모바일 단말용 KCMVP 암호모듈 구현을 위한 멀티스레드 병렬 처리 시험 도구 개발

장근서, 윤승환, 이옥연*

국민대학교, 국민대학교*

{jangks23, schneeleopard, oyyi*}@kookmin.ac.kr

A development of a test tool based on multithreading-based parallel processing for a KCMVP-approved cryptographic module for mobile devices

Keunseo Jang, Seunghwan Yun, Okyeon Yi*

Kookmin Univ., Kookmin Univ.*

요 약

국내에는 국가정보통신망에서 소통 또는 저장되는 비밀이 아닌 업무자료를 보호하기 위하여, 국가 또는 공공기관에서 도입하는 암호모듈의 안정성과 구현 적합성을 검증하는 암호모듈 검증제도가 있다. 이 암호모듈은 비밀이 아닌 업무자료를 보호하는 목적으로 정보의 유출, 위조 또는 변조, 훼손 등을 방지하기 위한 기밀성, 무결성, 인증, 부인방지 등의 기능을 제공하는데, 이러한 기능들을 검증하기 위하여 암호 알고리즘 구현적합성 시험을 수행한다. 본 논문은 이 시험을 위하여 암호모듈 시험기관에서 제공하는 테스트 벡터에 대한 응답 파일을 작성하는 과정에서 처리 속도를 향상하기 위한 방법을 고안하고 구현한 결과를 제공한다.

Ⅰ. 서론

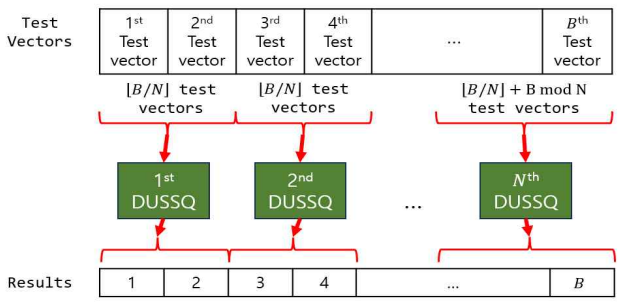
암호 알고리즘 구현적합성 시험(Cryptographic Algorithm Validataion Program, CAVP)은 암호모듈에 탑재된 암호 알고리즘의 입력에 따른 정확한 답을 출력하는지에 관한 정확성을 판단하기 위한 시험이다. 국내에서는 관련 법령에 따라 암호모듈 검증제도(Korea Cryptographic Module Validation Program, KCMVP)를 운영한다.[1] 벤더가 개발한 소프트웨어, 펌웨어, 하드웨어, 또는 이들을 조합한 하이브리드 형태의 암호모듈에 탑재된 암호 알고리즘이 비밀로 분류되지 않은 업무자료를 보호하기 위하여 잘 구현되었는지 암호모듈 보안 요구사항을 만족하는지에 대한 시험 제도를 마련해 시험/검증함으로써 향후 암호 알고리즘의 취약점이 발견된 경우 국가 차원에서 쉽게 대응할 수 있도록 제도를 마련하여 시행하고 있다.[2]

이러한 암호모듈은 모듈이 제공하는 암호 서비스를 정상 동작하는 것 뿐만 아니라 고성능이 요구되는 환경에서 암호모듈의 확장 운영을 통하여 안전성과 안정성을 모두 제공할 수 있는 운영환경이 제공되어야 한다. 이러한 운영환경 최근 자율주행 자동차나 인공지능 서비스가 개발 및 보급됨에 있어 데이터가 대용량화되고 복잡해짐에 따라 이를 빠르게 처리해야 하는 이슈와, 공격자에 의해 도청이나 변형되지 않도록 해야 하는 보안 이슈가 결합하여 암호모듈 운영환경이 암호 시장에서의 경쟁력을 키우는 데에 중요한 요소로 평가될 것이다.

본 논문에서는 차세대통신 환경의 모바일 단말에 적용하는 양자 엔트로피 칩 기반의 암호모듈 DUSSQ(Different Units Same Security with Quantum-based entropy chip)를 기반으로, 암호모듈 시험기관에서 제공하는 테스트 벡터를 사용하여 'DUSSQ CAVP 시험 도구' 상에서 작동하는 멀티스레드 기반 병렬 처리방식이 적용된 프로그램을 통해 멀티스레드 기반 병렬 처리방식을 제안하고 이를 구현한 결과를 제공한다.

Ⅱ. 본론

암호모듈의 운영자는 모듈이 정상 동작하는 동안 CAVP 시험을 위하여, 여러 개의 테스트 벡터들이 입력으로 주어질 때의 모든 입력들을 처리하기까지의 수행시간에 대해 고려해야 한다. 단순히 입력된 테스트 벡터들에 대해 암호모듈의 개수에 맞추어 순차적으로 적당히 나누어 분배하여 입력하는 방식은 시험 수행시간 면에 있어서 손해를 볼 수 있다.



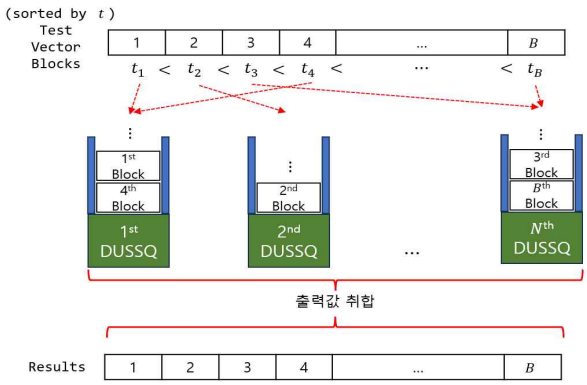
[그림 1] 테스트 벡터 입력에 대한 순차적 분배 처리 방식

예를 들어, 테스트 벡터의 앞부분에는 비교적 처리시간이 짧은 테스트 벡터가 있고 뒤로 갈수록 처리하는 시간이 긴 테스트 벡터가 있다면, 암호모듈이 모든 테스트 벡터에 대한 출력을 생성하기까지 걸리는 시간은 수행시간이 긴 테스트 벡터의 영향을 받게 된다. 따라서 테스트 벡터들을 순차적으로 분배하는 방법보다 효율적으로 분배하는 방법을 고안하는 것이 필요하다.

키 유도 알고리즘 시험의 경우 먼저 각 테스트 벡터에서 수행시간에 영향을 주는 정보들을 다음과 같이 고려할 수 있다: 반복 횟수, 평문 또는 암호문의 길이. 각 정보를 P_{PTLen}, $P_{\mathrm{Iteration}}$ 등의 변수로 저장한다. 그다음, 각 정보의 최댓값을 $\max(P_i)$로 나타낼 때, $a_i = P_i/\max(P_i)$을 계산해 각 블록에 저장한다. 블록은 하나 혹은 여러 개의 출력값을 생성하기 위한 입력값들의 정보를 하나로 묶어둔 단위이다. 각 블록에 저장된 a_i에

테스트 벡터의 각 정보가 수행시간에 영향을 주는 정도 w_i를 실험적 혹은 임의의 값을 설정해서 구축한다. 본 연구에서는 w_i를 적당한 값으로 설정하였다.

최종적으로 블록에 저장되는 시간 가중치 t는 $\sum_{i \in P} a_i w_i$로 계산된다. 계산된 t를 기준으로 블록들을 정렬한 후 t가 큰 블록부터 순서대로 순회하면서, 각 모듈이 처리할 블록들의 번호를 저장해둔 큐 중, t의 합이 가장 작은 큐에 삽입한다. 이 방식은 단일 개수의 모듈에서는 효과가 미미하지만, 2개 이상의 모듈을 병렬적으로 사용할 수 있는 경우 블록 분배 방식을 통해 각 모듈이 주어진 블록을 모두 처리하는 데에 비슷한 실행시간을 소요하게 될 것이라 기대할 수 있으며, 기존 순차적으로 처리하는 방법보다 효율적으로 데이터를 처리할 수 있다.



[그림 2] 제안하는 분배 처리 방식

'DUSSQ CAVP 시험 도구' 상에서 동작하는 프로그램은 Python 프로그래밍 언어를 기반으로 구현되어있으며, 도구가 실행되는 컴퓨팅 환경과 연결된 모든 혹은 일부 DUSSQ 암호모듈과 시리얼 통신을 통해 데이터를 서로 주고받는다.

[표 1] DUSSQ CAVP 시험 도구 사양

특성	구성 요소	규격
OS / 메모리	Raspberry Pi 4 model B	Linux raspberry 5.15 / 4GiB
USB 통신	USB 3.0 호스트 1개	Type-A 커넥터
이더넷 통신	기가비트 이더넷 1개	RJ45 커넥터
도구 인터페이스	터치스크린 1개	10인치 / HD
암호모듈 통신	모듈 인터페이스 8개	암호모듈 입출력 커넥터
상태 표시기	전원 표시 LED 1개 입출력 표시 LED 32개	적색 LED 황색/녹색 LED
전원	AC 입력 1개	88-264V, 47-63Hz, 1.3A/115VC, 0.8A/230VAC
응용 프로그램	CAVP Test Program	Version 0.9.5c

[그림 3] CAVP Test Program 메인 화면

프로그램은 DUSSQ에 탑재된 암호 알고리즘 중, 블록 암호(ARIA, SEED, LEA), 해시함수(SHA2), 메시지 인증(HMAC), 난수 발생기(Hash_DRBG), 공개키 암호(RSAES), 전자 서명(ECDSA), 키 설정(ECDH), 키 유도(PBKDF)에 대해 *.txt 혹은 *.req 형식의 확장자를 가진 테스트 벡터를 입력받아 암호모듈에 데이터를 적절하게 분배한 후, 각 암호모듈에서 출력한 값을 취합해 *.rsp 파일을 생성하는 매개 역할을 한다.

프로그램은 사용자가 시험하고자 하는 암호 알고리즘에 대해 *.req 확장자를 가진 테스트 벡터의 데이터를 블록의 형태로 재구성한다. 만약 테스트 벡터가 *.txt 파일 확장자로 주어진다면 암호모듈이 출력해야 하는 암호문 등을 제외한 나머지 값들을 *.req 파일로 작성한 후, 이 *.req 파일을 읽어 처리한다.

[표 2] 제안하는 방식을 적용한 PBKDF(HMAC-SHA2-256) KPG 시험 결과

사용한 암호모듈	시험 대상 암호 알고리즘	처리 방식	
		순차 분배 방식	제안하는 방식
2개	PBKDF (HMAC-SHA2-256) KPG	4시간 22분	2시간 6분

[그림 4] DUSSQ CAVP 시험 도구의 동작 및 결과 화면

Ⅲ. 결론

본 논문에서는 멀티스레드 기반 병렬 처리방식이 적용된 DUSSQ CAVP 시험 프로그램을 통해 멀티스레드 기반 병렬 처리방식을 제안하고 이를 구현한 결과를 설명했다. 이러한 처리방식은 현재 암호 알고리즘 중 많은 시간이 소요될 것으로 예상되는 PQC(Post-Quantum Cryptography) 암호 알고리즘에 대한 CAVP를 효율적으로 수행할 것으로 기대된다.

이후 추가적인 연구를 통해 분배 방식을 더 개선하고, 사용자가 프로그램을 수동으로 조작 및 시험하고, 영향을 주는 정도 w_i를 사용자가 정하는 것이 아닌, 인공지능 모델을 구축해 테스트 벡터와 임의의 w_i로 시험을 수행한 결과들을 프로그램이 스스로 학습 데이터로 구축하고 이를 이용해 모델이 w_i를 결정하여 단순히 사용자가 시험하고자 하는 데이터를 업로드하면 시험 결과를 한눈에 볼 수 있도록 프로그램을 개선하고자 한다.

ACKNOWLEDGMENT

본 과제(결과물)은 교육부와 한국연구재단의 재원으로 지원을 받아 수행된 첨단분야 혁신융합대학사업(차세대통신)의 연구 결과입니다.

참 고 문 헌

[1] 암호모듈 검증, 국가정보원, https://nis.go.kr/AF/1_7_3_1.do.

[2] 이용석, 이정훈, "국방논단," 제1760호, Jun 2019, 4p.