通信情報保護學會誌
第5卷 第2號, 1995. 6

다단계 p-cycle Cascade 생성기의 분석

이 상 진*, 박 상 준*, 고 승 철*

요 약

Gollmann이 제안한 Cascade 생성기는 비선형성, 발생되는 수열의 난수특성, 주기성등 암호 알고리즘으로서 필요한 제반 특성을 보장하기 때문에 그동안 스트림 암호의 핵심 논리로 널리 사용되어 왔다. 그러나 최근 생성기 내부의 각 단계별로 시각 제어 수열과 출력 수열 사이에 암호 알고리즘으로는 부적당한 상관관계 특성이 존재함이 입증되었다. 본 고에서는 이러한 상관관계 특성을 이용하여, 단순 순환 쉬프트 레지스터로 구성된 Cascade 생성기에 대한 기지 평문 공격 방식을 제안한다. 기존의 Lock-in effect 공격방식에 대하여 10^{21} 정도의 안전성을 보장하는 8단계 11-cycle Cascade 생성기에 본 방식을 적용한 결과 불과 88,000 출력 비트만을 사용하여 공격이 성공함을 실험적으로 입증하였다.

1. 서 론

스트림 암호에 대한 분석 방법은 선형복잡도(Linear Complexity)[11]와 상관관계 공격 방식[8]이 대표적이며, 그외 알고리즘의 특성에 따라 개별적으로 분석되고 있다[9]. 이런 이유로 스트림 암호의 안전성은 선형복잡도로 측정되고 있으며 입력 비트와 출력 비트 사이에 상관관계 특성이 존재하지 않도록 설계되고 있다. 시각 제어 논리는 이러한 설계 조건을 만족하는 암호 논리로 현재 스트림 암호 시스템의 세부 논리로 널리 사용되고 있다. 시각 제어 논리는 Stop-and-go generator[1]와 Cascade 생성기[4]가 대표적이지만 이들 논리의 통계적 특성이 문제점으로 지적되어 있고[5, 7], 이런 문제점을 개선하기 위하여 BRM(Binary Rated Multiplexer)[3], Step$_{(k,m)}$ Cascade generator[6] 등이 제안되어 있으나, 이들 논리를 실제 H/W로 구현할 경우에 시각 지연이 발생하는 단점이 역시 존재한다. 또한, 시각 지연이 발생하지 않으면서 동시에 통계적 특성이 우수한 Alternating step generator[7]가 발표되어 있으나, De Bruijn 수열을 이용하여 시각을 제어하기 때문에 H/W 구현에 약간의 어려움이 있다. Gollmann이 제안한 Cascade 생성기는 비선형성, 발생되는 수열의 난수특성, 주기성 등 암호 알고리즘으로서 필요한 제반 특성을 보장하기 때문에 그동안 스트림 암호의 핵심 논리로 널리 사용되어 왔다. 그러나 최근 생성기 내부의 각 단계별로 시각 제어 수열과 출력 수열 사이에 암호 알고리즘으로는 부적당한 상관관계 특성이 존재함이 입증되었다[10, 13].

본 고에서는 이러한 상관관계 특성을 이용하여,

* 한국전자통신연구소

단순 순환 쉬프트 레지스터로 구성된 Cascade 생성기에 대한 기지 평문 공격 방식을 제안한다. 기존의 Lock-in effect 공격방식에 대하여 10^{21} 정도의 안전성을 보장하는 8단계 11-cycle Cascade 생성기에 본 방식을 적용한 결과 불과 88,000 출력 비트만을 사용하여 공격이 성공함을 실험적으로 입증하였다.

제2절에서는 Cascade 생성기와 Lock-in effect를 이용한 공격 방식을 소개하며, 제3절에서는 상관관계 특성을 이용한 기지 평문 공격 방식을 제안한다. 그리고, 4절에서는 컴퓨터 실험 결과를 기술한다.

2. Cascade 생성기 소개

Cascade 생성기는 길이 p인 k개의 순환 쉬프트 레지스터를 연결하여 구성하고, 특별히 k와 p를 표시하고자 할 때는 k-단계 p-length Cascade 생성기라 말한다. 그림 1에서 i번째 쉬프트 레지스터로 구성된 부분을 i번째 단계라 하자. Cascade 생성기는 각 단계의 출력이 다음 단계 쉬프트 레지스터의 시각을 제어하는 방식으로 동작한다. 각 단계의 출력(c_t)는 전 단의 출력(a_t)와 쉬프트 레지스터 최종 단의 값을 XOR한 값이며, a_t = 1이면 쉬프트 레지스터를 1회 쉬프트하고 a_t = 0이면 쉬프트 레지스터를 동작시키지 않는다. 그리고 맨처음 단계에서는 전 단계의 출력이 항상 1인 것으로 간주한다. 최종 단계의 출력을 Cascade 생성기의 출력 수열로 한다. 이 때 전 단계의 출력 수열(a_t)를 그 단계의 시각 제어 수열이라 하자.

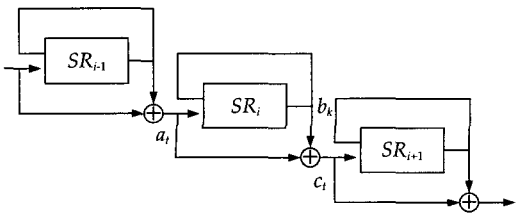


그림 1 Cascade 생성기 동작도

동작 방식이 시각 제어 수열과 쉬프트 레지스터의 최종 단을 XOR한 후 쉬프트 레지스터의 동작 여부를 결정하는 경우를 AS(Add-then-Step) Cascade 생성기라 하고 반대로 시각 제어 수열에 의해서 쉬프트 레지스터를 동작시킨 후에 쉬프트 레지스터의 최종 단과 XOR하는 경우를 SA(Step-then-Add) Cascade 생성기라 한다. 그리고 사용한 쉬프트 레지스터가 길이 p인 순환 쉬프트 레지스터인 경우에는 p-cycle Cascade 생성기라 하고 길이 l인 m-LFSR를 사용한 경우를 l-length m-LFSR Cascade 생성기라 한다. Cascade 생성기의 주기와 선형복잡도는 다음과 같다.

- k-단계 p-cycle Cascade 생성기[4]
  - 길이 p 〉 2가 소수이면 주기는 p^k.
  - p가 2-prime이고, $p^2 \nmid (2^{p-1} - 1)$이면 선형복잡도는 p^k 또는 $p^k - 1$.
- k-단계 l-length m-LFSR Cascade 생성기[5]
  - $T = 2^l - 1$일때 주기는 T^k.
  - 선형복잡도는 $1 + l(1 + T + \cdots + T^{k-1})$.

Cascade 생성기에 대한 분석은 Lock-in effect를 이용한 방법[2]과 시각 제어 수열과 출력 수열 사이의 상관관계 특성을 이용하는 방법이 있다. Lock-in effect로 k-단계 p-length Cascade 생성기를 분석하면 각 쉬프트 레지스터별 초기치의 값은 알고 위상만 모른다고 가정할 경우 kp^2의 출력 수열이 있으면 k^2p^2의 계산량으로 각 쉬프트 레지스터의 초기치에 대응되는 위상을 알 수 있다. 그런데 위상을 모르는 초기치의 개수가 $\frac{2^p - 2}{p}$이므로 Lock-in effect로 분석하는데 소요되는 계산량은 $k^2p^2(\frac{2^p - 2}{p})^k$이다. 그리고 k-단계 l-length m-LFSR Cascade 생성기는 k-단계 $2^l - 1$-cycle Cascade 생성기로 볼 수 있고 m-LFSR의 특성으로 초기치는 알 수 있다. 따라

서 Lock-in effect로 공격한다면 $k^2(2^l - 1)^2$의 계산량으로 해독될 수 있다.

3. Cascade 생성기 분석 방법

Cascade 생성기는 시각 제어 수열과 출력 수열 사이에 높은 상관관계 특성이 존재한다. 이에 대한 수학적 이론은 [10, 13]에 상세히 기술되어 있다. 특별히 최종 출력 수열이 연속해서 같은 값을 가지는 경우 1단계 쉬프트 레지스터 출력 수열이 1이 될 확률이 매우 크다. 표 1은 최종 출력 수열이 run을 발생하였을 때 run의 시작 시각에서 1단계 쉬프트 레지스터 출력 수열이 1이 될 확률이다.

표 1 Cascade 생성기의 상관관계 특성

	단 계						
run	5	6	7	8	9	10	11
5	0.662834	0.594787	0.552406	0.527978	0.514591	0.507493	0.503809
6	0.725845	0.646497	0.585263	0.548187	0.526250	0.513924	0.507247
7	0.786995	0.698443	0.627225	0.576758	0.544149	0.524471	0.513186
8	0.841053	0.754451	0.675578	0.613320	0.569185	0.540368	0.522711
9	0.885499	0.807033	0.726640	0.656148	0.601304	0.562443	0.536872
10	0.920004	0.853193	0.776742	0.702609	0.639428	0.590834	0.556431

Cascade 생성기의 상관관계 특성은 다음과 같이 정의한 전이 행렬을 반복하여 곱하면 알 수 있다.

■ 정의 1 임의의 n비트 이진 수열 $x = x_0x_1 \cdots x_{n-1}$는 다음과 같은 함수 f에 의해서 0에서 $2^n - 1$ 사이의 정수로 볼 수 있다.

$$f(x) = \sum_{k=0}^{n-1} x_k 2^k$$

n비트 시각 제어 수열은 쉬프트 레지스터의 step을 제어하여 n비트 출력 수열을 생성하므로 시각 제어 수열의 특정 형태가 출력 수열의 특정 형태를 생성할 확률을 다음과 같이 정의하자.

■ 정의 1 n비트 시각 제어 수열을 $a = a_0a_1 \cdots a_{n-1}$이라 하고 이 시각 제어 수열로부터 생성된 n비트 출력 수열을 $c = c_0c_1 \cdots c_{n-1}$이라 하면, $2^n \times 2^n$ 행렬 $T_n = (t_n[i, j])$의 각 entry 값을 다음과 같이 정의하자.

$$t_n[i, j] = P(f(c) = j | f(a) = i)$$

이 행렬을 전이 행렬이라 한다.

Cascade 생성기는 최종 출력 수열과 1단계 출력 수열은 시각이 동일하다. 그리고 1단계 출력 수열의 특정 형태가 최종 출력 수열의 특정 형태를 생성시킬 확률은 전이 행렬로부터 알 수 있다. 그러므로, Bayes' Theorem을 사용하면 최종 출력 수열의 특정 형태가 1단계 출력 수열의 특정 형태로부터 생성되었을 확률을 알 수 있다. 이러한 사실은 출력 수열만 알면 1단계 출력 수열의 값이 0 또는 1이 될 확률을 알 수 있음을 의미한다.

❖ 정리 1 1단계 출력 수열 n비트를 $a = a_0a_1 \cdots a_{n-1}$이라 하고 이에 대응되는 최종 출력 수열을 $c = c_0c_1 \cdots c_{n-1}$이라 하자. 그리고 전이 행렬 T_n를 $(k - 2)$번 곱한 행렬을 $T_n^{k-2} = (s_n[i, j])$라 하면, 즉,

$$P(f(c) = j | f(a) = i) = s_n[i, j]$$

그러면 $f(c) = j$인 경우 1단계 출력 수열의 각 비트별 확률은 다음과 같다.

$$P(a_0 = 0|f(c) = j) = \sum_{k\wedge 1=0} s_n[k, j]$$
$$P(a_1 = 0|f(c) = j) = \sum_{k\wedge 2=0} s_n[k, j]$$
$$\vdots$$
$$P(a_{n-1} = 0|f(c) = j) = \sum_{k\wedge 2^{n-1}=0} s_n[k, j]$$

$\wedge$는 비트 곱(bitwise and)이다.

정리 1을 이용하여 출력 수열 가 각각 $0 \le f(c) = j < 2^p$에 대해서 1단계 출력 수열 a의 비트별 확률을 미리 계산하여 데이타 베이스화 시킨다면 임의의 출력 수열로부터 초기치를 구하는데 사용할 수 있다.

알고리즘 A : k-단계 p-cycle Cascade 생성기의 초기치 추출 알고리즘

입력 적당한 양의 출력 수열 $c = c_0c_1 \cdots c_{N-1}$

출력 1단계 쉬프트 레지스터의 초기치 $Sr[p]$

예비계산 $T_n^{k-2} = (s_n[i, j])$를 계산하여 $P(a_i = 0|f(c) = j)$를 데이타 베이스화 함

Step 1. 초기치의 길이 p에 해당하는 $Counter[p][2]$ 초기화
초기치의 길이 p에 해당하는 $Zero[p]$, $One[p]$를 초기화
$t = 0$

Step 2. $c = c_ic_{i+1}\cdots c_{i+n-1}$, $j = f(c)$를 계산

Step 3. c에 대응되는 초기치 비트 각각에 대해서 $P(a_{t+i} = 0|f(c) = j)$가 $1/2 + \rho$ 보다 크면 $Counter[(t+i) \bmod p][1]$, $One[(t+i) \bmod p]$을 1 증가시킴
$1/2 - \rho$ 보다 작으면 $Counter[(t+i) \bmod p][0]$, $One[(t+i) \bmod p]$을 1 증가시킴

Step 4. $t = t + 1$, 만약 $t < N$이면 Step 2.로 감

Step 5. 초기치의 각 비트에 대해서 식 (1), (2)를 만족하면 $Sr[i] = 0$으로 출력
식 (1), (2)의 부등호가 반대이면 $Sr[i] = 1$로 출력함
식 (1)과 식 (2)의 부등호 방향이 서로 다르면 $Sr[i]$는 미정

$$Zero[i] > One[i] \quad (1)$$
$$0.5 - Counter[i][0]/(Zero[i]+One[i]) > Counter[i][1]/(Zero[i]+One[i]) - 0.5 \quad (2)$$

알고리즘 A가 성공하기 위해서는 각 비트가 0 또는 1로 나타날 확률이 $pr = 0.5 \pm \rho$일 경우 해당 비트가 0 또는 1로 나타날 확률이 0.5가 아니고 pr이 된다는 것을 판별할 수 있을 만큼의 출력 수열이 필요하다. 본 공격 방식에서는 각 비트가 0 또는 1로 나타날 확률이 정규 분포를 갖는다고 가정하여 필요한 출력 수열의 양 N을 다음과 같이 계산하였다.

1. ρ를 설정
2. 알고리즘 A의 예비계산에서 만들어 놓은 값 중 $0.5+\rho$ 보다 크거나 $0.5-\rho$ 보다 작은 것의 비율을 r라 함
3. $0.5+1.65\sqrt{\frac{0.5\times 0.5}{n}}$
$\le (pr - 1.65\sqrt{\frac{pr\times(1-pr)}{n}})$이 되는
최소의 정수 n을 계산
4. 필요한 출력 수열의 양은 $N = n/r$

알고리즘 A를 사용하여 k-단계 p-cycle Cascade 생성기를 공격하였을 때의 계산 복잡도

는 각 단계 쉬프트 레지스터의 초기치 별로 독립적으로 공격이 가능하므로 kN이다.

4. 분석 실험 결과

8-단계 11-cycle Cascade 생성기를 Lock-in effect로 공격하였을 경우의 계산량은 10^{21} 정도이다. 그런데 알고리즘 A를 적용하면 $\rho = 0.02$로 설정하였을 경우 $N \approx 88{,}000$이 된다. 그러므로 전체적인 계산량은 $11 \times 88{,}000 = 968{,}000$이면 가능할 것이다.

표 2 8-단계 11-cycle Cascade 생성기의 1단계 초기치 공격 실험 결과

초기치 (16진법)	ρ	공격에 성공한 출력 수열의 비트 수
99	0.02	40,000
10a	0.02	40,000
125	0.02	35,000
5b	0.02	10,000
2a	0.02	15,000
108	0.02	165,000
ab	0.005	140,000
103	0.02	25,000
57	0.02	55,000
673	0.005	195,000

8-단계 11-cycle Cascade 생성기를 실제 공격한 결과는 표 2와 같다. 이것은 1단계 쉬프트 레지스터의 초기치만을 구하였으며 모든 쉬프트 레지스터의 초기치를 구하기 위해서는 알고리즘 A를 k번 반복하면 될 것이다. 이 표에서 알 수 있듯이 대부분 88,000 비트 보다 작은 출력 수열로 초기치를 계산하였으며, 88,000 비트보다 많이 필요한 경우에는 초기치 중 약간의 비트를 결정하지 못한 경우로 출력 수열을 증가시키면 분석이 가능하였다.

5. 결 론

Gollmann이 제안한 Cascade 생성기는 비선형성, 발생되는 수열의 난수특성, 주기성 등 암호 알고리즘으로서 필요한 제반 특성을 보장하기 때문에 그동안 스트림 암호의 핵심 논리로 널리 사용되어 왔으나, Cascade 생성기를 stop and go 방식으로 동작시키면 출력 수열과 시각 제어 수열 사이에 암호 알고리즘으로는 부적당한 상관관계 특성이 존재하는 것이 입증되었다. 이 때문에 LFSR로 구성된 Cascade 생성기는 출력 수열에서 run이 발생한 경우 1단계 출력 수열이 1이 될 확률이 매우 높은 특성이 발견되어 해독되었다.

본 고에서는 이런 상관관계 특성을 이용하여 p-cycle Cascade 생성기에 대한 기지 평문 공격 방식을 제안하였으며, 기존의 Lock-in effect 공격 방식에 대하여 10^{21} 정도의 안전성을 보장하는 8-단계 11-cycle Cascade 생성기에 본 방식을 적용한 결과 불과 88,000 출력 비트만을 사용하여 공격이 성공하였다. 제안한 기지 평문 공격 방식은 출력 수열의 모든 비트를 이용하여 분석한 것이 특징이다. Cascade 생성기를 [6]에서 제안한 것처럼 시각 제어 수열이 0(1)인 경우 쉬프트 레지스터를 step1(step2)로 동작시키면 본 논문에서 제안한 공격 방식은 적용할 수 없음을 언급한다.

참 고 문 헌

[1] T. Beth and F. C. Piper, "The Stop-and-go Generator", *Advances in Cryptology: Proc. Eurocrypt '84*, Springer-Verlag, 1984, 88-92.

[2] W. G. Chambers and D. Gollmann, "Lock in Effect in Cascades of Clock Controlled Shift Register", *Advances*

in Cryptology: Proc. Eurocrypt' 88, Springer-Verlag, 1989, 331-343.

[3] W. G. Chambers and S. M. Jennings, "Linear equivalence of Certain BRM Shift Register Sequences", *Electronics Letters*, Vol. 20, No. 24, 1984, 1018-1019.

[4] D. Gollmann, "Pseudorandom Properties of Cascaded Connections of Clock Controlled Shift Registers", *Advances of Cryptology: Proc. of Eurocrypt '84*, Springer-Verlag, 1985, 93-98.

[5] D. Gollmann and W. G. Chambers "Clock-Controlled Shift Registers: A Review", *IEEE J. on Selected Areas in Comm.*, Vol. 7, No. 4, 1989, 525-533.

[6] D. Gollmann and W. G. Chambers "A Cryptanalysis of Step(k,m)-Cascade", *Advances in Cryptology-Eurocrypt '89*, Springer-Verlag, 1990, 680-687.

[7] C. G. Gunther, "Alternating Step Generators Controlled byy de Bruijn Sequences", *Advances in Cryptology: Proc. of Eurocrypt '87*, Springer-Verlag, 1988, 5-14.

[8] W. Meier and O. Staffelbach, "Fast Correlation Attacks on Certain Stream Ciphers", *Journal of Cryptology*, Vol. 1, No. 3, 1989, 159-176.

[9] W. Meier and O. Staffelbach, "Correlation Properties of Combiners with Memory in Stream Ciphers", *Journal of Cryptology*, Vol. 5, No. 1, 1992, 67-86.

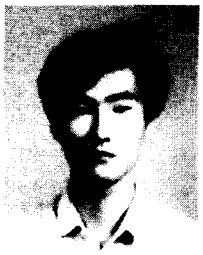
[10] S. J. Park, S. J. Lee, and S. C. Goh, "On the Security of the Gollmann Cascades", *To appear in Advances in Cryptology - Crypto' 95*, Springer-Verlag, 1995.

[11] R. A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, 1986.

[12] R. Vogel, "On the Linear Complexity of Cascaded Sequences", *Advances of Cryptology: Proc. of Eurocrypt '84*, Springer-Verlag, 198, 99-109.

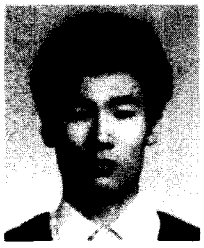
[13] 박상준, 이상진, 고승철, "Cascade 생성기 : 2단계 m-LFSR Cascade 분석", 통신정보보학회 논문지, 제4권, 제1호, 1994.

□ 著者紹介



이 상 진

1987년 2월 고려대학교 이과대학 수학과(이학사)
1989년 2월 고려대학교 대학원 수학과(이학석사)
1994년 8월 고려대학교 대학원 수학과(이학박사)
1989년 10월 ~ 현재 한국전자통신연구소 연구원, 선임연구원



박 상 준(정회원)

1984년 2월 한양대학교 자연과학대학 수학과(이학사)
1986년 2월 한양대학교 대학원 수학과(이학석사)
1986년 1월 ~ 현재 한국전자통신연구소 연구원, 선임연구원
1995년 3월 ~ 현재 성균관대학교 정보공학과 박사과정

고 승 철(정회원)

1981년 2월 연세대학교 수학과(이학사)
1983년 2월 연세대학교 대학원 수학과(이학석사)
1992년 8월 포항공대 대학원 수학과(이학박사)
1984년 3월 ~ 현재 한국전자통신연구소 연구원, 선임연구원, 책임연구원