전력 IoT 기기의 안전한 운영을 위한 펌웨어 KCMVP 암호모듈 설계 및 구현에 관한 연구

홍예진, 김태훈, 김민용, 이선우, 이준영*

한전KDN㈜

hongyj_28@kdn.com, thkim_5117@kdn.com, kmyong_0902@kdn.com, hangler_sunwoo1@kdn.com, *ljy.953386@kdn.com

A Study on the Design and Implementation of Firmware KCMVP Cryptographic Module for Safe Operation of Power IoT Devices

Hong Yejin, Kim Taehun, Kim Minyong, Lee Sunwoo, Lee Junyoung*

KEPCO KDN

요 약

에너지 ICT 환경에서 사용되는 단말 기기들은 관련 법령에 의거하여 KCMVP 암호모듈 적용이 필수로 요구되고 있으나 기개발된 소프트웨어 암호모듈은 저전력·저성능 IoT 기기 환경에 적용하기에는 기술적 제약사항이 존재하여 적용할 수 없는 상황이다. 또한, 전력 IoT 기기 내 IC칩 인터페이스 제공 및 펌웨어 암호모듈의 수요가 지속적으로 증가함에 따라 임베디드 환경에 최적화된 펌웨어 형태의 암호기술 개발이 필요성이 대두되고 있다. 따라서 본 논문에서는 소프트웨어 암호모듈을 기반으로 펌웨어 형태로 포팅 및 임베디드 환경에 적용할 수 있는 방안을 설계 및 제안하고 테스트 벡터를 활용하여 검증하고자 한다.

Ⅰ. 서 론

에너지 ICT 환경에서는 국가·공공기관의 중요정보 보호를 위해 관련 법령(국가정보원법 제4조, 사이버 안보 업무규정 제9조, 전자정부법 제56조 및 시행령 제69조 등)에 의거하여 KCMVP 암호모듈 적용이 필수로 요구되면서 전력 시스템과 및 기기에 암호모듈 적용이 확대되고 있으며, 최근 전력 인프라에 사물 인터넷(Internet of Things, IoT)을 활용한 서비스가 확대되면서 임베디드에 최적화된 암호모듈 필요성이 대두되고 있다.

경량화된 운영환경에서 데이터를 수집 및 가공하는 사물 인터넷 서비스의 세계 시장 규모는 점차 커지고 있으며 다양한 산업에 활용되고 있다. 하지만 이러한 추세에 맞춰 사물 인터넷 기기를 대상으로 사이버 공격도 증가하고 있는데 사물 인터넷은 전력 소모 및 비용의 문제로 저사양 디바이스를 사용하고 있어 기존의 소프트웨어 형태의 암호모듈과 같은 높은 성능을 요구하는 보안기술의 적용에 어려움이 존재한다[1].

따라서 본 논문에서는 전력 IoT 기기 환경에서 주로 활용되는 ARM Cortex-M 프로세서에 암호기능 적용을 위해 소프트웨어 암호모듈을 최적화하여 펌웨어 형태로 포팅하여 적용할 수 있는 방안을 설계 및 제안하고 신뢰할 수 있는 테스트 벡터를 활용하여 검증한다.

Ⅱ. 본 론

2.1. 펌웨어 암호모듈

펌웨어 암호모듈은 저전력·저성능 IoT 기기와 같이 제한적인 환경에서 암호기능을 지원하기 위한 라이브러리로서 운영환경이 존재하지 않는 Cortex-M 환경에서 블록암호 및 메시지 인증, 키 설정, 해시함수, 난수발생기, 전자서명 등 보안 기능을 제공한다. 또한 IC칩에서 발생하는 잡음원을 이용하여 난수를 생성하도록 TRNG 연동과 키, 인증서를 안전하게 관리하기 위한 보안 메모리(Trust Zone)를 활용하도록 설계하였다.

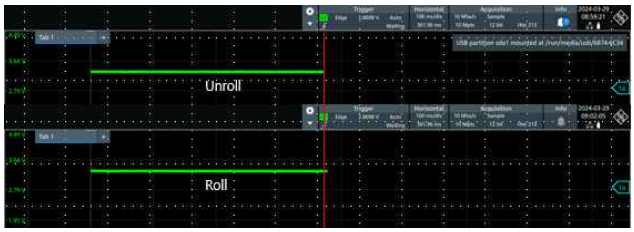
2.2. 펌웨어 암호기술 구현

2.2.1. 알고리즘 경량화

F/W 암호모듈은 특정 IC칩에 이식되어 어플리케이션의 호출에 의해 운영된다. 자원 확장이 자유로운 소프트웨어 암호모듈 동작 환경과 비교했을 때 펌웨어 암호모듈은 제한된 물리적인 환경에서 동작하기 때문에 포팅 시 암복호화 연산 속도의 영향을 최소화하면서 펌웨어 파일의 크기를 경량화할 필요가 있다. 기존 소프트웨어 암호모듈 파일을 경량화하기 위해 [그림 1]과 같이 매크로 함수를 삭제하고 루프 언롤링(loop unrolling) 기법을 롤링(rolling) 변환하여 펌웨어 암호모듈 파일 크기를 최적화하였으며 이러한 경량화 기법을 적용하였을 때 속도 저하가 발생하는지 검증하기 위해 테스트를 수행하였다.

[그림 1] 매크로 함수 삭제

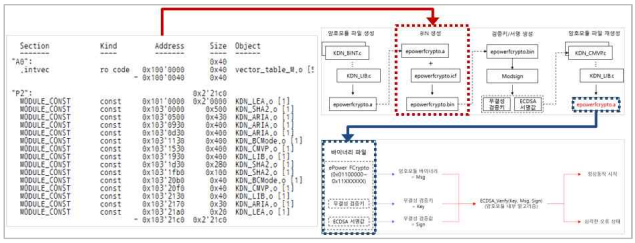
테스트 결과 암호모듈 사이즈는 약 1/5 수준으로 감소하였으며 속도 비교 결과는 [그림 2]와 같이 차이가 근소한 것으로 보아 연산 속도에 큰 영향이 없는 것을 확인했다. 이에 따라 제약된 메모리에서 펌웨어 암호기술이 구현될 수 있도록 위와 같은 암호모듈 사이즈 경량화 기법 적용을 결정하였다.



[그림 2] unroll / roll 코드 속도 비교

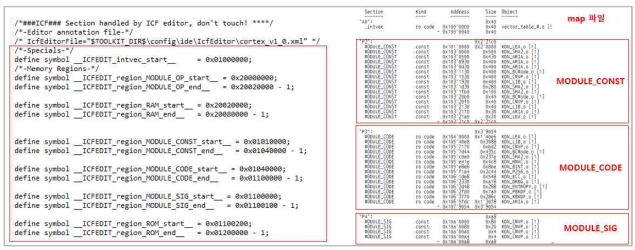
2.2.2. 펌웨어 무결성 검증

S/W 암호모듈 구현 시 사용하는 표준 C 라이브러리는 데이터가 적재되는 메모리 주소가 계속해서 변경된다. 이러한 동적 라이브러리 형태(.a)는 펌웨어 실행 간 암호모듈 무결성 검증 과정에서 해시값이 매번 변경되기 때문에 [그림 3]과 같은 무결성 검증 과정에서 정상적으로 이루어지지 않는다.



[그림 3] 펌웨어 암호모듈 무결성 검증 과정

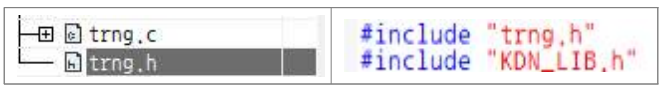
무결성 검증을 위해 라이브러리 코드 및 변수, 상수 데이터 섹션의 위치를 고정하고 해당 주소 고정 소스코드를 이용하여 암호모듈 파일을 생성하며 해당 파일에 암호모듈 바이너리, 무결성 검증키, 무결성 검증 값을 내부 암호모듈 알고리즘에 입력하여 펌웨어 암호모듈의 무결성을 검증하도록 [그림 4]와 같이 설계하였다.



[그림 4] 코드 및 데이터 섹션 정의

2.3. 칩셋 보안기능 활용(TRNG, Secure Memory)

난수발생기(RNG, Random Number Generator)는 암호모듈을 실행하는 과정에서 키 생성, 초기화 벡터(IV) 생성, 솔트 생성, 디지털 서명 등 암호 기술을 사용하기 위해 예측이 불가능한 값을 생성한다. 펌웨어 암호모듈은 IC칩에서 발생하는 잡음원을 이용하여 난수를 생성하도록 TRNG(True Random Number Generator)를 사용하게 된다[2].



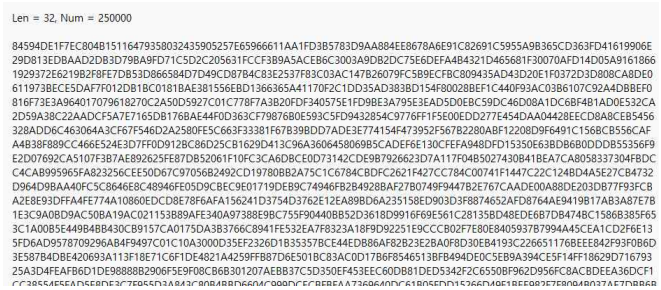
[그림 5] TRNG 파일 추가(좌) / TRNG 및 암호모듈 전처리(우)

펌웨어 암호모듈에서 난수발생기를 구현하기 위해서는 암호모듈이 적용되는 칩에서 제공하는 TRNG 영역과 연동이 필요하다. 이를 위해 [그림 6]과 같이 TRNG 라이브러리 헤더파일을 전처리하여 칩셋이 동작하는 과정에서 TRNG 초기화 및 수집한 엔트로피를 암호모듈 인자로 활용하도록 개발하였다.

```
int32_t initTrueRandom(void){
    pmc_enable_periph_clk(ID_TRNG);

    trng_disable(TRNG);

    trng_disable_writeprotect_all_regs(TRNG);

    trng_disable_interrupt(TRNG, TRNG_IDR_DATRDY | TRNG_IER_SECE | TRNG_IER_EOTPKB);

    trng_get_interrupt_status(TRNG);

    trng_enable_interrupt(TRNG, TRNG_IER_DATRDY);

    trng_enable(TRNG, sysclk_get_peripheral_hz());
  /*
    NVIC_DisableIRQ(TRNG_IRQn);
    NVIC_ClearPendingIRQ(TRNG_IRQn);
    NVIC_SetPriority(TRNG_IRQn, 0);
    NVIC_EnableIRQ(TRNG_IRQn);
*/
    return 0;
}
```

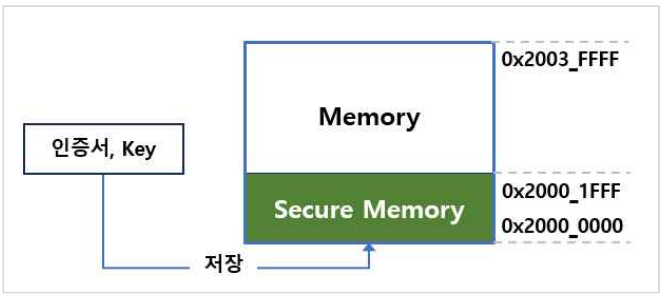
[그림 6] TRNG 드라이버 연동 구현

생성된 난수는 [그림 7]과 같이 KCMVP 검증 서비스(KISA)에서 제공하는 잡음원 수집 테스트에서 안전한 엔트로피 수집 결과를 확인하였다.



[그림 7] TRNG 기반 엔트로피 수집 결과

또한, 전력 IoT 기기에서 사용하는 IC칩은 중요정보 보호를 위해 보안 메모리(Trust Zone)를 제공하고 있으며, 인증서 및 키를 보안 메모리에 저장하여 무단 접근을 차단하고 안전하게 관리하도록 [그림 8]과 같이 설계하였다.



[그림 8] 전력 IoT 기기 메모리 구조

Ⅲ. 결 론

본 논문에서는 펌웨어 암호모듈을 설계 및 시험하여 전력 IoT 기기를 위한 암호모듈 구현 방안을 검증하였다. 암호모듈 적용 시 전력기기 및 전력망에서 통신되는 데이터에 강화된 보안 기능을 제공할 수 있을 것으로 기대한다. 향후 연구에서는 전력 IoT 기기에서 사용하는 다양한 칩셋 환경에 펌웨어 암호모듈을 이식하여 검증하고자 하며 KCMVP 인증 취득을 통해 전력 인프라에 안전한 통신환경을 제공하고자 한다.

참 고 문 헌

[1] 지장현(2022), “사물인터넷 디바이스 하드웨어 보안”, 한국정보보호학회 한국정보보호학회지 제32권 제2호, 51-58p

[2] 오상준(2015), “하드웨어 칩기반 TRNG 설계 및 분석”, 한양대학교 석사학위논문, 1p