2018년 정보보호학술논문발표회

효율적인 한국 암호 모듈 검증 제도를 위한 암호 모듈 자동 검증 시스템

박태환* 안규황** 권혁동** 서화정** 김호원*†

*부산대학교 대학원 전기전자컴퓨터공학과

**한성대학교 대학원 정보시스템공학과

Automatic Cryptographic Module Verification System for Efficient Korean Cryptographic Module Verification System

Taehwan Park* Kyuhwang An** Hyeokdong Kwon*
Hwajeong Seo** Howon Kim*†

*Department of Electrical and Computer Engineering, graduate school of Pusan National University.

**IT Department, graduate school of Hansung University.

요 약

최근 ICMC 2018 미국 국립표준연구소(NIST)에서 암호 모듈 자동 검증 도구 개발 내용에 대한 발표가 있었으며, 이를 위한 ACVP(Automated Cryptographic Validation Protocol)을 제시하고 있다. 이를 통한 암호 모듈 검증의 효율성 강화가 기대되고 있다. 암호 모듈 검증과 관련된 이러한 변화에 맞추어 본 논문은 암호 모듈 검증 효율성 강화를 위한 한국형 암호 모듈 자동 검증 시스템을 제시하며, 국산 해시함수 LSH-224/256/384/512와 블록암호 LEA-128/192/256 ECB, CBC, CTR 모드에 적용하였다.

I. 서론

오늘날, 암호 모듈 검증 제도는 미국 국립표준연구소(NIST)와 캐나다 통신보안기구(CSE)를 중심으로 CMVP(Cryptograph Module Validation Program)이 활발히 이루어지고 있다. 암호 모듈 구현 적합성 검증은 검증대상 암호 알고리즘 유형 및 특성에 따라 시험검증이 이루어지며, 대칭키 암호의 경우, KAT(Known Answer Test), MMT(Multiple Message Test), MCT(MonteCarlo Test)등을 수행하게 된다. 암호 모듈 구현 적합성 검증 시, 시험기관은 벤더(시험신청기관)에서 요청한 검증대상 암호 알고리즘 별 구현 적합성 확인 파일(Facts 파일), 구현 적합성 요청 파일(Request 파일), 구현 적합성 답변 파일(Response 파일)을 바탕으로 구현 적합성 검증을 실시하며, 시험기관과 벤더 간의 상호 요청 및 대응, 검증 기간이 필요하게 되며, 구현 적합성 검증에 있을 경우, 벤더에서 수정 작업 수행하는 시간 또한 필요하게 된다. 이러한 문제를 해결하고, 암호 모듈 검증 제도의 효율성 강화를 위해, 미국 NIST에서는 ACVP 및 관련 사항을 구축하고 있으며, 이에 대한 내용을 ICMC 2018에서 발표하였다.

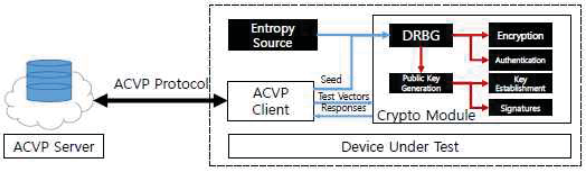
ACVP와 같은 암호 모듈 검증제도의 효율성 강화 연구 동향을 바탕으로 본 논문은 한국 암호 모듈 검증 제도의 효율성 강화를 위한 한국형 암호 모듈 자동 검증 시스템을 제시하고자 한다.

II. 관련 연구 및 동향

2.1. ACVP

ACVP(Automated Cryptographic Validation Protocol) [1]은 미국 NIST에서 주도하여 개발 중인 자동화 암호 검증 프로토콜이다. 최근 급속한 ICT 기술 발전으로 인해, 암호 모듈 검증 신청 건수의 급증으로 기존의 인적 자원 기반의 암호 모듈 검증에 있어 시간 지연 및 어려

움이 발생함에 따라 이를 해결하기 위한 방안으로 연구 개발 중에 있다. 그림 1은 NIST ACVP의 서버 클라이언트 구조를 나타낸다.



Fig, 1. NIST CAVP 서버-클라이언트 구조

그림 1에서 ACVP 서버는 Web 호스트 서비스를 제공하며, 검증 대상 암호 알고리즘 별 ACV 프로토콜에서 정해진 JSON 포맷에 따라 테스트벡터(기존 암호 모듈 구현 적합성 검증 시, FACTS 파일과 REQUEST 파일에 해당)를 생성한다. 그리고 ACV Protocol을 기반으로 ACVP 클라이언트에서 전달 받은 테스트벡터 수행 결과물(기존 암호 모듈 구현 적합성 검증 시, RESPONSE 파일에 해당)에 대한 검증 기능을 수행한다.

2.2. KCMVP

그림 2는 KCMVP(Korea Cryptography Module Validation Program)에 있어 벤더의 검증대상 구현 결과물에 대한 암호 알고리즘 시험 방식을 나타내고 있다. 아래의 그림에서 시험 기관은 KCMVP에서 검증대상 암호 알고리즘 별 구현 적합성 검증을 위한 FACTS 파일(벤더로부터 받은 RESPONSE 파일 검증 확인용), REQUEST 파일(벤더에게 전달하여 벤더의 암호 알고리즘 구현 적합성 확인을 위한 키, 평문, 초기화 벡터 등의 정보를 가지고 있음)들을 가지고 있다. 시험 기관은 KCMVP를 신청한 벤더들 중 암호 구현 적합성 검증이 필요한 벤더에게 REQUEST 파일을 전달하며, 벤더는 이에 대한 RESPONSE 파일을 생성하여 시험 기관에 제출한다. 이후, 시험기관은 벤더로부터 전달 받은 RESPONSE 파일에 대해 검증도구(KCAVS)를 활용하여 FACTS 파일과 비교 검증을 수행하게 된다. 이러한 일련의 과정에 있어 벤더 측에서 시험 기관의 REQUEST 파일에 대한 RESPONSE 파일 생성하는데 소요되는 시간, 시험 기관 측에서의 구현 적합성 검증 결과가 벤더의 구현물에 대한 구현 적합성 문제가 있는 경우, 벤더 측에 전달 및 벤더 쪽에서 구현 결과물 수정에 있어서 시간이 소요되게 된다는 문제점을 가지고 있다. 따라서 KCMVP의 전반적인 효율성 강화를 위해 이러한 문제점 해결이 필요할 것으로 보인다.

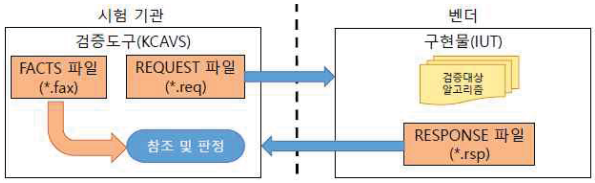


Fig. 2. KCMVP 암호 알고리즘 시험 방식

III. 제안 기법

미국 NIST는 암호 모듈 검증 제도의 효율성 강화를 위한 ACVP[1]를 개발 중에 있으며, 관련 제도상에 적용할 예정이다. 그러나 한국 암호 모듈 검증제도[2]의 경우 벤더 측에서 검증하는데 소요시간이 많이 걸린다는 문제점을 가지고 있다. 이러한 문제점을 해결하기 위해, 본 논문에서는 KCMVP의 효율성 강화를 위한 한국형 암호 모듈 자동 검증 시스템을 제안하며, 국산 해시함수 LSH-224/256/384/512와 블록암호 LEA-128/192/256 ECB, CBC, CTR 모드에 대하여 각각 실제로 적용하였다.

3.1. 제안 시스템 구조 및 동작 원리

그림 3은 제안 시스템의 구조를 나타내고 있다. 시험 기관 쪽에서는 제안 시스템을 웹 서버 형태로 운영한다. 제안하는 시스템에서 지원하는 검증 대상 암호 알고리즘 유형 별 FACTS, REQUEST 파일 생성 기능, 벤더 측에서의 검증 대상 암호 알고리즘 구현 물 업로드 기능, 벤더 구현 물 검증 및 검증 결과 송신 기능을 제공한다. 제안 시스템 상에서의 검증 대상 암호 알고리즘 유형 별 FACTS, REQUEST 파일 생성 기능은 벤더 측에서 구현 적합성 검증을 하고자하는 검증 대상 암호 알고리즘 유형을 선택함으로써, 해당하는 검증 대상 암호 알고리즘 유형에 맞는 FACTS, REQUEST 파일들이 생성된다.

제안 시스템 상에서의 벤더 측에서의 검증

대상 암호 알고리즘 구현 물 업로드 기능은 제안 시스템에서 허용하는 파일 유형(.zip, .c, .h 파일)에 맞춰진 벤더측 검증 대상 암호 구현물을 업로드 하는 기능을 제공한다. 파일 업로드 시, 웹 서버 측에서는 허용하는 포맷의 파일만 업로드가 가능하다.

마지막으로 제안 시스템 상에서의 벤더 측 구현 물에 대한 검증 및 검증 결과 송신 기능은 앞선 구 현물 업로드 기능을 통해 받은 벤더 구현 물에 대해 .zip 파일인 경우, 압축 해제를 실시하며, .c/.h 파일에 대한 컴파일 및 컴파일 결과물을 실행한다. (벤더 구현 물은 기존에 정해진 REQUEST, RESPONSE 파일 양식을 따른다는 가정) 벤더 측 구현 결과물에 대한 실행을 통해 얻은 RESPONSE 파일들과 기존에 생성된 FACTS 파일과의 비교를 통한 구현 적합성 검증을 실시하며, 이에 대한 결과를 웹상에 알려주는 기능(결과 송신)을 수행하게 된다.

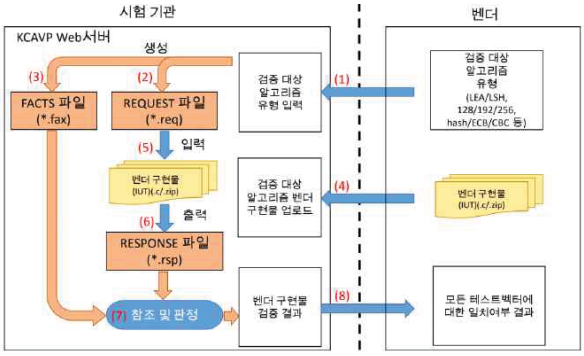


Fig. 3. 제안 시스템 구조

표 1은 본 제안 시스템 상에서 지원하는 검증 대상 암호 알고리즘을 나타내고 있다.

Table. 1. 제안시스템 상에서 지원하는 검증대상 암호 알고리즘

지원 검증대상 암호 알고리즘 유형			지원 검증대상 암호 알고리즘 명
비밀키	블록암호		LEA-128/192/256
	블록암호 운영모드	기밀성	ECB, CBC, CTR
해시함수			LSH-224/256/384/512

LEA-128/192/256 블록암호의 ECB, CBC, CTR 운영 모드를 지원하고 있으며, LSH-224/256/384/512 해시 함수를 지원하고 있다. 관련 테스트 유형으로는 블록암호에 대한 KAT(Known Answer Test) 기능과 해시함수에 대한 짧은 길이의 메시지, 긴 길이의 메시지, 임의의 길이에 대한 메시지 테스트를 지원한다.

3.2. 제안 시스템 동작 결과

그림 4는 제안 시스템의 메인 화면을 나타내고 있다. 제안 시스템의 메인화면에서 사용자가 선택한 검증대상 알고리즘 유형에 따라 화면이 변경된다. 사용자는 구현 적합성 검증을 받고자 하는 암호 알고리즘의 유형, 출력 비트, 운영모드 등을 선택한 후, Send to Server 버튼을 클릭하게 되면, 서버에서 해당하는 검증대상 암호 알고리즘에 대한 FACTS, REQUEST 파일을 생성하게 된다. 검증대상 암호 알고리즘에 대한 FACTS, REQUEST 파일을 요청한 이후 웹 서버 하단의 파일 업로드를 통해, .zip, .c, .h 파일을 업로드 할 수 있으며, 사용자(벤더)에서 업로드한 구현물에 대한 컴파일 수행 시 컴파일 에러가 발생하는 경우 컴파일 에러 알림 기능과 메인 페이지로 돌아가는 버튼을 제공한다.

Fig. 4. 제안 시스템 메인화면(LEA 블록암호)

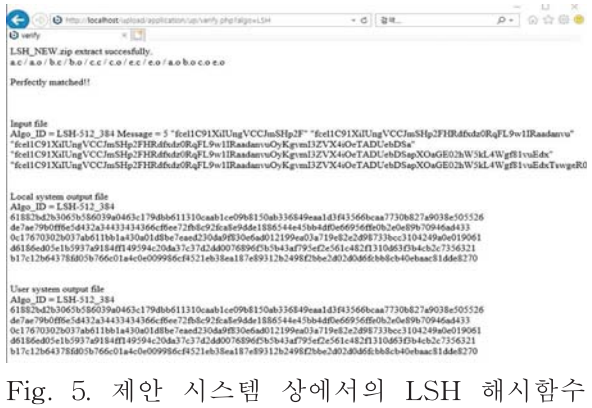


Fig. 5. 제안 시스템 상에서의 LSH 해시함수 수행 결과 비교 검증 화면

그림 5는 사용자(벤더 측)에서 LSH-512/384 해시 함수에 대한 구현 적합성 검증을 요청하여, 구현 결과물을 .zip 파일 형태로 업로드한 후, 서버측에서 구현물 컴파일/수행을 통해 얻은 RESPONSE 파일과 사용자 요청에 따라 미리 생성된 FACTS 파일과의 구현 적합성 비교 검증 결과를 알려주는 화면이다.

IV. 제안 방식 평가 및 비교

사용자(벤더) 및 시험 기관 측면에서의 효율성 강화 측면, 다양한 유형의 암호 모듈 적용 가능성 측면, 한국 암호 모듈 검증 제도 적용 가능성 관점에서 본 논문에서 제안하는 방식과 기존 관련 연구 및 방식간의 비교를 진행하였다.

Table. 2. 기존 관련 연구 및 방식과의 비교

연구 방식	사용자 효율성 강화	시험 기관 효율성 강화	다양한 유형의 암호 모듈 적용 가능성	한국 암호 모듈 검증 제도 적용 가능성
ACVP	O	O	O	X
KCMVP	-	-	O	O
제안 기법	O	O	X	O

미국 NIST의 ACVP는 사용자(벤더), 시험기관 측면에서의 효율성 강화와 다양한 유형의 암호 모듈 적용 가능성이 높다. 하지만 한국 암호 모듈 검증제도(KCMVP)와 검증 대상 암호 알고리즘과 제도적 측면에서 차이가 있기 때문에 적용이 불가능하다는 단점을 가지고 있다.

KCMVP에서의 암호 모듈 구현 적합성 검증 방식은 다양한 유형의 암호 모듈 적용이 가능하며, 한국 암호 모듈 검증 제도(KCMVP)에서의 검증 대상 암호 알고리즘에 대한 구현 적합성 검증이 가능함으로써 적용이 가능하다는 장점을 가지지만, 현재의 암호 모듈 구현 적합성 검증에 있어서 사용자(벤더) 측에서의 구현 적합성 검증 및 검증 결과에 따른 수정 보완 작업에 있어서 많은 시간이 소요된다는 단점을 가지고 있다.

본 논문에서의 제안 기법은 웹 서버 형태의 암호 모듈 구현 적합성 검증 시스템을 통해, 사용자(벤더) 측에서 구현 적합성 검증을 받고자 하는 암호 알고리즘에 대한 구현 적합성 검증 및 검증 결과를 받을 수 있으며, 이를 통해 기존 방식에 비해 사용자(벤더) 측면에서의 수정 및 보완 작업의 시간을 줄일수 있다는 장점(사용자 측면에서의 효율성 강화)과 시험기관 측면에서는 시험 검증 신청 벤더별 구현 적합성 검증 수행 및 벤더 측에서 알리는 시간을 절약할 수 있다는 장범이 있으며, LEA 블록암호와 LSH 해시함수에 대한 구현 적합성 검증 기능을 제공함으로써 KCMVP에 적용이 가능하다. 하지만 PC환경에 대한 암호 소프트웨어 모듈 외의 타 유형의 암호 모듈에 대해 지원하지 않는다는 단점이 있다.

V. 결론

본 논문에서는 미국 NIST의 ACVP와 한국 암호 모듈 검증 제도(KCMVP)에 대한 연구를 살펴보았으며, 시험 기관과 사용자(벤더) 간의 암호 모듈 구현 적합성 검증 시, 시간이 많이 소요된다는 문제점을 해결하기 위해 본 논문에서는 웹 서버 기반의 암호 모듈 구현 적합성 검증 시스템을 제안하였다.

제안하는 기법은 벤더별 구현 적합성 검증 수행 및 벤더 측에서 알리는 과정에서 소요되는 시간을 절약할 수 있다는 장점을 통해, 효율적인 암호 모듈 구현 적합성 검증이 가능해진다. 본 논문에서 제안하는 시스템의 소스는 Github[1]에서 확인할 수 있으며, LSH와 LEA에 실제로 적용하여 동작 수행하는 동영상은 Youtube[2]에서 확인이 가능하다.

[참고문헌]

[1] NIST, "Automated Cryptographic Validation Protocol(ACVP)", https://github.com/usnistgov/ACVP, June 2018.

[2] National Intelligence Agency, "Cryptographic Module Vlidation", http://www.nis.go.kr/AF/1_7_3_1.do

1) Github: https://github.com/kyu-h/Kcryptoforum_CAVP

2) Youtube: https://youtu.be/e-cjDbVDOcw