논문 99-24-5A-17 한국통신학회논문지 '99-5 Vol.24 No.5A

화상 회의에 적합한 T1급 암호 시스템

정회원 이 훈 재*

A Secure T1-Rate Digital Image Conference System

Hon-Jae Lee* *Regular Member*

요 약

본 논문에서는 2비트 메모리를 갖는 7비트 실가산기를 이용한 스트림 암호를 설계하였고, 신속하고 안정성 있는 2중 동기 구조의 전 이중 키 수열 동기 방식과 이를 이용한 암호 시스템을 제안하였다. 제안 시스템은 화상 회의에 적합한 암호 시스템이며, 이에 대한 암호 알고리듬과 동기 성능을 분석하였다.

ABSTRACT

In this paper we propose a secure T1-rate digital image conference system which consists a stream cipher of 7-bit real adder with 2-bit carry and a fast and stable 2-step full-duplex synchronization. And we analyze the cipher algorithm and the synchronization performance of the system.

I. 서 론

암호(cryptology)는 국가 안보 차원에서 보호를 받으면서 인류 역사와 더불어 정치·외교·군사 목적으로 발전해왔다. 금세기들어 통신과 컴퓨터가 발달하면서 암호 기술도 빠른 속도로 발달하고 있으며, 전자 화폐를 포함한 전자 상거래 시대의 개막이 임박하면서 암호가 우리 실생활에 큰 영향을 미치게 되었다. 즉, 고도화된 정보화 사회에서 각종 인증 문제(데이터 무결성, 사용자 인증, 사용 장비 인증 등)나 안전성 문제(프라이버시)를 해결해 줄 수 있는 믿을 만한 기술이 바로 암호라고 할 수 있다[1],[2].

암호화(encipher, encryption)란 누구나 알고 있는 정보인 평문(plaintext, message)을 허용된사람(특정인) 이외에는 알아볼 수 없는 형태의 신호인 암호문(ciphertext, cryptogram)으로 바꾸어주는 변환 과정을 말한다. 반대로 복호화(decipher, decryption)란 허용된 사람만이 암호문으로부터 평문을 찾아낼 수 있는 역변환 과정이다. 암호 공격(attack) 또는 암호 해독(cryptanalysis)은 비인가된 사람이 암호문을 도청하고 평문을 유추하여 프라이버시를 침해하려는 수동적 공격(passive eavesdropping)과 도청을 통해 절단·삽입·대체 등으로 내용을 바꾸거나 발신자를 실제의 발신자가 아닌 것처럼 속이려는 능동적인 공격(active eavesdropping)이 있다. 암호화는 보통 특정인 외에 암호 해독자가 해독할 수 없도록 방법을 비밀로 하거나 암호화 방법은 공개하고 키(key)를 비밀로 보관한다.

원거리 화자간의 화상 회의를 위하여 암호 알고리듬을 설계하려면 우선 고속 암호화가 가능하여야 하며, 채널에서 비트 에러가 발생될 경우 에러 확산이 없어야 한다. 또한 만일에 있을지도 모르는 프레임 손실에 대한 동기 복구 시간이 짧아야 한다. 이러한 암호에 적합한 방식이 스트림 암호이다[3],[4].
본 논문에서는 2비트 메모리를 갖는 7비트 실가산기를 이용한 스트림 암호를 설계하고, 신속하고 안정성 있는 2중 동기 구조의 전 이중 키 수열 동기 방식과 이를 이용한 암호 시스템을 제안하고자 한다. 제안될 시스템은 화상 회의등 T1급 링크 암호에 적합한 암호 시스템이며, 이에 대한 암호 알고리듬과 동기 성능을 분석한다.

* 경운대학교 컴퓨터공학과(hjlee@kyungwoon.ac.kr)
논문번호 : 98255-0619, 접수일자 : 1998년 6월 19일

Ⅱ. 스트림 암호와 동기

스트림 암호는 송·수신 키 수열의 동기 이탈시 그림 1 a)와 같이 통신을 유지하면서 자체 복구가 가능한 자체 동기식 스트림 암호(self-synchronous stream cipher)와 b)와 같이 자체 복구가 불가능하여 별도의 재동기 과정을 통하여 키 수열 동기를 재확립하는 동기식 스트림 암호로 구분된다[4]. 이 중에서 자체 동기식 스트림 암호는 채널 잡음에 대하여 오류 확산이 발생되므로 고품질 선로에서만 사용 가능하다.

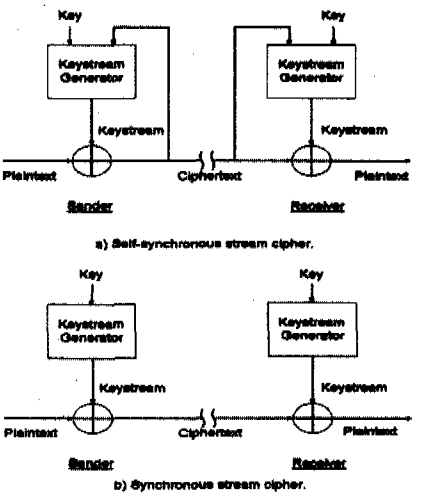


그림 1. 스트림 암호

동기식 스트림 암호는 송·수신 키 수열 발생기에서 발생되는 출력 수열의 동기가 일치되지 않으면 암호문을 평문으로 복호할 수 없기 때문에 키 수열 동기(keystream synchronization)가 필수적이다. 송·수신단에서 동일한 키 수열을 발생시키기 위해서는 키 수열의 시작점을 일치시켜야 하며, 실제로 시작점을 맞추기 위해서는 추가적인 동기 신호의 교환이 따라야 한다. 키 수열 동기 방식은 키 수열의 동기를 일치시키는 횟수에 따라 초기 동기 방식(initial synchronization)과 연속 동기 방식(continuous synchronization)으로 분류된다[4]. 초기 동기 방식은 그림 2 a)와 같이 암호 통신 시작시에만 동기를 확립시켰다가 통신 종료 또는 동기 이탈이 발생될 때까지 동기를 유지하는 방식이고, 연속 동기 방식은 b)와 같이 통신 도중에 주기적으로 동기 신호(SYNPAT)를 삽입하여 재동기시키는 방식이다. 초기 동기 방식에서는 1대 다수 통신시 나중 가입자에게는 암호 통신이 불가능하게 되지만, 연속 동기 방식에서는 나중 가입자도 암호 통신이 가능하다. 그러므로 연속 동기 방식은 통신 효율은 떨어지더라도 채널 오류가 많은 무선 통신망 또는 반이중(half duplex) 통신에 유리하며, 초기 동기 방식은 채널 상태가 양호한 유선 통신망, 전이중(full duplex) 통신에 많이 쓰인다.

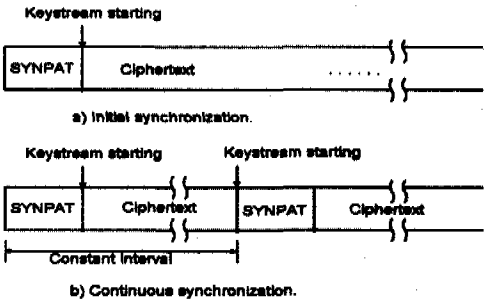


그림 2. 키 수열 동기 프레임 구조

Ⅲ. 암호 시스템 제안

1. 암호 시스템 제안

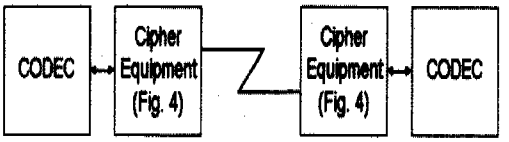


그림 3. 화상 회의 암호 시스템

화상 회의에 적합한 시스템으로 그림 3과 같은 구성을 갖는 암호 시스템을 제안한다. 그림에서 암호 장치(cipher equipment)는 CODEC 후단에 위치하며, 그 시스템 내부 구성은 그림 4와 같다. 블록1은 T1급 속도에 연결하기 위한 코덱 인터페이스 회로로서 T1 AMI 신호나 B8ZS신호[5]를 TTL 신호로 변경하는 신호 레벨 변환(AMI /B8ZS-to-TTL level converter) 기능 및 바이폴라 트위스트 페어 케이블(bipolar twisted-pair cable) 신호로부터 클럭과 데이터를 분리하는 하이브리드 회로를 포함한다. 또한 수신 프레임 신호로부터 프레임 동기를 감시하는

기능을 갖는다. 블록2는 블록1의 역 레벨 변환(TTL-to-AMI/B8ZS level converter) 및 역 하이브리드 회로이다. 이들 블록1 및 2는 이미 상용화된 소자(예, Rockwell사 R8070, T-1/CEPT PCM trans- ceiver)를 이용하여 구현이 가능하다. 블록3은 본 시스템 전체를 제어하는 주 제어 장치(main controller), 블록4는 키 수열 동기 패턴을 발생하는 동기 패턴 발생기(synchronization pattern generator), 블록5와 12는 송·수신 세션 키 버퍼(session key buffer), 블록6과 11은 공개 전송로 상에서 안전하게 세션 키를 분배하기 위한 송·수신 세션 키 구성(session key construction), 블록7과 13은 고비도 특성의 송·수신 키 수열 발생기, 블록8과 14는 송·수신 암호화, 복호화 연산(XOR), 스위치9는 동기 패턴/세션 키/암호문의 구분 선택을 위한 선택 스위치(data selector), 블록10은 송신단에서 발생한 키 수열 동기 패턴을 검출하기 위한 동기 패턴 검출기이다.

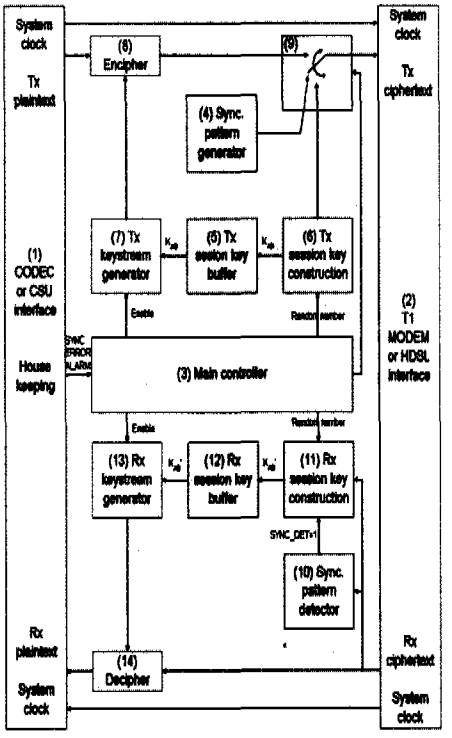


그림 4. 암호 장치의 블록 구성도

2. 키 수열 발생기 설계

스트림 암호의 키 수열 발생 방법은 일반적으로 두 가지 유형으로 나누어진다. 첫 번째 유형은 LFSR을 이용하여 아주 긴 주기와 비선형성을 갖는 형태로 설계함으로써 키 수열에 대한 유추가 불가능하도록 하는 것이며, 두 번째는 블록 암호 형태로 비선형성을 충분히 높인 후 키 수열로 전환시켜 이용하는 방법이다. 후자의 경우는 전자에 비해서 처리 속도가 느리며, DES의 OFB 모드, RC4 그리고 SEAL 등[1]을 들 수 있다. LFSR을 이용한 Geffe 발생기[6]는 3개의 LFSR(L_1 단 길이의 LFSR1, L_2 단 길이의 LFSR2, L_3 단 길이의 LFSR3)의 출력 3비트를 각 각 a_j, b_j, c_j라 할 때 다음과 같은 함수로 출력을 조합함으로서 비선형성을 높였다.

$$f(a_j, b_j, c_j) = a_j \cdot b_j \oplus c_j \cdot /b_j$$

Geffe 발생기의 비도 요소를 분석하면 키 수열 출력의 주기 $P = (2^{L_1}-1)\ (2^{L_2}-1)\ (2^{L_3}-1)$, 선형 복잡도 $LC = (L_1 L_2) + (L_3)(1+L_2)$ 로 크게 나타나지만, 상관 면역도=0차가 된다. 따라서 이 발생기는 Siegenthaler 등[6]에 의하여 상관성 공격에 취약함이 밝혀졌다.

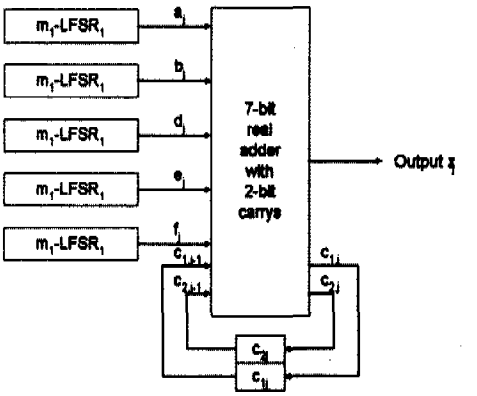


그림 5. 2비트 메모리를 갖는 7비트 실가산기

Rueppel[3]이 제안한 합산 수열 발생기 (summation generator)는 2개의 LFSR 출력 sequence (a_j 및 b_j)와 과거 carry(c_{j-1})를 이용하여 비선형 함수의 출력(z_j) 및 carry(c_j)을 다음과 같이 얻는다.

$$z_j = a_j \oplus b_j \oplus c_{j-1}$$

$$c_j = a_j b_j \oplus (a_j \oplus b_j) c_{j-1},\ j = 0, 1, 2, \ldots$$

Rueppel의 합산 수열 발생기에 대한 비도 요소는 주기 $P = (2^{L1}-1)(2^{L2}-1)$, 선형복잡도 $LC \approx P$, 상관 면역도=1차가 된다. 그러나 합산 수열 발생기도 Geffe 발생기와 비교 시 매우 큰 선형복잡도와 최대 차수 상관면역도를 동시에 갖고 있지만, 키 수열 출력에 연속 "0"이 나타날 경우 carry와 출력간의 상관 관계 특성으로 인하여 Meier등[8]과 Dawson[9]에 의해서 분석되었다. 그러나 이들의 분석에서도 Rueppel의 합산 수열 발생기를 일반화시킨 유형(LFSR이 3개 이상인 경우)에서는 안전성이 입증되었다. 그러므로 본 논문에서는 LFSR이 5개인 7비트 실가산기를 세부 설계 제안한다.

2비트 메모리를 갖는 7비트 실가산기 SUM7-BSG(7-bit real adder with 2-bit carrys)는 그림 5와 같다. 그림에서 입력 비트들(a_j, b_j, d_j, e_j, f_j, $c_{1,j-1}$, $c_{2,j-1}$)을 실수 합산하여 나타난 출력 3-비트 중에서 최하위 비트를 키 수열 출력으로 사용한다. 여기서 출력 3-비트($c_{2,j}$, $c_{1,j}$, y_j) 중에서 결합 함수의 비선형성을 증가시키고, "0"-"1" 균일 분포를 유지하고자 상위 2비트를 캐리 비트로 입력에 궤환시킨다. 이 형태의 결합 함수 입·출력은 표 1과 같고, 이 발생기는 3-비트 실가산기보다 선형 복잡도나 상관 면역도 등 비도 요소가 더 커진다.

표 1. SUM7-BSG의 입·출력 상태

Inputs							Outputs		
a_j	b_j	d_j	e_j	f_j	$c_{1,j-1}$	$c_{2,j-1}$	$c_{1,j}$	$c_{2,j}$	y_j
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	0	0	1
0	0	0	0	0	1	0	0	0	1
0	0	0	0	0	1	1	0	1	0
0	0	0	0	1	0	0	0	0	1
0	0	0	0	1	0	1	0	1	0
0	0	0	0	1	1	0	0	1	0
0	0	0	0	1	1	1	0	1	1
0	0	0	1	0	0	0	0	0	1
.	.	.	.	.	.	.	.	.	.
1	1	1	1	0	0	0	1	0	0
1	1	1	1	0	0	1	1	0	1
1	1	1	1	0	1	0	1	0	1
1	1	1	1	0	1	1	1	1	0
1	1	1	1	1	0	0	1	0	1
1	1	1	1	1	0	1	1	1	0
1	1	1	1	1	1	0	1	1	0
1	1	1	1	1	1	1	1	1	1

본 발생기의 LFSR 구성을 위한 원시 다항식은 참고 문헌[14]에 따라 다음과 같이 발생하였다.

$$g_1(x) = x^{19} + x^9 + x^6 + x^3 + x^2 + x + 1$$

$$g_2(x) = x^{23} + x^{12} + x^6 + x^3 + x^2 + x + 1$$

$$g_3(x) = x^{29} + x^{11} + x^7 + x^3 + x^2 + x + 1$$

$$g_4(x) = x^{31} + x^3 + 1$$

$$g_5(x) = x^{37} + x^{18} + x^2 + x + 1$$

3. 2중 동기 구조의 전이중 키 수열 동기 제안

제안된 2중 동기 신호(SYNC-1, SYNC-2) 및 보조 신호(그림 6)는 다음과 같다.

1) SYNC-1 신호 : 키 수열 동기 상실 시 상대 암호 시스템에게 재동기를 요구하고자 상호 교환하는 동기 신호이다. 이 신호는 상대방에서 응답(ACK=SYNC-1)이 올 때까지 계속해서 반복 전송한다.

2) SYNC-2 신호 : SYNC-1 신호의 상호 교환이 이루어진 후 키 토큰을 주고 받기 위한 비트 위치를 정확히 알려주는 신호이다. 자기 상관 특성이 양호한 신호를 선택하였다.

3) 키 토큰(KT: Key Token) : 세션 키를 만들기 위한 정보로서 송·수신 키 수열의 초기값을 제공하며, 전송시에는 에러 정정 부호를 도입하여 전송한다. 키 토큰의 발생 및 구성은 상호 인증이 가능한 세션 키 분배를 위하여 M-L 키 분배 프로토콜[13]이 적용된다.

4) 프레임 동기 신호 : 화상 데이터 장비(CODEC)는 T1 프레임 구조를 갖는 데이터를 출력하며 프레임 동기 신호[5]가 포함되어 있다. 수신단 암호 장치는 암복호된 프레임 동기 신호를 감시하게 되며, 이 때 정확한 프레임 동기가 이루어지지 않으면 키 수열 동기 에러이며 재동기 복구가 이루어져야 한다. 물론 프레임 동기가 정확히 이루어지면 키 수열 동기도 정상적이라 할 수 있다. 이러한 프레임 동기의 감시는 일반 상용 소자(R8069, R8070 등)를 이용한다.

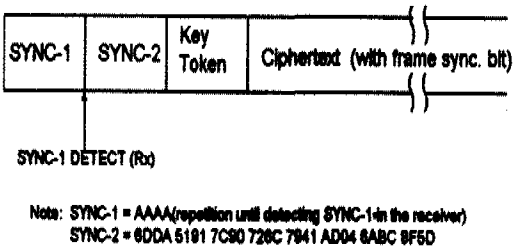


그림 6. 송신단 동기 데이터 형식

동기 패턴 발생은 몇가지 기준[11],[12]을 만족할 수 있도록 구성하였는데, SYNC-1는 재동기 요구 신호이고 SYNC-2는 키 토큰(KT)의 시작 비트 위치를 알려주는 신호이다. 암호 장치의 특성상 통신 동기의 유지에도 불구하고 키 수열 동기의 상실은 정상적인 통신이 이루어질 수 없으며 재동기를 위하여 쌍방 쌍신(full-duplex)에서는 SYNC-1 신호의 상호 교환이 선행되어야 한다. SYNC-2 신호에 대하여 송신된 동기 신호가 수신에서 정확히 검출될 확률(detection probability) P_D, 동기 신호를 놓쳐버릴 미검출 확률(missing probability) P_M, 랜덤하게 수신된 데이터로부터 동기 신호를 엉뚱하게 검출해 내는 오검출 확률(false detection probability) P_F, 그리고 오검출 (평균)시간 T_F등이 동기 검출기의 주요 성능을 나타내는 값이다. 검출 window N, 채널 비트 오류율 B, 전송속도 R bps하에서 N비트 동기 신호 송출시 문턱 값 $N_T(0 \le N_T \le N)$에 따라 이들 동기 확률을 계산 한다. 즉, 수신되는 신호는 랜덤 특성이 좋은 암호문으로 "0"과 "1" 균일 분포를 갖으며, 전송로의 BER이 B에서 1 비트를 한번 전송할 때 틀릴 확률이 B이고 옳을 확률은 $1-B$가 된다. 만약 N 비트로 구성된 동기 신호를 전송하면 전송로의 BER에 의해서 수신단에서는 0에서 N까지 에러가 발생될 수 있으며, 에러 개수 i 에 대한 동기검출 확률밀도함수 p_{Di}와 동기 검출 확률 P_D, 그리고 미검출 확률 P_M은 다음과 같다[11],[12].

$$p_{Di} = {}_NC_i\, B^i\,(1-B)^{N-i},\ i=0,1,\ldots,N \qquad (1)$$

$$P_D = \sum_{i=0}^{N_T} p_{Di} = \sum_{i=0}^{N_T} ({}_NC_i\, B^i\,(1-B)^{N-i}) \qquad (2)$$

$$P_M = 1-P_D \qquad (3)$$

한편 동기 신호를 전송하지 않아도 채널에서의 랜덤 잡음에 의해서 동기신호는 검출될 수 있으므로 이를 오검출(false detection)이라 하며, 에러 수 i 에 대한 오검출 확률 밀도 함수 p_{Fi}와 오검출 확률 P_F, 그리고 평균 오검출 시간 T_F는 아래와 같다[11],[12].

$$p_{Fi} = {}_NC_i\, 0.5^i\,(1-0.5)^{N-i} = {}_NC_i\, 2^{-N} \qquad (4)$$

$$P_F = 2^{-N} \sum_{i=0}^{N_T} {}_NC_i \qquad (5)$$

$$T_F = \frac{1}{P_F \cdot R} \qquad (6)$$

4. 세션 키 생성 및 분배

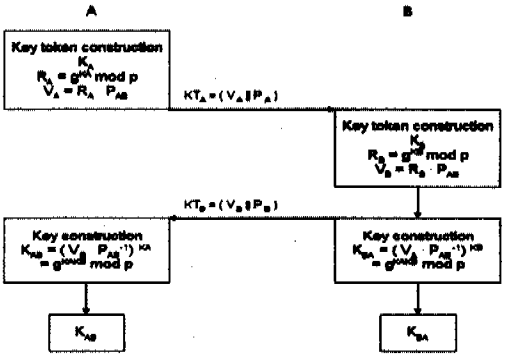


그림 7. M-L 2패스 키 분배 메커니즘

M-L방법[13]의 키 분배 시스템은 two-pass로 공유키(세션 키)를 설정하면서 간접 상호 인증 기능을 제공하며, 적법한 통신자를 A와 B로 나타내고 모든 연산은 $\bmod p$, p는 소수, 상에서 수행한다.

그림 7의 M-L 메카니즘은 다음과 같이 나타낼 수 있다.

(1) 두 통신자 A와 B는 각 각 비밀 키 S_A와 S_B, $1 < S_A, S_B < p-1$를 발생하고, 공개 키 $P_A = g^{S_A} \bmod p$ 와 $P_B = g^{S_B} \bmod p$ 를 공개한다.

(2) A와 B는 각 각 불규칙 정수 K_A와 K_B, $1 < K_A, K_B < p-1$를 발생시켜 $R_A = g^{K_A} \bmod p$ 와 $R_B = g^{K_B} \bmod p$ 를 구한 후 $V_A = R_A \cdot P_{AB}$와 $V_B = R_B \cdot P_{AB}$를 계산하여 공개된 전송망으로 서로 교환한다. 여기서 $P_{AB} = (P_A)^{S_B} = (P_B)^{S_A} \bmod p$ 이다.

(3) 두 통신자는 각 각 공유 키 $K_{AB} = (V_B \cdot P_{AB}^{-1})^{K_A} = g^{K_A K_B} \bmod p$와 $K_{BA} = (V_A \cdot P_{AB}^{-1})^{K_B} = g^{K_A K_B} \bmod p$ 로 같은 값을 얻는다.

M-L방법에서 K_{AB}는 정확한 공개 키와 개인 키를 사용했을 때에만 계산되기 때문에 간접 인증이 가능하며, 불규칙 비밀 수를 사용함으로써 이전 토큰의 재사용 공격을 방지할 수 있다. 그리고 $K_A \neq K_B$라면 생성되는 모든 세션 키는 달라지며, S_A와 S_B가 노출되어도 세션 키를 분석할 수 없기 때문에 키 관리 센터에서도 생성된 세션키를 알 수 없다. 또한 known key attack이나 impersonation

attack이 불가능하다[13].

5. 시스템 분석

표 2. SUM7-BSG의 랜덤 특성 검증 결과

Test items	Threshold	Test results		
		Sample 1	Sample 2	Sample 3
1) Frequency test	3.84	0.548	0.014	0.171
2) Serial test	5.99	0.617	1.003	0.757
3) Generalized				
t-serial t = 3	9.48	1.075	2.710	2.037
t = 4	15.50	1.671	5.205	4.881
t = 5	26.29	10.179	10.927	13.943
4) Poker test				
m = 3	14.067	10.310	9.650	6.105
m = 4	24.996	12.053	8.060	13.420
m = 5	44.654	29.071	26.658	28.921
5) Autocorrelation test	Max. ≤0.05	Max -0.006509	Max -0.006942	Max -0.008744

표 3. 유사 PN 발생기의 비교

Items	Geffe's generator	Rueppel's generator	Proposed generator
Length of each LFSR	L1=37, L2=49, L3=53; L1+L2+L3=139	L1=70, L2=69; L1+L2=139	L1=19, L2=23, L3=29, L4=31, L5=37; L1+L2+L3+L4+L5=139
Period	$P=(2^{L1}-1)(2^{L2}-1)=10^{42}$	$P=(2^{L1}-1)(2^{L2}-1)\approx 10^{42}$	$P=(2^{L1}-1)\cdots(2^{L5}-1)\approx 10^{42}$
Random-ness	Random	Random	Random
Linear complexity	$LC=(L1)(L2)+(L3)(L2+1)=4,463$	$LC \approx P \approx 10^{42}$	$LC \approx P \approx 10^{42}$
Correlation immunity	0	$CI = N-1 = 1$	$CI = N-1 = 4$
Correlation attack	Correlation breakable	Correlation breakable	Secure

제안된 SUM7-BSG에 대한 랜덤 특성 검증 결과는 표 2와 같고, 표본 1에 대한 자기 상관 특성은 그림 8과 같다. 또한 제안 발생기에 대한 주기(P), 선형 복잡도(LC), 상관 면역도(CI)는 다음과 같이 구해진다[3].

$$P=(2^{19}-1)(2^{23}-1)(2^{29}-1)(2^{31}-1)(2^{37}-1)\approx 10^{42}$$

$$LC \approx P \approx 10^{42}$$

$$CI=N-1=4$$

설계된 실가산기는 최대 주기를 보장하고, 선형 복잡도가 최대 주기에 근사하며, 상관 면역도는 N-1로 최대 값이 되므로 상관성 공격을 견딜 수 있는 고비도 결합 함수가 된다. 또한 3가지 샘플 데이터의 통계적인 랜덤 특성[10]-[12]이 기준치 이하로 나타나므로 랜덤 특성이 양호함을 알 수 있다. 표 3에는 기존 발생기와 동등 수준으로 LFSR 전체 길이를 일치시킨 후 비도 요소 비교 결과를 나타내었다.

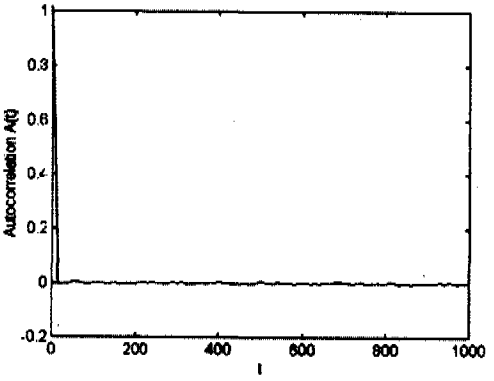


그림 8. SUM7-BSG의 자기상관성 검증 결과

표 4. 동기 확률(BER = 10-1, NT = 25)

N_T/BER	P_F	P_D	P_M
N_T=0	$2.938735877\times10^{-39}$	$1.390084229\times10^{-08}$	$9.999986099\times10^{-01}$
1	$3.790969281\times10^{-37}$	$2.116017137\times10^{-05}$	$9.999788398\times10^{-01}$
2	$2.426514213\times10^{-35}$	$1.606491218\times10^{-04}$	$9.998393508\times10^{-01}$
3	$1.027479040\times10^{-33}$	$8.115975682\times10^{-04}$	$9.991884024\times10^{-01}$
4	$3.237791337\times10^{-32}$	$3.071835266\times10^{-03}$	$9.969281647\times10^{-01}$
5	$8.098686849\times10^{-31}$	$9.300045916\times10^{-03}$	$9.906999540\times10^{-01}$
10	$7.271572314\times10^{-25}$	$2.559625999\times10^{-01}$	$7.440374000\times10^{-01}$
15	$4.465076540\times10^{-20}$	$7.912163018\times10^{-01}$	$2.087836981\times10^{-01}$
20	$4.294311477\times10^{-16}$	$9.838947814\times10^{-01}$	$1.610521856\times10^{-02}$
21	$2.237862512\times10^{-15}$	$9.917126802\times10^{-01}$	$8.287319761\times10^{-03}$
22	$1.103341505\times10^{-14}$	$9.959375044\times10^{-01}$	$4.062495589\times10^{-03}$
23	$5.156943983\times10^{-14}$	$9.981009409\times10^{-01}$	$1.899059021\times10^{-03}$
24	$2.289145482\times10^{-13}$	$9.991526115\times10^{-01}$	$8.473884503\times10^{-04}$
25	$9.666701992\times10^{-13}$	$9.996387170\times10^{-01}$	$3.612829337\times10^{-04}$
26	$3.889317585\times10^{-12}$	$9.998526865\times10^{-01}$	$1.473134079\times10^{-04}$
27	$1.493042993\times10^{-11}$	$9.999425009\times10^{-01}$	$5.749903758\times10^{-05}$
28	$5.475729948\times10^{-11}$	$9.999784979\times10^{-01}$	$2.150200760\times10^{-05}$
29	$1.920913323\times10^{-10}$	$9.999922899\times10^{-01}$	$7.710041871\times10^{-06}$
30	$6.452936410\times10^{-10}$	$9.999973470\times10^{-01}$	$2.652987683\times10^{-06}$
BER=10^{-1}	$9.666701992\times10^{-11}$	0.9996387171	3.612829337×10^{-4}
10^{-2}	$9.666701992\times10^{-11}$	1.0000000000	0.000000000
10^{-3}	$9.666701992\times10^{-11}$	1.0000000000	0.000000000
10^{-4}	$9.666701992\times10^{-11}$	1.0000000000	0.000000000
10^{-5}	$9.666701992\times10^{-11}$	1.0000000000	0.000000000

한편 128 비트 동기 패턴에 대한 동기 성능은 다음과 같이 얻어진다. SYNC-1에 대한 상호 동기 검출이 이루어진 후 SYNC-2 패턴의 동기를 검출하므로 SYNC-1에 대한 동기 확률은 계산에서 제외된다. SYNC-2의 동기 확률은 표 4와 같이 구해진다.

표에서 N_T = 25일 때 BER=0.1에서의 동기 확률은 P_F = 0.97 x 10^{-12}, P_D = 0.9996387, P_M = 0.36 x 10^{-3} 이 되며, 또한 BER=0.01에서는 P_D = 1-10^{-15} 이 되어 고신뢰도 성능을 갖는다고 할 수 있다.

Ⅳ. 결 론

본 논문에서는 T1급 화상 회의에 적합한 암호 시스템을 제안하였다. T1급의 고속, 고비도 암호 통신에 적합한 7비트 실가산 키 수열 발생기를 설계하였고, 키 수열 동기로는 신속하고 안정성이 있는 2중 동기 구조의 전이중 키 수열 동기방식을 제안하여 암호 시스템을 구성하였다. 또한

상호 인증이 가능한 세션 키 분배를 위하여 M-L 키 분배 프로토콜을 적용하였다.

제안 시스템에 대한 분석 결과 10^{42}의 주기, 주기에 근접하는 선형 복잡도, 최고 차수인 4차의 상관 면역도, 그리고 우수한 랜덤 특성등 고비도 암호 시스템이었고, 안전하고 간접 인증이 가능한 세션 키를 분배하며, 하드웨어 구현시 신속하고 안정성이 높은 키 수열 동기가 이루어진다. 본 시스템은 화상 회의등 링크 암호 형태로 적용되는 T1 급(1.544 Mbps) 고속 암호 통신에 적합한 암호 시스템이라고 할 수 있다.

참 고 문 헌

[1] B. Schneier, *Applied Cryptography : Protocols, Algorithms, and Source Code in C (2nd Edition)*, John Wiley & Sons, Inc., New York, USA, 1996.

[2] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, Inc., N.W., Boca Raton, Florida, 1995.

[3] R. A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer- Verlag, 1986.

[4] D. E. R. Denning, *Cryptography and Data Security*, Addison-Wesley Publishing Co., California, 1982.

[5] CCITT Recommendation: 'Physi-cal/Electrical Characteristics of Hierarchical Digital Interface', *CCITT red book*, Vol. III, Rec. G. 703, 1985.

[6] P. R. Geffe, "How to Protect Data with Ciphers that are really hard to Break," Electronics, Pp.99-101, Jan. 1973.

[7] T. Siegenthaler, "Decrypting a Class of Stream Ciphers Using Ciphertext Only," IEEE Trans. on Computer, Vol. C-34, N0.1, pp.81-85, Jan. 1985.

[8] W. Meier and O. Staffelbach, "Correlation Properties of Combiners with Memory in Stream Ciphers," Journal of Cryptology, Vol.5, pp.67-86, 1992.

[9] E. Dawson, "Cryptanalysis of Summation Generator," Advances in Cryptology-AUSCRYPT'92, Lecture Notes in Computer Science, Springer-Verlag, pp.209 -215, 1993.

[10] 이훈재, 문상재, "혼합형 이진 수열 발생 기," 한국통신정보보호학회논문지, 제7권, 제4호, pp.81-90, 1997년 12월.

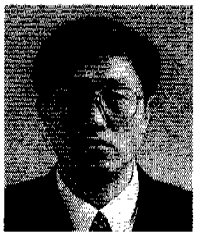
[11] 이훈재, 문상재, "고신뢰도 동기식 스트림 암호 시스템," 한국통신정보보호학회논문 지, 1998년 3월호.

[12] 이훈재, "링크 암호에 적합한 개선된 동기 식 스트림 암호 시스템," 경북대학교 박사 학위논문, 1997년 12월.

[13] 문상재, 이필중, "키 분배 프로토콜의 제 안," 제2회 정보보호와 암호에 관한 워크 샵 논문집 -WISC'90, pp. 117-124, 1990.

[14] B. Park, H. Choi, T. Chang and K. Kang, "Period of Sequences of Primitive Polynomials," *Elect- ronics Letters*, Vol. 29, No. 4, pp. 390-391, Feb. 1993.

이 훈 재(Hoon-Jae Lee) 정회원



1985년 2월 : 경북대학교 전자공학과(공학사)

1987년 2월 : 경북대학교 대학원 전자공학과(공학석사)

1987년 2월~1998년 1월 : 국방과학연구소 선임연구원

1993년 3월~1998년 2월 : 경북대학교 대학원 전자공학과(공학박사)

1998년 3월~현재 : 경운대학교 컴퓨터공학과 전임강사

<주관심 분야> 정보보호 및 인증, 정보통신망