情報保護學會論文誌
第16卷 第2號, 2006. 4

Shrinking 생성기와 Self-Shrinking 생성기에 대한 향상된 고속 상관 공격*

정기태,[1†] 성재철,[2] 홍석희,[1‡] 이상진,[1] 김재헌,[3] 박상우[3]
[1]고려대학교, [2]서울시립대, [3]국가보안기술연구소

Improved Fast Correlation Attack on the Shrinking and Self-Shrinking generators*

Kitae Jeong,[1†] Jaechul Sung,[2] Seokhie Hong,[1‡]
Sangjin Lee,[1] Jaeheon Kim,[3] Sangwoo Park[3]
[1]Korea University, [2]University of Seoul, [3]National Security Research Institute

요 약

본 논문에서는 shrinking 생성기와 self-shrinking 생성기에 대한 향상된 고속 상관 공격을 제안한다. 본 논문에서 제안하는 공격은 Zhang 등이 CT-RSA 2005에서 제안한 shrinking 생성기에 대한 고속 상관 공격을 개선한 것으로 shrinking 생성기에서 길이가 61인 생성 LFSR의 초기 상태값을 $2^{15.43}$ 키스트림 비트와 $2^{56.3314}$의 계산 복잡도로 성공 확률 99.9%로 복구할 수 있다. 또한 245.89 키스트림 비트와 $2^{112.424의}$ 계산 복잡도로 self-shrinking 생성기에서 길이가 2^{40}인 LFSR의 초기 상태값을 성공 확률 99.9%로 복구할 수 있다.

ABSTRACT

In this paper, we propose a fast correlation attack on the shrinking and self-shrinking generator. This attack is an improved algorithm of the fast correlation attack by Zhang et al. at CT-RSA 2005. For the shrinking generator, we recover the initial state of generating LFSR whose length is 61 with $2^{15.43}$ keystream bits, the computational complexity of $2^{56.3314}$ and success probability 99.9%. We also recover the initial state of generating LFSR whose length is 240 of the self-shrinking generator with $2^{45.89}$ keystream bits, the computational complexity of $2^{112.424}$ and success probability 99.9%.

Keywords : *Colock-controlled generator, Shrinking generator, Self-Shrinking generator, Fast correlation attack, Stream cipher*

Ⅰ. 서 론

일반적으로 스트림 암호는 블록 암호에 비해 경량 및 고속 동작이 용이하여 무선이나 스트리밍 서비스 등과 같은 환경에서 많이 사용되고 있다. 하지만, 블록 암호의 안전성 분석 기법에 비해 스트림 암호의 분석 기법으로는 최근에 개발되고 있는 다양한 스트림 암호 알고리즘들의 안전성을 체계적이고 논리적으로 분석하지 못하고 있다.

LFSR 기반 스트림 암호는 증명 가능한 주기성 및 좋은 통계적 특성을 가지고 있지만, 자체적으로

접수일: 2005년 10월 20일; 채택일: 2006년 2월 22일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 육성지원 사업의 연구결과로 수행되었음
† 주저자, kite@cist.korea.ac.kr
‡ 교신저자, hsh@cist.korea.ac.kr

는 선형이기 때문에 독립적으로 사용할 수는 없다. 따라서 LFSR 기반 스트림 암호를 결합 방식에 따라 분류하면, 비선형 결합 방식, 비선형 여과 함수를 이용한 방식, 시각 제어 방식 등으로 분류할 수 있다[5]. 이러한 LFSR 기반의 스트림 암호는 주로 유럽을 중심으로 70년대부터 설계 및 분석법이 중점적으로 연구되었다. 이러한 스트림 암호의 분석 방법으로 가장 대표적인 분석법이 상관 공격(Correlation Attack)[9] 과 고속 상관 공격(Fast Correlation Attack)[8]이며 최근에도 이 공격법들에 대한 연구가 꾸준히 진행되고 있다.

불규칙 시각 제어 생성기(Clock-controlled generator)는 그림 1과 같이 두 개의 레지스터 A, S로 구성된 생성기이다. 첫 번째 레지스터인 제어 레지스터(the control register) S는 규칙적으로 클럭된다. 두 번째 레지스터인 생성 레지스터(the generating register) A는 제어 레지스터 S의 상태값을 입력 값으로 하는 함수 F에 의해 클럭 수가 결정된다. 생성 레지스터에 의해 생성된 출력 비트는 키스트림 비트로 출력된다. 생성된 키스트림 수열은 긴 주기, 높은 선형 복잡도, 좋은 통계 특성 등 암호학적으로 좋은 성질을 지니고 있다. 불규칙 시각 제어 생성기에는 Stop and Go 생성기[4], Binary Rate Multi-plier[3], Cascade 생성기[5], Shrinking 생성기[6], Self- Shrinking 생성기[7], Alternating Step 생성기[5] 등이 있다.

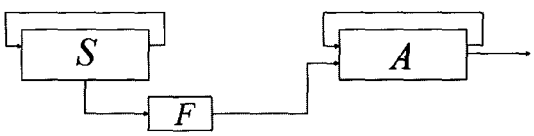

그림 1. 불규칙 시각 제어 생성기

스트림 암호의 가장 대표적인 분석 기법은 상관 공격(Correlation Attack) 기법이다. 이 분석 기법은 1985년 Siegenthaler에 의해 그 공격의 개념이 소개되었고[9], 1989년 Meier와 Staffelbach에 의해 공격 알고리즘이 제시되었다[8]. 이후, 이 공격의 개념을 이용하여 다수의 LFSR 기반 스트림 암호뿐 아니라, Summation generator 등이 분석되었다. 또한, 일반적인 스트림 암호의 안전성 분석에 활용될 수 있도록 상관 공격 알고리즘의 효율성 및 공격 복잡도를 개선시킨 다양한 연구 결과가 발표되었다. 최근에는 LFSR 기반 스트림 암호 뿐 아니라 일반적인 스트림 암호의 안전성 분석에 기본적인 분석 방법으로 활용되고 있다.

본 논문에서는 shrinking 생성기와 self-shrinking 생성기에 대한 향상된 고속 상관 공격을 제안한다. 본 논문에서 제안하는 고속 상관 공격은 2005년 Zhang 등[1]이 제안한 shrinking 생성기에 대한 고속 상관 공격을 개선한 것으로 구간 $I_{r/2}$ 내에 0 또는 1의 개수를 계산하여 그 비율이 $\frac{1}{2}+\varepsilon'$ 이상인 구간만을 이용한다. 이 구간들로부터 추정한 수열 $\hat{a}$를 구성한 후 2002년 Chose 등[2]이 제안한 방법을 이용하여 생성 LFSR의 상태 초기값을 복구한다. shrinking 생성기에서 길이가 61인 생성 LFSR의 초기 상태값을 $2^{15.43}$ 키스트림 비트와 $2^{56.3314}$의 계산 복잡도로 성공 확률 99.9%로 복구할 수 있다. 또한 $2^{45.89}$ 키스트림 비트와 $2^{112.424}$의 계산 복잡도로 self-shrinking 생성기에서 길이가 240인 LFSR의 초기 상태값을 성공 확률 99.9%로 복구할 수 있다.

본 논문의 구성은 다음과 같다. 2절에서는 shrinking 생성기에 대한 고속 상관 공격을 제안하고 3절에서는 self-shrinking 생성기에 대한 고속 상관 공격을 제안한다. 마지막 4절에서 결론을 맺는다.

II. Shrinking 생성기에 대한 고속 상관 공격

그림 2의 shrinking 생성기는 1993년 Copper 등[6]에 의해 제안된 키스트림 생성기이다. shrinking 생성기는 두 개의 LFSR, LFSR A와 LFSR S로 구성되어 있다. 두 개의 LFSR 모두 규칙적으로 클럭되고 생성 LFSR A의 출력 비트는 제어 LFSR S의 출력 비트가 1인 경우에만 키스트림 비트로 출력된다. 이 생성기는 생성기에 의해 생성된 키스트림 비트의 정확한 위치가 고정되어 있지 않다는 장점을 지니고 있다. 또한 생성된 키스트림 수열은 긴 주기, 높은 선형 복잡도, 좋은 통계 특성 등 암호학적으로 좋은 성질을 지니고 있다.

1. 기본 개념

본 절에서는 다음과 같은 표기를 사용한다.

SG : shrinking 생성기
$a=(a_0, a_1, \cdots)$: LFSR A의 출력 수열

$s=(s_0, s_1, \cdots)$: LFSR S의 출력 수열
$z=(z_0, z_1, \cdots)$: 키스트림 수열
$\hat{a}=(\hat{a_0}, \hat{a_1}, \cdots)$: 키스트림 수열을 이용하여 추

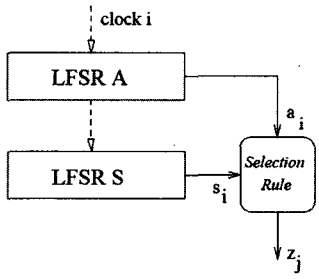

그림 2. shrinking 생성기

정한 LFSR A의 출력 수열

$1-p=P(\hat{a_i}=a_i)=\frac{1}{2}+\varepsilon$: 상관관계 $(\varepsilon>0)$

본 절에서 제시하는 shrinking 생성기에 대한 고속 상관 공격은 추정된 수열 $\hat{a}$을 Chose 등이 제안한 방법을 이용한다. $\hat{a}$을 추정하는 과정은 다음과 같다. 먼저, LFSR A와 LFSR S에 의해 생성된 수열은 난수성을 가짐을 가정한다. SG에서 z_k가 a_r과 같을 확률은 (1)과 같다 $(k\le r)$. 즉, $s_i=1$인 경우를 성공 사건이라 할 때, z_k가 a_r과 같을 사건은 수열 s의 k번째 성공 사건이 수열 a의 r번째 시도에 발생할 사건이다.

$$P(z_k=a_r)=\binom{r}{k}\left(\frac{1}{2}\right)^{r+1}. \quad (1)$$

한편, a_r이 키스트림 수열 z에 있을 경우를 (2)와 같은 경우로 고려한다.

$$a_r=z_{c_r},\ c_r=\sum_{i=0}^{r-1}s_i. \quad (2)$$

r이 증가할 때, 합 $\sum_{i=0}^{r-1}s_i$의 분포는 (3)과 같은 정규분포를 따른다.

$$\frac{\sum_{i=0}^{r-1}s_i-\frac{r}{2}}{\sqrt{\frac{r}{4}}}\sim N(0,1). \quad (3)$$

$I_{r/2}$를 (4)와 같이 정의한다. 여기서 임의의 확률 p에 대하여, α는 a_r이 키스트림 수열 z에 있을 때 (5)를 만족하는 값이다.

$$I_{r/2}=\left[\frac{r}{2}-\alpha\sqrt{\frac{r}{4}},\ \frac{r}{2}+\alpha\sqrt{\frac{r}{4}}\right]. \quad (4)$$

$$P\left(\sum_{i=0}^{r-1}s_i\in I_{r/2}\right)=p. \quad (5)$$

S_0와 S_1을 (6), (7)과 같이 각각 정의한다.

$$S_0=z_i|\ i\in I_{r/2},\ z_i=0. \quad (6)$$

$$S_1=z_i|\ i\in I_{r/2},\ z_i=1. \quad (7)$$

구간 $I_{r/2}$에 대하여 $\hat{a}_r$을 추정할 때 다음 방법을 사용한다.

$\frac{|S_0|}{|S_0|+|S_1|}\ge\frac{1}{2}+\varepsilon'$ 이면 $\hat{a}_r=0$으로 추정

$\frac{|S_1|}{|S_0|+|S_1|}\ge\frac{1}{2}+\varepsilon'$ 이면 $\hat{a}_r=1$로 추정

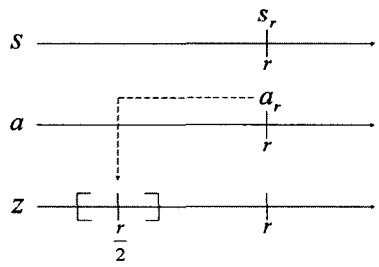

그림 3. 확률적으로 a_r이 존재하는 구간

추정된 $\hat{a}$을 이용한 고속 상관 공격[2]은 다음과 같다. 이 공격은 두 단계로 구성된다. 즉, 해밍 웨이트가 k인 패리티 검사 방정식들을 구성하는 전처리 단계와 초기 상태 값 $(x_0, x_1, \cdots, x_{L-1})$에서 처음 B 비트 $(x_0, x_1, \cdots, x_{B-1})$를 제외한 D 비트 $(D>L-B)$에 대하여 다수 투표(Majority Poll)가 적용되는 처리 단계로 구성된다.

세 가지 새로운 개념이 [2]에 제시되었다. 첫째, x_i가 주어졌을 때 (8)과 같은 형태의 패리티 검사 방정식을 구성하기 위해 비교 정렬 알고리즘 (Ma-

tch-and-sort algorithm)이 사용된다. 여기서 m_j $(1 \le j \le k-1)$는 키스트림 비트의 인덱스를 의미하고 우변의 합은 초기 상태 값의 처음 B 비트에 대한 부분적인 전수조사를 의미한다.

$$x_i = x_{m_1} \oplus \cdots \oplus x_{m_{k-1}} \oplus \sum_{j=0}^{B-1} c_j x_j. \quad (8)$$

(8)은 디코딩 과정에 필요한 패리티 검사 방정식을 제공한다. 둘째, 초기 상태 값의 $B-B_1$ 비트에 대하여 같은 패턴을 포함하는 패리티 검사 방정식들을 재 정렬한 뒤, 주어진 키스트림 비트 z_i에 대하여 처리 단계에서 패리티 검사 방정식을 계산하기 위해 Walsh 변환이 적용된다. 즉, $\omega=[x_{B_1}, x_{B_1+1}, \cdots x_{B-1}]$ 일 때 $F_i(\omega)=\sum(-1)^{t_i^1 \oplus t_i^2}$ 은 0으로 예측된 개수와 1로 예측된 개수의 차이를 의미한다. 여기서 t_i^1는 다음과 같다.

$$t_i^1 = z_{m_1} \oplus \cdots \oplus z_{m_{k-1}} \oplus \sum_{j=0}^{B_1-1} c_j x_j \quad , \quad t_i^2 = \sum_{j=B_1}^{B-1} c_j x_j.$$

그러면 각 D 비트에 대하여, $F_i(\omega) > \theta$ 이면 $x_i = 0$이고 $F_i(\omega) \leftarrow \theta$ 이면 $x_i = 1$ 이다. 여기서 θ는 임계값을 의미한다. 셋째, 고려한 D 비트 중에서 적어도 $L-B$ 비트를 정확하게 복구하기 위해 $L-B+\delta$ 비트 중에서 크기가 $L-B$인 모든 부분집합에 대해 전수조사를 필요로 하는 확인 과정이 사용된다. 처리 과정의 전체 복잡도는 (9)와 같다. 여기서 p_{err}은 잘못된 추측이 적어도 $L-B+\delta$ 비트에서 나타날 확률을 의미하고 Ω는 각 비트에 대하여 해밍 웨이트가 k인 패리티 검사 방정식의 수의 기대값을 의미한다.

$$O\left(2^B \cdot D \cdot \log_2 \Omega + \left(1 + p_{err}(2^B - 1)\right) \cdot \binom{L-B+\delta}{\delta} \frac{1}{\varepsilon^2}\right) \quad (9)$$

공격 과정은 다음과 같다. 여기서 $\varepsilon' = 0.02, 0.03$ 0.04이다.

입력 : LFSR A의 연결 다항식 $f(x)$, N 비트 키스트림 수열 $(z_0, \cdots, z_{N-1})$, 구간 $I_{t/2}$의 길이 $t = \lfloor 1 + \alpha\sqrt{r} \rfloor$, $\alpha = 1.376395$

키스트림 수열 $(z_0, \cdots, z_{N-1})$에서 구간 $I_{t/2}$ 내에 0 또는 1이 차지하는 비율을 계산하고 이 값이 고정된 값 $\frac{1}{2}+\varepsilon'$ 이상인 경우 $\hat{a}_r$을 0 또는 1로 선택한다. 이 방법으로 수열 $\hat{a}=(\hat{a_0}, \cdots, \hat{a_N})$을 구성한다.

모든 $(a_0, \cdots, a_{B-1})$ 과 비트 인덱스 i $(=B+1, B+2, \cdots, D)$ 에 대하여 Walsh 변환을 사용하여 패리티 검사 방정식을 계산한다. 위에서 언급한 확인 과정을 사용하여 LFSR A의 초기 상태값을 복구하기 위해 다수 투표 과정을 통과한 비트들을 선택한다.

LFSR A의 초기 상태값을 복구한 후, LFSR S의 초기 상태값도 복구하여야 한다. 그러나 LFSR A와 키스트림 수열 z를 알고 있기 때문에 LFSR S의 초기 상태값을 복구하는 문제는 LFSR A의 초기 상태값을 복구하는 문제에 비하여 매우 단순하다. 따라서 본 논문에서는 이 문제를 고려하지 않는다.

2. 상관관계 확률

Zhang 등이 제안한 고속 상관 공격[1]에서는 구간 $I_{t/2}$에 속하는 정수의 개수가 홀수이어야 하므로, 구성할 수 있는 구간의 개수 $n \approx N - \alpha \cdot \frac{\sqrt{N}}{2}$ 이다. 그러나 본 논문에서는 구간 $I_{t/2}$에 속하는 정수의 개수를 고려하지 않으므로 구성할 수 있는 구간의 개수 $n \approx 2 \cdot N - \alpha \cdot \sqrt{N}$ 이다.

LFSR A와 LFSR S에 의해서 생성된 수열은 난수성을 가지는 것으로 가정할 때, 구성한 수열 $\hat{a}_r$이 수열 a와 같을 확률은 (10)과 같다.

$$\begin{aligned}
P(a_r = \hat{a}_r) &= P(\hat{a}_r = 1) P(a_r = 1 \mid \hat{a}_r = 1) \\
&\quad + P(\hat{a}_r = 0) P(a_r = 0 \mid \hat{a}_r = 0) \\
&= P(\hat{a}_r = 1) P(a_r = 1 \mid \hat{a}_r = 1) \\
&\quad + (1 - P(\hat{a}_r = 1)) P(a_r = 1 \mid \hat{a}_r = 1) \\
&= P(a_r = 1 \mid \hat{a}_r = 1) \\
&= P\left(s_r = 1, \sum_{i=0}^{r-1} s_i \in I_{t/2}, z_{s_r} = 1\right) \\
&\quad + P(s_r = 0, a_r = 1) \\
&\quad + P\left(s_r = 1, \sum_{i=0}^{r-1} s_i \notin I_{t/2}, a_r = 1\right) \\
&= P(s_r = 1) P\left(\sum_{i=0}^{r-1} s_i \in I_{t/2}\right) P(z_{s_r} = 1) \\
&\quad + P(s_r = 0) P(a_r = 1) \\
&\quad + P(s_r = 1) P\left(\sum_{i=0}^{r-1} s_i \notin I_{t/2}\right) P(a_r = 1)
\end{aligned} \quad (10)$$

$$=\frac{1}{2}\cdot p\cdot\left(\frac{1}{2}+\delta\right)+\frac{1}{2}\cdot(1-p)\cdot\frac{1}{2}+\frac{1}{2}\cdot\frac{1}{2}$$
$$=\frac{1}{2}+\frac{p\delta}{2}.$$

여기서 δ는 구간 $I_{r/2}$에서 1의 비율의 기대값을 의미하고 본 공격에서 이 비율이 $\frac{1}{2}+\varepsilon'$ 보다 같거나 큰 구간을 이용하므로 다음과 같이 계산된다. 여기서 $|1|$과 i는 구간 $I_{r/2}$ 내 1의 개수를 의미한다.

$$\delta=\frac{1}{t}\left(\sum_{i=\lceil\left(\frac{1}{2}+\varepsilon\right)\cdot t\rceil}^{t} i\cdot P\left(i\,||1|\geq\left\lceil\left(\frac{1}{2}+\varepsilon'\right)\cdot t\right\rceil\right)\right)-\frac{1}{2}.$$

추정된 수열 $\hat{a}$의 길이 $N'=\beta\cdot n$ 이고 β는 (11)과 같이 계산된다.

$$\beta=\frac{1}{2^{t-1}}\left(\sum_{i=\lceil\left(\frac{1}{2}+\varepsilon\right)\cdot t\rceil}^{t}\binom{t}{i}\right) \tag{11}$$

3. 공격 복잡도

본 논문에서 제안하는 고속 상관 공격을 Zhang 등이 제안한 고속 상관 공격과 공격 복잡도를 비교하기 위해 같은 환경에서 구현한다. 즉, LFSR A의 길이는 61이고 LFSR S의 길이는 약 61이다. 매개변수는 다음과 같이 선택한다. $D=36$, $\delta=3$, $B=46$, $k=5$. $\alpha=1.376395$이고 이 값은 a_r이 키스트림 수열 z에 있을 확률인 $p=83.13\%$에 대응되는 값이다. 성공 확률을 약 99.9%로 하였을 때, 고정된 편차 $\varepsilon'=0.02$, 0.03, 0.04에 대한 상관관계 확률, 필요한 키스트림의 길이, 계산 복잡도는 표 1과 같다.

표 1. shrinking 생성기에 대한 Zhang 등의 고속 상관 공격과 본 논문에서 제안하는 고속 상관 공격의 비교

		상관관계 확률	데이터 복잡도	계산 복잡도
Zhang et al.		0.509824	$2^{17.1}$	$2^{56.7786}$
Our attack	$\varepsilon'=0.02$	0.516399	$2^{14.89}$	$2^{56.4815}$
	$\varepsilon'=0.03$	0.519654	$2^{15.09}$	$2^{56.4036}$
	$\varepsilon'=0.04$	0.523043	$2^{15.43}$	$2^{56.3314}$

Ⅲ. Self-Shrinking 생성기에 대한 고속 상관 공격

self-shrinking 생성기[7]는 shrinking 생성기의 변형된 버전으로 Meier와 Staffelbach에 의해 제안되었다.

self-shrinking 생성기는 그림 3과 같이 길이가 L인 한 개의 LFSR A만 필요로 한다. LFSR A에 의해 생성된 출력 수열을 $a=(a_0, a_1, \cdots)$ 라 할 때, 짝수 인덱스의 비트 $a_0, a_2, \cdots$가 shrinking 생성기의 LFSR S의 출력 수열 역할을 하고 홀수 인덱스의 비트 $a_1, a_3, \cdots$가 shrinking 생성기의 LFSR A의 출력 수열 역할을 한다. 즉, $a_{2i}=1$인 경우에만 a_{2i+1}을 키스트림 비트로 출력한다. 길이가 $|A|$인 LFSR A와 길이가 $|S|$인 LFSR S로 구성된 shrinking 생성기는 길이가 $L=2(|A|+|S|)$ 인 self-shrinking 생성기와 동일한 안전성을 가진다[7].

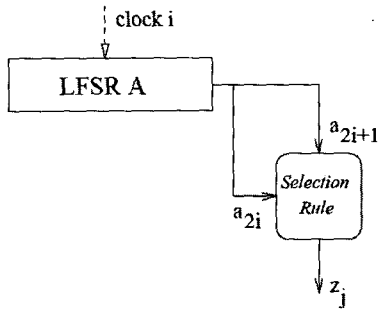

그림 3. Self-shrinking 생성기

$\hat{a}$을 추정하는 과정은 shrinking 생성기에 대한 고속 상관 공격과 매우 유사하다. 단지 키스트림 수열 z로부터 홀수 인덱스로 구성된 수열 $\hat{a}$을 구성한다. 구간 I_r에 대해서는 (12)와 같이 정의한다. 여기서 $\alpha=1.376395$이다.

$$I_r=\left[r-\alpha\sqrt{\frac{r}{2}}, r+\alpha\sqrt{\frac{r}{2}}\right] \tag{12}$$

a_{2r}이 구간 I_r에 있을 확률은 (13)과 같다.

$$P\left(\sum_{i=0}^{r-1}a_{2i}\in I_r\right)=\frac{1}{\sqrt{2\pi}}\int_{-\alpha}^{\alpha}e^{-x^2/2}=p_{2r} \tag{13}$$

상관관계 확률 $P(a_{2r\pm1}=\widehat{a_{2r\pm1}})$ 은 (14)와 같다.

$$
\begin{aligned}
&P(a_{2r+1}=\widehat{a_{2r+1}})=P(\widehat{a_{2r+1}}=1)P(a_{2r+1}=1|\widehat{a_{2r+1}}=1)\\
&+P(\widehat{a_{2r+1}}=0)P(a_{2r+1}=0 \mid \widehat{a_{2r+1}}=0)\\
&=P(\widehat{a_{2r+1}}=1)P(a_{2r+1}=1 \mid \widehat{a_{2r+1}}=1)\\
&+(1-P(\widehat{a_{2r+1}}=1))P(a_{2r+1}=1 \mid \widehat{a_{2r+1}}=1)\\
&=P(a_{2r+1}=1 \mid \widehat{a_{2r+1}}=1)\\
&=P\left(a_{2r}=1,\ \sum_{i=0}^{r-1}a_{2i}\in I_r,\ z_{a_{2r}}=1\right)\\
&+P(a_{2r}=0,\ a_{2r+1}=1)\\
&+P\left(a_{2r}=1,\ \sum_{i=0}^{r-1}a_{2i}\notin I_r,\ a_{2r+1}=1\right)\\
&=P(a_{2r}=1)P\left(\sum_{i=0}^{r-1}a_{2i}\in I_r\right)P(z_{a_{2r}}=1)\\
&+P(a_{2r}=0)P(a_{2r+1}=1)\\
&+P(a_{2r}=1)P\left(\sum_{i=0}^{r-1}a_{2i}\notin I_r\right)P(a_{2r+1}=1)\\
&=\frac{1}{2}\cdot p_{2r}\cdot\left(\frac{1}{2}+\delta\right)+\frac{1}{2}\cdot(1-p_{2r})\cdot\frac{1}{2}+\frac{1}{2}\cdot\frac{1}{2}\\
&=\frac{1}{2}+\frac{p_{2r}\delta}{2}. \qquad (14)
\end{aligned}
$$

추정된 수열 $\hat{a}$의 길이 $N'=\beta\cdot n$ 이고 β는 (15)와 같이 계산된다.

$$\beta=\frac{1}{2^{t-1}}\left(\sum_{i=\left\lceil\left(\frac{1}{2}+\varepsilon\right)\cdot t\right\rceil}^{t}\binom{t}{i}\right) \qquad (15)$$

표 2는 성공 확률을 약 99.9%로 하였을 때 Zhang 등이 제시한 고속 상관 공격을 Self-shrinking 생성기에 적용한 결과와 고정된 편차 $\varepsilon'=0.02,\ 0.03,\ 0.04$에 대한 고속 상관 공격을 비교한 것이다. 여기서 LFSR A의 길이는 240이고 매개변수는 다음과 같이 선택한다. $D=150,\ \delta=3,\ B=100,\ k=5$

표 2. Self-shrinking 생성기에 대한 Zhang 등의 고속 상관 공격과 본 논문에서 제안하는 고속 상관 공격의 비교

		상관관계 확률	데이터 복잡도	계산 복잡도
Zhang et al.		0.509824	$2^{46.77}$	$2^{112.768}$
Our attack	$\varepsilon'=0.02$	0.516399	$2^{45.36}$	$2^{112.571}$
	$\varepsilon'=0.03$	0.519654	$2^{45.56}$	$2^{112.495}$
	$\varepsilon'=0.04$	0.523043	$2^{45.89}$	$2^{112.424}$

Ⅳ. 결 론

본 논문은 불규칙 시각 제어 생성기인 shrinking 생성기와 self-shrinking 생성기에 대한 고속 상관 공격을 제안하였다. 본 논문에서 제안한 고속 상관 공격은 Zhang 등이 제안한 shrinking 생성기에 대한 고속 상관 공격의 변형된 것으로 구간 $I_{r/2}$ 내에 0 또는 1의 개수를 계산하여 그 비율이 $\frac{1}{2}+\varepsilon'$ 이상인 구간만을 이용한다. 이 구간들로부터 생성 LFSR의 수열 a를 추정한 수열 $\hat{a}$를 구성한 후 Chose 등이 제안한 방법을 이용하여 공격한다. 본 논문에서 제안한 고속 상관 공격을 이용하여 shrinking 생성기에서 길이가 61인 생성 LFSR의 초기 상태값을 $2^{15.43}$ 키스트림 비트를 이용하여 성공 확률 99.9 %와 $2^{56.3314}$의 복잡도로 복원하였다. 또한 $2^{45.89}$인 키스트림 비트를 이용하여 성공 확률 99.9 %와 $2^{112.424}$의 복잡도로 길이가 240인 LFSR의 초기 상태값을 복원하였다. 두 개의 생성기에 대한 공격 결과 모두 이전 공격보다 필요한 메모리 양와 계산 복잡도에서 더 효율적인 것으로 나타났다.

참 고 문 헌

[1] B. Zhang, H. Wu, D. Feng, F. Bao, "A Fast Correlation Attack on the Shrinking Generator", *CT-RSA 2005*, LNCS 3376, Springer-Verlag, pp. 72-86, 2005.

[2] P. Chose, A. Joux, M. Mitton, "Fast Correlation Attacks : An Algorithmic Point of View", *Advances in Cryptology-EUROCRYPT '02*, LNCS 2332, Springer-Verlag, pp. 209-221, 2002.

[3] W. G. Chambers, S. M. Jennings, "Linear equivalence of certain BRM shift register sequences", *Electronic Letters*, vol. 20, pp. 1018-1019, 1984.

[4] T. Beth and F. Piper, "The Stop and Go Generator", *in Advances in Cryptology : Proceedings of Eurocrypt '84*, LNCS 209, Springer-Verlag, pp. 88-92, 1985.

[5] A. Menezes, P. C. V. Oorschot, S. A. Vanstone, *Handbook of Applied Crytography*, Boca raton : CRC Press, 1997.
[6] D. Coppersmith, H. Krawczyk, Y. Mansour, "The Shrinking Generator", *Advances in Cryptologty - Crypto '93*, LNCS 773, Springer-Verlag, pp. 22-39, 1994.
[7] W. Meier, O. Staffelbach, "The Self-Shrinking generator", *Advances in Cryptology - EUROCRYPT '94*, LNCS 950, Springer-Verlag, pp. 205-214, 1995.
[8] W. Meier, O. Staffelbach, "Fast correlation attacks on certain stream ciphers", *Journal of Cryptology*, Vol. 1, No. 3, pp. 159-176, 1989.
[9] T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext-only", *IEEE Transactions on Computers*, Vol. C-34, pp. 81-85, 1985.

〈著者紹介〉

정 기 태 (Kitae Jeong)
2004년 2월: 고려대학교 수학과 학사
2006년 2월: 고려대학교 정보보호대학원 석사
2006년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 블록 암호, 스트림 암호 및 해쉬 함수의 분석 및 설계

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~현재: 서울시립대학교 수학과 조교수
〈관심분야〉 암호 알고리즘 설계 및 분석

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 2월: K.U.Leuven 박사후연구원
2005년 3월~현 재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 암호 알고리즘 설계 및 분석, 컴퓨터 포렌식

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

김 재 헌 (Jaeheon Kim) 정회원
1991년 2월: 한국과학기술원 수학과 학사
1993년 2월: 서울대 수학과 석사
2000년 8월: 서울대 수학과 박사
2000년 4월~현재: 국가보안기술연구소 선임연구원
〈관심분야〉 정보보호, 대수학

박 상 우 (Sangwoo Park) 정회원
1989년 2월: 고려대 수학교육과 학사
1991년 8월: 고려대 수학과 석사
2003년 2월: 고려대 수학과 박사
1991년 8월~1999년 12월: 한국전자통신연구원 선임연구원
2000년 1월~현재: 국가보안기술연구소 선임연구원
〈관심분야〉 암호이론, 정보보호