JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 18, No. 1 : 84~90 Jan. 2014

양자키 교환과 AES를 이용한 비밀통신 연구

정영철[1] · 임광철[2*]

Research of Secret Communication Using Quantum key Distribution and AES

Young-chul Choung[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

비밀통신의 발전은 아날로그 통신에서 디지털 통신으로 진보해 왔다. 디지털통신상의 비밀통신은 one-time pad의 안전성을 승계하여 주로 설계 되어 왔다. One-time pad의 안전성은 상호 보관하는 비밀키의 안전성에 기인하고 비밀키의 교환에 의한 상호 동기화가 가장 중요한 요소이다. 본 논문에서는 quantum cryptography system 중 BB84 알고리즘의 수학적 안전도를 살펴보고 이를 이용하여 양자 키 전송을 시행한다. 생성된 키는 개인의 각 단말에서 AES의 64번 라운드를 시행한 ciphertext을 상호 교환하는 One-time Pad 형 알고리즘을 제안한다.

ABSTRACT

Secret communication has developed from analogue communication to digital one. Secret communication which is based on digital communication has been designed succeeding safety of one-time pad. One-time pad's safety is attributed to the security of secret key's mutual storage and mutual synchronization that is the key's interchange basis is one of the essential factors. This manuscript examines mathematical stability of BB84 algorithm which is one of the quantum cryptography system, and conducts transmission of quantum key. The created key suggests One-time Pad algorithm which interchanges ciphertext implemented AES's 64th round.

키워드 : 암호화/복호화, 비밀통신, 원타임패드

Key word : encryption/decryption, secret communication, one-time pad

접수일자 : 2013. 12. 26 심사완료일자 : 2014. 01. 02 게재확정일자 : 2014. 01. 07

*** 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.2014.18.1.84 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

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[1-5].

이후 계산 복잡도를 이용한 공개키 암호 시스템이 제안되었고 현재까지 각 분야에서 활발히 사용되고 있다. 이후 계산 복잡도에 의한 보안성은 양자컴퓨터의 등장으로 더 이상 안전도를 보장할 수 없게 되었다. 이후 양자암호의 개발로 공격가능성을 배제한 암호알고리즘이 설계되었다[6].

모든 암호의 사용형식은 상호간의 통신을 그 어느 누구라도 감청이나 도청이 일어나는 것을 원하지 않은 데서 비롯되었다. 오늘날 통신기술의 급속한 발달은 무선통신의 비약적인 발전으로 집약되고 있고 이에 따른 상호간 통신상 보안에 대한 인식도 늘어나고 있는 실정이다.

국내 이동통신은 기본적으로 CDMA기법을 통신 표준으로 채택하여 이용하고 있다. CDMA 기법의 통신은 각 가입자간 고유의 식별부호를 가지고 있어서 보안상 안전하다고 하나 CDMA 시스템의 순방향 채널을 분석하여 가입자 단말기의 ESN 및 MIN가 알려지는 경우 도청이 가능함을 보였다. 현재 국내에서 서비스되고 있는 CDMA 시스템에서는 신호처리 과정에서 기본정보가 무선채널 상에서 노출되고 있으므로 비교적 간단한 방법으로 순방향 통화 채널을 모니터 할 수 있음이 증명되었다[7].

본고에서는 이러한 통신상 보안취약성에 대비하여 각자 보유한 단말을 이용한 비밀 통신기법으로 안전한 채널상에서의 양자암호 시스템을 도입하고 이를 통해 원타임패드의 비밀키를 상호 교환한다. 이후 생성된 비밀키로 상호 동기화를 완성하고 AES에 입력키로 전송된 키 수열을 적용한 난수열을 보내고자 하는 평문에 베타적 논리합을 이용한 스트림 암호를 구현 후 상호 암복호화를 실현하였다.

Ⅱ. 양자암호시스템

양자역학의 불확정성을 이용한 키분배 방식은 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 원타임 패드 암호 방식을 결합하여 해독이 불가능하게 만든 암호 방식이다[6].

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

비트값	⊕	⊗
0	$\|\updownarrow\rangle$	$\|\nwarrow\rangle$
1	$\|\leftrightarrow\rangle$	$\|\nearrow\rangle$

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

엘리스와 밥이 가로, 세로의 직선편광 광자와 대각선의 직선 편광 광자를 동시에 이용한다. 엘리스는 ⊕와 ⊗ 두 종류의 편광필터를 무작위로 사용하여 비트를 송신하고 밥도 두 종류의 검출기를 무작위로 사용하여 광

표 2. BB84 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	송신비트	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	

을 검출한다. BB84의 프로토콜은 다음과 같다.

- 엘리스는 ⊕와 ⊗ 편광필터를 무작위로 선택하여 0과 1이 무작위로 배열된 4n 비트 데이터를 송신한다.
- 밥은 ⊕와 ⊗편광검출기를 무작위로 택하여 편광방향을 관측한다. 엘리스는 밥에게 자신이 선택한 편광필터의 배열 순서를 공개된 채널을 통해 알린다.
- 두 사람은 검출기의 ⊕와 ⊗ 종류와 엘리스의 편광필터 ⊕와 ⊗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 복사하는 것은 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 유출에 대한 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.

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

이는 비트수가 많은 수록 도청자의 유무를 판별하기가 수월해진다. 각각 벡터들의 연결되는 사항을 일차결합을 이용하여 선형관계를 설명하고 스핀업과 스핀다운에 의해 설계된 벡터들을 크로스 벡터로 변환하는데 있어 고유벡터를 산출한 일차결합으로 표현하였다. 이는 스핀업과 스핀다운의 벡터들이 크로스 벡터로 변환하는 과정이 $\frac{1}{2}$의 확률로 도출됨을 보여준다.

Ⅲ. 양자키를 이용한 비밀통신

비밀통신은 아날로그를 신호를 이용한 방식과 디지털 신호를 이용한 통신 채널상에서의 방식이 혼용되어 사용 되고 있다. 제안하는 알고리즘은 디지털 방식의 데이터를 암호화 하는 기법을 논하였고 사용환경은 디지털화한 데이터를 중심으로 설계하였다. 현재의 디지털 통신은 CDMA방식을 따르고 있고 이는 통신 진행과정에서 디지털 신호의 분할 전송을 통해 통신이 이루어지는 형태이다. 제안하는 알고리즘은 디지털화 된 데이터에 AES로 암호화 하여 전송하는 방식으로 상호 암복호화를 위하여 양자키 전송방식으로 일회성 난수열을 전송 보관하고 이를 AES의 입력키로 사용한다. 통상적인 개념으로 전송자를 앨리스라 하고 수신자를 밥이라 칭하기로 한다.

표 3. 키 스케줄
Table. 3 key schedule

엘리스				밥			
S1	→	AES	일치확인	AES	←	S1	동기화
S2	암 복 호 화						
S3	암 복 호 화						

S1, S2, S3 : 128비트 수열

사용 예는 먼저 상호 인정되는 안정된 장소에 양자키 분배 센터를 만들고 이곳에서 실시간으로 상호 동기화된 키를 양자전송을 통해 교환한다. 양자전송에 의해 생성되는 비밀키는 안전한 장소에서 랜덤하게 생성된 난수열을 BB84프로토콜로 128bit씩 엘리스와 밥에게 전송한다.

엘리스와 밥은 상호 충분히 많은 양의 비밀키를 서로의 통신기에 가지고 있게 된다. 이후 비밀통신을 하기 위하여 상호 비밀키 동기화를 위해 각자 가지고 있던 키의 최초 128bit열을 AES를 통해 일치확인 한다. 이후 상호 키에 대해 동기화를 확인한 후 두 번째 키 수열을 이용하여 암 복호화를 진행한다. 두 번째 키 스케쥴이 끝나면 세 번째 키를 이용하여 라운드를 진행한다.

그림 1은 암호화 과정을 나타낸 것으로 암호화 과정은 크게 두 부분으로 나누어진다. 먼저 키 생성부 에서는 입력된 128비트 키 수열 a_1을 128비트 AES에 입력한다.

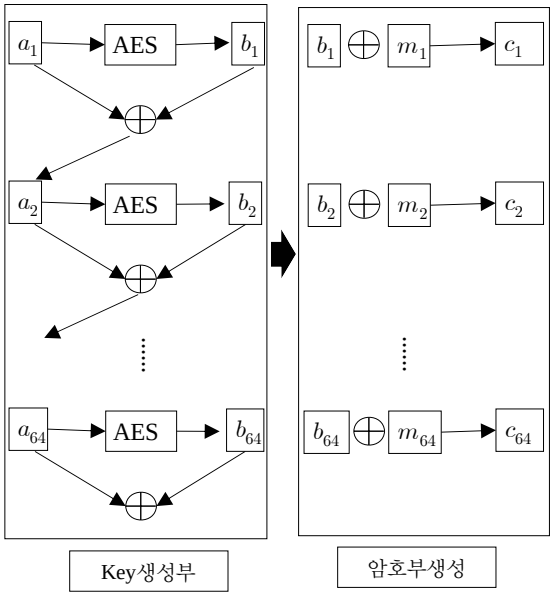

그림 1. 암호화
Fig. 1 encryption

출력 128비트 수열 b_1은 평문 128비트와 EX-OR(베타적 논리합)을 시행하여 128비트 암호문 c_1 으로 전송된다. 또한 출력된 b_1은 입력값인 a_1과 EX-OR연산을 수행 후 a_2로 치환된다. a_2는 다시 AES의 입력값으로 사용되어 새로운 128비트 수열 b_2를 얻는다. b_2는 다시 평문 m_2와 EX-OR을 하여 c_2로 암호화되어 전송된다. 이를 총 64회 반복 후 저장된 키에서 새로운 128비트 a_1을 얻는다. 이후 통신이 종료될 때 까지 이를 계속 반복하여 암호문을 생성한다. 복호화 과정은 암호화 과정과 마찬가지로 진행된다. 그림2 와같이 키 생성부 에서 양자키 교환에 의해 입력된 128비트 키 수열 a_1을 128비트 AES에 입력한다. 출력 128비트 수열 b_1은 암호문 128비트와 EX-OR을 시행하여 128비트 평문 m_1을 얻는다. 또한 출력된 b_1은 입력값인 a_1과 EX-OR연산을 수행후 a_2로 치환된다. a_2는 다시 AES의 입력값으로 사용되어 새로운 128비트 수열 b_2을 얻는다. b_2는 다시 암호문 c_2와 EX-OR을 시행하여 평문 m_2를 얻는다. 이를 총 64회 반복 후 저장된 키에서 새로운 128비트 a_1을 얻는다. 이후 통신이 종료될 때 까지 이를 계속 반복하여 평문을 생성한다.

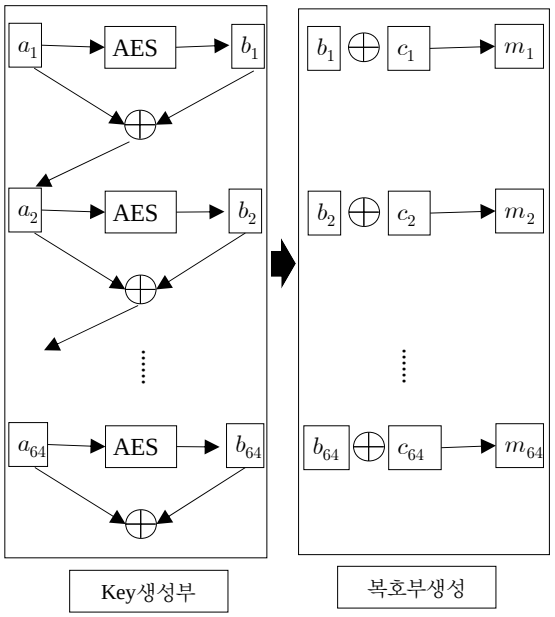

그림 2. 복호화
Fig. 2 decryption

상기과정은 총 3단계로 나누어 볼 수 있다.

1단계 양자키분배

기존 비밀통신은 일회성 키 분배를 위하여 단말이 특정한 장소에 모이거나 키를 특정 저장장치에 저장하여 교환하는 번거로움이 있었다. 제안하는 알고리즘은 양자암호를 이용하여 물리적 제안을 해결하고 각자의 단말에 양자방식을 이용한 원거리 키전송을 통해 일회성 키를 분배하는 방식을 따른다.

양자키전송의 안전도를 벡터를 통해 분석해 보면 다음과 같다.

$$|\uparrow><\uparrow| = \begin{pmatrix}1\\0\end{pmatrix}(1\ 0) = \begin{pmatrix}1&0\\0&0\end{pmatrix}$$
$$|\uparrow><\downarrow| = \begin{pmatrix}1\\0\end{pmatrix}(0\ 1) = \begin{pmatrix}0&1\\0&0\end{pmatrix}$$
$$|\downarrow><\uparrow| = \begin{pmatrix}0\\1\end{pmatrix}(1\ 0) = \begin{pmatrix}0&0\\1&0\end{pmatrix}$$
$$|\uparrow><\uparrow| = \begin{pmatrix}0\\1\end{pmatrix}(0\ 1) = \begin{pmatrix}0&0\\0&1\end{pmatrix}$$

와 같이 2행 2열로 표현되므로 스핀연산자는

$$\sigma_x = |\uparrow><\downarrow| + |\downarrow><\uparrow|$$
$$\sigma_y = -i(|\uparrow><\downarrow| - |\downarrow><\uparrow|)$$
$$\sigma_y = (|\uparrow><\uparrow| - |\downarrow><\downarrow|)$$

로 나타낼 수 있다.

$\sigma_x, \sigma_y, \sigma_z$는

$$\sigma_x = \begin{pmatrix}0&1\\1&0\end{pmatrix},\ \sigma_y = \begin{pmatrix}0&-i\\i&0\end{pmatrix},\ \sigma_z = \begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

로 정의되고 다음과 같은 성질을 만족한다.

$$\sigma_x\sigma_y = i\sigma_z = -\sigma_y\sigma_x$$
$$\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = \begin{pmatrix}1&0\\0&1\end{pmatrix}$$
$$\sigma_y\sigma_z = i\sigma_x = -\sigma_z\sigma_y$$

스핀행렬 $\vec{S} = \frac{\hbar}{2}\sigma$

$S^2 = S_x^2 + S_y^2 + S_z^2 = \frac{3}{4}\hbar^2\begin{pmatrix}1&0\\0&1\end{pmatrix}$ 이 된다.

$$S^2 = s(s+1) = \frac{1}{4}(\sigma_x^2 + \sigma_y^2 + \sigma_z^2)$$
$$= \frac{3}{4} = \frac{1}{2}(\frac{1}{2}+1)$$

으로부터 분명하게 $\frac{1}{2}$ 임을 알 수 있다.

아직은 양자전송이 국소적인 거리에서만 실험이 진행된 관계로 국가대 국가의 암호 전송은 연구를 보다 더 필요로 하고 있다.

2단계 암호화

전송된 키를 128비트 수열로 분할 하고 이 128비트 키를 AES의 입력키값으로 사용한다. 안전도에 대한 분석으로 AES에 대한 공격법은 주로 부채널공격으로 연구가 활발히 이루어 졌다. 그중 오류주입(Fault Analysis) 공격은 AES의 실행 과정에 정상 암호문과 오류발생 암호를 주입하여 얻은 암호문을 분석해서 공격하는 기법으로 1997년 Biham 과 Shamir의 차분오류 공격이 관용키 암호에 적용가능함을 제안하였다[8].

이후 AES로의 적용도 활발해 진행 되었다. AES에 대한 차분오류 공격은 AES의 진행되는 각 라운드에서 오류를 주입한 data를 확보하고 이를 적용한 공격이다. 이러한 공격들을 예방하기 위한 가장 안전한 수단은 비밀키를 1회만 사용함으로써 중간오류값에 의한 비밀키를 확보하더라도 전혀 쓸모가 없어지게 하는 것이다.

비밀키를 1회만 사용하는 기법을 원타임패드(One-time pad)라 하고 주로 스트림 암호로 연구되고 사용되었다. 원타임패드는 엘리스와 밥이 상호 동기화된 비밀키를 가지고 있다가 한번 암호문을 작성하면 버리는 방법으로 안전도에는 최상의 조건을 가지고 있지만 매번 키를 재분배하고 서로간에 키를 동기화시켜야 하는 불편함이 따른다.

원타임 패드는 한번 사용한 비밀키를 버리기 때문에 AES의 차분오류공격등 비밀키를 재사용하는 방식의 공격에 대처능력이 뛰어나다 할 수 있다.

3단계 복호화

암호화와 마찬가지로 1회성 비밀키를 생성하므로 안전도에 대한 절대값을 보장하고 설계도 또한 단순하게 진행하도록 하였다.

본고에서는 랜덤하게 생성된 난수열을 양자암호원리를 적용하여 수학적 안전도를 확보한 양자키 전송으로 키를 전송하고 원타임패드를 결합한 알고리즘으로 보안성에 탁월하게 설계하였다.

키분배에 의해 이루어진 난수열을 128비트 AES시스템에 맞추어서 설계하였고 베타적 논리합을 통해 원타임패드를 구현하였다. 이로 인해 기 알려진 공격법들에 대한 대응은 절대적 안전도를 보장하였다.

Ⅳ. 결 론

개인 대 개인의 통신 보안은 인류사에서 계속 되어온 주 관심사였다. 인류사는 비밀을 지키고자 하는자와 그 비밀을 깨려고 하는자의 영원한 싸움의 연속이었고, 본 논문에서는 통신의 최종단계인 개인 단말에서의 보안에 용이하게 사용될 수 있는 원타임 패드형 개인 보안 모듈을 설계하는 것이 주 목적으로 하였다. 이미 잘 알려진 양자 암호중 BB84 프로토콜을 이용하여 양자 전송을 이루고 AES의 128비트형을 이용하여 암호화와 복호화 하는 방법을 설계하였다. 안전도 측면에서 양자암호의 수학적 안전도를 살펴보았고, 그로인해 양자암호의 공격 불가능성을 기반으로 키전송이 이루어지게 하였다. 이에 AES의 알려진 차분공격은 비밀키를 매번 달리 사용하는 원타임패드형 알고리즘으로 공격위험을 벗어날 수 있음을 확인하였다.

본 알고리즘의 구현을 위하여 선행적으로 양자보안센터의 구축이 필요하고 그로인해 양자 전송이 보다 발전된 모습으로 구현된다면 응용할 수 있는 부분은 다양할 것으로 예측된다.

REFERENCES

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

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

[3] NIST, "*Federal Information Processing standards Publication 197 - Specification for the Advanced Encryption Standard (AES)*"

[4] http://csrc.nist.gov/publications/fips/fips-197.pdf, 2001 level Parallelism in AES Candidates.

[5] NIST, "Data Encryption Standard(DES)", http://www.itl.nist.gov/fipspubs/fip46-2.htm

[6] Charles H. Bennett, Gilles Brassard, Artur K. krt, Quantum Cryptography, Scientific American, October 1992.

[7] Ryu Dae-Hyun, Jang Seung-Ju “An Enhanced Mechanism of Security Weakness in CDMA Service” *Journal of Computing Science and Engineering*, 2003/30-6

[8] E.Biham and A.Shamir, “Differential Fault Analysis of Secret Key Cryptosystems,” *CRYPTO’97*, LNCS 1294, 1997.

정영철(Young-Chul Choung)

1987년 조선대학교 행정학과 학사
2003년 조선대학교 전자공학과 석사
2007년 조선대학교 정보통신공학과 박사
현재 제이앤아이코리아 연구소장, 조선대학교 컴퓨터공학부 외래교수
※관심분야 : 정보통신정책, 전자정부, 네트워크 보안, 융복합 응용

임광철(Kwang-cheol Rim)

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