5G 특화망 단말용 양자암호모듈 기반 단대단 보안 기법 구현 연구

김찬혁, 김형엽, 윤승환, 이옥연*

국민대학교, 국민대학교*

{20192223, gudduq159, schneeleopard, oyyi*}@kookmin.ac.kr

An establishment of an end-to-end security channel using a quantum entropy chip built-in cryptographic module in private network

Chanhuyk Kim, Hyeongyeop Kim, Seunghwan Yun, Okyeon Yi*

Kookmin Univ., Kookmin Univ.*

요 약

암호모듈은 정보의 유출, 위조 또는 변조, 훼손 등을 방지하기 위한 기밀성, 무결성, 인증, 부인 방지 등의 기능을 제공하기 위하여 암호 알고리즘을 구현한 소프트웨어, 펌웨어, 하드웨어 집합 또는 이들의 하이브리드 형태이다. 국내에서 수행하는 암호모듈 검증제도를 통한 암호모듈의 시험 및 검증은 국제표준에 기반한 검증기준 및 별도 공지한 검증 기준에 따라 수행되며, 세부 절차는 암호모듈 시험 및 검증지침을 적용한다. 본 논문은 이러한 검증제도를 통하여 검증필을 획득한 암호모듈을 이용하여 5G 특화망 단말에서 단대단 보안 서비스를 제공하기 위하여 필요한 암호모듈 및 암호모듈을 적용하기 위한 지침을 제시하고, 제안하는 양자암호모듈을 적용한 벤치마크를 보인다.

Ⅰ. 서론

최근 국내에서는 국방, 의료, 산업제어, 스마트 시티 등 높은 서비스 품질을 유지하는 것이 필요한 환경에서는 5G 특화망을 적용하는 사례가 증가하고 있다. 그러나 단말부터 코어망까지의 보안은 SIM, eSIM이 담당할 수 있으나 단대단 보안은 제공하지 못하고, 5G 특화망 단말부터 코어망까지의 보안만을 제공할 뿐, 망을 이용하는 응용 서비스의 단대단 보안은 제공해주지 못한다. 만약 단대단 서비스의 데이터 무결성이 확인되지 않으면 공격자가 데이터를 조작하여 코어망으로 전송할 수 있고, 중간자 공격에도 위협이 존재한다.

5G 특화망 환경에서 민감한 기업정보나 서비스 정보가 유통되는 경우에는 보다 높은 보안성이 요구되는 단말 보안이 고려되어야 한다. 특히 상호 인증을 기반으로 한 보안 통신을 수행해야 한다. 암호학적 상호 인증을 수행할 때에는 인증을 수행하는 두 개체가 모두 난수를 생성할 수 있어야 한다. 그러나 5G 특화망의 단말에서 제한된 시스템 자원을 갖춘 단말의 경우 난수 생성을 위한 엔트로피 소스를 얻기 어려운 환경도 존재한다. 이를 해결하기 위하여 양자암호모듈을 적용한다. 양자암호모듈은 암호모듈 내에 양자 특성을 이용한 엔트로피 생성기가 탑재되어 있다. 그러므로 제한된 시스템 자원을 가지고 있는 단말에서도 암호학적 인증을 수행하기 위해 필요한 좋은 엔트로피 입력을 생성할 수 있다.

국내에서 암호모듈 검증제도는 이 암호모듈에 대하여 [1]의 제9조와 [2]의 제69조 등에 따라 국가정보통신망에서 소통 및 저장되는 비밀이 아닌 업무자료를 보호하기 위하여 국가 또는 공공기관에서 도입하는 암호모듈의 안정성과 구현 적합성을 검증하는 제도이다.[3] 또한 이러한 검증제도를 통하여 검증필을 획득한 암호모듈에 대하여 사용자가 암호모듈 현장시험을 실시할 때 준수해야 하는 지침[4]이 있다.

본 논문에서는 이와 같은 제도와 지침을 바탕으로 5G 특화망 단말용 보안 서비스를 제공하기 위하여 필요한 암호모듈의 요구사항과 이 암호모듈을 적용하기 위하여 준수해야 하는 지침을 기술하고, 제안하는 양자암호모듈을 적용한 보안 서비스의 성능에 대한 벤치마크도 보인다.

Ⅱ. 본론

A. 5G 특화망 보안 요구사항

5G 특화망은 서비스의 연속성이 필요한 국가의 주요한 시설에서 사용되기 때문에 검증필 암호모듈이 사용되어야 한다.

B. 암호 알고리즘 요구사항

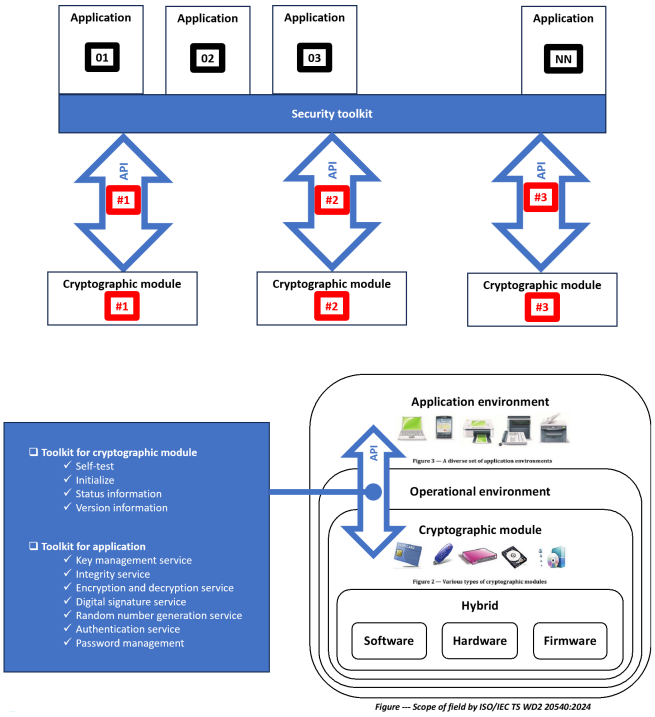
암호모듈이 제공하는 암호 알고리즘의 사양은 다음 표의 내용과 같다.

[표 1] 검증대상 암호 알고리즘의 사양[3]

분류	암호 알고리즘
블록암호	ARIA (ECB, CBC, CFB, OFB, CTR, CCM, GCM) SEED (ECB, CBC, CFB, OFB, CTR, CCM, GCM) LEA (ECB, CBC, CFB, OFB, CTR, CCM, GCM) HIGHT (ECB, CBC, CFB, OFB, CTR)
해시함수	SHA-2 (SHA-224/256/384/512) LSH (LSH-224/256/384/512/512-224/512-256) SHA-3 (SHA3-224/256/384/512)
메시지 인증	해시함수 기반 (HMAC) 블록암호 기반 (CMAC, GMAC)
난수발생기	해시함수 기반 (Hash_DRBG, HMAC_DRBG) 블록암호 기반 (CTR_DRBG)
공개키 암호	RSAES (공개키 길이: 2048, 3072, 해시함수: SHA2-224, SHA2-256)
전자서명	RSA-PSS (공개키 길이: 2048, 3072, 해시함수: SHA2-224, SHA2-256) KCDSA (키 길이: (2048, 224), (2048, 256), (3072, 256), 해시함수: SHA-224, SHA-256) EC-KCDSA (곡선: P-224,P-256, B-233,B-283, K-233,K-283, 해시함수: SHA2-224, SHA-256) ECDSA (곡선: P-224,P-256, B-233,B-283, K-233,K-283, 해시함수: SHA2-224, SHA-256)
키 설정	DH (키 길이: (2048, 224), (2048, 256), (3072, 256)) ECDH (곡선: P-224,P-256, B-233,B-283, K-233,K-283)
키 유도	KBKDF (HMAC, CMAC) PBKDF (HMAC)

C. 암호모듈 현장시험 지침

암호모듈 현장시험 지침은 [3]에서 검증받은 암호모듈을 사용자 응용환경에 적용하기 전에 사용자가 암호모듈 현장시험을 실시할 때 준수해야 하는 지침을 포함하고 있다.[4, 5]

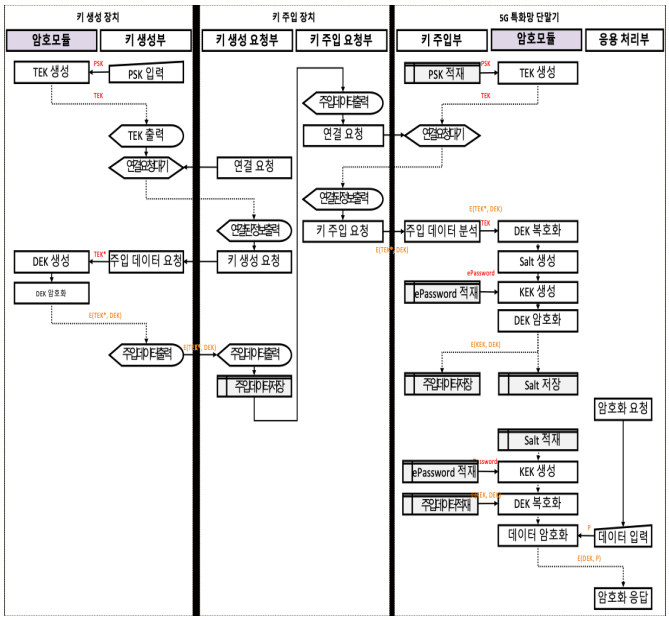


[그림 1] 암호모듈 현장시험 범위 및 툴킷[5]

암호모듈은 적용하려는 운영환경에서 요구하는 보안 기능을 제공하기 위하여 운영자는 암호 서비스에 관련한 모든 인터페이스를 제공할 수 있는지 확인해야 한다.

D. 제안하는 보안 기법

5G 특화망 단말에서 단대단 보안 서비스를 제공하기 위하여 암호모듈을 이용하는 방법을 제안한다.



[그림 2] 단대단 보안을 위한 키 주입 및 암호화 절차도

위의 그림에서 암호모듈은 다음과 같은 기능을 제공할 수 있어야 한다.

- 키 주입을 위한 키 설정/입력 기능
- 키 생성을 위한 난수 발생기 기능
- 키 암호화를 위한 키 유도 기능
- 키 저장 및 제거를 위한 키 저장 및 제로화 기능
- 데이터 암호화를 위한 블록암호 기능
- 서비스 사용을 위한 암호모듈 인증 및 인가 기능

E. 제안하는 보안 기법을 위하여 적용한 암호모듈 성능 결과

암호모듈의 인터페이스 처리 속도는 다음과 같다.

(단위: ms)

len_INPUT	0	16	32	64	128	256	512
t_RXTX	1.36	4.13	6.90	12.44	23.54	45.72	90.09
t_CRC	0.06	0.06	0.06	0.06	0.07	0.08	0.09

[그림 3] 암호모듈 입출력 속도

이 암호모듈을 이용하여 각각의 암호 서비스를 처리하는데 걸리는 시간은 다음과 같다.

(단위: ms)

암호알고리즘	데이터 크기(bytes)				
	16	32	64	128	256
LEA-128-GCM AE	2.80	5.59	11.17	22.37	44.75
LEA-128-GCM AD	2.80	5.59	11.17	22.38	44.75
ARIA-128-GCM AE	2.80	5.59	11.17	22.38	44.75
ARIA-128-GCM AD	2.80	5.59	11.17	22.38	44.75
ECDSA(P256) SG	295.76	298.54	304.14	315.31	337.64
ECDSA(P256) SV	735.25	738.03	743.74	755.00	777.52
ECDH(P256) KT	N/A	274.63	N/A	N/A	N/A
ECDH(P256) K	N/A	544.40	N/A	N/A	N/A
Hash_DRBG	N/A	64.64	N/A	N/A	N/A

[그림 4] 암호모듈의 암호 서비스 처리 속도

Ⅲ. 결론

5G 특화망 단말을 이용하여 단대단 보안을 제공하기 위하여 운영자는 본 논문에서 제안하는 기법을 적용하여 검증필 암호모듈을 이 운영환경에 정확하게 적용함으로써 서비스 중 발생할 수 있는 보안 서비스의 취약점을 최소화하여 시스템의 안전성을 확보할 수 있다.

ACKNOWLEDGMENT

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

참 고 문 헌

[1] 사이버보안 업무규정, https://www.law.go.kr/법령/사이버안보 업무규정,

[2] 전자정부법, https://www.law.go.kr/법령/전자정부법 시행령

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

[4] 암호모듈 현장시험 지침, TTAK.KO-12.0293, 2016.

[5] Testing cryptographic modules in their operational environment, ISO/IEC TS 20540, 2018.