경량 암호 CHAM을 사용한 암호학적 난수발생기 구현

유현도[2], 임형신[2], 강주성[1,2], 염용진[1,2]*
국민대학교 정보보안암호수학과[1] / 금융정보보안학과[2]
{dbguseh111, kuunh2, jskang, *salt}@kookmin.ac.kr

An Implementation of Cryptographic Random Number Generator Using Light-weight Cipher CHAM

Hyeondo Yoo[2], Hyoungshin Yim[2], Ju-Sung Kang[1,2], Yongjin Yeom[1,2]*
Dept. of Information Security, Cryptology, and Mathematics[1]/
Financial information security[2], Kookmin Univ.

요 약

BEMS는 시스템 내부에서 서버와 경량 IoT 기기와의 통신에 암호시스템을 사용하며, 모든 암호시스템은 안전한 난수를 생성하는 난수발생기가 존재한다는 전제하에 설계된다. 따라서, IoT 기기에서 동작하는 경량 환경에 적합한 난수발생기에 관한 연구가 필요하다. 본 논문은 경량 블록암호 CHAM을 사용하는 CTR_DRBG를 구현하여, PC와 경량 환경에서 성능을 비교 분석한다. CHAM을 사용하는 CTR_DRBG는 AES를 사용하는 CTR_DBRG보다 PC에서는 약 3.2배, 경량 환경에서는 약 4.1배의 더 좋은 성능을 가지며, 이를 통해 경량 환경에서 CHAM을 사용하는 CTR_DRBG가 적합함을 확인한다. 마지막으로 경량 환경인 NVIDIA Jetson Nano 보드에서 구현한 CHAM을 사용하는 CTR_DRBG를 BEMS에서 활용할 수 있는 방향을 제시한다.

Ⅰ. 서 론

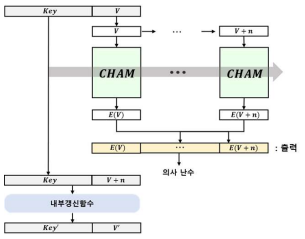
IoT(Internet of Things)는 무선 통신을 통해 각종 사물을 연결하는 기술이며, IoT 시장 규모는 계속 커지고 있다. 경량 IoT 기기를 통신에 적용하여 사용하기도 하는데[1], 건축물의 에너지를 효율적으로 관리하기 위한 시스템인 BEMS(Building Energy Management System)에서도 BEMS 서버와 통신하는 분산자원 건전성 관리 플랫폼으로 경량 IoT 기기를 사용한다[2]. 서버와 경량 IoT 기기 간의 통신에 암호통신 시스템이 필요하며, 모든 암호통신 시스템은 암호학적으로 안전한 난수를 출력하는 난수발생기가 있다는 가정하에 설계된다. 따라서, 자원이 제한적인 경량 IoT 기기에서는 메모리 사용량을 최소화하면서도 암호학적으로 안전한 난수발생기의 사용이 필요하다.

미국 NIST(National Institute of Standards and Technology) SP 800-90A는 결정론적 난수발생기(Deterministic Random Bit Generator, DRBG)의 구조를 제시하는 대표적인 국외 표준문서이다[3]. SP 800-90A에는 해시함수(hash function), HMAC, 블록암호(block cipher)를 기반으로 한 DRBG의 메커니즘이 작성되어 있다. CTR_DRBG에서 사용하는 블록암호로는 AES, LEA 등의 국내외 표준 블록암호를 사용할 수 있고, SP 800-90A에서는 AES에 기반한 CTR_DRBG의 사용을 권고한다.

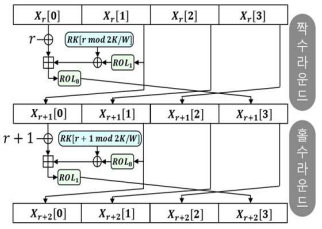
본 논문에서는 국내 경량 블록암호 알고리즘인 CHAM을 CTR_DRBG의 블록암호로 사용하여 경량 환경에 적합한 난수발생기를 제시한다. 또한, PC와 경량 환경에서 AES를 사용하는 CTR_DRBG(이하, AES_CTR_DRBG)와 CHAM을 사용하는 CTR_DRBG(이하, CHAM_CTR_DRBG)의 성능을 비교 분석한다. 이를 통해, 경량 환경에는 제시한 CHAM_CTR_DRBG를 사용하는 것의 적합함을 확인한다. 마지막으로 BEMS 내부에서 BEMS 서버와 경량 IoT 기기 간의 암호화된 통신에 CHAM_CTR_DRBG의 활용 가능성을 제시하며 결론을 내린다.

Ⅱ. CHAM 기반 CTR_DRBG

CTR_DRBG는 엔트로피 소스(entropy source)를 입력으로 사용하여 내부갱신함수(update function)와 출력생성함수(generate function)를 통해 의사 난수를 출력한다. CTR_DRBG의 주요 파라미터로는 블록암호의 암호키 역할을 하는 내부상태 Key와 블록암호의 평문으로 사용되는 내부상태 V가 있다. 내부갱신함수는 블록암호를 사용하여 Key와 V를 갱신한다. [그림 1]에서 보이는 바와 같이, 출력생성함수는 Key와 V를 블록암호에 사용하여 의사 난수를 생성한 후, 내부갱신함수를 통해 내부상태를 갱신한다.



[그림 1] CHAM_CTR_DRBG 출력생성함수의 동작 과정[4]



[그림 2] 경량 블록암호 CHAM의 2라운드 동작 과정

본 논문에서는 일반적으로 CTR_DRBG에 사용되는 블록암호인 AES 대신 경량 블록암호 CHAM을 사용한다[5]. 2017년 국가보안기술연구소에서 개발한 CHAM은 ARX(Addition Rotation XOR) 구조를 가지며, 128비트 크기의 평문과 키를 사용하여 128비트 크기의 암호문을 생성한다. CHAM 암호화의 라운드 수는 80이며, [그림 2]에서 보이는 바와 같이 라운드 수가 홀수일 때와 짝수일 때 동작 과정이 다르다.

Ⅲ. CTR_DRBG 성능 측정

성능 측정 실험에서는 두 블록암호 CHAM과 AES를 32비트 단위로 구현된 암호화 과정의 사용되는 메모리를 계산한다. PC와 경량 환경에서 블록암호의 암호화 과정에 대한 속도를 측정하고, CHAM_CTR_DRBG와 AES_CTR_DBBG의 성능을 비교하여 분석한다.

3.1 블록암호의 사용 메모리 비교

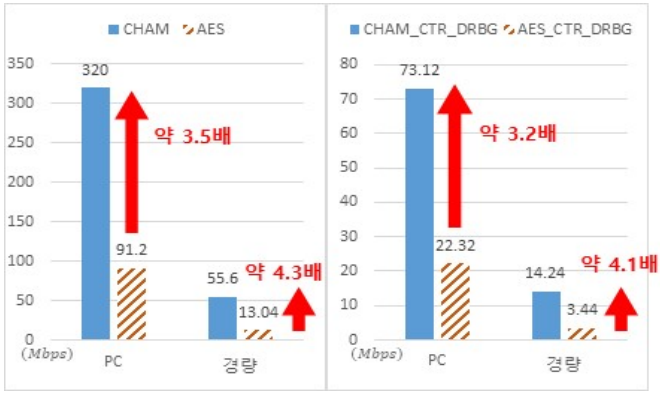
<표 1>은 AES와 CHAM이 암호화 과정에서 사용하는 메모리양을 계산한 결과이다. CHAM은 총 640비트를 사용하는 반면, AES는 CHAM의 약 57배의 해당하는 36,688비트의 메모리를 사용하였다. 이를 통해, CHAM이 AES보다 메모리 자원이 제한적인 경량 환경에 적합함을 확인하였다.

<표 1> 블록암호의 암호화 과정에 필요한 메모리(비트 단위)

파라미터	AES	CHAM
입·출력 크기	128	128
키 크기	128	128
라운드 키	1,408	256
S-box	2,048	-
Table	32,768	-
라운드 상수	80	-
총 메모리	36,688 ≈ 4.5KB	640 ≈ 0.08KB

3.2 블록암호 및 CTR_DRBG의 성능 측정 결과

성능 측정은 PC와 경량 환경인 NVIDIA Jetson Nano 보드에서 진행한다. PC는 6개의 코어를 가진 Intel core i7-8086K CPU를 사용하고, Jetson Nano 보드는 4개의 코어를 가진 Quad-core ARM Cortex-A57을 사용한다.



[그림 2] (좌) 블록암호의 속도 측정 (우) CTR_DRBG 속도 측정 (PC, 경량 환경(보드))

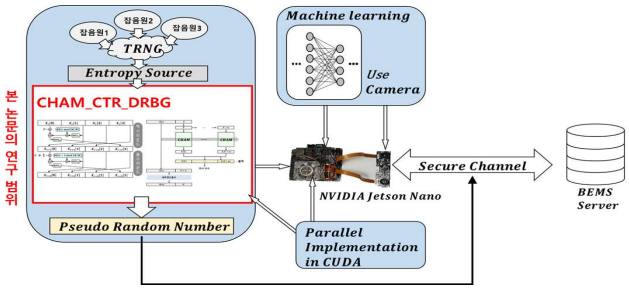
[그림 2]의 왼쪽 그래프는 PC와 경량 환경에서 AES와 CHAM의 암호화 과정을 통해 1초당 128 비트 크기의 암호문을 생성하는 속도를 보여준다. 속도 비교를 통해 PC에서는 CHAM이 AES보다 약 3.5배, 경량 환경에서는 약 4.3배 좋은 성능을 가지는 것을 확인하였다. PC보다 경량 환경에서 CHAM과 AES의 성능 차이가 큰 것은 CHAM의 주요 연산인 비트 순환 연산이 경량 환경에서 사용한 ARM에 내장된 Barrel Shifter 함수를 통해 효율적으로 실행되었기 때문이라 여긴다[5].

PC와 경량 환경에서 CHAM_CTR_DRBG와 AES_CTR_DRBG의 1초당 64 바이트 크기인 난수 출력 속도가 [그림 2]의 오른쪽 그래프에 나타나 있다. 이 결과를 분석하면 다음과 같다. PC에서 CTR_DRBG 동작 과정에서 AES가 차지하는 비율은 86%이다. CHAM이 AES보다 약 3.5배 좋은 성능을 가지기 때문에, CTR_DRBG에서 AES 대신 CHAM을 사용하면 약 3배의 성능 향상이 이루어질 것이라고 예상한다. CHAM_CTR_DRBG의 성능이 약 3.2배로 예상과 유사하게 향상됨을 확인한다. 경량 환경에서 AES가 CTR_DRBG 동작 과정에서 차지하는 비율은 93%이며, CHAM_CTR_DRBG가 AES_CTR_DRBG보다 약 3.5배 좋은 성능을 보일 것이라고 예상한다. 실험 결과, CHAM_CTR_DBRG는 약 4.1배 향상된 속도를 가지며, 예상한 결과보다 나은 성능을 가지는 것을 통해 실험의 타당성을 확인한다.

3.1절의 사용 메모리 크기를 비교한 결과와 위 실험 결과를 통해 자원이 제한적인 경량 환경에서는 CHAM을 사용한 CTR_DRBG가 적합함을 확인하였다.

Ⅳ. CHAM_CTR_DRBG 및 Jetson Nano 보드의 활용 시나리오

BEMS 상에서 IoT 기기가 건물 내의 데이터를 기계학습을 통해 분석하여 현재 에너지가 최적화되어 사용되고 있는지를 검사하는 연구가 진행되고 있다[2]. [그림 3]에서 보이는 바와 같이, NVIDIA Jetson Nano 보드는 카메라를 사용하여 기계학습을 할 수 있는 경량 IoT 기기이므로, BEMS 내에서 분산자원 건전성 관리 플랫폼으로 활용될 수 있다. 암호통신에서 난수발생기는 필수적 요소이므로, 본 논문에서 경량 환경에 적합하다고 확인한 CHAM_CTR_DRBG는 경량 IoT 기기인 Jetson Nano 보드에서 동작하는 난수발생기로 활용될 수 있다.



[그림 4] BEMS 내에서의 CHAM_CTR_DRBG 및 Jetson Nano 보드의 활용 시나리오

Ⅴ. 결론

PC와 경량 환경에서 AES와 CHAM의 암호화 과정과 이를 사용하는 CTR_DRBG의 성능을 분석하였다. 실험 결과를 통해, CHAM_CTR_DRBG가 경량 환경에서 최대 4.1배 좋은 성능을 가지기 때문에, 경량 환경에서는 CHAM을 사용하는 CTR_DRBG가 적합하다. 마지막으로 CHAM_CTR_DBRG가 경량 IoT 기기인 Jetson Nano 보드와 BEMS 서버 간의 암호통신에 활용될 수 있음을 제시하였다.

향후, 잡음원과 난수발생기의 출력에 대한 안전성 연구가 진행된다면, BEMS에서 이뤄지는 경량 IoT 기기와 서버 간의 통신에 안전한 암호시스템을 적용할 수 있을 것으로 사료된다.

ACKNOWLEDGMENT

이 성과는 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2021M1A2A2043893)

참 고 문 헌

[1] 김선태 외 3명, "경량 IoT 디바이스 플랫폼 동향 연구" 한국정보기술학회, December 2015.

[2] Zhishu Shen., et al., "In-Network Self-Learning Algorithms for BEMS Through Collaborative Fog Platform." IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), May 2018.

[3] NIST, "Recommendation for Random Number Generation Using Deterministic Random Bit Generators." SP 800-90A Rev.1, June 2015.

[4] 한국정보통신기술협회, "결정론적 난수발생기 - 제1부- 블록암호 기반 난수발생기.", 정보통신단체표준 TTAK.KO-12.0189/R1, June 2015.

[5] Bonwook Koo., et al., "CHAM: A Family of Lightweight Block Ciphers for Resource-Constrained Devices," Information Security and Cryptology - ICISC, December 2017.