情報保護學會論文誌
第17卷 第4號, 2007. 8

스트림 암호에 대한 개선된 다중 경로 고속 상관 공격

김 현[1†], 홍 석 희[2‡], 성 재 철[3], 이 상 진[2], 박 해 룡[1], 전 길 수[1]
[1]한국정보보호진흥원, [2]고려대학교, [3]서울시립대학교

Advanced Multi-Pass Fast Correlation Attack on Stream Ciphers

Hyun Kim[1†], Seok-hie Hong[2‡], Jae-chul Sung[3], Sang-jin Lee[2],
Hae-ryong Park[1], Kil-soo Chun[1]
[1]Korea Information Security Agency(KISA),
[2]Center for Information Security Technologies(CIST), [3]University of Seoul

요 약

기지 평문 공격 시나리오에서 스트림 암호에 대한 고속 상관 공격은 매우 강력한 공격 방법이다. 대부분의 고속 상관 공격은 암호학적인 문제를 적당한 디코딩 문제의 관점에서 접근한다. 본 논문에서는 이진 대칭 채널의 출력 값으로부터 입력 값을 복구하기 위해 사용되는 패리티 검사 방정식과 Fast Walsh Transform을 이용한 Chose 등이 제안한 고속 상관 공격[1]과 Zhang 등이 제안한 다중 경로 고속 상관 공격[11]을 개선한 다중 경로 고속 상관 공격을 제안한다. 이 공격기법은 기 제안된 공격 기법들과 마찬가지로 표적 LFSR(Linear Feedback Shift Register)의 초기 상태 값 중 일부를 추측하나, Zhang 등이 제안한 기법보다 각 경로에서 한 비트씩을 더 복구 할 수 있어 보다 효율적인 공격이 가능하게 한다.

ABSTRACT

In a known plaintext scenario, fast correlation attack is very powerful attack on stream ciphers. Most of fast correlation attacks consider the cryptographic problem as the suitable decoding problem. In this paper, we introduce advanced multi-pass fast correlation attack which is based on the fast correlation attack, which uses parity check equation and Fast Walsh Transform, proposed by Chose et al. and the Multi-pass fast correlation attack proposed by Zhang et al. We guess some bits of initial states of the target LFSR with the same method as previously proposed methods, but we can get one more bits at each passes and we will recover the initial states more efficiently.

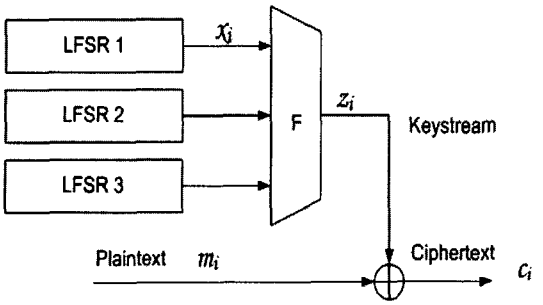
Keywords : *Stream cipher, Fast correlation attack, LFSR(Linear feedback shift register), Parity-check eqaution*

Ⅰ. 서 론

동기식 스트림 암호는 평문 수열 $m_1, m_2, \cdots$과 키 수열 생성기의 출력 수열 $z_1, z_2, \cdots$을 $m_i \oplus z_i = c_i$, $i = 1, 2, \cdots$와 같이 비트단위로 XOR하여 암호문 수열 $c_1, c_2, \cdots$을 생성한다. 이 때, 키 수열은 평문 수열과는 독립적으로, 오직 비밀 키 값과 키 수열 생성기의 초기 상태 값에 의해 생성된다.

안전한 스트림 암호는 효율적으로 난수에 가까운 키 수열을 생성하여 어떠한 공격자도 다항식 시간 안에 생

접수일: 2007년 4월 5일; 채택일: 2007년 7월 6일
* 본 연구는 정보통신부에서 지원하는 R&D 과제(2007-P10-33)와 고려대학교 특별연구비로 수행하였습니다.
† 주저자, hkim@kisa.or.kr
‡ 교신저자, hsh@cist.korea.ac.kr

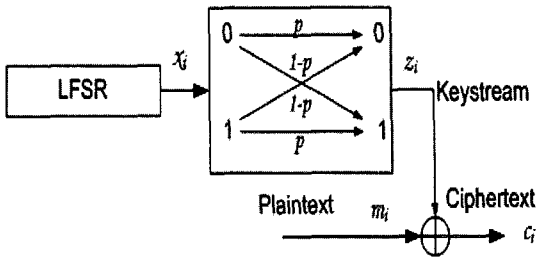


〔그림 1〕 비선형 결합 키 수열 생성기

성된 키 수열과 난수를 구별해 내지 못하게 해야 한다. 대부분의 스트림 암호는 의사난수열을 생성하기 위해 LFSR을 사용한다. LFSR에 기반한 스트림 암호는 증명 가능한 주기와 좋은 통계학적인 성질을 지니지만, LFSR의 출력 비트들이 서로 선형이기 때문에 LFSR을 단독으로 사용하지는 않는다. 예컨대 〔그림 1〕과 같은 비선형 결합 키 수열 생성기는 비선형 부울 함수를 이용하여 여러 LFSR의 출력들을 결합함으로써 키 수열을 생성한다.

스트림 암호를 분석하는 기법 중 고속 상관 공격은 가장 널리 사용되는 방법 중 하나이다. 특히 LFSR을 사용하는 스트림 암호의 경우 다른 스트림 암호보다 고속 상관 공격을 적용하기 쉽다. 1984년 Siegenthaler는 상관 면역성에 대한 논문[9]을 발표하였고, 1989년 Meier와 Staffelbach는 상관 면역성을 이용하여 스트림 암호를 분석하는 고속 상관 공격 기법을 처음으로 제안하였다[3]. 그 후 여러 암호학자들이 다양한 이론들[4][5][7][8]을 제안하였는데, 이러한 상관 공격은 특정 LFSR의 출력 비트와 키 수열 생성기의 출력 비트 간에 상관관계 확률이 클수록 공격을 성공할 확률이 커진다. 또한 상관 공격은 키 수열 생성기의 구조적인 영향을 거의 받지 않고 적용가능하다. 다만 특정 LFSR의 출력이 키수열에 직접적인 영향을 주어 상관관계를 형성해야 하고, 또한 대부분의 고속상관 공격은 특정 LFSR의 출력이 초기 상태값의 선형결합으로 이루어졌을 때 쉽게 공격을 할 수 있다. 따라서, 본 논문에서는 이러한 조건을 만족하는 비선형 결합 키수열 생성기를 사용하는 스트림암호를 공격의 대상으로 본다.

비선형 결합 키 수열 생성기에서, 각각의 LFSR의 출력은 함수 f의 입력이 되고, f의 출력은 키 수열이 된다. 생성된 키 수열이 특정 LFSR의 키 수열과 $p(=\Pr(z_i = x_i) \neq 0.5)$의 확률을 가지고 있을 때, 이를

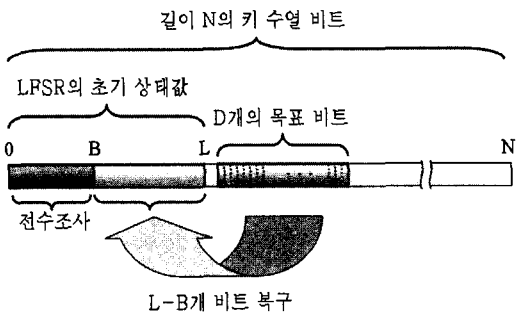


〔그림 2〕 확률 $1-p$로 잡음이 발생하는 이진 대칭 채널

이용하여 상관 공격 기법을 적용할 수 있다. 이때, 비선형 부울 함수 f의 출력을 표적 LFSR의 출력에 $1-p$의 확률로 잡음(Noise)이 섞인 것으로 생각할 수 있다. 즉, 비선형 결합 키 수열 생성기를 〔그림 2〕와 같이 잡음이 있는 이진 대칭 채널(BSC, Binary Symmetric Channel)로 대체할 수 있다. 이렇게 함으로써 출력 키 수열로부터 표적 LFSR의 출력 수열을 복구하는 암호학적인 문제를 $1-p$의 확률로 잡음이 섞이는 채널에서 정보 비트를 복원하는 디코딩의 문제로 바꾸어 접근할 수 있다.

본 논문은 2002년 Chose, Joux, Mitton이 제안한 고속 상관 공격 기법[1]과 2006년 Zhang과 Feng가 제안한 고속 상관 공격 기법[11]을 보완하여 LFSR을 이용하는 일반적인 스트림 암호에 적용 가능한 고속 상관 공격을 제안한다. 본 공격은 표적이 되는 LFSR(이후부터 표적 LFSR이라고 함)의 초기 상태 값을 몇 개의 파트로 나누어 복구하는 분할 정복 공격을 한다. 이때 각 파트를 〔11〕에서와 같이 경로(Pass)라고 한다. 본 공격 기법의 시간 복잡도는 Zhang 등이 제안한 공격 기법에서와 같이 첫 번째 경로에 의해 거의 결정되기 때문에, Zhang 등의 기법과 복잡도 관점에서는 큰 차이가 없을 수도 있다. 그러나 각 경로에서 기존 공격 기법보다 하나의 비트를 더 복구하기 때문에, 확실히 본 공격 기법이 더 나은 결과를 보인다. 또한 〔11〕에서 제시한 성공 확률을 계산하는 것보다 Matsui가 제시한 방법을 통해 좀 더 쉽게 매개변수를 결정하여 공격할 수 있다.

본 논문은 다음과 같이 구성된다. 기 제안된 공격기법의 기본 아이디어를 2장에서 제시하고, 3장에서는 제안되는 공격 기법을 설명한다. 그리고 4장에서는 이전에 제안된 두 개의 고속 상관 공격[1][11]과 본 논문에서 제안하는 공격을 비교 분석한다. 끝으로 5장에서는 본 논문의 결론을 다룬다.



〔그림 3〕 Chose 등이 제안한 공격기법

Ⅱ. 기 제안된 공격의 아이디어

본 단원에서는 본 논문에서 제안하는 공격의 기반이 되는 2002년 Chose, Joux, Mitton이 제안한 고속 상관 공격 기법[1]과 2006년 Zhang과 Feng가 제안한 고속 상관 공격 기법[11]의 아이디어를 살펴본다.

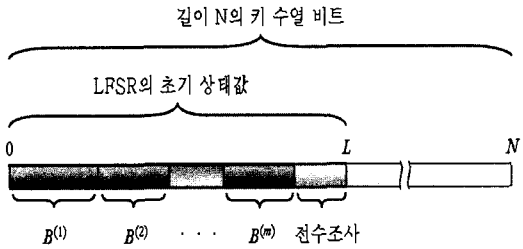
2.1. Chose 등이 제안한 공격기법[1]의 아이디어

본 공격은 길이 L인 LFSR에 대해, 초기 상태 값 중 B개 비트를 전수조사를 통해 추측하고, 남겨진 $L-B$개 비트들은 패리티 검사 방정식을 이용하여 복구한다. 〔그림 3〕은 Chose et. al의 공격기법을 그림으로 나타낸 것이다.

각각의 패리티 검사 방정식은 하나의 표적 비트를 포함하고, 같은 표적비트를 포함하는 방정식끼리 모아 하나의 표적비트에 대한 패리티 검사 방정식의 집합을 구성한다. 여기서 표적비트의 개수 D는 $L-B$보다 커야 한다. 구성된 각 패리티 검사 방정식의 집합에 대해, 초기 상태 값 B개 비트들에 대한 전수 조사를 통해 옳다고 추정되는 후보를 뽑고 연관된 표적비트의 값을 추정한다. 최종적으로 각 후보와 해당 후보가 연관된 표적비트들을 이용하여 올바른 후보를 찾은 후 간단한 선형 대수를 통해 D개의 표적 비트로부터 나머지 $L-B$개의 초기 상태 값을 복구한다.

2.2. Zhang 등이 제안한 공격기법[11]의 아이디어

본 공격은 길이 L인 LFSR의, 초기 상태 값 중 $B^{(1)}$개 비트를 패리티 검사 방정식 집합에 대해 전수 조사하여 높은 확률로 올바른 값을 추측한다. 올바로 추측된



〔그림 4〕 Zhang 등이 제안한 공격기법

$B^{(1)}$개 비트를 이용하여 $B^{(2)}$개의 비트를 같은 방식으로 추측한다. 이러한 방식을 m번 반복하여 $B^{(1)}+B^{(2)}+\cdots+B^{(m)}$개의 초기 상태 값을 추측하고, 남겨진 비트들을 전수 조사하여 최종적으로 L개의 초기 상태 값을 복구한다.

Ⅲ. 새로운 공격 기법

본 논문에서 제안하는 공격기법은 Chose 등과 Zhang 등이 제안한 공격 기법에서와 같이 공격을 전처리 단계와 처리 단계로 나눈다. 전처리 단계에서는 처리 단계에서 표적 LFSR의 초기 상태 값을 복원하기 위해 사용될 여러 개의 패리티 검사 방정식 집합들을 구성하고, 처리 단계에서는 패리티 검사 방정식 집합과 실제로 획득한 길이 N의 키 수열을 이용하여 표적 LFSR의 초기 상태 값을 복구한다.

본 단원에서는 Zhang 등이 제안한 다중 경로 고속 상관 공격을 개선한 고속 상관 공격 기법을 소개하고, 성공확률과 시간 및 메모리 복잡도를 살펴본다.

3.1. 전처리 단계

LFSR은 형 유한 상태 장치로써, t 클록 후 길이 L의 LFSR의 상태 값은 다음과 같이 GF(2)에서 벡터 행렬의 곱으로 표현된다.

$$\mathbf{x}_t = A^t\mathbf{x}_0, \quad t=0,1,2,\cdots,N-1 \tag{1}$$

여기서, $\mathbf{x}_0=[x_0,\cdots,x_{L-1}]^T$이고, $\mathbf{x}_t$는 t 클록 후 LFSR의 상태 값을 표현하는 이진 벡터이며, A^t는 GF(2)에서 상태 전이 $L\times L$ 이진 행렬 A를 t번 곱한 행렬이다.

LFSR의 특성 방정식이 $f(x)=c_0+c_1x+c_2x^2+\cdots+c_Lx^L$ 일 때, 행렬 A는

$$A=\begin{bmatrix} c_1 & c_2 & c_3 & \cdots & c_{L-1} & c_L \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}=\begin{bmatrix} A_0 \\ A_1 \\ A_2 \\ \vdots \\ A_{L-1} \end{bmatrix} \quad (2)$$

이다. 여기서, $A_i, i=0,1,2,\cdots,L-1$는 행벡터이다.

따라서 표적 LFSR의 모든 출력 비트 $x_i, i=L, L+1, \cdots, N-1$은 다음과 같이 표현된다.

$$x_i = A_0^{i-L+1}\mathbf{x_0}, \quad i=L, L+1, \cdots, N-1 \quad (3)$$

여기서, A_0^{i-L+1}는 A를 $i-L+1$번 제곱한 상태 전이 행렬 A^{i-L+1}의 첫 번째 행이다.

GF(2)에서 k개의 출력 비트들을 더하여 패리티 검사 방정식을 구성한다. 모든 패리티 검사 방정식은 한 개의 표적 출력 비트 x_i와 $k-1$개의 출력 비트 $x_{i_1}, x_{i_2}, \cdots, x_{i_{k-1}}$, 그리고 L개의 초기 출력 비트들의 합으로 다음과 같이 구성한다.

$$x_i \oplus x_{i_1} \oplus \cdots \oplus x_{i_{k-1}} = \sum_{l=0}^{L-1} \beta_l x_l \quad (4)$$

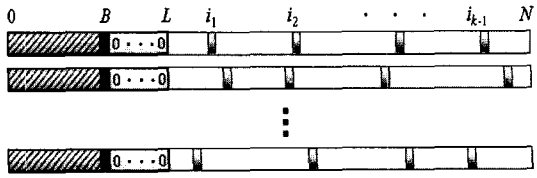
전처리 단계에서는, 각각의 표적 비트 x_i와 연관된 모든 패리티 검사 방정식들을 구하여 패리티 검사 방정식 집합 Ω_i를 구성한다. 각 방정식은 [1]에서 이용된 것과 같이 $k-1 \le 3$일 때는 전통적인 제곱근 TMTO (Time Memory Tradeoff) 알고리즘을 이용하고, $k-1>3$일 때는 [1]에서 제안한 방식을 따른다. 본 공격 기법은 $k-1 \le 3$을 고려하기 때문에, 전통적인 제곱근 TMTO를 따른다. 이때의 계산 복잡도와 메모리 복잡도는 각각 $O(N^{\lceil (k-1)/2 \rceil}\log_2 N)$와 $O(N^{\lfloor (k-1)/2 \rfloor})$이다.

첫 번째 경로에서 사용되는 패리티 검사 방정식의 표적 비트는 편의상 표적 LFSR의 초기 상태 값 중 x_{B_1}을 택하고 $\beta_l, l=B_1+1, \cdots, L-1$은 모두 0이 되도록 하여, 다음과 같은 패리티 검사 방정식들을 구성한다.

$$x_{B_1} \oplus x_{i_1} \oplus \cdots \oplus x_{i_{k-1}} = \sum_{l=0}^{B_1-1} \beta_l x_l \quad (5)$$

따라서 표적 비트 x_{B_1}에 대해 패리티 검사 방정식 집합 Ω_1은 [그림 5]와 같이 구성되고, 패리티 검사 방정식 집합 Ω_1의 크기는 $|\Omega_1| \approx \frac{1}{2^{L-B_1}}\binom{N}{k-1}$이다.

두 번째 경로에 대한 패리티 검사 방정식은 첫 번째 경로에서 알려진 값들을 이용하여 다음과 같이 구성된다.



[그림 5] x_{B_1}와 관련된 패리티 검사 방정식 집합 Ω_1

$$x_{B_2} \oplus x_{i'_1} \oplus \cdots \oplus x_{i'_{k-1}} \oplus \sum_{l=0}^{B_1} \beta_l x_l = \sum_{l=B_1+1}^{B_1+B_{2-1}} \beta_l x_l \quad (6)$$

첫 번째 경로의 패리티 검사 방정식을 구성한 방법으로 두 번째 이후의 경로에 대해서도 패리티 검사 방정식 집합 $\Omega_i, i=2, \cdots, m$을 구성한다.

3.2. 처리 단계

본 단계에서는 실제로 획득한 키 수열을 이용하여 표적 LFSR의 초기 상태 값들을 복구한다.

우선, 첫 번째 경로에서는 표적 비트 x_{B_1}에 대한 패리티 검사 방정식 집합 Ω_1에서, LFSR의 초반 B_1개 출력 비트들에 대한 올바른 후보를 찾기 위해 전수조사를 실시한다.

[그림 2]에서 $p=\Pr(z_i=x_i)=\frac{1}{2}+\epsilon, \epsilon>0$ 라고 하면, f함수의 j번째 입·출력 값은 확률 $\Pr(e_j=0)=\frac{1}{2}+\epsilon$을 가지는 랜덤한 잡음 e_j에 대해 $z_j=x_j \oplus e_j$이 되고, (5)는 다음과 같이 나타낼 수 있다.

$$x_{B_1} \oplus z_{i_1} \oplus \cdots \oplus z_{i_{k-1}} = \sum_{l=0}^{B_1-1} \beta_l x_l \oplus e_{i_1} \oplus \cdots \oplus e_{i_{k-1}} \quad (7)$$

표적 비트 x_{B_1}에 대해 $\mathrm{x}_{B_1}=(x_0, x_1, \cdots, x_{B_1-1})$의 가능한 모든 값들을 전수조사 하므로, 추측한 값 $\mathrm{x}'_{B_1}=(x'_0, x'_1, \cdots, x'_{B_1-1})$에 대해 (7)은 다음과 같이 나타낼 수 있다.

$$x_{B_1} \oplus z_{i_1} \oplus \cdots \oplus z_{i_{k-1}} \oplus \sum_{l=0}^{B_1-1} \beta_l x'_l = \sum_{l=0}^{B_1-1} \beta_l \cdot (x_l \oplus x'_l) \oplus e_{i_1} \oplus \cdots \oplus e_{i_{k-1}} \quad (8)$$

만약 x'_{B_1}을 올바르게 추측하였다면, (8)의 우변은 $e_{i_1}\oplus\cdots\oplus e_{i_{k-1}}$이 된다. 모든 랜덤 잡음이 균일하게 분포한다면, piling-up lemma[2]에 의해 다음을 얻는다.

$$q=\Pr(e_{i_1}\oplus\cdots\oplus e_{i_{k-1}}=0)=\frac{1}{2}+2^{k-2}\cdot\epsilon^{k-1} \tag{9}$$

따라서 올바르게 x'_{B_1}의 값을 추측하면 확률 q로 $z_{i_1}\oplus\cdots\oplus z_{i_{k-1}}\oplus\sum_{l=0}^{B_1-1}\beta_l x'_l=x_{B_1}$을 만족하고, 잘못 추측하면 확률 $\frac{1}{2}$로 $z_{i_1}\oplus\cdots\oplus z_{i_{k-1}}\oplus\sum_{l=0}^{B_1-1}\beta_l x'_l=x_{B_1}$을 만족한다.

추측한 x'_{B_1}과 키 수열을 이용하여 각 패리티 검사 방정식으로부터 x_{B_1}의 값이 1일 때의 개수 $T^1_{x'_{B_1}}$과 0일 때의 개수 $T^0_{x'_{B_1}}$을 구해, 두 수의 차이의 절대값 $\left|T^0_{x'_{B_1}}-T^1_{x'_{B_1}}\right|$이 0에 가깝다면 x'_{B_1}은 높은 확률로 틀린 값일 것이지만, 값이 임계치보다 크다면 x'_{B_1}은 높은 확률로 올바른 값일 것이라고 추측할 수 있다.

한편, 본 논문에서는 올바르게 추측한 값을 좀 더 효율적으로 찾기 위해 [1][11]에서와 같이 Walsh 변환을 이용한다. 우선, 패리티 검사 방정식 집합 Ω_1의 모든 방정식들을 x'_{B_1}의 패턴에 따라 새로 그룹을 지어 다음과 같이 정의된 $h(x'_{B_1})$을 계산한다.

$$h(x'_{B_1})=\sum_{x'_{B_1}}(-1)^{z_{i_1}\oplus\cdots\oplus z_{i_{k-1}}} \tag{10}$$

그러면, $\omega=(\omega_0,\omega_1,\cdots,\omega_{B_1-1})$에 대해 h의 Walsh 변환은 다음과 같다.

$$\begin{aligned}H(\omega)&=\sum_{x'_{B_1}\in GF(2)^{B_1}}h(x'_{B_1})(-1)^{\omega\cdot x'_{B_1}} \\ &=\sum_{\Omega_1}(-1)^{z_{i_1}\oplus\cdots\oplus z_{i_{k-1}}\oplus\sum_{l=0}^{B_1-1}\beta_l\omega_l} \\ &=T^0_{x'_{B_1}}-T^1_{x'_{B_1}}\end{aligned} \tag{11}$$

Walsh 변환을 계산하는데 걸리는 시간 복잡도와 메모리 복잡도는 각각 $O(2^{B_1}\cdot B_1)$와 $O(2^{B_1})$이다. h를 준비하는 데 $O(|\Omega_1|)$의 시간 복잡도가 걸리므로, Walsh 변환을 이용하여 올바른 x'_{B_1}를 추측하는 데 필요한 시간 복잡도는 $O(|\Omega_1|+2^{B_1}\cdot B_1)$이다.

한편, x'_{B_1}이 올바른 지를 판단하기 위해서는 임계치 T에 대해, $H(\omega)$가 $(|H(\omega)|+|\Omega_1|)/2\geq T$를 만족하도록 정한다. 만약 $|H(\omega)|\geq 2T-|\Omega_1|$을 만족한다면, 추측한 x'_{B_1}은 올바르게 추측된 값이라고 고려할 수 있다. 또한, 이 때 $H(\omega)$의 부호가 양수라면 표적 비트 x_{B_1}을 0이라고 추측하고 그렇지 않다면 1이라고 추측하여, 첫 번째 패리티 검사 방정식 집합으로부터 B_1+1개의 비트를 얻을 수 있다.

위와 동일한 방법으로 나머지 경로에 대해서도 같은 방식으로 해당 비트들을 복구하면, [11]에서 제안한 다중 경로 고속 상관 공격에 비해 각 경로에서 한 비트씩을 더 복구할 수 있다.

3.3. 성공확률

임계치 T에 대해, 공격의 성공확률을 높이기 위해 [11]에서는 두 개의 확률 P_1과 P_2를 다음과 같이 정의한다.

$$\begin{aligned}P_1&=\sum_{i=T}^{|\Omega_1|}\binom{|\Omega_1|}{i}(q)^i(1-q)^{|\Omega_1|-i} \\ &\rightarrow\int_T^{|\Omega_1|+0.5}\frac{1}{\sqrt{2\pi\sigma}}e^{-\frac{(x-\mu)^2}{2\sigma^2}}dx\end{aligned} \tag{12}$$

$$\begin{aligned}P_2&=\sum_{i=T}^{|\Omega_1|}\binom{|\Omega_1|}{i}\left(\frac{1}{2}\right)^{|\Omega_1|} \\ &\rightarrow\int_T^{|\Omega_1|+0.5}\frac{1}{\sqrt{2\pi\sigma'}}e^{-\frac{(x-\mu')^2}{2\sigma'^2}}dx\end{aligned} \tag{13}$$

여기서 P_1은 올바르게 추측한 x'_{B_1}이 테스트를 통과할 확률이고, P_2는 잘못 추측한 x'_{B_1}이 테스트를 통과할 확률이다. 또한, (12)에서는 $\mu=|\Omega_1|\cdot q$와 $\sigma=\sqrt{|\Omega_1|\cdot q(1-q)}$를 이용하고, (13)에서는 $\mu'=|\Omega_1|\cdot\frac{1}{2}$과 $\sigma'=\frac{1}{2}\sqrt{|\Omega_1|}$을 이용한다. 공격의 성공확률을 높이기 위해 주어진 T에 대해, 두 확률 P_1과 P_2는 각각 $P_1>0.99$와 $P_2<2^{-B}$를 만족해야 한다.

한편, 성공확률을 결정짓는 것은 패리티 검사 방정식의 개수 $|\Omega_i|$, $i=2,\cdots,m$이다. 충분한 패리티 검사 방정식을 얻었을 때, 비로소 높은 확률로 표적 LFSR의 상태 값들을 복구할 수 있다. 충분한 패리티 검사 방정식의 크기를 정하기 위해 Zhang등은 P_1과 P_2를 이용했다. 그러나 각각의 패리티 검사 방정식은 알려진 값과 알려지지 않은 값들의 선형식으로 이루어져 있어, 블록 암호에 대한 LC공격[2]에 사용되는 선형 근사식과 유

〔표 1〕 $L=40$, $p=0.469$일 때, 알고리즘 효율성 비교

알고리즘	키 수열 길이	메모리 복잡도	시간 복잡도	
			전처리 단계	처리 단계
[1]	$2^{16.29}$	$O(2^{25})$	$O(2^{37})$	$O(2^{31})$
[11]	2^{22}	$O(2^{23})$	$O(2^{26.52})$	$O(2^{25.01})$
[11]*	2^{22}	$O(2^{22})$	$O(2^{26.52})$	$O(2^{24.16})$
본 논문	2^{22}	$\boldsymbol{O(2^{22})}$	$\boldsymbol{O(2^{26.52})}$	$\boldsymbol{O(2^{24.14})}$

〔표 2〕 $L=40$, $p=0.490$일 때, 알고리즘 효율성 비교

알고리즘	키 수열 길이	메모리 복잡도	시간 복잡도	
			전처리 단계	처리 단계
[1]	$2^{16.29}$	$O(2^{35})$	$O(2^{37})$	$O(2^{40})$
[11]	2^{24}	$O(2^{29.585})$	$O(2^{28.64})$	$O(2^{29.74})$
본 논문	2^{24}	$\boldsymbol{O(2^{27.52})}$	$\boldsymbol{O(2^{28.64})}$	$\boldsymbol{O(2^{29.74})}$

사한 형태로 구성된다. 즉, 찾고자 하는 x'_{B_1}과 x_{B_1}의 값이 선형 근사식의 키 값에 대응된다. 따라서 필요한 패리티 검사 방정식의 개수도 [2]에서 제시한 algorithm 2의 성공확률을 따라 $16|q-1/2|^{-2}$개 정도의 패리티 검사 방정식 들이면 99.9%의 확률로 성공할 수 있다. 예컨대 〔11〕에서 제시한 방정식들의 수는 $32|q-1/2|^{-2}$개와 $16|q-1/2|^{-2}$개로 정도의 식들을 공격에 이용하였다.

Ⅳ. 공격의 효율성 비교

본 논문에서 제안하는 알고리즘의 실제 성능을 검증하기 위해 펜티엄 4 프로세서에서 C언어로 구현한 코드로 실험을 수행하였고, 99%이상의 성공확률을 가지는 것을 확인하였다. 본 단원에서는 새로 제안된 스트림 암호에 대한 간단한 고속 상관 공격과 기존에 제안된 가장 좋은 결과를 갖는 두 논문〔1〕〔11〕을 비교 분석한다. 여기서 사용되는 매개변수들은 정확한 비교를 위해 〔1〕과 〔11〕에서 제시한 것들을 사용한다.

표적 LFSR의 길이가 $L=40$이고, $p=0.469$일 때, 세 알고리즘의 효율성을 비교한 결과는 〔표 1〕과 같다. 여기서 이용된 매개 변수들은 $N_1=2^{22}$, $N_2=2^{15}$, $B_1=19$, $B_2=13$, $k=3$이다. 한편, 〔11〕에서는 첫 번째 경로에서 $32|q-1/2|^{-2}$개의 패리티 검사 방정식들을 이용한다. 그

〔표 3〕 $L=89$, $p=0.469$일 때, 알고리즘 효율성 비교

알고리즘	키 수열 길이	메모리 복잡도	시간 복잡도	
			전처리 단계	처리 단계
[1]	2^{28}	$O(2^{25})$	$O(2^{61})$	$O(2^{44})$
[11]	2^{32}	$O(2^{31})$	$O(2^{37.08})$	$O(2^{32.35})$
[11]**	2^{32}	$O(2^{31})$	$O(2^{37.07})$	$O(2^{31.83})$
본 논문	2^{32}	$\boldsymbol{O(2^{31})}$	$\boldsymbol{O(2^{37.07})}$	$\boldsymbol{O(2^{31.70})}$

러나 $16|q-1/2|^{-2}$개의 패리티 검사 방정식들을 이용해도 99.9%에 가까운 성공확률을 가질 수 있으므로 이를 바탕으로 〔11〕*의 결과를 얻을 수 있다. 이 경우 〔11〕*와 본 논문에서 제안하는 공격의 결과가 큰 차이가 없음을 알 수 있는데, 이는 공격의 시간 복잡도를 크게 좌우하는 첫 번째 경로가 같은 매개변수를 이용해서 구해지기 때문이다.

〔표 2〕는 $L=40$이고, $p=0.490$일 때, 효율성을 비교한 결과이다. 이용된 매개 변수들은 $N_1=2^{24}$, $N_2=2^{18}$, $B_1=19$, $B_2=10$, $k=3$이다.

〔표 3〕은 $L=89$이고, $p=0.469$일 때, 효율성을 비교한 결과로 이론적으로 계산된 결과들을 비교 하였다. 이용된 매개 변수들은 $N_1=2^{32}$, $N_2=2^{31}$, $N_3=2^{20}$, $B_1=26$, $B_2=23$, $B_3=21$이다, 그리고 첫 번째 경로에서 $k=4$이고, 두 번째와 세 번째 경로에서는 $k=3$이다. 위에서와 마찬가지로 〔11〕**는 앞에서 설명한 것과 마찬가지로 〔11〕에서 제시한 매개변수를 개선한 결과이다. 이 경우 〔11〕**에 비해 본 논문의 결과가 약 9%정도의 성능 향상을 가져오고 있음을 알 수 있다.

본 논문에서 제안하는 공격 기법은 Zhang 등이 제안한 논문과 복잡도 측면에서는 큰 차이가 없어 보인다. 이는 비록 첫 번째 경로에서 한 비트가 더 복구된다고 하더라도, 전체 복잡도를 결정짓는 첫 번째 경로가 Zhang 등이 제안한 공격 기법과 동일하기 때문이다. 그러나 〔표 3〕의 결과에서 볼 수 있듯이 LFSR의 길이가 길어져 경로가 더 많아진다면 공격 복잡도에 더 큰 영향을 미칠 수도 있음을 알 수 있다.

Ⅴ. 결 론

본 논문에서는 패리티 검사 방정식 집합을 구성하여 분할 정복 공격 방식으로 여러 경로를 통해 표적 LFSR

의 초기 상태 값들을 복구한다. 제안되는 공격기법은 표적 LFSR의 출력과 스트림암호의 출력 사이에 일정한 상관관계가 존재하고, LFSR의 출력이 초기 상태값의 선형 결합을 이루도록 설계된 일반적인 스트림암호에만 적용이 된다. 때문에 비선형 필터 생성기나 시각제어 생성기 혹은 LFSR에 비해 비선형성이 강한 FCSR이나 NLFSR 등에 대해서는 직접적인 적용이 힘들 것으로 보인다.

제안된 공격기법은 기 제안된 이론들에 비해 복잡도의 측면에서는 크게 개선된 점이 없어 보이지만, 각 경로에서 한 비트를 추가로 더 복구함으로써 경로가 많이 만들어지는 경우에는 충분히 성능이 개선됨을 알 수 있다.

참고문헌

[1] P. Chose, A. Joux, M. Mitton, "Fast correlation attacks: an algorithmic point of view", *Advances in Cryptology - EUROCRYPT'02*, Lecture Notes in Computer Science, Vol. 2332, Springer-Verlag, pp. 209-221, 2002.

[2] Matsui, M., "Linear cryptanalysis method for DES cipher", *Advances in Cryptology - EUROCRYPT'93*, Lecture Notes in Computer Science, Vol. 765, Springer-Verlag, pp. 386-397, 1994.

[3] Meier, W., Staffelbach, O., "Fast correlation attacks on stream ciphers", *Advances in Cryptology - EUROCRYPT'88*, Lecture Notes in Computer Science, Vol. 330, Springer-Verlag, pp. 301 - 314, 1988.

[4] Meier, W., Staffelbach, O., "Fast correlation attacks on certain stream ciphers", *Journal of Cryptology*, Vol. 1, No. 3 pp. 159 - 176, 1989.

[5] Meier, W., Staffelbach, O., "Correlation properties of combiners with memory in stream ciphers", *Journal of Cryptology*, Vol. 5, No. 1, pp. 67 - 86, 1992.

[6] Menezes, A., Oorschot, P. C. V., Vanstone, S. A., "Handbook of Applied Cryptography", *CRCPress*, 1997.

[7] Mihaljevic, M. J., Fossorier, M. P. C., Imai, H., "A low-complexity and high- performance algorithm for the fast correlation attack". *The 7th Fast Software Encryption Workshop(FSE 2000)*, Lecture Notes in Computer Science, Vol. 1978, Springer-Verlag, pp. 196 - 212, 2000.

[8] Mihaljevic, M. J., Fossorier, M. P. C., Imai, H., "Fast correlation attack algorithm with list decoding and an application", *The 8th Fast Software Encryption Workshop(FSE 2001)*, Lecture Notes in Computer Science, Vol. 2355, Springer-Verlag, pp. 208 - 222, 2001.

[9] Siegenthaler, T., "Correlation-immunity of nonlinear combining functions for cryptographic applications", *IEEE Transactions on Information Theory*, Vol. IT-30, pp. 776 - 780, 1984.

[10] Siegenthaler, T., "Decrypting a class of stream ciphers using ciphertext- only", *IEEE Transactions on Computers*, Vol. C-34, pp. 81 - 85, 1985.

[11] Zhang, B., Feng, D., "Multi-Pass Fast Correlation Attack on Stream Ciphers", *Selected Areas in Cryptography(SAC 2006)*.

〈著者紹介〉

김 현 (Hyun Kim) 정회원
2005년 2월 : 고려대학교 수학과 학사
2005년 3월~현재 : 고려대학교 정보경영대학원 석사(수료)
2006년 4월~현재 : 한국정보보호진흥원 연구원
<관심분야> 암호 알고리즘 분석, 개인정보보호

홍 석 희 (Seokhie Hong) 종신회원
1995년 2월 : 고려대학교 수학과 학사
1997년 2월 : 고려대학교 수학과 석사
2001년 2월 : 고려대학교 수학과 박사
1999년 8월~2004년 2월 : (주) 시큐리티 테크놀로지스 선임연구원
2003년 2월~2004년 2월 : 고려대학교 시간강사
2004년 4월~2005년 5월 : K.U.Leuven 박사후연구원
2005년 3월~현 재 : 고려대학교 정보경영대학원 조교수
<관심분야> 암호 알고리즘 설계 및 분석, 컴퓨터 포렌식

성 재 철 (Jaechul Sung) 종신회원
1997년 8월 : 고려대학교 수학과 학사
1999년 8월 : 고려대학교 수학과 석사
2002년 8월 : 고려대학교 수학과 박사
2002년 8월~2004년 1월 : 한국정보보호진흥원 선임연구원
2004년 2월~현 재 : 서울시립대학교 수학과 조교수
<관심분야> 암호 알고리즘 설계 및 분석

이 상 진 (Sangjin Lee) 종신회원
1987년 8월 : 고려대학교 수학과 학사
1989년 8월 : 고려대학교 수학과 석사
1994년 2월 : 고려대학교 수학과 박사
1989년 2월~1999년 2월 : 한국전자통신연구원 선임연구원
1999년 2월~2001년 8월 : 고려대학교 자연과학대학 조교수
2001년 9월~현 재 : 고려대학교 정보경영대학원 부교수
<관심분야> 대칭키 암호의 분석 및 설계, 정보은닉이론, 컴퓨터 포렌식

박 해 룡 (Haeryong Park) 종신회원
1999년 2월 : 전남대학교 수학과 학사
2001년 2월 : 서울대학교 수학과 석사
2006년 8월 : 전남대학교 정보보호협동과정 박사
2000년 12월~ 현재 : 한국정보보호진흥원 선임연구원
<관심분야> 전자서명 알고리즘/암호프로토콜 설계 및 분석

전 길 수 (Kilsoo Chun) 종신회원
1991년 2월 : 서강대학교 수학과 이학사
1993년 2월 : 서강대학교 대학원 수학과 이학석사
1998년 2월 : 서강대학교 대학원 수학과 이학박사
1998년 10월~1999년 9월 : 서강대학교 기초과학연구소 박사후 연구원
2001년 3월~2001년 6월 : 서강대학교 컴퓨터학과 연구교수
2001년 7월~현재 : 한국정보보호진흥원 암호응용팀장
<관심분야> 암호학, PET, Digital ID Management