정 보 보 호 학 회 지
제 30 권 제6호, 2020. 12

5G+ 초연결 환경을 위한 암호기술 연구

장 찬 국*, 김 현 기*, 윤 승 환**,이 옥 연***

요 약

4G/LTE로 일컫는 4세대 이동통신 이후 등장한 5세대 이동통신 기술은 초고속, 초연결, 초저지연 등을 기술적 요구사항으로 정의하다. 특히, 초연결을 위한 요구사항으로 1㎢ 단위 면적당 1백만개의 사용자 단말장치 또는 기기 등을 이동통신망에 연결토록 하는 것이고. 사용자 및 개체와 이동통신망 사이에서 식별을 포함하여 상호 인증 및 키 일치와 같은 암호기술을 요구하고 있다.

이때 사용자 및 개체 인증을 위한 많은 양의 난수가 소요되며, 이를 구현하기 위한 홈 네트워크 뿐만 아니라 단말 등에 적합한 난수기반의 암호장비 수요가 가시화 되고 있다. 본 논문에서는 5G 이동통신 환경에서 암호기술을 소개하고, 5G 이후 초연결을 위한 암호기술의 연구결과를 제시한다.

Ⅰ. 서 론

이동통신 기술은 1984년 음성 아날로그 중심의 1세대(1st Generation, 1G) 이동통신에서 약 10년마다 신기술로 도약하였다. 1990년대 2G, 2000년대 3G, 2010년대 4G를 거쳐 2020년 현재 5G 이동통신 시대가 되었다. 이동통신 기술의 발전 속에서 'Generation', G가 붙는 기준은 이전 세대의 이동통신과 비교하였을 때 급격한 기술 발전 및 변화, 기술적 요구사항, 서비스 요구사항을 제공할 때이다. 즉 세대가 변해갈수록 이동통신은 다양한 통신 기술의 변화를 거듭해갔으며, 5세대 이동통신 기술인 5G 이동통신 또한 마찬가지이다.

이처럼 5G 이동통신은 데이터 전송, 속도, 최대 기기 연결 수, 처리 지연 속도 등 4G의 모든 면에서보다 성능 향상이 요구되고 있으며, 초고속 eMBB (Enhanced Mobile Broadband), 초연결 mMTC(Massive Machine Type), 고신뢰-초저지연 URLLC(Ultra-Reliable Low Latency Communications) 등을 5G 이동통신의 기술적 요구사항으로 정의하였다. 이러한 고성능의 통신기능의 처리를 위한 정보보안 및 암호기술에는 가용성 보장이라는 커다란 도전이 되고 있다.

〔표 1〕 이동통신 세대별 성능 비교

구분	1G	2G	3G	4G	5G
상용화 연도	1980 - 1990년대	1990 -2000년대	2000 - 2010년대	2010 - 2020년대	현재
통신 방식	아날로그	GSM/ CDMA	WCDMA	LTE, WiMAX	MIMO, OFDM
최대 전송 속도	2Kbps	64Kbps	2Mbps~ 100Mbps	1Gbps	20Gbps
주파수 효율성 (3배)		-	-	-	4G 대비 3배
처리 지연 속도	-	-	-	10ms	1ms
최대 기기 연결 수	-	-	-	10만대/㎢	100만대/㎢
특징	-	디지털 신호 사용	UMTS 시스템	네트워크의 ALL-IP	4G 대비 100배
제공 서비스	음성	문자 메시지 (SMS, MMS)	영상통화, 멀티미디어	실시간 스트리밍	AR/VR 등

Ⅱ. 관련 기술

5G 이동통신의 첫 번째 요구사항인 eMBB는 사용자 단말을 중심으로 4G 이동통신에 비해 향상된 전송 속도, 최대 전송 속도 및 이동성 등을 제공받는 시나리오이다.

Capacity가 목적인 eMBB는 최대 10Gbps의 피크 데이터 속도와 평균 100Mbps를 목표로 한다. 따라서

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2020-0-00085, 5G+ 기반 6G 이동통신 정보보안 기술 연구).
* 국민대학교 금융정보보안학과(대학원생, jangchankuk@kookmin.ac.kr, 대학원생, lplp456@kookmin.ac.kr)
** 국민대학교 산학협력단(전임연구교수, schneeleopard@kookmin.ac.kr)
*** 국민대학교 정보보안암호수학과(교수, oyyi@kookmin.ac.kr), 교신저자

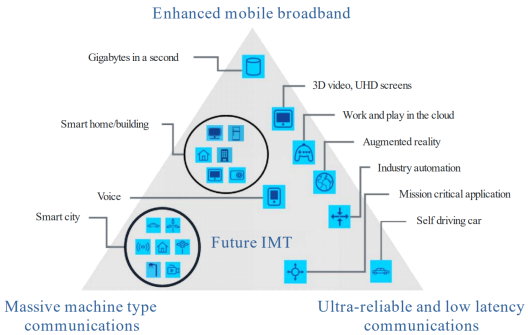
해당 요구사항을 만족해야하는 5G+ 응용분야로는 가상현실(VR), 증강현실(AR)등으로 불리우는 서비스와 4K/8K 화질의 UHD 스트리밍, 홀로그램서비스 등 다양한 사용자체감 서비스가 있다.

두 번째 요구사항인 mMTC는 가능한 많은 장치를 네트워크에 연결하는 목적을 의미하며 1 평방 킬로미터당 최대 1백만개의 장치를 달성하는 것을 목표로 한다. 따라서 해당 요구사항을 만족해야 하는 5G+ 응용 분야로는 다양한 센서 네트워크 및 Massive IoT 네트워크를 포함하는 스마트 시티, 스마트 홈 또는 스마트 팩토리가 있다.

마지막 요구사항인 URLLC는 초고신뢰/초저지연을 목표로 한다. 해당 요구사항을 만족해야하는 5G+ 응용분야로는 스마트 팩토리 등으로 불리우는 공장 자동화 시스템, 커넥티드 카 등으로 불리우는 자율주행차량시스템 등이 있다.

이러한 다양한 5G+ 응용서비스에서 정보보안 및 암호기술을 고려할 경우 위 세 가지 요구사항을 만족할 수 있는 기술을 제공해야 한다.

eMBB를 제공하는 서비스에서 정보보안 및 암호기술을 제공할 경우에는 정보보안 및 암호기술이 피크 데이터 속도를 제공할 수 있어야 하고, mMTC를 제공하는 서비스에서 정보보안 및 암호기술을 제공할 경우, 수많은 기기에 동시적으로 수용하여 암호기술을 제공할 수 있어야 한다. 마지막으로 URLLC를 제공하는 서비스에서 정보보안 및 암호기술을 제공할 경우, 전송지연시간 내 수행해야 한다.



〔그림 1〕 Usage scenarios of 5G and 5G requirements〔1〕

Ⅲ. 5G에서의 암호기술

5G는 네트워크 구조의 변화에 맞춰 보안 구조 역시 변경되었다. 5G 이동통신에서의 사용자 및 개체 인증은 크게 Primary Authentication과 Secondary Authentication으로 분류된다. Primary Authentication은 UE(User Equipment)와 Core Network 간 상호인증 및 키 일치을 진행한다. 이때, 상호인증 및 키 일치 기법으로 5G-AKA(5G Authentication and Key Agreement)와 EAP(Extensible Authentication Protocol) -AKA`를 상황에 따라 사용할 수 있다.

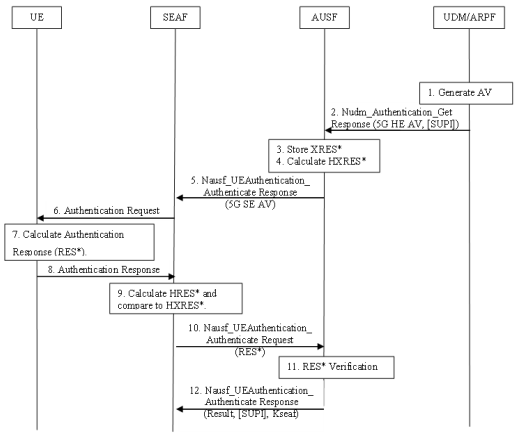
5G-AKA의 상호인증 절차는 4G 상호인증 절차의 보안 취약점을 보완하여 설계되었다. 예를 들어, 5G의 단말(UE) 인증 요청 과정 중, 단말이 보유한 가입자 식별정보인 SUPI(SUbscriber Permanent Identifier)를 공개키 암호인 ECIES 암호화 스킴을 이용하여 암호화 처리 후, SUCI (SUbscription Concealed Identifier)로 보내는 것이다.

4G에서는 단말의 인증 요청 단계에서 단말은 가입자 식별정보인 IMSI(International Mobile Subscriber Identity)를 전송한다. 4G에서는 암호화되지 않은 IMSI를 가지고 단말의 서비스를 차단하거나 서비스 정보를 탈취하는 등의 공격 가능성이 존재했다. 5G에서는 IMSI 또는 NAI(Network Access Identifier)를 SUPI로 통합하여 칭하는데, 이를 공개키 암호화 방법인 ECIES를 사용하여 SUCI로 암호화함으로써 4G에서와 같은 공격을 방지할 수 있도록 인증 요청 단계가 강화되었다.

아래 그림은 5G-AKA의 사용자와 통신망 사이의 상호인증 절차를 나타낸다[2]. 이 과정으로 단말과 5G 망 간 상호인증 및 키 일치를 수행하며, NAS/AS Security Setup 절차 등 모든 절차가 완료되면 이후 무선 구간에서의 Control Plane 및 User Plane 데이터에 기밀성 및 무결성을 보장하는 데이터 보호가 이루어진다.

5G의 AKA와 4G의 EPS-AKA 사이의 또 하나의 차이점은 위에서 언급한 가입자 식별정보를 암호화한 SUCI의 전송하는 것 외에도 단말에 대한 인증을 HN(Home Network)에서도 진행하는 것이다.

EPS-AKA에서는 SN(Serving Network)에서만 RES와 XRES를 비교하여 단말을 인증하였지만, 5G-AKA에서는 단말에서 전송한 RES*를 HN인 AUSF가 XRES*와 비교하여 HN에서도 단말에 대한 인증을 수



〔그림 2〕 5G-AKA 상호인증 절차

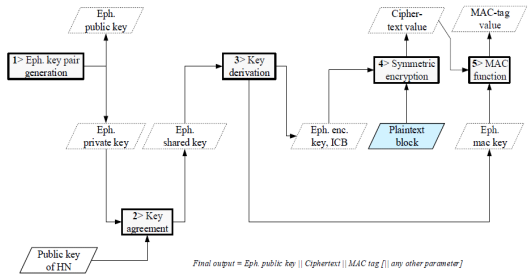
행하여 한층 강화된 인증을 수행한다. 이처럼 암호기술 관점에서의 가장 큰 변화는 SUPI와 SUCI의 도입이다. 이는 과거 3G, 4G 이동통신에서 사용자를 구별하는데 사용되었던 IMSI가 단말이 이동통신망에 초기접속 시 노출되는 취약점을 막고자 한 것으로, 3GPP의 TS 33.501[2]에서 정의한 내용은 [그림 3]과 같다.

SUPI가 IMSI 타입인 경우, 해당 문서에서 정의한 ECIES 스킴 기반 MSIN 암호화 과정은 다음과 같다. 타원곡선 도메인 파라미터의 경우 Profile A에서는 Curve25519를, Profile B에서는 secp256r1을 사용하도록 정의한다.

해당 파라미터들은 임시 공유키(Ephemeral shared key)를 생성하는 데에 사용되며 이때, UE에는 홈 네트워크의 공개키가 미리 주입된 상태로, 홈 네트워크에는 SUCI를 통해 UE의 공개키를 전달받은 상태로 존재한다.

	Profile A	Profile B
EC domain parameters	Curve25519	secp256r1
EC Diffie-Hellman primitives	X25519	Elliptic Curve Cofactor Diffie-Hellman Primitive
point compression	N/A	True
KDF	ANSI-X9.63-KDF	
Hash	SHA-256	
SharedInfo$_1$	$\overline{\text{R}}$ (the ephemeral public key octet string)	
MAC	HMAC-SHA-256	
mackeylen	256-bit	
maclen	64-bit	
SharedInfo$_2$	The empty string	
ENC	AES-128 in CTR mode	
enckeylen	128-bit	
icblen	128-bit	

〔그림 3〕 5G의 ECIES 개요〔2〕



〔그림 4〕 UE에서의 ECIES기반 SUPI 암호화 도식도〔2〕

생성된 임시 공유키는 MSIN을 암·복호화하는 키와 초기 카운터 블록(Initial Counter Block, ICB), 메시지 인증 코드(Massage Authentication Code, MAC)에 사용되는 키를 정의된 키 유도 함수(Key Derivation Function, KDF)로 생성한다. 이후 생성된 키로 MSIN 암·복호화하고 MAC을 생성한다.

또 다른 암호기술로는, UE, gNB, ng-eNB, AMF에 대한 요구사항으로 사용자 데이터와 시그널링 데이터에 대한 기밀성 및 무결성 항목이 존재한다.

5G에서 기밀성 제공을 위한 알고리즘은 NEA(Encryption Algorithm for 5G)로, 무결성 제공을 위한 알고리즘은 NIA(Integrity Algorithm for 5G)로 정의한다.[2] NEA와 NIA 입력 파라미터의 구성 및 출력값의 정의는 각각의 알고리즘마다 조금씩 상이하다.

NEA0, NIA0 알고리즘의 경우 보안 기능을 제공하지 않는 NULL scheme을 의미한다. 128-NEA1, 128-NEA2, 128-NEA3은 각각 128-bit 블록 암호 알고리즘을 사용해 구성하며, 데이터 암·복호화 과정은 그림14와 같다.

128-NIA1, 128-NIA2, 128-NIA3 역시 128-bit 블록 암호 알고리즘을 사용해 구성하며, 그림15와 같이 32-bit 메시지 인증 코드(MAC-I/NAS-MAC, XMAC-I/XNAS-MAC)를 생성한다. 이때 생성된 메시지 인증 코드값은 데이터 뒤에 붙여 전송 데이터에 대한 무결성을 제공한다.

이 외에도 UE의 초기 5G망 접속 시 인증 및 키 일치 프로토콜 수행을 위해 사용하는 암호 알고리즘인

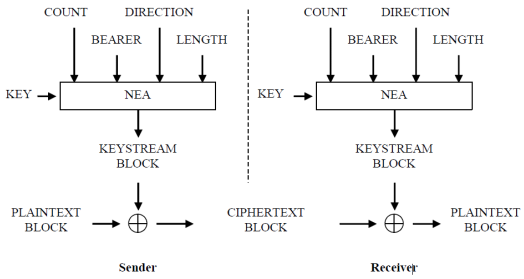
SNOW 3G	128-NEA1	128-NIA1	128-bit SNOW 3G based algorithm
AES	128-NEA2	128-NIA2	128-bit AES based algorithm
ZUC	128-NEA3	128-NIA3	128-bit ZUC based algorithm

〔그림 5〕 기밀성 및 무결성 제공을 위한 알고리즘 목록〔2〕

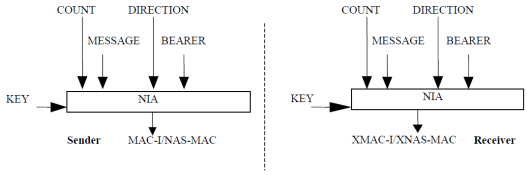
$f1, f1^*, f2, f3, f4, f5, f5^*$은 기존과 같이 AES 기반의 MILENAGE 알고리즘[3]과 Keccak 기반의 Tuak[4]가 존재한다.

이처럼 다양한 암호기술들이 5G 이동통신 내에 표준화되어 있지만, 해당 기술들이 구동되는 USIM 등의 구현환경 발전이 크지 않기 때문에, 5G의 기술적 요구사항인 eMBB, mMTC, URLLC를 위한 암호기술의 가용성이 보장되는 것은 아니다. 첫 번째로 5G 이동통신에서 처음 도입된 SUCI 기술은 공개키 암호를 이용한 임시 키 공유과정을 거치지만, 5G 이동통신의 mMTC 요구사항은 평방 킬로미터당 1백만개의 UE 수용이 목표이므로 5G 홈 네트워크에서는 전체적으로 수백억 개 기기의 키를 관리해야 하는 어려움이 생긴다. 따라서 5G에서는 이 과정에 공개키 암호화 방식을 적용하여 키 관리의 효율성을 높였다. 하지만, 공개키 암호를 적용할 경우 해시함수 또는 블록 암호 알고리즘보다 연산량이 월등히 많아, UE에서는 공개키 암호 연산에 대한 부담이 생긴다.

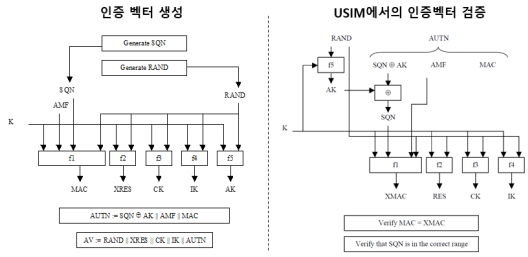
두 번째로, 5G 이동통신에서는 인증, 키 일치, 데이터 기밀성 및 무결성 등을 제공하기 위해 다양한 암호 알고리즘을 사용한다. 하지만 5G 요구사항인 mMTC와 URLLC를 목표로 표준화 한 것이 아니라 기존 4G 이동통신에서 사용하는 암호 알고리즘을 그대로 사용하고 있다.따라서, 5G 이동통신에서 목표하는 최대 전송속도와 지연시간(Latency)을 만족시키기 위해 최적화 구현



〔그림 6〕 데이터 암·복호화 과정〔2〕



〔그림 7〕 MAC-I/NAS-MAC, XNAS-MAC 유도〔2〕



〔그림 8〕 인증 데이터 생성 및 검증 과정〔6〕

연구가 필요하다.

Ⅳ. 5G기반 통신에서의 난수 발생

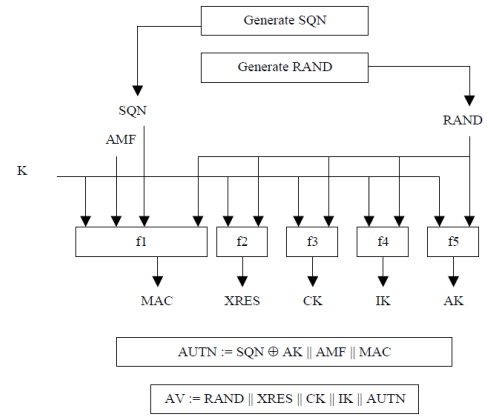
위에서 언급한 두 가지 문제점 외에도 여러 이슈 등이 존재하지만, 본 논문은 5G의 난수 생성 및 사용에 초점을 맞춘다.

5G 통신망에 기기가 접근을 요구할 때부터 인증이 끝나 홈네트워크와 암호화 통신을 진행할 때까지 크게는 앞서 소개한 부분에서 난수가 필요하다. USIM은 ECIES 스킴으로 IMSI를 SUCI로 암호화 하여 통신망에게 보내는데, 이때, USIM측에서는 통신망과 ephemeral Key agreement(ECDHE)를 진행하기 위해 난수를 생성해야 한다.

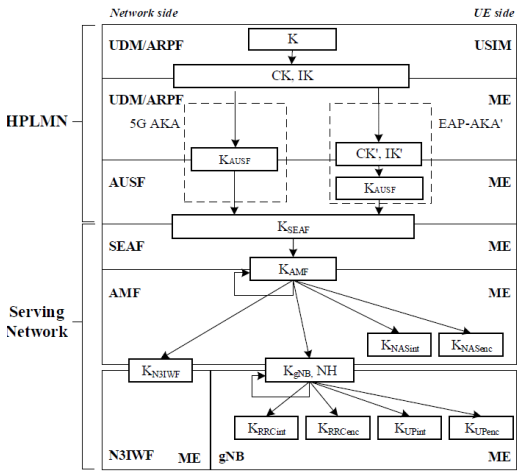
이와는 반대로, 접근이 허가된 이후, AKA (Authentication and Key Agreement, 인증 및 키일치)를 진행할 때에는 홈 네트워크가 USIM을 인증하기 위해 난수를 생성해야 한다. 홈 네트워크가 하나의 USIM을 인증하기 위해 홈 네트워크는 적어도 하나의 AV(Authentication Vector, 인증벡터)를 생성해야 하며, AV는 16-Byte의 난수를 포함한다.

[그림 9]는 홈 네트워크가 AKA에 사용할 AV를 생성하는 과정이다. 이 때 AKA를 수행하는 개체는 AV의 각 필드를 일련의 키유도 과정을 통해 [그림 10]과 같이 키 생성과정을 거쳐 다양한 키를 생성하여 인증 및 기밀성, 무결성 키로 사용한다.

[그림 9]와 [그림 10]에서 알 수 있듯이, 5G 키 계층에서 최상위 계층에 해당하는 CK, IK는 하위 키를 유도하기 위한 키_유도_키로 사용된다. 이 키_유도_키의 근본이 되는 입력값은 최초 홈 네트워크와 USIM이 공유하고 있던 마스터 키 K와, AKA 진행을 위해 새롭게 생성한 RAND이다. [2] 및 [6]에서는 마스터 키 MK를 생성하는 방법은 정의하고 있지 않으며, RAND는 예측



〔그림 9〕 홈 네트워크에서의 AV 생성 과정



〔그림 10〕 5GS의 키 계층

할 수 없는 비트열(Unpredictable Challenge)을 생성하라는 정도만 언급하고 더 이상의 방법은 다루지 않는다. 하지만, NIST의 키 유도함수 표준 SP 800-108[7]에 의하면 키 유도함수에 사용할 입력값은 암호학적인 방법(검증대상 암호 알고리즘)으로 생성된 값이어야 하며, 키 유도함수에 의해 생성된 키의 보안강도는 입력된 파라미터의 보안강도를 넘을 수 없다. 즉, 5G에서 다양한 하위 계층 키를 유도하는 입력값 MK와 RAND는 하위 계층 키의 보안강도를 결정하므로 암호 시스템의 근본이 되는 파라미터이다. 위에서 언급한 것과 같이, 5G표준은 기밀성, 무결성, 메시지 인증 등 모든 보안강도의 기준이 128-bit 이상으로 정의한다. 따라서 이에 상응하는 보안강도를 제공하기 위해서 홈네트워크는 최초에 주입하는 마스터키 MK와, 매 인증마다 새롭게 생성하는 RAND가 보안강도 128-bit 이상 되도록 생성하여야 한다.

이때 5G 이동통신 환경에서 고려할 사항은 다음과 같다. NIST의 난수발생기 표준[8]에 의하면 보안 강도를 만족하는 하나의 엔트로피 소스 당 최대 2^{16}Byte만큼 출력하면 반드시 새로운 엔트로피 소스를 주입한는 리시드 과정을 거쳐야 한다. 홈 네트워크에서 각 USIM을 인증하기 위해 16바이트 크기의 RAND를 한번의 리시드 과정으로 생성하고자 하면 최대 4,092개까지 가능하다. 반면 5G 이동통신의 기술적 요구사항인 mMTC의 요구사항으로 5G 네트워크의 셀은 평방 킬로미터당 최대 1백만개의 노드를 수용해야 하므로 한 셀이 한 번에 노드들을 수용하기 위해서는 한 셀당 최소 244번의 리시드 과정이 필요하다. 한국의 총 국토면적이 약 100,401㎢ 임을 고려하면, 국내에서 5G-mMTC 서비스를 만족하기 위해서는 최소 100,401셀 이상이다. 5G 통신사가 각각의 스몰셀 커버리지를 겹치도록 설계하였다면 셀의 수가 더 늘어날 수도 있기 때문이다.

따라서 5G 통신 중 mMTC 서비스를 정상적으로 제공하기 위해서는 100,401,000개의 난수열 (RAND)을 단시간에 출력할 능력을 갖추어야 하며, 이에 따라 해당 난수열이 모두 보안 강도 128-bit 이상을 충족할 수 있도록 엔트로피 소스 또한 그만큼 축적하고 있어야 한다. 따라서, 이를 만족시키기 위해 다음 세 가지 방법을 고려할 수 있다.

첫 번째 방법으로는 엔트로피 소스 저장 풀(pool)을 구성한다. 엔트로피 소스가 필요할 때마다 상시 보안 강도 이상을 제공할 수 있도록 대량의 엔트로피 소스를 저장한다. 엔트로피 소스는 데이터 특성상 단시간에 수집, 축적되지 않기 때문에 많은 양의 엔트로피 소스를 안전하게 축적해두어야 한다. 두 번째 방법으로는 의사난수열 저장 풀도 비슷한 맥락으로 축적해야 한다. 한번의 엔트로피 소스 주입으로 생성할 수 있는 난수열은 기껏해야 최대 2^{16}Byte이고, 모든 노드에 대하여 인증 절차를 수행하기 위해서는 현저히 부족한 양이다. 그러므로 엔트로피 소스 풀에 엔트로피 소스가 일정량 축적될 때마다 의사난수열 풀에도 같이 축적해두어야 한다. 이때 의사난수를 생성하거나, 축적된 데이터를 호출할 때, GPGPU 등을 통해 병렬로 진행한다면 대량의 5G 개체가 인증을 요청해도 지연없이 권고되는 보안강도

이상을 제공할 수 있다. 마지막 세 번째 방법으로는 대량의 안전한 난수(RAND)를 기반으로 5G 자체의 안전성 및 그 위의 응용환경인 5G+ 기반의 서비스를 구성하는 인증서버뿐만 아니라, USIM, 드론, 자율비행체, 로봇, 의료기기와 같은 IoT 기기를 위한 다양한 운영환경에서의 고속 난수발생기 구현기술의 연구가 지속되어야 한다.

Ⅴ. 결 론

이제 안전한 5G 이동통신과 이에 기반한 5G+ 응용환경에서의 초고속, 초저지연, 초연결 서비스를 위하여, 1㎢ 당 1백만개의 많은 사용자 및 IoT 개체에 대한 원활하고 안전한 인증을 수행할 수 있는 환경 구축을 위해서는 빠르고 안전한 통신 환경뿐만 아니라 이러한 환경에 적합하면서도 암호학적 안전성과 함께 가용성을 보장하는 암호기술이 구현된 난수기반 기기 등의 개발 연구가 필요하다.

참 고 문 헌

[1] ITU-R, “Framework and overall objectives of the future development of IMT for 2020 and beyond”, 2015.09

[2] 3GPP TS 33.501, “Security Architecture and procedures for 5G System”, 2020.09

[3] TS 35.205, “3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General”, 2020

[4] TS 35.231, “Specification of the TUAK algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: Algorithm specification”, 2020

[5] T. Specification, “TS 33 401 - V14.2.0 - Universal Mobile Telecommunications System(UMTS) 3G security Security Architecture(3GPP TS 33.401 version 14.2.0 Release 14)”, 2017

[6] T. Specification, “TS 33 102 - V16.0.0 - 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (3GPP TS.33. 102 version 16.0.0 Release 16)

[7] Lily Chen, “ Recommendation for Key Derivation Using Pseudorandom Functions” (Revised), NIST Special Publication 800-108, October 2009

[8] Elaine Barker, John Kelsey, “ Recommendation for Random Number Generation Using Deterministic Random Bit Generators ”, NIST Special Publication 800-90A, June, 2015

〈저 자 소 개〉

장 찬 국 (Chan-Guk Jang)

학생회원

2016년 2월 : 국민대학교 수학과 졸업

2018년 2월 : 국민대학교 금융정보보안학과 석사

2018년 3월~현재 : 국민대학교 금융정보보안학과 박사과정

<관심분야> 네트워크보안, 이동통신보안, 위성통신보안, 암호모듈 검증제도

김 현 기 (Hyunki Kim)

학생회원

2016년 2월 : 국민대학교 수학과 졸업

2018년 2월 : 국민대학교 금융정보보안학과 석사

2018년 3월~현재 : 국민대학교 금융정보보안학과 박사과정

<관심분야> 이동통신보안, 암호학적 난수응용,암호모듈 검증제도, 딥러닝

윤 승 환 (Seunghwan Yun)

정회원

2005년 2월 : 국민대학교 수학과 졸업

2007년 2월 : 국민대학교 수학과 석사

2019년 2월 : 국민대학교 금융정보보안학과 박사

2019년 3월~현재: 국민대학교 산학협력단 전임연구교수

<관심분야> 암호모듈, 무선이동통신보안, 양자난수, 정보보호

이 옥 연 (Okyeon Yi)

정회원

1988년 2월 : 고려대학교 수학과 졸업

1990년 2월 : 고려대학교 수학과 석사

1996년 8월 : Univ. of Kentucky 박사

<관심분야> 5G/6G 보안, 위성통신보안, KCMVP