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

박태환* 안규황** 권혁동** 서화정** 김호원*†
*부산대학교 대학원 전기전자컴퓨터공학과
**한성대학교 대학원 정보시스템공학과

요 약

● 최근 ICMC 2018 미국 국립표준연구소(NIST)에서 암호 모듈 자동 검증 도구 개발 내용에 대해 발표

● 한국의 경우 암호 모듈을 개발할 경우 시험 기관과 벤더(사용자) 간 대조 작업을 통해 구현 적합성을 판단

연구 목적

● 미국 NIST에서 주도하여 개발 중인 자동 암호 검증 프로토콜을 국산 암호에 맞게 도입하고자 함

● 적합성 검증에 있어, 옳게 구현 하였는지 확인하는데 오랜 시간이 소모 됨

● 검증하는 사람이 다수건을 처리하는데 오랜 시간이 소요되며, 암호구현 적합성 검증에 대한 자동화로 해결

연구 방법

- 기존에 제안 된 NIST와 국내에서 검증하는 방법에 대한 비교 분석

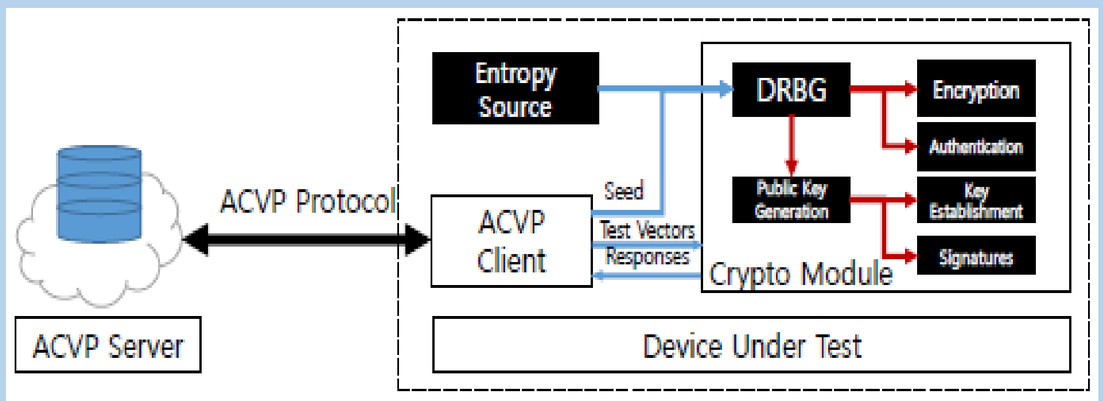

Fig. 1. NIST CAVP 서버-클라이언트 구조

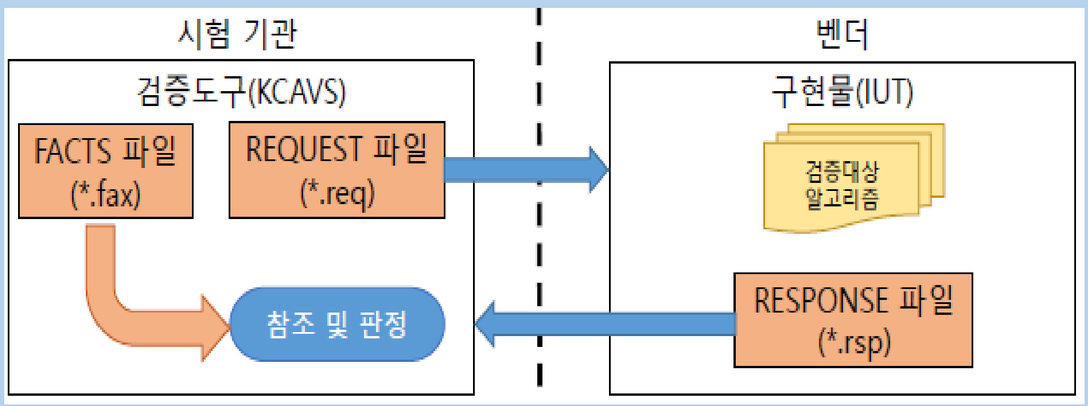

Fig. 2. KCMVP 암호 알고리즘 시험 방식

연구 결과

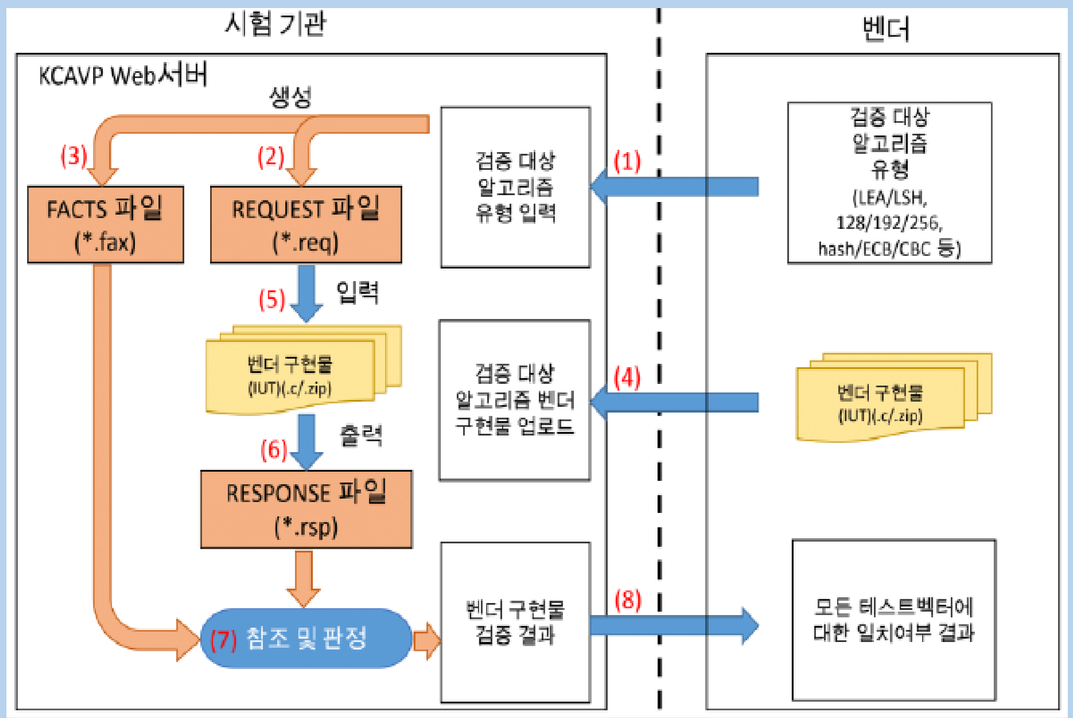

Fig. 3. 제안 시스템 구조

① 벤더측에서 시험 기관에 검증 받고자하는 알고리즘 유형을 선택해 전송
② 시험 기관은 입력 된 알고리즘 유형에 맞는 REQUEST 파일을 생성
③ 시험 기관은 자체적으로 가지고 있는 검증 된 알고리즘을 통해 REQUEST 파일 기반의 출력 파일인 FACTS 파일을 생성
④ 벤더측에서 구현한 벤더 구현물을 ‘.C, .h, .zip’의 형태로 시험 기관에 제출
⑤ 시험 기관에서는 벤더 측에서 제출한 구현물에 기존에 만들어 놓은 REQUEST 파일을 입력 값으로 대입
⑥ 벤더 측 구현물에 대한 RESPONSE 파일 생성
⑦ 벤더측에서 구현 값에 대한 RESPONSE 파일과 시험 기관측 구현 값에 대한 FACTS 파일을 비교 분석
⑧ 벤더측에게 구현 적합성에 대하여 통보

결 론

● 미국 NIST의 ACVP와 한국 암호 모듈 검증 제도(KCMVP)에 대한 연구들을 살펴 봄

● 시험 기관과 벤더간의 암호 모듈 구현 적합성 검증시, 많은 시간이 소요 된다는 문제점을 해결

● 사람이 관여해서 검증하는 시스템이 아닌 컴퓨터에 의해 자동으로 검증하는 시스템을 제안

Github: https://github.com/kyu-h/Kcryptoforum_CAVP / Youtube: https://youtu.be/e-cjDbVDOcw