JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 12 : 2318~2324 Dec. 2017

시간지연을 이용한 양자비밀직접통신

임광철[1] · 임동호[2*]

Quantum Secure Direct Community using Time Lag

Kwang-cheol Rim[1] · Dong-ho Lim[2*]

[1]Department of Mathematics, Chosun University, Kwangju 61452, Korea
[2*]Department of Mathematics Education, Sehan University, Yeongam, JunranamDo 58447, Korea

요 약

차세대 암호로 대두 되고 있는 양자암호는 양자키전송 프로토콜과 양자비밀직접통신으로 나뉘어 연구되고 있다. 양자키전송 프로토콜은 사용상의 비효율성 때문에 현대암호와 병합하여 사용하거나 OTP를 포기한 형태로 사용될 수 있다. 본 고에서는 양자키전송이 아닌 직접통신을 양자암호화 하여 진행하는 알고리즘을 제안하였다. 양자비밀직접통신을 구현하는 방식은 2채널 방식을 이용하였다. 두 채널 중 한쪽 채널에 아인슈타인의 중력장에의한 시간지연 함수를 적용하여 두 채널간 시간차를 적용하는 방식의 양자비밀직접통신 프로토콜을 설계 하였다. 제안하는 시간지연 효과는 중력렌즈 현상을 반영한 것으로 점질량에 의한 시간지연을 제안하였다. 원심가속도를 이용한 중력 발생기는 점질량계에 포함되며 이를 이용한 시간지연은 중력계의 변화에 의한 상관관계를 보임을 알 수 있다.

ABSTRACT

Quantum cryptography, which is emerging as a next generation password, is being studied by quantum cryptographic transfer protocols and quantum secret communication. Quantum key transfer protocol can be used in combination with the modern password because of the inefficiency of the use of the password, or the use of OTP(one time password). In this paper an algorithm for direct communication by means of direct cryptographic communications rather than quantum keys. The method of implementing quantum secure direct community was adopted using 2-channel methods using Einstein gravity field. Two channels were designed to adopt a quantum secret communication protocol that applies time delay between 2-channels of channel to apply time difference between 2-channels. The proposed time delay effect reflects the time delay by reflecting the gravitational lensing phenomenon. Gravity generator with centrifugal acceleration is incorporated in the viscometer, and the time delay using this implies the correlation between the variance of the metametry.

키워드 : 양자비밀직접통신, QSDC, QKD, 양자통신

Key word : Quantum secure direct community, QSDC, QKD, Quantum community

Received 26 October 2017, **Revised** 23 November 2017, **Accepted** 05 December 2017

* **Corresponding Author** Dong-Ho Lim(E-mail:rim1201@hanmail.net, Tel:+82-62-230-6610)
Department of Mathematics Education, Sehan University, Yeongam, JunranamDo 58447, Korea

Open Access https://doi.org/10.6109/jkiice.2017.21.12.2318 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

양자통신의 근간은 양자상태가 여러 상태를 동시에 갖고 있고 이를 동시에 정확하게 측정할 수 없기 때문에 양자비트는 복제 불가능하다는 전제를 바탕으로 발달하였다. 현재 각국에서 경쟁적으로 양자키분배(Quantum Key Distribution, QKD) 방법에 대한 연구가 활발히 진행되고 있으며 양자 암호시스템인 QKD는 높은 엔트로피의 암호키를 출력하는 장점을 가지고 있지만 구현상의 어려움과 출력속도면의 저조로 인하여 현대암호시스템과 결합하는 형태로 연구되고 있는 실정이다. 또한 양자암호와 현대암호의 대표주자인 RSA공개키 암호방식의 상호 보완적인 구조로 이중키 생성이 활발히 연구되고 있다[1].

KIST는 2013년 25km 떨어진 송/수신자가 비밀키를 나누어 가질 수 있는 BB84 프로토콜을 구현 성공 하였으며 유럽에서는 현재 100km 이상 떨어진 곳의 양자비밀통신이 성공하였다. 2011년 캐나다와 미국에서는 국방, 제약 및 생명공학 분야에 양자컴퓨터와 양자통신을 접목할 것에 대한 연구가 활발히 진행되고 있으며 중국은 2015년 북경에서 상하이까지 양자 암호 네트워크를 구축하였다.

QKD시스템에서 가장 중요한 부품중 하나는 광자단일검출기이다. 광자단일검출기는 전류의 노이즈를 최소화하기 위하여 동작 시간에 대한 제어가 가장 중요하다. 현재 광자단일 검출기는 나노초 단위로 동작시간을 최소화 시켰다[2].

본고에서는 나노초 단위의 동작시간 검출에 더불어 시간지연현상의 검출도 또한 나노초 단위로 진행 될 것이라는 예측 하에서 양자비밀직접통신 시스템을 설계하였다.

2장에서 양자통신의 기본이론인 BB84 프로토콜을 살펴보고 여러 가지 양자비밀직접통신의 한 종류인 2채널방식 프로토콜을 살펴본다. 3장에서 제안하는 시간지연효과를 이용한 양자비밀직접통신 프로토콜을 제안하고 4장에서 결론을 맺는다.

Ⅱ. 양자통신

양자통신은 크게 양자키 전송과 양자평문전송으로 나뉠 수 있다. 양자키 전송은 양자역학의 불확정성을 이용하여 공격자의 가로채기 공격의 징후를 파악할 수 있는 전송 방식이다. RSA 공개키 암호화 기법의 계산 복잡도에 의한 안전도는 양자컴퓨터의 지수급수에 의한 계산 단축으로 미래 보안환경의 안전성을 보장 할 수 없게 됐다. 이를 대체하기 위한 키전송 프로토콜의 일환으로 양자키 전송 프로토콜이 개발되었다. 양자키 전송 프로토콜은 양자역학의 불확정성을 이용한 BB84 프로토콜과 양자얽힘의 성질을 이용한 E91프로토콜로 양분해 볼 수 있다 [3].

양자평문전송 프로토콜을 현재 활발히 연구되고 있는 분야중 하나이며 다채널을 이용한 프로토콜과 경로분배를 이용한 프로토콜등 여러 방향으로 개발이 진행되고 있다[4-9]. 본고에서는 BB84 프로토콜과 양자평문전송에서 2채널을 이용한 프로토콜을 살펴본다.

2.1. BB84 protocol

양자역학의 불확정성을 이용한 키전송 프로토콜은 도청자의 유무를 파악할 수 있기에 새로운 암호이론으로 각광받고 있다. 편광된 광자를 이용하는 양자암호방식은 베넷(C. H. Bennett)과 브라사드(G. Brassard)에 의해 1984년에 제안된 이후 두 사람의 이니셜을 따서 BB84라 명명하였다. BB84 프로토콜은 양자역학의 관측이론과 OTP(One Time Pad, OTP) 암호 방식을 결합하여 해독이 불가능하게 만든 암호 방식이다.

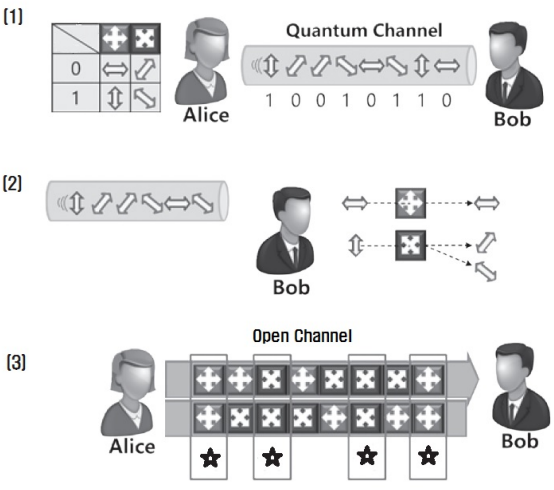

Fig. 1 BB84 protocol

가로와 세로로 편광된 $|\leftrightarrow\rangle$와 $|\updownarrow\rangle$상태, 대각방향 $+45^\circ$와 -45°로 편광된 $|\nearrow\rangle$와 $|\nwarrow\rangle$상태 등 총 네 종류의 편광을 사용한다.

그림 1의 (1)에서 보는 바와 같이 직선편광과 대각방향 편광을 이용하여 비트를 표현한다. 엘리스와 밥 간의 통신은 비트를 편광에 의해 표현된 신호를 이용한다. (2)에서 양자화된 편광을 광통신을 이용하여 전송한다. 전송단계에서 공격자 이브는 가로채기 공격이나 위변조 공격을 가할 수 있으나 양자상태의 불확정성에 의하여 송수신되는 편광을 복사할 수 없다. (3)에서 전송된 편광을 임의의 편광 검출기로 검출하여 공격징후를 파악한다.

논리의 흐름은 다음과 같다.

① 엘리스는 $\oplus$와 $\otimes$편광필터를 랜덤하게 선택하여 0과 1이 무작위로 배열된 4n 비트 데이터를 송신한다.

② 밥은 $\oplus$와 $\otimes$편광검출기를 무작위로 택하여 편광방향을 관측한다. 엘리스는 밥에게 자신이 선택한 편광필터의 배열 순서를 오픈채널을 통해 알린다.

③ 그림 1의 (3)에서처럼 검출기의 $\oplus$와 $\otimes$ 종류와 엘리스의 편광필터 $\oplus$와 $\otimes$가 일치하는 경우만 인정하고 나머지는 버린다. 편광필터와 편광검출기가 일치할 확률은 $\frac{1}{2}$이므로 2n비트의 동일한 데이터를 공유하게 된다. 그중 n비트의 데이터를 상호 조합하여 확인하고 나머지 n비트를 이용하여 OTP를 만든다.

④ 엘리스는 n비트의 OTP를 이용하여 암호화 하고 이를 밥에게 보낸다.

⑤ 밥은 받은 암호문을 공유하는 OTP로 해독한다. 가로 세로 편광상태는 검출기의 대각편광으로 검출을 하면 $\frac{1}{2}$의 확률로 대각편광상태로 관측된다. 만약 중간에 공격자가 가로채기를 하고 다시 밥에게 신호를 보낸다면 이는 $\frac{1}{4}$이상의 오류를 보여주게 된다. 오류 상태가 정상적인 확률로 도출 되지 않을 때는 송수신된 모든 데이터를 패기 하고 안전한 채널을 이용하여 다시 시작한다.

2.2. 양자 직접통신 프로토콜

양자키전송의 키분배 효율은 고전암호에 비하면 상당히 미약한 편이다. 그러한 이유로 양자 키전송은 OTP를 적절히 포기하고 QKD의 안전성을 담보로 한 키전송에만 치중할 가능성이 농후하다. 그로인해 양자보안 직접통신(Quantum Secure Direct Community, QKDC) 즉 키분배 없이 양자데이터를 암호화하고 복호화 하여 키를 사용하지 않고 직접 평문전송을 하는 알고리즘이 활발히 연구되었다. 대부분 QSDC의 연구는 양자얽힘과 양자메모리에 기반한 연구가 주를 이루고 있다. 양자메모리는 기술 발전이 초보적 단계에 머물러 있어 구현이 힘들다.

BB84 프로토콜의 사용자 인증기법을 이용한 2채널 방식 QSDC를 살펴보자. 표 1은 1라운드와 2라운드로 진행되는 양자상태와 비트도출의 예를 보여준다.
통신상의 data흐름에 대한 논리 진행은 다음과 같다.

Table. 1 1 round and 2 round data flowchart of 2 channel QSDC

	1	⋯	60	61	⋯	127	128
Alice	0	⋯	1	1	⋯	0	0
	$\oplus$	⋯	$\oplus$	$\otimes$	⋯	$\oplus$	$\otimes$
	$\|\updownarrow\rangle$	⋯	$\|\leftrightarrow\rangle$	$\|\nearrow\rangle$	⋯	$\|\updownarrow\rangle$	$\|\nwarrow\rangle$
Bob	$\oplus$	⋯	$\oplus$	$\oplus$	⋯	$\oplus$	$\oplus$
	$\|\updownarrow\rangle$	⋯	$\|\leftrightarrow\rangle$		⋯	$\|\updownarrow\rangle$	$\|\updownarrow\rangle$
	0	⋯	1	1	⋯	0	0
concurrence	T	⋯	T	F	⋯	T	F
bit	0	⋯	1		⋯	0	
2 round							
Bob	$\otimes$	⋯	$\otimes$	$\otimes$	⋯	$\otimes$	$\otimes$
		⋯		$\|\nwarrow\rangle$	⋯		$\|\nwarrow\rangle$
		⋯		0	⋯		0
concurrence	F	⋯	F	T	⋯	F	T
bit		⋯		0	⋯		0

① 엘리스는 평문 64비트와 난수 64비트를 연결하여 생성한다.

② 표 1의 엘리스가 보내는 난수열을 이용한 편광기로 양자화 하여 128비트 광자를 전송한다.

③ 표 1의 1라운드 시행에서 밥은 128개의 + 편광기로 양자검출 한다.

④ 밥은 검출된 비트에서 난수부분은 데이터와 편광기

를 공개하고 평문부분은 저장한다.

⑤ 엘리스는 난수부분 64비트의 데이터와 전체 편광기를 공개한다.

⑥ 공개채널에서 밥과 엘리스의 일치한 편광에 대한 데이터를 비교하고 일치하지 않는 데이터는 버린다. 이후 공격징후가 없으면 2라운드를 진행한다.

⑦ 1라운드와 동일하게 엘리스는 난수 64비트와 동일 평문 64비트를 난수편광 64개와 2라운드 동일 편광 64개로 평문 양자화 한 후 전송한다.

⑧ 표 1의 2라운드 밥에서처럼 128개의 ⊗편광기로 검출한다.

⑨ 엘리스와 밥은 난수부분의 데이터와 편광기를 공개하여 공격징후를 확인한다.

⑩ 평문부분 64비트를 저장 후 4단계와 병합하여 평문 저장한다.

Ⅲ. 시간지연을 이용한 QSDC

3.1. 시간지연

아인슈타인의 일반 상대성 원리에 의하여 중력과 관성계의 속도에 대한 시간지연현상은 현대물리학의 자연스런 현상으로 인식된다. 광원에서 진행된 파형이 목적지에 도달하는데 걸리는 시간은 진행경로에 따라 차이가 생긴다. 시간차의 원인은 시공간의 왜곡에 의한 중력렌즈 현상에 의해 중력렌즈 평면을 통과하면서 중력 포텐샬 차로 인해 생성된다. 기하학적 광경로 차로 인한 시간지연은 식(1)의 t_g로 나타낼 수 있는데 여기서 중력렌즈현상의 허상 두 개를 A와 B라 하였고 α_A는 A상에 대한 충격 매개변수에 대한 빛의 편향 각(deflection algle)이고 α_B는 B상에 대한 빛의 편향각이다.

$$t_g = \frac{1}{2}(\alpha_A^2 - \alpha_B^2) \tag{1}$$

중력렌즈 평면의 포텐셜 차에 의한 시간 지연은 식(2)와 식(3)과 같이 t_p로 표현할 수 있다.여기서 식(3)은 중력렌즈가 점질량인 경우를 나타낸다. G는 만유인력 상수이고 c는 빛의 속도, M은 중력렌즈의 질량, r은 impact parameter 이다.

$$t_p = \frac{4G}{c^2}\int_{r_B}^{r_A}\frac{M(r)}{r}dr \tag{2}$$

$$t_p = \frac{4G}{c^2}\ln\left(\frac{r_A}{r_B}\right) \tag{3}$$

따라서 총 시간지연 은 식(4) Δt로 나타낼 수 있다.

$$\Delta t = t_g + t_p \tag{4}$$

3.2. 시간지연을 이용한 QSDC

제안하는 시스템은 2채널 방식의 QSDC에 시간지연 장치를 추가하여 수신자의 수신 상황에서 시간지연 함수에 의한 공격자 탐지를 구현하는 방식이다. 그림 2에서 보는 바와 같이 엘리스는 먼저 이중광자발생기(Double Photon Generate, DPG)를 통해 이중광자를 발생하여 편광기로 양자화 하여 전송한다. 전송 data는 2장에서 살펴본 2채널 QSDC의 규약을 따른다. 그림2의 (2)번 채널로 전송되는 양자라인에 시간지연 발생함수를 적용하여 (2)번 채널의 시간지연을 유도한다. 밥은 수신방식에서 (1)번 채널과 (2)번 채널의 시간간극을 측정하여 공격자 탐지를 수행할 수 있고 또한 BB84프로토콜의 안정성을 동시에 확보 할 수 있다.

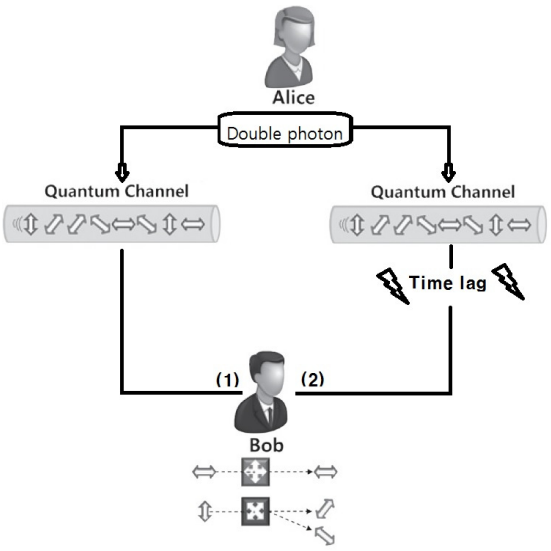

Fig. 2 QSDC using Time lag

그림 2에서 보는바와 같이 2번째 채널에 전송되는 과정에서 시간지연에 의한 data 검출을 시행하는 것을 볼 수 있다. 제안하는 시간지연 효과는 중력렌즈 현상을 반영한 것으로 점질량에 의한 시간지연을 제안하였다. 원심가속도를 이용한 중력 발생기는 점질량계에 포함되며 이를 이용한 시간지연은 중력계의 변화에 의한 상관관계를 보임을 알 수 있다.

점질량에서의 시간지연 함수는

$$t_p = \frac{4G}{c^2}\ln\left(\frac{\mathrm{rA}}{\mathrm{rB}}\right) \quad (5)$$

이므로

$$G = (6.67384 \pm 0.000008)\times 10^{-11}\, Nm^2kg^{-2}$$

에 의하여

$$t_p = \frac{4 \cdot \Delta G}{c^2}\ln\left(\frac{\mathrm{rA}}{\mathrm{rB}}\right) \quad (6)$$

의 값을 가진다. 여기서 ΔG에 의한 변이를 충족시키기 위하여 원심가중력에 의해 10G를 생성하였다면

$$\frac{4\times 10G}{c^2}\ln\left(\frac{\mathrm{rA}}{\mathrm{rB}}\right) = 10\times\frac{4\mathrm{G}}{\mathrm{c}^2}\ln\left(\frac{\mathrm{rA}}{\mathrm{rB}}\right) = 10t_p \quad (7)$$

가 되어

$$\Delta t = t_g + 10t_p \quad (8)$$

으로 도출되게 된다. 즉 가중력에 의한 시간지연 값을 산출하게 된다.

시간지연을 생성하는 발생장치로는 원심가속도를 이용한 중력발생기와 가중질량을 이용한 중력발생기 등을 들 수 있는데 본고에서는 다루지 않았다. 양자통신과 양자컴퓨터의 구현에서 가장 중요한 시간간극측정에 대한 연구가 활발히 진행되어지고 있는 시점에 나노초 단위의 시간간극을 측정하는 일을 병행해서 연구되고 있다.

Table. 2 QSDC data flowchart using time lag

	1	⋯	60	61	⋯	127	128
Alice	0	⋯	1	1	⋯	0	0
	⊕	⋯	⊕	⊗	⋯	⊕	⊗
	$\|\updownarrow\rangle$	⋯	$\|\leftrightarrow\rangle$	$\|\nearrow\rangle$	⋯	$\|\updownarrow\rangle$	$\|\nwarrow\rangle$
Bob	⊕	⋯	⊕	⊕	⋯	⊕	⊕
	$\|\updownarrow\rangle$	⋯	$\|\leftrightarrow\rangle$		⋯	$\|\updownarrow\rangle$	$\|\updownarrow\rangle$
	0	⋯	1	1	⋯	0	0
concurrence	T	⋯	T	F	⋯	T	F
bit	0	⋯	1		⋯	0	
After time lag							
Bob	⊗	⋯	⊗	⊗	⋯	⊗	⊗
		⋯		$\|\nwarrow\rangle$	⋯		$\|\nwarrow\rangle$
		⋯		0	⋯		0
concurrence	F	⋯	F	T	⋯	F	T
bit		⋯		0	⋯		0

시간지연을 이용한 QSDC의 논리 진행은 표2의 데이터 흐름도를 이용해 설명하면 다음과 같다.

① 엘리스는 평문 64비트와 난수 64비트를 연결하여 128비트 전송 데이터를 생성한다.

② 표 2의 엘리스가 보내는 난수열은 송신자의 편광기로 양자화 하여 128비트 광자를 이중광자발생기에 의해 2채널로 전송한다.

③ 표 2의 첫 번째 시행에서 밥은 2채널 QSDC에서와 마찬가지로 128개의 + 편광기로 양자검출 한다.

④ 밥은 검출된 비트에서 난수부분은 데이터와 편광기를 공개된 채널에 공개하고 후위 64비트의 평문부분은 저장한다.

⑤ 엘리스는 난수부분 64비트의 데이터와 전체 편광기를 공개채널에 공개한다.

⑥ 공개채널에서 밥과 엘리스의 일치한 편광에 대한 데이터를 비교하고 일치하지 않는 데이터는 버린다. 동시에 시간간극을 측정하여 시간지연 함수의 시간간극과 측정시간 간극에 오차를 비교한 후 허용범위 안의 시간간극이라면 공격징후가 없는 것으로 간주하여 데이터를 저장한다.

⑦ (1)번 채널과 동일하게 엘리스는 난수 64비트와 동일 평문 64비트를 난수편광 64개와 (2)번 채널 동일 편광 64개로 평문 양자화 한 후 전송한다.
⑧ 표 2의 (2)번 채널 밥에서처럼 128개의 ⊗ 편광기로 검출한다.
⑨ 평문부분 64비트를 저장 후 4단계와 병합하여 평문 저장한다.

Ⅳ. 결 론

현대의 관용키암호와 공개키 암호의 공통적인 안전성은 계산복잡도에 근간한 계산 시간에 의존한다. 양자컴퓨터의 출현으로 인해 지수급수적인 계산시간 단축은 현대암호의 근간을 흔들어 놓았다. 양자컴퓨터시대의 암호알고리즘으로 양자이론의 불확정성을 근간으로 하는 양자암호가 설계되었다. 이러한 양자암호는 편광을 이용한 빛의 양자성을 이용하는 BB84스타일 암호와 양자얽힘을 이용하는 E91스타일 암호가 연구되었다. BB84 알고리즘과 E91 알고리즘은 둘 다 현대의 공개키 암호기법을 대체할 수단으로 암호키 전송 프로토콜로 연구되었으나 프로토콜의 비효율성에 의하여 현대암호와 병합으로 사용되어지는 방법으로 연구가 진행되고 있다. 본고에서는 이러한 암호키전송 알고리즘이 아닌 양자비밀직접전송 방식을 채택하여 평문에 대한 양자암호 전송 시스템을 제안하였다. 기존 양자비밀직접전송 방식중 2채널 방식을 개선하여 이중광자 생성기를 이용한 전송을 설계하였다. 또한 양자통신망의 한 개 채널에 아인슈타인의 중력장에 의한 시간지연함수를 적용하여 주어진 시간지연 함수의 지연시간에 대한 나노초 단위의 검출로 공격자의 공격여부를 탐지하고 또한 알려진 BB84프로토콜의 안전도도 또한 계승하였다. 향후 나노시간검출과 중력장에 대한 연구가 더 진행되면 보다 안정적인 암호 알고리즘으로 사용되리라 생각된다.

ACKNOWLEDGMENTS

D.H. Lim was supported by the Sehan University research fund(2017)

REFERENCES

[1] H. J. Park, M. Y. Bae, J. S. Kang. and Y. J. Yeom, “Key derivation functions using the dual key agreement based on QKD and RSA cryptosystem,” *Journal of The Korean Institute of Communication Sciences*, vol. 41, no. 4, pp. 479-488, Apr. 2016.

[2] S. U. Han, B. K. Park, Y. S. Kim. and S. U. Mun, “New concept of physical layer security communication technology, quantum secure community,” *Journal of The Korean Institute of Communication Sciences*, vol. 31, no. 6, pp. 46-52, May 2014.

[3] C. H. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin tossing,” *In proceedings of IEEE INternational Conference on Computers, Systems and Signal Processing*, Bangalore, India , p.175-179, 1984.

[4] J. J. Seol. K. C. Rim. “Using double photon transmission of quantum cryptography.” *Journal of the korea Institute of Information and Communication Engineering*, vol. 17. no. 8. pp. 1857-1864. Aug. 2013.

[5] J. H. Min. J. H. Bang, and B. S. Ham, “A security enhanced quantum secure direct communication protocol,” *in Proceedings of Symposium of the Korean Institute of communications and Imformation Sciences*, Hiwon, pp. 496-497, 2016.

[6] A. Meslouhi. Y. Hassouni. “A quantum secure direct communication protocol using entangled modified spin coherent states,” *Quantum Information Process*, vol. 12, no. 7, pp. 2603-2621, Jul. 2013.

[7] J. Li. D. J. Song. R. Li. and X. Lu. “A quantum secure direct communication protocol based on four-qubit cluster state,” *Security and Communication Networks*, vol. 8, no. 1, pp. 36-42, Jan. 2015.

[8] A. Farouk. M. Zakaria. A. Megahed. and F. A. Omara. “A generalized architecture of quantum seure direct communication for N disjointed users with authentication,” Nature Scientific Reports, Sci-16080, 2015.

[9] S. Madhavi, “Secured Data Aggregation Scheduling in Ubiquitous Quantum Sensor Networks”, *Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology*, vol. 4, no. 1, pp.17-30, June 2014.

임광철(Kwang-Cheol Rim)

조선대학교 수학과 이학박사
※관심분야 : 응용수학, 정보보안, 양자암호, 양자정보통신

임동호(Dong-Ho Lim)

한국외국어대학교 수학과 이학박사
※관심분야 : 응용수학, 다양체론, 양자암호, 개인인증