한국지능시스템학회 논문지 2010, Vol. 20, No. 6, pp. 837-842
DOI : 10.5391/JKIIS.2010.20.6.837

이진 병합에 의한 양자암호 취약성

(An) analysis of quantum cryptography vulnerability by Binary merge

임광철* · 최진석**+
Kwang-Cheol Rim* and Jin-suk Choi**+

*조선대학교 수학과
**조선대학교 전자계산학과

요 약

본 논문에서는 양자암호 시스템의 설계과정에서 필연적으로 사용되는 의사난수들의 비트열들이 다수개 존재하는 현상과 이를 상호 공개된 채널에서 부분정보를 공유해야 하는 상황은 비트열들의 쌍을 노출 시킨다. 본고에서는 이러한 의사난수열의 기본 테스트 과정과 이를 벗어나는 이진 병합 비트열의 난수성에 대하여 살펴 본다.

키워드 : 암호화/복호화, 양자암호, 의사난수, 시리얼테스트

Abstract

In this paper, quantum cryptography systems used in the design process inevitably open bit stream of pseudo-random number that exists multiple open channels between them and the need to share information on the part of the situation exposes a pair of bit stream. In this paper, the base test of pseudo-random number I tested out this process and the merge bit binary column look out for randomness.

Key Words : encryption/decryption, quantum cryptography, Pseudo-random numbers, serial test

1. 서 론

암호학의 고전에는 주로 단순한 문자를 대입하고 이를 치환하여 정보를 은닉하였다. 이는 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 그 시절에는 안전한 시스템 이라 볼 수 있었다. 하지만 현대 정보전산능력이 뛰어난 시기에는 그도 또한 쉽게 해독할 수 있다. 이후 Shannon에 의해 복잡도가 높은 암호 알고리즘의 실현이 가능하게 되었고 현대암호학의 기본 토대를 형성하게 되었다.[2,3]

현대암호는 크게 대칭키 암호시스템과 공개키 암호시스템으로 나눌 수가 있다. 1970년대 초 Shannon에 의해 주장된 혼돈(confusion)과 확산(diffusion)을 여러번 반복하면 강력한 암호 알고리즘을 구현할 수 있다는 이론에 의해 미국의 표준암호 알고리즘인 DES(data encryption standard)가 IBM에 의해 제안되어 많은 기간 사용되었으며 이후 AES로 발전하였다.[1,4,9,10]

원타임패드(one-time pad)와 유사한 안전성을 보장하며 일반적인 통신망에도 적용할수 있는 암호 알고리즘으로 스트림 암호 시스템이 있는데 이는 난수를 생성하여 평문과 1-1대칭으로 암복호화 하는 방식이다. 이도 또한 엄밀한 의미로는 대칭키 암호 알고리즘으로 볼 수 있다. 대칭키 암호 알고리즘은 일단 키를 송신자와 수신자가 똑같이 나누어 가져야 한다는 불편이 있다. 이를 해소하기 위하여 암호화와 복호화과정에서 서로 다른 키를 사용하고 암호화키를 공개하여 키의 전송 및 비밀 보관 등이 필요 없게 만든 것이 공개키 암호 시스템이다. 이는 1976년 Diffe와 Hellman의 논문 “New Directions in Cryptography"에 발표가 되었다. 이도 또한 발전을 거쳐서 현재 RSA, ElGamal, 타원곡선암호, 땋임군 암호 등이 나와 있으나 계산양이 너무 많기 때문에 일반 평문에 대한 암호화는 힘들고 주로 키분배 알고리즘과 짧은 길이의 데이타에 대해 사용되고 있는 실정이다.[11,12,13,14]

의사난수 발생기는 거의 모든 암호학적 알고리즘에서 뼈대와 같이 사용되는 가장 중요한 암호학적 함수 중의 하나이다. 기존 의사난수 생성 알고리즘은 대수학적 이론에 기반을 둔 것과 하드웨어적 알고리즘에 기반을 둔 것으로 볼 수 가 있다. 의사난수 생성기는 스트림 암호의 원천을 이루고 또한 암호 프로토콜의 초기 벡터 또는 비밀키, 전자 서명 및 전자 결제 시스템의 비밀 파라미터, 각종 키관리/인증메커니즘에서의 세션키나 랜덤첼린지(random challenge)의 생성 등에 사용된다. 난수에는 크게 실 난수(true random) 와 의사난수(pseudo random) 두 가지로 볼 수 있는데 그 차이점은 표 1 과 같다.

접수일자 : 2010년 7월 23일
완료일자 : 2010년 12월 6일
+ : 교신저자

표 1. 난수의 비교
Table 1. Comparison of random number

실난수(true random numbers)	의사난수(pseudo-random numbers)
비결정적	컴퓨터는 논리적이고 결정적이므로 실 난수를 산출 하지 못함
예측 불가능한 어떤 물리적인 소스로부터 획득 : 반도체, 방사선 붕괴 등으로부터 전자소음 혹은 열 소음 등	S/W에 기반 한 RNG는 최상의 경우에 의사난수를 생성 가능
	PRNG : 길이가 짧은 랜덤 비트 열(seed)을 길이가 긴 랜덤에 근접한 비트열로 출력하는 알고리즘

또한 난수성을 만족하는 좋은 난수의 특징은 다음과 같다.

- 긴 주기를 가져야 함
- 패턴과 역산관 관계를 알수 없어야 함
- 1과 0의 평균 생성횟수가 동일하여야 함
- “01010101”과 같은 형태가 길지 않아야 함
- 간단한 알고리즘으로 설계와 구현이 쉬워야 함
- 이미 나온 출력으로부터 그 전의 값을 유추할 수 없어야 함

본고에서는 양자암호시스템 내에서 사용되고 있는 난수열들에 대하여 의사난수를 이용하는 구간을 분석하고 이에 대한 이진병합적 접근으로 부분정보를 유추할 수 있는 방법에 대하여 이야기 한다. 원타임패드의 안정성에 의하여 절대적 도청불가 상태의 암호 구현을 실현한 양자 암호시스템 내에서 사용자의 실난수 사용에 대한 불편함으로 인하여 의사난수를 사용한다. 이는 단일 비트열에서는 입증된 난수성이 다중비트열의 병합에 의하여 부분정보나 난수성의 오류를 보이는 것을 알 수 있다.

2. 양자암호시스템

암호용 키 분배는 크게 두가지로 볼 수 있다. 비밀키를 담당자에게 배포하여 관리하는것과 공개키분배방식이다. 전자는 사람에 대한 신뢰를 믿을 수 가 없으며 후자는 소인수분해의 해법이 완성되면 안전성을 보장 할 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 암호방식을 결합하여 해독이 불가능하게 만든 암호 방식이다.[15]

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 2. 편광된 광자의 이진 대응표
Table 2. Pilarized light map

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 않을때는 첫 단계부터 다시 편광을 보내서 시작하면 된다.

<표3>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 편광복사는 존재할 수가 없다. 다만 엘리스와 밥이 사용하는 송신 비트와 편광기 선택 비트 그리고 밥이 선택하는 검출기 선택비트들에서 실난수 사용상의 애로점으로 인하여 의사난수를 사용하므로 맨인더미들 어택과 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 3. BB84 프로토콜
Table 3. 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	

3. 난수성 테스트

좋은 의사난수 생성기는 입력과 출력을 통한 공격을 막기 위한 방법으로 중간 상태변수를 알 수 없게 하여야 한다. 이를 위해서는 초기값과 상태값들을 일정 출력과 일정 시간이 흐른 후에는 갱신과정을 통하여 새롭게 입력되고 변화하여야한다.

미 NIST에서 제공하는 의사난수 테스트에는 16가지가 있다. 여기서는 앞부분의 중요한 프리퀀시 (frequency) 테스트, 런(run) 테스트에 대하여 살펴보기로 한다.

3.1 프리퀀시(frequency) 테스트

이진수열 (s_t)의 N개의 항$s_0,\ s_1, s_{t+2}, ,\cdots, s_{N-1}$을 처음부터 차례로 m개씩 나누면, 다음과 같이 m차원 벡터공간 $GF(2)^n$에 속하는 $n=[\frac{N}{m}]$개의 벡터가 생긴다.

$$\begin{aligned}&(s_0,\ s_1, s_{t+2}, ,\cdots, s_{m-1})\\ &*\ (s_m,\ s_{m+1}, s_{m+2}, ,\cdots, s_{2m-1})\\ &\cdots\cdots\cdots\cdots\\ &(s_{(n-1)m},\ s_{(n-1)m+1}, \cdots, s_{nm})\end{aligned} \tag{2}$$

이제 체 $GF(2)=\{0,1\}$ 위의 m 차원 벡터공간

$$GF(2)^n=\{(x_1,x_2,\cdots,x_m)\mid x_1,x_2,\cdots,x_m\in GF(2)\} \tag{3}$$

에 속하는 2^m개의 벡터를 적당히 번호를 정하여,
(*) 에 있는 벡터중에서

$$\begin{aligned}&(0,0,\cdots,0)\text{인 것의 개수를 } n(0)\\ &(0,0,\cdots,1)\text{인 것의 개수를 } n(1)\\ &\cdots\cdots\cdots\cdots\\ &(1,1,\cdots,1,1)\text{인 것의 개수를 } n(2^m-1)\end{aligned} \tag{4}$$

라고 하자. 이 때, N개의 항으로 이루어진 유한 이진 수열

$$s_0, s_1, s_{t+2}, \cdots, s_{N-1} \tag{5}$$

이 완전한 random 수열인 경우에는 $GF(2)^n$에 속해 있는 각 벡터가 (*) 에 있는 n개의 벡터 중의 하나로 나타날 확률은 $\frac{n}{2^m}$이다. 따라서 통계량

$$\begin{aligned}T&=\sum_{i=0}^{2^m-1}\frac{\left\{n(i)-\frac{n}{2^m}\right\}^2}{\frac{n}{2^m}}\\ &=\frac{2^m}{n}\sum_{i=0}^{2^m-1}n(i)^2-n\end{aligned} \tag{6}$$

은 근사적으로 자유도가 2^m-1인 χ^2분포를 따른다.

이제 $0<\alpha<1$ 인 α에 대하여

$$P(\chi^2\geqq x_\alpha)=\alpha \tag{7}$$

인 실수 x_α 를 χ^2 분포표에서 구하면, 유의수준 α에 대하여 기각역은 $T>x_\alpha$ 이다.

예를 들어, $\alpha=0.01$에 대하여

$$P(\chi^2\geqq x_{\alpha)}=0.01 \tag{8}$$

일때, T 의 값이 α 보다 크면 주어진 수열은 랜덤(random) 하지 않다고 말 할 수 있고 T 의 값이 α 보다 작으면 이 테스트로는 랜덤(random) 하지 않다고 판정할 수는 없다.

일반적으로, 모든 m에 대하여 일일이 이와같은 테스트를 시행할 수는 없으므로 경우에 따라 m 의 값을 적절히 택한다.

특히, m=1 인 경우에 이 테스트를 흔히 프리퀀시테스트라고 한다. 이 경우에 식은 다음과 같다.

$$T=\frac{2}{N}\sum_{i=1}^{1}\left(n(i)-\frac{N}{2}\right)^2 \quad (9)$$

여기서 $n(0)$ 과 $n(1)$은 각각 $s_0,s_1,s_2,\cdots,s_{N-1}$ 중에서 0인 것의 개수와 1인것의 개수를 뜻한다. 이제 $n_0=n(0),\ n_1=n(1)$ 이라고 놓으면,

$$N=n=n(0)+n(1)=n_0+n_1 \quad (10)$$

이므로, 위의 식은 다음과 같이 변형된다.

$$T=\frac{(n_0-n_1)^2}{N} \quad (11)$$

그리고, 이 경우에 통계량

$$Z=\frac{1}{\frac{\sqrt{n}}{4}}\left\{n_1-\frac{n}{2}\right\} \quad (12)$$

는 근사적으로 표준정규분포 $N(0,1)$ 을 따른다. 한편, χ^2분포에서 유의수준 5%의 한계값은 3.84 이다. 따라서 T의 값이 3.84 보다 큰 경우에, 프리퀀시검정에 대하여 유의수준 5%로 이 이진수열은 난수성이 없다고 판단되어 기각한다. 이에 대한 판단으로 P-value를 사용하는데 P-value 0.01 이상에 대하여 유의수준을 결정한다.

예를 보면 다음과 같다

표 4. 프리퀀시 테스트 예

Table 4. Sample of frequency test

input	e=11001001000011111101101010100010001000 01011010001100001000110100110001001100011 10011000101000010111000
	n=100
processing	Sn = -16
	sobs = 1.6
output	P-value = 0.109599

결과 는 P-value > 0.01 이므로 이 수열은 랜덤하다고 할 수 있다.

3.2 런(run)테스트

진수열 (s_t) 에서 , 0 또는 1 이 처음부터 끝까지 반복해서 연이어 나타나는 부분을 이 이진수열의 런 이라고 한다. 예를 들어, 0110001은 한 개의 0 으로 이루어진 런과 두 개의 1로 이루어진 런, 세 개의 0 으로 이루어진 런, 그리고 한 개의 1 로 이루어진 런 을 포함하고 있다. 특히, 0 만으로 이루어진 런을 그 수열의 갭(gap) 이라 하고, 1 만으로 이루어진 런을 그 수열의 블록(block) 이라 한다. 다음은 주기가 N 인 이진 수열의 임의성에 관한 Golomb의 공리계이다.

R1 먼저 N이 짝수인 경우에, 길이가 N인 순환마디에는 $\frac{N}{2}$개의 0과 $\frac{N}{2}$개의 1 이 들어 있다. 한편, N이 홀수인 경우에는 0 또는 1이 $[\frac{N}{2}]$개씩 들어 있다. R2 길이가 N인 순환마디에 들어 있는 런 가운데 절반은 길이가 1 이고 $\frac{1}{4}$은 길이가 2 이며, 일반적으로 이 순환마디에 적어도 2^{i+1} 개의 런이 들어 있다면 이 중에서 $\frac{1}{2^i}$ 은 길이가 i 이다. 또한, 각 $i>1$ 에 대하여 길이가 i 인 갭 과 블록의 개수는 동일하다. R3 이 수열의 out-of-phase 자기상관은 일정하다. 위의 R1, R2, R3 를 만족시키는 무한 이진수열을 흔히 G-random 수열 또는 PN 수열 이라고 한다. 이진수열 (s_t) 의 N 개의 항 $(s_0,\ s_1,s_2,,\cdots,s_{m-1})$ 에서 갭의 개수와 블록의 개수를 각각 r_0,r_1이라 하고 $n=r_0+r_1$이라고 하자. 또, 각 $i(1\leq i\leq L)$에 대하여 길이가 i인 갭의 개수와 길이가 i인 블록의 개수를 각각 $n_{0i},\ n_{1i}$ 라 하고 $n_i=\ n_{0i}+n_{1i}$ 라고 하면, n은 런의 개수이고, n_i는 길이가 i인 런의 개수이다. 이때, 갭 중에서 그 길이가 i일 확률은 $\frac{1}{2^{i+2}}$ 이고 블록 중에서 그 길이가 i일 확률은 $\frac{1}{2^{i+2}}$ 이다. 따라서 통계량

$$T=\sum_{j=0}^{1}\sum_{i=1}^{L}\frac{\left(n_i^k-\frac{n}{2^{i+2}}\right)^2}{\frac{n}{2^{i+2}}} \quad (13)$$

은 근사적으로 자유도가 2L인 카이제곱 분포를 따른다. 이와 같은 통계량을 이용하는 테스트를 매개변수가 L 인 런 테스트라 한다.

예를 보면 다음과 같다.

표 5. 런 테스트 예

Table 5. Sample of run test

input	e=11001001000011111101101010100010001000 01011010001100001000110100110001001100011 10011000101000010111000
	n=100
	t = 0.02
processing	p = 0.42
	Vn(obs) = 52
output	P-value = 0.500798

결과 : P-value > 0.01 이므로 이 수열은 랜덤하다고 볼 수 있다.

4. 이진병합과 양자암호의 안전성 고찰

암호학의 역사속에서 숨기는자와 찾고자하는자의 싸움은 언제나 흥미진진하게 진행되어왔다. 고전암호 체계에서 발

전하여 기계식 암호가 나왔으며 세계대전을 치루면서 보다 깊고 인간의 계산영역을 넘어서는 기계를 개발하였으나 전산학과 컴퓨터의 발달은 이러한 노력을 무너뜨리기에 충분하였다. 이후 전산학의 연산영역을 넘어서는 계산이론에 의한 공개키암호방식이 도출되었다. 한동안 계산량의 안전성에 머물러 있던 공개키암호방식이 쇼어의 양자이론을 이용한 소인수분해 해법을 찾음으로 인해서 안전성에 치명적 타격을 입게 되었다.

이에 포톤을 이용한 양자암호방식의 제안으로 중간 도청자로부터 안전한 암호체계인 BB84가 제안되었고 아직까지 그 안전성에 대한 신뢰는 견고한 편이다. 모든 계는 사용자의 편리성을 찾아 가다보면 신뢰도에 어느정도 약점을 보이기 마련이다. 양자암호시스템도 실난수의 사용에 불편함을 이용하여 엘리스와 밥의 의사난수사용은 난수성의 도출에 취약성을 발견하는 경우를 볼 수 있다. 기본적으로 의사난수로써의 가치를 인정받기 위하여 NIST의 난수성 테스트를 이진비트열 상태에서 통과하여야 한다. 하지만 난수성 테스트를 통과한 비트들이라도 다중 비트열들의 병합과정에서 병합비트열들의 난수성을 온전히 보전되지 않는 경우를 발견할 수 있다.

<표3>에서 엘리스의 입력신호를 하나의 비트열로 간주하고 편광필터를 고르는 무작위성을 다른 하나의 이진수열로 볼 수 있다.

$$a_1 = \ 10101101111001010010 \text{ 송신비트열}$$

$$a_2 = \ 01101110001001110100 \text{ 편광필터선택비트열}$$

에 대하여

$$a_1 * a_2 = \binom{1}{0}\binom{0}{1}\binom{1}{1}\binom{0}{0}\binom{1}{1}\binom{1}{1}\binom{0}{1}\binom{1}{0}\binom{1}{0}\binom{1}{0}$$

$$\binom{1}{1}\binom{0}{0}\binom{0}{0}\binom{1}{1}\binom{0}{1}\binom{1}{1}\binom{0}{0}\binom{0}{1}\binom{1}{0}\binom{0}{0}$$

과 같이 나타낼 수 있다. 이는 의사난수기본테스트인 런테스트, 모노비트테스트, 시리얼 테스트를 모두 통과 하는 결과를 볼 수 있다. 상기 이진 수열들의 엘리스와 밥의 상호 선택에 의한 무작위 이진 수열들을 살펴보면 최소한 3개 이상의 의사난수비트열을 유추할 수 있다. 이에 3개의 이진비트열을 상호 일치하는 데이터 쌍들의 진행과 불일치하는 데이터의 쌍으로 이진화 하여 비교해 보면 이들은 난수성을 잃어버리는 경우를 바로 볼 수 있다.

$$b_1 = 11001101000110100011 \text{ 밥검출기선택비트열}$$

$$a_1 * a_2 * b_1 = \binom{1}{0}\binom{0}{1}\binom{1}{1}\binom{0}{0}\binom{1}{1}\binom{1}{1}\binom{0}{1}\binom{1}{0}\binom{1}{0}\binom{1}{1}$$

$$\binom{1}{0}\binom{0}{0}\binom{0}{0}\binom{1}{1}\binom{0}{1}\binom{1}{1}\binom{0}{0}\binom{0}{1}\binom{1}{0}\binom{0}{0}$$

를 엘리스와 밥의 필터와 검출기의 일치 여부를 연결하는 이진 비트열을 완성하면 다음과 같다.

$$c = 10011111000000001110$$

5. 결 론

본 논문에서는 의사난수열의 기본 테스트 과정과 이를 벗어나는 이진 병합 비트열의 난수성에 대하여 제안 하였다. 엘리스에 의해 생성된 2진 비트열 중 송신 비트와 필터 생성 비트열을 밥에게 공개 한 후 밥의 검출필터 생성비트열과의 3중 비트 결합을 시키면 이진 수열 c와 같은 일치 비트열을 얻을 수 있다. 이는 1과 0의 균등분포를 검출하는 프리퀀시 테스트는 통과함을 알 수 있으나 3번째 런과 4번째 런의 결과는 1과 0의 규칙적 패턴으로 확연히 런테스트의 실패임을 알 수 있다. 암호시스템 내에서 작은 데이터양이라도 부분정보의 유출은 심각한 피해를 초래 할 수 있다. 실질적으로 구현하는 BB84 양자암호시스템 내에서 난수성이 파괴된다는 것은 데이터 이동 경로상의 안전성이 입증이 되더라도 오픈채널에서 전위비트열을 공유하는 한 의사난수의 안전성을 확보하지 못한다면 부분정보 노출에 대하여 취약할 수밖에 없다.

보다 안전한 양자암호 시스템들이 속속 개발되고 있는 현재 시점에서 의사난수열을 사용하는 시스템의 트렙도어를 제거해야하는 노력이 필요하고 이진비트열들의 이진병합에 대한 의사난수성을 입증하는 테스트까지 통과하는 의사난수비트열들에 대해서만 난수열의 사용을 허용하거나 실난수를 사용할 수 있는 인프라 구축이 필요하다고 본다.

참 고 문 헌

[1] H. Feistel, *Block Cipher Cryptographic System*, U.S. Patent #3,798,359,19 Mar 1974.

[2] L. R. Knudsen, "Block Ciphers-Analysis," Computer Science department, Aarhus University, 1994.

[3] C. E. Shannon, "Communication theory ofsecrecy system," *BSTJ,* vol. 28, pp. 656-715, 1949

[4] NIST, "Federal Information Processing Standards Publication 197 - Specification for the Advanced Encryption Standard (AES)," Available: http://csrc.nist.gov/publication/fips/fips-197.pdf, 2001, [Accessed: Apl 12, 2010]

[5] J. Daemen, L.Knudsen and V. Rijmen, *The block cipher Square*, In Fast Software Encryption, Lecture Notes in Computer Science(LNCS) 1267, Springer-Verlag, 1997

[6] M. Akkar and C. Giraud, "An Implementation of DES and AES, Secure against Some Attacks," *CHES 2001*, LNCS 2162, pp. 309-318, 2001

[7] Hoon.Lim "A Revised Version of CRYPTON," Information and Commuications Research Center

[8] B.Schneier, "The uses and Abuses of Biometrics,"*Communications of the ACM*, vol 42, no, 8, 1999, p136

[9] NIST, "Instruction-level Parallelism in AESC andidates"

[10] NIST, "Data Encryption Standard(DES)", Available:http://www.itl.nist.gov/fip-spubs/fip46-2.htm, 1993, [Accessed: Apl 2, 2010]

[11] B. Schneier, *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (cloth),* 1996
[12] A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
[13] N.Goots, B. Izotov, A. Moldovyan, N. Moldovyan, *Modern Cryptography: Protect Your Data with Fast Block Ciphers* A-LIST Publishing, 2003
[14] D. Stinson, *Cryptography: Theory and Practice,* CRC Press, 1995
[15] Charles H. Bennett, Gilles Brassard, Artur K. Ekert, *Quantum Cryptography*, Scientific American, October 1992

저 자 소 개

최진석(Jin-Suk Choi)
1998년 : 경희대학교 대학원 수학과 (이학석사)
2001년～현재 : 조선대학교 전자계산학과 박사과정

관심분야 : 퍼지 이론, 소프트컴퓨팅, 양자암호
E-male : cjspro1525@naver.com

임광철(Kwang-Cheol Rim)
2006년 : 조선대학교 대학원 수학과 박사
관심분야 : 퍼지 이론, 소프트컴퓨팅, 양자암호
E-male : rim1201@hanmail.net