3GPP에서 IMT-2000용 보안 아키텍처 및 보안 알고리즘에 관한 연구

홍성남*, 최성*, 정일용*
*조선대학교 전자계산학과
e-mail:dory9241@stmail.chosun.ac.kr

The Study on Security Architecture and Security Algorithm on IMT-2000 of 3GPP

*Dept of Computer Science, Chosun University

요약

IMT-2000 시스템의 서비스는 회선 방식의 음성 및 데이터 서비스를 지원하는 기존 시스템의 기능을 포함하면서 데이터 전송률을 최대 2Mbps로 광대역화하여 고속 데이터 전송 등의 멀티미디어 서비스를 제공하며 국제 표준화된 이동 전화망의 접속 표준을 사용하여 글로벌 로밍 서비스가 제공된다. 그 중 정보보호 서비스의 요구는 기존 이동통신 시장에서와 같이 중요한 부분으로써 이미 ITU-R에서는 그 동안 발생한 보안 침범의 유형을 분석하고 방어 방법에 대한 연구를 진행하고 있다. 그러므로 본 논문은 국내 정보통신망 환경에서 적용될 IMT-2000 보안기술의 개발과 보안 구조의 국제 표준기술 연구개발을 위하여 3GPP에서 연구중인 UMTS(유럽형 IMT-2000)에서 표준화 작업중인 보안 아키텍처와 여기서 사용하는 KASUMI 알고리즘을 분석한다.

1. 서론

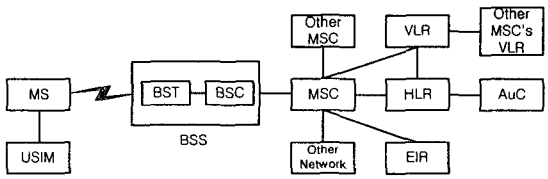
정보통신 서비스의 목표는 언제, 어디서나, 누구와도, 그리고 어떠한 서비스 유형이든지 서비스가 가능하도록 하는 것이며 현재 세계적으로 급속하게 보급되고 있는 이동통신서비스를 위한 무선통신망도 멀티미디어 서비스까지 지원할 수 있는 IMT-2000 (International Mobile Telecommunication-2000)망으로 진화하고 있다.[1]

그러나 IMT-2000에서는 이동단말의 발호나 착호시, 위치등록이나 위치 갱신시에 방문망의 전송로를 경유하여 단말기가 등록된 홈 망의 인증센터에서 인증과정을 수행하여 통보한다. 이를 위해 단말과 사용자, 그리고 인증센터는 인증에 필요한 비밀 데이터를 보유, 관리하고 있다. 그러나 현재 제시되어 있는 인증과정은 단말과 인증센터간에 비밀 데이터를 평문으로 전송하기 때문에 외부에 노출되기 쉽다는 문제점으로 IMT-2000의 보안원칙에 관련된 ITU-R M.1078에서는 서비스 관련, 접근제어 관련, 이동단말 관련, 사용자 관련, 네트워크 운용 관련, 및 보안관리 관련 등에 대해 최소한의 기본 요구사항을 제시하고 있으며, 3GPP의 TSG3-SA에서도 UMTS(유럽형 IMT-2000)용 보안 아키텍처 및 무결성 안내서와 암호화 알고리즘 요구사항 등의 표준화 작업을 보완해가며 계속해서 진행하고 있는데, 무선통신시스템의 보안위협에 대적할 수 있는 구체적인 방안이나 조치는 제시되지 않고 있다. 또한 국내 정보통신망 환경에서 적용될 IMT-2000 보안기술의 개발과 보안 구조의 국제 표준기술 연구개발 노력이 절실한 실정이다.[2]

본 논문의 2장에서는 IMT-2000의 네트워크 구조를 설명하고 그 기술동향을 기술하고, 3장에서는 IMT-2000의 보안구조와 기능화(functional)된 모듈 및 보안방식과 보안 알고리즘인 KASUMI에 대하여 기술하며, 4장에서 결론을 맺는다.

2. IMT-2000 기능망 구조

IMT-2000의 실현을 위해서는 다양한 네트워크 기술이 요구된다. 그림 1은 IMT-2000의 기능적 객체들의 상호 연결을 나타낸다[3][4].



(그림 1) IMT-2000 참조 모델

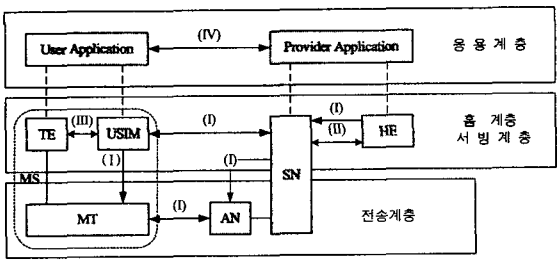
① MS(Mobile Station) : 이동국으로서 사용자 단말기
② BSS(Base Station System) : 기지국 하위 시스템으로서 BTS(기지국 송수신 시스템)과 BSC(기지국 제어기)로 구성
③ MSC(Mobile Switching Centre) : 이동 서비스 교환센터
④ HLR(Home Location Register) : 소속위치 기록
⑤ VLR(Visitor Location Register) : 이동국위치 등록
⑥ EIR(Equipment Identity Register) : 장비식별 등록
⑦ AuC(Authentication Center) : 가입자 인증에 관한 기능을 담당하는 인증센터
⑧ USIM(User Service Identity Module) : 가입자를 식별하기 위해 인자, 인증/암호화 알고리즘 및 식별번호 등이 저장된 Smart Card 형태의 모듈로 기술할 수 있다.

3. 보안 아키텍처

세계적으로 다양한 정보통신 기반구축 및 서비스 등장

으로 인하여 차세대이동통신, 전자상거래 등에서 민감한 정보를 보호할 수 있는 안정성과 신뢰성이 포함된 암호알고리즘의 개발이 요구되는 실정이다. 특히 차세대이동통신인 IMT-2000 3GPP 진영에서는 진화된 GSM 핵심망과 무선접속기술(W-CDMA)을 기반으로 하여 범세계적으로 적용할 수 있는 기술규격들의 작성을 거의 완료하였다[5].

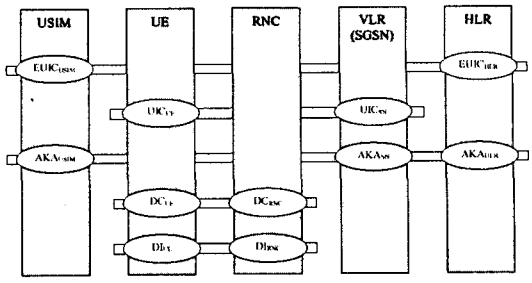
이 중 한 기술그룹인 TSG-SA에서는 3세대 이동가입자들의 인증부문에 적용할 새로운 체계의 Ciphering (F8) 및 Integrity(F9) 알고리즘을 설계하였는데 이를 통칭 3GPP 알고리즘이라 한다. 이 알고리즘은 1999년 5월 서울에서 개최된 3GPP 제2차 PCG(사업조정그룹) 회의에서 각 기관참가자들을 공동투자로 개발 및 시험키로 결정되어 추진되어 왔다[6][7]. 이 프로젝트는 유럽 표준화기구인 ETSI의 이동통신표준연구센터(MCC) 관리하에 TSG-SA산하 SAGE(Security Algorithm Group of Experts) 특별위원회에서 주도적으로 개발되었고, 이 과정에 일본 미쓰비시 암호기술인 MISTY가 기본으로 사용되었으며 일본에서는 이에 대한 지적재산권을 무료로 공개하였다. 이에 따라 한국의 표준화기관인 TTA에서도 3GPP 알고리즘의 공동소유 및 관리기관의 일원으로서 ARIB(일본), ETSI(유럽), T1(미국)과 함께 공동협약체결을 서면으로 진행하고 있으며 조만간 이에 대한 국내외 배포 및 관리가 시행되리라 본다.



(그림 2) IMT-2000 보안구조

3.1 보안구조

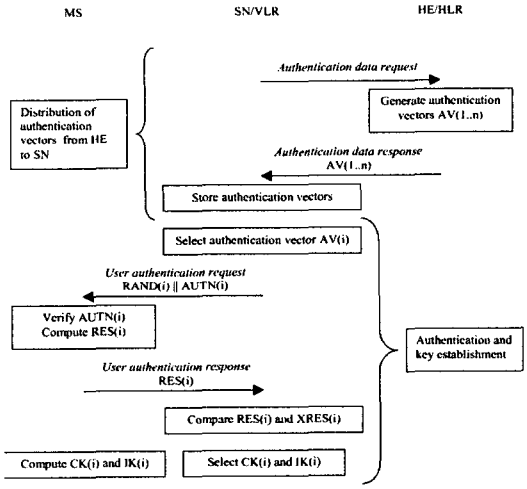
이에 관련된 IMT-2000에서 보안구조를 그림 2와 같이 특징 그룹으로 분류하자면 첫 번째는 Network access security (I)는 무선 링크상에서 가입자가 안전하게 기지국에 접속하는데 필요한 보안사항이고, 두 번째는 Network domain security (II)로서 각 도메인화 되어있는 네트워크상에서의 안전한 유선링크 접속에 필요한 보안사항이다[8][9]. 세 번째는 User domain security (III)로서 이동가입자 및 단말기의 접속에 사용되는 보안사항이며 마지막으로 Application domain security (IV)는 사용자의 응용프로그램과 서비스 제공자의 응용프로그램간의 메시지 교환에 필요한 보안사항으로 분류할 수 있다[10]. 그림 3은 보안구조를 기능적으로 분류한 것인데, 여기서 EUIC는 강화된(enhanced) 사용자 식별 비밀성이고, UIC는 사용자 식별 비밀성을 위한 일반 메카니즘이며, AKA는 인증과 키 협상을 위한 메카니즘으로서 사용자의 재인증을 위한 함수가 포함되어 있다. DC는 사용자 데이터와 시그널 데이터의 비밀성을 위한 메카니즘이고, DI는 시그널 데이터의 데이터 무결성용 메카니즘이다[11].



(그림 3) IMT-2000(UMTS)의 기능별 보안구조

3.2 인증과 키 공유(AKA)

사용자와 네트워크가 사용자의 HE내에 있는 USIM과 AuC사이에 공유되어지는 비밀키(K)을 보임으로써 상호인증을 제공하는 메카니즘이다. 또한 USIM과 HE는 각각의 네트워크 인증을 제공하기 위해 SEQ_{MS}와 SEQ_{HE}를 갖는다.



(그림 4) 인증과 키 협상

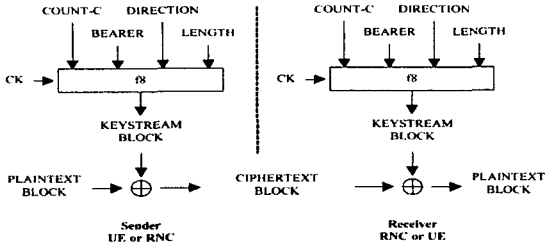
사용자 인증을 수행하기 위해 사용자의 HE로부터 새로운 인증벡터 배열을 VLR/SGSN에게 제공하고 도착한것 중 하나를 VLR이 선택하여 생성한 인증토큰(AUTN)을 MS에게 전송한다. MS는 이 토큰을 검증하여 사용자 인증과 암호키와 무결성키를 공유하게 된다.[11]

3.3 로컬 인증과 사용자 데이터의 무결성

인증과 키 세팅은 인증 프로시저에 의해 수행되고 네트워크 오퍼레이터가 희망할 때마다 네트워크에 의해 초기화된다. 키 세팅은 무선 가입자의 식별이 VLR/SGSN에 의해서 알려지면 곧 수행되어지며, CK와 IK는 VLR/SGSN에 저장되어 있다가 필요시 RNC로 전송되고 도메인용 CK와 IK은 USIM에 저장되다가 이 도메인의 차기 인증 시 갱신된다.

또한, 사용자의 데이터와 시그널링 정보 요소들의 비밀성 보호를 위하여 암호화 모드와 블록 암호화를 사용한다. 사용자 데이터의 암호화는 여러 가지 입력 파라

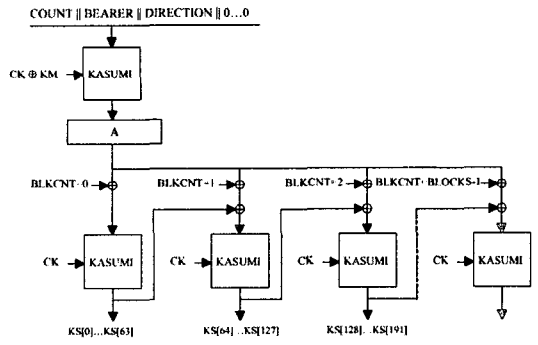
메터를 가지고 f8 함수를 이용하여 암호화할 원문 길이의 Keystream Block을 생성하고 이를 원문과의 XOR 연산으로 생성한다.



(그림 5) 사용자 데이터의 암호화와 RAN에서의 전송

3.4. KASUMI 암호 알고리즘의 구조

여기서는 함수 f8과 f9에 대하여 좀더 자세히 알아보도록 하겠다. 암호화 알고리즘 f8은 스트림 암호화 방식으로서 데이터의 암호화/복호화 블록에 암호키(CK)를 이용하여 사용하며, 데이터의 각 블록은 1에서 5114 비트 사이의 길이를 갖는데 이 알고리즘은 키스트림 생성기로서 output-feedback 형태의 KASUMI를 사용한다.



(그림 6) F8 keystream 생성기

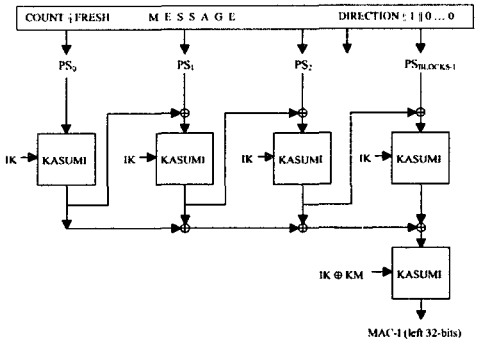
다음은 keystream 생성 알고리즘이다.[12]

(a) plaintext/cypertext는 LENGTH-bit(1-5114)로 구성되고, keystream 생성기는 이를 64비트의 스트림 비트로 재구성
(b) BLOCKS는 LENGTH/64와 같다.
ex. 만약 LENGTH = 128 이면 BLOCKS = 2,
(c) 각 keystream 블록(KSB)를 생성하기 위해 다음 연산을 수행 ($1 \le n \le BLOCKS$)
i.e $KSBn = KASUMI[A \oplus BLKCNT \oplus KSBn-1]_{CK}$
(d) keystream의 각 비트에 KSB1부터 KSBBLOCKS까지 대입됨 ($1 \le n \le BLOCKS$, $0 \le i \le 63$))
ie. $KS[((n-1)*64)+i] = KSB_n[i]$
(e) 암호화/복호화는 입력데이터(IBS)와 생성된 keystream(KS)의 XOR 연산으로 수행
i.e $OBS[i] = IBS[i] \oplus KS[i]$ ($0 \le i \le LENGTH-1$)

무결성 함수 f9는 무결성키(IK)를 이용하여 주어진 입력 메시지에 대해 32비트 MAC의 생성을 목적으로 CBC-MAC 모드의 형태로 KASUMI를 사용한다.[12]

다음은 MAC 생성 알고리즘이다.

(a) PS를 64비트 단위의 block으로 나눈다.
i.e $PS = PS0 \parallel PS1 \parallel PS2 \parallel ... \parallel PS_{BLOCKS-1}$
(b) 임시 변수 A와 B 세팅 ($0 \le n \le BLOCKS-1$)
i.e $A = KASUMI[A \oplus PSn]_{IK}$, $B = B \oplus A$
(c) 마지막으로 나온 B를 무결성키(IK)와 수정키 (KM)을 이용하여 KASUMI로 암호화
i.e $B = KASUMI[B]_{IK} \oplus KM$
(d) 결과로 나온 B의 상위 32비트를 MAC-I로 사용하고 나머지는 사용하지 않음
ie. MAC-I = lefthalf[B]
$MAC\text{-}I[i] = B[i]$ ($0 \le i \le 31$)



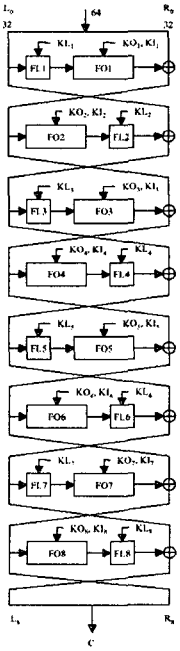
(그림 7) f9 MAC 생성기

KASUMI는 128비트 키를 컨트롤하여 64비트 입력으로 64비트 출력을 갖는 블록 암호화 알고리즘으로서 구조는 다음과 같다.[13]

- KASUMI는 서브키(KL, KO, KI)와 연관되어 함께 사용되는 세 개의 서브 함수(FL, FO, FI)로 구성됨
- 서브 함수들은 다수의 라운드로 이루어진 Feistel 구조를 이루어짐
- $XX_{i,j}$로 표현되는 서브 함수나 키에서 i는 KASUMI의 내부 라운드 번호이고, j는 외부 라운드 번호
- fi() : KASUMI의 i 번째 라운드 함수
- FI() : 16bit 입력과 서브키를 이용한 서브함수
- FL() : 32bit 입력과 서브키를 이용한 서브함수
- FO() : 두 개의 48bit 서브키를 이용한 32bit 입출력 서브함수
- K : 128 비트 키
- KLi,KOi,KIi : i 번째 라운드에서 사용하는 키
- S7[] : 7비트 입출력 S-box
- S9[] : 9비트 입출력 S-box

KASUMI는 8 라운드로 된 Feistel구조의 암호화 알고리즘으로서 다음의 과정으로 수행된다.

(a) 연산은 128비트 K를 사용하여 64비트 입력 I를 64비트 출력 OUTPUT을 생성
(b) 입력 I는 두 개의 32비트 스트링 L_0와 R_0로 나뉨
i.e $I = L_0 \parallel R_0$
(c) ($1 \le i \le 8$)까지 다음을 계산
i.e $R_i = L_{i-1}$, $L_i = R_{i-1} \oplus fi(L_{i-1}, RK_i)$
(d) 위의 계산을 8번 라운드하여 64비트 스트링($L_8 \parallel R_8$)을 출력(OUTPUT)으로 함
i.e $OUTPUT = KASUMI[I]_K$



(그림 8) KASUMI

다음은 KASUMI서브함수(fi, FL, FO, FI)의 설명이다.

① fi 함수 (그림 8 참조)

(a) 세 개의 서브키(KL_i, KO_i, KI_i)로 구성된 라운드키(RK_i)를 제어하여 32비트 입력 I를 32비트 출력 O로 변환시킴

(b) fi 함수는 FL과 FO함수로 구성되며, 짝수 라운드와 홀수 라운드 두 가지 형태

i.e 1, 3, 5, 7 라운드 : $fi(I, RK_i) = FO(FL(I, KL_i), KO_i, KI_i)$

2, 4, 6, 8 라운드 : $fi(I, K_i) = FL(FO(I, KO_i, KI_i), KL_i)$

② FL 함수 (그림 9 참조)

(a) 함수 Fl에서 입력은 32비트 입력 (I)와 32비트 서브키 (KL_i)로 구성됨

(b) 서브키(KL_i)는 16비트 $KL_{i,1}$, $KL_{i,2}$로 나뉨

i.e $KL_i = KL_{i,1} \| KL_{i,2}$

(c) 입력 I도 16비트 L과 R로 나뉨

i.e $I = L \| R$

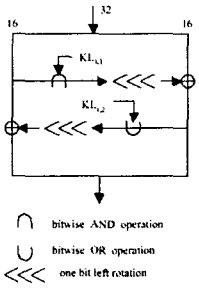
(d) 다음 R'과 L'를 계산

i.e $R' = R \oplus ROL(L \cap KL_{i,1})$

$L' = L \oplus ROL(R \cup KL_{i,2})$

(e) R'와 L'을 합하여 32비트 출력(O) 생성

i.e $O = L' \| R'$



(그림 9) FL 함수

③ FO 함수(그림 10 참조)

(a) 함수 FO의 입력은 32비트 입력 I와 48비트 서브키 두 쌍(KO, KI)으로 구성됨

(b) 32비트 입력I는 16비트씩 L_0와 R_0로 나뉨

i.e $I = L_0 \| R_0$

(c) 두 개의 48비트 서브키는 다시 3개의 16비트 서브키로 분할

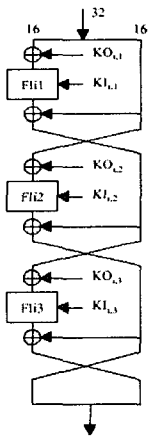
i.e $KO_i = KO_{i,1} \| KO_{i,2} \| KO_{i,3}$

$KI_i = KI_{i,1} \| KI_{i,2} \| KI_{i,3}$

(d) 다음을 ($1 \le j \le 3$)으로 계산

$R_j = FI(L_{j-1} \oplus KO_{i,j}, KI_{i,j}) \oplus R_{j-1}$

$L_j = R_{j-1}$



(그림 10) 함수 FO

(e) 위 식으로 출력된 L_3와 R_3를 합하여 32비트 출력 생성

④ FI 함수 (그림 11참조)

(a) 함수 FI는 16비트 입력 I, 16비트 서브키 $KI_{i,j}$를 입력으로하고 내부에서 S-box(S_7, S_9)로 계산

(b) 입력 I는 상위 9비트 L_0와 하위 7비트 R_0로 분할

i.e $I = L_0 \| R_0$

(c) 같은 방법으로 서브키 $KI_{i,j}$도 7비트 $KI_{i,j,1}$와 9비트 $KI_{i,j,2}$로 분할

i.e $KI_{i,j} = KI_{i,j,1} \| KI_{i,j,2}$

(d) 여기서 사용하는 S-box중, S7은 7비트 입출력 함수이고 S9은 9비트 입출력

(e) 비트열 교정 함수

ZE(x)는 7비트 입력값 x의 상위에 0을 2비트 추가

TR(x)는 9비트 입력값 x의 상위 2비트 삭제

(f) 다음을 계산

$R_1 = S9[L_0] \oplus ZE(R_0)$

$L_2 = R_1 \oplus KI_{i,j,2}$

$R_2 = S7[L_1] \oplus TR(R_1) \oplus KI_{i,j,1}$

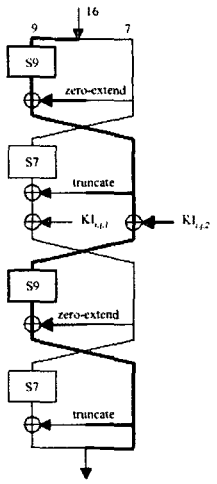
$L_3 = R_2$

$R_3 = S9[L_2] \oplus ZE(R_2)$

$L_4 = S7[L_3] \oplus TR(R_3)$

$R_4 = R_3$

(g) 마지막 계산된 L_4와 R_4를 합하여 출력 생성



(그림 11) 함수 FI

4. 결론

IMT-2000이 추구하는 목적을 실현하기 위해서 이미 아날로그나 디지털 이동통신에서 발생한 보안관련문제를 해결하는 대책이 서비스 제공 이전 시점에서 준비하여야 한다. 본 논문에서는 이를 위해 방어 방법을 연구하여온 ITU의 수집자료를 분석하였으며 표준화관점에서 국내 표준화 설계를 위해 3GPP의 기반기술과 표준안 분석을 수행하였다. 향후 연구는 동기식(3GPP2)의 보안구조를 분석하고, 이를 바탕으로 국내 정보통신망에서 적용될 IMT-2000 보안기술을 개발하고 국내 정보통신망에 적합한 보안 시스템의 개발을 목표로 하겠다.

5. 참고 문헌

[1] 이태훈, 정일용, 김용득, "IMT-2000에서 안전한 전송을 위한 ID정보기반 인증메카니즘의 설계", 통신학회논문지, 제23권, 제12호, 1998.12

[2] ITU-R Rec.M1078, "Security Principles for Future Land Mobile Telecommunications Systems"

[3] ETSI, TS 123 060, "General Packet Radio Service (GPRS); Stage 2", 2000.4

[4] 정만영, 김기선, 최정희, "21세기 이동통신", 시그마 프레스, 2000

[5] 장면국, "3GPP 알고리즘 배포 · 관리 방안", TTA 저널 6월호, 2000.6

[6] ETSI, 3G TS 33.105: "Cryptographic Algorithm Requirements" 2000.3

[7] ETSI, 3G TS 21.133, "Security Threats and Requirements", 2000.1

[8] ETSI, UMTS 33.21, "Security requirements", 1999.2

[9] ETSI, UMTS 33.22, "Security features", 1999.2

[10] ETSI, TS 133.102, " Security Architecture", 2000.1

[11] ETSI, TS 133.103, "Integration Guidelines", 2000.3

[12] 3GPP, TS 35.201, "Specification of the 3GPP confidentiality and integrity algorithms; Document1: f8 and f9 specifications"., 2000.10

[13] 3GPP, TS 35.202, "Specification of the 3GPP confidentiality and integrity algorithms; Document2: Kasumi algorithm specification", 1999.12