상태를 적용한 QKD는 펄스당 평균광자수가 μ인 레이저 펄스(신호상태)와 ν인 레이저 펄스(미끼상태)를 임의로 생성하고 이를 이용하여 양자통신을 수행한다. 도청자는 각각의 광펄스가 신호상태에 해당하는지 미끼상태에 해당하는지 알 수 없으므로, PNS 공격을 수행할 경우 QKD 송·수신자는 신호상태와 미끼상태에 대하여 서로 다른 비밀키 생성률과 QBER을 얻게 된다. 따라서 QKD 송·수신자는 신호상태와 미끼상태의 비밀키 전송률, QBER 등을 바탕으로 도청자에 의한 PNS 공격 유무를 판단할 수 있다. 미끼상태는 실제 QKD 시스템의 안전성을 비약적으로 발전시켰으며, 둘 이상의 미끼상태를 QKD 시스템에 적용할 경우 이상적인 단일광자를 이용한 QKD 시스템과 비슷한 수준의 안전성을 제공하는 것으로 알려져 있다 [5].

양자정보에서 널리 연구되고 있는 얽힘 상태(Entangled state)를 QKD 시스템의 광원으로 사용하는 방법도 있다. Ekert는 이를 이용한 프로토콜을 개발하여 QKD시스템으로의 응용 가능성을 입증하였다 [6]. 얽힘 상태는 양자상태가 가지는 독특한 성질로, 둘 이상의 입자들이 서로 강한 상관관계를 가지고 있어서 입자들의 상태를 각각의 파동함수 곱으로 기술할 수 없는 상태를 말한다. 이런 상태는 D. Bohm이 제안한 스핀이 1/2인 한 쌍의 전자 사이에 존재하는 스핀의 비대칭 상관관계와 두 전자의 스핀 중첩상태, 즉 식(2)와 같이 표현할 수 있다.

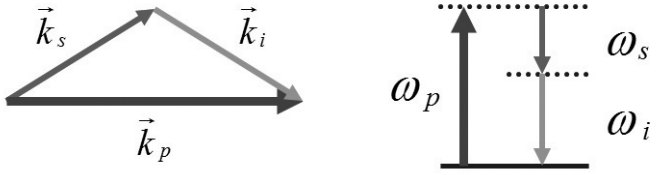
$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_1|\downarrow\rangle_2 - |\downarrow\rangle_1|\uparrow\rangle_2\right) \quad (2)$$

공간적으로 아무리 멀리 떨어져 있더라도 두 입자의 스핀 상태는 up(↑) & down(↓)의 상태가 서로 얽혀 있고, 한 입자의 스핀이 특정 방향으로 결정되면 동시에 다른 입자의 스핀은 반대 방향으로 결정된다. 이런 얽힘 상태를 이용한 QKD 방식은 특히 양자리피터(quantum repeater)를 이용한 원거리 양자암호통신에 직접 적용할 수 있어 차세대 QKD 방식으로 주목 받고 있다 [7].

얽힘 상태를 만들기 위한 대표적인 방법으로는 자발매개하향변환(Spontaneous Parametric Down-Conversion, SPDC)이 있다. SPDC는 높은 에너지를 가진 레이저를 높은 비선형 계수를 갖는 매질에 입사시킬 때 입사하는 광자의 일부가 상대적으로 낮은 에너지를 가진 한 쌍의 광자로 자발적으로 변환하는 과정을 말한다. 일반적으로 발생한 광자 쌍의 광자들을 각각 Signal 광자와 Idler 광자라고 부른다. 그림 5와 같이 SPDC는 펌프 광자와 비선형 매질 내에서 하향 변환된 Signal, Idler 광자간 에너지 보존법칙과 운동량 보존법칙을 만족하며 발생하며, 수식으로는 아래와 같이 나타낼 수 있다.

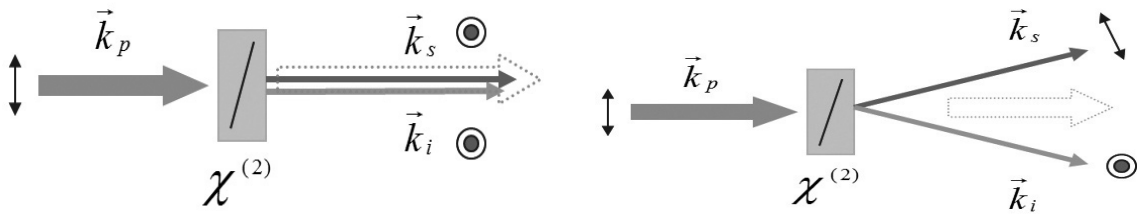
$$\omega_p = \omega_s + \omega_i, \quad \vec{k_p} = \vec{k_s} + \vec{k_i} \quad (3)$$

SPDC에서 발생하는 두 광자는 에너지 보존법칙과 운동량 보존법칙에 의해 서로 강한 상관관계를 가지고 있어, Signal 광자가 임의의 진동수와 파수 벡터를 갖고 발생하면 이에 대응하는 진동수와 파수 벡터를 가지는 Idler 광자 한 개가 반드시 발생하게 된다. SPDC 과정에서 발생한 두 광자의 편광이 같으면



(a) 운동량 보존 법칙 (b) 에너지 보존 법칙

그림 5. 위상정합조건. p : pump, s : signal, i : idler 광자를 나타낸다.



(a) Type-I collinear (b) Type-II non-collinear

그림 6. SPDC 과정에서 발생한 광자쌍.

제1형(type-I), 편광이 서로 수직이면 제2형(type-II)이라 하며, 발생한 광자 쌍이 펌프 레이저와 같은 방향으로 나아가면 Collinear, 일정한 각도를 가지며 발생하면 Non-Collinear라고 한다. 그림 6은 각각 제1형 collinear SPDC와 제2형 non-collinear SPDC를 도식적으로 나타낸 것이다. 이러한 SPDC와 양자 간섭계를 적절히 이용함으로써 얽힘 상태를 만들 수 있으며, 이는 QKD 시스템의 광원은 물론 다양한 양자광학/양자정보 기초실험의 광원으로 활용된다. KIST에서는 SPDC를 이용하여 유선 QKD에 활용하기 위한 1,550nm의 얽힘 광원 생성에 대한 연구를 수행하고 있다.

4. 단일광자 검출

QKD 시스템 구성요소 중 단일광자 검출기는 전체 시스템의 성능을 좌우하는 핵심 소자인 동시에 QKD 시스템의 병목 기술이기도 하다 [8, 9]. 단일광자 검출기에 대한 연구는 스위스, 일본, 캐나다 등의 국가 연구기관과 IDQ, 도시바와 같은 기업에서 널리 수행하고 있다 [10].

광통신망을 활용하는 유선 QKD 시스템에서는 가시광선(500-900nm) 파장영역보다 상용 통신 파장영역(1550nm)이 선호된다. 현재 유선 QKD 시스템에서는 통신 파장영역에서의 광 흡수율이 높고, 구동전압이 낮은 InGaAs/InP Avalche Photo Diode(APD)가 단일광자 검출 소자로 가장 많이 이용되고 있다. 하지만 InGaAs/InP APD에는 After-Pulse와 Dark Current로 인한 노이즈가 가시광선 파장영역에서 주로 이용되는 Si APD에 비해 높은데, 이러한 노이즈는 QKD의 비밀키 생성율과 안전성에 영향을 미친다.

QKD 성능을 개선하기 위해 InGaAs/InP APD의 노이즈를 줄이려는 다수의 연구가 진행되어 왔다. 대표적인 방법으로는 레이저 펄스가 들어오는 시간에만 단일광자 검출기를 동작시키는 게이트 모드(Gated mode) 동작이 있다 [11]. 이는 Dark Current가 신호로 검출되는 시간을 줄임으로써 Dark Count 비율을 효과적으로 낮추는 방법이다. 그러나 게이트 모드의 사용만으로는 Dark Current 노이즈를 충분히 줄이기 힘들어 부가적으로 APD를 냉각시켜 열에 의해 발생하는 Dark Current를 줄인다 [12].

KIST에서는 냉각시스템을 부착한 APD모듈에 저잡음 검출방식을 이용하여 APD의 주요 노이즈를 효과적으로 감소시킨 단일광자 검출기를 개발하였으며 이는 KIST QKD 시스템에 적용되어 QKD의 성능을 개선하는데 이용되었다 (그림 3) [13].

KIST에서는 Dark Current 노이즈를 줄이기 위해 APD 모듈 외부에 TEC(Thermal Electric Cooler)를 이용하여 모듈을 냉각시키고, 저온상태를 유지하기 위해

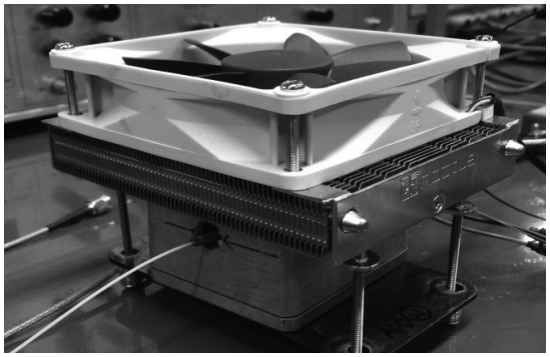
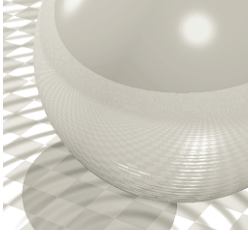


그림 7. KIST에서 제작한 InGaAs/InP APD를 이용한 단일광자 검출기



단열성이 높은 기구를 설계하여 최대 −45℃까지 냉각이 가능하도록 제작하였다. 또한 팬을 TEC에 연결시켜 TEC 동작 시 발생하는 열에 의한 노이즈를 제거함으로써 냉각효율을 높였다. 고효율 APD 동작을 위해서는 온도를 일정하게 제어하는 것이 중요하므로, TEC의 동작을 제어할 수 있는 회로를 설계하여 모듈 내부를 일정한 저온상태로 유지하게 만들었다. 추가적으로 온도측정소자(Thermistor)를 사용하여 APD 내부 온도변화를 실시간으로 확인할 수 있도록 디스플레이용 디바이스(Display Device)도 부착하였다. 제작된 모듈은 양자효율이 15.6%일 때 7.8×10^{-6}수준의 Dark Count 확률을 나타낸다.

After-Pulse 노이즈를 줄이기 위해서는 트랩된 캐리어가 소멸하기까지의 시간을 충분히 늘리는 방법도 있지만, 광자 검출 시간이 길어지는 치명적인 단점으로 이해 QKD 시스템에는 적용할 수 없다 [14]. 따라서 KIST에서는 광자검출시간은 유지하면서 After-Pulse 노이즈를 줄이기 위하여 적분기(Integrator)를 이용한 저잡음 검출방식을 적용하였다. 이 방식을 적용하면 APD의 출력신호를 적분함으로써 Background 신호보다 낮은 레벨의 Weak Avalanche 신호를 검출할 수 있어 효과적으로 After-Pulse를 줄일 수 있다. 또한 APD 내부에 입력되는 전류의 크기를 줄여도 양자효율은 변하지 않기 때문에 입력전류를 줄여 APD내부에 트랩된 캐리어의 수를 감소시킬 수 있다. 결과적으로 15.64%의 양자효율을 가질 때 일반적인 방식으로는 11%의 After-Pulse를 보인 반면 KIST에서 제안한 방식은 1.48%로 현저히 적은 After-Pulse 노이즈가 발생함을 볼 수 있었다.

5. QKD시스템에 대한 공격

양자암호의 안전성은 자연의 근본원리인 양자상태의 복제불가능성(no-cloning theorem)에 그 기반을 두고 있어 이론적으로는 도청이 허용될 여지가 전혀 없다 [14]. 그러나 실제로는 완벽한 장비를 이용하여 QKD를 구현하는 것이 불가능하다. 최근에는 이러한 사실에 기반하여 시스템의 불완전성을 포함한 안전성 증명(security proof)을 연구하고 있다 [15].

QKD 시스템의 안전성 증명이 연구됨과 동시에 기존에 개발된 QKD 시스템을 공략하여 도청하는 방법도 계속해서 연구되고 있다. QKD 공격에 대한 연구를 하면 QKD 시스템의 안전성을 사전에 보완하는데 활용할 수 있기 때문이다. 현재까지 개발된 공격 방식으로는 Blinding attack, After-gate attack, Time-shift attack, Trojan-horse attack 등이 있으며 대부분의 공격 방법에 대한 해결책 역시 제시되었다. 아래는 주요한 양자 공격 방식을 정리한 것이다.

양자 공격 방식

A. Blinding 공격

APD의 Dead time을 이용하는 방법으로 도청자가 APD에 의도적으로 강한 빛을 보내 APD를 가열시킨 다음, 낮아진 인가 전압(Bias voltage)와 광검출 효율(Detect efficiency)을 이용해 정보를 얻는다. 강한 빛이 들어오는지 여부를 모니터링 함으로써 이러한 도청을 피할 수 있다 [16].

B. After-gate 공격

Blinding 공격의 일종으로 APD의 게이트 타이밍(Gate timing) 이후에 강한 빛을 APD에 입사시켜 Dead time을 만들거나 선형 동작 클릭(Linear operation click)을 이용하여 검출기의 작동을 조절한다. 강한 빛 대신 약한 빛을 사용하는 것을 Faint after-gate 공격이라 부른다. 도청자는 이를 통해 송신자와 수신자 사이에서 광자를 가로채서 측정하고 다시 보내는 행위를 효과적으로 할 수 있고 이로써 비밀키 전체를 얻게 된다. 해결책으로는 APD에 들어오는 빛의 세기를 실시간으로 모니터링하는 시스템이 있다 [16, 17].

C. Time-shift 공격

한 시점에서 두 개의 APD 간의 검출효율이 다른 경우를 이용한 공격으로 도청자가 송신자로부터 광자를 가로채 확인한 후 광자의 타이밍을 조절해서 수신자에게 보내면, 수신자의 APD 작동을 조절할 수 있게 되고 이를 통해 정보를

얻는다. 해결책은 도청자가 알아차리지 못할 정도로 미세한 Delay line을 만들어 검출효율을 모니터링하는 방법이 있다 [18, 19].

D. Trojan-horse 공격

QKD 시스템을 가동하지 않는 시간에 도청자가 송신자와 수신자 간의 광섬유를 통해 수신자 쪽으로 레이저를 보내어 되돌아 오는 빛을 분석하여 정보를 얻는다. 이 공격 방식에는 OTDR(Optical Time Domain Reflectometry) 기술이 사용된다. 해결책으로는 QKD 시스템을 가동하지 않는 시간에는 수신자 측 장비를 닫아두거나 수신자 측에 들어오는 빛을 모니터링하는 방법이 있다 [20].

QKD 시스템은 위와 같은 다양한 공격을 염두에 두고 구현되어야 한다. 이런 공격들에는 주로 APD, 즉 검출부의 결함을 이용하는 방법이 많이 사용되고 있기 때문에 측정장비에 무관한 QKD 방법에 대한 연구 역시 진행되고 있다 [21].

6. 결론

본 고에서는 QKD 시스템과 이를 구성하는 핵심 기술인 단일광자 생성 및 검출기술에 대하여 알아보았다. 또한 QKD를 구현하는 장비의 불완전성을 이용한 주요한 양자 공격에 대해서도 살펴보았다. QKD는 이론적으로 완벽하지만 실용화를 위해서는 아직 넘어야 할 산이 많이 남아있다. 단일광자 생성에서는 고속으로 동작하는 QKD시스템에 적합한 유사 단일광자 상태를 효율적으로 만드는 기술이 필요하며 SPDC 과정에 의해 생성된 단일 광자쌍을 QKD에 응용하는 방법도 계속 연구되어야 한다. 단일광자 검출에서는 통신파장영역에서 높은 검출효율을 가진 APD가 필요하며 Dark Current와 After-Pulse로 인한 노이즈를 동시에 줄일 수 있는 연구가 진행되어야 한다. 또한 QKD 시스템에 대한 공격에서는 실효적인 안전성 증명과 각 공격방법을 막을 수 있는 해결책이 요구되고 있다. 이러한 연구가 모두 이루어진다면 보다 완성도 높고 실제 광통신망에 적용 가능한 QKD 시스템을 개발할 수 있고, 이를 통한 양자암호통신 네트워크의 구현으로 더 안전한 정보 생활을 보장할 수 있을 것이다.

Acknowledgement

본 연구는 미래창조과학부 및 한국산업기술평가관리원의 산업융합원천기술개발사업의 일환으로 수행하였음.
[10044559, 양자암호통신 네트워크 구축을 위한 요소기술 개발]

참고문헌

[1] P. Shor, in Proc. of the 35th Annu. Symp. on Foundations of Computer Science, edited by S. Goldwasser, IEEE Computer Society Press, Los Alamitos, California, p.124, (1994).
[2] C.H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", in Proc. of IEEE Int'l Conf. on Computers, Systems and Signal Proc., Bangalore, India, IEEE, New York, p.175, (1984).
[3] N. L. tkenhaus, M. Jahma, "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack", New J. Phys. 4, 44 (2002).
[4] H. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution", Phys. Rev. Lett. 94, 230504 (2005).
[5] A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem", Phys. Rev. Lett. 67, 661-663 (1991).
[6] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics", Rev. Mod. Phys. 83, 33 (2011).
[7] D. Stucki, N. Gisin, O. Guinnared, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug & play system", New J. Phys. 4, 41.1-41.8 (2002).
[8] S.-B. Cho, and S.-K. Kang, "Weak avalanche discrimination for gated-mode single-photon avalanche photodiodes", Opt. Express 19, 18510-18515 (2011).
[9] Zhang, Jun, et al., "Practical fast gate rate InGaAs/InP single-photon avalanche photodiodes", App. Phys. Lett. 95, 1-3 (2009).
[10] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, "Evolution and prospects for single-photon avalanche diodes and quenching circuits", J. Mod. Opt. 51, 1267-1288 (2004).
[11] Cerberis from ID quantique http://www.idquantique.com/network-encryption/cerberis-layer2-encryption-and-qkd.html

[12] A. Bouzid, J. B. Park, S. M. Kim, and S. moon, "Near Infrared Single photon Detector Using an InGaAs/InP Avalanche Photodiode Operated with a Bipolar Gating Signal", J. Jpn. Appl. Phys. 51, 034401 (2012).
[13] M. Ware, A. Migdall, J. C. Bienfang, and S. V. Polyakov, "Calibrating photon-counting detectors to high accuracy: background and deadtime issues", J. Mod. Opt. 54, 361-372 (2007).
[14] W.K. Wooters and W.H. Zurek, "A Single Quantum Cannot be Cloned", Nature 299, 802, (1982).
[15] D. Gottesman, H.K. Lo, N. Lutkenhaus, and J. Preskill, "Security of Quantum Key Distribution with Imperfect Devices", Quantum Inf. Comput. 4, 325, (2004).
[16] Thiago Ferreira da Silva, Guilherme B. Xavier, Guilherme P. Temporî o, and Jean Pierre von der Weid, "Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems", Opt. Express 20, 19812-18924 (2012).
[17] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, "After-gate attack on a quantum cryptosystem", New J. Phys. 13, 013043 (2011).
[18] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystem", Quantum Inf. Comput. 7, 073 - 082 (2007).
[19] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems", Phys. Rev. A 78, 042333 (2008).
[20] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems", Phys. Rev. A 73, 022320 (2006).
[21] H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution", Phys. Rev. Lett. 108, 130503 (2012).

약 력

김용수

• 2012. 02
POSTECH 물리학 박사
• 2012. 03 ~ 2013 .05
NIST 박사후 연구원
• 2013. 06 ~ 현재
KIST 나노양자정보연구센터 선임연구원

최유준

• 2014. 03 ~ 현재
나노양자정보연구센터 석박사통합과정

이민수

• 2011. 09 ~ 현재
나노양자정보연구센터 석박사통합과정

권오성

• 2012. 2
포항공과대학교 물리학 박사.
• 2012. 2 ~ 2012. 8
광주과학기술원 고등광기술연구소 박사후 연구원
• 2012. 9 ~ 현재
KIST 나노양자정보연구센터 박사후 연구원

한상욱

• 2006. 08
KAIST 전기및전자공학 박사
• 2006. 01 ~ 2009. 01
(주)픽셀플러스 선임연구원
• 2009. 02 ~ 2012. 04
삼성종합기술원 전문연구원
• 2012. 05 ~ 현재
KIST 나노양자정보연구센터 선임연구원

문성욱

• 1989년 ~ 현재
KIST 나노양자정보연구센터장