Cortex-M4 에서 RM-Code 인코딩의 전력 누출 취약성 분석

김동현, 전재호, 김영식
대구경북과학기술원

dhkim200426@dgist.ac.kr, dgwogh@dgist.ac.kr, ysk@dgist.ac.kr

Power Leakage Vulnerability Analysis of RM-Code Encoding on Cortex-M4

Dong Hyun Kim, Jae Ho Jeon, Young-Sik Kim
DGIST

요 약

Reed- Muller(RM) 코드는 단순한 부호 구조와 빠른 연산 특성으로 통신 채널 오류 정정뿐 아니라 암호 구현에서도 널리 사용된다. 그러나 저사양 임베디드 장치에서 비트 단위 연산을 수행하면 전력 소모가 데이터에 의존적으로 변화하며, 이는 전력 분석의 공격 표면을 확장한다. 본 연구는 PQClean 코드베이스의 rm-encode 구현을 기준으로, Cortex-M4(CW308 보드)에서 메시지 인코딩 과정 중 전력 누출이 관측됨을 확인하였다. 본 연구에서는 PicoScope 3403D 로 수집한 트레이스를 이용해 학습 기반 분석을 수행한 결과, 약 150 개의 trace 만으로도 비밀 메시지를 98.3% 정확도로 복구할 수 있음을 보였다. 이는 RM-code 인코딩이 단순한 비암호 연산으로 간주되더라도 실제 구현에서는 고위험 누출원이 될 수 있음을 시사한다.

Ⅰ. 서 론

임베디드 시스템은 부채널 분석(Side-Channel Analysis, SCA)에 취약하며, 특히 ARM Cortex-M4 와 같은 저전력 MCU 를 대상으로 한 전력 분석 공격은 지속적으로 연구되어 왔다. 이러한 공격을 통해 공격자는 연산 과정에서 나타나는 전력 소모의 미세한 차이를 이용해 내부 처리 데이터나 비밀 값을 추정할 수 있다[1]. 전통적으로는 암호 연산이 주요 표적이었지만[2], 실제 구현에서는 오류정정 같은 보조 연산도 비밀 정보와 결합되어 공격 표면을 넓힐 수 있다.

한편, V2X(Vehicle-to-Everything) 통신에서는 양자 컴퓨터의 위협에 대비하여 기존 암호체계를 양자 내성 암호(PQC)로 전환할 필요성이 대두되고 있다. 특히 KEM(Key Encapsulation Mechanism) 적용 시 HQC(Hamming Quasi-Cyclic)가 유력한 후보로 고려되는데, HQC 는 내부적으로 Reed- Muller(RM) 코드를 활용한다. RM 코드는 단순한 구조와 비트 연산 기반의 효율성으로 통신 분야에서 널리 쓰이며, 최근에는 PQC 구현에서도 보조 구성요소로 활용된다. 그러나 분기 없는 상수 시간 형태로 구현되더라도, 마스크, 시프트, XOR 중심 연산에서는 입력 비트에 따라 중간값의 해밍가중치와 비트 전이가 달라지므로 전력 누출이 발생할 수 있다[3]. 이는 V2X 환경에서 HQC 기반 KEM 을 적용할 경우, RM 코드 인코딩 과정에서 비밀 정보가 유출될 수 있음을 의미한다.

본 연구에서는 PQClean 기반 rm-encode 를 Cortex-M4(CW308 보드)에서 실행하고 PicoScope 3403D 로 전력 트레이스를 측정하여 누출 특성을 분석하였다. 그 결과 약 150 개의 trace 만으로 메시지를 98.3% 정확도로 복구할 수 있음을 확인하였으며, RM-code 인코딩과 같은 보조 연산도 임베디드 환경에서 중요한 부채널 위험 요인이 될 수 있음을 보였다.

Ⅱ. 본론

본 연구는 PQClean 코드베이스의 encode(uint64_t *cword, uint8_t message) 구현을 대상으로 한다. 해당 함수는 8 비트 입력 메시지 message 로부터 128 비트 코드워드 cword[0], cword[1]를 생성한다. 이 구현에서는 분기(branch) 없이 BITOMASK, 시프트(shift), AND/XOR 조합을 이용해 메시지 비트를 일정한 패턴 마스크로 확장한 뒤, 이를 누적하여 코드워드를 구성한다.

```
static void encode(uint64_t *cword, uint8_t message) {
    uint32_t first_word;
    // bit 7 flips all the bits, do that first to save work
    first_word = BIT0MASK(message >> 7);
    // bits 0, 1, 2, 3, 4 are the same for all four longs
    // (Warning: in the bit matrix above, low bits are at the left!)
    first_word ^= BIT0MASK(message >> 0) & 0xaaaaaaaa;
    first_word ^= BIT0MASK(message >> 1) & 0xcccccccc;
    first_word ^= BIT0MASK(message >> 2) & 0xf0f0f0f0;
    first_word ^= BIT0MASK(message >> 3) & 0xff00ff00;
    first_word ^= BIT0MASK(message >> 4) & 0xffff0000;
    // we can store this in the first quarter
    cword[0] = first_word;
    // bit 5 flips entries 1 and 3; bit 6 flips 2 and 3
    first_word ^= BIT0MASK(message >> 5);
    cword[0] |= (uint64_t)first_word << 32;
    first_word ^= BIT0MASK(message >> 6);
    cword[1] = (uint64_t)first_word << 32;
    first_word ^= BIT0MASK(message >> 5);
    cword[1] |= first_word;
}
```

그림 1. PQClean rm-encode 구현 코드

핵심은 BITOMASK(message >> k)가 메시지의 k 번째 비트를 0 또는 all-ones(예: 0xFFFFFFFF) 형태로

확장한다는 점이다. 이후 이 값과 상수 마스크(예: 0xaaaaaaaa, 0xcccccccc, 0xf0f0f0f0, 0xff00ff00, 0xffff0000)의 AND 연산을 수행하여, 특정 비트가 1 일 때만 미리 정해진 비트 패턴이 first_word 에 XOR 로 반영된다. 결과적으로 first_word 는 메시지 비트들의 선형 결합으로 생성되는 32 비트 패턴이며, 이후 일부 비트(예: bit5, bit6)를 반영하는 추가 단계를 거쳐 cword[0], cword[1]에 저장된다.

Cortex-M4 와 같은 MCU 에서 CMOS 로직의 동적 전력 소모는 일반적으로 스위칭 활동(switching activity)에 비례하며, 실무적으로는 (1) 레지스터 값의 해밍가중치(Hamming Weight, HW) 또는 (2) 연속 상태 간 해밍거리(Hamming Distance, HD) 모델로 근사한다. 본 구현에서는 메시지 비트를 BITOMASK 로 32 비트 전체로 확장한 뒤, 넓은 비트 폭에 걸친 패턴을 생성하므로 다음 특성을 가진다.

1. 메시지 비트 1 개가 32 비트 다수 위치에 반복 반영됨
2. 중간값(first_word)이 메시지에 직접 종속됨
3. 레지스터의 갱신이 연속적으로 발생하여 HD 누출이 강해짐

위 이유로 rm-encode 는 분기 없는 상수 시간 구현처럼 보이더라도, 전력 관점에서는 상수 누출(constant-leakage)이 아니며, 메시지 비트에 대한 강한 데이터 의존 누출을 가진다. PicoScope 로 수집한 전력 트레이스를 사용해 TVLA 를 수행한 결과, 아래와 같이 임계값 4.5 를 넘는 점이 다수 발생함을 확인하였다. 본 실험에서는 0 번째 비트를 0 또는 1 로 설정하여 각각 1,000 개의 트레이스를 수집하였고, 두 집단의 전력 차이가 뚜렷하게 확인되었다.

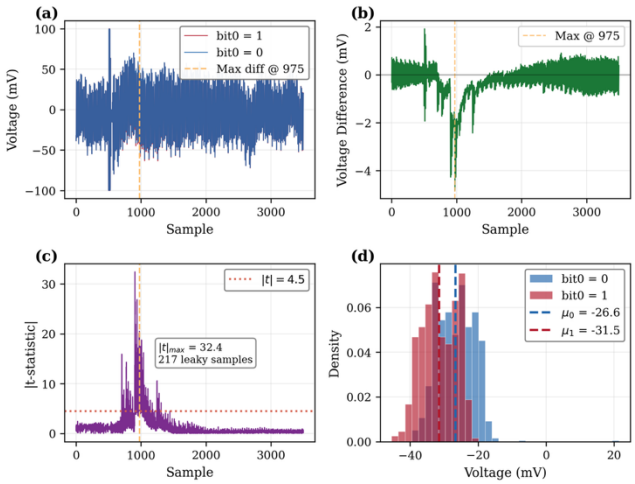

그림 2. RM-encode TVLA 결과

누출점이 TVLA 로 확인되었으므로, 이어서 CNN 기반의 Classifier 를 사용해 수집한 트레이스를 바탕으로 메시지를 복구하였다. 그 결과, 약 150 개의 trace 만으로 메시지를 98.3%의 정확도로 복구할 수 있음을 확인하였다. 이처럼 적은 양의 트레이스만으로도 높은 정확도로 메시지를 복원할 수 있다는 점은 rm-encode 의 부채널 누설이 심각함을 의미한다.

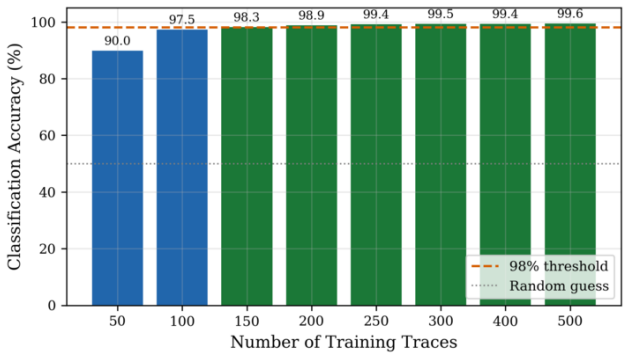

그림 3. 트레이스 수에 따른 정확도

Ⅲ. 결론

본 연구에서는 PQC 의 보조 연산으로 사용되는 rm-encode 함수가 Cortex-M4 와 같은 MCU 환경에서 고위험 부채널 취약점을 가짐을 TVLA 를 통해 보였다. 또한 CNN 을 활용한 메시지 복원을 통해 실제로 적은 수의 트레이스만으로도 공격이 가능함을 입증하였다. 이는 부채널 취약점을 고려할 때 핵심이 되는 암호 연산뿐만 아니라 이를 보조하는 연산 또한 고려 대상에 포함해야 함을 시사한다.

ACKNOWLEDGMENT

이 논문은 2024 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (RS-2024-00442085, 자율주행 차량 서비스 보호를 위한 V2X 무선통신 인프라 보안 핵심기술 개발).

참 고 문 헌

[1] Zhao, M., & Suh, G. E. (2018, May). FPGA-based remote power side-channel attacks. In *2018 IEEE symposium on security and privacy (SP)* (pp. 229-244). IEEE.

[2] Beckwith, L., Zhou, H., Kaps, J. P., & Gaj, K. (2024, December). Power Side-Channel Key Recovery Attack on a Hardware Implementation of BIKE. In *2024 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)* (pp. 1-6). IEEE.

[3] Dewar, A., Thibault, J. P., & O'Flynn, C. (2020). NAEAN0010: Power Analysis on FPGA Implementation of AES Using CW305 & ChipWhisperer R O.

[4] 최기훈, 오충연, 김주환, 박혜진, 한동국. (2025). HW 구현 대칭키 암호에 대한 범용적 딥러닝 기반 프로파일링 부채널 분석 방안. 정보보호학회논문지, 35(1), 37-46.

[5] Huang, Z., Wang, H., Cao, B., He, D., & Wang, J. (2024). A comprehensive side-channel leakage assessment of CRYSTALS-Kyber in IIoT. Internet of Things, 27, 101331. Elsevier.