이중 S박스를 이용한 스트림 암호 알고리즘

박미옥° 최연희 강정호 전문석
숭실대학교 일반대학원 컴퓨터학과
mopark°@kingdom.ssu.ac.kr

Stream Cipher using Double S-boxes

Miog Park° Yeonhee Choi Jungho Kang Moonseog Jun
Soongsil University Computer Science

요 약

본 고에서는 지속적으로 증가하는 이동통신 사용자들에게 이동통신의 편리성뿐만 아니라 안전한 통신을 제공하기 위해 기존의 스트림 암호알고리즘의 비도 향상을 위한 메커니즘을 제안한다. 본 논문에서는 이동통신상의 데이터를 보다 안전하게 암호화하기 위한 메커니즘으로서 블록암호 알고리즘에서 주로 사용하는 S 박스를 이중으로 사용하는 메커니즘과 이중으로 사용되는 S 박스를 위한 행·열 메커니즘을 제안한다. 본 고에서 사용하는 S 박스는 DES의 S 박스의 일부를 사용하며, 사용되는 S 박스는 스트림 암호 알고리즘의 모든 비트에 대해 통과되는 것이 아니라 0인 경우에만 제안하는 이중 S 박스를 통과하는 방법을 사용한다. 제안한 모델은 4장의 실험에서 기존모델과 비교·분석하여 제안한 모델의 효율성을 증명한다.

1. 서 론

스트림 암호시스템은 주로 1970년대 초반부터 유럽에서 연구발전 되어 온 암호시스템으로서 LFSR(Linear Feedback Shift Register)을 이용한 이진수열 발생기이다. 스트림 암호시스템은 최대주기를 보장하는 LFSR을 비선형으로 결합한 비선형 이진수열 발생기를 근간으로 하는 암호시스템으로 평문을 이진수열로 부호화하여 이진수열 발생기에서 발생된 이진수열과 비트별로 XOR하여 이진수열로 된 암호문을 발생한다. 스트림 암호시스템의 동작은 다음과 같다.

$$C_i = M_i \oplus K_i \qquad \text{for i=1,2,3,.... (1)}$$

여기서, C_i는 암호문의 비트열, M_i는 평문문자의 비트열, K_i는 키수열, $\oplus$는 XOR 연산자를 나타낸다.

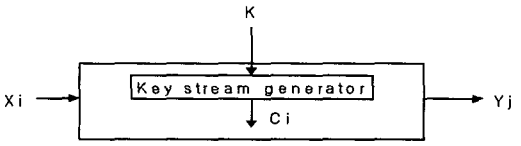

그림 1 일반적인 스트림 암호시스템

스트림 암호의 종류는 동기방식에 따라 자체 동기식 암호방식과 동기식 암호방식으로 구분된다. 자체 동기식암호는 암호문을 입력에 피드백시킴으로서 스트림 동기 이탈시 수신단에서 자체적으로 동기를 복구시킬 수 있는 반면, 한 비트의 오류가 발생하여도 레지스터 단수 크기의 비트 오류가 확산되므로 채널 오류대책이 마련된 통신망에 적용된다. 동기식 암호방식은 스트림 동기 이탈시 자체 복구가 불가능하므로 통신을 중단하고 재동기를 확립해야한다. 이 방식은 비트 삽입이나 소실과 같은 송수신간의 클럭슬립 발생시 동기가 이탈되는 문제를 보완하여야 하지만 비트오류의 확산이 없으므로 일반적으로 많이 사용된다[1][2][3].

본 논문의 구성은 2장에서 제안한 모델과 그에 대한 동작원리를 설명하고, 3장에서는 실험결과를 비교분석하여 제안한 모델의 안전성을 제시하고 증명한다. 마지막으로, 4장에서는 결론을 언급하고 본 고를 마친다.

2. 제안한 모델

본 절에서는 기존의 스트림 암호알고리즘의 비도를 향상시키기 위한 방법으로서 블록 암호방식에서 사용하는 S박스의 사용을 제안한다. 제안모델에서 사용하는 S박스는 DES(Data Encryption Standard)[4]의 8개 S박스 중 3개의 S박스를 이중으로 사용한다. 또한, 이중으로 사용되는 S박스는 비트에 따라 비트가 0이면 이중 S박스단계를 통과하고, 1이면 S박스를 통과하지 않는 메커니즘에 따라 S박스를 사용할 수도 있고, 사용하지 않을 수도 있게 함으로써 기존 알고리즘을 개선시키고자 하였다. 제안한 모델의 기존 암호알고리즘으로는 A5를 사용한다. A5는 유럽에서 주로 사용하는 이동통신상의 암호알고리즘으로서, 비밀키와 프레임 번호를 입력으로 하여 3개의 LFSR 동작에 의해 키수열을 생성한다. 3개의 LFSR은 각각 23단, 22단, 19단으로 구성되며, 생성된 키수열은 평문과 함께 XOR되어 전송된다[5][6].

제안한 모델의 동작절차는 그림 2와 같이 기존 알고리즘의 일부함수 결과값에 따라 결과값이 0이면 본 고에서 사용하는 S박스 결정 메커니즘에 의해서 이중의 S박스를 통과하고, 결과값이 1이면 S박스를 통과하지 않고 기존의 알고리즘 방식대로 처리하게 된다. 그림에 나타낸 S4, S6, S8의 의미는 DES에서 사용하는 8개의 S박스 순서를 나타낸 것으로서, S2는 2번째, S4는 4번째, S8은 8번째의 S박스라는 의미이다. 이러한 방법으로 처리된 결과값은 평문과 XOR을 수행하여 최종적인 암호문을 생성한다.

제안모델의 동작절차는 다음과 같다.

[1단계] 비밀키와 프레임번호를 입력으로 받아 A5 알고리즘을 수행하여 키수열을 생성한다.

[2단계] 1단계에서 생성된 비트가 1이면, 기존의 스트림 암호방식대로 처리한 후, 4단계로 이동한다.

[3단계] 1단계에서 생성된 비트가 0이면, 첫번째 S박스 단계를 통과한 후, 두 번째 S박스 행열 메커니즘에 의해 두번째 S박스단계를 수행한다. 그 다음 4단계로 이동한다.

[4단계] 각 2단계와 3단계에서의 결과 값을 평문과 함께 XOR을 수행한다.

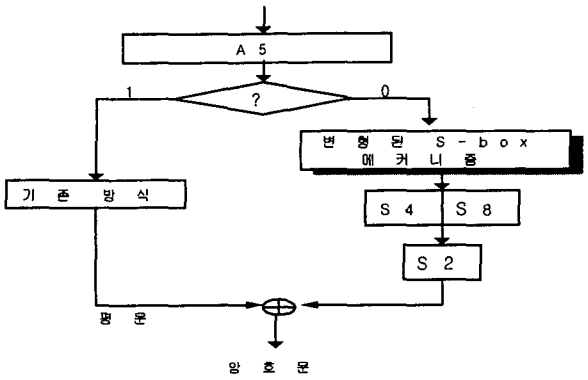

그림 2 제안 모델의 구조

제안모델의 첫 번째 S박스 통과단계는 기존의 DES에서 사용하는 행열방법에 따라 $S(b_0\ b_1\ b_2\ b_3\ b_4\ b_5)$의 여섯 개 비트중 b_0와 b_5로 행을 결정하고, 나머지 비트로 열을 결정한다. 두 번째 S박스 통과단계에서는 표 1의 방식에 따라 행열을 결정한다.

표 1 두 번째 S박스 통과단계 행·열 메커니즘

```
S2_row = gb[n1]*2 + gb[n2];
S2_col =  gb[n1]*8+gb[n2]*4+gb[n3]*2+gb[n4];
S2_out = S_box2[S2_row][S2_col];
```

표 1의 S2_row는 행을 결정하는 값을 저장하는 변수이고, S2_col은 열을 위한 값을 저장하는 변수이다. gb[]로 표시된 부분은 제안모델의 첫 번째 S박스 통과단계에서 출력된 비트들의 순서를 나타낸 것으로서, []안의 숫자는 여섯개의 비트중 몇 번째를 나타내는가를 의미한다. 예를 들어, gb[n1]은 첫번째 비트, gb[n2]는 두 번째 비트를 의미한다. 두 번째 S박스 통과단계에서 사용하는 행·열 메커니즘은 바로 전단계의 첫 번째 S박스 단계에서 출력한 4개비트를 사용해 행과 열을 결정한다.그 이유는 DES의 S박스 입력은 6개 비트이고, S박스를 통과한 후의 출력비트는 4개이기 때문에 두 번째 S박스 통과단계의 입력으로 6개비트가 생성되기를 기다리는 지연시간을 없애고 첫 번째 S박스의 출력인 4개비트를 그대로 사용하기위함이다. S_box2는 두 번째 S박스 통과단계로서, 그림 2에서 S2라고 표기된 S박스 통과단계이다. S2_out은 두 번째 S박스를 통과한 후의 출력 값을 저장하는 변수를 의미한다.

4. 실험결과 및 분석

본 절에서는 기존의 스트림 알고리즘인 A5와 제안한 모델을 비교 실험하여 그에 대한 효율성을 검증한다. 실험환경은 UltraSPAC-II 400MHz(두개)의 CPU와 2048M의 메모리, 디스크는 8G(7개)인 Sun Enterprise 3500에서 실험하였고, 사용한 언어는 C 언어이다. 각 출력수열의 랜덤성을 테스트하기 위해 Ent(Pseudorandom Number Sequence Test Program)프로그램을 사용하였다[7].

Ent 입력으로 사용한 총 비트는 약 30500 비트이며, 127번의 횟수로 나누어 실험하였다. 임의의 횟수로 나누어 그 횟수만큼 반복실험한 이유는 비교모델의 최종적인 값만 비교하는 것이 아니라 각 반복실험마다 상대적으로 얼마나 더 좋은 랜덤성을 나타내는지를 조사하기 위해서이다.

4.1 기존모델과 제안모델의 비교

그림3은 제안한 모델과 기존의 스트림 알고리즘을 이용한 모델을 실험한 결과로서, 스트림 암호알고리즘의 가장 큰 관점인 랜덤성에 대한 테스트이다.

Y축의 랜덤값은 arithmetic mean값을 의미하는 것이고, 그에 대한 정의는 파일 안의 모든 바이트를 합하여 파일 길이로 나눈 결과로서 127.5에 가까울수록 더 좋은 랜덤성을 가지는 것을 의미한다. 그림 3에서 제안모델은 1번째의 68.9344값에서 시작하여, 3번째의 가장 낮은 값인 68.1967을 출력한 후, 그 이후부터는 68.373에서 0.01씩 값이 계속 증가하여 마지막에서는 68.9431을 출력하였다. 기존모델은 4번째에서 가장 높은 값인 57.6107을 출력하였고, 나머지는 모두 이보다 작은 값으로서 57.대와 56.대의 값을 번갈아가면서 출력하였고, 비트가 증가할수록 56.76대로 값이 조금씩 감소하는 것을 볼 수 있다. 기존모델의 각 실험에 대한 평균값은 56.9256690이고 마지막 출력 값은 56.7660이다.

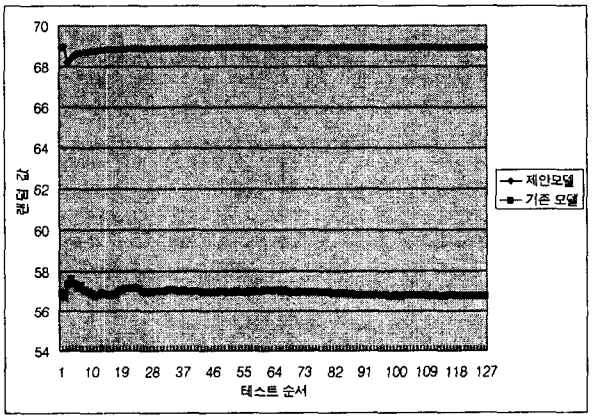

그림 3 제안모델과 기존모델의 랜덤성 비교

그래서, 두 모델에 대한 랜덤성의 비교는 제안모델이 항상 기존모델보다 더 높은 값을 출력하기 때문에 arithmetic mean의 정의에 따라 제안모델이 더 좋은 랜덤특성을 가진다고 말할 수 있다.

Serial correlation은 파일 안의 각 바이트와 이전 바이트와의 의존도를 나타내는 것으로서, 양수나 음수 값을 가질 수 있으며 0에 가까울수록 더 좋은 상관특성을 의미한다.

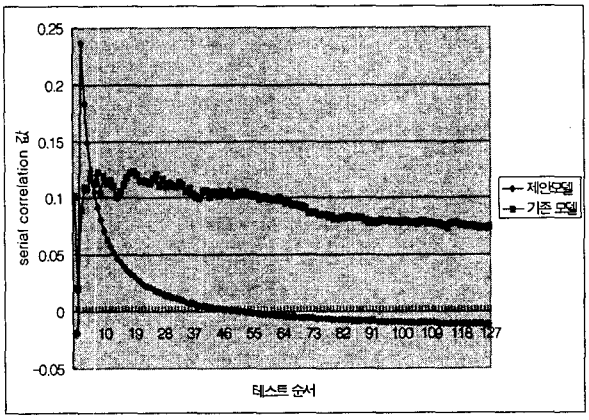

그림 4 Serial correlation 비교

그림 4에서 두 모델에 대한 선형특성의 비교는 기존모델은 대부분 0.1대의 값을 출력하면서 비트가 증가할수록 0.09, 0.08, 0.07대까지 값이 낮아지면서, 마지막은 0.074632를 출력하였다. 제안모델은 세 번째의 실험횟수에서부터 4번의 높은 값을 출력하는 것을 제외하고는 0에 훨씬 가까운 값을 출력하였고, 비트가 증가할수록 0.0001대의 값에서 0.001씩 값이 증가하면서 마지막에서는 0.010966값을 출력하였다. 127번의 횟수에서 4번(0.236685, 0.183043, 0.148477, 0.124272)을 제외한 나머지 모든 부분에서 제안모델이 기존모델보다 0에 훨씬 더 가까운 값을 출력하기 때문에 serial correlation의 정의에 따라 제안모델이 기존모델보다 더 좋은 상관특성을 가진다는 것을 의미한다.

그림 3과 그림 4의 실험을 통해서 제안모델은 기존모델보다 더 좋은 랜덤 특성과 향상된 상관 특성을 나타냄으로써 제안된 메커니즘의 효율성을 증명한다고 말할 수 있다. 또한, 더 좋은 랜덤성과 향상된 상관특성을 가진다는 것은 그 만큼 공격에 강하게 된다는 것을 의미하기 때문에 결과적으로 제안모델은 기존모델보다 공격에 더 강하여 알고리즘의 비도가 향상되었다고 할 수 있다.

5. 결론

본 고에서 제안한 모델은 기존의 스트림 암호알고리즘인 A5의 비도를 향상시켜 이동통신상에 전송되는 데이터를 보다 안전하게 보호하기 위한 메커니즘으로서 세 개의 S박스를 사용하여 이중으로 통과시키는 방법을 사용하였다. 또한, 이중의 S박스 통과단계는 비트에 따라 0인 경우에만 이중의 S박스를 통과하도록 하여 기존의 모델보다 더 좋은 랜덤성과 0에 훨씬 더 가까운 선형상관특성을 나타냄으로써 모델의 효율성을 증명하였다.

결과적으로, 본 논문은 간단한 메커니즘에 의해 이동통신상의 데이터를 보다 안전하게 보호할 수 있는 암호 알고리즘의 개발에 기여할 것으로 기대되며, 이진수열 발생기가 필요한 다른 응용 분야에도 응용되어질 수 있을 것으로 기대된다.

참 고 문 헌

[1] 박종욱, 황인호, 홍재근 ,"RMVD를 이용하는 동기식 스트림 암호 데이터 통신시 난수동기 이탈 검출 알고리즘", 정보보호학회 논문지, 제 10권 3호, p.21~29, 2000.

[2] A. Ruppel, "Analysis and Design of Stream Ciphers", p.5-16, Springer-Verlag, 1986.

[3] 이민섭, "현대 암호학", pp118-155, 교우사, 2000.

[4] William Stallings, "Network and Internetwork Security Principles and Practice", IEEE Press, p.41~69, 1995

[5] Alex Biryukov, Adi Shamir, David Wager, "Real Time Cryptanalysis of A5/1 on a PC," Fast Software Encryption Workshop 2000, Vol.40, pp.71-79, Apr. 2000.

[6] Eli Biham, Orr Dunkelman, "Cryptanalysis of the A5/1 GSM Stream Cipher", Progress in Cryptology - INDOCRYPT 2000, LNCS 1977, pp.43-51, Dec. 2000.

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