通信情報保護學會論文誌
第 7 卷 第 3 號, 1997. 9

T1 전송시스템 보호를 위한 ZS 동기 알고리듬

이 훈 재* , 박 봉 주*, 장 병 화*, 문 상 재**, 박 영 호***

A ZS Synchronization Algorithm for the Security of T1 Carrier System

Hoonjae Lee*, Bongjoo Park*, Byunghwa Chang*,
Sangjae Moon**, Youngho Park***

요 약

고속 데이터 통신을 위한 T1 전송시스템에 동기식 스트림암호를 적용시 수신 데이터는 매우 긴 비트 간격 동안 연속해서 "0" 또는 "1"이 발생될 수 있다. 이러한 경우 수신클럭 복구가 어려울 뿐 아니라 통신규약을 위반하게 된다. 본 논문에서는 T1 전송시스템에 동기식 스트림암호를 적용시 출력단에서 암호문의 연속 "0" 비트수를 $k(\geq 2)$ 이하로 억제하는 블록검출방식과 직렬검출방식(ZS, Zero Suppression)을 제안한다. 제안된 ZS방식들은 암호학적 비도를 유지하면서 스트림동기 문제를 효과적으로 해결한다.

Abstract

When we apply a synchronous stream cipher to the T1 carrier system, it can occur long consecutive 0's(or 1's) sequences in the received data. In this case, it is difficult to recover receiver clock and violates a communication protocol. This paper proposes block detection and serial detection method which suppress 0's sequences of more than $k(\geq 2)$ of the stream ciphertext in the T1 carrier system. These ZS methods keep security level and solve problems of stream synchronization.

1. 서 론

최근 정보의 홍수라고 불릴 정도로 취급하여야 할 정보가 기하 급수적으로 늘어나는 추세이며, 이에 따라 통신망을 통하여 전송되는 정보의 양도 많아질 뿐 아니라 중요 정보에 대한 보호가 요구되고 있다. 화상회의 등과 같이 통신시스템이 고속화, 대용량화 될수록 고

* 국방과학연구소 ** 경북대학교 전기전자공학부
*** 상주산업대학교 전자공학과

속처리가 가능한 암호시스템의 개발이 필수적이라 할 수 있으며, 이에 적합한 암호방식의 한가지로 동기식 스트림암호시스템[1-3]을 들 수 있다. 동기식 스트림암호는 디지털 평문 데이타에 Pseudo-Noise 특성[3]을 갖는 이진 키수열(keystream)을 XOR시키며 이 때 출력되는 암호문 데이타는 "1"과 "0"이 균일하게 분포되는 특성을 갖는다. 이런 암호방식을 T1 전송시스템(1.544 Mbps 전송속도, 24채널 PCM/TDM, AMI부호 및 D3/PCM frame format방식)[4]등에 적용하면, 수신 데이타속에 연속해서 "0"이 나타나고 클럭 재생이 불안정하게 되는 문제가 발생한다. 즉, 수신 데이터가 0에서 1로 또는 1에서 0으로 천이시 PLL(Phase Locked Loop)은 클럭신호를 복원하며, 송신 데이타상에서 천이가 발생하지 않을 경우("0" 또는 "1"이 연속 한계를 넘어설 경우)에는 수신측에서 클럭복구가 불가능해지는 문제가 있다. 이러한 문제를 해결하기 위해서는 평문에서와 마찬 가지로 암호화 후에도 k=15개 이하로 연속 "0"이 억제되는 암호 방식이 필요하다.

본 연구에서는 수신클럭 복구상의 문제점을 해결할 수 있는 연속 "0" 억제 알고리듬(ZS, Zero Suppression)을 블록검출방식과 직렬검출방식의 2가지 형태로 제안하고자 한다. ZS-1 알고리듬은 암호문에 n 비트 값이 모두 "0"이 나타날 때 같은 시점의 키수열 블록을 대체시킴으로서 연속 "0"의 과다발생을 방지하는 방법이다. 이 때 키수열 블록이 아닌 임의의 랜덤 블록을 대체하면 수신단에서 완전 복구가 불가능하다. 그러나 ZS-1 알고리듬은 스트림암호의 입·출력 상에서 "0" 비트 억제를 위하여 블록단위로 재배열시켜야 하기 때문에 수신단에서 블록동기를 일치시켜야 하는 문제가 있다. 이러한 문제를 해결하기 위하여 수신단에서 입력되는 데이터를 직렬검출(serial detection)토록 하여 검출된 경우에만 블록단위로 대체 또는 역대체시키는 직렬검출/블록대체 방식인 ZS-2 알고리듬을 제안한다. 또한, 본 논문에서는 스트림암호의 적용으로 인한 암호동기오류의 성능저하 및 개선 여부, 비도측면 그리고 오류확산 측면에서 제안한 방식들을 분석한다. 제안한 방식들은 T1 회선 암호화와 병행하여 사용시 암호시스템에서 수신클럭을 불안정하게 유발하는 문제를 해결할 수 있기 때문에 Daemen등[5]이 지적한 잦은 재동기로 인한 비도저하를 막을 수 있으며 다른 여러형태의 통신망에도 적용이 가능하다.

II. Zero Suppression 알고리듬

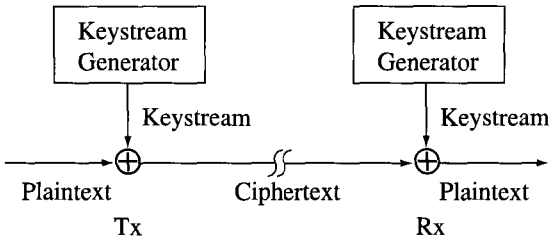
그림 1 a)는 일반적인 동기식 스트림 암호의 모델이며 b)는 ZS 알고리듬을 갖는 동기식 스트림 암호를 나타낸 것이다. ZS 알고리듬에 사용될 변수 k는 최대로 허용되는 연속 "0" 비트수이며, 알고리듬에서 처리하는 블록 크기는 n=[(k+1)/2]이다([x]는 x를 넘지않는 최대정수). 그리고 ZS 알고리듬은 기능상으로 연속 "0"을 검출하는 검출부와 블록크기만큼 다른 값으로 대체시키는 대체부로 나누어진다. 검출부와 대체부는 각각 블록(block)방식과 직렬(serial)방식으로 나누어지며, 제안될 ZS-1 알고리듬은 블록검출/블록대체방식이고, ZS-2 알고리듬은 직렬검출/블록대체방식이다.

1) ZS-1 알고리듬

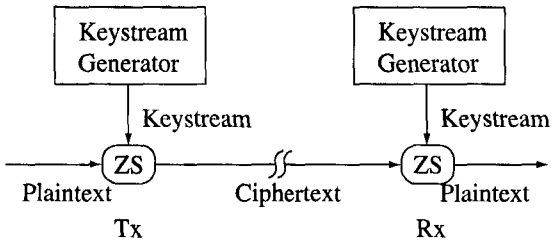
T1 전송시스템에서는 8-비트 채널데이타는 0-레벨(8-비트 모두 "0")이 허용되지 않는다는 사실에 기초하여 블록검출/블록대체방식의 ZS-1 알고리듬을 설계하였다. 편의상 평문블록, 키수열 블록, 암호문 블록, 복호평문블록, **0** 벡터를 다음과 같이 둔다.

i번째 n비트 평문블록 $\mathbf{P}_i$:$(p_{in}, p_{in+1}, \ldots, p_{in+n-1})$

i번째 n비트 키수열 블록 $\mathbf{K}_i$:$(k_{in}, k_{in+1}, \ldots, k_{in+n-1})$



a) Synchronous stream cipher



b) Synchronous stream cipher with ZS

그림 1. 연속 "0" 억제 알고리듬 삽입위치

i번째 n비트 암호문 블록 $\mathbf{C}_i$:$(c_{in}, c_{in+1}, \ldots, c_{in+n-1})$
i번째 n비트 복호평문블록 $\mathbf{Q}_i$:$(q_{in}, q_{in+1}, \ldots, q_{in+n-1})$
n 비트 0 벡터 $\mathbf{0}$:(0, 0, ..., 0)

(가정)

1) 암호 시스템에서 잉여비트를 삽입 또는 삭제할 수 없다.(CODEC과 MODEM 중간에 위치한 암호시스템에서 시스템 클럭 rate를 임의로 증감하기 어려움)
2) 모든 i에 대하여 평문블록 $\mathbf{P}_i \neq \mathbf{0}$이다. 즉, $\mathbf{P}_i$는 nonzero vector($i \geq 0$)임.
3) 키수열 발생기는 암호학적으로 충분한 비도를 갖는다.

(ZS-1 알고리듬) : 그림 2 참조

(송신)

1) $\mathbf{P}_i \oplus \mathbf{K}_i$ 연산된 암호문블록과 $\mathbf{K}_i$가 각각 n단 이동레지스터에 입력된다.
2) $\mathbf{P}_i \oplus \mathbf{K}_i$ 연산된 암호문블록이 $\mathbf{0}$인지 검사한다.
3) $\mathbf{P}_i \oplus \mathbf{K}_i = \mathbf{0}$ 일 경우, $\mathbf{C}_i = \mathbf{K}_i$ 출력시킴.(키수열 블록 출력) 그 외의 경우, $\mathbf{C}_i = \mathbf{P}_i \oplus \mathbf{K}_i$ 출력시킴.(암호문블록 출력)

(수신)

1) $\mathbf{C}_i \oplus \mathbf{K}_i$ 연산된 복호문블록과 $\mathbf{K}_i$가 각각 n단 이동레지스터에 입력된다.
2) $\mathbf{C}_i \oplus \mathbf{K}_i$ 연산된 복호문블록이 $\mathbf{0}$인지 검사한다.
3) $\mathbf{C}_i \oplus \mathbf{K}_i = \mathbf{0}$일 경우, $\mathbf{Q}_i = \mathbf{K}_i$로 출력시킴. 그 외의 경우, $\mathbf{Q}_i = \mathbf{C}_i \oplus \mathbf{K}_i$로 출력시킴.

[정리 1] 임의의 평문블록 $\mathbf{P}_i \neq \mathbf{0}$ 하에서 ZS-1 알고리듬을 동기식 스트림 암호에 적용할 경우 송신단 암호문 출력에 $2n$-1(=k or k-1) 비트 연속 "0"이 억제되며, 채널오류가 없을 경우 수신단에서 평문이 완벽하게 복호된다.

(증명)

(i) 임의의 $\mathbf{P}_i \neq \mathbf{0}$이기 때문에, 송신단에서 ZS

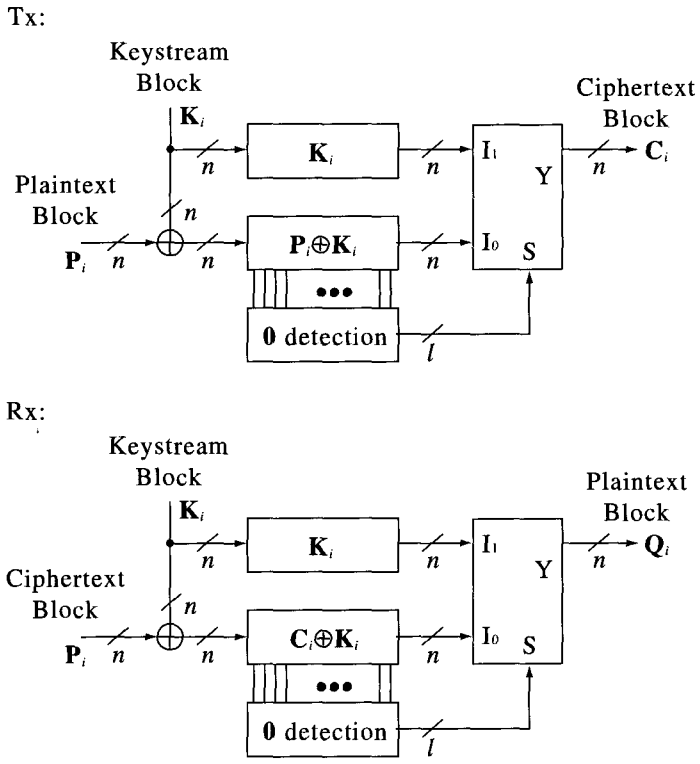


그림 2. ZS-1 알고리듬

출력은 $(2n-1)$ 비트 초과 연속 "0"이 허용되지 않는다.

(ii) $\mathbf{P}_i \oplus \mathbf{K}_i = \mathbf{0}$이 검출될 경우, $\mathbf{C}_i = \mathbf{K}_i$ 이 수신단으로 전송되고, $\mathbf{P}_i = \mathbf{K}_i$이 된다. 이 때 수신단에서는 $\mathbf{C}_i \oplus \mathbf{K}_i = \mathbf{K}_i \oplus \mathbf{K}_i = \mathbf{0}$을 검출함으로서 $\mathbf{Q}_i = \mathbf{K}_i = \mathbf{P}_i$을 출력하게 되고, 결국 평문 블록이 완전히 복호된다.

(iii) $\mathbf{P}_i \oplus \mathbf{K}_i \neq \mathbf{0}$이 검출될 경우, $\mathbf{C}_i = \mathbf{P}_i \oplus \mathbf{K}_i$이 수신단으로 전송된다. 이 때 수신단에서는 $\mathbf{C}_i \oplus \mathbf{K}_i = (\mathbf{P}_i \oplus \mathbf{K}_i) \oplus \mathbf{K}_i = \mathbf{P}_i \neq \mathbf{0}$로 복호하고 $\mathbf{Q}_i = \mathbf{C}_i \oplus \mathbf{K}_i = \mathbf{P}_i$를 출력함으로서 결국 평문 블록이 정상 복호된다.

본 알고리듬의 대체방법 중 $\mathbf{P}_i \oplus \mathbf{K}_i = \mathbf{0}$ 검출시 $\mathbf{C}_i = \mathbf{R}(\neq \mathbf{K}_i)$의 임의 값을 대체시킬 수도 있지만, 이때 수신단에서는 $\mathbf{R}$을 검출하여 역대체 과정에서 암호문 벡터 $\mathbf{R}(=\mathbf{P}_i \oplus \mathbf{K}_i)$값과 대체된 값 $\mathbf{C}_i = \mathbf{R}$ 간의 구별이 불가능하게 된다. 그러므로 임의 벡터 $\mathbf{R}(\neq \mathbf{K}_i)$의 대체 방법은 완전한 알고리듬이 될 수 없으며, 키수열 블록만이 유일한 대체방법임을 알 수 있다.

2) ZS-2 알고리듬

ZS-1 알고리듬은 실제 구현상에 있어서 평문 블록의 모든 비트가 "0"이 아니다($\mathbf{P}_i \neq \mathbf{0}$)는 가정을 충족시키기 위해서 평문에서의 프레임 동기 탐색(searching frame sync.)[6-7]이 필요하며, 또한 수신단에서 블록동기를 유지시켜야 하는 어려움이 따른다. 이는 근본적으로 스트림암호를 블록암호처럼 처리하기 때문에 발생

되는 문제이며, 스트림암호와 유사하게 직렬검출(serial detection)과정을 거쳐서 연속"0"을 검출하고 검출된 경우에 한하여 블록단위로 처리할 필요성이 생긴다. 본 논문에서는 이러한 원리로 직렬검출/블록대체방식의 ZS-2 알고리듬을 추가로 제의하였는데, ZS-1 알고리듬과 달리 블록동기가 불필요하므로 하드웨어 구현이 간단해진다.

ZS-1에서는 블록검출 방법에 따라 데이터를 n비트 크기로 분리하여 정의하였지만, ZS-2에서는 직렬검출 방법이므로 연속되는 이웃 블록간에서 겹칠 수 있도록 i번째 블록들을 다음과 같이 재정의한다.

i번째 n비트 평문블록 $\mathbf{P}_i$:$(p_i, p_{i-1}, \ldots, p_{in+1})$
i번째 n비트 키수열 블록 $\mathbf{K}_i$:$(k_i, k_{i-1}, \ldots, k_{in+1})$
i번째 n비트 암호문 블록 $\mathbf{C}_i$:$(c_i, c_{i-1}, \ldots, c_{in+1})$
i번째 n비트 복호평문블록 $\mathbf{Q}_i$:$(q_i, q_{i-1}, \ldots, q_{in+1})$
n비트 0 벡터 $\mathbf{0}$: (0, 0, ..., 0)

(가정)

1) 암호 시스템에서 잉여비트를 삽입 또는 삭제할 수 없다.(CODEC과 MODEM 중간에 위치한 암호시스템에서 시스템 클럭 rate를 임의로 증감하기 어려움)
2) 평문에서 임의의 k 비트(k=2n-1 또는 k=2n)이하로 연속 "0"이 억제된다.
3) 키수열 발생기는 암호학적으로 충분한 비도를 갖는다.

상기 가정 2)에서는 ZS-1에서와 달리 평문블록에서도 n비트 연속 "0"이 발생될 수 있도록 기준을 완화함으로서 보다 현실적인 접근이 용이하게 하였다. ZS-2 알고리듬은 그림 3과 같이 암호문블록에 n비트 연속 "0"이 검출되면 평문블록을 1블록 대체 출력시키고, 평문블록에 n비트 연속 "0"이 검출되면 이전블록||현블록||다음블록의 평문블록 3블록을 대체 출력시키는 블록검출/블록대체방식으로 송·수신부가 동일하다.

ZS-2 알고리듬 : 그림 3 참조

(송신)

1) $P_i \oplus K_i$ 암호문과 P_i가 비트크기로 각각 n단 이동레지스터에 1비트씩 입력된다.
2) $\mathbf{P}_i$블록과 $\mathbf{P}_i \oplus \mathbf{K}_i$블록이 각각 $\mathbf{0}$인지 검사한다.
3) $\mathbf{P}_i \neq \mathbf{0}$, $\mathbf{P}_i \oplus \mathbf{K}_i \neq \mathbf{0}$인 경우($\mathbf{P}_i \neq \mathbf{K}_i$):$C_{i-n}=P_{i-n} \oplus K_{i-n}$를 1비트 출력시킨다.
   $\mathbf{P}_i \neq \mathbf{0}$, $\mathbf{P}_i \oplus \mathbf{K}_i = \mathbf{0}$인 경우($\mathbf{P}_i = \mathbf{K}_i$):$\mathbf{C}_i=\mathbf{P}_i$의 n비트 블록을 출력시킨다.
   $\mathbf{P}_i = \mathbf{0}$ 경우($\mathbf{P}_i \oplus \mathbf{K}_i$와 무관):$\mathbf{C}_{i-n}=\mathbf{P}_{i-n}$, $\mathbf{C}_i=\mathbf{P}_i$, $\mathbf{C}_{i+n}=\mathbf{P}_{i+n}$ 연속 3블록을 출력시킨다.

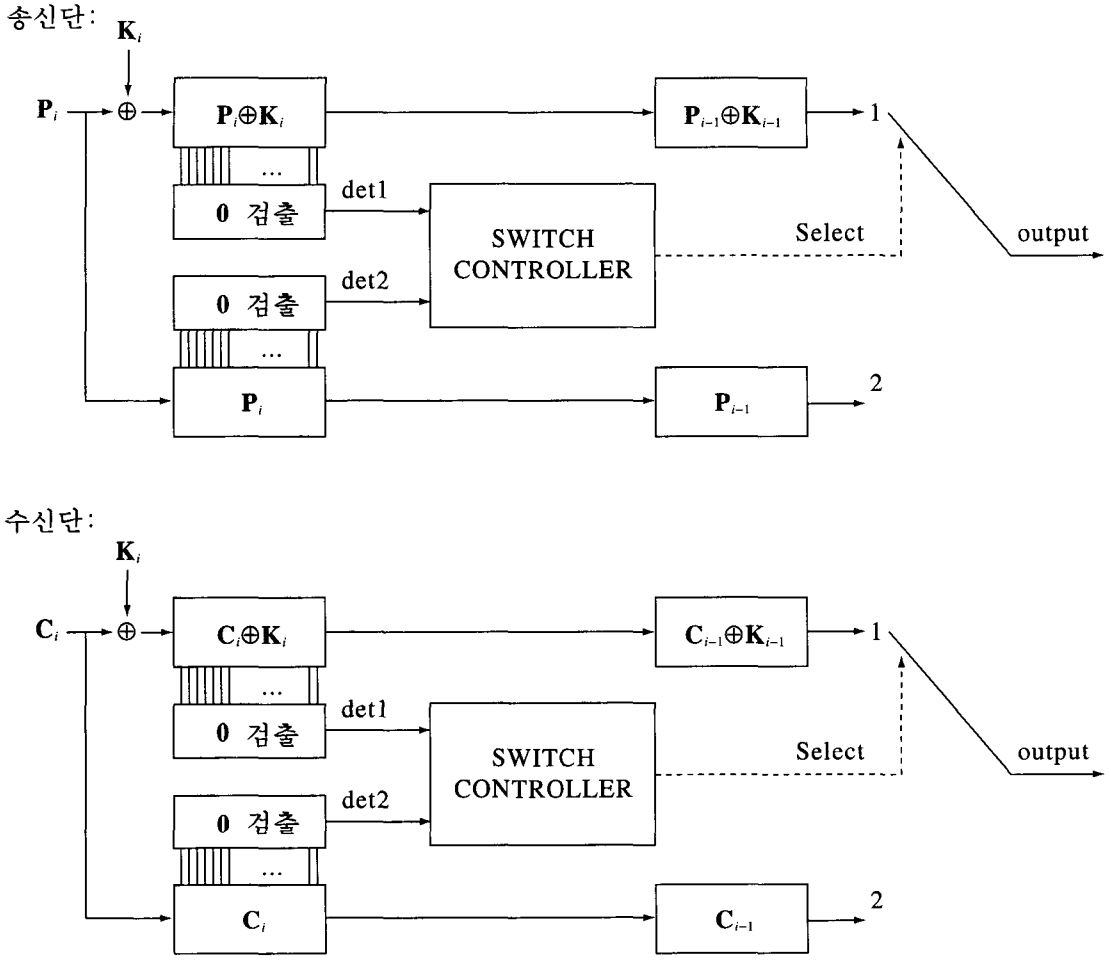
(수신)

1) $C_i \oplus K_i$ 복호문과 C_i가 비트크기로 각각 n단 이동레지스터에 1비트씩 입력된다.
2) $\mathbf{C}_i$블록과 $\mathbf{C}_i \oplus \mathbf{K}_i$블록이 각각 $\mathbf{0}$인지 검사한다.
3) $\mathbf{C}_i \neq \mathbf{0}$, $\mathbf{C}_i \oplus \mathbf{K}_i \neq \mathbf{0}$인 경우($\mathbf{C}_i \neq \mathbf{K}_i$):$Q_{i-n}=C_{i-n}K_{i-n}$를 1비트 출력시킨다.
   $\mathbf{C}_i \neq \mathbf{0}$, $\mathbf{C}_i \oplus \mathbf{K}_i = \mathbf{0}$인 경우($\mathbf{C}_i = \mathbf{K}_i$): $\mathbf{Q}_i=\mathbf{C}_i$의 n비트 블록을 출력시킨다.
   $\mathbf{C}_i = \mathbf{0}$ 경우($\mathbf{C}_i \oplus \mathbf{K}_i$와 무관):$\mathbf{Q}_{i-n}=\mathbf{C}_{i-n}$, $\mathbf{Q}_i=\mathbf{C}_i$, $\mathbf{Q}_{i+n}=\mathbf{C}_{i+n}$ 연속 3블록을 출력시킨다.

[정리 2] 평문에서 임의의 k 비트(k=2n-1 또는 k=2n)이하로 연속 "0"이 억제된다는 가정하에서 ZS-2 알고리듬을 동기식 스트림 암호에 적용할 경우 송신단 암호문 출력에 역시 k 비트 이하로 연속 "0"이 억제되며, 채널오류가 없을 경우 수신단에서 평문이 완벽하게 복호된다.

(증명) 채널오류가 없을 경우 수신평문의 복호상태는 다음과 같이 완벽하게 복호된다.

1) 블록대체 없는 경우($\mathbf{P}_i \neq \mathbf{0}$ 및 $\mathbf{P}_i \oplus \mathbf{K}_i \neq \mathbf{0}$): 송신단에서는 $\mathbf{P}_i \neq \mathbf{0}$ 및 $\mathbf{P}_i \oplus \mathbf{K}_i \neq \mathbf{0}$이므로 $C_i=P_i \oplus K_i$의 1비트 암호문이 송신되고, 수신단에서는 $\mathbf{C}_i \neq \mathbf{0}$ 및 $\mathbf{C}_i \oplus \mathbf{K}_i \neq \mathbf{0}$이므로



* SWITCH CONTROLLER : if det 2=1, select SW=2 and output 3n bits
else if det1=1, select SW=2 and output n bit
else, select SW=1 and output 1 bit

그림 3. ZS-2 알고리듬

$Q_i=C_i \oplus K_i=P_i \oplus K_i \oplus K_i=P_i$로 1비트 평문이 정상복호된다.

2) 1 블록만 대체 있는 경우($\mathbf{P}_i \neq \mathbf{0}$ 및 $\mathbf{P}_i \oplus \mathbf{K}_i=\mathbf{0}$):송신단에서는 $\mathbf{P}_i \neq \mathbf{0}$ 및 $\mathbf{P}_i \oplus \mathbf{K}_i=\mathbf{0}$이므로 $\mathbf{C}_i=\mathbf{P}_i$의 n비트 블록이 송신되고, 수신단에서는 $\mathbf{C}_i \neq \mathbf{0}$ 및 $\mathbf{C}_i \oplus \mathbf{K}_i=\mathbf{0}$이므로 $\mathbf{Q}_i=\mathbf{C}_i=\mathbf{P}_i$로 n비트 블록이 정상복호된다.

3) 3 블록 대체 있는 경우($\mathbf{P}_i=\mathbf{0}$, $\mathbf{P}_i \oplus \mathbf{K}_i$는 무관함):송신단에서는 $\mathbf{P}_i=\mathbf{0}$이므로 $\mathbf{C}_{i-n}=\mathbf{P}_{i-n}$, $\mathbf{C}_i=\mathbf{P}_i$, $\mathbf{C}_{i+n}=\mathbf{P}_{i+n}$의 n비트 3 블록이 송신되고, 수신단에서는 $\mathbf{C}_i=\mathbf{0}$이므로 $\mathbf{Q}_{i-n}=\mathbf{C}_{i-n}=\mathbf{P}_{i-n}$, $\mathbf{Q}_i=\mathbf{C}_i=\mathbf{P}_i$, $\mathbf{Q}_{i+n}=\mathbf{C}_{i+n}=\mathbf{P}_{i+n}$로 각각 n비트 3 블록이 정상복호된다.

ZS-2 알고리듬은 블록 대체된 부분에 채널 오류가 발생되면 오류가 확산되는 단점이 있

지만, $P_i \neq 0$의 가정이 필요없어 T1급 PCM회선등에 적용시 블록동기를 일치시켜야 하는 하드웨어 부담이 감소되므로 실현이 용이하다.

III. 알고리듬 분석

1. 스트림동기 오류 개선

평문통신에서 연속 "0"의 수가 k 비트 이하로 억제된 통신망에 동기식 스트림암호방식을 적용하여 암호통신을 할 경우 스트림 암호문의 랜덤특성 때문에 연속 "0"은 2^{-k}의 확률로 나타난다. 이 때마다 수신단에서는 클럭 슬립(clock slip)이 생겨 송·수신간의 스트림 동기가 이루어지지 않는다. 이러한 스트림동기는 그림4와 같이 전송데이터 수가 늘어날수록 평균 동기이탈 횟수는 늘어난다. 또한 k값이 작을 수록 이 값은 기하 급수적으로 늘어나 원활한 암호통신을 수행할 수 없고, 스트림동기 오류가 일어날 때마다 재동기를 시도하여야하므로 통신성능이 크게 저하된다. 그러나 동기식 스트림암호방식을 개선하여 ZS알고리듬을 적용할 경우 연속 "0"으로 인한 스트림동기오류 문제는 완전히 해결될 수 있으며, 암호통신에서의 통신성능을 크게 개선시킬수 있다.

2. 비도측면 분석

ZS 알고리듬을 갖는 스트림암호에 대하여 암호문만으로 공격(ciphertext-only attack)시 암호문의 랜덤특성이 뛰어나다는 가정에 따라 도청자(eavesdropper)는 송신단에서 대체시킨 키수열 블록과 그렇지 않은 블록을 구별할 방법이 없다. 이는 스트림 암호 원리상 n비트 키수열 블록이 연속 "0"(000...000b)이면 암호문에 평문블록이 그대로 나타나지만 도청자는 이를 구별해 낼 수 없듯이, ZS에서 대체된 키수열블록도 역시 구별해 낼 수 없기 때문이다. 한편, ZS 알고리듬에 대하여 기지 평문 공격(known-plaintext attack)과 선택적 평문 공격(chosen-plaintext attack)을 할 경우에는 키수열 발생기(keystream generator)의 비도에 따라 안전성이 결정되므로 ZS와는 무관하다. 결론적으로 ZS 알고리듬의 적용으로 인한 암호

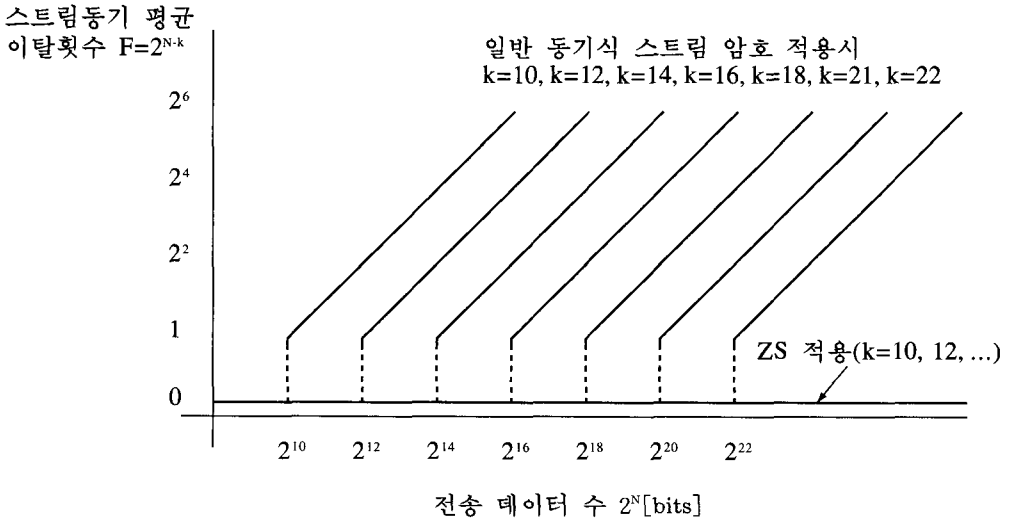


그림 4. 난수 동기 오류 예 (k=10,12,...,22)

학적인 비도수준의 저하는 없으며, 다만 ZS 적용시에도 안전성이 뛰어난 키수열발생기의 설계가 요구된다.

3. 오류 특성

ZS 알고리듬은 채널오류가 없는 이상적인 채널에서는 문제가 없지만, 그렇지 않은 채널에서는 블록대체로인한 비트오류확산(bit error propagation)이 발생되며, 블록크기(n)와 채널오류율(B)에 따른 전체비트오류율이 어느정도로 나타나는지 알아볼 필요가 있다.

1) ZS-1 알고리듬

ZS-1 알고리듬 적용시 송신단에서 균일분포를 갖는 암호문 입력으로부터 송신블록대체가 일어날 확률은 2^{-n}이며, 그 반대 확률은 $1-2^{-n}$이다. 마찬가지로 수신단에서 균일분포를 갖는 복호문 입력으로부터 수신블록대체가 일어날 확률은 2^{-n}이며, 그 반대 확률은 $1-2^{-n}$이다. 이 때 임의의 n에 대하여 P_M은 송신 대체시에 수신단에서 미검출되는 미검출확률(miss-detection probability), P_F는 송신 비대체시에도 채널오류로 인하여 수신단에서 대체블록으로 검출되는 오검출확률(false-detection probability), 채널의 비트 오류율(BER, bit error rate)을 B라 둘때 ZS-1 적용시 전체 비트오류율 P_E는 다음과 같이 계산된다.

P_M = (송신단에서 블록대체될 확률)×(수신단에서 대체블록을 미검출할 확률)×(미검출에 따른 블록내 평균 오류확산비트 수)
$= (2^{-n})[1-(1-B)^n](n/2)=(n)2^{-(n+1)}[1-(1-B)^n]$

P_F = (비대체블록에 채널오류가 발생될 확률)×(수신단에서 대체블록으로 판단할 오검출확률)×(오검출로 인한 블록내 평균 오류확산비트 수)
$= [1-(1-B)^n](2^{-n})(n/2)=(n)2^{-(n+1)}[1-(1-B)^n]$

$P_E = P_M+P_F+B=2P_M+B=(n)2^{-n}[1-(1-B)^n]+B$

2) ZS-2 알고리듬

평문과 암호문이 균일분포를 갖는다는 가정하에서 송신단에서 $\mathbf{P}_i=\mathbf{0}$ 발생확률과 $\mathbf{P}_i\oplus\mathbf{K}_i=\mathbf{0}$ 발생확률은 2^{-n}이고, 각각 3블록, 1블록이 대체된다. 마찬가지로 수신단에서 $\mathbf{C}_i=\mathbf{0}$ 발생확률과 $\mathbf{C}_i\oplus\mathbf{K}_i=\mathbf{0}$ 발생확률은 2^{-n}이고, 각각 3블록, 1블록이 대체된다. 이 때 충분히 큰 n에 대해서 P_{M1}는 송신단에서 1블록 대체시의 미검출확률, P_{M3}는 송신단에서 3블록 대체시의 미검출확률, P_{F1}는 채널오류로 인하여 수신단에서 1블록 대체될 오검출확률, P_{F3}는 채널오류로 인하여 수신단에서 3블록 대체될 오검출확률, 블록대체에 영향을 미치지 않는 채널의 비트오류율을 B라 둘때 전체 비트오류율 P_E는 다음과 같이 계산된다.

P_{M1} = (송신1블록 대체될 확률)×(블록 미검출확률)×(블록내 평균 오류확산비트)
$= (2^{-n})[1-(1-B)^n](n/2)=(n)2^{-(n+1)}[1-(1-B)^n]$

P_{M3} = (송신3블록 대체될 확률)×(블록 미검출확률)×(블록내 평균 오류확산비트)
$= (2^{-n})[1-(1-B)^n](3n/2)=(3n)2^{-(n+1)}[1-(1-B)^n]$

P_{F1} = (블록에 채널오류 발생될 확률)×(수신1블록 대체될 오경보확률)×(블록내 평균 오류확산비트) $= [1-(1-B)^n](2^{-n})(n/2)=(n)2^{-(n+1)}[1-(1-B)^n]$

P_{F3} = (블록에 채널오류 발생될 확률)×(수신3블록 대체될 오경보확률)×(블록내 평균 오류확산비트) $= [1-(1-B)^n](2^{-n})(3n/2)=(3n)2^{-(n+1)}[1-(1-B)^n]$

$$P_E=P_{M1}+P_{M3}+P_{F1}+P_{F3}+B=8P_{M1}+B$$
$$=(n)2^{-(n-2)}[1-(1-B)^n]+B \qquad (5\text{-}3)$$

BER	total error rate of ZS-1(k=15, n=8)	total error rate of ZS-2(k=15, n=8)
10^{-1}	1.1779790×10^{-1}	1.7119160×10^{-1}
10^{-2}	1.2414228×10^{-2}	1.9656913×10^{-2}
10^{-3}	1.2491268×10^{-3}	1.9965071×10^{-3}
10^{-4}	1.2499125×10^{-4}	1.9996500×10^{-4}
10^{-5}	1.2499912×10^{-5}	1.9999650×10^{-5}
10^{-6}	1.2499991×10^{-6}	1.9999965×10^{-6}
10^{-7}	1.2499999×10^{-7}	1.9999997×10^{-7}
10^{-8}	1.2500000×10^{-8}	2.0000000×10^{-8}
10^{-9}	1.2500000×10^{-9}	1.9999999×10^{-9}
10^{-10}	$1.2500000 \times 10^{-10}$	$2.0000000 \times 10^{-10}$
n	total error rate of ZS-1(BER=10^{-5})	total error rate of ZS-2(BER=10^{-5})
6	1.5632498×10^{-5}	3.2529991×10^{-5}
7	1.3833208×10^{-5}	2.5332834×10^{-5}
8	1.2499912×10^{-5}	2.0013229×10^{-5}
9	1.1584116×10^{-5}	1.6336465×10^{-5}
10	1.0977844×10^{-5}	1.3911378×10^{-5}
11	1.0591593×10^{-5}	1.2366372×10^{-5}
15	1.0068753×10^{-5}	1.0275012×10^{-5}
20	1.0003819×10^{-5}	1.0015278×10^{-5}
25	1.0000186×10^{-5}	1.0000746×10^{-5}
31	1.0000004×10^{-5}	1.0000018×10^{-5}

표 1. ZS 알고리듬의 전체 비트오류율(BER 또는 n에 따른)

k=15, n=8인 T1 전송시스템($\mathbf{P}_i \neq \mathbf{0}$)에 링크 암호화(link encryption)로 암호시스템을 설계할 경우 전체 비트오류율은 표 1의 위쪽 결과와 같아지며 n=8일 때 전체 비트오류율은 BER에 비하여 ZS-1에서는 평균 1.25배, ZS-2에서는 약 2배정도 증가하였다. 그러나 이러한 증가는 표 1의 아래쪽 결과에서 알 수 있는 바와 같이 n을 크게할 경우 전체 비트오류율은 1에 근사하게 되어 오류확산은 무시된다.

IV. 결 론

제안된 ZS 알고리듬은 k 비트 초과 연속 "0"이 암호문 출력에 나타날 때 이를 난수블록을 이용하여 대체시킴으로서 평문통신에서 정의된 연속 "0" 제약성을 암호시스템 적용시에도 그대로 유효하게 만들어주는 알고리듬으로서, 수신단에서 평문이 완전하게 복호될 수 있음을 증명을 통해 확인하였다. 즉, 평문통신시에는 source coding출력에 k 비트 초과 연속

"0"이 나타나지 않도록 설계된 통신망에 동기식 스트림 암호를 적용할 경우 송신암호문에 k 비트 연속 "0"이 나타날 확률은 2^{-k}로 크게 늘었으며, 이를 보완한 본 알고리듬 적용시에는 다시 확률이 0으로 떨어진다. 본 알고리듬은 동기식 스트림 암호시스템 적용시에 암호문에서 나타나는 연속 "0" 비트수가 허용된 비트 수를 초과할 경우 나타나는 수신클럭복구의 어려움, 암호시스템의 스트림동기이탈과 재확립으로 데이터 손실 및 비도 저하 요인등 여러 가지 문제점들을 해소시켜 주는 해결책이 된다. 제안된 알고리듬을 T1 전송시스템에 적용시(k=15, n=8), 상기 문제점들이 해결됨을 확인할 수 있었다. 그리고 일반 동기식 스트림 암호에 비하여 ZS 알고리듬의 적용으로 인한 암호학적인 비도수준의 저하는 없음을 알 수 있었으며, 키수열 발생기의 비도가 안전성에 가장 중요한 역할을 담당하기 때문에 ZS 적용시에도 안전성이 뛰어난 키수열발생기의 설계가 요구된다.

참 고 문 헌

[1] H.J. Beker and F.C. Piper, Cipher Systems: The Protection of Communications, orthwood Books, London, 1982.

[2] Henk C.A. van Tilborg, An Introduction to Cryptology, KLUWER ACADEMIC PUBLISHERS, Boston, etc., 1988.

[3] S.W. Golomb, Shift Register Sequences, Holden-Day, San Francisco, 1967.

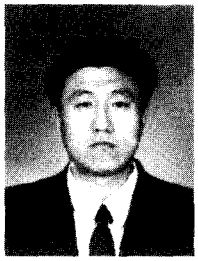
[4] CCITT Rec. G.703: 'Physical/Electrical Characteristics of Hierar-chical Digital Interface,' CCITT red book, Vol.III, 1985.

[5] J. Daemen, R. Govaerts and J. Vandewalle: 'Resynchronization Weaknesses in Synchronous Stream Ciphers', Advances in Cryptology - Eurocrypto'93, Lecture Notes in Computer Science, No. 765, Springer-Verlag, pp.159-167, 1994.

[6] D. E. Dodds, L. R. Button and S. Pan, "Robust Frame Synchronization for Noisy PCM Systems," IEEE Trans. on Comm., Vol. COM-33, No. 5, pp. 465-469, May 1985.

[7] R. Maruta, "A Simple Firmware Realization of PCM Framing Systems," IEEE Trans. on Comm., Vol. COM-28, No. 8, pp. 1228-1223, Aug. 1980.

□ 著者紹介



이 훈 재

1985년 2월 경북대학교 공과대학 전자공학과(전자공학, 공학사)
1987년 2월 경북대학교 대학원 전자공학과(통신공학, 공학석사)
1987년 2월 ~ 현재 국방과학연구소 선임연구원
1993년 3월 ~ 현재 경북대학교 정보통신 박사과정

※ 주관심분야 : 정보보호기술, 디지털 통신, 정보통신망

박 봉 주

1986년 2월 서강대학교 수학과 졸업(이학사)
1988년 2월 서강대학교 대학원 수학과 졸업(이학석사)
1988년 2월 ~ 현재 국방과학연구소 선임연구원

※ 주관심 분야 : 정수론, 대수론, 암호이론

장 병 화

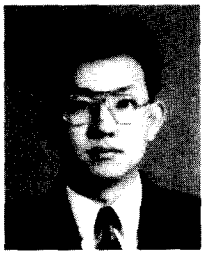
1975년 2월 연세대학교 공과대학 전기공학과 졸업(공학사)
1978년 2월 한국과학기술원 전자공학과 졸업(공학석사)
1988년 2월 한국과학기술원 전자공학과 졸업(공학박사)
1975.11 ~ 1983.3 KIST 연구원
1982년 3월 ~ 현재 국방과학연구소 책임연구원

※ 주관심 분야 : 암호응용, 디지털 통신

문 상 재

1972년 2월 서울대학교 공과대학 공업교육과(전자공학, 공학사)
1974년 2월 서울대학교 대학원 전자공학과(통신공학, 공학석사)
1984년 6월 미국 UCLA(통신대학, 공학박사)
1984년 6월 ~ 85년 6월 UCLA Postdoctor 근무
1984년 6월 ~ 85년 6월 미국 OMNET 컨설턴트
1974년 ~ 현재 경북대학교 공과대학 전기전자공학부 교수

※ 주관심분야 : 정보보호, 디지털 통신, 정보통신망



박 영 호

1989년 2월 경북대학교 공과대학 전자공학과(전자공학, 공학사)
1991년 2월 경북대학교 대학원 전자공학과(통신공학, 공학석사)
1995년 8월 경북대학교 대학원 전자공학과(통신공학, 공학박사)
1996년 3월 ~ 현재 상주산업대학교 전자전기공학과 전임강사
1997년 3월 ~ 현재 한국통신정보보호학회 대구 경북지구 이사

※ 주관심 분야 : 정보보호, 정보통신망