通信情報保護學會論文誌
第 8 卷 第 1 號. 1998. 3

고신뢰도 동기식 스트림 암호 시스템

이 훈 재*, 문 상 재**

A High Reliable Synchronous Stream Cipher System

Hoon Jae Lee, Sang Jae Moon

요 약

본 논문에서는 스트림 암호와 공개 키 알고리듬을 혼합하여 초기 동기 방식의 고신뢰도 동기식 스트림 암호 시스템을 제안하였다. 스트림 동기를 위하여 열악한 채널에서도 동기를 유지할 수 있는 고신뢰도 초기 스트림 동기를 제안하고, 데이터 기밀성을 위한 혼합형 키 수열 발생기, 시스템의 안정성 재고를 위한 ZS 알고리듬, 그리고 세션 키 분배를 위한 M-L 키 분배 방식을 적용하여 분석하였다.

Abstract

In this paper we proposed a high reliable synchronous stream cipher system which combined a stream cipher with a public key cryptosystems. For stream synchronization, we proposed a high reliable initial synchronization method in a noisy channel(BER = 0.1). And we designed and analyzed a hybrid sequence generator for the data confidentiality, a zero suppression algorithm for system stabilization, and M-L protocol for session key exchange.

Keyword : 스트림 암호, 스트림 동기, 키 수열 발생기, zero suppression, 세션 키 분배

I. 서 론

고속 데이터 처리가 요구되는 암호 구현에 있어서는 실질적으로 공개키 암호 보다는 스트림 암호나 블록 암호가 많이 쓰인다. 블록 암호는 소프트웨어 구현이 용이한 반면 채널 에러시 수신단에서 블록 크기만큼 에러가 확산되어 채널 효율(channel efficiency)이 떨어진다. 그러나 스트림 암호는 이러한 에러 확산이 없을 뿐 아니라 비도 수준에 대한 정량화가

* 한국산업대학교 컴퓨터공학과
** 경북대학교 공과대학 전기전자공학부

가능하고, 하드웨어 구현이 용이하며, 통신 지연이 없고, 고속 통신이 가능한 것 등의 잇점으로 인해서 전송로 구간의 링크 암호에 많이 적용된다.

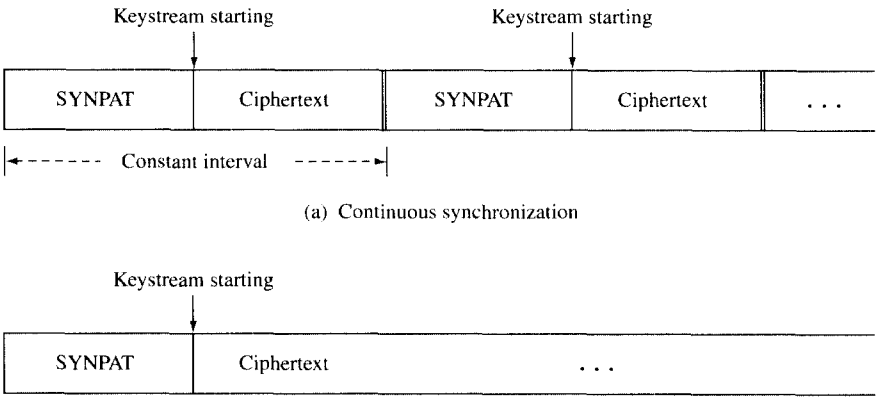
암호 적용 방법은 링크 암호(link encryption)와 단대단 암호(end-to-end encryption)로 분류할 수 있다. 링크 암호는 이웃하는 노드간에 선로 데이터를 보호하기 위해서 모뎀과 노드사이에 암호 장치를 삽입하며, 선로 구간마다 서로 다른 키로 암복호가 이루어지기 때문에 군용 통신망등에 적합하다[1-2]. 단대단 암호는 사용자들간에 전송되는 데이터를 최종단에서만 암복호시키며, 컴퓨터 통신망 보호에 적합하다. 본 논문에서는 전송로 구간 보호에 유리한 링크 암호에 대하여 암호 시스템을 제안 및 분석한다.

스트림 암호 시스템 설계시 키수열에 대한 동기(스트림 동기), 키수열 발생기, 채널 특성을 만족하는 ZS 동기 알고리듬, 세션 키 분배 방식등의 설계가 핵심적으로 필요하다. 송·수신 키 수열 발생기의 출력을 일치시키는 스트림 동기(keystream synchronization)는 초기에만 동기 신호를 교환하는 초기 동기 방식(initial synchronization)과 초기 동기가 이루어진 후에도 주기적인 재동기를 이루는 연속 동기 방식(continuous synchronization)으로 분류되며, 스트림 동기의 성능에 따라 통신 효율이나 통신 신뢰도가 결정되므로 동기 방식 설계에 신중을 기하여야 한다. 본 논문에서는 열악한 무선 환경에서도 동기 성능이 뛰어난 고신뢰도 초기 스트림 동기를 제안한다. 또한 고비도의 키수열 발생을 위하여 혼합형 키수열 발생기를 적용하고, ZS 동기 알고리듬으로는 블록검출형 ZS 알고리듬[6, 7], 상호 인증이 가능한 세션 키 분배를 위하여 M-L 키 분배 프로토콜[8]을 적용한다. 제안 시스템에 대하여 동기 성능과 비도 특성을 분석하고, 컴퓨터 시뮬레이션으로 검증한다.

II. 스트림 동기 방식

스트림 암호는 동기 방식에 따라 자체 동기식(self-synchronous) 스트림 암호와 동기식 스트림 암호로 구분된다. 자체 동기식 스트림 암호는 암호문을 입력에 궤한시킴으로써 스트림 동기 이탈시 수신단에서 자체적으로 동기를 복구할 수 있는 반면, 채널 오류시 이동 레지스터 만큼의 비트 오류가 확산되므로 채널 오류 대책이 마련된 통신망에서만 적용된다. Vigenere 암호, 이동 레지스터 방법, 블록암호의 CFB(cipher feedback) 모드등이 있다[2]. 동기식 스트림 암호는 스트림 동기 이탈시 자체 복구가 불가능하므로 통신을 중단하고 재동기를 확립하여야 한다. 이 방식은 비트 삽입이나 소실과 같은 송·수신간 클럭 슬립(clock slip) 발생시 동기가 이탈되는 문제점을 보완하여야 하지만 비트 오류의 확산이 없으므로 일반적으로 많이 사용된다. 키 수열 발생기, Vernam 암호, Rotor 기계, 블록암호의 OFB(output feedback) 모드, 블록 암호의 계수기(counter) 모드등이 있다[2].

한편, 동기식 스트림 암호에서 송·수신 키 수열을 일치시키는 스트림 동기(keystream synchronization)는 별도의 동기 신호(synchronization pattern, SYNPAT) 교환을 통하여 키 수열의 시작점(starting point)을 일치시킨다. 스트림 동기 방식은 동기 시기에 따라 초기 동기 방식(initial synchronization)과 연속 동기 방식(continuous synchroni- zation)으로 분류된다[2]. 그림 1 (a)의 연속 동기 방식은 통신 도중에 일정한 주기로 재동기시키므로 나중 가입자에게는 유리하지만 통신효율이 나빠서 채널 상태가 극히 저조한 통신망에서만 이용된다. 반면 초기 동기 방식(그림 1 (b))은 암호 통신 시작이나 이탈시에만 동기시키므로 1-대-다수 통신에서 나중 가입자에게는 불리하지만 통신 효율이 좋기 때문에 전이중 통신(full duplex)에서 주로 많이 사용된다.



(a) Continuous synchronization

(b) Initial synchronization

그림 1. 스트림 동기 방법

Fig. 1. Method of stream synchronization.

III. 동기식 스트림 암호 시스템

그림 2는 초기동기방식의 스트림 암호 시스템을 제안한 것이다. 그림에서 블록 (1)은 데이터 터미널 장치(DTE 또는 CODEC), 블록 (2)는 본 시스템 전체를 제어하는 주제어 장치(main controller), 블록 (3)은 스트림 동기 패턴을 발생하는 동기 패턴 발생기(synchronization pattern generator), 블록 (4)와 (12)는 송·수신 세션 키 버퍼(session key buffer), 블록 (5)와 (11)은 공개 전송로상에서 안전하게 세션 키를 분배하기 위한 송·수신 세션 키 구성(session key construction), 블록 (6)과 (13)은 고비도 특성의 송·수신 키 수열 발생기(keystream generator), 블록 (7)과 (14)는 모뎀측 암호문 데이터 특성을 조절하기 위한 송·수신 ZS 알고리듬, 스위치 (8)은 동기 패턴/세션 키/암호문의 구분 선택을 위한 선택 스위치(data selector), 블록 (9)는 선로측 모뎀(DCE: MODEM), 블록 (10)은 송신단에서 발생한 스트림 동기 패턴을 검출하기 위한 동기 패턴 검출기(synchronization pattern detector)이다.

1. 고신뢰도 초기 스트림 동기

스트림 동기부는 그림 2의 블록 (3) 동기 패턴 발생기와 블록 (10) 동기패턴 검출기로 구성되며, 동기식 스트림 암호의 송·수신 키 수열을 일치시키는 역할을 한다. 초기 동기 방식에서는 그림 1 (b)에서와 같이 동기 패턴(SYNPAT)과 세션 키를 일치시킨 후에 암복호가 이루어진다.

다음과 같은 통계 특성을 고려하여 동기 패턴 평가 기준을 설정한다[7, 9].

① 자기 상관 특성이 우수하여야 한다.

② "0"과 "1"의 구성 비율이 비슷하여야 한다.

③ 짧은 run의 반복 횟수는 긴 run의 반복 횟수보다 많아야 한다.

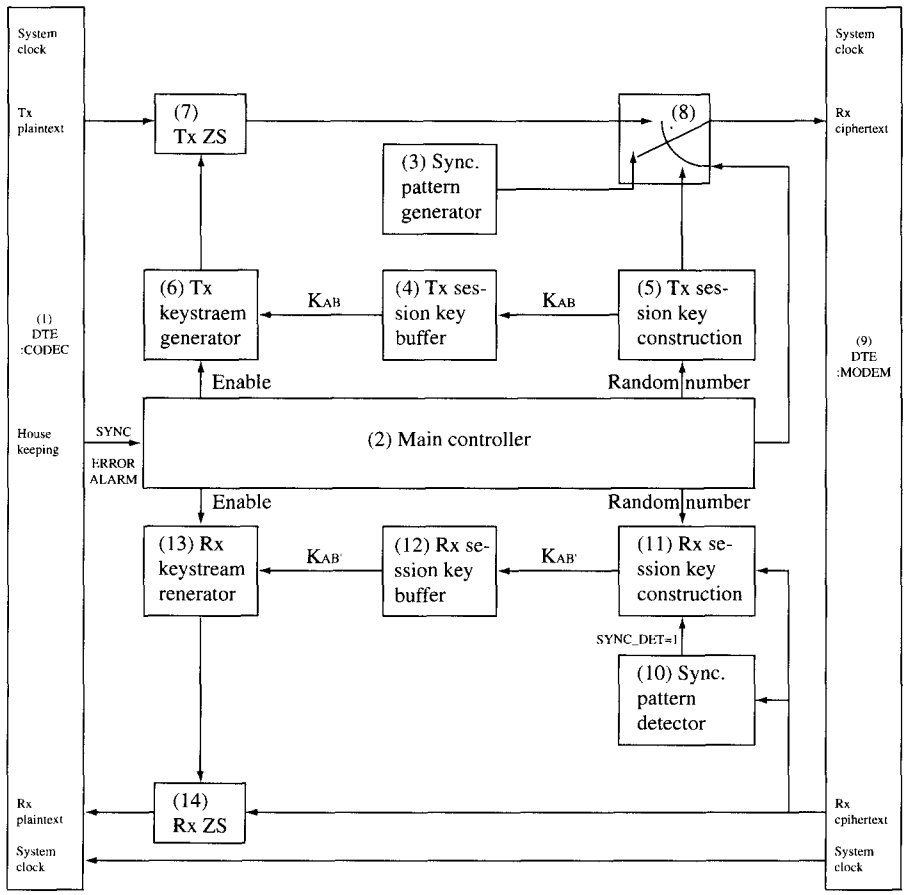


그림 2. 동기식 스트림 암호 시스템

Fig. 2. Synchronous stream cipher system.

상기 기준을 만족시키는 패턴은 그림 3과 같은 Gold 수열 발생기[9]를 통하여 얻을 수 있다. 다음과 같은 원시 다항식을 갖는 31단 LFSR1 및 LFSR2 출력을 서로 XOR시켜 평가 기준을 만족하는 N(여기서는 128) 비트 동기 패턴을 발생하였다.

$$h_1(x) = x^{31} + x^{11} + x^2 + x + 1,$$

$$h_2(x) = x^{31} + x^9 + x^3 + x + 1$$

SYNPAT = 6DDA 5191 7C90 726C 7941

AD04 6ABC 8F5D (hexa)

그림 4의 문턱값을 갖는 동기 패턴 검출기는 송신된 동기 패턴 검출을 위해서 비교부(correlator)와 판정부(decision)로 구분한다. 비교부는 입력 패턴(input pattern)과 기준 패턴(reference pattern) 간의 일치 비트 수(number of agreement bits) $A_g(t)$를 계산해내며, 판정부는 일치 비트수가 문턱 값(threshold, THR) 이상이면 "동기 검출(SYNC_DET=1)"을, 그 외는 "동기 실패(SYNC_DET=0)"를 판단해 낸다.

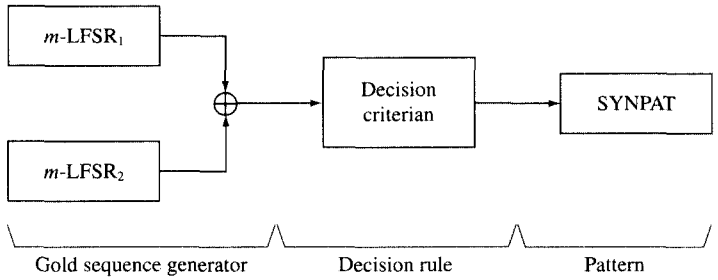


그림 3. 동기 패턴 발생기

Fig. 3. Synchronization pattern generator.

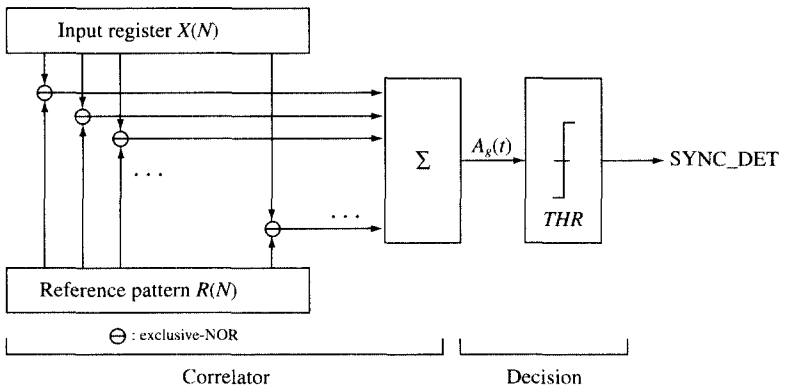


그림 4. 동기 패턴 검출기

Fig. 4. Synchronization pattern detector.

동기 패턴에 대한 자기 상관값 $A(t)$, 문턱값 THR, N_T는 다음과 같다.

$$\begin{cases} A(t) = \dfrac{A_g(t) - D_g(t)}{N} \\ \text{THR} = N - N_T \end{cases} \quad (1)$$

여기서, $A_g(t) = \sum_{i=0}^{N} X(i) \ominus R(i)$는 일치 비트수,

$D_g(t) = \sum_{i=0}^{N} X(i) \oplus R(i)$는 불일치 비트수,

$A_g(t) + D_g(t) = N$이다.

스트림 동기 방식의 성능은 주어진 채널 조건하에서 동기 신호를 얼마나 정확히 검출해 내는가 여부와 유사한 신호를 오판없이 잘 여과해 낼 수 있는가에 달려 있다. 성능을 나타내는 확률 즉, 송신측에서 송신한 동기 신호를 수신측에서 정확히 검출해 내는 검출 확률 P_D (detection probability), 동기 신호를 놓치는 미검출 확률 P_M(missing probability), 그리고 송신측에서 전송하지 않았는데도 잘못 검출해 내는 오검출 확률 P_F(false detection probability), 그리고 오검출 (평균)시간 T_F등

이 동기 검출기의 주요 성능을 나타내는 값이다. 검출 window N, 채널 비트 오류율 B, 전송 속도 R bps하에서 N비트 동기 신호 송출시 문턱 값 $N_T(0 \le N_T \le N)$에 따라 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-B가 된다. 만약 N 비트로 구성된 동기 신호를 전송하면 전송로의 BER에 의해서 수신단에서는 0에서 N까지 에러가 발생될 수 있으며, 에러 개수 i에 대한 동기검출 확률밀도함수 p_{Di}와 동기 검출 확률 P_D, 그리고 미검출 확률 P_M은 다음과 같다[10].

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

$$P_D = \sum_{i=0}^{N_T} p_{Di} = \sum_{i=0}^{N_T} ({}_NC_i\, B^i\, (1 - B)^{N-i}) \qquad (3)$$

$$P_M = 1 - P_D \qquad (4)$$

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

$$p_{Fi} = {}_NC_i\, 0.5^i\, (1 - 0.5)^{N-i} = {}_NC_i\, 2^N \qquad (5)$$

$$P_F = 2^{-N} \sum_{i=0}^{N_T} {}_NC_i \qquad (6)$$

$$T_F = \frac{1}{P_F \cdot R} \qquad (7)$$

2. 혼합형 수열 발생기

스트림 암호의 비도 요소는 각 형태별로 서로 다르고, 비도 요소를 모두 만족하는 발생기를 얻기란 쉽지 않으므로, 각 요소별 특성이 뛰어난 발생기를 적절히 조합하여 고비도 시스템을 설계할 수 있다. 이러한 키수열 발생기의 일종으로 혼합형 키수열 발생기를 들 수 있으며, 본 시스템에서는 F_4를 갖는 HYB-BSG[5]를 적용한다. 설계된 F_4를 갖는 HYB-BSG 발생기의 주기, 선형 복잡도, 상관 면역도 및 출력 키 수열 수는 다음과 같다[5].

- $P \ge 10^{51}$
- $LC \simeq 10^{20}$
- $CI \ge 1$
- $N \simeq 10^{36}$

3. ZS 알고리듬

ZS-1 알고리듬[6, 7]은 $T1$ 회선에서 μ 법칙 PCM 출력 데이터는 8비트 표본 샘플링할 뿐 아니라 $P_i \neq 0$인 조건을 만족하므로 블록 크기 $n = 8$을 채택하면 암호문 출력에서 $k = 15$ 이하로 연속 "0"이 억제될 수 있다.

4. 세션 키 생성 및 분배

D-H 방법[3]은 two-pass로 인증 기능이 없이 두 통신자의 공유 키만을 설정하지만 적은 통신 횟수로 상호 인증을 제공하고 공유 키를 설정할 수 있는 M-L방법[8]의 키 분배 시스템은 two-pass로 공유 키를 설정하면서 간접 상호 인증 기능을 제공한다. 이 시스템을 구현하기 위하여 각 객체 X는 X만이 알고 있는 $S_X \in H$와 $P_X = g^{S_X} \bmod N$를 개인 키로 가져야 한다.

그림 5의 M-L 메카니즘은 다음과 같이 나타낼 수 있다.

(A1) A는 불규칙 비밀 수 $r_A \in H$를 생성하고 $R_A = g^{r_A}$를 계산하여 키 토큰 KT_{A1}을 만들어 B에게 전송한다.

$$KT_{A1} = (R_A \parallel P_A)$$

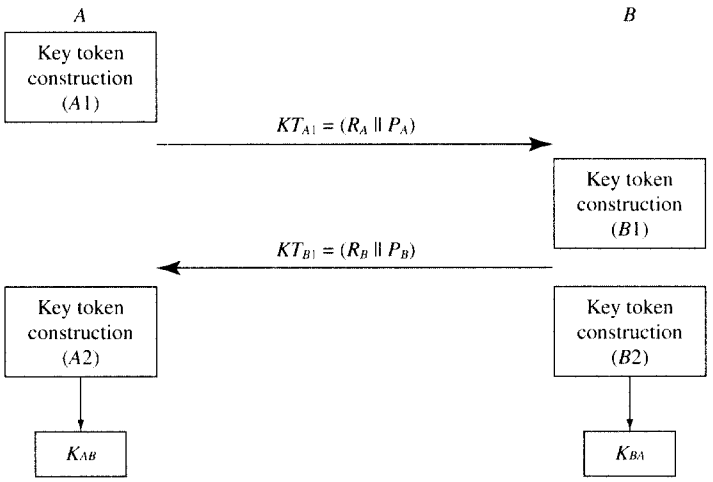


그림 5. M-L 방법의 상호 간접 인증 가능한 2패스 키 분배 메커니즘

Fig. 5. M-L two-pass key agreement mechanism with mutual implicit authentication.

(*B*1) *B*는 불규칙 비밀 수 $r_B \in H$를 생성하고 $R_B = g^{r_B}$를 계산하여 키 토큰KT_B1을 만들어 A에게 전송한다.

$$KT_{B1} = (R_B \| P_B)$$

(*A*2) *A*는 수신된 B의 키 토큰 KT_{B1}으로부터 R_B와 P_B를 추출하여 공유 키를 계산한다.

$$K_{AB} = R_B^{S_A} \cdot P_B^{r_A} = g^{r_B \cdot S_A + r_A \cdot S_B} \quad (8)$$

(*B*2) *B*는 수신된 A의 키 토큰 KT_{A1}으로부터 R_A와 P_A를 추출하여 공유 키를 계산한다.

$$K_{AB} = R_A^{S_B} \cdot P_A^{r_B} = g^{r_A \cdot S_B + r_B \cdot S_A} \quad (9)$$

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. 또한, 전송되는 토큰에 공개 키 정보를 포함시킴으로써 별도의 공개 키 목록이 필요 없어 공개 키 인증 문제가 해결되며 메모리의 효율성을 기할 수 있다. 한편, 키 토큰 전송시 전송 채널상의 오류를 방지하기 위하여 오류 정정 부호를 추가할 수도 있다.

IV. 시뮬레이션 및 분석

1. 스트림 동기 성능 분석

$N = 128$, $N_T = 25$일 때 $THR = 128\text{-}25 = 103$ 이며, 표 1에서는 BER = 0.1에서의 동기 확률이 $P_F = 0.96667 \times 10^{-12}$, $P_D = 0.9996387$, $P_M = 0.36 \times 10^{-3}$ 이고, 표 2에서는 BER = 0.01에서의 검출 확률이 $P_D = 1 - 10^{-15}$ 이상임을 알 수 있다.

2. 암복호 시뮬레이션

제안된 시스템에 대하여 시험 방법을 그림6과 같이 간단히 모델링하여 시험 과정에서의 생성 결과를 요약한다.

1) 기본 파라메터

시스템 기본 파라메터인 원시 원 및 모듈러스는 다음과 같이 취하였다.

- 원시 원 g = 17e4 a2d6 f551 6389 c514 5639 096f dd5c c928 2097 ad21 1a5b ea56 4bab 28c0 6bba 0a00 81f7 a58b 42cf d959 2d72 e001 0c34 bb17 35e6 72cf bf47 d247 ca13 6297 6549
- 모듈러스 N = 9505 e383 51fc 6769 8fcb e0a8 da98 95b2 e74f c59e ce12 6073 8e49 b2da 49b2 32cc 0f8f dc9e 9769 21da 2947 f4ef f5b4 ba61 33d7 34d7 6689 3bd0 801b 1643 4df4 2465

2) 공유 키 생성

공유 키 생성을 위하여 필요한 A와 B 각각에 대한 비밀 키, 랜덤 수, 공개 키, 키 토큰 및 공유 키는 다음과 같이 계산된다.

표 1. NT 가변에 따른 동기 확률(BER = 10^{-1})

Table 1. Sync. probability for variable NT(BER = 10^{-1})

N_T	P_F	P_D	P_M
0	2.938735877055719e-39	1.390084229174165e-06	9.999986099157708e-01
1	3.790969281401877e-37	2.116017137142591e-05	9.999788398286286e-01
2	2.426514213684907e-35	1.606491218512547e-04	9.998393508781488e-01
3	1.027479040902622e-33	8.115975682014417e-04	9.991884024317985e-01
4	3.237791337733303e-32	3.071835266561997e-03	9.969281647334380e-01
5	8.098686849208071e-31	9.300045916275050e-03	9.906999540837249e-01
10	7.271572314915841e-25	2.559625999178171e-01	7.440374000821830e-01
15	4.465076540551982e-20	7.912163018922382e-01	2.087836981077618e-01
20	4.294311477937454e-16	9.838947814335587e-01	1.610521856644131e-02
21	2.237862512500631e-15	9.917126802385244e-01	8.287319761475564e-03
22	1.103341505902957e-14	9.959375044101476e-01	4.062495589852388e-03
23	5.156943983868469e-14	9.981009409782960e-01	1.899059021703953e-03
24	2.289145482496759e-13	9.991526115496695e-01	8.473884503304996e-04
25	9.666701992393990e-13	9.996387170662638e-01	3.612829337361623e-04
26	3.889317585852534e-12	9.998526865920681e-01	1.473134079319482e-04
27	1.493042993527993e-11	9.999425009624112e-01	5.749903758878183e-05
28	5.475729948142875e-11	9.999784979923908e-01	2.150200760919763e-05
29	1.920913323991833e-10	9.999922899581286e-01	7.710041871389350e-06
30	6.452936410277733e-10	9.999973470123162e-01	2.652987683759989e-06

표 2. BER 가변에 따른 동기 확률(NT = 25)

Table 2. Sync. probability for variable BER(NT = 25).

BER	P_F	P_D	P_M
10^{-1}	$9.666701992 \times 10^{-11}$	0.9996387171	$3.612829337 \times 10^{-2}$
10^{-2}	$9.666701992 \times 10^{-11}$	1.0000000000	0.000000000
10^{-3}	$9.666701992 \times 10^{-11}$	1.0000000000	0.000000000
10^{-4}	$9.666701992 \times 10^{-11}$	1.0000000000	0.000000000
10^{-5}	$9.666701992 \times 10^{-11}$	1.0000000000	0.000000000

- 비밀 키 S_A = 8726 376a 5346 ebb1 a9ee acbf 9812 2678 aa4d 27d0
- 공개 키 P_A = 257a 6dc2 50e1 073f c0b9 a39e 32f7 2ac5 d9d9 dcc9 e8a2 b20b a4a8 a61c 6a66 fe05 0f5a 9406 2fa2 8b33 d06d 1c63 ddcd 546a 1111 a1ac 7b87 09db b266 8711 860e 350b
- 비밀 키 S_B = aace 433e cbcb baef 2489 2363 cc47 cbaa 345a 2347
- 공개 키 P_B = 5f78 8f3b cc84 5c58 4d5f 3cbe 1408 7d5a 8add 9f22 1e2f ffdf f0e3 93a0 a75b b585 f141 3157 bb91 66e8 32f9 20a7 c3ea 26fb 6b37 dc2c 2d72 b456 9d5d 78b5 0f16 796d
- 랜덤 수 r_A = eadd cbcb 4573 1029 010d 3176 a999 acdb 4382 ccdd
- 키 토큰 R_A = 0a97 edbe ce1a 9c3e 97e2 f7d0 ec8c d428 1fc7 02cd 1a3f af48 2cb4 281d ac61 5d05 54d5 fe15 2822 17f6 fb72 a02f fd44 a176 9e5b 1c13 8eba dbf1 4d43 89f4 de39 0da4
- 랜덤 수 r_B = bcdc 093a 0112 28a7 0001 4578 dd43 dafe ac12 5762
- 키 토큰 R_B = 92ec 322e 1204 57f6 e34e 6e75 c36c 6980 54ed e28d 213e e797 d3b6 2339 28e8 7f04 c50c 5f6e 3da0 8824 6410 e21f a853 5877 874a 372b d800 02be 0d0b 1fb2 4a1a 552b
- 공유 키 K_{AB} = 145d 1bf1 70ef 6428 c9d9 9bbc ed5f b597 c771 f6fb d373 149f b298 0b28 64bb 0ab0 3dc0 f6a3 98cc b2a6 d805 2ede 1bca 5e4b c2f0 8a3d c93b 8874 abf0 18e1 bcc8 2fad
- 공유 키 K_{BA} = 145d 1bf1 70ef 6428 c9d9 9bbc ed5f b597 c771 f6fb d373 149f b298 0b28 64bb 0ab0 3dc0 f6a3 98cc b2a6 d805 2ede 1bca 5e4b c2f0 8a3d c93b 8874 abf0 18e1 bcc8 2fad

3) 암복호

동일한 공유 키로부터 생성된 키 수열을 이용하여 평문을 암복호하였으며, 이 때 복호 평문은 평문과 동일한 값으로 복호됨을 확인하였다.

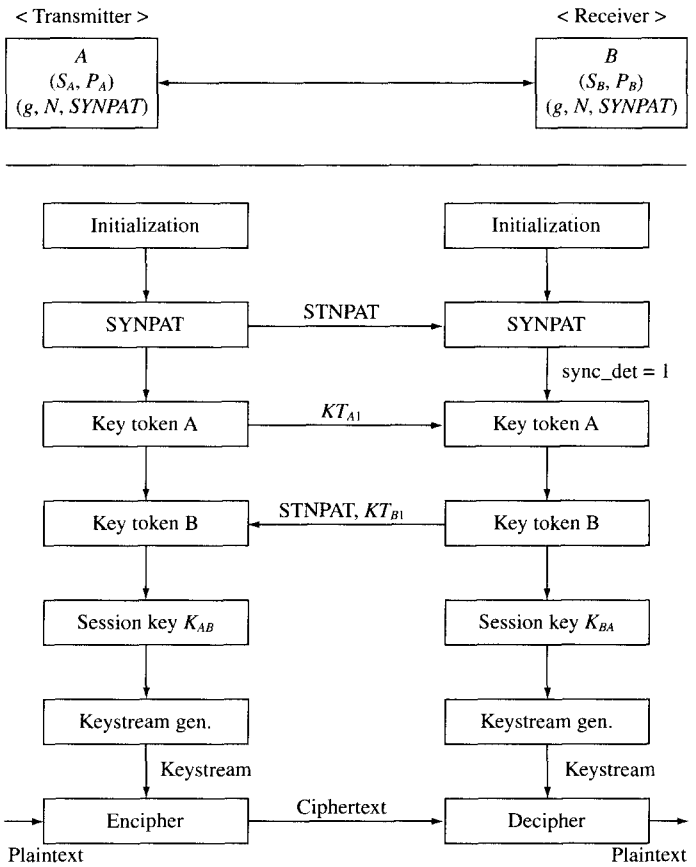


그림 6. 통신 프로토콜

Fig. 6. Communication protocol.

3. 시스템 종합 평가

분석한 바와 같이 설계 시스템은 주기 10^{51}, 선형 복잡도 10^{20}, 1차 상관 면역도, 10^{36}개의 키 수열 수를 갖는 고비도 시스템이고, 안전하고 간접 인증이 되는 세션 키 분배가 가능하다. 또한 키 수열 발생기 구현시 메모리(RAM) 엑세스 시간 10ns 수준에서 DS1급(1.544 Mbps, 647ns/1-bit output)뿐 아니라 DS3급(44.736 Mbps, 22ns/1-bit output)의 고속 암호 통신이 가능함을 알 수 있다. 그리고 BER = 10^{-1}에서 동기 확률이 0.9996 이상, 오검출 확률이 10^{-12}이하인 고신뢰도 시스템이며, 이 때 평균 오검출 시간은 1.544 Mbps 속도에서는 6.7×10^{5}초, 64 kbps에서는 1.6×10^{7}초, 2,400 bps에서는 4.4×10^{8}초가 소요되어 시스템 life cycle이라 할 수 있는 10년(3.15×10^{8}초)에 근사한다. 본 시스템은 소프트웨어나 하드웨어로 구현이 용이하며, 링크 암호에 적합한 모델이다.

VI. 결 론

본 연구에서는 데이터 보호를 위한 스트림 암호와 세션 키 분배를 위한 공개 키 알고리듬을 혼합하여 초기동기방식의 스트림 암호 시스템을 제안, 분석하였다. 시스템 설계를 위하여 열악한 무선 환경에서도 동기 성능이 뛰어난 고신뢰도 초기 스트림 동기를 제안하였고, 고비도의 키수열 발생기를 위하여 혼합형 키수열 발생기를 적용하였으며, ZS 동기 알고리듬으로는 블록검출형 ZS 알고리듬, 상호 인증이 가능한 세션 키 분배를 위하여 M-L 키 분배 프로토콜을 적용하였다.

설계 시스템에 대한 분석 결과 10^{51}의 주기, 10^{20}의 선형 복잡도, 최소 1차 이상의 상관 면역도 및 10^{36}의 키 수열의 수를 갖는 고비도 시스템이고, 안전하고 간접인증이 가능한 세션 키를 분배하며, 하드웨어 구현시 1.544 Mbps급 이상의 고속 암호 통신이 가능함을 알 수 있었다. 또한 BER = 10^{-1}에서도 동기 확률이 0.9996 이상이고 오검출 확률이 10^{-12}이하인 고신뢰도 시스템이며, 소프트웨어나 하드웨어로 구현이 용이하다.

참 고 문 헌

[1] B. Schneier, Applied Cryptography : Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc., New York, USA, 1994.

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

[3] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Trans. on Infor. Theory, Vol. IT-22, No. 6, pp. 644-654, Nov. 1976.

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

[5] 이훈재, 문상재, "혼합형 이진 수열 발생기," 한국정보보호학회논문지, 제7권, 제4호, pp.81-90, 1997년 12월.

[6] 이훈재, 박봉주, 장병화, 문상재, "동기식 스트림 암호를 위한 연속 '0' 억제 알고리듬," 한국통신학회 논문지, 1998년 3월호 게재 예정.

[7] 이훈재, "링크 암호에 적합한 개선된 동기식 스트림 암호 시스템," 경북대학교 박사학위논문, 1997년 12월.

[8] 문상재, 이필중, "키 분배 프로토콜의 제안," 제2회 정보보호와 암호에 관한 워크샵 논문집-WISC' 90, pp. 117-124, 1990.

[9] R. C. Dixon, Spread Spectrum Systems, Wiley, New York, 1976.

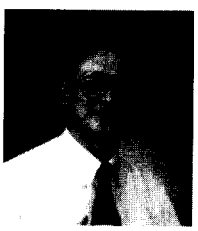
[10] H. J. Beker and F. C. Piper, Secure Speech Communications, Academic Press, London, 1985.

□ 著者紹介

이 훈 재

1985년 2월 경북대학교 공과대학 전자공학과(전자공학, 공학사)
1987년 2월 경북대학교 대학원 전자공학과(통신공학, 공학석사)
1987년 2월 ~ 1998년 1월 국방과학연구소 선임연구원
1993년 3월 ~ 1998년 2월 경북대학교 대학원(정보통신, 공학박사)
1998년 2월 ~ 현재 한국산업대학교 컴퓨터공학과 (전임강사)

※ 주관심분야 : 정보보호기술, 디지털 통신, 정보통신망



문 상 재

1972년 2월 서울대학교 공과대학 공업교육과(전자공학, 공학사)
1974년 2월 서울대학교 대학원 전자공학과(통신공학, 공학석사)
1984년 6월 미국 UCLA(통신공학, 공학박사)
1984년 6월 ~ 1985년 6월 UCLA Postdoctor 근무
1984년 6월 ~ 1985년 6월 미국 OMNET 컨설턴트
1974년 ~ 현재 경북대학교 공과대학 전기전자공학부 교수

※ 주관심분야 : 정보보호, 디지털 통신, 정보통신망