JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 17, No. 8 : 1857~1864, August. 2013

이중광자 전송을 통한 양자비밀통신

설정자[1] · 임광철[2*]

Using Double Photon Transmission of Quantum Cryptography

Jung-ja Seol[1] · Kwang-cheol Rim[2*]

[1] Department of Computer Engineering, Chosun University, Gwangju 230-7381, Korea
[2] Department of Mathmatics, Chosun University, Gwangju 230-6610, Korea

요 약

본 논문에서는 양자암호 시스템을 개선하여 이중 광자전송을 이용한 사용자 비밀 평문 교환을 구현하는 알고리즘을 설계하였다. 기존 양자암호 알고리즘에서는 주로 키전송 프로토콜로써의 양자 암호 시스템을 사용하였으나 본고에서는 이를 보다 개선하여 이중 광자 전송 방식을 통한 양자 평문 전송 알고리즘을 재안한다.

ABSTRACT

In this paper, we improve the quantum cryptography system using a dual photon transmission plaintext user password algorithmwas designed to implementthe exchange. Existing quantum cryptographic key transport protocols, algorithms, mainly as a quantum cryptography system using the paper, but it improved the way the dual photon transmission through the quantum algorithm re not getting transmitted plaintext.

키워드 : 암호화/복호화, 양자암호, 양자평문전송

Key word : encryption/decryption, quantum cryptography, quantum mean text transfort

접수일자 : 2013. 06. 07 심사완료일자 : 2013. 07. 01 게재확정일자 : 2013. 07. 11

*** Corresponding Author** Kwang-cheol Rim (E-mail:rim1201@hanmail.net, Tel:+82-62-230-6610)
Department of Mathmatics, Chosun University, Gwangju 230-6610, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2013.17.8.1857 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

인류의 가장 대표적인 실적은 문자와 기록에 있다고 볼 수 있다. 문자와 기록은 자신의 정보를 타인과 공유하고 서로의 정보를 서로의 목적에 맞게 수정하고 또다시 이를 공유하는 과정에서 정보기술과 문명은 동일하게 발달하였다. 이후 정보전송은 인류사에서 빼놓을 수 없는 커다란 획을 장식한다. 현대사회에서의 정보는 단순히 공유차원이 아닌 가공, 보존, 습득 등 여러 가지 형태로 변화하여 사용되고 있는 실정이다. 정보는 재산과 권력의 유지에 필요불가결한 요소로 작용하며 이를 소유하고 공유하는 과정에서 다른이들의 정보접근을 차단하기 위한 방편으로 암호학이 탄생하였다.

암호학의 발달 과정은 고전에는 주로 단순한 문자를 대입하고 이를 치환하여 정보를 은닉하였다. 하지만 문장에 나타나는 문자들의 통계적 특성을 그대로 나타내기에 암호문의 통계적 특성을 분석하여 암호문을 해독할 수 있었다. 이후 복잡한 기계를 이용하여 암호문을 작성하였는데 이를 해독하기 위해서는 많은 양의 계산을 필요로 하였기에 안전한 시스템이라 볼 수 있었다. 그러나 현대와 같이 정보전산능력이 뛰어난 시기에는 그도 또한 쉽게 해독할 수 있다. 이후 Shannon에 의해 복잡도가 높은 암호 알고리즘의 실현이 가능하게 되었고 현대 암호학의 기본 토대를 형성하게 되었다.[8]

현대암호는 크게 대칭키 암호시스템과 공개키 암호시스템으로 나눌 수가 있다. 1970년대 초 Shannon에 의해 주장된 혼돈(confusion)과 확산(diffusion)을 여러 번 반복하면 강력한 암호 알고리즘을 구현할 수 있다는 이론에 의해 미국의 표준암호 알고리즘인 미국 상무성 표준국(NBS : National Bureau of Standard 후에 NIST : National Institute of Standards and Technology)은 Brooks ACT 89-306에 따라 암호 표준화 연구를 시작하였다. 미국 상무성은 1973년 5월 다음 8가지 조건 즉

- 표준 암호 알고리즘은 높은 수준의 안전성을 보장할 수 있어야 한다.
- 사양의 정의가 완전하여 쉽게 이해할 수 있어야 한다.
- 알고리즘의 비밀성에 의존 되어서는 안된다.
- 사용자나 제작자가 모두 사용 가능해야 한다.
- 표준 암호 알고리즘의 응용이 다양해야 한다.
- 전자 장치로써 제품화가 간단해야한다.
- 사용이 간단해야 한다.
- 알고리즘 타당성 검증에 협력해야 한다.
- 표준 암호 알고리즘은 수출할 수 있어야 한다.

위와 같은 전제로 표준 암호 알고리즘을 공모하여 DES(data encryption standard)가 IBM에 의해 제안되어 많은 기간 사용되었으며 이후 AES로 발전하였다.[2,3,4,5,6]

원타임 패드(one-time pad)와 유사한 안전성을 보장하며 일반적인 통신망에도 적용할 수 있는 암호 알고리즘으로 스트림 암호 시스템이 있는데 이는 난수를 생성하여 평문과 일대 일로 대칭하여 암복호화하는 방식이다. 이것 또한 엄밀한 의미에서 대칭 키 암호 알고리즘으로 볼 수 있다. 대칭 키 암호 알고리즘은 일단 키를 송신자와 수신자가 똑같이 나누어 가져야 한다는 불편이 있다. 이를 해소하기 위하여 암호화와 복호화 과정에서 서로 다른 키를 사용하고 암호화 키를 공개하여 키의 전송 및 비밀 보관 등이 필요없게 만든 것이 공개키 암호 시스템이다. 이는 1976년 Diffe와 Hellman의 연구 [New Directions in Cryptography]에 발표가 되었다. 이도 또한 발전을 거쳐서 현재 RSA, ElGamal, 타원곡선 암호, 땋임군 암호 등이 나와 있으나 계산량이 너무 많기 때문에 일반 평문에 대한 암호화는 힘들고 주로 키 분배 알고리즘과 짧은 길이의 데이타에 대해 사용되고 있는 실정이다.[7,8,9,10]

공개키 암호화기법은 소인수분해의 시간적 제약으로 인한 안전도를 확보한 것이다. 약 128자리 이상의 소수에 대하여 현존하는 소인수분해 알고리즘으로는 매우 많은 시간을 요구한다. 하지만 쇼알고리즘에 의하여 양자컴퓨터의 구현은 공개키 암호화 기법에서 주요 변수로 적용되는 시간제약을 양자이론을 이용한 소인수분해 알고리즘으로 해결하였다. 아직 양자 컴퓨터의 개발 소식은 전해지지 않고 있지만 이미 각국에서 상당히 많은 예산과 인력을 투입하여 진행하고 있는 상황이므로 그리 멀지 않은 시점에 양자 컴퓨터의 구현을 볼 것이라 예상된다.

본고에서는 이러한 기술의 발달 과정에 대하여 양자암호 시스템의 기본성질과 원리를 살펴보고 이러한 양자암호 시대에 알맞은 양자 평문전송방식에 대하여 제안한다. 양자 암호이론은 주로 비밀키 전송에 틀을 세워서 설계 되었는데 양자 평문전송 알고리즘은 비밀키

전송의 양자중첩원리를 이용한 양자 평문전송 방식에 대하여 수학적 안전도를 입증한 상태로 설계하였다.

Ⅱ. 양자암호시스템

2.1. BB84 프로토콜

암호용 키 분배는 크게 두가지로 볼 수 있다. 비밀키를 담당자에게 배포하여 관리하는 것과 공개키분배방식이다. 전자는 사람에 대한 신뢰를 믿을 수가 없으며 후자는 소인수분해의 해법이 완성되면 안전성을 보장할 수 가 없다. 양자컴퓨터를 이용한 쇼의 소인수분해 알고리즘이 상용화되면 RSA공개키 암호기법은 근본적인 안정성에 문제가 발생한다. 양자역학의 불확정성을 이용한 키분배방식은 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 두사람의 이니셜을 따서 BB84라 명명하였다. BB84 프로토콜은 양자역학의 관측이론과 원타임 패드 암호 방식을 결합하여 해독이 불가능하게 만든 암호 방식이다.[1,11] 가로와 세로로 직선편광된 $|\leftrightarrow\rangle$와 $|\updownarrow\rangle$상태, 대각방향 $+45^\circ$와 -45°로 편광된 $|\nearrow\rangle$와 $|\nwarrow\rangle$상태 등 총 네 종류의 광을 사용한다.

표 1. 편광된광자의 이진 대응표
Table. 1 binary table of polarizing photon

비트값	$\oplus$	$\otimes$
0	$\|\updownarrow\rangle$	$\|\nwarrow\rangle$
1	$\|\leftrightarrow\rangle$	$\|\nearrow\rangle$

엘리스와 밥이 가로, 세로의 직선편광 광자와 대각선의 직선 편광 광자를 동시에 이용한다. 엘리스는 $\oplus$와 $\otimes$ 두 종류의 편광필터를 무작위로 사용하여 비트를 송신하고 밥도 두 종류의 검출기를 무작위로 사용하여 광을 검출한다. BB84의 프로토콜은 다음과 같다.

- 엘리스는 $\oplus$와 $\otimes$편광필터를 무작위로 선택하여 0과 1이 무작위로 배열된 4n 비트 데이터를 송신한다.
- 밥은 $\oplus$와 $\otimes$편광검출기를 무작위로 택하여 편광방향을 관측한다. 엘리스는 밥에게 자신이 선택한 편광필터의 배열순서를 공개된채널을 통해 알린다.
- 두 사람은 검출기의 $\oplus$와 $\otimes$ 종류와 엘리스의 편광필터 $\oplus$와 $\otimes$가 일치하는 경우만 참값으로 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 원타임패드를 만든다.
- 엘리스는 평문을 n비트의 원타임패드를 이용하여 암호화 하고 이를 밥에게 보낸다.
- 밥은 받은 암호문을 공유하는 원타임패드로 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 정상적이지 않을 때는 첫 단계부터 다시 편광을 보내서 시작하면 된다.

<표2>에서 나타난바와 같이 엘리스가 보내는 데이터에는 보내고자 하는 송신 비트들을 이진 비트가 아닌 편광 형태로 변형하여 무작위 선택한 편광기를 사용한다. 중간에 도청자가 새로운 검출기를 사용하여 편광을 복사하는것은 이론상 불가능하므로 도청에 의한 편광 복사는 존재할 수가 없다. 다만 엘리스와 밥이 사용하는 송신 비트와 편광기 선택 비트 그리고 밥이 선택하는 검출기 선택비트들에서 실난수 사용상의 애로점으로 인하여 의사난수를 사용하므로 man-in-the-middle attack에 대한 부분정보 유출에대한 애로점은 존재한다고 볼 수 있다. BB84 프로토콜에 의하여 n개의 비트 값을 관찰하고 도청자를 발견할 확률은 각각의 비트들이 난수성을 확보했다는 가정하에 다음과 같은 계산결과를 볼 수 있다.

$$P(n) = 1 - \left(\frac{3}{4}\right)^n \tag{1}$$

이는 비트수가 많은 수록 도청자의 유무를 판별하기가 수월해진다.

표 2. 편BB84 데이터 흐름도
Table. 2 data flowchart of BB84 protocol

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
엘리스	송신 비트	0	1	1	0	1	1	1	0	0	0	1	0	0	1	1	1	0	1	0	0
	필터	⊕	⊗	⊕	⊗	⊕	⊕	⊗	⊕	⊕	⊕	⊕	⊗	⊗	⊕	⊗	⊕	⊗	⊗	⊕	⊗
	상태	$\|\updownarrow\rangle$	$\|\nearrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nwarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nearrow\rangle$	$\|\updownarrow\rangle$	$\|\updownarrow\rangle$	$\|\updownarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nwarrow\rangle$	$\|\nwarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nearrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nwarrow\rangle$	$\|\nearrow\rangle$	$\|\updownarrow\rangle$	$\|\nwarrow\rangle$

밥	검출	⊕	⊕	⊗	⊗	⊕	⊕	⊗	⊕	⊗	⊗	⊗	⊕	⊕	⊗	⊕	⊗	⊗	⊗	⊕	⊕
	관측	$\|\updownarrow\rangle$	$\|\updownarrow\rangle$	$\|\nearrow\rangle$	$\|\nwarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nearrow\rangle$	$\|\updownarrow\rangle$	$\|\nearrow\rangle$	$\|\nearrow\rangle$	$\|\nearrow\rangle$	$\|\updownarrow\rangle$	$\|\updownarrow\rangle$	$\|\nearrow\rangle$	$\|\updownarrow\rangle$	$\|\nearrow\rangle$	$\|\nwarrow\rangle$	$\|\nearrow\rangle$	$\|\updownarrow\rangle$	$\|\updownarrow\rangle$
	비트	0	0	1	0	1	1	1	0	1	1	1	0	0	1	0	1	0	1	0	0

일치	T	F	F	T	T	T	T	T	F	F	F	F	F	F	F	F	T	T	T	F
원타임	0			0	1	1	1	0									0	1	0	

2.2. E91프로토콜

BB84 프로토콜이나 B92 프로토콜은 서로 직교하지 않는 양자상태는 복제불능이라는 이론에 의해 안전성이 보증된 비밀열쇠 분배법이다. 이들 두 프로토콜에는 양자역학의 불확정성 관계가 본질적 역할을 하고있다. 두 입자가 상관된(entangled) 양자상태 즉 EPR쌍을 이용하여 암호 열쇠를 안전하게 분배할 수 있다.

E91 프로토콜의 경우 송신자 와 수신자 는 스핀 0으로 결합한 두 입자계, EPR 쌍을 관측한다. EPR 쌍은 스핀 $\frac{1}{2}$ 인 입자를 이용하면

$$|\Psi>_{12}=\frac{1}{\sqrt{2}}\{|\uparrow>_1|\downarrow>_2-|\downarrow>_1|\uparrow>_2\} \quad (2)$$

과 같이 된다. EPR 쌍은 두 개의 광자로도 만들어질 수 있다. EPR 쌍은 z축 반대방향으로 발사되며 송신자와 수신자는 서로 떨어진 장소에서 각 각의 편광 검출기로 한 개의 입자의 스핀 방향을 관측한다. 단위 벡터 a_i와 b_j $(i=1,2,3)$ 로 검출기의 방향을 표시하며 이 두 단위 벡터가 z축에 수직한 xy평면에 위치하게 한다. 송신자가 a_i의 검출기를 이용하고 수신자는 b_j검출기를 이용하여 스핀의 방향을 측정하면 상행인 +방향과 하향인 -방향의 상관식은 다음과 같다.

$$\begin{aligned} E(a_i,b_j) &= E_{++}(a_i,b_j)+E_{--}(a_i,b_j) \\ &\quad -E_{+-}(a_i,b_j)-E_{-+}(a_i,b_j) \\ &= -(a_i,b_j) \end{aligned} \quad (3)$$

과 같이 a_i와 b_j의 내적으로 주어진다.

벨의 부등식의 한 종류인 CHSH 부등식(Clauser, Horne, Shimony, Holt 부등식) 을 유도하기 위해 상관함수

$$S=E(a_1,b_1)-E(a_1,b_3)+E(a_3,b_1)+E(a_3,b_3) \quad (4)$$

을 생각하자. 위 식을 구하려면 송신자와 수신자가 다른 방향에서 EPR 쌍을 지정된 방향으로 4회 측정해야 된다. 양자역학적 관측결과는

$$\begin{aligned} S_{QM}= & -\cos(\phi_1-\theta_1)+\cos(\phi_1-\theta_3) \\ & -\cos(\phi_3-\theta_1)-\cos(\phi_3-\theta_3) \end{aligned} \quad (5)$$

로 주어지며, E91 프로토콜은 다음과 같다.

단계 1 : 송신자와 수신자는 EPR 쌍을 측정기를 이용하여 관측한다.

단계 2 : 송신자와 수신자는 검출기 방향을 공개하고 측정결과를

(a) 다른 방향의 검출기를 이용한 결과

(b) 같은 방향의 검출기를 이용한 결과

의 두 종류로 분류한다.

단계3 : 송신자와 수신자는 (a) 그룹에 속하는 결과만 공개하고 CHSH 부등식 S가 만족되는지를 확인한다.

단계4 : CHSH 부등식 $S=-2\sqrt{2}$ 가 만족되는 경우에만 (b) 그룹의 결과를 원타임 패드용 비밀열쇠로

사용한다.

EPR 쌍의 관측결과로부터 송신자와 수신자는 E91 프로토콜에 의해 비밀 열쇠를 분배했다고 하자. 도청자가 E91 프로토콜을 부수고 비밀열쇠를 훔치고자 할 때 CHSH 부등식은 어떻게 변화하는가가 문제이다. 도청자가 EPR 쌍으로부터 정보를 훔치려고 할 경우의 CHSH 부등식을 유도해 보자. E91 프로트콜의 제 1 특징은 도청자가 가령 송신자와 수신자가 관측하고자 하는 모든 EPR 쌍을 관측하였다 하더라도 어떤 정보도 얻을 수 없다는 것이다. 즉 비밀열쇠인 EPR 쌍 자체가 아니라 송신자와 수신자가 이 관측을 한 후 단계 2의 (b) 데이터만을 선택하여 만들어지기 때문이다. 도청자가 암호열쇠의 정보를 얻으려면 EPR 쌍을 관측한 후 다시 EPR 쌍을 송신자와 수신자에게 발신하여 두 사람의 검출기 종류를 알아야 한다. 그래서 도청자는 두 대의 검출기 $A,\ B$ 를 이용하여 ϕ_A와 θ_B 방향에서 EPR쌍의 스핀을 관측하고 그 관측한 스핀과 같은 방향으로 다시 두 개의 입자를 발신한다고 생각해 보자. 도청자가 ϕ_A와 θ_B방향을 임의 확률 $P(\phi_A,\theta_B)=|a(\phi_A,\ \theta_B)|^2$ 로 택했다고 할 때 발신된 두 입자의 상태는 진폭 $a(\phi_A,\ \theta_B)$ 를 이용하여

$$|\Psi(A,\,B)\geqq\int_0^{2\pi}d\phi_A\int_0^{2\pi}d\theta_B\,a(\phi_A,\theta_B)|\phi_A>_1|\theta_B>_2 \tag{6}$$

로 표현된다.

여기서 직교규격화 되어있으므로 $|\Psi(A,\,B)>$ 도

$$<\Psi(A,\,B)|\Psi(A,\,B)> =\int_0^{2\pi}\int_0^{2\pi}|a(\phi_A,\theta_b)|^2d\phi_Ad\theta_B=1 \tag{7}$$

로 규격화 된다. 도청자가 발신한 $|\phi_A>$, $|\theta_B>$ 상태를 송신자와 수신자는 검출기 a와 b를 이용하여 그 스핀방향을 관측한다면 도청자가 존재하는 경우

$$E'(a,b)=\iint p(\phi_A,\theta_B)\cos(\phi-\phi_A)\cos(\theta-\theta_B)d\theta_Ad\theta_B \tag{8}$$

로 표현된다.

도청자가 도청한 결과 상관함수는

$$-\sqrt{2}\leq S'\leq\sqrt{2} \tag{9}$$

으로 되며 양자역학의 원리로부터 유도된 결과인 $S_{QM}=-2\sqrt{2}$ 와 모순이 된다. 이렇게 일반화된 벨의 정리, CHSM 부등식을 이용하여 송신자와 수신자는 도청자의 존재 여부를 알 수 있게 된다.

도청자가 EPR쌍을 관측하는 것은 스핀의 방향을 확인하려는 것이다. 즉 관측에 따라 양자역학적인 2체계 상태가 수축하여 어떤 특정 스핀방향이 정해지게 되기 때문이다. 즉 도청자가 존재하면 EPR 쌍이 교란을 받아 고전적 벨의 부등식이 성립하게 된다는 의미이다. 몇 가지 다른 방향에 있는 검출기 측정 결과로부터 도청자의 존재를 알 수 있는 이유는 “서로 얽힌”상태를 설명해 주는 양자역학의 원리를 잘 이용하기 때문이다.

Ⅲ. 이중광자 평문전송 프로토콜

BB84프로토콜이나 E91프로토콜등 양자암호 알고리즘들은 양자암호이론을 이용한 비밀키 전송 방식에 중심이 맞춰져 있다. 양자 비밀키를 이용하여 송신자와 수신자의 동기화된 비밀키로 각자의 관용키를 형성하고 이를 이용한 암호와 복호가 이루어지는 원리를 이용한다.

평문전송 프로토콜은 이러한 관용키를 사용하여 다시 평문에대한 암복호화 과정에서 중간단계 관용키 암호 생성을 생략하고 바로 전송가능한 평문 암호전달 방식에 대한 알고리즘이다.

양자평문 전송프로토콜은 양자암호의 근간이론인 복재불가능성을 이용하여 사용자 인증을 하고 동시에 양자화된 평문전송을 실현한다.

양자 비트 전송은 BB84 프로토콜에서 살펴본 것 처럼 편광기에 대한 확률적 도출을 이용하여 사용자 인증을 수행한다.

양자평문전송 프로토콜은 다음과 같은 순서로 진행된다. 편의상 송신자는 엘리스, 수신자는 밥이라 칭하고 공격자는 이브라 칭하기로 한다.

표 3. 이중광자 평문전송 1라운드 데이터 흐름도
Table. 3 1round data flowchart of double poton transform

		1	2	3	4	⋯	60	61	62	63	64	65	66	67	68	⋯	124	125	126	127	128
엘리스	송신비트	0	1	1	0	⋯	1	1	0	0	0	1	0	0	1	⋯	1	0	1	0	0
	필터	⊕	⊗	⊕	⊗	⋯	⊕	⊗	⊕	⊕	⊕	⊕	⊗	⊗	⊕	⋯	⊕	⊗	⊗	⊕	⊗
	상태	|↕〉	|↗〉	|↔〉	|↖〉	⋯	|↔〉	|↗〉	|↕〉	|↕〉	|↕〉	|↔〉	|↖〉	|↖〉	|↔〉	⋯	|↔〉	|↖〉	|↗〉	|↕〉	|↖〉
밥	검출	⊕	⊕	⊕	⊕	⋯	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⋯	⊕	⊕	⊕	⊕	⊕
	관측	|↕〉	|↕〉			⋯	|↔〉		|↕〉				|↕〉	|↕〉		⋯				|↕〉	|↕〉
	비트	0	0	1	0	⋯	1	1	0	1	1	1	0	0	1	⋯	1	0	1	0	0
일치		T	F	T	F	⋯	T	F	T	T	T	T	F	F	T	⋯	T	F	F	T	F
원타임		0		1		⋯	1		0	0	0	1			1	⋯	1			0	

- 공개채널에서 엘리스 전송필터와 전위 64비트 공개
- 공개채널에서 밥의 전위 64비트 검출필터와 검출 데이터공개
- 후위 검출 64비트 저장

단계1. 엘리스는 평문 64비트와 난수 64비트를 연결하여 생성한다.
2. 난수열을 이용한 편광기로 양자화 하여 128비트 광자를 전송한다.
3. 밥은 128개의 + 편광기로 양자검출 한다.
4. 밥은 검출된 비트에서 난수부분은 데이터와 편광기를 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 다음 진행

7. 엘리스는 난수 64비트와 동일 평문 64비트를 난수편광 64개와 2단계 동일 편광 64개로 평문 양자화 후 전송한다.
8. 밥은 128개의 X편광기로 검출한다.
9. 엘리스와 밥은 난수부분의 데이터와 편광기를 공개하여 공격징후를 확인한다.
10. 평문부분 64비트를 저장후 4단계와 병합하여 평문 저장한다.

양자비밀 평문전송 프로토콜의 공격관점에서 바라보면 전송되는 데이터는 intercept에 대한 정보노출의 최소 이어야하고 도청자의 위장 인증을 바로 감지 할 수 있어야 한다. 여기서는 intercept-resend 도청방식과 man-in-the-middle 공격에 대한 안전성을 살펴보자.

intercept-resend 공격에 대한 안전도는 (표 3)에서 보여지는 바와 같이 엘리스가 보내는 128비트의 큐빗 상태에 대해 전위 64비트의 확인과정을 통해 확률적 안전도를 확보할 수 있다. 만약 중간 공격자에 의한 데이터 가로채기가 발생한다면 각 비트별 $\frac{1}{4}$의 확률로 오류가 생성된다. 이를 64비트의 병렬데이터로 환산하면 $(\frac{1}{4})^{64}$의 확률로 일치하게 되므로 공격이 불가능하다.

man-in-the-middle 공격에 대하여 악성 공격자의 위장 데이터 교환은 공개채널에서 엘리스와 밥의 상호 이차인증으로 실질 사용자의 존재성을 확인 할 수 있으므로 공격 불가능성을 확보한다.

표 4. 이중광자 평문전송 2라운드 데이터 흐름도
Table. 4 2round data flowchart of double poton transform

		1	2	3	4	⋯	60	61	62	63	64	65	66	67	68	⋯	124	125	126	127	128
엘리스	송신비트	1	1	0	1	⋯	1	0	1	1	0	1	0	0	1	⋯	1	0	1	0	0
	필터	⊕	⊗	⊕	⊗	⋯	⊕	⊗	⊕	⊕	⊕	⊕	⊗	⊗	⊕	⋯	⊕	⊗	⊗	⊕	⊗
	상태	|↔〉	|↗〉	|↕〉	|↗〉	⋯	|↔〉	|↖〉	|↔〉	|↔〉	|↕〉	|↔〉	|↖〉	|↖〉	|↔〉	⋯	|↔〉	|↖〉	|↗〉	|↕〉	|↖〉

밥	검출	⊗	⊗	⊗	⊗	⋯	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⋯	⊗	⊗	⊗	⊗	⊗
	관측		|↗〉		|↗〉	⋯		|↖〉					|↖〉	|↖〉		⋯		|↖〉	|↗〉		|↖〉
	비트		1		1	⋯		0					0	0		⋯		0	1		0

일치	F	T	F	T	⋯	F	T	F	F	F	F	T	T	F	⋯	F	T	T	F	T
원타임		1		1	⋯		0					0	0		⋯		0	1		0

- 엘리스가 전위 랜덤64비트와 후위 동일 64비트 전송
- 밥의 ⊗ 검출기 검출 후 전위 64비트 공개
- 엘리스의 전위 64검출비트와 데이터 공개
- 밥의 후위 64 비트 저장 후 1라운드 저장 64비트와 or 연산 시행

Ⅳ. 결 론

본 논문에서는 암호학의 발달과정과 그에 따른 관용키 암호기법의 기본모형을 토대로 양자 암호 시스템의 대표형식을 알아보았고 일반적인 양자암호 시스템의 키전송 프로토콜을 이용한 양자 평문 전송 알고리즘을 제안하였다.

양자 평문전송 알고리즘은 BB84프로토콜과 E91 프로토콜의 양자 얽힘에 의해 공격자의 유무를 판단하고 공격 징후에 대처하는 형식을 사용하여 원타임패트와 같은 안전도를 확보하였다. 병합적으로 양자화된 데이터를 후진비트열로 저장, 전송하면 양자암호의 안전도를 승계하면서 평문전송도 원활히 이루어지는 모습을 볼 수 있었다. 공격자에 대한 사용자 인증은 기존 BB84 프로토콜의 안전도를 승계하므로 안전함을 입증하였고 백도어에 대한 공격도 꾸준히 연구되고 있는 실정이므로 공격 안전성은 좋다고 볼 수 있다.

아직까지의 기술로는 양자화된 데이터의 양을 원활히 수행할 수 있을 만큼의 전송 능력히 완성되지 않은 실정이다. 앞으로 양자전송이나 양자컴퓨테이션의 발달은 양자화된 평문전송의 사용을 급진적으로 늘릴것이라 기대된다.

양자 평문전송 알고리즘은 양자키분배와 양자평문전송을 병합하여 사용함으로써 사용자 인증과 동시에 평문전송을 수행하는 결과를 가져올 것이다. 앞으로 보다 많은 연구가 이루어져 보다 안정되고 사용자 편리성에 수월한 알고리즘 개발이 완성되리라 기대된다.

References

[1] C. H. Bennett and G. Brassard, In proceedings of IEEE INternational Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984), p.75.

[2] L. R. Knudsen, “Block Ciphers-Analysis, Dsign and Applications,” Ph.D Thesis, Computer Science department, Aarhus University, 1994.

[3] P. Dusart, G. Letourneux, and O. Vivolo, “Differential Fault Analysis on A.E.S”, http://eprint.iacr.org/2003/010.pdf

[4] NIST, “Federal Information Processing standards Publication 197-Specification for the Advanced Encryption Standard (AES)”

[5] http://csrc.nist.gov/publications/fips/fips-197.pdf, 2001

level Parallelism in AES Candidates.
[6] NIST, “Data Encryption Standard(DES)”, http://www.itl.nist.gov/fipspubs/fip46-2.htm
[7] B. Schneier, Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (cloth), 1996.
[8] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
[9] N.Goots, B. Izotov, A. Moldovyan, N. Moldovyan, Modern Cryptography: Protect Your Data with Fast Block Ciphers, A-LIST Publishing, 2003.
[10] D. Stinson, Cryptography: Theory and Practice, CRC Press, 1995.
[11] Charles H. Bennett, Gilles Brassard, Artur K. krt, Quantum Cryptography, Scientific American, October 1992.

설정자(Jung-Za Seol)

2000년 조선대학교 교육대학원 교육학 석사
2007년 조선대학교 컴퓨터공학 박사수료
현재 조선대학교 컴퓨터공학부 외래교수
※관심분야 : 통신 네트워크 및 정보보안, 유비쿼터스

임광철(Kwang-cheol Rim)

2000년 조선대학교 대학원 이학석사
2006년 조선대학교 대학원 이학박사
현재 조선대학교 수학과 외래교수
※관심분야 : 응용수학, 정보보안, 양자암호, 암호학