Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.4, Aug. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.4.803

연관키 차분 특성을 이용한 Fantomas와 Robin의 키 복구 공격*

김 한 기,[1†] 김 종 성[1,2‡]
[1]국민대학교 금융정보보안학과, [2]국민대학교 정보보안암호수학과

Key Recovery Attacks on Fantomas and Robin Using Related-Key Differentials*

Hangi Kim,[1†] Jongsung Kim[1,2‡]
[1]Dept. of Financial Information Security, Kookmin University,
[2]Dept. of Information Security, Cryptology and Mathematics, Kookmin University

요 약

Fantomas와 Robin은 FSE 2014에서 제안된 경량 블록암호 패밀리 LS-designs에 포함되는 블록암호로, 비트슬라이스 구현이 가능한 L-Box와 S-Box를 사용하여 부채널 분석 대응기법인 마스킹 기법을 효율적으로 적용할 수 있도록 설계되었다. 본 논문은 연관키 차분경로 분석을 통한 Fantomas와 Robin의 전체 128비트 키의 복구 공격이 각각 2^{56}, 2^{72}의 시간 복잡도와 2^{52}, 2^{69}개의 선택 평문으로 가능함을 보인다.

ABSTRACT

The Fantomas and the Robin are the block ciphers included in the LS-designs, the family of block ciphers. They are designed to efficiently apply the masking technique, which is a side-channel analysis countermeasure technique, using L-boxes and S-boxes capable of bit slice implementation. In this paper, we show that the key recovery attacks of Fantomas and Robin through the related-key differential analysis are possible with 2^{56} and 2^{72} time complexity, 2^{56} and 2^{69} chosen plaintext respectively.

Keywords: Fantomas, Robin, LS-design, Related-key attack, Differential path, Key recovery attack

I. 서 론

IoT 기기 사용자가 늘어남에 따라, 경량 프로토콜이나 저사양 기기와 같은 경량 플랫폼에서의 보안이 중요해지고 있다. 경량 블록암호이면서 부채널 대응 기법 적용이 효율적인 블록암호로는 PICARO[1]와 Zorro[2]등이 있지만, 마스킹 기법 적용 시 오버헤드를 높이는 비선형 연산이 여전히 많이 사용되었다. LS-designs는 이러한 한계를 극복하기 위해 S-Box와 L-Box에 사용되는 비선형 연산 개수를 획기적으로 줄이면서 비트슬라이스로 손쉽게 구현 가능하도록 설계된 블록암호 패밀리이다[3]. 대표적으로는 Fantomas와 Robin이 있다.

연관키 차분공격은 공격자가 마스터키의 차분을 선택할 수 있다는 가정의 공격으로, Knudsen[5]과 Biham[4]이 독립적으로 제안하였다. LS-designs

Received(04. 17. 2018), Modified(07. 13. 2018), Accepted(07. 14. 2018)
* 이 논문은 2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2016R1D1A1A09919726)
† 주저자, tiontta@kookmin.ac.kr
‡ 교신저자, jskim@kookmin.ac.kr(Corresponding author)

의 키 스케줄을 매우 간단하게 설계되어, 연관키 공격 가정에서 라운드키에 사용될 차분을 직접적으로 선택할 수 있다. 본 논문에서는 연관키 차분공격을 이용해 Fantomas와 Robin의 마스터키를 각각 2^{52}, 2^{69}의 선택평문을 사용하여 2^{56}과 2^{72}의 시간 복잡도로 복구할 수 있음을 보인다.

II. Fantomas와 Robin의 구조

Grosso 등은 [3]에서 비트슬라이싱 구현이 용이함과 동시에 적절한 암호학적 안전성을 가지는 S-Box와 L-Box를 조합하여 LS-designs에 적용, 128비트 평문과 128비트 마스터키를 사용하는 블록암호 Fantomas와 Robin를 제안하였다. Fantomas는 non-involutive L-Box와 non-involutive S-Box로 12라운드를 사용하는데 비해, Robin은 involutive L-Box와 involutive S-Box로 16라운드를 사용한다는 점이 그 특징이다. LS-designs 블록암호의 암호화 과정은 Fig. 1과 같이 S-Layer와 L-Layer, 라운드키 XOR 과정으로 이루어져 있다(Fantomas: $r=12$, Robin: $r=16$). 라운드키로는 마스터키 K에 상수 $Cst(i)$를 XOR한 값이 사용된다.

LS-designs의 state를 Fig. 2과 같이 각 셀을 한 비트로 표현하여 나타낼 수 있다. 비트슬라이스 기법으로 구현할 시, S-Layer는 각 열에 S-Box를

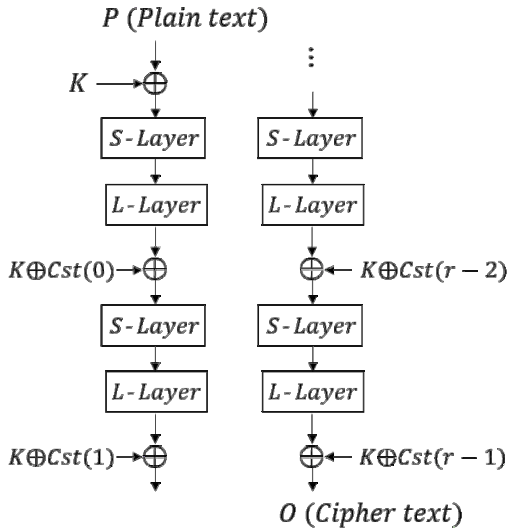

Fig. 1. Encryption process of LS-designs

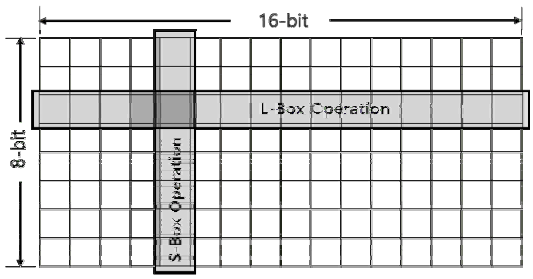

Fig. 2. S-Box and L-Box operation of Fantomas and Robin

적용하며, L-Layer는 각 행 L-Box를 행렬 곱한다. 따라서 128비트 암호문을 가지는 Fantomas와 Robin의 경우 각 라운드마다 총 16번의 S-Box 연산과 8번의 L-Box 연산이 시행된다. Fantomas와 Robin에서 사용하는 L-Box는 Fig. 3과 같이 정의되어 있으며, S-Box는 비트슬라이스 연산과정으로 정의되어 있다.

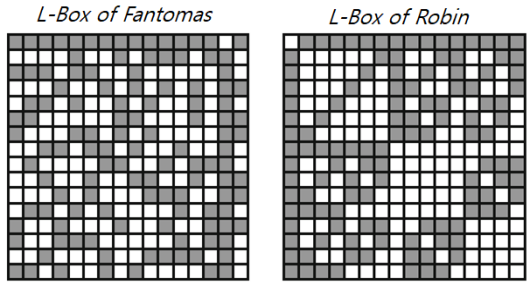

Fig. 3. L-Boxs of Fantomas and Robin (□: 0, ■: 1)

III. Fantomas와 Robin의 연관키 차분경로

LS-designs는 마스터키에 상수를 XOR한 값을 라운드키로 사용하기 때문에, 연관키 차분공격에서 매 라운드키에 같은 차분 값을 줄 수 있다. 이를 이용하여 한 라운드 단위로 반복되는 연관키 차분경로를 Fig. 4와 같이 만들 수 있다. A_i, B_i, C_i는 각각 i 라운드의 S-Layer 입력, S-Layer의 출력, L-Layer의 출력 값을 나타낸다($0 \leq i < r$).

Fig. 4와 같이 한 라운드 단위로 반복되는 연관키 차분경로의 확률은 A_i의 차분인 $\alpha \oplus \beta$가 S-Layer를 통과한 뒤에 γ가 될 확률에 기반한다. 따라서 $\alpha \oplus \beta$를 A_i의 한 열의 차분으로 하고, 그 중

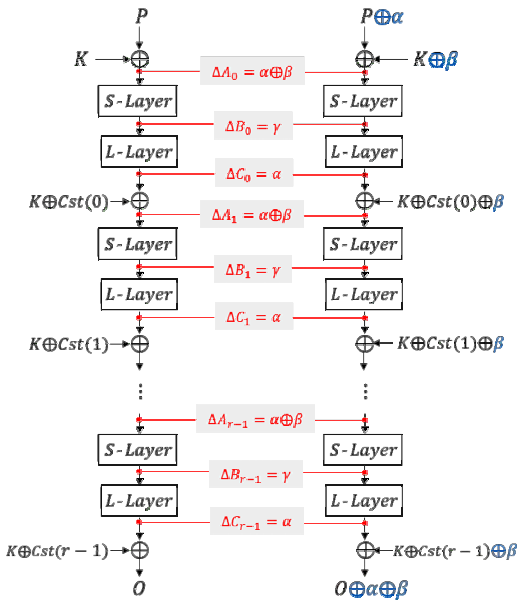

Fig. 4. Related-key differential path of LS-designs

가장 높은 확률의 S-Box 차분경로를 찾는 것이 전체 라운드 차분경로의 확률을 높이는데 중요하다.

Fantomas와 Robin에서 사용하는 S-Box의 차분분포표(Differential Distribution Table, DDT)를 분석한 결과, 두 경우 모두 2^{-4} 확률을 가지는 차분경로가 존재하였다. 실제로 Fantomas의 S-Box는 $0x04$ 차분을 가진 바이트 쌍이 입력되었을 때, 출력으로 $0xc1$차분의 바이트 쌍이 출력될 확률이 2^{-4}이다. 이를 이용한 Fantomas의 한 라운드 반복 연관키 차분경로의 예시를 Fig. 5에 제시한다. Fig. 5에 표현된 셀들은 각각 한 개의 셀이 한 개 비트의 차분 상태를 나타내며, 비어있으면 차분이 0, 명암이 있는 셀은 차분이 1임을 뜻한다.

Fig. 5는 LS-designs의 각 라운드에서 차분이 S-Layer, L-Layer에 의해 어떻게 확산되며, Key-XOR에서 어떻게 상쇄되는지 잘 보여주고 있다. 예시로서는 $\alpha \oplus \beta$ 차분이 첫 번째 열에 있는 경우를 나타내었지만, 16개의 열 중 어떤 열에도 적용이 가능하다. Robin 또한 이와 같은 방법으로 2^{-4} 확률의 한 라운드 반복 연관키 차분경로를 구할 수 있다. 따라서 전체 라운드 연관키 차분경로의 확률은 각각 Fantomas, Robin에 대해서 각각 $(2^{-4})^{12} = 2^{-48}$, $(2^{-4})^{16} = 2^{-64}$임을 알 수 있다.

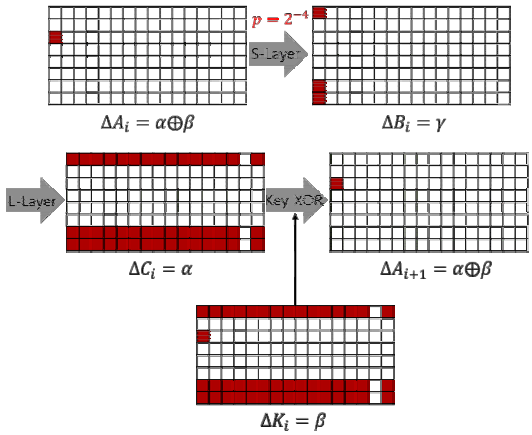

Fig. 5. Example of related-key one-round iterative differential path of Fantomas
(□: zero difference, ■: non-zero difference)

IV. Fantomas와 Robin에 대한 키 복구 공격

L-Layer는 선형연산이므로, Fantomas의 마지막 라운드의 차분경로는 Fig. 6와 같이 생각해 볼 수 있다. 이때 $B_{11} = L^{-1}(O) \oplus L^{-1}(K \oplus Cst(11))$ 이며, 이 중 $L^{-1}(O)$는 공격자가 계산해 낼 수 있으므로, $L^{-1}(K \oplus Cst(11))$의 실제 값을 정확히 예측한다면 정확한 B_{11}의 값이 복구된다. Fig. 6의 $\triangle A_{11} = \alpha \oplus \beta$는 한 바이트 차분으로, 만약 B_{11}의 같은 위치의 바이트를 정확히 추측하여 S-Box의 역함수를 계산한다면, $\alpha \oplus \beta$ 차분이 복구 될 것이다.

예를 들어, Fig. 5의 연관키 차분경로를 이용한 공격 시에는 $L^{-1}(K \oplus Cst(11))$의 첫 번째 열에 해당하는 값을 추측한다. 만약 옳은 값을 추측하였다면 Fig. 5의 B_{11}와 $B_{11} \oplus \gamma$가 S-Box 역함수를 통과하였을 때 $\triangle A_{11} = \alpha \oplus \beta$를 만족한다. 이때, 2^{-4}의 확률을 가지는 차분경로를 사용하였으므로 2^4개의

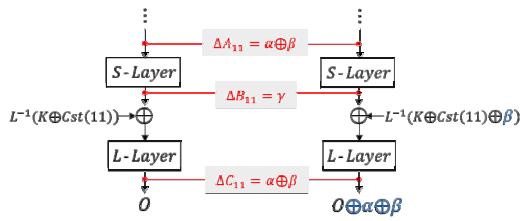

Fig. 6. Modified related-key differential path of the last round of Fantomas

$L^{-1}(K \oplus Cst(11))$의 첫 번째 열 후보를 얻을 수 있다. 이 과정을 차분경로를 만족시키는 평문, 키 쌍 두 개에 대해서 각각 수행하면 $L^{-1}(K \oplus Cst(11))$의 첫 번째 열 후보의 개수를 줄일 수 있다.

$L^{-1}(K \oplus Cst(11))$의 한 열에 해당하는 바이트를 복구해 냈다면, $\alpha \oplus \beta$를 다른 열에 해당하는 바이트로 바꾸어, 새로운 연관키 차분경로를 이용해 같은 과정을 반복한다. 총 16번 시행을 통해 $L^{-1}(K \oplus Cst(11))$의 모든 비트를 복구할 수 있으며, 최종적으로 마스터키 K를 복구할 수 있다.

본 키 복구 공격은 $L^{-1}(K \oplus Cst(11))$의 각 바이트를 복구하는데 연관키 차분경로를 만족시키는 평문, 키 쌍이 최소 두 개 필요하다. Fantomas의 연관키 차분경로의 확률이 2^{-48}임은 3장에서 논의된 바 있다. 따라서 2^{51}개의 차분경로를 테스트한다면 (2^{52}개의 평문, 키 쌍) 아래와 같은 확률로 Fantomas의 연관키 차분경로를 만족하는 평문, 키 쌍을 2개 이상 얻을 수 있다.

$$\sum_{i=2}^{2^{51}} \binom{2^{2^{51}}}{i} \times (1-2^{-48})^{2^{51}-i} \times (2^{-48})^{i} \approx 0.963$$

따라서, 마스터키의 모든 비트를 복구하기 위해서는 2^{52}개의 선택 평문과 총 $(2^{52}+2^{8}) \times 16 \approx 2^{56}$의 시간복잡도가 필요하며 성공확률은 $0.963^{16} \approx 0.547$이다. Robin의 경우에도 Fantomas 공격법과 같은 방법으로 공격이 가능하지만, 연관키 차분경로의 확률이 2^{-64}이므로 $(2^{68}+2^{8}) \times 16 \approx 2^{72}$의 시간복잡도와 2^{68}개의 선택 평문이 필요하며 성공확률은 0.547이다.

V. 결 론

[3]에서는 LS-designs가 연관키 및 선택키 차분 공격에 대한 안전성을 고려하지 않은 구조임을 밝혔다. 하지만 보안 프로토콜 설계자는 블록암호 기반 해시함수와 같이 연관키 및 선택키 차분 공격을 가정할 수 있는 환경에 LS-designs 구조의 블록암호를 사용할 수 있다. 따라서 본 논문은 객관적인 분석을 통해 연관키 차분 공격에 대한 LS-designs의 안전성을 제시하여 실제 사용자가 필요로 하는 암호학적 안전성을 만족하는지 판단 할 수 있게 하는데 의미를 가진다.

[3]에서는 연관키 공격 가정에서 라운드당 한 개의 active S-Box를 가지는 간단한 차분경로가 존재 할 것임을 언급하였지만 실제 연관키 차분 경로를 제시하지는 않았다. 또한 SEM 스킴으로서의 일반적인 연관키 혹은 선택키 차분 공격이 전체 라운드에 적용이 가능할 수 있음을 언급하였지만 본 논문의 4장에서 소개하는 키 복구 공격과 같이 객관적인 방법론을 제시하지는 않았다. 따라서 본 논문은 LS-designs으로 설계된 블록암호에 대해 연관키 차분 경로를 이용한 키 복구 공격을 실질적인 방법론적으로 보이고 그 공격복잡도를 측정했다는 의미가 있다.

본 논문을 통해 Fantomas와 Robin은 연관키 공격을 통한 마스터키 복구가 2^{56}과 2^{72}의 연산량으로 가능함을 알 수 있다. 이러한 암호학적 취약성은 LS-design의 라운드키가 마스터키의 상수 XOR로 만들어진다는 점에 기인한다. 설계자는 경량암호를 설계하기 위하여 키 스케줄을 최소화하는 방법을 택하였지만, 이로 인해 연관키 공격에 취약점이 생긴 것을 알 수 있다. NIST에서도 경량 블록암호가 연관키 공격에 내성을 지니는 것을 권장하는바[6], 향후 설계되는 경량암호는 연관키 공격을 염두하고 키 스케줄을 설계해야 할 것이다.

References

[1] Gilles Piret, Thomas Roche, Claude Carlet, "PICARO - a block cipher allowing efficient higherorder side-channel resistance", *ACNS 2012,* LNCS 7341, pp. 311 - 328, Springer, 2012.

[2] Benoît Gérard, Vincent Grosso, María Naya-Plasencia, François-Xavier Standaert, "Block Ciphers that are Easier to Mask: How Far Can we Go?", *CHES 2013,* LNCS 8086, pp. 383-399, Springer, 2013.

[3] Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, and Kerem Varici, "LS-designes: Bitslice encryption for efficient masked software implementations" *FSE 2014*, LNCS 8540,

pp. 18-37, Springer, 2014.
〔4〕 Eli Biham, "New Types of Cryptanalytic Attacks Using Related Keys" *Journal of Cryptology,* Vol. 7, No. 4, pp. 229-246, 1994.
〔5〕 Lars R. Knudsen, "Cryptanalysis of LOKI91", *AUSCRYPT 1992,* LNCS 718, pp. 196-208, Springer, 1993.
〔6〕 Kerry A. McKay, Lawrence E. Bassham, Meltem Sonmez Turan, Nicky W. Mouha, "Report on Lightweight Cryptography", NIST, 2016.

〈저자소개〉

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