情報保護學會論文誌
第 21 卷 第 3 號, 2011. 6

스트림 암호 Rabbit에 대한 전력분석 공격

배 기 석,[1†] 안 만 기,[2‡] 박 제 훈,[2] 이 훈 재,[3] 문 상 재[1]
[1]경북대학교, [2]국방기술품질원, [3]동서대학교

Power Analysis Attacks on the Stream Cipher Rabbit

KiSeok Bae,[1†] ManKi Ahn,[2‡] JeaHoon Park,[2] HoonJae Lee,[3] SangJae Moon[1]
[1]Kyungpook National University, [2]DTaQ, [3]Dongseo University

요 약

무선 센서 네트워크(wireless sensor network)의 센서 노드는 특성상 전력 소모량, 전송 속도 및 도달 거리 등이 고려되어 설계되야 하며, 여러 형태의 공격(도청, 해킹, 가입자 비밀정보 유출, 서비스 도착상태 등)에 안전해야 한다. 최근 유럽연합의 eSTREAM 공모사업에서 소프트웨어 분야에 선정된 Rabbit 알고리듬은 ISO/IEC 18033-4 기술분야에 추가 선정되었으며 무선 센서 네트워크에 적용 가능한 스트림 암호이다. 이러한 Rabbit 알고리듬은 이론적 분석에 의해 부채널분석 공격에 대한 복잡도가 중간수준(medium)으로 평가됨에 따라, 본 논문에서는 Rabbit에 대한 전력분석 공격방법을 제안하고 실험을 통하여 검증하였다. 실험을 위해서 프로그래밍이 가능한 고성능 8비트 RISC 계열의 AVR 마이크로프로세서 (ATmega128L)를 장착한 IEEE 802.15.4/ZigBee 보드에 전력분석 공격의 대응방법이 적용되지 않은 시스템을 구현하고, 해밍무게 모델을 적용한 전력분석 공격을 실시하였다.

ABSTRACT

Design of Sensor nodes in Wireless Sensor Network(WSN) should be considered some properties as electricity consumption, transmission speed, range, etc., and also be needed the protection against various attacks (e.g., eavesdropping, hacking, leakage of customer's secret data, and denial of services). The stream cipher Rabbit, selected for the final eSTREAM portfolio organized by EU ECRYPT and selected as algorithm in part of ISO/IEC 18033-4 Stream Ciphers on ISO Security Standardization recently, is a high speed stream cipher suitable for WSN. Since the stream cipher Rabbit was evaluated the complexity of side-channel analysis attack as 'Medium' in a theoretical approach, thus the method of power analysis attack to the stream cipher Rabbit and the verification of our method by practical experiments were described in this paper. We implemented the stream cipher Rabbit without countermeasures of power analysis attack on IEEE 802.15.4/ZigBee board with 8-bit RISC AVR microprocessor ATmega128L chip, and performed the experiments of power analysis based on difference of means and template using a Hamming weight model.

Keywords: Stream Cipher, Rabbit, Side Channel Cryptanalysis, Differential Power Analysis

I. 서 론

정보화 기술 및 정보화 기기의 발달로 언제라도 원하는 정보를 실시간으로 이용자 요구에 맞춘 형태로 제공할 수 있는 유비쿼터스 시대가 도래하고 있다. 이는 전자금융서비스, 근거리 무선 통신, 물류/유통, 환경감시, 홈 오토메이션 등 다양한 분야에 적용되고 있다. 따라서 유비쿼터스 핵심기술 중 하나인 무선 센서 네트워크에 대한 관심이 높아지고 있다 [1].

접수일(2010년 11월 17일), 게재확정일(2011년 1월 10일)
† 주저자, gith@ee.knu.ac.kr
‡ 교신저자, amk93@paran.com

무선 센서 네트워크는 필요로 하는 모든 곳에 연산과 무선 통신능력을 지닌 여러 센서 노드(sensor node, MOTE)들을 부착하여 자율적으로 정보를 수집, 관리 및 제어하는 무선 시스템이다. 이러한 센서 노드는 여러 형태의 공격(도청, 해킹, 가입자 비밀정보 유출, 서비스 도착상태(마비) 등)에 취약한 것으로 알려져 있다. 따라서 고속의 암/복호화를 위한 스트림 암호가 요구되어지고 있다.

부채널분석 공격(side channel cryptanalysis)은 암호 알고리듬을 설계할 때 고려되지 못한 부가적인 정보의 누출에 의해 비밀 정보를 알아내는 방식으로 스트림 암호 역시 공격의 대상이 될 수 있다 [2]. 특히, 기존 암호 알고리듬 외에 유럽연합(EU)에서 수행한 eSTREAM 공모사업에서 최종 선정된 알고리듬도 공격 가능성이 언급되었다. 선정된 알고리듬중의 하나인 Rabbit 암호 알고리듬[3]은 2009년 12월에 국제 표준화기구/국제 전자기술 위원회(ISO/IEC)의 ISO /IEC 18033-4 안전성 기술분야[4]에 추가되었고, 전력분석 공격에 대한 이론적 분석 결과 그 안전성이 중간수준(Medium)[5]로 평가받고 있다.

본 논문은 블록암호 상의 초기화 방법과 암호화 방식과는 구조적으로 다른 스트림 암호에서 적용가능한 전력분석공격 모델을 설정한 다음, 최근 센서 노드로 많이 사용되는 고성능 8비트 RISC 계열의 AVR 마이크로프로세서(ATmega128L)를 장착한 IEEE 802.15.4/ZigBee 보드에 부채널분석 공격의 대응방법이 적용되지 않은 Rabbit 알고리듬을 구현하고 해밍무게 모델을 적용한 실제적인 전력분석 공격에 취약함을 실험으로 검증한다.

II. Rabbit 알고리듬 DPA 공격 모델

2.1. 최종 선정된 알고리듬

eSTREAM 공모사업은 안전한 스트림 암호의 분석과 설계능력을 향상시키고, 향후 우수한 스트림 암호를 선정하는 유럽연합 ECRYPT의 프로젝트였다. 소프트웨어 분야에서는 8비트 데이터를 10 클럭 내에 처리하여야 하며, 최소 128비트의 비밀키와 64비트에서 128비트의 초기벡터를 갖는 암호알고리듬이며, 하드웨어 분야에서는 최대 3,000게이트 이하를 사용한 최소 80비트의 비밀키와 32비트에서 64비트의 초기벡터를 갖는 암호 알고리듬의 구현 조건을 제시하였다. [표 1]은 2008년 분야별로 최종 선정된 알고리듬을 보여주고 있다.

2008년 eSTREAM 3 단계에서 Benedikt Gierlichs는 [표 2]와 같이 각 알고리듬에 대한 부채널분석 공격의 가능성을 이론적으로 분석하였다[5]. 소프트웨어 분야 중 Rabbit 알고리듬과 하드웨어 분

[표 1] 최종 선정된 알고리듬

Profile 분야	알고리듬	비밀키	초기벡터
소프트웨어	Rabbit	128	64
	HC-128	128	128
	Salsa20/12	128 or 256	65
	Sosemanuk	128/256	64/128
하드웨어	Grain v1	128	96
	Mickey v2	128	64
	Trivium	80	80 or 64

[표 2] 최종 선정된 알고리듬의 이론적 부채널분석 공격의 취약성 평가결과

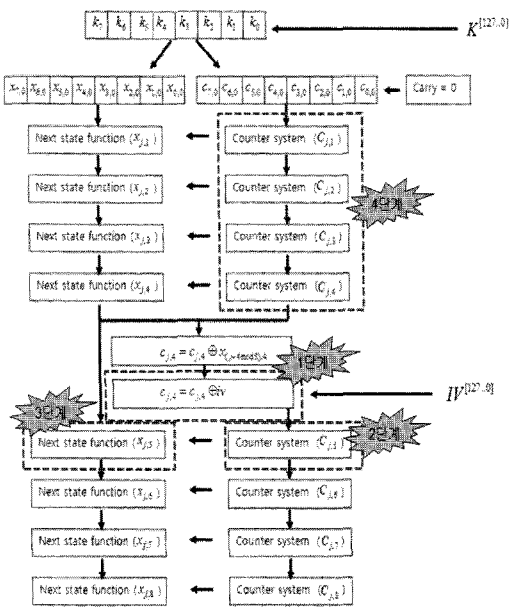
평가항목 \ 알고리듬	Rabbit	HC-128	Salsa20/12	Sose-manuk	Grain	Mickey	Trivium
시차공격 취약성	No	Maybe	No	Maybe	No	Yes	No
조건분기 취약성	No	No	No	No	No	Yes	No
데이터의 해밍무게 누설 가능성, 단순 전력분석 가능성	Yes	Yes	Yes	Yes	Yes	Yes	Yes
차분전력분석 공격 취약성	Yes	Yes	Yes	Yes	Yes	Yes	Yes
차분전력분석 공격의 복잡성	**Medium**	**Low**	**Low**	**Low**	**Medium**	**Medium**	**Medium**
대응방법의 비용	High	High	High	High	-	-	-

야의 3종 알고리듬에 대해서 차분전력분석 공격의 복잡성이 중간수준(medium)으로 높게 분석되었다. 소프트웨어 분야에 부채널분석 공격은 이론적인 분석 외에 실제적인 전력분석 공격의 연구결과는 E. Zenner[6]에 의해 256비트의 비밀키를 사용하는 HC-256에 대한 시차분석 공격을 실시한 사례 외에는 현재까지 발표된 바가 없으나, 하드웨어 분야에서는 실제적인 전력분석 공격 및 전자파분석 공격의 연구결과가 발표되었다.

2.2. Rabbit 알고리듬의 구조

Rabbit 알고리듬은 스웨덴의 M. Boesgaard에 의해 발표된 동기 스트림 암호로 비밀키와 초기벡터의 초기화, 513 비트 내부변수 갱신, 128비트 키수열 발생 등으로 구성된다[3]. 2009년에 SSL/TLS 프로토콜로 전자상거래에 사용되는 CyaSSL 소프트웨어에 적용되었다. 현재까지는 대수적 공격, 차분공격, 상관공격, 각개공격, 상관공격, 추측결정공격 등의 대표적인 공격들에 안전한 것으로 발표되어지고 있다[7]. 또한 무선센서 네트워크에 적용될 수 있도록 안전성 및 저전력 특성을 확보하는 연구가 진행되고 있다[8].

Rabbit 알고리듬은 다음과 같은 과정으로 구성되어 있다.



[그림 1] Rabbit 알고리듬의 비밀키 설정과 초기벡터 설정

1) 비밀키 설정과정(key setup scheme)

입력된 128비트의 비밀키 $K^{[127...0]}$을 8개의 부분키(subkey) k_i로 분할(key expansion)한 후, 이를 이용하여 내부 중간 값인 256비트의 상태 변수(state variables) $x_{j,0}$과 계수변수(initial counters) $c_{j,0}$을 생성한다. 내부 중간 값들은 각기 여덟 개의 블록으로 동작하며, 하나의 블록은 32비트가 된다. 1비트의 올림수(carry)를 포함하여 총 513비트의 내부 중간 값들은 계수 시스템(counter system)과 상태천이함수(next state function)에 의해서 각기 갱신하는 과정을 4회 반복하게 된다. 이는 [그림 1]을 통해서 확인할 수 있다. 또한 마지막으로 갱신된 상태 변수와 계수변수를 조합하여 초기벡터 설정과정에서 사용하는 마스터 계수변수 $c_{j,4}$로 변경(modification)한다.

2) 초기벡터 설정과정(Initial Vector setup scheme)

먼저 입력된 64비트 초기벡터(IV)로 비밀키 설정과정에서 생성된 마스터 계수변수를 초기화한다. 초기화 된 계수변수 $c_{j,4}$는 앞서 비밀키 설정과정에서 사용한 계수 시스템과 상태천이함수를 동일하게 사용하여 4회 반복적으로 갱신한다.

3) 키수열 생성과정(extraction scheme)

비밀키 설정과정과 초기벡터 설정과정으로 생성된 상태변수간의 XOR 연산으로 128비트 키수열 블록을 생성.

4) 암/복호화 과정(encryption/ decryption scheme)

생성된 128비트 키수열 블록과 입력된 평문 또는 암호문을 XOR 연산으로 암/복호하는 과정.

2.3. Rabbit 알고리듬의 전력분석 공격 모델

Rabbit 알고리듬의 전력분석 공격은 알고 있는 초기벡터의 입력으로부터 시작한다. 초기벡터 설정과정에 의한 내부 중간값(계수변수, 상태변수, 올림수)을 알아낸 후, 이를 이용하여 비밀키 설정과정의 비밀키를 알아낼 수 있다. 32비트 단위의 중간 값을 알아낼 때, Benedikt Gierlichs 등이 분석한 1비트 단위의 이론적인 분석[5]와 다르게 8비트 단위의 공격과 1비

트의 올림수에 대한 1비트 단위의 전력분석 공격을 실시한다. 실험에서 사용한 ATmega 128칩은 8비트 단위로 연산 동작하기 때문에 8비트 단위로 분석하는 것이 용이하며 해밍무게 논리에 의해 전력소모량의 차이를 쉽게 얻을 수 있다. 그러나 가정해야할 경우의 수가 2^8으로 증가하는 단점이 있으며, 실험에 필요한 전력소모파형의 수를 줄이기 위해서 시뮬레이션을 통해 입력되는 IV에 의한 중간 값의 해밍무게를 인위적으로 7이상과 1이하로 구분하였다. 〔그림 1〕은 Rabbit 알고리듬의 상세 흐름도로 내부 중간 값의 변화를 파악할 수 있다. 다음은 Rabbit 알고리듬의 차분전력분석 공격의 절차이다.

1) 1단계 차분전력분석 공격

초기벡터 설정과정의 아래와 같은 초기화 연산과정에서 실시한다. 마스터 계수변수 $c_{j,4}$와 초기벡터를 입력으로 하는 연산 과정에서 예측한 마스터 계수변수에 대한 결과 값을 이용한 헤밍무게 모델을 이용하여 차분전력분석 공격을 통해 마스터 계수변수와 연산의 결과인 갱신된 계수변수를 알아낸다.

$$\begin{aligned} c_{0,4} &= c_{0,4} \oplus IV^{[31..0]} \\ c_{1,4} &= c_{1,4} \oplus (IV^{[63..48]} \| IV^{[31..16]}) \\ &\vdots \\ &\vdots \\ c_{7,4} &= c_{7,4} \oplus (IV^{[47..32]} \| IV^{[15..0]}) \end{aligned} \quad (1)$$

2) 2단계 차분전력분석 공격

초기벡터 설정과정의 5회째 계수시스템 연산과정에서 올림수(carry)를 알아내는 것이다. 1단계에서 알아낸 갱신된 계수변수와 고정된 상수 그리고 올림수가 더해지는 과정에서 올림수를 제외한 나머지 값들은 알고 있으므로, 올림수를 추정하여 차분전력분석 공격을 수행한다. 이 때 올림수는 1비트에 불과하므로 '0'과 '1'의 두 경우에 대해서 고려한다. 이를 통해 올림수를 알 수 있다면 순차적인 덧셈연산을 수행하여 모든 256비트 계수변수 $c_{j,5}$을 자연스럽게 알아낼 수 있다.

$$\begin{aligned} c_{0,i+1} &= c_{0,i} + 0x4D34D34D + Carry \\ c_{1,i+1} &= c_{1,i} + 0xD34D34D3 + Carry \\ &\vdots \\ &\vdots \\ c_{7,i+1} &= c_{7,i} + 0xD34D34D3 + Carry \end{aligned} \quad (2)$$

3) 3단계 차분전력분석 공격

초기벡터 설정과정의 수식 (3)과 같은 내부상태천이 연산단계 중 함수 $g_{j,4}$는 수식 (4)과 같이 32비트 상태변수 $x_{j,4}$와 32비트 계수변수 $c_{j,5}$의 덧셈 연산 값을 사용한다. 따라서 공격자는 알고 있는 초기벡터를 입력하여 앞서 2단계에서 확인한 계수변수 $c_{j,5}$의 값을 변화시켜가며 덧셈연산 시점에서 상태변수 $x_{j,4}$을 알아낸다.

$$\begin{aligned} x_{0,i+1} &= g_{0,i} + (g_{7,i} \lll 16) + (g_{6,i} \lll 16) \\ x_{1,i+1} &= g_{1,i} + (g_{0,i} \lll 8) + g_{7,i} \\ &\vdots \\ &\vdots \\ x_{7,i+1} &= g_{7,i} + (g_{6,i} \lll 8) + g_{5,i} \end{aligned} \quad (3)$$

$$g_{j,i} = ((x_{j,i} + c_{j,i})^2 \oplus ((x_{j,i} + c_{j,i})^2 \gg 32)) \bmod 2^{32} \quad (4)$$

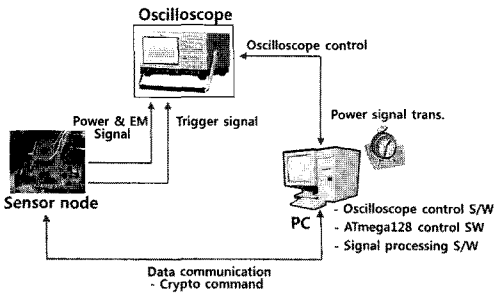
4) 4단계 템플릿을 이용한 전력분석 공격

1~3단계 과정을 거치게 되면 비밀키 생성 과정에서 연산된 상태변수 $x_{j,4}$와 마스터 계수변수 $c_{j,4}$을 찾아낼 수 있다. 마스터 계수 변수는 비밀키 생성 과정에서 마지막 갱신 과정 후의 상태변수 $x_{j,4}$와 계수변수 $c_{j,4}$을 조합한 것이므로 공격자는 계산을 통해 갱신된 계수변수를 찾아낼 수 있다. 초기벡터 설정과정과 달리 비밀키 설정과정은 입력되는 초기벡터와 무관하게 항상 동일한 값으로 동일한 연산을 수행하므로 1~3단계와 같이 내부의 중간값을 바꿔가면서 전력의 변화를 확인하는 공격은 불가능하다. 따라서 공격대상의 센서 노드와 동일한 실험 센서 노드를 사용하여 공격 시점에 대한 템플릿을 생성하여 공격 대상의 전력파형과 템플릿을 비교하는 방식을 사용한다. 일부 부분키 k_i을 찾기 위해서 갱신 과정의 결과물에서부터 역추적을 수행한다. 계수 시스템은 수식 (2)의 첫 번째 연산의 올림수만 알게 되면 이전 계수 변수 $c_{j,3}$, $c_{j,2}$, $c_{j,1}$, $c_{j,0}$들을 계산할 수 있다. 이를 이용해서 상태변수들도 찾아낼 수 있으며, 비밀키에서 생성된 부분키 k_i들도 확인할 수 있다. 따라서 4회의 갱신과정에 대해 템플릿과의 상관도 조사 공격을 총 4회 수행한다면 최초의 비밀키 $K^{[127...0]}$을 복원할 수 있다. 공격 대상은 올림수 1비트의 덧셈 연산이므로 0과 1의 경우에 대한 템플릿만이 사용한다.

III. 전력분석 공격 실험 및 분석

3.1. 실험 환경 설정

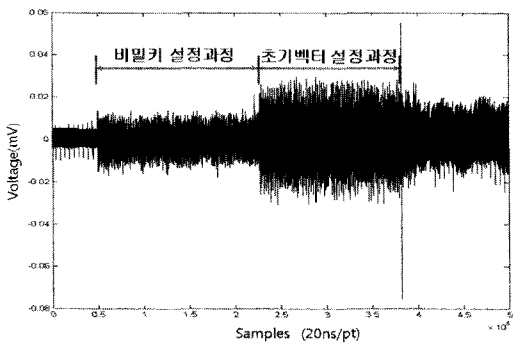
실험을 위해서 ZigBee 보드로 구현된 센서 노드에 공개된 Rabbit 알고리듬을 탑재한다. Rabbit 알고리듬은 AVR Studio의 컴파일러를 통해 코드를 생성하였다. 칩에서 소모되는 전력을 측정하기 위해서 디지털 오실로스코프를 사용하며, PC에서는 제어프로그램을 통해 전력소모파형을 수집한다. 또한 칩에 인가되는 초기벡터의 해밍무게를 구분하거나 수집된 전력소모파형을 분석하기 위해서 MATLAB Toolbox 프로그램을 사용하며, 센서 노드가 동작할 때 반복적인 초기벡터의 입력을 위해서 칩과 연동되는 신호처리 제어프로그램을 구현하여 사용한다. [그림 2]는 전력분석 공격을 위한 구성과 실제 장비 설치도이다.



[그림 2] 부채널분석 공격을 위한 장비간 제어신호 구성

3.2. 전력분석 공격 모델의 공격결과

Rabbit 알고리듬이 동작할 때 각 단계별로 전력분석 공격을 수행한다. 전체 전력소모파형에서 초기벡터 설정과정이 동작하는 시점을 알기 위해 입력되는 초기벡터를 변경시켜가며 1000개의 전력소모파형을 수집하여 평균한 후 차분하여, [그림 3]과 같은 파형을 얻는다. 항상 동일한 값으로 동일한 연산을 수행하는 비밀키 설정과정의 경우 차분에 의해 0에 가까운 결과를 보이며, 입력된 초기벡터에 의해 매번 서로 다른 연산을 수행하는 초기벡터 설정과정의 경우 비밀키 설정과정에 비해서 전력소모량의 차이가 크게 나타난다. 이는 [그림 3]과 같이 확실한 구분이 가능하다.



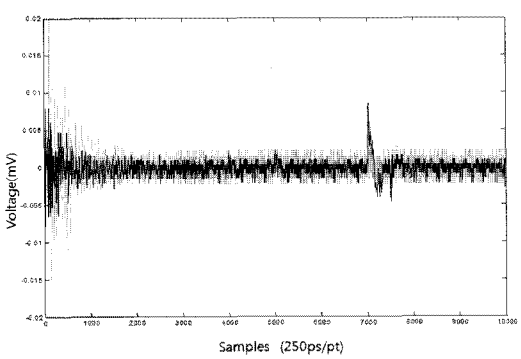
[그림 3] 차분 전력소모파형을 통한 초기벡터 설정과정 수행시점 확인

1) 1단계 차분전력분석 공격 결과

입력된 초기벡터는 식 (1)의 계수연산에서 32비트씩 차례로 연산되나 실험에 사용한 마이크로프로세서는 8비트 연산을 수행하므로 8비트씩 추측하여 총 4회에 걸친 분석으로 계수변수를 알 수 있다. 이러한 과정을 8회 수행하면 전체 256비트의 계수변수 $c_{j,4}$를 알아낼 수 있다. 공격자는 식 (5)와 같은 추정모델을 적용하며, 차분을 위해 수집해야할 전력소모파형의 수를 최소화하기 위한 방안으로 임의의 추측한 계수변수 $c_{0,4}$의 하위 8비트 해밍무게가 7 이상인 경우와 1 이하인 경우로 분류하였다. 수집된 전력소모파형은 평균을 취한 후 차분한다.

$$HW((C_{0,4} \oplus Modifed\ IV)|_{\text{하위 8비트}}) \tag{5}$$

랜덤한 초기벡터 값을 생성하여 해밍무게에 맞춰 각기 1,000개씩 분류한다. 이들을 칩에 입력하여 각 모델에 대해 1,000개의 전력소모파형을 수집하고 평균을 수행하였다. [그림 4]는 올바르게 추측한 경우와 잘못된 추측한 경우 XOR 연산시점에서 피크 파형을



[그림 4] 계수변수 $c_{0,4}$의 하위 8비트를 차분전력분석 공격결과

보여 주고 있다. 올바르게 추측한 경우는 진한 검정색 파형이고 엷은 회색 파형들은 틀리게 추측한 경우이다. 전체 차분파형은 한 포인트당 샘플률은 250ps/pt로 10,000개의 샘플 포인트를 가지고 있다.

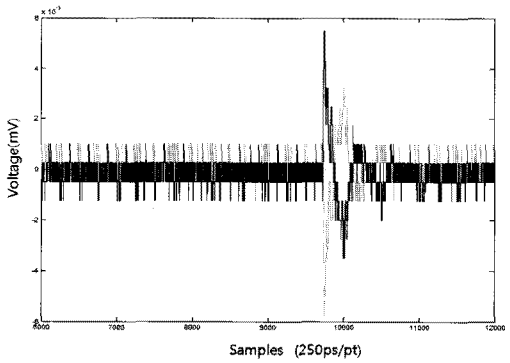
2) 2단계 차분전력분석 공격 결과

2단계 전력분석 공격의 목적은 5회째 계수시스템 연산중 올림수(Carry)를 알아내는 것이다. 이는 랜덤하게 입력할 수 있는 초기벡터와 1단계 전력분석을 통해 알아낸 계수변수로 갱신된 계수변수 $c_{0,4}$을 입력하여, 식 (2)의 연산과정 중에서 계수변수 $c_{0,5}$을 계산하는 과정에서 사용되는 올림수 1비트를 추측하여 알아내는 것이다. 이때 함께 더해지는 상수는 고정되어 이미 알고 있는 값이다. [표 3]은 최하위비트(LSB)의 해밍무게 모델을 적용하여 추측한 올림수에 따른 최하위 비트가 0과 1일 경우 차분파형 관계를 보여주고 있다.

[표 3] 추측한 올림수에 따른 해밍무게 결과

추측한 올림수	계수변수의 최하위비트	덧셈 연산 결과	분류한 해밍무게	차분 파형
0	1	1	High HW	(+) 피크
	0	0	Low HW	
1	1	0	Low HW	(-) 피크
	0	1	High HW	

[그림 5]는 차분파형으로 추측한 해밍무게 모델에 따라 피크 성분이 (+)로 나타남을 확인하였다. 따라서 올바른 올림수는 0임을 알 수 있다. 따라서 256비트의 계수변수 $c_{j,5}$을 자연스럽게 알아낼 수 있다.



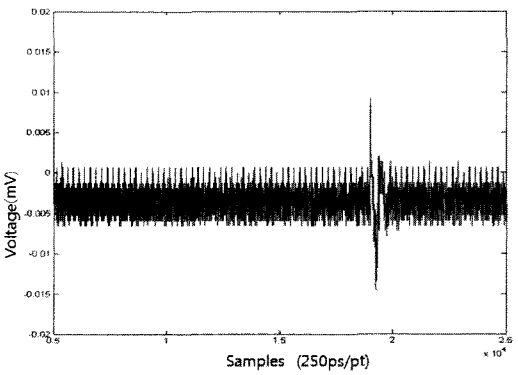
[그림 5] 올림수를 0으로 추측한 경우 (+) 차분파형

3) 3단계 차분전력분석 공격 결과

내부 상태천이연산 과정 중 함수 $g_{j,4}$의 입력 값은 이전에 생성된 32비트 상태변수 $x_{j,4}$와 32비트 계수변수 $c_{j,5}$의 덧셈 연산 결과로 수식 (4)과 같다. 3단계 전력분석 공격의 목적은 1, 2 단계를 통해 확인한 갱신된 계수변수 $c_{j,5}$의 값을 이용하여 피연산자인 256비트 상태변수 $x_{j,4}$을 알아내는 것이다. 식 (6)과 같은 추정 모델을 적용하여 임의의 추측한 상태변수 $x_{0,4}$의 하위 8비트 해밍무게가 7 이상인 경우와 1 이하인 경우로 분류하고 전력소모파형을 수집 및 평균을 취한 후 차분한다.

$$HW((x_{0,4}+c_{0,5})|_{\text{하위 8비트}}) \tag{6}$$

[그림 6]은 올바르게 추측한 상태변수에 대한 차분전력소모파형의 결과로 첫 번째 덧셈 연산하는 시점에서 피크가 생성되었다. 이와 같은 방법을 반복하면 전체 256비트의 상태변수 $x_{j,4}$을 알아낼 수 있다.



[그림 6] 상태변수 $x_{0,4}$의 하위 8비트에 대한 차분전력분석 파형결과(올바른 계수)

4) 4단계 템플릿을 이용한 전력분석 공격 결과

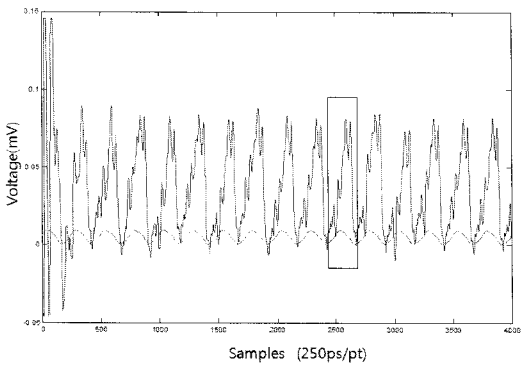
2단계와 달리 4단계에서 공격이 적용되는 시점은 비밀키 생성 과정으로 공격자가 입력하는 초기벡터와는 아무 상관없이 동일한 값들로 동일한 연산을 수행한다. 따라서 공격대상의 센서 노드와 동일한 환경의 실험 센서 노드로 수식 (2)과 동일한 계수 시스템의 올림수 덧셈 연산에 대한 템플릿을 생성한다.

이때 올림수는 1비트이므로 1단계에서 알아낸 계수

변수 $c_{j,4}$와 덧셈 연산될 상수 0x4D34D34D를 고려하여 '1'과 '0'에 대한 2가지 템플릿을 생성한다. 식 (7)을 이용하여 add 명령어 수행시점에 대한 템플릿의 평균값 M_0, M_1을 계산한다.

$$M_i = \frac{1}{D}\sum_{j=1}^{D} t_j \quad (7)$$

〔그림 7〕은 실험 센서 노드에서 1000개의 전력소모파형을 평균한 파형으로 한 클럭에 동작하는 add 명령어의 연산시점을 표시하였다. 동작 클럭 신호를 확인하여 공격 대상의 센서 노드에서 덧셈 연산이 수행되는 정확한 지점을 찾은 후, 해당 지점을 추출하여 템플릿과 비교하는 방식으로 템플릿 공격의 오차를 줄였다.



〔그림 7〕 덧셈 연산과정에서 add 명령어의 연산시점

공격 대상의 센서 노드에서 연산된 올림수가 1일 때, 〔표 4〕와 같이 공격 대상의 센서 노드와 실험 센서 노드간의 계산된 상관도를 얻을 수 있다. 두 상관계수 평균값은 약 0.045의 차이를 보이고 있어 실제 올림수도 0x01임을 알 수 있다.

〔표 4〕 add 명령어 수행시점의 평균 전력소모파형간 상관계수

공격 대상 센서 노드	실험 센서 노드		상관계수	측정값
상수와 덧셈연산 전 계수변수의 최하위 비트(LSB)	추측한 계수변수의 최하위 비트(LSB)	입력된 올림수		
1	1	0x00	ρ_{00}	0.9765
				0.9186
				0.9772
				0.8945
	0	0x01	ρ_{01}	0.9899
				0.9811
				0.9864
				0.9906

비밀키 설정 과정에서 마지막 계수 시스템으로 갱신된 계수변수 $c_{j,4}$와 상수, 올림수를 알고 있기 때문에 공격자는 갱신되기 이전의 계수변수 $c_{j,3}$를 연산할 수 있다. 비밀키 설정 과정동안 총 4회에 걸친 갱신과정에 대해서 템플릿과의 비교 공격을 3회 더 반복하면서 역추적하게 된다면, 공격자는 부분키 k_i에서 바로 생성된 $c_{j,0}$와 $x_{j,0}$을 찾아낼 수 있다. 초기 올림수는 0x00으로 설정되어 있으므로 비밀키 초기화 단계의 연접 배열구조에 의해 최종 비밀키를 확인 할 수 있다.

3.3 결과 분석

Festal 구조나 S-box를 사용하는 블록암호는 특정 시점에 연산되는 해밍무게를 추측하고 한 단계의 부채널분석 공격으로 비밀키를 알아낼 수 있는 반면, 스트림 암호인 Rabbit 알고리듬은 4단계의 전력분석 공격을 수행해야 최종 비밀키를 알아낼 수 있었다. 또

〔표 5〕 단계별 부채널분석 공격의 요약

구 분	단계	공격시점	공격 대상	전력분석 공격 유형
초기벡터 설정과정	1단계	초기벡터에 의한 계수변수 초기화단계	256비트 계수변수	평균 차분
	2단계	5회째 내부상태천이 연산단계의 계수변수 갱신단계	1비트 올림수, 256비트 계수변수	평균 차분
	3단계	5회째 내부상태천이 연산단계의 상태변수 갱신단계	256비트 상태변수	평균 차분
비밀키 설정과정	4단계	1~4회째 내부상태천이 연산단계의 계수변수 갱신단계	1비트 올림수, 256비트 계수변수	템플릿의 상관도

한 스트림 암호의 특성상 비밀키, 초기벡터들과 연관된 새로운 내부변수들이 사용되기 때문에, 추측해야 하는 해밍무게 모델도 4가지로 구분해야 했으며 공격을 위한 연산시점도 다양하였다. 또한 각 단계별로 연관성이 있어 1단계 전력분석 공격이 이루어질 수 없다면 비밀키를 알아낼 수 없는 구조를 이루고 있다. [표 5]는 단계별 전력분석 공격의 과정을 요약하였다. 1,2,3단계 부채널분석 공격은 차분전력분석 공격으로 수행 가능하지만, 4단계에서는 단일 비트 템플릿을 이용한 전력분석 공격이 요구되었다. 물론 각 단계에서도 템플릿 공격이 가능하나, 추측해야하는 템플릿의 수가 256가지이므로 계산해야 할 상관계수가 256개로 증가하여 연산량 증가를 가져온다.

IV. 결론

본 논문에서는 최근 유럽연합에서 ISO/IEC 18033-4 스트림 암호분야에 추가 선정되었으며, 무선 센서 네트워크의 센서 노드에 적용 가능한 Rabbit 알고리듬의 부채널 공격을 실험적으로 분석하였다. 8비트 마이크로프로세서를 사용하는 센서 노드에 Rabbit 알고리듬을 구현하여 1차 전력분석 공격을 4단계에 걸쳐 공격함으로써 비밀키를 찾아낼 수 있음을 확인하였다. 이러한 제안 공격방법은 타 동기식 스트림 암호 알고리듬을 사용하는 스마트카드, RFID 등 임베디드 암호시스템에도 적용될 수 있을 것으로 기대된다. 마지막으로 향후 소프트웨어 기반 스트림 암호분야에 대한 부채널분석 연구활동은 다양한 대응방법의 적용과 함께 고차 부채널분석 공격 가능성도 활발히 연구되어져야 할 것이다.

참고문헌

[1] Feng Zhao and Leonidas Guibas, Wireless Sensor Networks : An Information Processing Approach, Morgan Kaufmann Publishers Inc., July 2004.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," In Advances in Cryptology, CRYPTO'99, LNCS 1666, pp. 388-397, 1999.

[3] M. Boesgaard, M. Vesterager, T. Pedersen, J. Christiansen, and O. Scavenius. "Rabbit: A new high-performance stream cipher," Proc. of FSE 2003, LNCS 2887, pp. 307-329, 2003.

[4] ISO/IEC 18033-4 AMD 1 : Information technology - Security techniques - Encryption algorithms - Part 4 : Stream ciphers AMENDMENT 1: Rabbit and Decim, JTC 1/SC 27(IT security tech.), Dec. 2009.

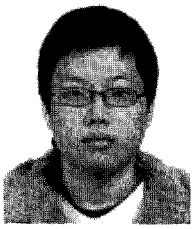
[5] B. Gierlichs, L. Batina, C. Clavier, T. Eisenbarth, A. Gouget, Helena H, T. Kasper, K .Lemkerust, S. Mangard, A. Moradi and E. Oswald, "Susceptible of eSTREAM Candidates towards Side Channel Analysis," Proceeding of SASC 2008 - Candidate of the Art of Stream Ciphers, pp. 123-150, Feb. 2008.

[6] E. Zenner, "A Cache Timing Analysis of HC-256," Selected Areas in Cryptography, SAC'09, LNCS 5381, pp. 199-213, 2008.

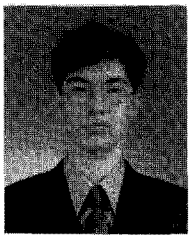
[7] M. Boesgaard, T. Pedersen, M. Vesterager, and E. Zenner. "The Rabbit Stream Cipher - Design and Security Analysis," Proceeding of SASC 2004 - The State of the Art of Stream Ciphers, pp. 7-29, Oct. 2004.

[8] Ruhma Tahir, Muhammad Younas Javed, Attiq Ahmad, and Raja Iqbal, "SCUR: Secure Communications in Wireless Sensor Networks using Rabbit," Proceedings of the World Congress on Engineering - WCE 2008, pp. 523-527, July 2008.

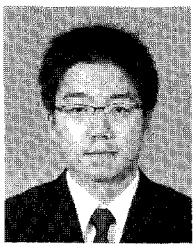
〈著者紹介〉



배 기 석 (KiSeok Bae) 학생회원
2006년 8월: 경북대학교 전자·전기공학부 졸업
2008년 8월: 경북대학교 전자공학과 석사
2009년 3월~현재: 경북대학교 전자공학과 박사과정
〈관심분야〉 정보보호, 네트워크 보안, 스마트카드 보안

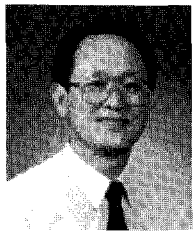


안 만 기 (MahnKi Ahn) 정회원
2000년 2월: 경북대학교 전자전기공학부 졸업(학사)
2000년 1월~2001년 1월: 삼성전자 프린터사업부 C-LBP 연구원
2003년 2월: 경북대학교 전자공학과 석사(정보통신공학)
2011년 2월: 경북대학교 정보보호학과 박사
2003년 4월~현재: 국방기술품질원 선임연구원
〈관심분야〉 정보보호, RFID/USN 보안, 부채널분석 공격



박 제 훈 (JeaHoon Park) 학생회원
2004년 2월: 경북대학교 전자·전기공학부 졸업
2006년 2월: 경북대학교 전자공학과 석사
2011년 2월: 경북대학교 전자공학과 박사
2011년 1월~ 현재: 국방기술품질원 선임연구원
〈관심분야〉 정보보호, 네트워크 보안, 스마트카드 보안

이 훈 재 (HoonJae Lee) 정회원
1985년 2월 : 경북대학교 전자공학과 졸업(공학사)
1987년 2월 : 경북대학교 전자공학과 졸업(정보통신공학, 공학석사)
1998년 2월 : 경북대학교 전자공학과 졸업(정보통신공학, 공박사)
1987년 2월~1998년 1월 : 국방과학연구소 선임연구원
1998년 2월~2002년 1월 : 경운대학교 컴퓨터전자정보공학부 조교수
2002년 2월~현재 : 동서대학교 컴퓨터정보공학부 조교수
〈관심분야〉 암호이론, 네트워크보안, 디지털 통신



문 상 재 (SangJae Moon) 종신회원
1972년 2월: 서울대학교 공업교육(전자전공)과 학사
1974년 2월: 서울대학교 전자공학과 석사
1984년 6월: 미국 UCLA 전기공학과 박사
1984년 7월~1985년 6월: UCLA Postdoctor 근무
1984년 7월~1985년 6월: 미국 OMNET 컨설턴트
1997년 9월~1998년 8월: 경북대학교 전자전기공학부 학부장
1974년 12월~현재: 경북대학교 전자전기컴퓨터공학부 교수
2000년 8월~현재: 경북대학교 이동네트워크 정보보호기술 연구센터장
2002년 2월~현재: 한국정보보호학회 명예회장
〈관심분야〉 정보보호, 디지털 통신, 이동 네트워크