무선채널에 적합한 DES의 S박스에 관한 연구

정회원 박 미 옥*, 최 연 희*, 전 문 석*

A Study on Appropriate S-box of DES in Radio Channel

Mi-Og Park*, Yeon-Hee Choi*, Moon-Seog Jun* ***Regular Members***

요 약

현대의 이동통신 발달은 사용자들에게 많은 편리성을 제공해주고 있다. 이와 반면에, 이동통신의 개방성은 심각한 보안위협이 되고있으며, 안전한 통신채널을 제공하기 위한 이동통신망의 보안은 필수적이다. 이동통신상의 보안으로 주로 사용되는 방법은 의사난수를 생성하는 스트림 암호알고리즘이다.

본 고에서는 이동통신상에서 전송되는 데이터를 보다 안전하게 보호하기 위한 연구로서 스트림 암호알고리즘에 비선형 함수인 S박스의 사용과 그에 대한 메커니즘을 제안한다. 또한, 사용된 S박스 중에서 이동통신 환경에 가장 좋은 랜덤특성을 가지는 S박스에 관한 연구도 병행한다. 실험을 통해, 이동통신 환경에 가장 적합한 DES의 S박스를 조사하고, 기존의 스트림 사이퍼와 제안한 모델의 랜덤성을 비교분석하여 제안한 모델의 효율성을 증명한다.

Key Words : stream cipher; random number; S-box.

ABSTRACT

Nowadays, the development of wireless communications provides a convenience for many people. On the other hand, the openness of wireless communications poses serious security threats and the security of wireless communications is necessary to support the secure communication channel. The common security method on wireless is the stream cipher that generates the pseudorandom number.

In this paper, we propose the usage of the nonlinear function S-box and the mechanism according to it in stream cipher as the study to securely protect data transferred on wireless communications. Besides, it goes abreast a study on S-box with the best random characteristic among the used S-boxes on wireless communications. By means of test, we investigate the most appropriate S-box of DES on wireless communications environment and prove the efficiency of the proposed model by comparing and analysis of the randomness of the based stream cipher and the proposed model.

Ⅰ. 서 론

이동통신의 발달로 인하여 우리는 언제, 어디서나 원하는 사용자와 통화를 할 수 있고 이동단말기를 이용한 다양한 서비스도 제공받을 수 있다. 하지만, 이러한 이동통신의 편리성에도 불구하고 이동통신의 방성은 날로 급증하는 무선해킹과 같은 심각한 보안문제와 함께 그에 따른 피해도 날로 급증하고 있다. 스트림 사이퍼는 이동통신상의 보안문제를 해결하기 위해 주로 사용하는 암호알고리즘으로서, 비트열로 입력되는 데이터를 비트단위로 암호화하는 방법이다. 스트림 사이퍼는 고속처리가 가능하다는 장점때문에 통신기술의 발전과 함께 유럽 등지에서 많이 사용되어 왔으며 현대에도 기밀성 보장을 위한 용도로 많이 사용되고 있다[1][2][3].

본 고는 기존의 스트림 사이퍼를 보다 안전하게 하기 위한 메커니즘으로서 블록암호에서 주로 사용하는 비선형 함수인 S박스의 적용과 그에 따른 부가적인 메커니즘을 제안한다. 또한, 사용된 S박스들 의 랜덤특성에 관한 고찰을 통하여 이동통신상에 가장 적합한 S박스를 조사한다.

* 숭실대학교 컴퓨터학과 (mopark@kingdom.ssu.ac.kr, mjun@computing.ssu.ac.kr)

논문번호 : 030278-0701, 접수일자 : 2003년 7월 1일

본 논문의 구성은 2장에서 스트림 사이퍼의 기본 개념을 살펴보고, 3장에서는 제안한 모델의 개념과 동작절차를 효과적으로 적용하기 위한 메커니즘을 설명한다. 4장에서는 실험을 통해 제안한 모델의 효율성을 증명하고, 사용된 S박스중 이동통신상에 가장 적합한 S박스의 결과를 보인다. 마지막으로, 5장에서는 결론을 내리고 본고를 마친다.

II. 관련 연구

스트림 사이퍼는 주로 1970년대 초반부터 유럽에서 연구발전되어 온 암호방식으로서 LFSR(Linear Feedback Shift Register)을 비선형으로 결합한 비선형 이진수열 발생기를 근간으로한다. 스트림 사이퍼는 이진수열 발생기에서 생성된 이진수열과 평문을 비트별로 XOR(eXclusive OR)하여 암호문을 생성한다. 스트림 사이퍼에서는 연속적인 비트 $x_1, x_2, \ldots, x_n$을 평문 메시지 X로 하고, x_i는 키수열 생성기에서 발생되는 키 비트 수열인 $Z=(z_1, z_2, \ldots, z_n, \ldots)$의 i번째 요소인 Z_i에 의해 암호화되어 i번째 비트의 암호문 y_i가 생성된다. 이러한 과정은 그림 1과 같고 수식으로는 다음과 같은 함수관계를 갖는다.

$$y_i = E_{z_i}(x_i) \quad (1)$$

이때, 암호변환 함수인 E_{z_i}는 암호기의 내부상태에 의존하는 시변환함수(time-varing function)로 시간 i일 때의 키 비트 스트림 Z_i는

$$Z_i = f(K, s_i) \quad (2)$$

와 같이 외부키 K와 시간 i일때의 내부상태 s_i에 의해 결정된다. 또한, s_i는 x_i가 y_i를 암호화한 후 일정한 규칙에 따라 s_{i+1}로 천이된다. 따라서, 동일한 평문에 대응되는 암호문이 항상 같은 블록 암호방식에 비해 스트림 암호방식은 일정한 평문·암호문쌍을 이루지 않으므로 비밀 유지면에서 효과적이다. 스트림 암호방식의 암호화과정은 보통 $y_i = x_i \oplus z_i$인 XOR 함수관계를 이용하고, 복호화 과정은 $x_i = y_i \oplus z_i$가 된다[4][5].

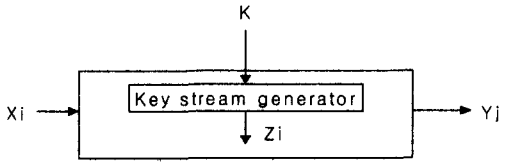

그림1. 일반적인 스트림 암호 시스템

III. 제안 모델

1. 기본 개념

본 절에서는 제안한 모델의 구조와 동작절차에 대해 설명한다. 제안한 모델에서는 기존의 스트림 사이퍼에 DES(Data Encryption Standard)의 S박스를 실제로 적용하고, 이 8개 S박스들중에서 가장 좋은 랜덤성을 가지는 S박스에 대한 실험을 통해 이동통신상에 가장 적합한 랜덤성을 가지는 DES의 S박스를 고찰한다. DES의 S박스를 적용한 이유는 이동통신 단말기의 특성상 큰 사이즈의 S박스를 사용하는 것은 계산상이나 메모리측면에서 부담이 되기 때문에 DES의 8개 S박스를 모두 사용하는 것이 아니라 실험을 통해 가장 좋은 랜덤성을 가지는 S박스 하나만을 사용함으로써 더 효율적인 메모리 사용과 연산의 효율성, 그리고 비도를 이루고자한다[6][7]. 또한, DES는 AES 알고리즘이 나오기전까지 은행업무와 같은 여러분야에서 실제적으로 가장 많이 사용되어온 알고리즘이고, DES의 S박스 구성도 어떠한 변형없이 그 자체의 구성을 그대로 유지할 때 가장 안전하다는 사실이 많은 연구문헌을 통해 검증되었기 때문이다[8][9].

제안모델의 기준모델로는 A5알고리즘을 사용한다. A5는 유럽에서 주로 사용하는 이동통신상의 암호알고리즘으로서, 이동단말기에서 기지국까지 전송되는 데이터를 암호화한다. A5는 비밀키와 공개정보인 프레임번호를 입력으로하여 3개의 LFSR(23단, 22단, 19단)에 의한 동작으로 키 수열을 생성한다.

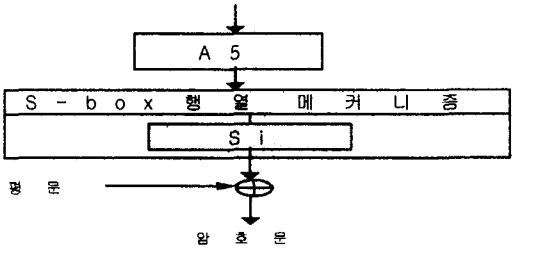

그림 2. 제안한 모델의 구조도

생성된 키 수열은 일반적인 스트림 사이퍼처럼 평문과 함께 XOR되어 전송된다[10][11].

제안모델의 동작원리는 기존모델에서 생성된 키 수열을 평문과 XOR하기 바로 전 단계에서 S박스를 통과하도록하는 것이다. 그림 2에서 S-box 행열 메커니즘은 제안모델에서 사용하는 행열방법을 의미하고, Si는 A5에서 출력된 키 수열을 입력으로 받아 8개 S박스중 가장 좋은 랜덤성을 가지는 하나의 S박스를 통과함을 의미한다. 이 과정은 기존모델의 비도를 높여주는 역할을 담당하게 된다. A5의 출력으로 생성된 키 수열은 S박스 통과단계에서 사용된 각 S박스의 비선형 함수특성을 거치기 때문에 사용된 S박스의 비선형 함수특성만큼 비도가 향상될 것이다.

제안한 모델의 동작절차는 다음과 같다.

① 비밀키와 프레임번호를 입력으로 받아 A5알고리즘을 수행한다.

② ①단계의 출력을 S박스 입력으로 사용하여 하나의 S박스를 통과한다.

③ ②단계에서 출력된 결과와 평문을 XOR한다.

2. 행·열 메커니즘

동작절차 ②단계는 S박스 통과단계로서 DES의 S박스를 사용하기 때문에 입력비트를 DES의 S박스 입력비트로 조정해야한다. DES의 S박스는 입력으로 6개비트를 사용하고, 이 6개비트중 첫번째와 여섯번째 비트로 행을 결정하고 나머지 비트로 열을 결정한다. 제안모델에서 사용하는 행·열 메커니즘은 ①단계에서 생성된 첫번째와 두번째 출력비트로 S박스의 행을 결정하고, 3~6번째 출력비트로 열을 결정하는 방법을 사용한다. 표 1에 제안모델에서 사용하는 행·열 메커니즘을 나타내었다.

표 1. S박스의 행·열 메커니즘

```
Sbox_row = gb[0]*2 + gb[1];
Sbox_col = gb[2]*8 + gb[3]*4 +gb[4]*2 + gb[5];
Sbox_out = Sbox_input[Sbox_row][Sbox_col];
```

Sbox_row는 ①단계에서 생성된 비트중 첫번째 비트인 gb[0]와 두번째 비트인 gb[1]을 사용해 계산된 결과값을 저장하는 변수로서, 행을 계산한 결과값을 나타낸다. Sbox_col은 ①단계에서 생성된 3~6번째 비트인 gb[2], gb[3], gb[4], gb[5]를 계산해 열을 결정하는 변수이다. Sbox_out은 Sbox_input인 배열을 통해 앞에서 계산된 행과 열의 값으로 S박스를 통과한 후의 출력값을 의미한다.

다음은 두 번째 행·열 메커니즘으로서 기존의 DES S박스와 같은 방법으로 행열을 결정할 경우 열에 치우친 계산의 부담을 줄이기 위해 다음 표 2와 같이 각각 3개비트로 행과 열을 결정하는 방법이다. 두 번째 행·열 메커니즘을 위한 S박스의 구성은 4X16행열인 S박스를 8X8행열로 새롭게 구성한다. 이 때, 8X8행열로 구성할 때의 규칙은 4개의 각 행의 절반이 되는 열의 위치에서 하나의 행을 두 개로 나누어 나눈 앞부분은 첫번째 행으로, 뒷부분은 두번째 행으로 구성해 기존의 4X16행열의 함수특성이 변경되지 않도록 지원한다. 예를 들어, 하나의 행이 [1,2,3,4,5,6,7,8,9,0,11,12,13,14,15,16]과 같이 구성되어 있을 때, 음영처리를 하지 않은 부분이 첫번째 행이 되고, 음영처리한 부분은 두번째 행이 되도록 해야한다.

표 2. 두 번째 행·열 메커니즘

```
Sbox_row = gb[0]*4 + gb[1]*2 + gb[2];
Sbox_col = gb[3]*4 + gb[4]*2 + gb[5];
```

두 번째 행·열 메커니즘의 실험결과 처음 3번의 테스트까지는 첫 번째 행·열 메커니즘보다 더 좋은 랜덤성을 나타내었고, 4번째부터는 첫 번째 행·열 메커니즘과 동일한 랜덤성을 나타냈다.

S박스를 통과한 후의 출력비트는 다음 식(3)과 같이 표현할 수 있다.

$$Out_{last_i} = S_i[\ Out_{pre_i}\ ] \qquad (3)$$

여기서, Out_{pre_i}는 S박스를 통과하기 전의 출력으로서 ①단계에서 생성된 출력을 의미하고, $S_i[\ ]$는 제안모델에서 사용하는 임의의 S박스를 나타내는 것으로서 ②단계에 속하는 과정이다. Out_{last_i}는 ②단계의 출력으로서 S박스를 통과한 후의 출력을 의미한다. 이러한 방법으로 모든 단계를 수행한 모델은 평문의 각 비트와 순서대로 XOR를 수행하여 전송된다.

Ⅳ. 실험결과 및 분석

본 절에서는 제안한 모델이 더 높은 랜덤성을 실제로 제공하는지에 대한 검증을 하고, 또 하나의 목적인 가장 좋은 랜덤특성을 가지는 DES의 S박스에

대한 실험을 한다. 전자의 목적을 검증하기 위해 기존의 모델과 제안한 모델에 대한 실험결과를 비교·분석하고, 후자를 검증하기 위해 8개 S박스의 각각에 대한 랜덤테스트를 실행하고 비교분석한다.

실험환경은 IBM pc에서 C언어를 사용하였고, 랜덤성 테스트툴로는 J. Walker가 만든 Ent Pseudorandom Number Sequence Test Program을 사용하였다[12].

1. 기존 모델

실험에 사용한 총 비트는 약 15360비트이고, 이 전체 비트를 64번으로 나누어 첫번째 그룹비트에 랜덤성을 실험하고, 다음은 첫번째와 두번째 그룹비트를 합쳐서 랜덤성을 실행, 그 다음은 첫번째와 두번째 그룹비트에 세번째 그룹비트를 합쳐서 실험하하는 방법을 사용하였다. 표 3은 랜덤성과 serial correlation을 실행한 결과의 일부이다. 64번의 실험결과에서 arithmetic mean은 몇 번의 57.대의 값을 제외하고는 거의 대부분 56.대의 값을 출력했고, serial correlation의 값은 10번 미만의 0.09대의 값을 출력하는 것을 제외하고는 거의 대부분 0.1대의 값을 출력하였다.

2. 각 S박스를 적용한 모델

본 절에서는 DES의 8개 S박스 중에 가장 좋은 랜덤특성을 가지는 S박스를 찾아내고 그 S박스를 제안모델에 적용하기 위해서, 각 S박스에 대한 랜덤성을 테스트한다. 테스트를 위해 각 S박스를 제안모델의 구조에 따라 스트림 사이퍼에 적용하여 시뮬레이션하였다. 8개의 S박스 비교를 위해 사용된 총 비트는 약 30500비트로서 127번으로 나누어 실험하였다. 그림 3은 각 S박스에 대한 랜덤테스트 결과이다. 실험결과를 통해 8개의 모든 S박스가 기존의 방법보다 더 좋은 랜덤특성을 가지는 것은 아니라는 사실을 알 수 있었고, 사용한 S박스 중에 가장 좋은 랜덤특성을 가지는 S박스는 S4로 나타났다.

표 3. 기존 모델의 실험결과

Arithmetic mean	Serial correlation
56.8852	0.101178
56.7131	0.020351
57.3497	0.089625
57.6107	0.109424
57.3770	0.108014
57.1503	0.118398
57.2881	0.112420

그래서, 기존모델과 S4적용모델을 비교하기 위해서 약 15360비트에 대해 다시 랜덤성을 테스트하였다.

Arithmetic mean값에서 기존모델은 대부분 56.대의 값을 출력하고, S4를 적용한 모델에서는 대부분 57.대의 값을 출력하였다. 반복횟수마다 두 개의 값을 비교해서 더 좋은 랜덤값을 생성하는 횟수에 대한 비율은 약 1:4로서 제안모델이 더 좋은 랜덤값을 생성하는 것을 알 수 있었다. Serial correlation 값은 S4적용모델이 0.01~ 0.04의 값을 출력하고 기존모델은 4.1절에서 보는바와 같이 0.09~0.1대의 값을 출력함으로써 S4적용모델의 상관확률이 개선되는 것을 알 수 있다. 결과적으로, S4박스를 적용한 모델은 기존모델뿐만 아니라 다른 S박스들과 비교할 때 가장 좋은 랜덤성을 가짐으로써 이동통신상의 암호전송에 가장 효율적인 사용이 가능함을 알 수 있다. 또한, 랜덤테스트 결과에서 알 수 있듯이 S박스를 적용하였을 경우 모든 S박스에서 기존모델보다 더 좋은 serial correlation값을 출력함으로써 상관확률이 개선되는 것을 알 수 있다.

3. S박스의 행·열 메커니즘

본 절에서는 제안모델에서 사용하는 첫번째 행·열 메커니즘과 두번째 행·열 메커니즘의 실험을 통해 각 행·열 메커니즘의 효율성을 증명하고자한다. 첫번째 행·열 메커니즘을 검증하기 위해 기존의 DES S박스 행열방법과 비교실험한다. 첫번째

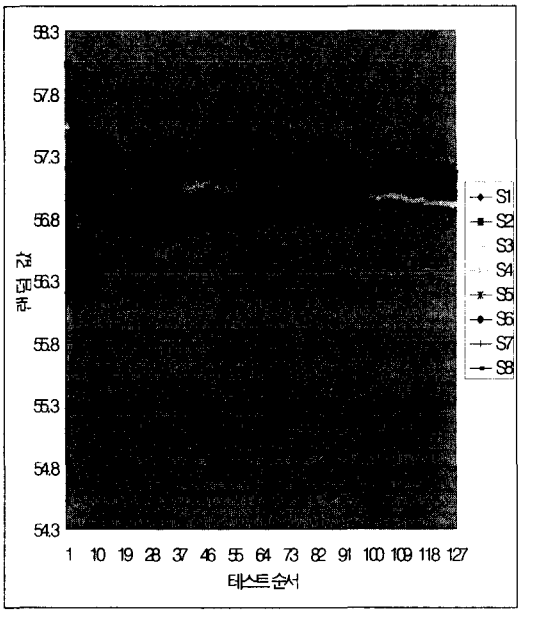

그림 3. 각 S박스에 대한 랜덤성 비교

행·열 메커니즘은 제안모델에서 사용하는 기본적인 행·열 메커니즘으로서 그림 3의 실험결과도 첫번째 행·열 메커니즘을 사용한 제안모델에 각각의 S박스를 적용한 결과를 나타낸 것으로서, 그림 3은 첫번째 행·열 메커니즘을 사용한 제안모델의 결과를 보여주는 것이다. 첫번째 행·열 메커니즘은 DES의 S박스 행열방법을 변형한 것으로서 표 4에 DES S박스 행열방법을 실험한 결과의 일부를 나타내었다. 표 4는 총 1920비트에 대해 32번의 그룹으로 나누어 첫번째 그룹부터 32번 그룹까지 테스트한 결과이다. 두 모델의 비교결과, 첫번째 행·열 메커니즘은 32번의 모든 경우에 DES의 S박스 행열방법보다 더 높은 랜덤값을 출력함으로써 첫번째 행·열 메커니즘이 DES의 S박스 행·열 메커니즘보다 더 좋은 랜덤특성을 나타냄을 알 수 있다.

두번째 행·열 메커니즘의 랜덤성테스트는 4.2절에서 가장 좋은 랜덤성을 가지는 것으로 조사된 S4박스를 사용한 첫번째 행·열 메커니즘(그림 3)과 S4박스를 사용한 두번째 행·열 메커니즘을 비교·실험한다. 여기서는 960비트를 16번 나누어 테스트하였고, 실험결과의 일부를 표 5에 나타내었다. 두번째 행·열 메커니즘을 그림 3에 나타난 S4적용모델과 비교할 때 3번째 테스트까지는 두번째 행·열 메커니즘이 더 높은 랜덤값을 출력하였고, 4번째부터는 첫번째 행·열 메커니즘과 동일한 랜덤값을 출력하여 arithmetic mean의 정의에 따라 127.5에 더 가까운 값을 출력한 두번째 행·열 메커니즘이 첫번째 행·열 메커니즘보다 더 좋은 랜덤성을 나타낸다고 말할 수 있다. 또한, 이 두개의 메커니즘은 표 3에 나타낸 기존모델의 랜덤값과 비교할 때도 더 높은 값을 출력하기 때문에 기존모델보다 더 좋은 랜덤특성을 가진다고 말할 수 있다. 결과적으로, 제안한 첫번째와 두 번째 행·열 메커니즘을 사용한 제안모델은 기존모델보다 더 좋은 랜덤성을 제공하여 제안모델의 효율성을 증명했다.

표 4. DES S박스 행·열 메커니즘

Arithmetic mean	Serial correlation
56.9180	0.143173
55.5820	0.110241
56.4590	0.076962
56.4385	0.088662
56.5148	0.088662
56.6066	0.088310
56.7447	0.084738

표 5. 두 번째 행·열 메커니즘

Arithmetic mean	Serial correlation
57.7377	-0.044541
57.5328	-0.093626
57.0874	-0.144067
56.9918	-0.083778
57.3082	-0.037564
57.5820	-0.054280
57.5059	-0.061407

4. 안전성 분석

4.1 비선형 함수

제안한 모델에서는 비선형 함수의 특성을 가지는 S박스의 사용을 제안하였다. 일반적으로 함수가 선형적이면 결과를 통해 입력을 유추하기가 비교적 쉽기때문에 이러한 선형함수의 단점을 보완하는 역할을 하기 위한 방법으로 비선형함수 성질을 갖는 S박스를 사용하여, 블록 암호알고리즘의 비도를 높인다. 이와 같은 특성은 비선형 함수인 S박스를 스트림 암호알고리즘에 적용함으로써 불안전한 기존의 스트림 알고리즘에 비선형 특성을 부여하여 출력에 의한 입력을 유추하기가 더 어렵게 되기 때문에 결과적으로 스트림 암호알고리즘의 비도를 높인다고 말할 수 있다.

S박스의 구성은 미리서 계산이 되어 있는 lookup table형태이기 때문에 사용할 때마다 계산을 해야하는 연산의 비효율성을 줄일 수 있다. 이것은 빠른 계산시간을 필요로 하는 이동통신단말기의 특성을 고려할 때 사용할 때마다 계산을 하는 것이 아니라 이미 계산이 되어있는 비선형 함수인 S박스를 통과만하면 되기 때문에 연산의 효율성을 이룰 수 있다.

일반적으로 LFSR을 결합한 형태로 이루어진 스트림 암호알고리즘은 상관공격(correlation attack)이란 강력한 공격방법에 의하여 대부분 약점이 있음이 밝혀졌다[2],[9]. 하지만, S박스는 선형공격에 강하도록 입·출력의 상관계수가 작도록 설계되기 때문에 S박스를 적용한 제안모델은 상관공격에 더 강하여 기존의 스트림 암호알고리즘보다 더 높은 비도를 제공한다고 말할 수 있다. 이에 대한 결과는 각 테스트에서 serial correlation값에 의하여 나타내었다.

4.2 랜덤성과 상관특성

스트림 암호에서의 비도수준은 암호공격에 강한 키 수열 발생기의 설계에 의해 결정되므

로 일반적으로 키 수열의 주기에 대한 최대값의 보장, Golomb의 좋은 랜덤특성, 좋은 상관면역성을 가질 것, 큰 선형복잡도를 가질 것 등의 요구사항을 만족해야 한다[13]. 본 절에서는 제안한 모델의 비도조건 중 좋은 랜덤특성과 좋은 상관면역성에 대한 조건을 실험결과를 분석함으로써 제안한 모델의 비도가 증가함을 밝혔다.

좋은 랜덤특성에 대한 조건은 표에서는 arithmetic mean값으로 그림에서는 Y축의 랜덤값으로 표시된 출력값으로 측정되었다. 각 실험결과에서, 제안모델은 기존모델보다 더 높은 arithmetic mean값을 출력하기 때문에 arithmetic mean의 정의에 따라서 더 좋은 랜덤특성을 나타내어 두번째 비도 조건에 대해 제안모델이 기존모델보다 더 높은 비도를 제공한다고 말할 수 있다.

좋은 상관면역성을 가져야한다는 조건은 serial correlation값으로 측정되었다. 표 3,4,5에 나타난 값을 비교해보면 좋은 랜덤특성을 가지는 S박스를 적용한 제안모델이 기존모델보다 0에 더 가까운 값을 출력함으로써 serial correlation의 정의에 따라 상관특성이 향상됨을 알 수 있다. 상관특성이 향상되었다는 것은 바이트들의 의존도가 그 만큼 낮아지기 때문에 입·출력과의 일정한 패턴을 찾기가 더 어렵게 되어 공격에 더 강해진다. 이 테스트는 비도 조건 중 세 번째 조건에 대해 제안모델이 기존모델보다 더 좋은 특성을 가진다는 것을 나타내는 것이다. 결과적으로, 두 개의 비도조건에서 제안한 모델이 기존모델보다 더 좋은 특성을 나타낸다는 것을 알 수 있다.

V. 결 론

본 논문에서는 이동통신채널상의 효율적인 암호통신을 제공하는 메커니즘으로서 기존의 스트림 사이퍼에 비선형 특성을 제공하는 S박스를 적용한 모델에 대한 연구를 하였다. 사용한 S박스는 DES의 S박스로서 8개 S박스중 가장 좋은 랜덤성을 가지는 S박스를 테스트하여 제안한 모델에 사용하였다. 실험결과 사용된 S박스 중에는 각 S박스 특성에 따라서 기존의 스트림 사이퍼보다 더 낮은 랜덤성을 나타내는 것도 있었다. 하지만, S박스를 적용한 모든 모델은 기존의 알고리즘보다 더 좋은 상관특성을 가지는 것으로 나타났고, 가장 좋은 랜덤성을 가지는 S박스는 S4를 적용한 제안모델이였다. 결론적으로, 사용된 8개 S박스들중에서 이동통신환경에 가장 좋은 랜덤성을 지닌 DES의 S박스는 S4이고, 기존모델보다 더 향상된 랜덤성과 더 좋은 serial correlation의 특성을 가진다는 것을 알 수 있었다.

향후 과제로는 이동통신보안에 보다 효율적으로 대응할 수 있는 스트림 사이퍼상에서의 다른 S박스에 대한 연구가 필요하리라 본다.

참 고 문 헌

[1] 진양규, 임환주, 김창규, 이만영, "다수의 원시다항식을 이용한 비선형 스트림 암호기와 오류제어에 관한 연구", *한국통신학회 추계종합학술 발표회 논문집*, pp. 219-224, 1990

[2] 지성택, 박춘식, "비밀키 암호", *TELECOMMUNIATIONS REVIEW*:10(5), pp. 877-885, 2000

[3] 박종욱, 황인호, 홍재근, "RMVD를 이용하는 동기식 스트림 암호 데이터 통신시 난수동기 이탈 검출 알고리즘", *정보보호학회 논문지*, 10(3), 2000

[4] 태영수, 이만영, "오류정정부호를 이용한 스트림 암호시스템에 관한 연구", *통신정보보호학회 논문지*, 2(1), Dec. 1991

[5] A. Ruppel, "Analysis and Design of Stream Ciphers," *Springer-Verlag*, pp. 1-16, 1986.

[6] M. Maxim, D. Pollino, "Wireless Security," *AMcGraw-Hill RSA press*, pp.15-19, 2002

[7] X. Zhu, H. M. Heys, "The Analysis of a New class Unbalanced CAST Ciphers," *CCECE'97 IEEE*, pp.326-329, 1997.

[8] 임웅택, 남길현, "DES 암호알고리즘의 안전성분석과 확장된 DES-like 암호알고리즘의 설계에 관한 연구", *통신정보보호학회 논문지*, 3(2), pp.3-15, Dec. 1993

[9] M. H. Dawon, S. E. Tavares, "An Expanded Set of Design Criteria for Substituotuin Boxes and Their in strenrhening DES-like Cryptosysems," *IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, pp. 9-10, May 1991.

[10] 김범식, 신인철, "해쉬함수와 스트림 암호기

의 개발 및 GSM 보안 시스템의 적용", *한국정보처리학회 논문지*, 7(8), 2000

[11] A. Biryukov, A. Shamir, D. Wager, "Real time Cryptanalysis of A5/1 on a PC," *Fast software Encryption Workshop 2000(FSE 2000)*, pp. 1-18, April 2001.

[12] J. Walker, "ENT A Pseudorandom Number Sequence Test Program," *http://www.fourmilab.ch/random*

[13] 홍진근, 손해성, 황찬식, 김상훈, 윤기철, "무선채널에서의 암호통신을 위한 동기식 스트림 암호시스템 구현", *한국통신학회논문지*, C(24), pp.894-904, 6.1996

박 미 옥(Mi-Og Park) 정회원

1991년 2월 : 조선대학교 전산 통계학과졸업(학사)
1993년2월 : 숭실대학교 컴퓨터학과 졸업(석사)
1996년 3월~현재 : 숭실대학교 컴퓨터학과 박사과정

<주관심분야> 이동통신보안, 암호학, 정보보호

최 연 희(Yeon-Hee Choi) 정회원

1991년 2월 : 목포대학교 전산 통계학과졸업(학사)
1993년2월 : 숭실대학교 컴퓨터학과 졸업(석사)
1996년 3월~현재 : 숭실대학교 컴퓨터학과 박사과정

<주관심분야> 이동통신보안, 암호학, 정보보호

전 문 석(Moon-Seog Jun) 정회원

1986년 :Unviersity of Maryland 전산과 졸업(석사)
1989년 : Unviersity of Maryland 전산과졸업(박사)
1989년 : Morgan State University 전산수학과 조교수
1991년 ~현재 : 숭실대학교 정보과학대학 정교수

<주관심분야> 네트워크 보안, 컴퓨터 알고리즘, 병렬 처리, VLSI설계, 암호학