Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.5, Oct. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.5.1059

Zorro의 연관키 차분특성을 이용한 키 복구 공격 및 PGV-Zorro의 충돌쌍 공격*

김 기 윤,[1†] 박 은 후,[2] 이 종 혁,[1] 장 성 우,[1] 김 지 훈,[2] 김 한 기,[2] 김 종 성[1,2‡]
[1]국민대학교 정보보안암호수학과, [2]국민대학교 금융정보보안학과

Key Recovery Attacks on Zorro Using Related-Key Differential Characteristics, and Collision Attacks on PGV-Zorro*

Giyoon Kim,[1†] Eunhu Park,[2] Jonghyeok Lee,[1] Sungwoo Jang,[1] Jihun Kim,[2]
Hangi Kim,[2] Jongsung Kim[1,2‡]
[1]Dept. of Information Security, Cryptology and Mathematics, Kookmin University
[2]Dept. of Financial Information Security, Kookmin University

요 약

블록암호 Zorro는 AES와 비슷한 연산과정을 거치나 S-box 개수를 줄여 부채널 공격에 대비한 마스킹을 구현 비용을 줄일 수 있게 설계되었다. 하지만 마스터키를 라운드키로 그대로 사용하기 때문에 연관키 차분공격 관점에서 취약하다. 본 논문에서는 Zorro의 연관키 차분특성을 이용해 키 복구 공격을 보인다. 또한 안전성이 증명된 12가지의 PGV 모델을 Zorro를 기반으로 할 때 블록암호의 연관키 차분 특성이 해시함수 충돌쌍 공격에 어떻게 활용될 수 있는지 설명하고 실제 충돌쌍을 제시한다.

ABSTRACT

The block cipher Zorro is designed to reduce the implementation cost for side-channel countermeasure. It has a structure similar to AES, but the number of S-Boxes used is small. However, since the master key is used as the round key, it can be vulnerable to related key attacks. In this paper, we show key recovery attacks on Zorro using related-key differential characteristics. In addition, the related key differential characteristics are fatal when Zorro is used as the base block cipher of the hash function. In this paper, we describe how these characteristics can be linked to collision attacks in the PGV models.

Keywords: block cipher, Zorro, Related-key differential characteristic, key recovery, PGV model, Collision attacks

I. 서 론

디지털 기기의 발전에 따라 다양한 환경에 적합한 암호알고리즘이 제안된 바 있다. 특히, 블록암호 Zorro는 부채널 공격 대응기법인 마스킹 기법을 보다 적은 비용으로 적용하기 위하여 암·복호화 과정의 S-box 연산의 개수를 획기적으로 줄인 바 있다[1]. 하지만 Rasoolzadeh 외 세 명은 [2]에서 위 블록암호의 차분 및 선형 분석으로 키 복구 공격에 성공하였다. 본 논문에서는 Zorro는 키스케줄 과정 없이 마스터키를 라운드키로 사용하기 때문에 연관키 가정에서 효율적인 키 복구 공격을 할 수 있음을 밝힌다.

Received(06. 14. 2018), Modified(10. 01. 2018), Accepted(10. 01. 2018)
* 본 연구는 고려대 암호기술 특화연구센터(UD170109ED)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.
† 주저자, gi0412@kookmin.ac.kr
‡ 교신저자, jskim@kookmin.ac.kr(Corresponding author)

저전력 IoT환경에서는 해시함수를 블록암호 기반으로 사용하는 경우가 있는데, 이 때 Zorro의 연관키 차분특성은 큰 취약점으로 사용될 수 있다. 따라서, PGV와 같이 안전성이 증명된 해시함수를 사용하더라도, 기반 블록암호를 마스터키를 라운드키로 사용하는 Zorro와 같은 경량 블록암호를 사용하면 안전성을 보장할 수 없다. Table 1. 에는 본 논문에서 제시하는 연관키 복구 공격 및 Zorro 기반 PGV 해시함수에 대한 충돌쌍 공격 결과를 정리하였다. 본 연구는 [2]에서 제시한 차분경로가 연관키 차분경로를 구성하는데도 유용하게 사용될 수 있음을 보이며, 더 나아가 이 성질이 해시함수에서 치명적으로 작용함을 보인다.

Table 1., Table 2.는 본 논문의 요약 결과이며 본 논문의 구성은 다음과 같다. 2장에서는 Zorro 알고리즘에 대한 설명과 그 차분특성을 설명한다. 3장에서는 연관키 차분특성을 이용한 키 복구 공격을 서술한다. 4장에서는 Zorro 기반의 PGV 해시함수에 대한 충돌쌍 공격방법을 서술한다. 5장에 결론을 제시한다.

Table 1. The related-key differential key-recovering attack complexities

	Data complexity	Time complexity	Reference
32 bits partial key recovery	2^{24} CP	2^{24}	Chapter 3, Related-key differential attack
	$2^{54.2}$ CP	$2^{54.2}$	[2] Differential attack
128 bits key recovery	2^{24} CP	2^{96}	Chapter 3, Related-key differential attack
	$2^{56.7}$ CP	$2^{56.8}$	[2] Differential attack
	$2^{45.4}$ KP	$2^{45.5}$	[2] Linear attack

* CP: Chosen Plaintext, KP: Known Plaintext

Table 2 . The collision attack complexities on Zorro based PGV model

PGV	Time complexity	PGV	Time complexity
No.1	$2^{53.2}$	No.7	$2^{20.7}$
No.2	$2^{53.2}$	No.8	$2^{20.7}$
No.3	$2^{53.2}$	No.9	$2^{53.2}$
No.4	$2^{53.2}$	No.10	$2^{53.2}$
No.5	$2^{53.2}$	No.11	$2^{20.7}$
No.6	$2^{53.2}$	No.12	$2^{20.7}$

* The actual collision pair for PGV Nos. 7, 8, 11, 12 is attached int the appendix.

II. Zorro 및 기존의 분석 결과

2.1 블록암호 Zorro

2013년에 발표된 경량 블록암호 Zorro는 AES와 같이 평문을 Substitution 단계와 Permutation, 그리고 Mixing 단계로 구성된 SPN 구조를 가진다[1]. 총 24라운드의 암호화 과정으로 128비트 평문과 128비트 마스터키를 입력받아 128비트 암호문을 생성한다. 첫 라운드 시작 전에 화이트닝키를 사용한 후, 4라운드마다 키를 XOR 해주는 AK (AddKey) 단계를 거친다. 각 라운드는 SB^* (SubBytes*), AC (AddConstants), SR (ShiftRows), MC(MixColumns)의 과정으로 구성되어 있다. SR와 MC 단계는 AES와 연산이 동일하다. 라운드키는 마스터키를 그대로 사용하며, 128비트 평문을 8비트씩 나누어 4×4의 행렬로 볼 때 첫 번째 행만 AC단계와 SB^*단계를 거친다는 특징이 있다. 각 단계의 연산은 다음과 같으며 전체 알고리즘은 Fig. 1.과 같다.

- AK (AddKey) : 평문과 마스터 키를 XOR한다.
- SB^*(SubBytes*) : 1행의 총 32비트 값을 S-box에 따라 치환한다.
- AC (AddConstants) : $i(1 \le i \le 24)$번째 라운드의 1행과 $\{i, i, i, i << 3\}$을 XOR한다.
- SR (ShiftRows) : AES와 동일하게 i번째 행은 왼쪽으로 $i-1(1 \le i \le 4)$칸 이동하여 행을

회전시킨다.

- *MC* (MixColumns) : AES의 MixColumns와 동일하게 열에 속한 모든 비트를 순환 행렬을 사용하여 열을 변화시킨다.

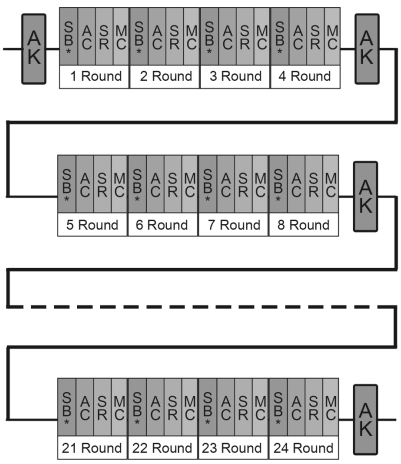


Fig. 1. Zorro's encryption Process

2.2 기존에 연구된 Zorro의 차분특성

*SR*이나 *MC*과 같은 선형함수는 입력과 출력의 차분의 변화를 예측할 수 있기 때문에 차분 경로의 확률에 영향을 미치지 않지만, SB^*과 같은 비선형 함수는 차분 경로의 확률을 떨어뜨린다. Zorro의 경우 1행만 S-box를 거치므로 1행의 차분 값이 차분 경로 예측에 중요한 역할을 한다. Rasoolzadeh등은 이러한 특징을 이용하여 SB^* 연산을 통과하는 1행의 차분 값이 0이 되도록 조절하여 높은 확률의 차분 경로를 Fig. 2와 같이 제시하였다[2].

Fig. 2에서는 네 번째 라운드를 제외한 라운드의 1행은 모두 차분 값이 0 이므로 1, 2, 3 라운드의 SB^*에서는 차분 경로를 1의 확률로 정할 수 있다. 따라서 4개의 라운드 중 네 번째 라운드에서만 차분 확률이 발생한다. 또한 첫 번째 라운드의 시작 차분(#1)과 네 번째 라운드의 마지막 차분(#1)을 일치시켜 네 라운드씩 반복되는 차분 경로를 구성했다. [2]에서는 이렇게 반복되는 4개의 라운드를 Step이라고 명명하고 있다.

Fig. 2의 차분 경로를 만족하기 위해서는 #10에서 1행1열과 1행3열의 S값이 SB^*을 거쳐 #11에서 1행1열과 1행3열의 S값을 가져야 하고, #10에서

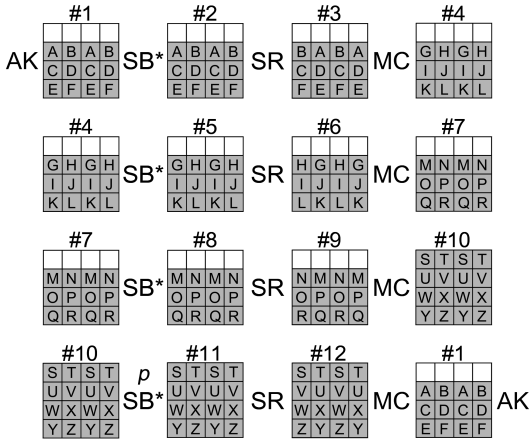


Fig. 2. Zorro's differential path

1행2열과 1행4열의 T값은 #11에서 1행2열과 1행4열의 T값을 가져야 하는 사실을 알 수 있다. 이 때 Zorro에서는 SB^* 과정을 첫 번째 행에만 시행하므로 나머지 행에서의 차분경로는 확률 1로 결정된다. [2]에 의하면 Fig.2. 를 만족하는 차분 값은 Table 3. 과 같이 총 여섯 가지가 있다. 이 때 Table 3. 에서 S가 값을 가질 경우 T는 0이 되며 반대로 T가 값을 갖는 경우 S은 0이 된다.

1, 2, 3라운드에서는 1행의 차분 값이 0이기 때문에 한 Step에서의 확률은 4라운드인 Fig. 2.의 #10에서 #11의 과정에서만 발생한다. 이때 S가 S 혹은 T가 T로 될 확률은 6/256이다. 앞서 설명한 S와 T의 관계에 의하면 둘 중 하나가 차분 값을 가질 때 나머지 하나는 0차분을 가지므로 1의 확률을 가진다. 따라서 Fig. 2에서 #10의 첫 번째 행이 S-box를 거쳐 #11의 첫 번째 행이 될 확률은 다음과 같다.

$$p = DP(\mathrm{S}\rightarrow\mathrm{S}) \times DP(\mathrm{T}\rightarrow\mathrm{T}) = \left(\frac{6}{256}\right)^2 \times 1^2 = \left(\frac{6}{256}\right)^2 \quad (1)$$

이때, $DP(\mathrm{S}\rightarrow\mathrm{S})$는 S가 S-box를 거쳐 S로 나올 확률을 의미한다. Zorro는 총 6 Step으로 구성되어 있다. 따라서 Zorro의 6 Step의 차분 경로가 Fig. 2. 의 차분 경로를 만족할 확률은 다음과 같다.

$$((\frac{6}{256})^2)^6 = (2^{-10.8})^6 = 2^{-64.8} \quad (2)$$

Table 3. The difference value satisfying the differential path of Fig. 2.

No.	A	B	C	D	E	F	G	H	I
1	136	158	22	22	149	175	178	164	88
2	158	136	22	22	175	149	164	178	0
3	92	55	107	107	143	50	225	138	183
4	55	92	107	107	50	143	138	225	0
5	22	78	88	88	98	138	254	166	123
6	78	22	88	88	138	98	166	254	0

No.	J	K	L	M	N	O	P	Q	R
1	0	205	178	20	178	254	254	185	51
2	88	178	205	178	20	254	254	51	185
3	0	56	225	255	225	169	169	89	145
4	183	225	56	225	255	169	169	145	89
5	0	25	254	80	254	213	213	210	204
6	123	254	25	254	80	213	213	204	210

No.	S	T	U	V	W	X	Y	Z
1	0	123	85	136	0	35	42	131
2	123	0	136	85	35	0	131	42
3	0	234	168	92	0	93	113	228
4	234	0	92	168	93	0	228	113
5	0	247	79	22	0	140	168	58
6	247	0	22	79	140	0	58	168

〔2〕에서는 이와 같은 확률을 갖는 차분 경로를 Fig. 2. 과 같이 여섯 가지를 제시하였다. 본 논문에서는 〔2〕에서 제시한 여섯 가지의 차분 값인 Table 3.의 차분 값을 동일하게 사용한다.

Fig. 2.의 차분 특성은 동일한 키에 대한 경로를 가정한 것으로 키의 차분이 0이다. 본 논문에서는 평문 차분이 ΔP, 키 차분이 ΔK 일 때 암호문 차분이 ΔC인 연관키 차분 특성 또는 차분 특성을 $(\Delta P,\Delta K,\Delta C)$와 같이 표시한다. 따라서 Fig. 2 에서의 차분 특성은 $(\alpha,0,\alpha)$이다.

III. Zorro에 대한 연관키 차분 경로를 이용한 키 복구 공격

연관키 공격(Related-key Attack)이란 평문 뿐만 아니라 키에도 차분을 설정하여 각 키로부터 생성된 평문과 암호문 쌍을 이용해 키를 찾아낼 수 있는 방법이다. 본 절에서는 기존에 적용되지 않았던 연관키 공격을 이용한 마스터키 키 복구 공격을 설명한다.

3.1 Zorro의 연관키 공격

Zorro는 첫 Step이 시작하기 전과, 각 Step이 끝날 때마다 마스터키(이하 키)를 XOR한다. 따라서 키에도 평문과 동일한 차분을 설정한다면 차분을 설정하지 않은 경우보다 더 높은 확률로 차분 경로를 만족하는 암호문 쌍을 얻을 수 있다.

Fig .2. 에서 사용한 평문 차분 #1을 $\Delta\alpha$라하고, 2개의 키 K, K′의 차분 또한 평문 차분과 동일하게 $\Delta\alpha$이라하자($K\oplus K'=\alpha$). 첫 번째 라운드에서 AK 단계를 거치면 두 평문의 차분이 0이 된다. 따라서 첫 번째 Step은 모두 차분이 0이 된다. 두 번째 Step의 시작부분에서 평문의 차분은 0이지만, 키의 차분은 $\Delta\alpha$이므로 AK단계를 거치면 다시 두 메시지의 차분이 $\Delta\alpha$인 상태로 Step을 시작하게 된다. 이를 계속 진행하면 세 번째 Step이 시작할 때는 AK 단계에 의해 #1의 차분이 $\Delta 0$가 된다. 이를 그림으로 표현한다면 Fig. 3와 같다.

따라서 홀수 번째 Step의 모든 과정은 0차분을 갖고, 짝수 번째 Step의 결과는 $\Delta\alpha$차분을 갖는다는 것을 알 수 있다. 홀수 번째 Step에서는 모든 과정이 0차분을 가지므로, 차분 특성의 확률은 $p=1$이 되고, 짝수 번째 Step에서는 기존 논문의 확률인 $p=(6/256)^2$를 그대로 따른다. 따라서 키에 평문과 같은 차분을 설정하는 경우 총 6 Step의 확률은 다음과 같다.

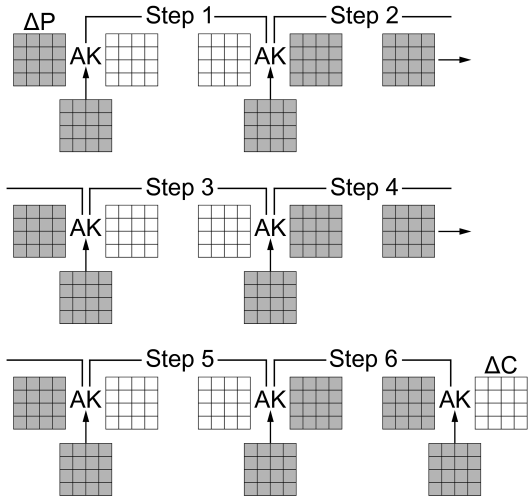


Fig. 3. Zorro's relative key differential characteristic $(\alpha,\alpha,0)$

$$p = ((\frac{6}{256})^2)^3 = (\frac{6}{256})^6 = (2^{-10.8})^3 \approx 2^{-32.4} \quad (3)$$

위 연관키 차분 특성은 $(\alpha, \alpha, 0)$로 표현할 수 있다.

만약 2개의 평문의 차분이 0 이고 K, K′ 의 차분이 $\Delta\alpha$ 라면 위의 경우와 정 반대로 홀수 번째 Step의 차분은 $\Delta\alpha$, 짝수 번째 Step의 차분은 0이 된다. 따라서 이 경우에도 차분경로의 확률은 (3)과 동일하며 $(0, \alpha, \alpha)$라고 표현할 수 있다. 이를 그림으로 표현한다면 Fig. 4와 같다.

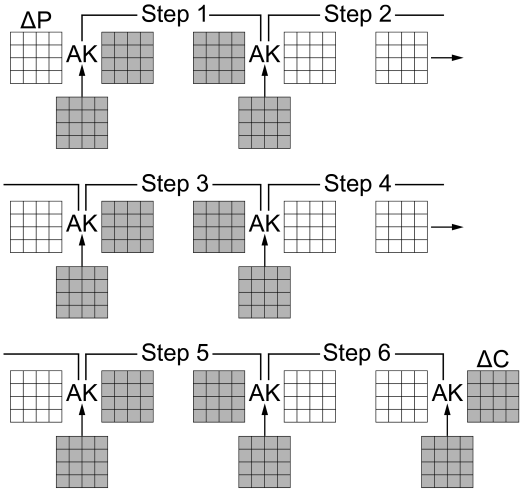


Fig. 4. Zorro's relative key differential characteristic $(0, \alpha, \alpha)$

3.2 Zorro의 키 복구 공격

본 논문의 키 복구 공격에서는 Zorro의 23라운드까지는 연관키 3.1절의 차분 경로를 동일하게 구성하되, 24라운드에서는 차분경로를 고려하지 않는다. 이때의 연관키 차분 경로는 Fig. 5와 같으며, 차분경로의 확률은 아래와 같다.

$$p = ((\frac{6}{256})^2)^2 = (\frac{6}{256})^4 = (2^{-10.8})^2 \approx 2^{-21.6}$$

따라서, 2^{24}개의 평문쌍을 암호화하면 최종적으로 Fig. 5와 같은 암호문 쌍을 5개 정도 기대할 수 있다.

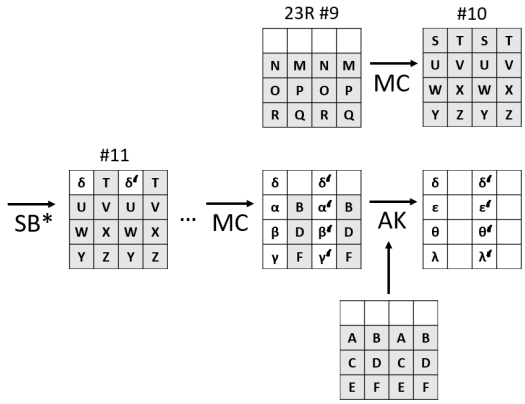


Fig. 5. 23, 24 round differential path used for key recovery attack

$\because p \times N \approx 2^{-21.6} \times 2^{24} = 2^{2.4} \approx 5$
(N: 실행 평문쌍의 개수)

이렇게 준비된 5쌍의 암호문쌍으로 마지막 한 라운드를 복호화하여 키 복구 공격을 한다. 24라운드에서의 1행1열의 입력 차분 S에 대한 출력 차분을 δ이라고 하고 1행3열의 입력차분 S에 대한 출력차분을 δ'라고 하자. 이때 δ와 δ'의 값은 DDT (Differnetial Distribution Table)를 통해 알 수 있다. 0차분인 T은 S-box를 거치면 1의 확률로 0차분을 가지고, 나머지 2, 3, 4행은 S-box의 영향을 받지 않으므로 차분 값이 변하지 않는다. 이후 SR, MC, AK를 거쳐 암호문이 되었을 때 암호문의 차분은 2, 4열이 0이고 1,3열의 차분 값 δ과 δ'에 의해 다양한 결과가 나온다. 이를 통해 2^{24}개의 평문쌍으로 23개의 라운드만 연관키 차분 경로를 만족하는 암호문쌍을 얻는다면 그 암호문쌍은 반드시 2,4열의 차분이 0이고 1,3열은 임의의 값이 될 것이며 이러한 암호문 쌍의 개수가 약 5개라는 것을 알 수 있다. 이렇게 얻은 5개의 암호문 쌍을 통해 키복구 공격을 진행한다.

SR, MC, AK는 선형연산이므로 아래와 같이 연산의 순서를 바꿔도 암호화 과정이 성립한다.

$$SB \rightarrow SR \rightarrow MC \rightarrow AK \rightarrow C \quad (4)$$

$$SB \rightarrow AK' \rightarrow SR \rightarrow MC \rightarrow C \quad (5)$$

마지막 라운드의 과정을 표현하면 (4)과 같다. 그리고 키의 정보를 찾기 위해 AK 과정을 SR 과정 앞

으로 이동하면 (5)와 같다. 단, AK 과정과 AK'에서 사용되는 키가 달라진다. (4)의 AK 과정에서 사용되는 키의 차분을 $\triangle MK$라 하면, (5)의 AK' 과정에서 사용되는 키의 차분은 $SR^{-1}(MC^{-1}(\triangle MK))$이다.

(2)에서 5개의 암호문쌍에 SR, MC 연산을 역연산하고 AK'과정을 거치면 그 결과는 24라운드에서 SB를 거친 직후이므로 Fig. 5의 #11에 해당하는 차분 값을 갖는다. 따라서 #11에 해당하는 차분을 식으로 표현하면 다음과 같다.

$$SR^{-1}(MC^{-1}(\triangle C)) \oplus SR^{-1}(MC^{-1}(\triangle MK))$$

Fig. 5의 #10의 차분 값과 #11의 차분 값을 알고 있다면 차분이 0이 아닌 열에 대하여 #11에 SB의 역 연산을 적용해 #10의 차분 값이 나올 경우 키로 추측이 가능하다. 마찬가지로 위의 과정과 동일하되, T가 차분 값을 갖고 S가 0차분이 되는 평문 차분을 구성해 동일하게 진행하면 AK' 단계 키의 1행에 대한 정보를 모두 얻을 수 있다. AK' 단계에 키는 $SR^{-1}(MC^{-1}(MK))$ 인데 SR 단계는 1행에 영향을 끼치지 않으므로 결국 이 과정을 통해 $(MC^{-1}(MK))$ 의 첫 번째 행의 32비트를 알 수 있다. 그러므로 $(MC^{-1}(MK))$ 의 2, 3, 4행에 대한 전수 조사를 하며 MC, SR 를 순서대로 진행하면 완전한 키를 복구할 수 있다. 이를 통해 전수 조사량이 2^{128}에서 2^{96}으로 줄어들었음을 알 수 있다.

실제 구현을 통해 암호화 키 하나에 서로다른 평문을 2^{24}번의 암호화 후 필터링하기를 반복한 결과 경로를 만족하는 암호문쌍을 평균적으로 3.6쌍 얻을 수 있었고. 3.6쌍에 대하여 키 복구를 시행해본 결과 3.6쌍의 암호문에 대해 역연산 한 32비트 키 복구에 성공하였다.

IV. 차분 특성을 이용한 PGV-Zorro 공격방법

본 장에서는 Zorro 기반의 PGV 해시함수에 대한 충돌쌍 공격을 소개한다. PGV-모델은 블록암호를 이용해 해시함수(이하 PGV)를 구성하는 방법으로 Preneel 등이 제안하였다[3]. 총 64가지 방법 중 Table 4 의 12가지 PGV-모델들만이 이상적인 블록암호를 기반으로 할 때 해시함수로서 안전하다[4]. PGV 모델은 블록암호의 평문과 키를 적절히 조합하여 안전한 해시함수를 생성하는데, 이러한 구조로 인해 연관키 차분 경로를 가지는 블록암호를 사용하였을 때에 취약점이 드러날 수 있다. 특히 기반 블록암호가 연관키 반복 차분특성을 가지는 경우에는 해시함수의 충돌쌍 공격으로 쉽게 확장될 수 있음이 연구된 바 있다[5].

4.1절부터 사용되는 기호는 다음과 같다.

M_i : i 번째 메시지 블록

C_i : i 번째 암호문 블록

H_i : i 번째 해시 블록

IV : 초기화 벡터

$E_K(P)$: 평문 P와 KEY를 입력으로 받는 블록암호

Table 4. 12 safe PGV-Model

PGV Model	i^{th} compression function
No.1	$H_i = E_{H_{i-1}}(M_i) \oplus M_i$
No.2	$H_i = E_{H_{i-1}}(M_i \oplus H_{i-1}) \oplus M_i \oplus H_{i-1}$
No.3	$H_i = E_{H_{i-1}}(M_i) \oplus M_i \oplus H_{i-1}$
No.4	$H_i = E_{H_{i-1}}(M_i \oplus H_{i-1}) \oplus M_i$
No.5	$H_i = E_{M_i}(H_{i-1}) \oplus H_{i-1}$
No.6	$H_i = E_{M_i}(M_i \oplus H_{i-1}) \oplus M_i \oplus H_{i-1}$
No.7	$H_i = E_{M_i}(H_{i-1}) \oplus M_i \oplus H_{i-1}$
No.8	$H_i = E_{M_i}(M_i \oplus H_{i-1}) \oplus H_{i-1}$
No.9	$H_i = E_{M_i \oplus H_{i-1}}(M_i) \oplus M_i$
No.10	$H_i = E_{M_i \oplus H_{i-1}}(H_{i-1}) \oplus H_{i-1}$
No.11	$H_i = E_{M_i \oplus H_{i-1}}(M_i) \oplus H_{i-1}$
No.12	$H_i = E_{M_i \oplus H_{i-1}}(H_{i-1}) \oplus M_i$

4.1 선택 평문 또는 선택 키 공격

Fig. 2에서 #1의 차분 $\Delta\alpha$로 만들어진 #10의 차분을 $\Delta\delta$라 한다면, #10에서 #11로의 결과가 $\Delta\delta$를 만족하는 #10을 #1까지 복호화 했을 때 $\Delta\alpha$의 차분을 가짐은 자명하다. 이 때 #10의 $\Delta\delta$차분이 다시 #11의 $\Delta\delta$차분이 되는 경우는 #10의 경우의 수 2^{127}쌍에 P를 곱한 $2^{127} \times \left(\frac{6}{256}\right)^2 \approx 2^{116.2}$ 쌍 존재함을 알 수 있다.

이러한 $\Delta\delta$ 에서 $\Delta\delta$로 가는 충분히 많은 #10 중 한 쌍을 #1까지 복호화한 후 평문 또는 키의 값을 조절 하면 차분 특성을 만족하는 연관키 차분 특성의 확률을 다음과 같이 높일 수 있다.

$$(\alpha,0,\alpha) \approx 2^{-54.2}$$
$$(\alpha,\alpha,0) \approx 2^{-21.7}$$
$$(0,\alpha,\alpha) \approx 2^{-21.7}$$

위의 확률을 갖는 평문과 키를 선택함으로써 생일 공격인2^{-64}보다 더 큰 확률을 가지므로 유의미한 공격이 가능하다.

4.2 Zorro 기반 PGV-모델 공격

본 논문의 Zorro 기반 PGV-모델에 대한 공격은 생일 공격과 비교하여 확률이 더 큰 경우만 공격에 성공하였다고 가정하였으며 이는 n비트 길이의 해시 함수에 대하여 $2^{n/2}$번 이하의 시도로 공격 성공 확률이 40% 이상임을 뜻한다. Zorro 기반 해시 함수는 연관키 차분 특성에 의해 PGV-모델 별로 한 블록 또는 두 블록의 충돌쌍을 찾을 수 있다.

4.2.1 한 블록으로 공격이 가능한 PGV-모델

본 절에서는 PGV-모델 No.1을 예로 들어 한 블록으로 충돌쌍을 찾는 방법을 설명한다. PGV-Model No.1은 키에 차분을 선택할 수 없기 때문에 $(\alpha,0,\alpha)$ 특성을 이용 한다.

Setup Phase. Table 3. 을 이용하여 $\Delta\alpha$의 차분을 갖는 메시지를 다음과 같이 구성한다.
$(M_1,M'_1),(M_2,M'_2),\ldots,(M_i,M'_i)$
($i \geq p^{-1}$, p는 연관키 차분 특성의 확률)

Search Phase. 메시지를 암호화한 암호문의 차분이 $\Delta\alpha$인 (c_n,c'_n) 을 찾는다.

Construction Phase. 암호문을 PGV-모델의 남은 과정을 연산하여 충돌쌍 (H_1,H_1')을 얻는다.

-충돌 쌍 확인

$$H_1 = E_{IV}(M_1)\oplus M_1$$

$$\begin{aligned} H_1' &= E_{IV}(M_2)\oplus M_2 \\ &= c_1\oplus\Delta\alpha\oplus M_1\oplus\Delta\alpha \\ &= c_1\oplus M_1 \\ &= E_{IV}(M_1)\oplus M_1 = H_1 \end{aligned}$$

-공격 시간 복잡도

*Search Phase*에서 $2^{54.2}$의 시간 복잡도가 필요하다.

-공격 성공 확률

*Search Phase*의 성공확률 : $1-(1-\frac{1}{2^{54.2}})^{2^{53.2}} \approx 0.4$

따라서 Zorro을 이용한 PGV-모델 No.1에 대한 충돌쌍 공격의 성공 확률은 $2^{53.2}$회 시도 시 40% 이고 이는 2^{64}인 생일공격보다 더 우위에 있으므로 유효한 공격이다.

위와 유사한 방법으로 PGV모델 2,3,4,7,8,11,12번 모두 한 블록으로 공격이 가능하며 공격에 필요한 연관키 차분 특성과 공격복잡도는 Table 5.와 같다. 이 중 공격복잡도가 낮은 Zorro 기반 PGV 7, 8, 11, 12의 대한 실제 충돌쌍을 부록에서 보인다.

Table 5. PGV-Zorro's one block collision attack

No.	relative key differential characteristic	Probability of differential path	Time complexity	Success rate
1	$(\alpha,0,\alpha)$	$\approx 2^{-54.2}$	$2^{53.2}$	40%
2	$(\alpha,0,\alpha)$	$\approx 2^{-54.2}$	$2^{53.2}$	40%
3	$(\alpha,0,\alpha)$	$\approx 2^{-54.2}$	$2^{53.2}$	40%
4	$(\alpha,0,\alpha)$	$\approx 2^{-54.2}$	$2^{53.2}$	40%
7	$(0,\alpha,\alpha)$	$\approx 2^{-21.7}$	$2^{20.7}$	40%
8	$(\alpha,\alpha,0)$	$\approx 2^{-21.7}$	$2^{20.7}$	40%
11	$(\alpha,\alpha,0)$	$\approx 2^{-21.7}$	$2^{20.7}$	40%
12	$(0,\alpha,\alpha)$	$\approx 2^{-21.7}$	$2^{20.7}$	40%

4.2.2 두 블록으로 공격이 가능한 경우

본 절에서는 PGV-모델 No.5 을 예로 들어 두 블록으로 충돌쌍을 찾는 방법을 설명한다. PGV-모델 No.5 은 첫 블록에서 Zorro 암호 알고리즘에 들어가는 평문이 IV이므로 첫 번째 블록은 $(0,\alpha,\alpha)$의 특성을 이용하며 두 번째 블록은 $(\alpha,0,\alpha)$의 특성을 이용한다.

Storage Phase. Table 3. 을 이용하여 $\Delta\alpha$의 차분을 갖는 메시지 $(M_n^1, M_n^{1'})$을 구성해 암호화한 후 (H_1, H_1')의 차분이 $\Delta\alpha$ 인 것을 저장한다.

Setup Phase. $\Delta 0$ 차분의 메시지를 구성한다.
$(M_1^2, M_1^2), (M_2^2, M_2^2), \ldots, (M_i^2, M_i^2)$
($i \geq p^{-1}$, p는 연관키 차분 특성의 확률)

Search Phase. 메시지를 키로 사용해 (H_1, H_1')을 암호화한 암호문 중 차분이 $\Delta\alpha$인 (c_n, c'_n) 을 찾는다.

Construction Phase. 암호문을 PGV-모델의 남은 절차대로 XOR하여 충돌쌍 (H_2, H_2')을 얻는다.

- 충돌 쌍 확인

$$H_1 = E_{M_i^1}(IV) \oplus IV = c_1 \oplus IV$$
$$H_1' = E_{M_i^{1'}}(IV) \oplus IV$$
$$\therefore H_1 \oplus H'_1 = \Delta\alpha$$

$$H_2 = E_{M_i^2}(H_1) \oplus H_1 = c_2 \oplus H_1$$
$$\begin{aligned} H_2' &= E_{M_i^2}(H_1') \oplus H_1' \\ &= c_2 \oplus \Delta\alpha \oplus H_1 \oplus \Delta\alpha \\ &= c_2 \oplus H_1 \\ &= E_{M_i^2}(H_1) \oplus H_1 = H_2 \end{aligned}$$

- 공격 시간 복잡도

Storage Phase에서 $2^{21.7}$ 정도의 시간 복잡도가 필요하며 Search Phase에서 $2^{54.2}$정도의 시간 복잡도가 필요하다. 따라서 시간 복잡도는 $2^{54.2} + 2^{21.7} \approx 2^{54.2}$이다.

- 공격 성공 확률

*Storage Phase*의 성공확률 : $1-(1-\frac{1}{2^{21.7}})^{2^{20.7}} \approx 0.4$

*Search Phase*의 성공확률 : $1-(1-\frac{1}{2^{54.2}})^{2^{53.2}} \approx 0.4$

따라서 Zorro을 이용한 PGV-모델 No.5에 대한 충돌쌍 공격의 성공확률은 $2^{53.2}$회 시도 시 40% 이고 이는 2^{64}인 생일공격보다 더 우위에 있으므로 유효한 공격이다.
위와 유사한 방법으로 PGV-모델 5,6,9,10번 모두 두 블록으로 공격이 가능하며 공격에 필요한 차분 특성과 공격복잡도는 Table 6와 같다.

Table 6. PGV-Zorro's two block collision attack

No.	relative key differential characteristic	Probability of differential path	Time complexity	Success rate
5	$(0,\alpha,\alpha)$, $(\alpha,0,\alpha)$	$\approx 2^{-54.2}$	$2^{53.2}$	40%
6	$(\alpha,\alpha,0)$, $(\alpha,0,\alpha)$	$\approx 2^{-54.2}$	$2^{53.2}$	40%
9	$(\alpha,\alpha,0)$, $(\alpha,0,\alpha)$	$\approx 2^{-54.2}$	$2^{53.2}$	40%
10	$(0,\alpha,\alpha)$, $(\alpha,0,\alpha)$	$\approx 2^{-54.2}$	$2^{53.2}$	40%

* 연관키 차분 특성은 순서대로 첫 번째 블록에서 사용해야 하는 차분 특성, 두 번째 블록에서 사용해야 하는 차분 특성을 의미한다.

V. 결 론

본 연구에서는 블록암호 Zorro가 키스케줄을 사용하지 않고 마스터키를 라운드키로 사용한다는 점을 이용하여, [2]에서 제시한 차분경로를 연관키 차분 특성으로 적용시켰다. 결과적으로, 연관키 차분경로를 구성하는데 효과적으로 적용되었으며 키 복구 공격의 데이터 복잡도를 2^24으로 낮출 수 있었다.

더나아가 Zorro의 반복 차분특성은 해시함수의 기반 블록암호로 사용될 때 충돌쌍 공격으로 이어질 수

있는 치명적인 성질임을 보인다. Zorro와 같이 키스케줄을 가지지 않는 블록암호는 반복 차분특성을 가지기 쉽기 때문에, 블록암호 기반 해시함수에 이용하기에는 부적절함을 알 수 있다.

References

[1] B. Gérard, V. Grosso, Naya-Plasencia, and M. Standaert, F.-X., "Block ciphers that are easier to mask: how far can we go?" In: Bertoni, G., Coron, J.-S. (eds.) CHES 2013. LNCS, vol. 8086, pp. 383 - 399, Aug 2013

[2] S. Rasoolzadeh, Z. Ahmadian and M. Salmasizadeh, Aref, M.R. "Total break of Zorro using linear and differential attacks." IACR Cryptology ePrint Archive, 220, Jine. 2014.

[3] B. Preneel, R. Govaerts and J. Vandewalle "Hash functions based on block ciphers: A synthetic approach." In: Advances in Cryptology - Proceedings of CRYPTO '93, LNCS 773. Springer, pp 368 - 378, July. 2001

[4] J. Black, P. Rogaway and T. Shrimpton, "Black-box analysis of the block-cipher-based hash-function constructions from pgv." In: Advances in Cryptology - Proceedings of CRYPTO '02, LNCS 2442. Springer, pp 320 - 335, Sep. 2002

[5] H. Kim, D. Kim, O. Yi and J. Kim "Cryptanalysis of hash functions based on blockciphers suitable for IoT service platform security" - Multimedia Tools and Applications in Springer, pp 1-24, Mar. 2018

부 록

A. 충돌쌍

Table 7. PGV-Model No.7

IV	
{102, 186, 99, 106, 185, 126, 62, 233, 157, 29, 56, 129, 30, 132, 35, 126}	
M1	M2
0x2995CD00, 0x00939093, 0xD2E02917, 0xEB00B000	0x290BDBAF, 0x001B8606, 0xD27E3FB8, 0xEB88A695
0x1EE45ED9, 0x8402B67B, 0xE58EBA99, 0x4C9119E8	0x1E7A4876, 0x848AA0EE, 0xE510AC36, 0x4C190F7D

Table 8. PGV-Model No.8

IV	
{145, 27, 92, 156, 188, 217, 193, 179, 235, 90, 157, 100, 233, 58, 174, 252 }	
M1	M2
0x8C4A87D9, 0xCB0035CF, 0x435A9980, 0xBD6F6380	0x8CD49176, 0xCB88235A, 0x43C48F2F, 0xBDE77515
0x37E0AC71, 0x4C02612F, 0xF845B22B, 0x856DF560	0x377EBADE, 0x4C8A77BA, 0xF8DBA484, 0x85E5E3F5

Table 9. PGV-Model No.11

IV	
{234, 116, 234, 213, 159, 135, 211, 35, 229, 42, 55, 239, 204, 240, 198,222 }	
M1	M2
0x4EE2F02F, 0x963AC11B, 0xEB66BA52, 0xBCBA9C00	0x4E7CE680, 0x96B2D78E, 0xEBF8ACFD, 0xBC328A95
0x8C889AF7, 0xC82886CF, 0x29B5D057, 0x76A8AAD4	0x8C168C58, 0xC8A0905A, 0x292BC6F8, 0x7620BC41

Table 10. PGV-Model No.12

IV	
{215, 145, 92, 60, 8, 127, 67, 29, 220, 49, 48, 146, 143, 53, 139, 234 }	
M1	M2
0x98C37474, 0xA1FE1675, 0x98B4CBB8, 0x3E97BF71	0x985D62DB, 0xA17600E0, 0x982ADD17, 0x3E1FA9E4
0x0DE97680, 0x3647801E, 0x0D1CC9EA, 0x042EE31A	0x0D77602F, 0x36CF968B, 0x0D82DF45, 0x04A6F58F

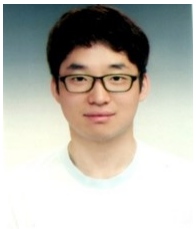
〈저자소개〉

김 기 윤(Giyoon Kim) 학생회원
2013년 3월~현재: 국민대학교 정보보안암호수학과 재학중
〈관심분야〉 정보보호, 암호 알고리즘, 디지털 포렌식

박 은 후(Eunhu Park) 학생회원
2018년 8월: 국민대학교 정보보안암호수학과 졸업
2018년 9월~현재: 국민대학교 금융정보보안학과 석사과정
〈관심분야〉 정보보호, 디지털 포렌식

이 종 혁(Jonghyeok Lee) 학생회원
2017년 3월~현재: 국민대학교 정보보안암호수학과 재학중
〈관심분야〉 정보보호, 암호 알고리즘, 디지털 포렌식

장 성 우(Sungwoo Jang) 학생회원
2012년 3월~현재: 국민대학교 정보보안암호수학과 재학중
〈관심분야〉 정보보호, 암호 알고리즘, 디지털 포렌식



김 지 훈 (Jihun Kim) 학생회원
2017년 2월: 국민대학교 수학과 졸업
2017년 3월~현재: 국민대학교 금융정보보안학과 석사과정
〈관심분야〉 정보보호, 암호 알고리즘

김 한 기(Hangi Kim) 학생회원
2016년 2월: 국민대학교 수학과 졸업
2018년 3월: 국민대학교 금융정보보안학과 이학석사
2018년 3월~현재: 국민대학교 금융정보보안학과 박사과정
〈관심분야〉 정보보호, 암호 알고리즘, 디지털 포렌식

김 종 성(Jongsung Kim) 종신회원
2000년 8월/2002년 8월: 고려대학교 수학 전공 학사/이학석사
2006년 11월: K.U.Leuven. ESAT/SCD-COSIC 정보보호 전공 공학박사
2007년 2월: 고려대학교 정보보호대학원 공학박사
2007년 3월~2009년 8월: 고려대학교 정보보호기술연구센터 연구교수
2009년 9월~2013년 2월: 경남대학교 e-비즈니스학과 조교수
2013년 3월~2017년 2월: 국민대학교 수학과 부교수
2014년 3월~현재: 국민대학교 일반대학원 금융정보보안학과 부교수
2017년 3월~현재: 국민대학교 정보보안암호수학과 부교수
〈관심분야〉 정보보호, 암호 알고리즘, 디지털 포렌식.