Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.3, Jun. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.3.445

최신 경량 블록 암호 PRINCE에 대한 향상된 연관키 공격*

주 왕 호,† 안 현 정, 이 옥 연, 강 주 성, 김 종 성‡
국민대학교 금융정보보안학과

Improved Related-key Attack against Recent Lightweight Block Cipher PRINCE*

Wangho Ju,† Hyunjung An, Okyeon Yi, Ju-Sung Kang, Jongsung Kim‡
Department of Financial Information Security (BK21 Plus Future Financial Information Security Specialist Education Group), Kookmin University

요 약

블록 암호에 대한 안전성 평가시 연관키 공격은 중요한 분석툴로 간주된다. 이는 블록 암호에 대한 연관키 공격이 키를 컨트롤 할 수 있는 블록 암호기반 해쉬모드와 같은 응용환경에 강력하게 적용될 수 있기 때문이다. 본 논문에서는 FSE 2013에 제안된 경량 블록 암호 PRINCE에 대한 연관키 공격을 향상시킨다. 본 논문에서 제안하는 PRINCE에 대한 새로운 연관키 공격은 기존 가장 강력한 연관키 공격[4]의 데이터 복잡도를 2^{33}에서 2로 낮춘다.

ABSTRACT

The related-key attack is regarded as one of the important cryptanalytic tools for the security evaluation of block ciphers. This is due to the fact that this attack can be effectively applied to schemes like block-cipher based hash functions whose block-cipher keys can be controlled as their messages. In this paper, we improve the related-key attack on lightweight block cipher PRINCE proposed in FSE 2013. Our improved related-key attack on PRINCE reduces data complexity from 2^{33}[4] to 2.
Keywords: PRINCE, related-key attack, lightweight primitives.

I. 서 론

Asiacrypt 2012에서 제안된 경량 블록 암호 PRINCE[3]는 128-비트 비밀키를 사용하는 64-비트 블록 암호로써 하드웨어 구현에 적합하도록 설계되었다. FX 구조[2]로 되어있어서 암호화 프로세스의 키 변형을 통해 복호화를 수행할 수 있다. 이 특성을 α-reflection이라고 부르고, 이 특성은 암-복호화 구현에 효과적이다. 하지만, α-reflection 특성은 안전성 관점에서는 효과적이지 못하다. 이는 PRINCE 내에 강력한 연관키를 존재케 하는 성질을 제공하기 때문이다.

연관키 공격[1]은 블록 암호의 키를 컨트롤 할 수 있는 블록 암호기반 해쉬모드와 같은 응용환경에 대한 중요한 안전성 분석툴로 사용된다. 본 논문에서는 PRINCE의 α-reflection 특성을 사용한 강력한 새로운 연관키 공격에 대한 시나리오를 작성하고 그에

접수일(2013년 11월 18일), 게재확정일(2014년 4월 8일)
* 이 논문은 2013년도 정부(교육부)의 재원으로 한국연구재단의 (부분적인) 지원을 받아 수행된 기초연구사업임 (No. 2013R1A1A20598). 이 논문은 2014년도 BK21 플러스 사업에 의하여 (부분적으로) 지원되었음(No. 31Z20130012918).
† 주저자, nandars2@kookmin.ac.kr
‡ 교신저자, jskim@kookmin.ac.kr(Corresponding author)

대한 안전성 분석을 한다. FSE 2013에 제안된 기존 가장 강력한 연관키 공격[4]은 2^{33} 데이터 복잡도, 2^{64} 시간 복잡도, 2^{33} 메모리 복잡도를 가지고 있다. 본 논문에서는 2 데이터 복잡도, 2^{64} 시간 복잡도, 2 메모리 복잡도를 가지고 PRINCE의 128-비트 키 전체를 복구하는 향상된 연관키 공격을 제안한다. Table 1.은 기존 가장 강력한 연관키 공격과 본 논문에서 제안한 새로운 연관키 공격에 대한 공격 복잡도를 나타낸다.

본 논문은 다음과 같이 구성되어 있다. 2장에서 블록 암호 PRINCE에 대한 구조를 소개한다. 3장에서는 PRINCE에 대한 기존 연관키 공격을 소개하고 4장에서 PRINCE에 대한 향상된 새로운 연관키 공격을 소개한다. 마지막으로 5장은 본 논문에 대한 결론을 맺는다.

Table 1. Comparison of the previous FSE 2013 attack and ours on PRINCE

	FSE 2013[4]	This paper
Rounds	12 (full)	12 (full)
Data	2^{33}	2
Time	2^{64}	2^{64}
Memory	2^{33}	2

II. PRINCE

64-비트 경량 블록 암호 PRINCE[3]는 128-비트 비밀키 k를 사용한다. PRINCE에 대한 소개 및 공격 과정에서는 다음과 같은 표기법을 사용한다.

- P : 64-비트 평문
- C : 64-비트 암호문
- (k_0, k_1) : 128-비트 비밀키 k
- $\|$: 연접
- $\oplus$: 배타적 논리합
- $\gg$: 쉬프트
- $\ggg$: 로테이션

PRINCE는 간단한 키스케줄을 통해 128-비트 키 k를 가지고 192-비트 키 $(k_0 \| k_0' \| k_1)$를 생성한다. 키스케줄은 다음과 같다.

$$k = (k_0 \| k_1) \rightarrow (k_0 \| k_0' \| k_1) = (k_0 \| L(k_0) \| k_1)$$
$$\because L(x) = (x \ggg 1) \oplus (x \gg 63)$$

64-비트 서브키 k_0, k_0'는 입력 바로 직후와 출력 바로 전에 적용되고 k_1는 $PRINCE_{core}$ 내부에서 Fig.1.과 같이 적용된다. 이와 같은 구조를 FX구조[2]라 한다.

$$PRINCE((k_0.k_0'.k_1), x) = k_0' \oplus PRINCE_{core}(k_1, x \oplus k_0)$$

$PRINCE_{core}$는 SPN(Substitution-Permutation Network)구조이고 총 12 라운드로 이루어져 있다. 코어 함수 내부에서 사용되는 라운드 함수 R_i는 Fig.2.와 같다.

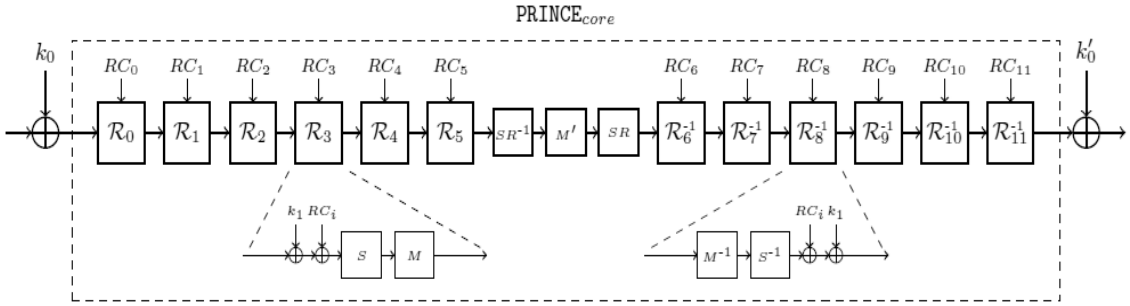

Fig.1. Description of the PRINCE encryption

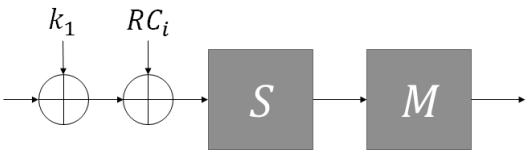

Fig.2. Description of the round function R_i

$PRINCE_{core}$의 암호화 과정은 6번의 R_i를 수행하고 선형 변환 $SR^{-1} \circ M' \circ SR$를 수행한 후, 마지막으로 6번의 R_i^{-1}를 수행한다. 여기서, SR는 4-비트 단위 쉬프트 함수이고 M'은 Involution 행렬이다. 라운드 함수 내부에서 사용되는 라운드 상수 RC_i에 대한 성질은 다음과 같다.

모든 $0 \le i \le 11$에 대해,
$RC_i \oplus RC_{11-i} = \alpha = 0xc0ac29b7c97c50dd.$

이 성질과 Involution 구조인 행렬 M'에 의하여 α-reflection[4]이라고 불리는 특성이 발생한다. 본 논문에서 제안하는 공격은 $PRINCE_{core}$를 구성하는 라운드 상수 RC_i의 값들과 S-box S, 쉬프트함수 SR, 그리고 행렬 M, M'에 구체적인 구성 성분에 대한 성질을 이용하지 않으므로 그들에 대한 설명을 생략하기로 한다. 본 논문에서 사용하는 핵심 특성인 α-reflection과 이 특성을 이용한 기존 연관키 공격 과정은 다음 장에서 소개한다.

III. FSE 2013에 제안된 PRINCE에 대한 연관키 공격[4]

α-reflection에 대한 개념을 소개하고 다음으로 이 특성을 이용한 기존 연관키 공격을 소개한다.

3.1 α-reflection 특성

$PRINCE_{core}$에서 사용되는 라운드 함수는 라운드 상수 RC_i의 값들을 고려하지 않는다면 $SR^{-1} \circ M' \circ SR$ 부분을 기준으로 왼쪽 과정과 오른쪽 과정이 대칭적으로 진행된다. 그리고 함수 내부에 사용되는 행렬 M'은 Involution 구조이므로 RC_i 값들의 차이를 고려하지 않는다면 전체적인 $PRINCE_{core}$의 암호화 과정과 복호화 과정이 정확히 같아진다. 이는 $PRINCE_{core}$에 대한 암호화 과정과 복호화 과정의 같은 위치에 있는 라운드 함수는 RC_i와 RC_{11-i}에 대한 고정된 차분 α 외의 차이점이 존재하지 않음을 의미한다. 이러한 차분 α는 연관키에 대한 차분으로 상쇄 시킬 수 있다. 즉, $k_1 \oplus RC_i = k_1 \oplus (RC_{11-i} \oplus \alpha) = (k_1 \oplus \alpha) \oplus RC_{11-i}$ 이므로 키 k_1와 연관키 $k_1 \oplus \alpha$에 대한 $PRINCE_{core}$의 암호화 과정과 복호화 과정이 정확히 같아진다. 이를 α-reflection이라 부른다. Fig.3.은 위와 같은 상황에 대한 중간 과정(라운드 5, 6)을 나타낸다.

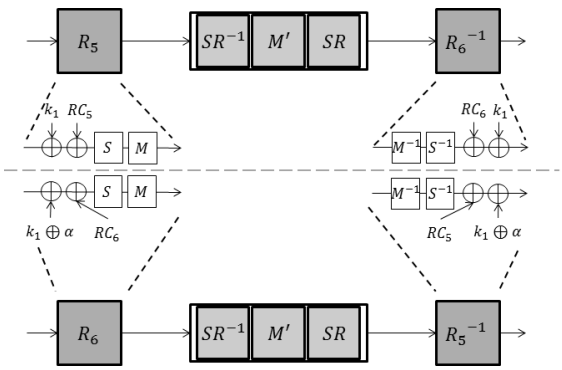

Fig.3. Intermediate step of $PRINCE_{core}(k_1, x)$ (above)
Intermediate step of $PRINCE_{core}^{-1}(k_1 \oplus \alpha, x)$ (below)

$$PRINCE_{core}(k_1, x) = PRINCE_{core}^{-1}(k_1 \oplus \alpha, x)$$

3.2 α-reflection 특성을 이용한 기존 연관키 공격

연관키 공격은 다음과 같은 성질을 이용한다. 비밀키 $k = (k_0, k_1)$와 연관키 $k' = (k_0, k_1 \oplus \alpha)$에 대한 PRINCE 알고리즘이 있고 k에 대한 임의의 평문-암호문 쌍을 (P, C)라고 하고, k'에 대한 임의의 평문-암호문 쌍을 (P', C')라고 하자.

만약 $P' \oplus C = k_0 \oplus L(k_0)$ 를 만족한다면, $P \oplus C' = k_0 \oplus L(k_0)$를 만족한다. 즉,

○ 연 관 키 : $k = (k_0, k_1)$
$k' = (k_0, k_1 \oplus \alpha)$

○ 정 보 : $C =$ PRINCE(P, k)
$C' =$PRINCE(P', k')
$P' \oplus C = x' \oplus y \oplus k_0 \oplus L(k_0)$
$P \oplus C' = x \oplus y' \oplus k_0 \oplus L(k_0)$
$(x, x', y, y'$은 Fig.4. 참조)

○ 성 질 : 만약 $P' \oplus C = k_0 \oplus L(k_0)$
$\Rightarrow x' = y$이고
$P \oplus C' = k_0 \oplus L(k_0)$이다.

위 성질은 α-reflection에 의해 발생한다. Fig.4.에서 $y = C \oplus L(k_0) \rightarrow C = y \oplus L(k_0)$이고 $x' = P' \oplus k_0 \rightarrow P' = x' \oplus k_0$임으로 $P' \oplus C = x' \oplus y \oplus k_0 \oplus L(k_0)$이다. 이와 같은 방법으로 $P \oplus C' = x \oplus y' \oplus k_0 \oplus L(k_0)$이 성립한다. 만약 $P' \oplus C = k_0 \oplus L(k_0)$을 만족한다면 $x' = y$가 성립하고 α-reflection에 의해 $x = y'$임으로 $P \oplus C' = k_0 \oplus L(k_0)$가 된다.

기존 연관키 공격은 키 k에 대한 2^{32}개의 평문-암호문 (P, C)쌍과 연관키 k'에 대한 2^{32}개의 평문-암호문 (P', C')쌍을 요구한다. 위의 두 평문-암호문 쌍들에 대해서 생일 역설에 의해 $x' = y$가 성립하는

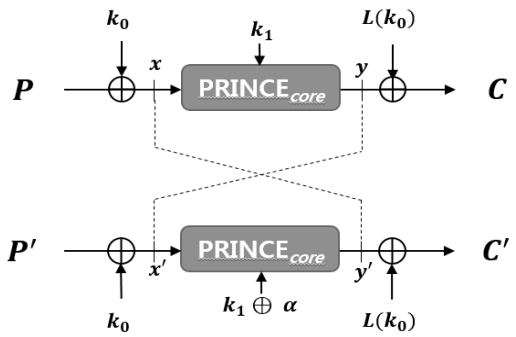

Fig.4. Existing related-key attack[4] using the α-reflection property

평문-암호문 쌍이 높은 확률로 존재한다. 이와 같은 쌍을 찾기 위해 $P \oplus C = P' \oplus C'$을 체크한다. 만약 $P \oplus C = P' \oplus C'$이면 $P' \oplus C = P \oplus C' = k_0 \oplus L(k_0)$를 만족하는지에 대한 추가적인 검사 후 64-비트 k_0를 복구한다. 마지막으로 64-비트 k_1에 대해서는 전수조사를 통해 획득한다. 본 연관키 공격은 2^{33} 데이터, 2^{64} 시간, 2^{33} 메모리 복잡도로 128-비트 키 k를 찾아낸다(자세한 공격 과정은 [4]를 참조).

IV. PRINCE에 대한 향상된 새로운 연관키 공격

본 논문이 제안하는 PRINCE에 대한 공격은 특정 연관키 차분 공격이다. 먼저 복구할 키에 대한 알고리즘에 하나의 선택된 평문 P를 입력하고 그에 대한 암호문 C를 취득한다. 다음으로 취득한 암호문 C를 평문으로 연관키에 대한 암호화 알고리즘에 입력한 후 그에 대한 암호문 C'을 취득한다. 해당 공격에서는 단 두 개의 평문-암호문 쌍을 취득하여 α-reflection 성질과 키 스케줄 특징을 사용하여 64-비트 키 k_0를 복구한다. 64-비트 키 k_1에 대해서는 전수조사를 시행한다. 결과적으로 128-비트 키 k를 복구하는데 64-비트 전수조사를 하여 찾아내는 공격이다.

4.1 공격 가정

공격자는 128-비트 키 k와 연관키 k'를 사용하는 두 개의 PRINCE 암호화 알고리즘을 가지고 있다. 공격자가 알고 있는 정보는 오직 연관키 사이의 관계뿐이다. 연관키는 다음의 관계를 갖는다.

$$\text{연관 관계} \begin{cases} k = (k_0, k_1) \\ k' = (L(k_0), k_1 \oplus \alpha) \end{cases}$$

4.2 공격 시나리오

1) 하나의 평문 P를 선택하고 k에 대한 P의 암호문 C를 획득한다.
2) 연관키 k'를 이용하여 C의 암호문 C'를 획득한다.
3) 현재 획득한 3가지 정보 P, C, C'에 대한 정보

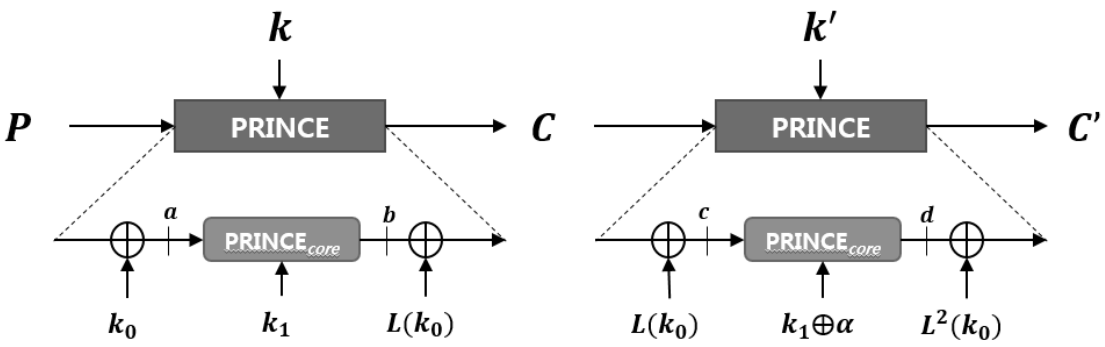

Fig.5. Configuration about Improved Related-key Attack against PRINCE

와 연관키 사이의 관계를 사용하여 64-비트 k_0를 획득한다.

4) k_0 획득 후, 64-비트 k_1에 대한 전수조사를 수행한다.

k_0를 획득하는 방법은 α-reflection 성질과 키스케줄에 사용되는 L 함수의 특징을 이용한다. 전체적인 공격 구성은 Fig.5.에 나와 있다. a, b, c, d는 중간 상태 값이다.

4.3 k_0, k_1 획득 과정

P 와 C'를 취득한 공격자는 추가적인 정보를 계산할 수 있다. 계산에 대한 원리를 설명하고, 다음으로 키 취득 과정을 설명한다.

4.3.1 k_0에 대한 정보 획득

Fig.5.에서 $b = C \oplus L(k_0) = c$ 이 성립하고 α-reflection 성질에 의해 $a = d$ 가 성립한다. 또, $P \oplus k_0 = a$, $C' \oplus L^2(k_0) = d$ 가 성립하므로 $P \oplus k_0 = C' \oplus L^2(k_0) \rightarrow P \oplus C' = k_0 \oplus L^2(k_0)$ 이다. 여기에서 $P \oplus C'$는 알고 있는 정보이고 L 함수는 알려진 로테이션 함수이므로 위의 두 정보와 L 함수의 특징을 사용하여 k_0를 획득할 수 있다.

L 함수의 규칙성을 이용하여 k_0를 찾아간다.

$$L(k_0) = (k_0 \ggg 1) \oplus (k_0 \gg 63)$$

x_i를 k_0의 i번째 비트라고 표기한다. 즉, $k_0 = (x_{63}, x_{62}, \cdots, x_1, x_0)$ 이다. 그러면,

$$\begin{aligned} &L^2(k_0) = L(L(k_0)) \\ &= L((x_0, x_{63}, \cdots, x_2, x_1) \oplus (0,0,\cdots,0,x_{63})) \\ &= L(x_0, x_{63}, \cdots, x_2, x_1 \oplus x_{63}) \\ &= (x_1 \oplus x_{63}, x_0, \cdots, x_2) \oplus (0,0,\cdots,0,x_0) \\ &= (x_1 \oplus x_{63}, x_0, x_{63}, \cdots, x_3, x_2 \oplus x_0) \end{aligned}$$

$$\begin{aligned} &\Rightarrow k_0 \oplus L^2(k_0) \\ &= (x_{63} \quad , x_{62}, x_{61}, \cdots, x_1, x_0 \quad) \oplus \\ &\quad (x_1 \oplus x_{63}, x_0 \, , x_{63}, \cdots, x_3, x_2 \oplus x_0) \\ &= (x_1, x_{62} \oplus x_0, x_{61} \oplus x_{63}, \cdots, x_2 \oplus x_4, x_1 \oplus x_3, x_2) \end{aligned}$$

이 성립한다.

$P \oplus C'$으로부터 x_1과 x_2를 획득할 수 있고, 나머지 정보에 대해서는 홀수 번호에 대한 비트는 x_1을 통하여, 짝수 번호에 대한 비트는 x_2를 통하여 알 수 있다. k_0의 비트열을 찾아가는 과정은 Fig.6.과 같다.

본 k_0 획득과정에 대한 시간 복잡도는 매우 작다.

본 k_0 획득 과정을 구현을 통하여 테스트 하였다. 테스트 환경은 운영체제 : Window 7 64비트, CPU : Intel(R) Core(TM) i7-2600 CPU @ 3.40GHZ, RAM : 4.00GB 이다. 테스트는 아래 과정을 모두 실행한 후의 소요된 clock 수를 측정하였다.

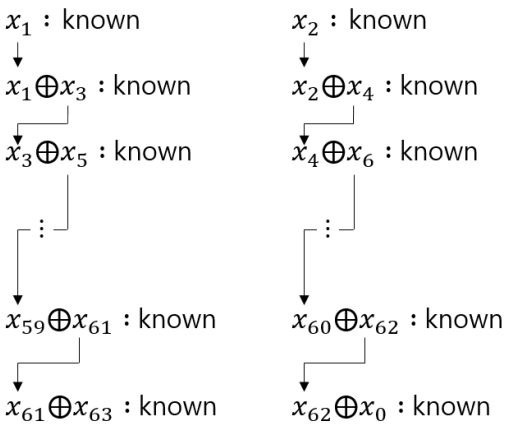

Fig.6. Our improved related-key attack on PRINCE

$$C = PRINCE(k_0 || k_1, P) \quad (1)$$

$$C' = PRINCE(L(k_0) || k_1 \oplus \alpha, C) \quad (2)$$

$$findkey = FIND(P \oplus C') \quad (3)$$

$findkey$는 64-비트 k_0를 의미하며 $FIND$ 함수는 Fig.6. 과정을 진행한다. 위 과정을 독립적으로 100번 실행한 결과, 키 복구에 모두 성공하였고, 평균적으로 12.5의 clock 수를 가졌으며, 이는 약 0.012초의 시간을 의미한다.

4.3.2 k_1에 대한 정보 획득

k_1에 대한 정보는 전수 조사를 통하여 획득한다. 64-비트 k_1을 획득하는데 소요되는 시간 복잡도는 2^{64}이다. 따라서, 본 연관키 공격은 2 데이터 복잡도, 2^{64} 시간 복잡도, 2 메모리 복잡도로 128-비트 키 k를 찾아낸다.

V. 결론

본 논문에서는 블록 암호 PRINCE에 대한 기존에 제안된 연관키 공격[4]을 확장하여 강력한 새로운 연관키 공격을 제안하였다. 본 논문에서 제안한 공격은 기존 공격의 데이터 복잡도를 2^{33}에서 2로 낮추었다. 결과적으로, 본 공격에 사용된 α-reflection은 하드웨어 구현상 장점이 있지만, 연관키 공격에는 취약한 점을 제공한다고 할 수 있다.

본 논문에서 제안한 연관키 공격은 직접적으로 PRINCE의 안전성을 위협하지는 않지만 만약 PRINCE가 해쉬모드와 같은 특정상황에 적용될 경우 그의 안전성이 급격하게 떨어진다는 것을 의미한다.

References

[1] Eli Biham, "New types of cryptanalytic attacks using related keys," Journal of Cryptology, vol. 7, no. 4, pp. 229-246, 1994.

[2] Alex Biryukov, "DES-X (or DESX)," Encyclopedia of Cryptography and Security (2nd Ed.), pp. 331, 2011.

[3] Julia Borghoff, Anne Canteaut, Tim Guneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzi Nikov, Christof Paar, Christian Rechberger, Peter Rombout s, Soren S. Thomsen, and Tolga Yalcin, "PRINCE: a low-latency block cipher for pervasive computing applications," Advances in Cryptology, ASIACRYPT'2012, LNCS 7658, pp. 208-225, 2012.

[4] Jeremy Jean, Ivica Nikolic, Thomas Peyrin, Lei Wang, and Shuang Wu, "Security analysis of PRINCE", FSE 2013, To appear.

〈저자소개〉

주 왕 호 (Wangho Ju) 학생회원
2013년 8월: 국민대학교 수학과 학사
2013년 9월~2014년 2월: 국민대학교 일반대학원 수학과 석박사 통합과정
2014년 3월~현재: 국민대학교 일반대학원 금융정보보안학과 석박사 통합과정
〈관심분야〉 암호 알고리즘, 정보보안

안 현 정 (Hyunjung An) 학생회원
2013년 8월: 국민대학교 수학과 학사
2013년 9월~2014년 2월: 국민대학교 일반대학원 수학과 석사과정
2014년 3월~현재: 국민대학교 일반대학원 금융정보보안학과 석사과정
〈관심분야〉 이동통신보안, CMVP

이 옥 연 (Okyeon Yi) 정회원
1988년: 고려대학교 수학과 학사
1990년: 고려대학교 일반대학원 수학과 (이학석사)
1996년: University of Kentucky 수학과 (이학박사)
1999년~2001년: 한국전자통신연구원 선임연구원, 팀장
2001년~현재: 국민대학교 수학과 교수
2014년~현재: 국민대학교 일반대학원 금융정보보안학과 교수
〈관심분야〉 정보보호, 이동통신, 암호론 등

강 주 성 (Ju-Sung Kang) 종신회원
1989년: 고려대학교 수학과 학사
1991년: 고려대학교 일반대학원 수학과 (이학석사)
1996년: 고려대학교 일반대학원 수학과 (이학박사)
1996년~1997년: 과학재단 박사후연구원
1997년~2004년: 한국전자통신연구원 선임연구원, 팀장
2001년~2002년: 벨기에 루벤대학 COSIC 방문연구원
2004년~현재: 국민대학교 수학과 교수
2014년~현재: 국민대학교 일반대학원 금융정보보안학과 교수
〈관심분야〉 암호 알고리즘, 정보보호 프로토콜

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