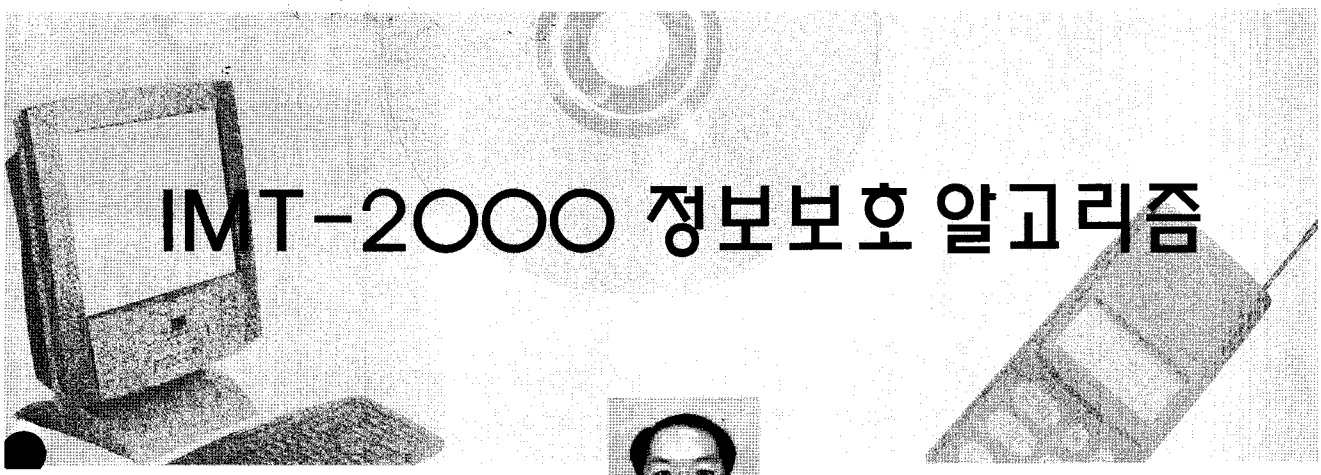


IMT-2000 정보보호 알고리즘

이옥연
ETRI 정보보호기술연구본부 선임연구원

홍도원
ETRI 정보보호기술연구본부 선임연구원

정배은
ETRI 정보보호기술연구본부 선임연구원

1. 개요

고도의 정보화 사회에서 요구하는 음성 서비스와 화상, 데이터 등의 멀티미디어 서비스를 제공할 3세대 이동통신인 IMT-2000 시스템의 개발에는 민감한 정보를 보호할 수 있는 많은 보안 특성들이 요구된다. 따라서 이들을 현실화할 수 있는 안전성과 신뢰성이 검증된 암호 알고리즘의 개발과 표준화가 요구되는 실정이다. 진화된 GSM 핵심망에 기반한 DS-CDMA 방식의 무선 접속기술을 바탕으로 3세대 이동통신망에 대하여 전세계적으로 적용 가능한 기술규격을 준비하기 위해 유럽의 ETSI와 일본의 ARIB 등의 표준개발 기관들이 중심이 되어 결성한 3GPP의 3세대 시스템(UMTS라고 불림) 보안 구조는 f0~f10이라 불리는 11개의 보안 관련 알고리즘을 필요로 한다. 그 중 국제적인 로밍에 필수적인 암호화 알고리즘 f8과 무결성 알고리즘 f9는 표준화하기로 결정되어, 3GPP의 기술그룹인 TSG-SA는 이 알고리즘의 설계를 ETSI의 암호알고리즘전문가그룹(SAGE)에 의뢰하였다(1999. 8.). ETSI SAGE는 Task Force 팀을 결성하여, 이미 평가가 이루어진 일본 미쓰비시의 알고리즘 MISTY를 기반으로 KASUMI(MISTY의 일본말)라는 새로운 블록 암호를 f8과 f9의 핵심 알고리즘으로 개발하였다(2000.1.). 이 알고리즘의 공개검증 여부는 2000년 7월 18-19일 중국 베이징에서 열린

3GPP OP 3차 회의에서 논의되었다. ETSI과 ARIB은 3GPP 알고리즘(f8, f9)의 완전 공개에 찬성하였고, 미국의 T1은 정부와의 협의문제로 공식적인 의사표명은 하지 않았지만 비공식적으로는 찬성 의사를 밝혔으므로 조만간 알고리즘의 완전 공개가 이루어 질 것으로 보인다.([8]) 3GPP 알고리즘의 국내 배포 및 관리는 한국의 표준화 기관인 TTA에서 현재 시행중에 있다.([15])

3GPP의 인증 및 키 일치(AKA) 관련 알고리즘 f0~f5에 대해서도 각 사업자의 독자적인 알고리즘 사용을 허용하면서도 국제적인 3G 네트워크에서의 사용을 위해서 2000년 8월 중순 SAGE 주도의 Task Force팀을 결성하여 사용자 인증 알고리즘 개발에 착수하였으며, 2000년 11월 말까지 개발을 완료할 예정이다. 현재 사용자 인증 알고리즘에 관련하여 TIA TR-45 AHAG 그룹이 3GPP와 협력체계를 유지하고 있으며, 3GPP의 SAGE에서 이들이 제시한 내용을 검토하고 있다. Lucent Technology가 SHA-1에 기반한 인증 알고리즘을 제시하였으나, 3GPP에서는 KASUMI를 사용할 것으로 보이며, AES의 사용여부도 배제할 수 없다.([7])

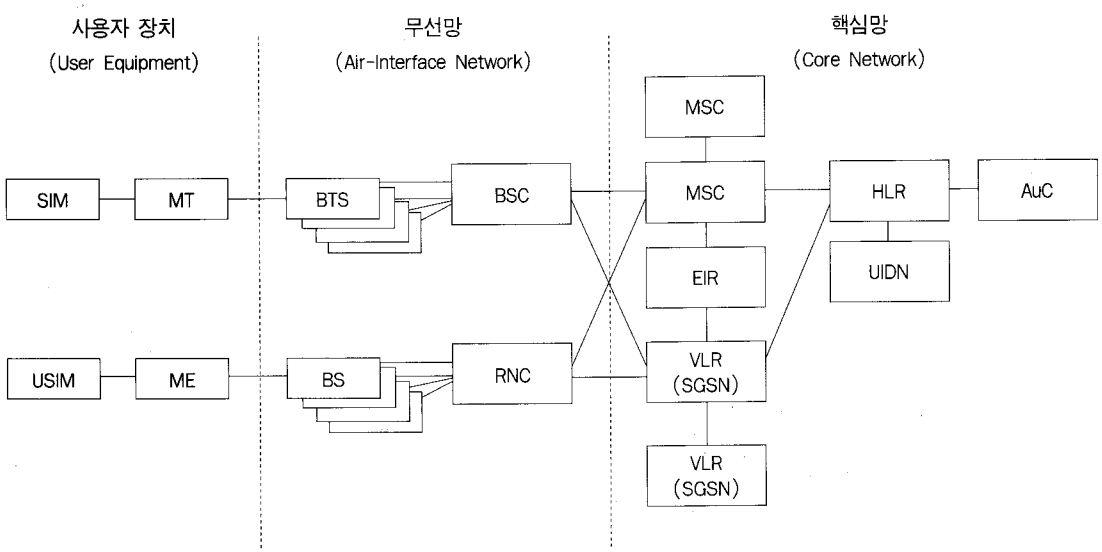
3세대 ANSI-41 네트워크와 MC-CDMA 무선접속 기술규격 작성을 위해 미국이 주축이 되어 결성된 3GPP2의 경우 ANSI-41 네트워크에서 IS-95를 토대로 한 CDMA2000은 Global과 Unique challenge의 두 가지 인증을 제공하고 인증 절차, 공유 비밀키(SSD)를 이용한 AUTH_Signature 생성절차, 신호 메시지 암호화, 음성 비화의 경우 IS-95와 큰 차이가 없다. 하지만 IS-95 시스템의 인증절차에서 사용되는 약점이 노출된 짧은 키의 CAVE 알고리즘을 대치하는 강화된 인증과 IMT-2000의 요구사항인 이동국과 네트워크의 상호인증을 제공하기 위한 강화된 사용자인증(ESA)의 필요성이 대두되어, TR-45의 AHAG가 ESA 프로토콜을 만드는 작업중에 있다. TR-45는 ESA 키 일치 프로토콜로 3GPP의 AKA를 채택하였으며, TR-45 네트워크에서 3GPP AKA를 위한 지역적 인증 알고리즘으로 SHA-1을 채택하였다.([13]) 또한 AHAG는 CDMA2000을 위한 강화된 암호 알고리즘(ESP)의 선택을 TR-45.5에 제의하였다.([12])

2. 3GPP 정보보호 알고리즘 기술동향

2.1 3G 정보보호 구조의 개요

3GPP의 정보보호와 관련된 3세대(3G) 네트워크는 (그림 1)과 같이 사용자 영역, 서비스 네트워크(SN) 영역, 홈 환경(HE) 영역으로 나누어진다. 사용자 영역은 3G 서비스에의 접근을 위한 사용자 신분 확인 및 인증에 필요한 데이터 및 함수를 저장한 USIM(User Service Identity Module)과 ME(Mobile Equipment)로 구성된다. 서비스 제공영역은 무선접근을 제어하는 RNC(Radio Network Controller), 서킷 전환서비스와 패킷 전환서비스를 위한 위치 등록소인 VLR(Visitor Location Register)과 SGSN(Serving GPRS Support Node)로 구성되며, 홈 환경영역은 3세대 서비스 가입자에 대한 서비스 제공에 전반적인 책임이 있는 HLR(Home Location Register), 인증센터 AuC(Authentication Center), UIDN(User Identity Decryption Node)으로 이루어진다.

제 3세대 시스템이 만날 수 있는 다양한 보안 위협 중에서 무선 접속링크에 대한 정보보호를 제공하는 네트워크 접근 보호에 요구되는 보안 특성들은 사용자 신분 비밀성, 개체 인증, 데이터 비밀성과 무결성이다. 먼저 사용자 신분 비밀성과 관련된 보안 특성에는 사용자 영구 ID(IMUI)와 위치의 비밀성, 그리고 어떤 서비스가 같은 사용자에게 제공되는지 알 수 없어야 하는 사용자 추적불가능성이 포함된다. 이러한 목적을 달성하기 위해서 사용자가 방문한 서비스 제공 네트워크에서 임시 ID나 암호화된

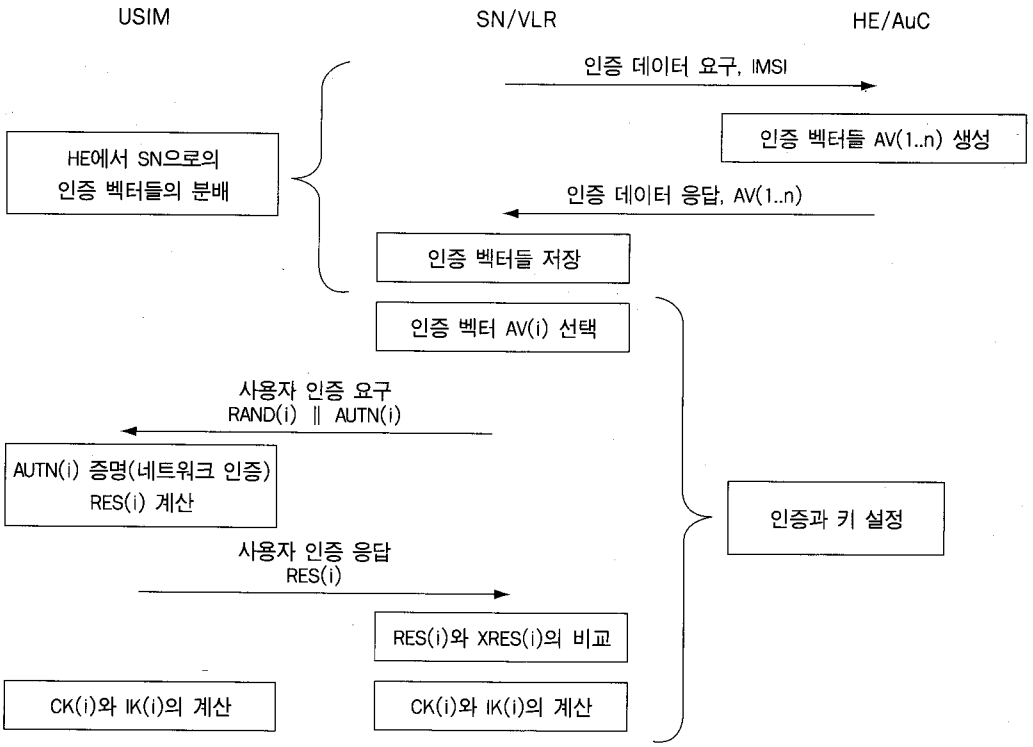


(그림 1) 3GPP Security 구조

영구 ID에 의해 신분 확인이 수행되어야 하며, 사용자의 신분이 노출될 수 있는 어떤 시그널이나 사용자 데이터도 무선 접근 링크상에서는 암호화되어야 한다. 두 번째로 개체 인증과 관련된 보안 특성에는 사용자와 서비스 제공 네트워크 사이에 상호 인증과 키 일치를 위한 메커니즘의 안전한 결정과 네트워크에 의한 사용자 인증, 사용자에 의한 네트워크의 인증이 포함된다. 개체 인증은 사용자와 네트워크 사이에서 연결 설정이 될 때마다 발생해야 하며, 사용자의 HE/HLR에서 서비스 제공 네트워크(VLR/SGSN)으로 전송되는 인증 벡터를 이용한 인증 메커니즘과 인증과 키 설정 과정의 수행기간 동안 사용자와 서비스 제공 네트워크 사이에 설정된 무결성 키를 이용한 지역적인 인증 메커니즘이 포함된다. 세 번째로 네트워크 접근 링크 동안 데이터의 비밀성을 보장하기 위해서 이동국과 서비스 제공 네트워크 사이의 암호화 알고리즘과 키 일치, 무선 접근 인터페이스 상에서의 사용자 데이터와 시그널 데이터의 비밀성을 제공하는 보안 특성들이 요구된다. 암호화 키 일치는 인증과 키 일치(AKA) 메커니즘의 수행중에 실현되며, 암호화 알고리즘 일치는 사용자와 네트워크 사이의 보안 모드 수행 메커니즘에 의해 실현된다. 마지막으로 네트워크 접근 링크 동안 데이터의 무결성을 제공하는 보안 특성에는 이동국과 서비스 제공 네트워크 사이의 무결성 알고리즘과 무결성 키의 일치, 무선 접근 인터페이스 상에서의 데이터의 무결성과 시그널 데이터의 출처 인증이 포함된다. 무결성 키 일치는 AKA의 수행중에 실현되며, 무결성 알고리즘 일치는 사용자와 네트워크 사이의 보안 모드 수행 메커니즘에 의해 실현된다.

2.2 인증과 키 일치(AKA : Authentication and Key Agreement)

이 메커니즘은 USIM과 HE의 AuC만 이용할 수 있는 분배된 비밀키 K의 정보를 이용하여 사용자와 네트워크의 상호인증을 이룬다. 이 방법은 ISO 표준 ISO/IEC 9798-4에서 나온 네트워크 인증을 위한 수열 기반 one-pass 프로토콜과 결합한 GSM 가입자 인증과 키 설정 프로토



(그림 2) 인증과 키 일치

콜과 일치하는 도전/응답 프로토콜이다. 메커니즘의 개요는 (그림 2)에 나타나 있다.

VLR/SGSN으로부터 요구를 받는 즉시 HLR/AuC는 n개의 인증벡터들을 VLR/SGSN에 보낸다. 각각의 인증벡터는 난수 RAND, 기대응답 XRES, 암호화 키 CK, 무결성 키 IK, 인증토큰 AUTN으로 구성된다. VLR/SGSN은 배열로부터 하나의 인증벡터를 선택한 후 사용자에게 변수 RAND와 AUTN을 보낸다. USIM은 AUTN이 받아들일 수 있는 것인지를 확인한 후, 네트워크가 인증이 되면 응답 RES를 VLR/SGSN에 보내고 키 CK와 IK를 생성한다. 마지막으로 VLR/SGSN은 RES와 XRES를 비교하여 USIM을 인증하고 설정된 키 CK와 IK로 USIM과 VLR/SGSN 사이의 암호화와 무결성 함수들을 수행한다.

위의 메커니즘에서 사용하는 인증벡터의 생성절차와 구성요소를 살펴보자. HLR/AuC에서 인증벡터 Quintet의 생성하는 과정은 다음장 (그림 3)과 같다.

VLR/SGSN으로부터 (RAND, AUTN)쌍을 받은 후 USIM은 다음장 (그림 4)와 같이 네트워크 인증에 필요한 MAC(or XMAC), 응답 RES, 암호화 키 CK, 무결성 키 IK를 생성한다.

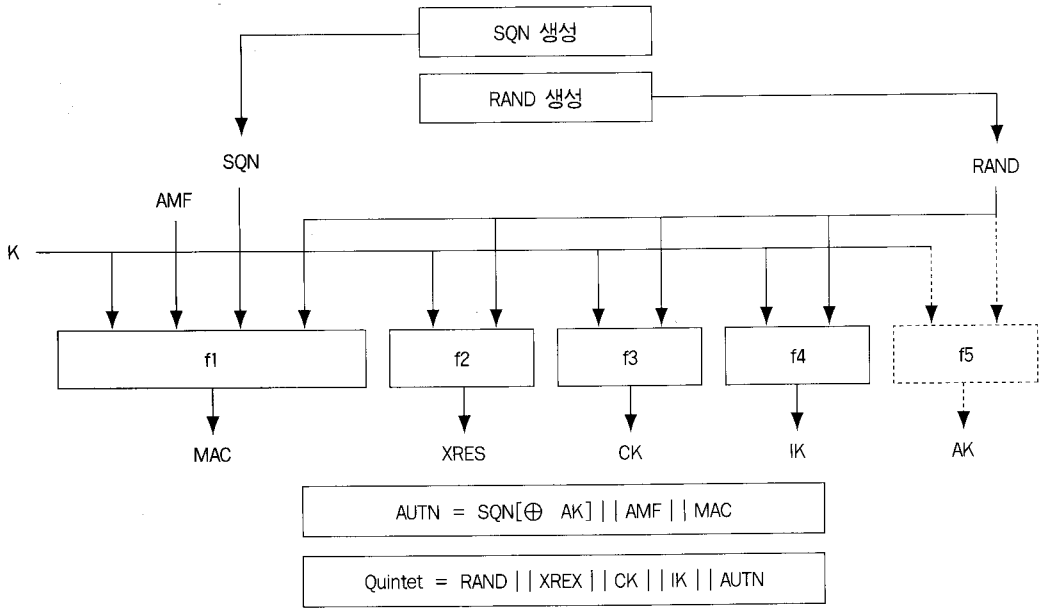
2.3 데이터 기밀성과 무결성

2.3.1 데이터 기밀성(Data confidentiality)

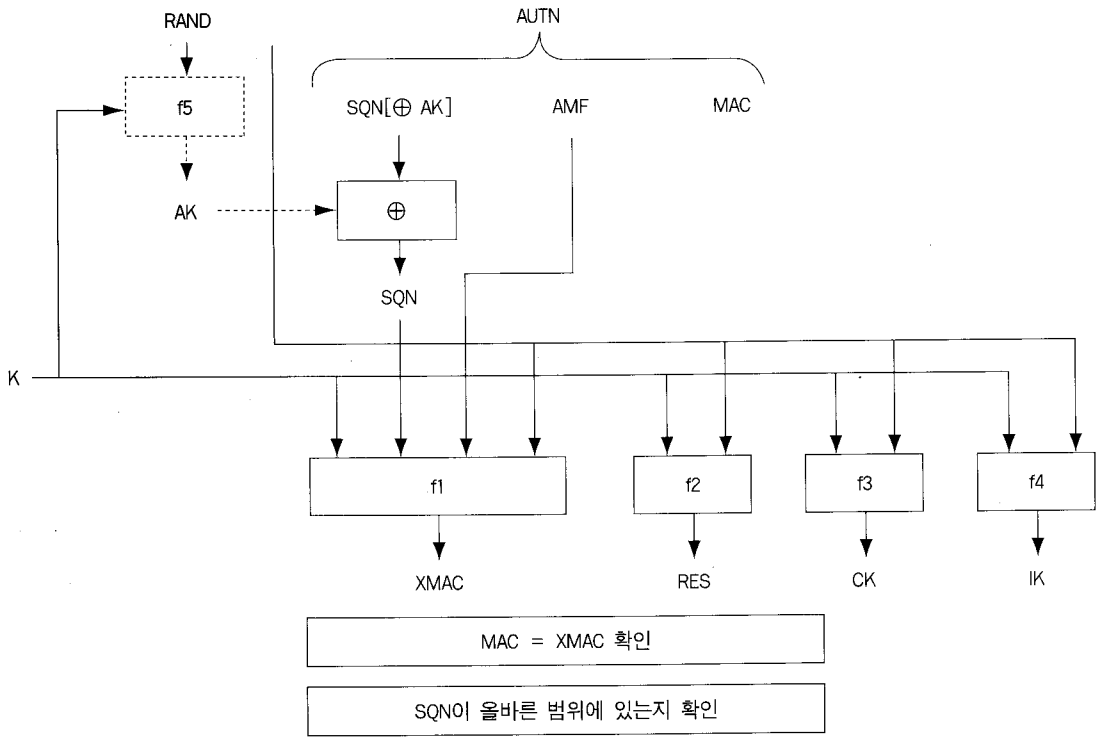
사용자 데이터와 시그널 데이터의 기밀성을 위한 메커니즘은 다음과 같은 암호함수를 요구한다.

- f8 : UMTS 암호화 알고리즘

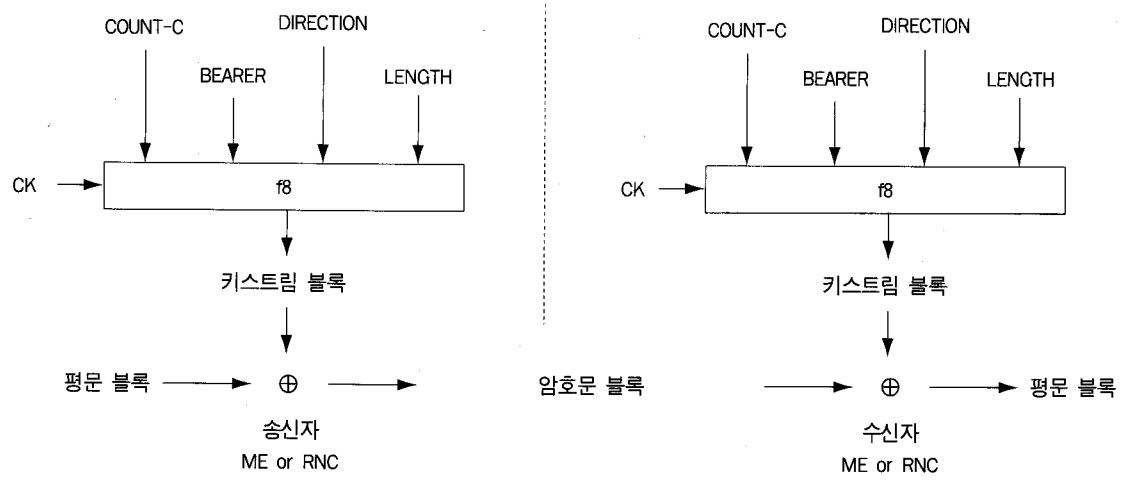
(그림 5)는 암호화 함수 f8을 이용해 만든 키스트림과 평문을 XOR 비트 연산을 하여 평문을 암호화하고 또 암호문을 복호화하여 평문으



(그림 3) AuC에서의 인증벡터 생성



(그림 4) USIM에서의 인증과 키 유도



(그림 5) 암호화된 사용자 데이터와 시그널 데이터

로 만드는 과정을 나타낸다.

128비트의 암호화 키 CK, 수열번호 COUNT-C, 베어러 ID BEARER, 암호화된 베어러의 전송방향을 나타내는 DIRECTION, 입력비트 스트림의 비트 수를 나타내는 LENGTH와 같은 입력변수 값을 함수 f8에 대입하면 알고리즘은 입력 평문 블록과 XOR 비트 연산을 통해 암호문 블록을 만드는 키스트림 블록을 출력한다.

이 UMTS 암호화 함수(UEA) f8은 완전하게 표준화되며, 총 16개가 사용될 수 있는 데 현재 정의되어 있는 것은 다음 2개이다.

"0000_2" : UEA0, 암호화 안함

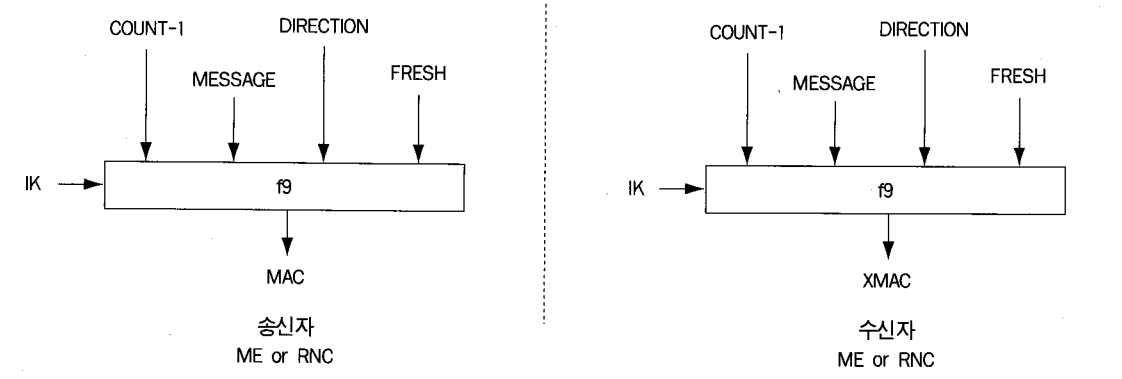
"0001_2" : UEA1, Kasumi

2.3.2 데이터 무결성(Data Integrity)

이동국에서 네트워크로 보내어지는 대부분의 제어 시그널 데이터들은 무결성이 보장되어야 한다. 시그널 데이타의 무결성을 위한 메커니즘에는 다음과 같은 암호함수가 요구된다.

- f9 : UMTS 무결성 알고리즘

(그림 6)은 무결성 함수 f9를 이용하여 시그널 메시지로부터 메시지 인증코드 MAC을 유도하는 과정을 보여준다.



(그림 6) 시그널 메시지에 대한 MAC(or XMAC)의 생성

무결성 키 IK, 수열번호 COUNT-I, RNC에서 만들어진 32비트 난수 FRESH, 시그널 메시지의 전송방향을 나타내는 DIRECTION과 같은 입력변수 값을 함수 f9에 대입하면 알고리즘은 데이터 무결성을 위한 메시지 인증코드 MAC을 계산한다. 그리고 MAC은 무선접근 링크상에서 메시지에 부가되어 보내지고, 수신자는 같은 방식으로 XMAC를 계산하여 송신자가 보내온 MAC 값과 비교해 봄으로써 메시지의 무결성을 검증한다.

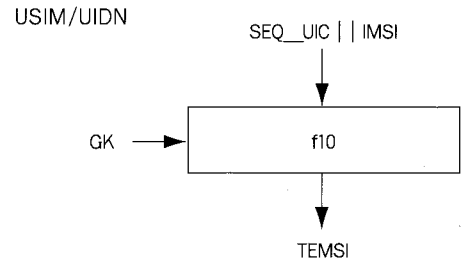
이 UMTS 무결성 함수(UIA) f9는 완전하게 표준화되며, 총 16개가 사용될 수 있는 데 현재는 다음 값만이 정의되어 있다.

"0001_2" : UIA1, Kasumi

2.4. 사용자 신분 비밀성

임시 ID를 이용한 사용자 신분 확인이 실패할 때 서비스 제공 네트워크는 사용자의 영구 ID의 노출을 피하기 위해 암호화된 사용자 영구 ID EMSI를 사용할 수 있다. (그림 7)은 IMSI와 사용자 ID 암호화 수열 SEQ_UIC를 EMSI로 암호화하는 사용자 ID 암호화 함수 f6과 EMSI로부터 SEQ_UIC와 IMSI를 복호화하는 데 사용되는 사용자 ID 복호화 함수 f7을 설명한다.

사용자 ID 암호화 함수 f6은 USIM에서 수행되어 EMSI를 계산하고 사용자 ID 복호화 함수 f7은 HE에 있는 UIDN에서 수행된 후 얻어진 사용자의 IMSI를 다시 SN/VLR에 보낸다. SN이 특별한 사용자를 찾을 때 강화된 사용자 신분 비밀성 보호를 위해 평문 형태의 IMSI를 사용하는 대신에 임시적인 암호화된 사용자 ID TEMSI를 사용할 수 있다. (그림 8)은 페이징 ID 함수 f10을 이용하여 TEMSI를 생성하는 과정을 설명한다.

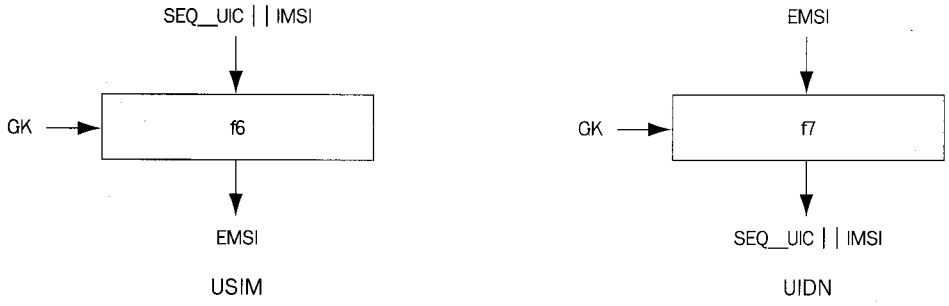


(그림 8) TEMSI의 계산

사용자가 방문한 네트워크 VLR/SGSN에서 USIM으로 받은 EMSI를 HE/UIDN에 보내면, UIDN은 f7 함수를 이용하여 EMSI로부터 IMSI를 계산한 후 f10 함수를 이용하여 TEMSI를 계산하여 IMSI와 TEMSI를 SN/VLR/SGSN에 보낸다.

강화된 사용자신분 비밀성 메커니즘은 계속 수정중에 있으며 Release 2000에서 완료될 계획이다.

2.5 KASUMI



(그림 7) 영구 사용자 ID의 암/복호화

이 절에서는 표준 3GPP 암호화 알고리즘 f8과 무결성 알고리즘 f9의 요구사항, 설계 및 평가와 관련된 제반사항 및 블록암호알고리즘 KASUMI를 사용한 자세한 구조를 살펴본다. 암호화 알고리즘 f8과 무결성 알고리즘 f9의 요구사항은 다음과 같다.

- f8 함수는 동기식 스트림 암호이고 f9 함수는 MAC 함수여야 함
- 저 전력과 작은 게이트 수의 소프트웨어 및 하드웨어 구현이 가능해야 함
- 전수 키 조사보다 더 효율적인 공격법이 없어야 함
- 터미널(또는 USIM)에 대한 수출제약이 없어야 함 : Wassenaar 협정(1998)에 따라 licence를 가지면 네트워크 장비를 수출할 수 있음
- 6개월 이내에 개발해야 함

설계기관으로 임명된 ETSI SAGE는 짧은 개발시간 때문에 기존의 알고리즘을 바탕으로 개발하기로 결정하고 f8과 f9를 위한 building 블록으로 블록 암호 MISTY1을 이용하기로 했는데 그 이유는 다음과 같다.

- 충분히 연구되었으며, 증명할 수 있는 security aspects를 가짐
- 변수 크기가 적당함
- 하드웨어와 소프트웨어에 효율적으로 설계되었음
- Mitsubishi가 로열티없이 무료로 제공

알고리즘의 설계는 Gert Roelofsen 주도의 SAGE 팀과 Mitsubishi의 Mitsuru Matsui(MISTY의 설계자) 등의 외부 전문가에 의해 이루어졌으며, 평가는 SAGE 평가팀과 Nokia, Ericsson, Motorola의 평가자들과 외부 평가기관으로 Leuven 대학, Ecole Normale, Royal holloway가 참가하였다.

MISTY1 알고리즘을 변형한 KASUMI(MISTY의 일본말) 알고리즘의 특징은 MISTY와 비교해서 다음과 같다.

- MISTY보다 단순한 키 스케줄 사용
- Cryptanalysis를 복잡하게 하는 부가적인 함수 사용
- 통계적인 성질을 향상시키기 위한 변화
- 하드웨어를 단순화하고 속도를 향상시키기 위한 변화

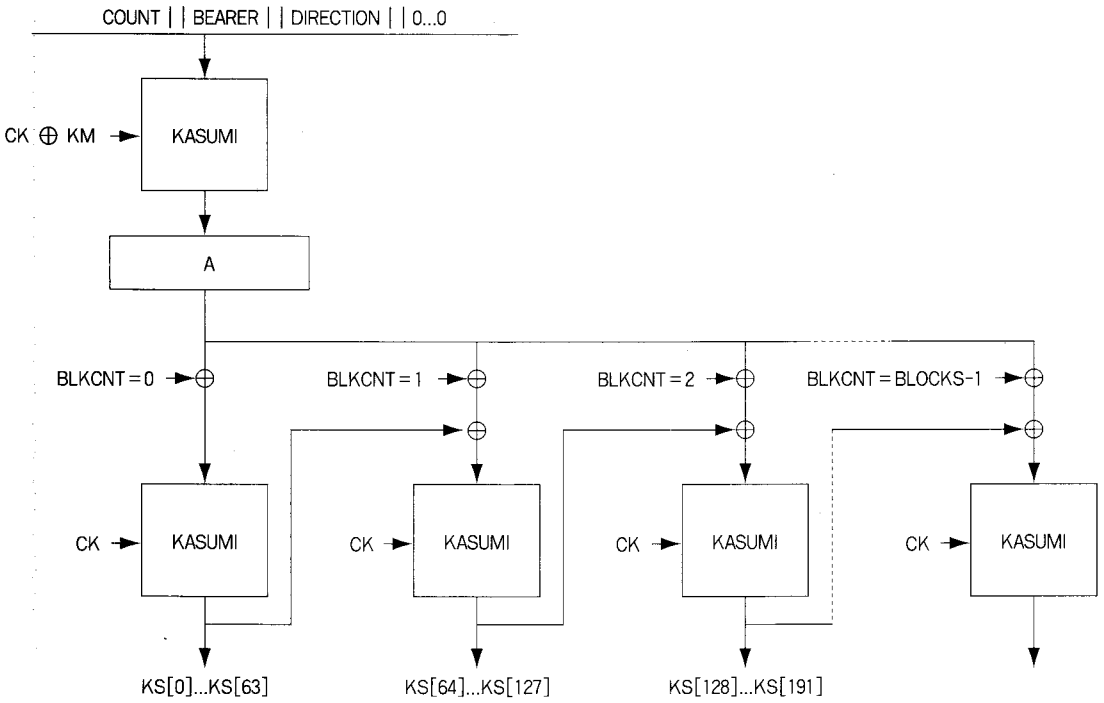
스트림 암호 f8은 output feedback 모드로 KASUMI를 사용하였다. 부가적으로 cycling을 방지하기 위하여 BLKCNT(Block Count)를 사용하였으며, 선택 평문 공격과 충돌을 방지하기 위하여 초기의 별도의 암호화 과정을 추가하였다. KASUMI를 사용한 f8의 구조는 다음장 (그림 9)와 같다. 무결성 함수 f9는 CBC MAC 모드로 KASUMI를 사용하였으며 2nd feedforward의 nonstandard addition을 이용하였다. 동작 모드는 다음장 (그림 10)과 같다.

2000년 9월 초 현재 KASUMI 알고리즘의 완전한 구조는 공개되지 않았다. 하지만 2000년 7월 18-19일 중국 베이징에서 열린 3GPP OP 3차 회의에서 공개검증 문제가 논의되었고 조만간 KASUMI의 자세한 구조가 밝혀질 것으로 보인다.

3. 3GPP2 정보보호 알고리즘 기술동향

3.1 CDMA2000 정보보호

진화된 ANSI-41 핵심망을 기반으로 하고 무선 접속기술로는 cdma MC방식을 채택한 시스템으로 3GPP2에 의해 규격화되고 있는 cdma2000에서의 인증은 기존의 IS-54나 IS-95의 인증방식과 매우 유사하다. 인증은 처음 가입할 때 주어지는 비밀 키인 A-key와 공유 비밀 자료(SSD)에 대한 지식을 보임으로써 이루어진다. Global(Broadcast) Challenge와 Unique Challenge의 인증방식을 제공하며, 보조절차로써 SSD 갱신 및 COUNT 갱신 등이 있다. SSD는 A-key로부터 생성되며 128 비트로 구성되는데, 이 중 64비트(SSD_A)는 인증 알고리즘에 사



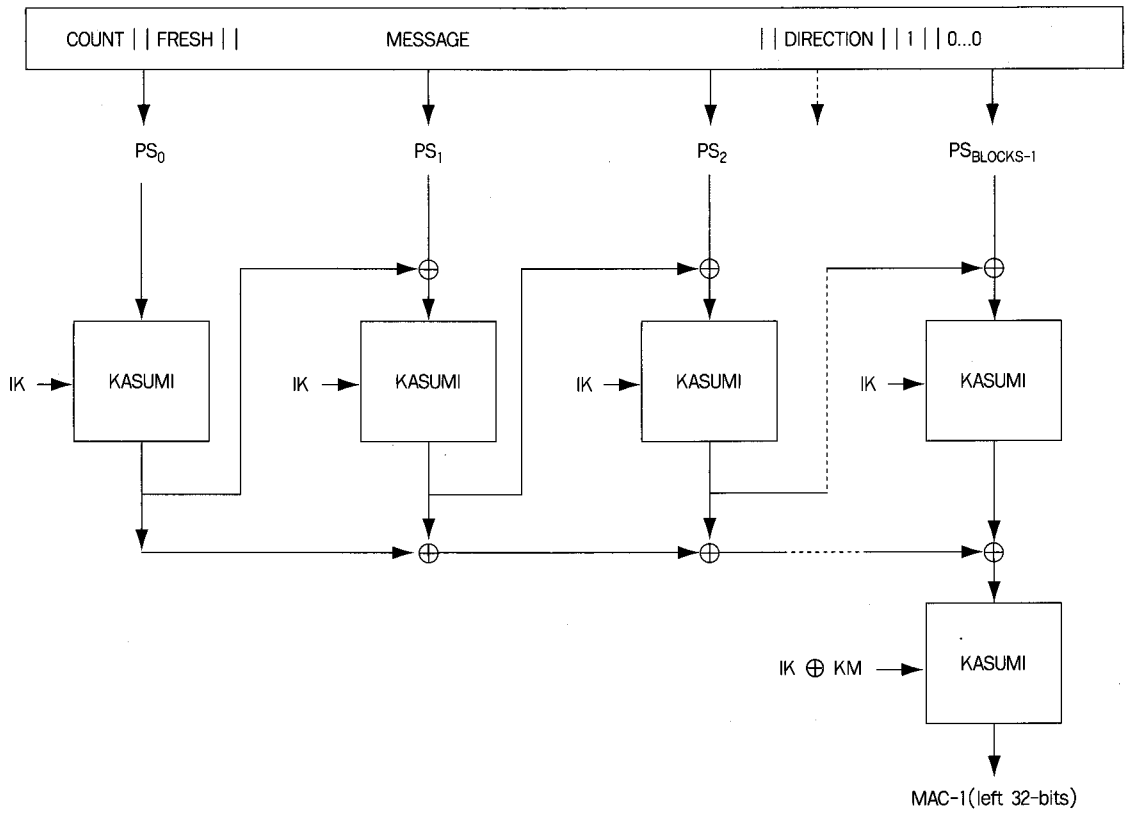
(그림 9) 암호화 알고리즘 f8

용되고 나머지 64비트(SSD_B)는 음성 비화(Vocie Privacy)와 메시지 암호화에 사용된다. SSD 갱신은 SSD 생성절차(SSD_Generation procedure)를 통하여 갱신된다. 등록인증 및 SSD 갱신과정 중 발생하는 기지국 인증과 유일 시도 인증 등에서는 모두 같은 알고리즘(Auth_Signature procedure)이 사용된다.

인증과정을 강화하고 가입자의 민감한 정보(예를 들면, PIN)를 보호하기 위한 방법으로 시그널 메시지 암호화를 수행하며 이를 위해 Cellular Message Encryption Algoritym이 필요하다. CDMA 모드에서의 음성 비화는 Pseudo Noise를 이용한 개인용 긴 코드 마스크 방법을 이용하여 이루어지며, cdma2000에서는 IS-95에는 없는 계층 3의 시그널링 서비스 데이터 유닛(SDU)를 암호화하는데 사용될 수 있는 시그널 메시지와 사용자 정보의 확장된 암호화를 수행할 수 있다. ANSI-41 네트워크에서 비동기식 W-CDMA(또는 CDMA-DS) 접속을 허용하는 경우, 즉 DS-41 시스템에서 인증절차는 cdma2000의 인증절차를 이용하고 메시지 암호화 복호화는 cdma2000의 확장된 암호화 절차를 따른다.

인증과 메시지 암호화 알고리즘에 사용되는 암호 알고리즘 CAVE는 짧은 키 길이와 안전성에 이미 약점이 드러나 강한 인증에 대한 요구가 나왔으며, 또 IS-95 시스템은 IMT-2000의 요구사항인 이동국과 네트워크의 상호인증을 보장하지 못한다. 이러한 필요성에서 3GPP2의 미국 표준개발 기구인 TIA의 TR-45 AHAG (Ad hoc Authentication Group)은 강화된 가입자 인증(ESA: Enhanced Subscriber Authentication)이라 불리는 인증방식에 관하여 작업을 진행하고 있다. 또한 CDMA 2000을 위한 ESP (Enhanced Subscriber Privacy) 알고리즘을 고려하고 있다.

3.2 ESA 관련 개발동향



(그림 10) 무결성 알고리즘 f9

ESA에 관한 요구사항과 개발과정을 정리하면 다음과 같다. ESA를 위해 CAVE알고리즘을 대치할 강화되고 안전성이 증명된 HASH함수의 사용과 키 길이를 128비트 정도로 늘리기로 하였다. 후보 HASH 함수로서 MD5, SHA-1, MD4를 기반으로 한 KT proposal, 그리고 Advanced Hash Algorithm이 고려되었는데, TR-45는 SHA-1을 채택하고 모든 키 길이를 128비트로 결정하였다. 또한 TR-45는 ESA 키 일치 프로토콜로 3GPP의 AKA를 선택하였으며, AKA에서 해쉬 함수로 SHA-1을 사용하기로 결정하였다. TR-45의 AHAG는 2000년 4월 중순 스톡홀름에서 열린 3GPP SA와의 협력회의에서 3GPP의 AKA를 위한 우선 알고리즘으로 SHA-1을 사용할 것을 SA에게 추천하였다. TR-45.1, TR-45.3, TR-45.4, TR-45.5는 ESA 절차와 관련하여 네트워크 프로토콜을 지지하기 위한 시그널링을 개발하고 있다.

4. 결론

3GPP 시스템의 경우 본 고에서 살펴본 f0~f10의 11개의 정보보호 알고리즘 이외에도 2세대 GSM 시스템과의 역방향 호환성(Backward Compatibility)을 제공하기 위해 관련되는 정보보호 알고리즘으로 c1~c5, 5개의 표준화된 알고리즘이 있다. 또한 네트워크 기반의 end-to-end security 보장을 위한 네트워크간의 정보보호 알고리즘과 GSM 기반의 GERAN 접근보호를 위한 정보보호 알고리즘에 관련된 사항이 Release 2000에서 고려될 것이다. 한편, 3GPP2의 CDMA2000의 완전한 인증절차는 TR-45의 ESA와 ESP에 대한 논의가 완결되어져야 분명

해질 것이다.

지금까지 유럽식 IMT-2000 시스템인 3GPP의 UMTS와 미국식 IMT-2000 시스템인 3GPP2의 CDMA2000의 정보보호 구조와 필요한 알고리즘 및 표준화 동향을 살펴보았다. 국제적인 3G 네트워크에서의 사용을 위한 표준화된 알고리즘의 개발과 이용을 위해 표준화 단체의 활동에 적극 동참하고 기술동향을 파악하는 것과 더불어 국내실정에 맞는 암호와 인증 알고리즘의 개발을 수행해야 할 것이다.

• **저자약력**

1988. 3~1990. 3 고려대학교 대학원 수학과(대수학 석사)
1991. 9~1996. 8 University of Kentucky(대수학 박사)
1997. 3~1998. 2 고려대학교 기초과학연구소 Post Doc.
1997. 6~1998. 5 학술진흥재단 Post Doc.
1997. 10~1999. 6 고려대학교 암호학 연구실 선임연구원
1999. 7~현재 한국전자통신연구원 선임연구원

참고문헌

[1] "Security Architecture", 3G TS 33.102 V3.5.0, July 2000.
[2] "Integration Guidelines", 3G TS 33.103 V3.2.0, March 2000.
[3] "Cryptographic Algorithm Requirements", 3G TS 33.105 V3.3.0, March 2000.
[4] "General Report on the Design, Specification and Evaluation of 3GPP Standard Confidentiality and integrity algorithms", 3G TR 33.908 V3.0.0, March 2000.
[5] "Use of SHA-1 for AKA f0-f5", 3GPP TSG SA WG3 Security-S3#13, May 2000.
[6] M. Walker, "On the Security of 3GPP Networks", Eurocrypt 2000.
[7] "Draft Report of SA WG3 Meeting #14", August 2000.
[8] "Open Publication of 3G Ciphering and Integrity Algorithms(Algorithms f8 and f9)", 3GPP OP#3, July 2000.
[9] "Upper Layer(Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems", cdma2000 Release A, June 2000.
[10] "Direct Spread Specification for Spread Spectrum Systems on ANSI-41(DS-41) (Upper Layers Air Interface)", 3GPP2 C.S0007-0, June 2000.
[11] "Removable User Identity Module(R-UIM) for cdma2000 Spread Spectrum Systems", 3GPP2 C.S0023-0, June 2000.
[12] "Ad-Hoc Authentication Group Meeting Summary", 3GPP2_S0020000606-009, June 2000.
[13] "The ESA Process", 3GPP S3-000276, April 2000.
[14] "TR45 Committee Correspondence Re: ESA Standards Development", 3GPP2_S0020000606-015A, June 2000.
[15] 장명국, "3GPP 알고리즘 배포·관리 방안", TTA 저널 6월호, 2000
[16] http://www.3gpp.org
[17] http://www.3gpp2.org