한국항행학회 논문지 제15권 제5호 2011년 10월

무선 센서 네트워크 환경에 적합한 블록 암호 MD-64에 대한 안전성 분석

Security Analysis of Block Cipher MD-64 Suitable for Wireless Sensor Network Environments

이창훈*

Chang-Hoon Lee*

요 약

64-비트 블록 암호 MD-64는 WSN과 같은 환경에서 효율적으로 구현이 가능하도록 설계된 블록 암호이다. 본 논문에서는 MD-64의 전체 라운드에 대한 확장된 연관키 부메랑 공격을 제안한다. 본 논문에서 소개하는 공격은 MD-64에 대한 첫 번째 공격이며, $2^{45.5}$개의 연관키 선택 평문을 이용하여 2^{95}의 MD-64 암호화 연산을 수행하여 MD-64의 비밀키를 복구한다.

Abstract

MD-64 is a 64-bit block cipher suitable for the efficient implementation in hardware environments such as WSN. In this paper, we propose a related-key amplified boomerang attack on the full-round MD-64. The attack on the full-round MD-64 requires $2^{45.5}$ related-key chosen plaintexts and 2^{95} MD-64 encryptions. This work is the first known cryptanalytic result on MD-64.

Key words : Block Cipher, MD-64, Crypt Analysis

Ⅰ. 서 론

최근 하드웨어 환경에서 효율적으로 구현이 가능한 DDP(Data Dependent Permutation)-기반 블록 암호에 대한 연구가 활발히 진행되고 있고, 그 결과로서 SPECTR-H64 [1], CIKS-family (CIKS-1 [2], CIKS-128 [3]), Cobra-family (Cobra-S128 [4], Cobra-F64a [4], Cobra-F64b [4], Cobra-H64 [5], Cobra-H128 [5]), Eagle-64 [6] Eagle-128 [7], SCO-family [8] 등이 제안되었다. 이 알고리즘들은 매우 단순한 키 스케줄을 사용하기 때문에, 비밀키가 빈번하게 변경되는 환경에 적용될 경우 높은 효율성을 갖는다. 그러나 DDP의 선형성과 단순하게 설계된 키스케줄 때문에 대부분의 알고리즘들이 분석되었다 [9-17].

64-비트 블록 암호 MD-64 [18]는 위에서 언급한 DDP-기반 블록 암호와 유사한 설계 논리를 가지며, WSN (Wireless Sensor Network)과 같이 자원이 제한된 환경에서 효율적으로 동작하도록 설계되었다. 하지만, 본 논문에서는 전체 라운드 MD4에 대한 확장된 연관키 부메랑 공격을 제안함으로서, 기제안된

* 한신대학교 컴퓨터공학부(School of Computer Engineering, Hanshin University)
· 제1저자 (First Author) : 이창훈
· 투고일자 : 2011년 9월 28일
· 심사(수정)일자 : 2011년 9월 28일 (수정일자 : 2011년 10월 24일)
· 게재일자 : 2011년 10월 30일

DDP-기반 블록 암호와 마찬가지로 MD-64도 여전히 연관키 공격에 취약함을 보인다. 본 논문에서 제안하는 공격은 $2^{45.5}$개의 연관키 선택 평문을 이용하여 2^{95}의 MD-64 암호화 연산을 수행하여 MD-64의 128-비트 비밀키를 복구한다. 본 논문에서 소개하는 공격은 MD-64에 대한 첫 번째 공격이다.

본 논문의 구성은 다음과 같다. 2장에서는 블록 암호 MD-64를 간략히 소개하고, 3장에서는 MD-64에 대한 확장된 연관키 부메랑 공격을 소개한다. 마지막으로 4장에서 결론을 맺는다.

Ⅱ. 블록 암호 MD-64 소개

본 장에서는 64-비트 블록 암호 MD-64를 소개한다. 이에 앞서, 본 논문에서는 다음과 같은 표기를 사용한다. 비트 표기는 왼쪽에서 오른쪽으로 1부터 표기된다. 예를 들어, $P=(p_1,p_2,\cdots,p_n)$이면 P의 최상위 비트는 p_1이고, P의 최하위 비트는 p_n이다. 그리고 e_i는 i번째 비트만 1이고, 나머지 비트는 0인 이진 수열을 의미한다. 예를 들어, $e_1=(1,0,\cdots,0)$이다.

블록 암호 MD-64는 128-비트 비밀키 $K=(K_1, K_2, K_3, K_4)$를 사용하는 64-비트 블록 암호로서 라운드 수는 8이다. MD-64의 라운드 함수인 $Crypt^{(e)}$는 그림 1과 같다. 여기서 $e=0(1)$은 암호화(복호화) 과정을 의미한다. 표 1은 MD-64의 8-라운드 암호화 과정$(e=0)$을 나타낸 것이다.

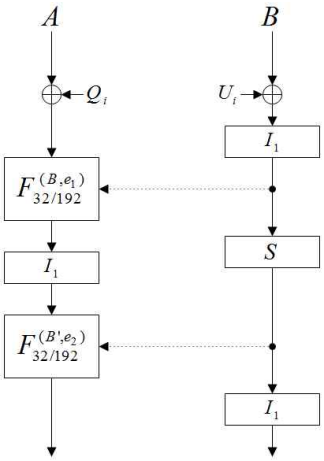

그림 1. 라운드 함수 $Crypt^{(e)}$
Fig. 1. Round function $Crypt^{(e)}$

표 1. MD-64의 암호화 과정
Table 1. The encryption process of MD-64.

1. A 64-bit input block P is divided into two 32-bit subblocks A and B.
2. For $i=1$ to 7 do:
   $(A,B)\leftarrow Crypt^{(0)}(A,B,Q_i,U_i)$;
   $(A,B)\leftarrow(B,A)$;
3. Perform transformation:
   $(A,B)\leftarrow Crypt^{(0)}(A,B,Q_8,U_8)$;
4. Perform final transformation:
   $(A,B)\leftarrow(A\oplus Q_9, B\oplus U_9)$;

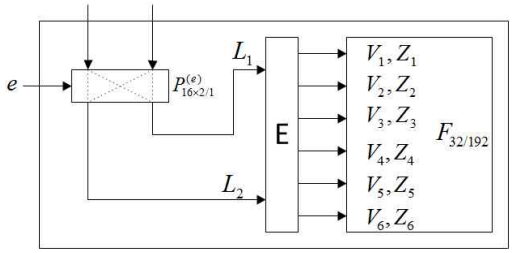

그림 2. $F_{32/192}^{(B,e)}$
Fig. 2. $F_{32/192}^{(B,e)}$

그림 2와 같이, $F_{32/192}^{(B,e_1)}$와 $F_{32/192}^{(B',e_2)}$는 $P_{16\times2/1}^{(e)}$와 $F_{32/192}$를 이용하여 구성된다. $P_{16\times2/1}^{(e)}$는 1-비트 값 e에 따라 다음과 같이 정의된다.

- $P_{16\times2/1}^{(0)}(x_1,x_2)=(x_1,x_2)$.
- $P_{16\times2/1}^{(1)}(x_1,x_2)=(x_2,x_1)$.

32-비트 입력값 (L_1,L_2)에 대해 extension box E의 출력값 $(V_1,\cdots,V_6,Z_1,\cdots,Z_6)$은 다음과 같이 계산된다.

$V_1=L_1$	$V_2=L_1^{\lll 4}$	$V_3=L_1^{\lll 8}$
$V_4=L_2^{\lll 8}$	$V_5=L_2^{\lll 4}$	$V_6=L_2$
$Z_1=L_1^{\lll 6}$	$Z_2=L_1^{\lll 12}$	$Z_3=L_1$
$Z_4=L_2$	$Z_5=L_2^{\lll 12}$	$Z_6=L_2^{\lll 6}$

그림 3과 같이, $F_{32/192}$는 다음과 같이 정의되는 $F_{2/2}$를 결합하여 구성된다.

$$F_{2/2}(x_1,x_2,v,z)=(y_1,y_2)$$
$$y_1=vz(x_1\oplus x_2)\oplus v\oplus z(x_1\oplus 1)\oplus x_1\oplus x_2.$$
$$y_2=vzx_2\oplus z(x_1\oplus x_2\oplus 1)\oplus x_2.$$

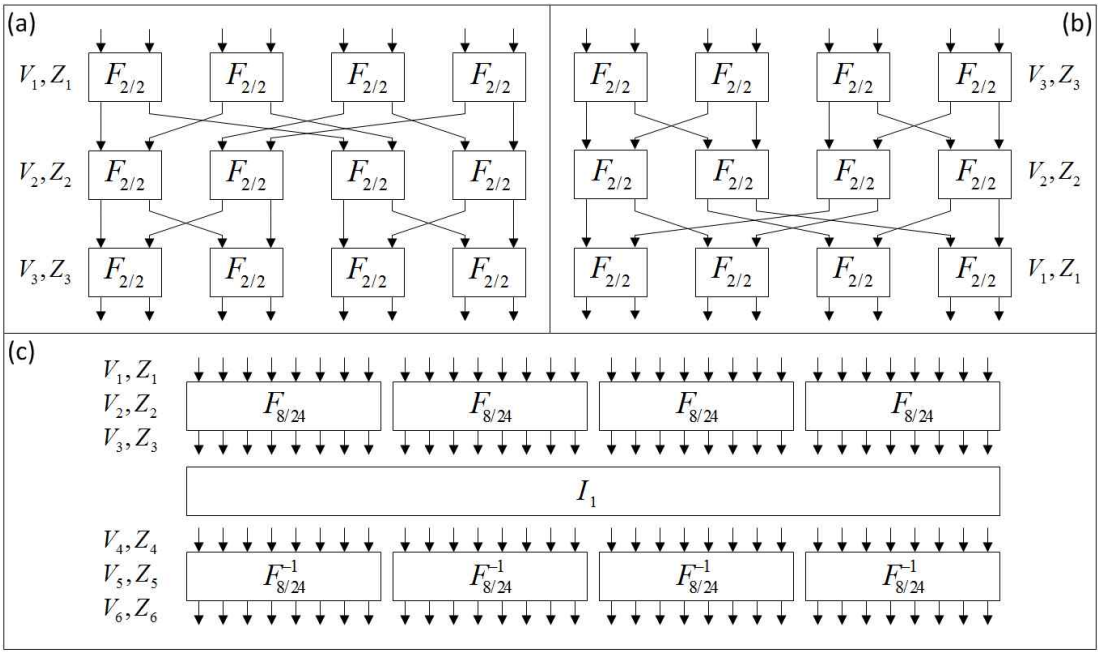

그림 3. (a) $F_{8/24}$ (b) $F_{8/24}^{-1}$ (c) $F_{32/192}$
Fig. 3. (a) $F_{8/24}$ (b) $F_{8/24}^{-1}$ (c) $F_{32/192}$

그림 3에서 알 수 있듯이, $F_{32/192}$와 역함수인 $F_{32/192}^{-1}$은 $F_{2/2}$에 대한 제어 비트의 입력 순서만 다르고 나머지는 동일하다. 여기서 $F_{32/192}$과 $Crypt^{(e)}$에 사용되는 치환 함수 I_1은 다음과 같다.

$$I_1 = (1)(2,9)(3,17)(4,25)(5)(6,13)(7,21)(8,29)(10)(11,18)(12,26)(14)(15,22)(16,30)(19)(20,27)(23)(24,31)(28)(32).$$

$Crypt^{(e)}$에 사용되는 함수 S는 8개의 4×4 S-box로 구성되어 있는데, 구체적인 구조는 [18]을 참조하라.

마지막으로, MD-64의 키 스케줄은 매우 단순하다. 128-비트 비밀키 $K=(K_1,K_2,K_3,K_4)$가 바로 $Crypt^{(e)}$에 사용된다. 표 2는 MD-64의 라운드 키와 매개변수 $e'(=e_1\oplus e)$, $e''(=e_2\oplus e)$을 나타낸 것이다.

표 2. MD-64의 라운드 키와 매개변수 e', e''
Table 2. The round keys of MD-64 and the parameters e', e''.

Round r	Q_r	U_r	e'	e''
1	K_1	K_3	1	0
2	K_2	K_3	0	0
3	K_3	K_2	1	1
4	K_4	K_1	1	0
5	K_4	K_4	0	1
6	K_1	K_4	1	1
7	K_2	K_3	0	0
8	K_3	K_2	0	1
FT	K_1	K_3	·	·

Ⅲ. MD-64에 대한 확장된 연관키 부메랑 공격

본 장에서는 MD-64에 대한 확장된 연관키 부메랑 공격을 제안한다.

평문 P, P^*, P', P'^*를 비밀키 K, K^*, K', K'^*로 각각 암호화한다고 가정한다. 이때 각각의 평문과 비밀키는 다음 조건을 만족한다.

- $\alpha = P\oplus P^* = P'\oplus P'^* = (e_1,0)$.

- $\Delta K = K \oplus K^* = K' \oplus K'^* = (e_1,0,0,0)$.
- $\Delta K' = K \oplus K' = K^* \oplus K'^* = (0,e_1,0,0)$.

그러면 표 3과 같이, 라운드 $1 \sim 2$에 대한 확률 1의 2-라운드 연관키 차분 특성 $\alpha \rightarrow \beta = (0,0)$을 구성할 수 있다. 그림 4-(a)는 라운드 1의 차분 특성을 나타낸 것이다.

표 3. MD-64에 대한 두 개의 연관키 차분 특성
Table 3. Two related-key differential characteristics of MD-64.

Round r	ΔI_r	$(\Delta Q_r, \Delta U_r)$	확률
1	$(e_1,0) = \alpha$	$(e_1,0)$	1
2	$(0,0)$	$(0,0)$	1
Output	$(0,0) = \beta$	·	·
3	$(0,e_1) = \gamma$	$(0,e_1)$	1
4	$(0,0)$	$(0,0)$	1
5	$(0,0)$	$(0,0)$	1
6	$(0,0)$	$(0,0)$	1
7	$(0,0)$	$(e_1,0)$	2^{-12}
8	$(0,e_1)$	$(0,e_1)$	1
FT	$(0,0)$	$(0,0)$	1
Output	$(0,0)$	·	·

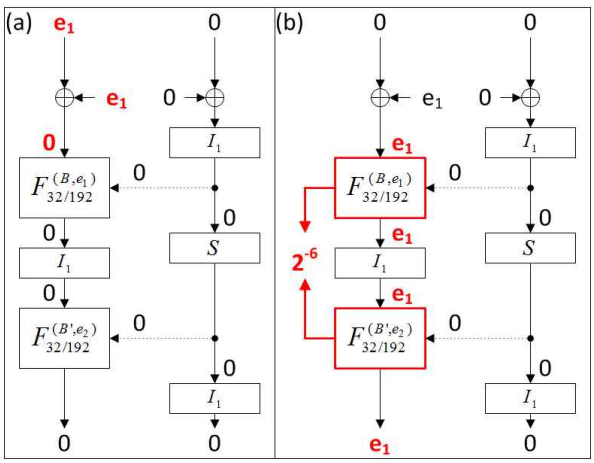

그림 4. (a) 라운드 1 (b) 라운드 7의 차분 특성
Fig. 4. Differential characteristics of (a) round 1 (b) round 7

이와 유사하게 라운드 $3 \sim 8$에 대한 6-라운드 연관키 차분 특성도 구성할 수 있다. 중간 상태값 I, I^*, I', I'^*를 비밀키 K, K^*, K', K'^*로 각각 암호화한다고 가정한다. 이때 각각의 중간값은 다음 조건을 만족한다: $\gamma = I \oplus I' = I^* \oplus I'^* = (0,e_1)$. 그러면 표 3과 같이, 라운드 $3 \sim 8$에 대한 확률 2^{-12}의 6-라운드 연관키 차분 특성 $\gamma \rightarrow \delta = (0,0)$를 구성할 수 있다. 그림 4-(b)는 라운드 7의 차분 특성을 나타낸 것이다. 먼저, $F_{2/2}$는 다음과 같은 특성을 만족한다.

- $\Pr[F_{2/2}(x_1,x_2,v,z) \oplus F_{2/2}(x_1 \oplus 1,x_2,v,z) = (1,0)] = 2^{-1}$.

이를 이용하여 $F_{32/192}^{(B,e_1)}$와 $F_{32/192}^{(B',e_2)}$는 다음을 만족함을 쉽게 알 수 있다.

$$\Pr\left[F_{32/192}^{B,e_1}(X) \oplus F_{32/192}^{B,e_1}(X \oplus e_1)\right] = 2^{-6}.$$

$$\Pr\left[F_{32/192}^{B',e_2}(X) \oplus F_{32/192}^{B',e_1}(X \oplus e_1)\right] = 2^{-6}.$$

따라서 라운드 7에 대한 확률 2^{-12}의 연관키 차분 특성 $(0,0) \rightarrow (e_1,0)$을 구성할 수 있다.

8-라운드 확장된 연관키 부메랑 차분 특성을 이용하여 전체 라운드 MD-64에 대한 확장된 연관키 부메랑 공격을 수행한다. MD-64가 $\Delta K = K \oplus K^* = K' \oplus K'^* = (e_1,0,0,0)$, $\Delta K' = K \oplus K' = K^* \oplus K'^* = (0,e_1,0,0)$을 만족하는 비밀키 K와 연관키 K^*, K', K'^*를 사용한다고 가정할 때, 전체 라운드 MD-64에 대한 확장된 연관키 부메랑 공격은 다음과 같은 과정을 수행한다.

차분 $\alpha = (e_1,0)$을 만족하는 $2^{44.5}$개의 평문 쌍 (P_j, P_j^*)를 선택한다 $(j = 1,\cdots,2^{44.5})$. 이를 이용하여 2^{88}개의 평문 quartet $(P_i, P_i^*, P_i', P_i'^*)$를 구성한 후, 비밀키 K와 연관키 K^*, K', K'^*로 각각 암호화하여 대응되는 암호문 quartet $(C_i, C_i^*, C_i', C_i'^*)$를 계산하고 테이블에 저장한다.

각각의 i에 대해, $C_i \oplus C_i' = C_i^* \oplus C_i'^* = (0,0)$을 만족하는지 체크하고 이를 만족하는 암호문 quartet에 대해 단계 3을 수행한다.

96-비트 부분키 (K_1,K_2,K_3)을 추측한 후, 다음을 수행한다.

추측한 (K_1,K_2,K_3)을 이용하여 (K_1^*, K_2^*, K_3^*), (K_1', K_2', K_3'), $(K_1'^*, K_2'^*, K_3'^*)$를 계산한다.

추측한 부분키 quartet을 이용하여 라운드 7의 입력값을 각각 계산한다. 이 64-비트 값을 $(T_i, T_i^*, T_i', T_i'^*)$라 할 때, 각각의 i에 대해 $T_i \oplus T_i' = T_i^* \oplus T_i'^* = (0,0)$을 만족하는지 검사한다. 이를 만

족하는 부분키 quartet에 대해, 단계 4를 수행한다.

단계 3을 통과한 부분키 quartet에 대해, 나머지 32-비트 부분키 K_4를 전수조사하고 1개의 평문/암호문 쌍을 이용하여 검사한다. 이를 만족하는 128-비트 비밀키를 MD-64의 옳은 128-비트 비밀키로 출력하고 연관키 K^*, K', K'^*도 출력한다. 그렇지 않으면 단계 3으로 간다.

이 공격을 수행하기 위해 $2^{44.5}$개의 선택 평문 쌍이 필요하므로 이 공격의 데이터 복잡도는 $2^{45.5}$개의 연관키 선택 평문이다. 그리고 이 공격에 필요한 메모리는 $2^{48.5}(=2^{44.5}\cdot 2\cdot 8)$ 메모리 바이트이다.

단계 1의 계산 복잡도는 $2^{45.5}$ MD-64 암호화 연산이다. 각각의 암호문 quartet이 단계 2를 통과할 확률은 $2^{-128}(=(2^{-64})^2)$이다. 그래서 단계 2를 통과할 틀린 quartet의 개수의 기댓값은 $2^{-40}(=2^{88}\cdot 2^{-128})$이다. 이는 옳은 quartet만이 단계 2를 통과함을 의미한다. 단계 3의 계산 복잡도는 평균 $2^{95}(=2^{96}\cdot 4\cdot \frac{2}{8}\cdot \frac{1}{2})$ MD-64 암호화 연산이다. 틀린 부분키 quartet이 단계 3을 통과할 확률은 $2^{-128}(=(2^{-64})^2)$이다. 그래서 옳은 부분키 quartet만이 단계 3을 통과한다. 단계 4의 계산 복잡도는 2^{32} MD-64 암호화 연산이다. 그러므로 이 공격 알고리즘의 계산 복잡도는 약 2^{95} MD-64 암호화 연산이다 $(2^{95}(\approx 2^{45.5}+2^{95}+2^{32}))$.

한편, 각각의 128-비트 틀린 비밀키가 단계 4를 통과할 확률은 2^{-64}이므로, $2^{-32}(=2^{32}\cdot 2^{-64})$개의 틀린 비밀키가 단계 4를 통과한다. 이는 본 논문에서 제안하는 공격 알고리즘이 틀린 비밀키 quartet을 출력할 확률이 매우 낮음을 의미한다. 그러므로 본 논문에서 제안하는 확장된 연관키 부메랑 공격은 MD-64의 128-비트 비밀키를 복구할 수 있다.

Ⅳ. 결 론

본 논문에서는 확장된 연관키 부메랑 공격을 이용하여 64-비트 블록 암호 MD-64에 대한 첫 번째 안전성 분석 결과를 제안하였다. 본 논문에서 소개한 공격은 전수보다 효율적인 2^{95}의 계산 복잡도를 필요로 한다. 이는 MD-64가 기제안된 DDP-기반 블록 암호와 마찬가지로 연관키 공격에 매우 취약함을 의미한다.

감사의 글

본 논문은 한신대학교 학술연구비 지원에 의하여 연구되었음.

참 고 문 헌

[1] N. Goots, A. Moldovyan, N. Moldovyan, “Fast Encryption Algorithm Spectr-H64”, *MMM- ACNS'01, LNCS 2052*, pp. 275-286, Springer- Verlag, 2001.

[2] A. Moldovyan and N. Moldovyan, “A cipher Based on Data-Dependent Permutations”, *Journal of Cryptology,* Vol.15, No.1, pp. 61-72, 2002.

[3] N. Goots, B. Izotov, A. Moldovyan and N. Moldovyan, “Modern cryptography: Protect Your Data with Fast Block Ciphers”, *Wayne, A-LIST Publish.*, 2003.

[4] N. Goots, N. Moldovyan, P. Moldovyanu and D. Summerville, “Fast DDP-Based Ciphers: From Hardware to Software”, *46th IEEE Midwest International Symposium on Circuits and Systems*, 2003.

[5] N. Sklavos, N. Moldovyan and O. Koufopavlou, “High Speed Networking Security: Design and Implementation of Two New DDP-Based Ciphers”, *Mobile Networks and Applications-MONET, Kluwer Academic Publishers*, Vol.25, Issue 1-2, pp. 219-231, 2005.

[6] N, Moldovyan, A. Moldovyan, M. Eremeev and D. Summerville, “Wireless Networks Security and Cipher Design Based on Data-Dependent Operations: Classification of the FPGA Suitable Controlled Elements”, *CCCT'04, Vol.VII,* pp. 123-128, Texas, USA, 2004.

[7] N. Moldovyan, A. Moldovyan, M. Eremeev and N.

Sklavos, “New Class of Cryptographic Primitives and Cipher Design for Networks Security”, *International Journal of Network Security,* Vol.2, No.2, pp. 114-225, 2006.

[8] N. Moldovyan, “On Cipher Design Based on Switchable Controlled Operations”, *MMM- ACNS'03, LNCS 2776,* pp. 316-327, Springer- Verlag, 2003.

[9] Y. Ko, D. Hong, S. Hong, S. Lee and J. Lim, “Linear Cryptanalysis on SPECTR-H64 with Higher Order Differential Property”, *MMM-ACNS'03, LNCS 2776,* pp. 298-307, Springer- Verlag, 2003.

[10] Y. Ko, C. Lee, S. Hong and S. Lee, “Related Key Differential Cryptanalysis of Full-Round SPECTR-H64 and CIKS-1”, *ACISP'04, LNCS 3108*, pp. 137-148, Springer-Verlag, 2004.

[11] Y. Ko, C. Lee, S. Hong, J. Sung and S. Lee, “Related-Key Attacks on DDP based Ciphers: CIKS-128 and CIKS-128H”, *Indocrypt'04, LNCS 3348*, pp. 191-205, Springer-Verlag, 2004.

[12] C. Lee, D. Hong, S. Lee, S. Lee, H. Yang and J. Lim, “A Chosen Plaintext Linear Attack on Block Cipher CIKS-1”, *ICICS'02, LNCS 2513*, pp. 456-468, Springer-Verlag, 2002.

[13] C. Lee, J. Kim, S. Hong, J. Sung and S. Lee, “Related-Key Differential Attacks on Cobra- S128, Cobra-F64a, and Cobra-F64b”, *MYCRYPT'05, LNCS 3715,* pp. 245-263, Springer-Verlag, 2005.

[14] C. Lee, J. Kim, J. Sung, S. Hong and S. Lee, “Related-Key Differential Attacks on Cobra- H64 and Cobra-H128”, C*CC'05, LNCS 3796,* pp. 201-219, Springer-Verlag, 2005.

[15] J. Lu, C. Lee and J. Kim, “Related-Key Attacks on the Full-Round Cobra-F64a and Cobra-F64b”, *SCN'06, LNCS 4116,* pp. 95-110, Springer-Verlag, 2006.

[16] K. Jeong, C. Lee, J. Sung, S. Hong and J. Lim, “Related-Key Amplified Boomerang Attacks on the Full-Round Eagle-64 and Eagle-128”, *ACISP'07, LNCS 4586,* pp. 143-157, Springer-Verlag, 2007.

[17] K. Jeong, C. Lee, J. Kim and S. Hong, “Security analysis of the SCO-family using key schedules”, *Information Sciences*, Vol. 179, pp. 4232-4242, Elsevier, 2009.

[18] N. Minh, D. Bac and H. Duy, “New SDDO-Based Block Cipher for Wireless Sensor Network Security”, *IJCSNS,* Vol. 10, No. 3, pp. 54-60, 2010.

이 창 훈 (李昌勳)

2001년 2월 : 한양대학교 수학과 학사
2003년 2월 : 고려대학교 정보보호대학원 석사
2008년 2월 : 고려대학교 정보경영공학전문대학원 박사
2009년 3월~현재 : 한신대학교 컴퓨터공학부 조교수
관심분야 : 암호학, 디지털포렌식, 정보보호