通信情報保護學會論文誌
第 1 卷, 第 1 號, 1991. 12

오류정정부호를 이용한 스트림 암호시스템에 관한 연구

태영수* · 이만영**

A Study on the Stream Cipher System using Error Correcting Codes

Young-Soo Tai and Man-Young Rhee

요 약

본 논문에서는 스트림 암호시스템의 종류와 오류전파 특성에 대해 분석한다. 또한, 암호문 전송중 전송로상에서 발생하는 오류를 제어할 목적으로 DSEC(31, 27) RS 부호를 암호문 귀환 암호시스템에 내부오류제어 및 외부오류제어로 분류하여 적용하고 오류정정과정을 분석한다.

Abstract

In this paper, the stream cipher systems and the error propagation are analyzed. During the ciphertext transmission, for the error control of errors occurred in the channel, the DSEC (31, 27) RS codes will be used for both internal and external error controls for the self-synchronizing cipher system with ciphertext feedback.

1. 서 론

최근 컴퓨터통신에 대한 요구와 수요가 확대되어감에 따라 암호통신기술은 통신망을 통한 정보의 전송과 데이타 저장에 있어서 정보의 수록 및 저장시 제3자에 의해 노출되거나 도난당하는 것을 방지할 목적으로 상용통신(business communication) 및 개인간통신(private communication) 분야에 이르기까지 널리 이용되고 있는 추세이다[7].

이중 근래 상업적으로 이용되는 암호시스템의 하나인 스트림 암호에 기초를 두고 새로운 알고리즘 제안에 대한 연구가 미국을 비롯한 세계 선진각국

* 국립서울산업대학 전자공학과 교수
** 한양대학교 전자통신공학과 명예교수, 한국통신정보보학회 회장

에서서 심도 깊게 수행되고 있다. 스트림 암호 시스템에서는 m단의 선형 귀환 치환 레지스터(linear feedback shift register)에 의해 생성되는 부호계열인 키 비트 수열이 평문(plaintext)과 2원 가산(modulo-2 sum) 되어 암호문(ciphertext)을 형성한다. 이 방식의 주된 이점은 LFSR을 쉽게 구현할 수 있으며 비교적 저렴하는데 있다[11].

이러한 스트림 암호시스템은 키 비트 수열을 생성하는 방법에 따라 키 자동키법(key auto-key mode)을 포함하는 동기 스트림 암호시스템(synchronous stream cipher system)과 암호문 귀환법(ciphertext feedback mode)과 평문 귀환법(plaintext feedback mode)을 포함하는 자기동기 암호시스템(self-synchronizing stream cipher system)으로 나눌 수 있다.

암호시스템에서는 불가피하게 생기는 인위적인 조작과 자연발생잡음으로 인해 오류전파(error propagation)가 발생한다. 디지틀 통신시스템이나 컴퓨터 시스템에서는 이러한 오류를 제어하기 위해서 오류정정부호(error correcting codes)를 사용하는데 암호시스템에서도 오류전파의 대책일환으로 오류정정부호의 도입은 매우 바람직하다[9,10].

따라서, 본 논문에서는 오류정정부호를 스트림 암호시스템에 적용함으로써 완전한 평문 복원에 획기적인 기여를 할 것이며 암호시스템에서의 잡음없는 완벽한 복호, 오류전파의 최소화, 그리고 인증(authentication)등과 같은 문제점을 분석 및 해결할 수 있게 될 것이다. 이를 위해 제2장에서는 스트림 암호시스템의 종류와 오류전파특성을 분석하고, 제3장 오류정정이 가능한 암호문 귀환 암호시스템에서는 RS부호의 기본이론과 효율적 복호알고리즘인 PGZ(Peterson-Gorenstein-Zieler) 알고리즘에 대해 실현예를 암호문 귀환 암호시스템에 적용한다. 특히, 내부 및 외부오류제어기법으로 나누어 각 방식별 특성을 검토한다. 그리고 제4장에서 결론을 맺는다.

2. 스트림 암호시스템

2.1 스트림 암호시스템[11]

스트림 암호시스템에서는 연속적인 비트 x_1, x_2, …, x_n, …을 평문 메세지 **X**로 하고, x_i는 키 스트림 생성기(key stream generator)에서 발생되는 키 비트 스트림인 $\mathbf{Z}=(z_1, z_2, \cdots, z_n, \cdots)$의 i번째요소인 z_i에 의해 암호화 되어 암호문 **Y**의 i번째 비트인 y_i가 생성된다. 이러한 과정은 그림 1과 같고 식(2.1)과 같은 함수관계를 갖는다.

$$y_i = E_{z_i}(x_i) \tag{2.1}$$

이때, 암호변환함수인 E_{z_i}는 암호기의 내부상태(initial state)에 의존하는 시변환함수(time-varing function)로 시간 i일때의 키 스트림 비트 z_i는

$$z_i = f(K, s_i) \tag{2.2}$$

와 같이 외부 키(external key) K와 시간 i일때의 내부상태 s_i에 의해 결정된다. 또한, s_i는 x_i가 y_i로 암호화 된 후 일정한 규칙에 따라 s_{i+1}로 천이된다. 따라서, 동일 평문에 대응되는 암호문이 항상 같은 블럭 암호에 비해, 스트림 암호시스템은 일정한 평문, 암호문쌍을 이루지 않으므로 비밀 유지력면

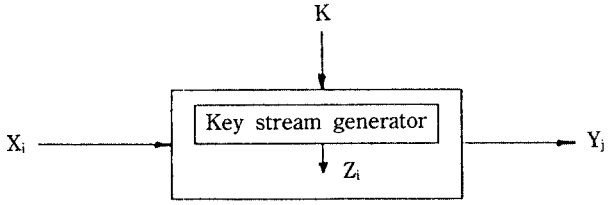


그림 2. 1. 일반적인 스트림 암호시스템

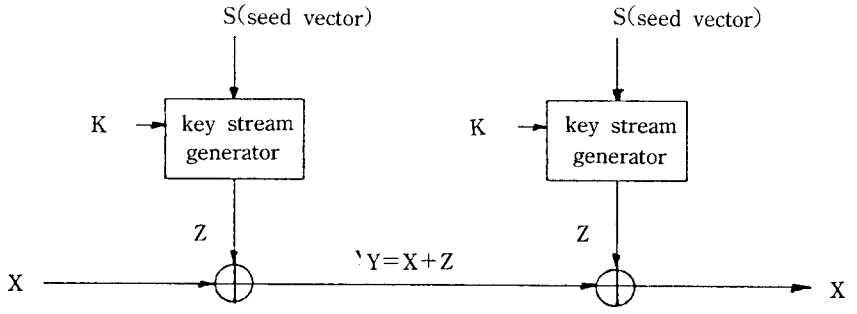
에서 효과적이다.

스트림 암호시스템의 암호화(enciphering)는 보통 $y_i=x_i+z_i$인 EX-OR 함수관계를 이용하고, 복호화(deciphering)는 $x_i=y_i+z_i$가 된다. 따라서, 스트림 암호시스템은 출력과 입력이 서로 뒤바뀐다는 것 이외에는 동일하므로 키 스트림 생성함수에 의해 암호기의 성능이 크게 의존된다.

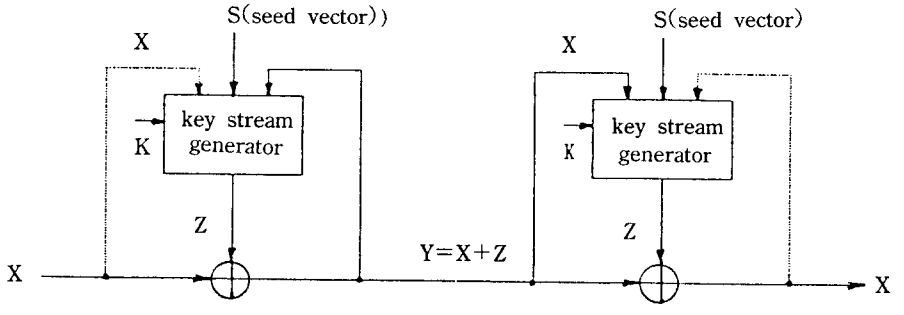
2.2 스트림 암호시스템의 종류와 오류전파특성

스트림 암호시스템은 키 비트 수열(key-bit stream)의 생성방법에 따라 동기식(synchronous)과 자기 동기식(self-synchronizing)으로 분류된다. 전자는 키 비트 수열이 평문 또는 암호문과 독립적으로 생성되어 키 자동키 동기 암호기(key autokey synchronous cipher)를 구성하는 반면에, 후자는 일정한 평문 비트에 지배를 받는 평문 귀환 암호기(plaintext feedback cipher)와 일정한 암호문 비트에 지배를 받는 암호문 귀환 암호기(ciphertext feedback cipher)로 다시 구분되어 지며, 그림 2. 2와 같다.

키 스트림 생성기의 구조를 세분하여 보면 긴 주기의 출력을 갖도록 상태변화를 이끄는 유도부(driving part)와 내부상태의 주기를 유지하면서 출력비트의 무작위성(randomness)을 증가시키는 비선형함수인 결합부(combining part)로 나뉘어진다. 그 예로, 유도부에서는 최대장(maximun length) LFSR을 들 수 있고, 결합부에서는 대수표준형(ANF, algebraic normal form), 비선형 함수



(a) 동기식 스트림 암호



(b) 자기 동기식 스트림 암호

⋯⋯→ : 평문 귀환

——→ : 암호문 귀환

그림 2. 2. 스트림 암호시스템

(nonlinear function)나 DES 알고리즘등을 들 수 있다.

본 절에서는 스트림 암호시스템을 구성시 유도부의 출력변수들을 비선형화 시키는 역할을 하는 결합부는 제외하고 키 스트림 생성기를 LFSR만으로 구성하여 암호문 귀환 암호기에서의 오류전파 특성을 분석한다.

암호문 귀환 암호기는 암호문 비트열을 키 스트림 생성 LFSR에 귀환 입력하여 암호화는 기법으로 m단 LFSR을 이용한 암호문 귀환 암호기의 일반형은 그림 2. 3과 같다.

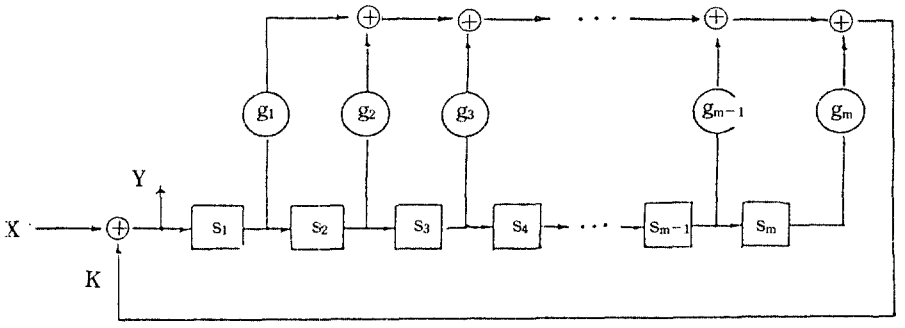


그림 2. 3. 암호문 귀환 암호시스템

그림 2. 3에 의한 m단 LFSR 암호문 귀환 암호기에서 임의의 시간 i에 대한 키 비트 스트림 z_i의 수시적 표현은

$$z_i=\begin{cases}\sum_{k=1}^{i} g_k y_{i-k}+\sum_{k=i+1}^{m} g_k s_{k-i}, & 0\le i\le m-1\\ \sum_{k=1}^{m} g_k y_{i-k}, & i\ge m\end{cases} \qquad (2.3)$$

와 같다. 따라서, 암호화 및 복호화는 식(2-3)을 이용한 비트간 2원 합(modulo 2 sum)에 의해 수행되므로

$$y_i=x_i+z_i \quad (\text{암호화}) \qquad (2.4)$$
$$x_i=y_i+z_i \quad (\text{복호화})$$

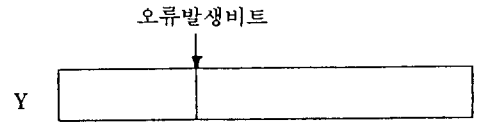
가 된다.

식(2. 3)과 (2. 4)를 근거하여 암호문 귀환 암호기에서의 오류전파특성을 분석할 수 있다. 즉, 시간 t에서의 암호문 비트 y_t에 발생한 오류의 경우는

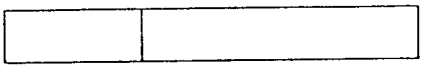
$$\begin{aligned}
&x_{t-1}=y_{t-1}+\mathrm{LFSR}[y_{t-2},\ y_{t-1},\ \cdots,\ y_{t-m-1}]\\
&x_t'=y_t'+\mathrm{LFSR}[y_{t-1},\ y_{t-2},\ \cdots,\ y_{t-m+1}]\\
&x_{t+1}'=y_{t+1}+\mathrm{LFSR}[y_t',\ y_{t-1},\ \cdots,\ y_{t-m+2}]\\
&x_{t+2}'=y_{t+2}+\mathrm{LFSR}[y_{t+1},\ y_t',\ \cdots,\ y_{t-m+2}]\\
&\qquad\vdots \qquad (2.5)\\
&x_{t+m}'=y_{t+m}+\mathrm{LFSR}[y_{t+m-1},\ y_{t+m-2},\ \cdots,\ y_t']\\
&x_{t+m+1}=y_{t+m+1}+\mathrm{LFSR}[y_{t+m},\ y_{t+m-1},\ \cdots,\ y_{t+1}]
\end{aligned}$$

와 같은 오류전파특성을 갖으며, 복호화(deciphering) 단계에서 최대 (m+1회) 관여함을 알 수 있다.

그림 2. 4는 전송도중 한 비트의 오류가 발생한 암호문을 복호시 그 오류전파 영향을 비교한 것이다. 키 자동키 암호시스템은 대응되는 평문 한 비트에만 영향을 받을 뿐이다. 평문 귀환 암호시스템의 경우 오류를 포함한 암호문 비트에 대응되는 평문 비트 뿐만 아니라 그 이후 모든 평문이 오류를 포함한채 복호된다.



(a) 전송도중 한 비트의 오류가 발생한 암호문 Y



(b) 키 자동키 암호시스템에 의해 Y를 복호한 결과

(c) 암호문 귀환 암호시스템에 의해 Y를 복호한 결과

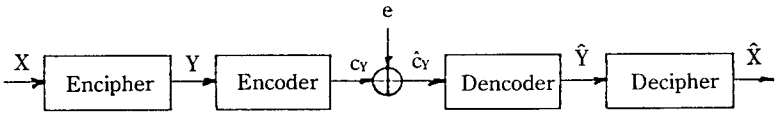
(d) 평문 귀환 암호시스템에 의해 Y를 복호한 결과

그림 2. 4. 스트림 암호시스템의 오류전파특성

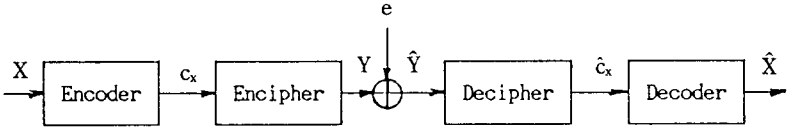
3. 오류정정부호를 도입한 암호문 귀환 암호시스템

오류정정부호는 디지틀통신시스템이나 컴퓨터시스템에서의 데이타 전송시 발생하는 오류를 검출하고 정정하기 위한 기법으로, 암호통신시스템에서도 오류전파에 대한 대책 및 인증(authentiction) 효과의 일환으로 사용가능하다.

암호시스템에 오류정정부호를 도입하여 구현하고자 할때, 그림 3. 1과 같이 두 가지 형태로 나누어진다.



(a) 내부오류제어



(b) 외부오류제어

그림 3. 1. 오류제어를 도입한 암호시스템

본 장에서는 오류정정부호로 사용할 수 있는 Read-Solomon(이하, RS) 부호의 제원에 대해 간략히 소개하고, 정정능력이 적을 경우 효율적인 PGZ(Peterson-Gorenstein-Zieler) 복호알고리즘을 암호문 귀환 암호시스템에 적용하 그 실현예를 보인다.

3.1 RS부호[1,2,9,10]

RS부호는 비 2원 BCH 부호의 한 부류로 산발

오류(random error) 뿐만 아니라 연집오류(burst error)를 모두 정정할 수 있는 강력한 부호로, m 비트로 이루어진 2^m개의 원소를 갖는 GF(2^m) 상에서 오류정정능력이 t라 할때 그 제원(parameter)은 다음과 같다.

부호장(code length) : $n=2^m-1$(symbols)
정보장(information length) : $k=n-2t$(symbols)
최소거리(minimum distance) : $d_{min}=2t+1$ (symbols)

RS부호의 복호는 수신다항식 r(x)에 대한 오증(syndrome) **s**의 계산으로 부터 시작된다. 실제로, v, $1\geq v\geq t$개의 오류가 l_1, l_2, …, l_v의 위치에서 발생하였다면 오류다항식은

$$e(x)=e_{l_1}x^{l_1}+e_{l_2}x^{l_2}\cdots+e_{l_v}x^{l_v} \qquad (3.1)$$

으로 표현된다. 여기서, e_{li}, $1\leq i\leq v$는 GF(2^m)의 원소이다.

오류치(error value)를 $Y_i=el_i$, 오류위치번호(error locator number)를 $Z_i=\alpha^{li}$라 치환하면 오증요소 s_k, $1\leq k\leq 2t$는 식(3. 1)을 이용하여

$$s_\lambda=\sum_{k=1}^{v}Y_kZ_k^\lambda,\quad 1\leq k\leq 2t \qquad (3.2)$$

즉,

$$\begin{aligned}
s_1&=Y_1Z_1+Y_2Z_2+\cdots+Y_vZ_v\\
s_2&=Y_1Z_1^2+Y_2Z_2^2+\cdots+Y_vZ_v^2\\
&\cdots\\
s_{2t}&=Y_1Z_1^{2t}+Y_2Z_2^{2t}+\cdots+Y_vZ_v^{2t}
\end{aligned} \qquad (3.3)$$

와 같은 2t개의 방정식으로 표현가능하다.

또한, 오류위치다항식(error locator polynomial) σ(x)를

$$\begin{aligned}
\sigma(x)&=\prod_{i=1}^{v}(1+Z_ix)\\
&=1+\sigma_1x+\sigma_2x^2+\cdots+\sigma x^v
\end{aligned} \qquad (3.4)$$

라 정의할때, 식(3. 3)과 (3. 4)로 부터

$$\begin{aligned}
&s_{j+v}+\sigma_1s_{j+v-1}+\sigma_2s_{j+v-2}+\cdots\\
&\qquad+\sigma_vs_j=0,\quad 1\leq j\leq v
\end{aligned} \qquad (3.5)$$

와 같은 Newton의 항등식을 얻을 수 있고, 식(3-5)를 행렬로 표시하면

$$\begin{bmatrix}\sigma_v\\ \sigma_{v-1}\\ \cdot\\ \cdot\\ \cdot\\ \sigma_1\end{bmatrix}=\mathbf{M}^{-1}\begin{bmatrix}S_{v+1}\\ S_{v+2}\\ \cdot\\ \cdot\\ \cdot\\ S_{2v}\end{bmatrix} \qquad (3.6)$$

가 된다. 여기서 **M**은 오증요소로 구성된 행렬이다. 즉,

$$\mathbf{M}=\begin{bmatrix}S_1 & S_2 & \cdots & S_v\\ S_2 & S_3 & \cdots & S_{v+1}\\ \cdot & & & \cdot\\ \cdot & & & \cdot\\ \cdot & & & \cdot\\ S_v & S_{v+1} & \cdots & S_{2v}\end{bmatrix} \qquad (3.7)$$

이다. 수신다항식 r(x)로 부터 계산된 오증을 식(3. 6)에 대입하여 오류위치 다항식의 계수를 결정할 수 있다면 이를 이용하여 오류위치번호 Z_i를 구할수 있게 된다. 오류치 Y_k. $1\leq k\leq v$, 역시, 오증요소 s_λ, $1\leq\lambda\leq 2t$와 오류위치번호 Z_k, $1\leq k\leq v$를 이용하면 쉽게 결정할 수 있다.

다음 절에서는 스트림 암호시스템의 오류제어를 위해 유한체 GF(2^5) 상의 DSEC(31, 27) RS 부호를 암호문 귀환 암호시스템에 내부오류 및 외부오류 제어로 구분하여 적용한다.

3.2 암호문 귀환 암호시스템의 내부오류제어

우선, 다음과 같은 내용으로 구성된 평문을 고려하자.

A study on the stream cipher system using error correcting codes.

암호화 과정은 일반적으로 평문내의 각 문자들을 2진수(binary)로 변환하는 것으로 부터 시작된다. 일부 암호시스템에서는 ASCII 부호를 사용하는 것이 편리하므로, 여기에서도 위의 평문을 ASCII 부호를 이용하여 변환하면 표 3.1과 같다.

표 3.1 ASCII 부호로 표현된 평문 내용

00100000	11000001	00100000	01110011	11110100	01110101
01100100	01111001	00100000	11101111	01101110	00100000
11110100	01101000	11100101	00100000	01110011	11110100
11110010	11100101	01100001	01101101	00100000	11100011
11101001	01110000	01101000	11100101	11110010	00100000
01110011	01111001	01110011	11110100	11100101	01101101
00100000	01110101	01110011	11101001	01101110	01100111
00100000	11100101	11110010	11110010	11101111	11110010
00100000	11100011	11101111	11110010	11110010	11100101
11100011	11110100	11101001	01101110	01100111	00100000
11100011	11101111	01100100	11100101	01110011	10101110

표 3.2 암호문 귀환에 의한 키 수열

11100111	11110100	11010011	01010001	10001101	10111100
00010111	01010011	11100111	11111100	01010111	10101111
10101100	11100111	10101001	01110111	01111010	00111100
01100000	00100110	11111010	00000000	00101010	11011110
10111111	00100111	01111101	11101011	11110000	10110000
10110111	00110000	00010011	00110110	10001000	00111110
01000011	11111110	10101000	00101111	10001111	01000000
11000110	10100011	10100111	11101111	10111110	11000100
00110101	11101010	00111011	10110010	00110111	01000101
00110010	11000101	11000011	11110011	10010010	11010011
01111010	10010101	01011111	00101100	00010011	00100110

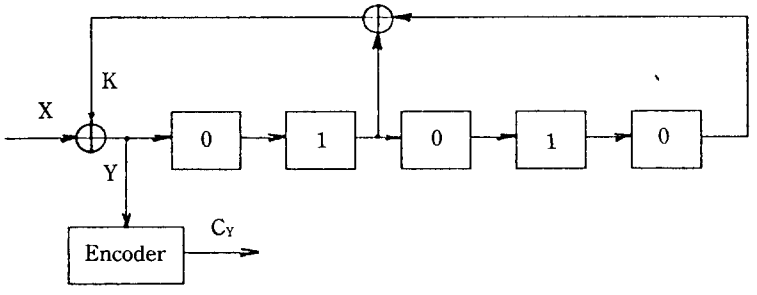


그림 3. 2. 암호문 귀환 키 생성기

표 3.1과 같은 평문 비트계열이 탭 계수가 **T**=(01001)이며 초기치벡터가 **S**=(01010)인 그림 3.2과 같이 m=5인 암호문 귀환 생성기에 입력된다고 할때, 평문 X는 암호문 귀환으로 생성된 표 3.2와 같은 키 수열에 의해 암호문 Y를 발생시킨다. 그 결과는 표 3.3과 같다.

표 3.3 암호문 귀환 방식에 의한 암호문

11000111	00110101	11110011	00100010	01111001	11001001
01110011	00101010	11000111	00010011	00111001	10001111
01011000	10001111	01001100	01010111	00001001	11001000
10010010	11000011	10011011	01101101	00001010	00111101
01010110	01010111	00010101	00001110	00000010	10010000
11000100	01001001	01100000	11000010	01101101	01010011
01100011	10001011	11011011	11000110	11100001	00100111
11100110	01000110	01010101	00011101	01010001	00110110
00010101	00001001	11010100	01000000	11000101	10100000
11010001	00110001	00101010	10011101	11110101	11110011
10011001	01111010	00111011	11001001	01100000	10001000

표 3.3의 밑줄친 부분과 일치하는 암호문 Y가 (31, 27) RS 부호의 생성다항식 $g(x)=\alpha^{10}+\alpha^{29}x+\alpha^{19}x^2+\alpha^{24}x^3+x^4$에 의해 부호화 된다면 5비트 단위로 구성된 암호문 $\mathbf{c}_Y$는 표 3.4와 같다.

표 3.4. 표 3.3의 밑줄친 부분을 부호화시킨 암호문

11100	10001	00100	10110
00011	10011	01101	10110
10000	10100	01111	01010
10110	01010	11100	01010
10000	11100	00000	10100
10000	11000	10001	00100
10110	00001	10000	11101
10111	10000	01010	

만일 전송로상에서 $\mathbf{c}_{21}=(10100)=\alpha^5$과 $\mathbf{c}_{12}=(00000)=0$에서 심볼 오류 $\mathbf{e}_{21}=(10010)=\alpha^{29}$와 $\mathbf{e}_{12}=(10001)=\alpha^{10}$으로 발생하였다면, 수신된 해당심볼들은 $\mathbf{r}_{21}=(00110)=\alpha^{20}$과 $\mathbf{r}_{12}=(10001)=\alpha^{10}$이 될 것이다. 여기서, 오류다항식이 $e(x)=\alpha^{10}x^{12}+\alpha^{29}x^{27}$의 형태로 발생되었다고 가정하자. 발생된 오류를 정정하기 위해서는 우선, 수신된 벡터 r_Y으로 부터 오증을 계산해야 되며, e(x)에 α, α^2, α^3과 α^4를 대입함으로써 오증요소 S_i, $1\le i\le 4$를 모두 구할 수 있다.

$$\begin{aligned}\mathbf{s}_1&=e(\alpha)=\alpha^{17}=(11001)\\ \mathbf{s}_2&=e(\alpha^2)=\alpha^{30}=(01001)\\ \mathbf{s}_3&=e(\alpha^3)=\alpha^{8}=(10110)\\ \mathbf{s}_4&=e(\alpha^4)=\alpha^{11}=(11100)\end{aligned}\qquad(3.8)$$

(31, 27) RS 부호는 이중 심볼 오류정정부호이므로 (v=2), 식(3. 7)의 오증요소행렬식에 의한 표현은 다음과 같다.

$$\mathbf{M}=\begin{bmatrix}\mathbf{s}_1 & \mathbf{s}_2\\ \mathbf{s}_2 & \mathbf{s}_3\end{bmatrix}=\begin{bmatrix}\alpha^{17} & \alpha^{30}\\ \alpha^{30} & \alpha^{8}\end{bmatrix}\qquad(3.9)$$

식 (3. 6)을 이용하면, 오류위치다항식 $\sigma(x)$의 계수는 각각

$$\begin{aligned}\sigma_2&=(\alpha^{16}+\alpha^{10})/(\alpha^{25}+\alpha^{29})=\alpha^6/\alpha^4=\alpha^2\\ \sigma_1&=(\alpha^7+\alpha^{28})/(\alpha^{25}+\alpha^{29})=\alpha/\alpha^4=\alpha^{28}\end{aligned}\qquad(3.10)$$

이 되므로 오류위치다항식 $\sigma(x)$는

$$\sigma(x)=1+\alpha^{28}x+\alpha^{2}\,x^{2} \qquad (3.11)$$

이다. $\sigma(x)=0$이 되는 $\sigma(x)$의 근은 α^{19}와 α^{10}이므로 오류위치번호는 다음과 같다.

$$Z_1=1/\alpha^{19}=\alpha^{12}=(01110)$$
$$Z_2=1/\alpha^{10}=\alpha^{21}=(00011) \qquad (3.12)$$

오류치 Y_1과 Y_2는 식 (3. 3)인

$$s_1=Y_1\,Z_1+Y_2\,Z_2$$
$$s_2=Y_1\,Z_1^2+Y_2\,Z_2^2 \qquad (3.13)$$

으로 부터

$$Y_1=(s_1\,Z_2+s_2)/(Z_1\,Z_2+Z_1^2)$$
$$Y_2=(s_1\,Z_2+s_2)/(Z_1\,Z_2+Z_1^2) \qquad (3.14)$$

가 되어

$$Y_1=\alpha^{10}=(10001)=e_{12}$$
$$Y_2=\alpha^{29}=(10010)=e_{21} \qquad (3.15)$$

임을 알 수 있다. 결국, 오류위치다항식은

$$e(x)=\alpha^{10}x^{12}+\alpha^{29}x^{21} \qquad (3.16)$$

와 같다. $\mathbf{c}=\mathbf{e}+\mathbf{r}$이므로, $\mathbf{c}_{21}=\mathbf{e}_{21}+\mathbf{r}_{21}=\mathbf{Y}_2+\mathbf{r}_{21}=(10010)+(00110)=(10100)$이며, $\mathbf{c}_{12}=\mathbf{e}_{12}+\mathbf{r}_{12}=\mathbf{Y}_1+\mathbf{r}_{12}=(10001)+(10001)=(00000)$이 된다. 이와 같이 표 3.4의 부호화된 암호문은 오류정정 방식을 사용하여 완전하게 복구된다. 마지막으로, 검사심볼을 제거하고, 표 3.2의 키 수열을 이용하여 암호문을 복호하게 되고, 표 3.1에 나타난 평문의 완벽한 형태로 복구할 수 있다.

3.3 암호문 귀환 암호시스템의 외부오류제어

본 절에서는 부호화(encoding) 과정이 암호화(enciphering) 과정보다 먼저 수행되고, 복호(deciphering) 과정이 오류정정(decoding) 과정보다 앞선 암호문 귀환 암호시스템에서의 외부오류제어기법에 대해 다룬다.

이 경우 앞 절에서 사용된 평문 원문과 DSEC (31, 27) RS 부호를 외부오류제어로 적용한다. 그림 3. 3은 앞 절의 분석내용과 비교하기 위해서 키 생성기의 탭계수 $\mathbf{T}=(01001)$와 초기치벡터 $\mathbf{S}=(01010)$를 다시 사용한 암호문 귀환 암호기에서의 외부오류제어 시스템이다.

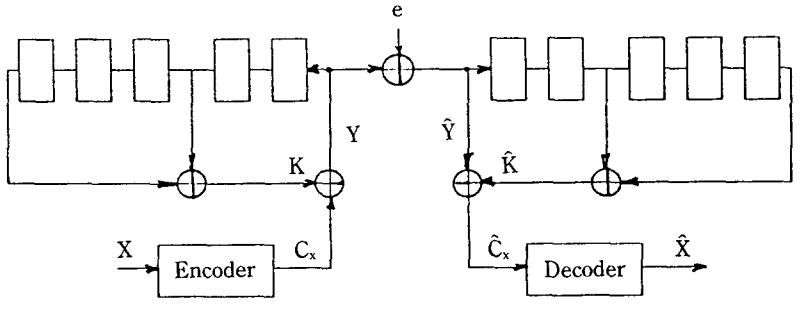


그림 3. 3. 암호문 귀환 외부오류제어시스템

표 3.1의 밑줄친 부분을 5비트 단위로 27개의 입력 심볼로 구성하여 부호화하면 표 3.5와 같다.

표 3.5. 부호화된 평문 $\mathbf{c}_x$

11111	01001	11100	10111	00101	01100
00101	10110	10010	00001	11000	11111
01001	01110	00001	10100	01110	01011
11100	10001	00000	01110	01101	11100
10111	00111	11101	11000	01001	11100
01111					

암호문 **Y**는 암호문에 의해 귀환되는 키 생성기로부터 발생되는 키 수열 **K**와 부호화된 평문 $\mathbf{c}_x$를 암호화함으로써 얻어진다. 대칭형태의 암호시스템(symmetric cryptosystem)에서의 송신자(sender)와 수신자(receiver)에 의해 공유되는 키 수열 **K**에 의해 암호화한 암호문 **Y**는 표 3.6과 같다.

표 3.6. 평문 $\mathbf{c}_x$를 **K**로 암호화한 암호문 **Y**

00001	00000	11010	11011	00111	10110
00011	01110	01111	10010	11101	01000
00001	00110	10011	11001	11001	11101
01011	00010	10111	00001	00101	10100
00011	11010	10011	10110	01100	10101
10111					

전송도중 암호문 **Y**의 $\mathbf{y}_{21}=(10010) \rightarrow \mathbf{y}_{21}'=(00000)$과 $\mathbf{y}_{12}=(01011) \rightarrow \mathbf{y}_{12}'=(11010)$의 위치에서 2개의 심볼오류가 발생하였다고 가정하자. 복호된 평문 $\mathbf{c}_x'$는 **Y**와 수신측 암호문 귀환으로 생성된 K의 2원합으로 구해지며 그 결과는 표 3.7과 같다.

표 3.7. 복호된 평문 $\mathbf{c}_x'$

11111	01001	11100	10111	00101	01100
00101	10110	10010	10111	11010	11111
01001	01110	00001	10100	01110	01011
01001	01000	00000	01110	01101	11100
10111	00111	11101	11000	01001	11100
01111					

표 3.5의 $\mathbf{c}_x$와 표 3.7의 $\mathbf{c}_x'$를 비교하여 다음과 같은 4개의 심볼 오류가 발생하였음을 알 수 있다.

$$\begin{aligned} \mathbf{c}_{21}&=(00001) \rightarrow \mathbf{c}_{21}'=(10111) \\ \mathbf{c}_{20}&=(11000) \rightarrow \mathbf{c}_{20}'=(11010) \\ \mathbf{c}_{12}&=(11100) \rightarrow \mathbf{c}_{12}'=(01001) \\ \mathbf{c}_{11}&=(10001) \rightarrow \mathbf{c}_{11}'=(01001) \end{aligned} \tag{3.17}$$

오류 심볼은 $\mathbf{e}_i=\mathbf{c}_i+\mathbf{c}_i'$으로 표시 되므로,

$$\begin{aligned} \mathbf{e}_{21}&=\mathbf{c}_{21}+\mathbf{c}_{21}'=(10110)=\alpha^8 \\ \mathbf{e}_{20}&=\mathbf{c}_{20}+\mathbf{c}_{20}'=(00010)=\alpha^3 \\ \mathbf{e}_{12}&=\mathbf{c}_{12}+\mathbf{c}_{12}'=(10101)=\alpha^{22} \\ \mathbf{e}_{11}&=\mathbf{c}_{11}+\mathbf{c}_{11}'=(11001)=\alpha^{17} \end{aligned} \tag{3.18}$$

가 되어, 오류다항식은

$$e(x)=\alpha^{17}x^{11}+\alpha^{22}x^{12}+\alpha^3x^{20}+\alpha^8x^{21} \tag{3.19}$$

으로 표현됨을 알 수 있다. 또한, 식 (3. 19)를 이용하여 오증요소는 식 (3. 20)와 같이 얻어진다.

$$\begin{aligned} \mathbf{s}_1&=e(\alpha)=\alpha^{21}=(00011) \\ \mathbf{s}_2&=e(\alpha^2)=\alpha^9=(01011) \\ \mathbf{s}_3&=e(\alpha^3)=\alpha^{22}=(10101) \\ \mathbf{s}_4&=e(\alpha)=\alpha^{22}=(10101) \end{aligned} \tag{3.20}$$

따라서, v=2인 오증요소행렬은

$$\mathbf{M}=\begin{bmatrix} \mathbf{s}_1 & \mathbf{s}_2 \\ \mathbf{s}_2 & \mathbf{s}_3 \end{bmatrix}=\begin{bmatrix} \alpha^{21} & \alpha^9 \\ \alpha^9 & \alpha^{22} \end{bmatrix} \tag{3.21}$$

이며, 여기서, $|\mathbf{M}| = \alpha^{30} \neq 0$이 된다. 따라서, $\sigma(x)$의 계수는

$$\sigma_2 = (\alpha^{13} + \alpha^1)/\alpha^8 = \alpha^6 = (01010)$$
$$\sigma_1 = (\alpha^1 + \alpha^{12})/\alpha^8 = \alpha^{15} = (11111) \qquad (3.22)$$

와 같다. 그러므로 오류위치다항식 $\sigma(x)$는

$$\sigma(x) = 1 + \alpha^{15}x + \alpha^6 x^2 \qquad (3.23)$$

이 되며, $\sigma(x)$의 근은 α^{11}과 α^{14}이다. 이때, 오류위치번호는

$$Z_1 = 1/\alpha^{14} = \alpha^{17} = (11001) \qquad (3.24)$$
$$Z_2 = 1/\alpha^{11} = \alpha^{20} = (00110)$$

이고, 오류치를 계산하면

$$Y_1 = \alpha^{26} = (11101)$$
$$Y_2 = \alpha^8 = (10110) \qquad (3.25)$$

와 같다. 결국, 오류다항식은

$$e(x) = \alpha^{26}x^{17} + \alpha^8 x^{20} \qquad (3.26)$$

으로 표현됨을 알 수 있다. 식 (3-18)과 (3-26)을 이용하여, x^{11}, x^{12}, x^{17}, x^{20}, x^{21}의 위치에서, 5개의 심볼 오류들이 존재함을 알 수 있고, $x_i = e_i + c_i$이므로 실제로 복화된 심볼 x_i는 다음과 같다.

$$\mathbf{x}_{21} = \mathbf{e}_{21} + \mathbf{c}_{21} = (10110) + (00001) = (10010)$$
$$\mathbf{x}_{20} = \mathbf{e}_{20} + \mathbf{c}_{20} = (00010) + (11000) = (00111)$$
$$\mathbf{x}_{17} = \mathbf{e}_{17} + \mathbf{c}_{17} = (11101) + (01110) = (10011)$$
$$\mathbf{x}_{12} = \mathbf{e}_{12} + \mathbf{c}_{12} = (10101) + (11100) = (00001)$$
$$\mathbf{x}_{11} = \mathbf{e}_{11} + \mathbf{c}_{11} = (11001) + (10001) = (10010) \qquad (3.27)$$

그러나, 표 3.8에서와 같이 복호된 오류치는 예상과는 다른 형태로 나타난다.

표 3.8. 잘못 복호된 평문 x

11111	01001	11100	10111	00101	01100
00101	10110	10010	10111	01100	11111
01001	10011	00001	10100	01110	01011
01001	01000	00000	01110	01101	11100
10111	00111	11101	11000	01001	11100
01111					

표 3.8의 검사심볼(x_3, x_2, x_1, x_0)을 제거하고, x_{30}을 x_0로, x_{29}를 x_1으로 대체하여 $X = (x_0, x_1, \cdots, x_{25}, x_{26})$와 같이 역순에 의해 다시 배열하면, 최종적으로 복호화된 평문은 표 3.1의 밑줄친 부분에 해당한다.

표 3.9. 검사심볼을 제거한 후 복구된 평문

11111	01001	11100	10111	00101	01100
00101	10110	10010	10111	01100	11111
01001	10011	00001	10100	01110	01011
01001	01000	00000	01110	01101	11100
10111	00111	11101			

표 3.1의 밑줄친 내용을 표 3.9의 내용으로 대체하면, 표 3.10과 같이 복구된 형태의 ASCII 평문을 구할 수 있다.

표 3.10을 표 3.1과 비교해보면, 표 3.10이 5곳에서 잘못 복호되었다는 것을 쉽게 알 수 있고, 표 3.10과 일치되는 복구된 평문은 아래와 같다.

A study on the stream+31 he% system using error correcting codes.

결과적으로, 암호문 귀환 암호기를 이용하여 외부오류제어 방식을 채택할때 전송로 상에서 발생한 이중 오류의 경우 DSEC (31, 27) RS 부호를 사용하여 복호 과정을 거친다할지라도 4개의 심볼 오류가 정정되지 않기 때문에 오류제어 방법으로는 부적합 하다는 사실을 알 수 있다. 반면에 내부 오류정정 방법은 앞 절에서 분석된 바와 같이 오

표 3.10 복구된 ASCII 평문

00100000	11000001	00100000	01110011	11110100	01110101
01100100	01111001	00100000	11101111	01101110	00100000
11110100	01101000	11100101	00100000	01110011	11110100
11110010	11100101	01100001	01101101	00101011	10110011
11101001	10011000	01101000	11100101	10100101	00000000
01110011	01111001	01110011	11110100	11100101	01101101
00100000	01110101	01110011	11101001	01101110	01100111
00100000	11100101	11110010	11110010	11101111	11110010
00100000	11100011	11101111	11110010	11110010	11100101
11100011	11110100	11101001	01101110	01100111	00100000
11100011	11101111	01100100	11100101	01110011	10101110

류를 제어하는데 매우 효과적이다.

4. 결 론

본 논문에서는 스트림 암호시스템의 종류와 오류전파 특성에 대해 분석하였다. 특히, 전송로상에서 발생하는 오류전파에 대한 대책으로 오류정정부호를 암호시스템에 도입이 가능하며 이를 내부오류제어와 외부오류제어로 나누어 암호문 귀환 암호시스템에 대해 적용하고 그 결과를 분석하였다. 동일한 조건으로 전송로상에서 발생한 오류제어를 위해 여러가지 방식간의 비교 연구한 결과, 키 자동키 스트림암호시스템은 내부오류제어 방식이나 외부오류제어 방식에 공히 오류전파의 영향을 받지 않는 시스템이라는 것을 알 수 있으나, 암호문의 지연, 삽입등으로 동기를 잃으면 재동시키지 않는한 모든 메세지는 쓸모없게 된다. 또한, 암호문 귀환 스트림 암호시스템은 외부 오류제어 방법이 오류정정에 다소 미흡한 점도 있으나 자동인증의 효과를 볼 수 있다. 마지막으로 평문 귀환 스트림 암호시스템은 무한한 오류전파 특성으로 인한 메세지 변형이 심하므로 내부오류제어에 의한 자연발생잡음 제거만이 유용하다.

참 고 문 헌

1. Berlekamp, E.R. : Algebraic Coding Theory, McGraw-Hill, New York, 1968.

2. Blaut, R.E. : Theory and practice of Error Cotrol Codes, Addison-Wesley, Reading, Mass., 1983.

3. Chambers, W.G. and S.M. Jennings : "Linear Equivalence of Certain BRM Shift-Register Sequences," Electr. Letters, vol. 20, pp.1018-1019, Nov. 1984.

4. Golomb, S.W. : Shift Register Sequences, Holden-Day, San Francisco, CA, 1967.

5. Maritsas, D.G. : "The Autocorrelation Function of the Two Feedback Shift Register Pseudorandom Source," IEEE Trans. Computers, vol. C-22, pp.962-964, Oct. 1973.

6. Maritsas, D., A. Arvillias, and A. Bounas : "Phase-Shift Analysis of Linear Feedback Shift Register Structures Generating Pseudorandom Sequences," IEEE Trans. Computers, vol. C-27, no. 7, July 1978.

7. Pless, V.S. : "Encryption Schemes for Computer Confidentiality," IEEE Trans. Computers, vol. 1, C-26, pp.1133-1136, Nov. 1977.

8. Reeds, J. : "Cracking a random number generator," Cryptologia, vol. 1, pp.20-26, Jan. 1977.

9. Rhee, M.Y. : Error Correcting Coding Theory, McGraw-Hill, New York, 1989.

10. _____ : BCH Codes and Reed-Solomon Codes, Minum Sha, Seoul, Korea, 1990.

11. Rueppel, R.A. : Analysis and Design of Stream Ciphers, Springer-Verlag, Berlin, Germany, 1986.

12. Rueppel, R.A. : "Linear Complexity and Random Sequences," Proc. Eurocrypt'85, pp.167-188, 1986.

□ 著者紹介

太 榮 秀(正會員)

한양대학교 공과대학 전기공학과(전자전공) 공학사
숭전대학교 대학원 전자공학과 공학석사
한양대학교 대학원 전자통신공학과 박사과정
현재 : 국립서울산업대학 전자공학과 교수
著書 : 電子応用回路 (서울산업대학 출판부)

李 晩 榮(正會員)

本誌 15P참조