情 報 保 護 學 會 誌
第 12 券 第 5 號, 2002. 10

GSM, EDGE, GPRS 시스템의 새로운 표준 암호 알고리즘 분석

홍 도 원*, 류 회 수*

요 약

GSM(Global System for Mobile Communications)은 현재 가장 광범위하게 사용되고 있는 디지털 이동 통신의 표준이다. 또한 GSM 표준에서 데이터 전송의 최종 evolution 버전인 EDGE(Enhanced Data for GSM Evolution)와 GSM Phase 2+ 개발의 일부분인 GSM 망에서 packet switching을 구현하는 기술인 GPRS(General Packet Radio Service)가 현재 유럽의 정보통신 표준화 기구인 ETSI(European Telecommunications Standards Institute)에 의해 표준화가 진행 중에 있다. GSM 시스템은 사용자 데이터의 기밀성을 보장하기 위한 암호화 알고리즘 A5를 사용하고 있지만 그 취약성이 계속 보고되고 있다.[10,11] 따라서 GSM의 강화된 암호화 알고리즘과 EDGE와 GPRS에서 사용자 데이터를 보호하기 위한 새로운 암호화 알고리즘의 개발이 요구되어왔다. 최근 ETSI의 SAGE(Security Algorithms Group of Experts)는 이러한 목적을 달성할 수 있는 새로운 표준 암호화 알고리즘 A5/3과 GEA3을 개발하였다.[3,4,5,6] 본 고에서는 GSM, EDGE, GPRS에서의 새로운 표준 암호화 알고리즘 A5/3과 GEA3을 분석하여 정리하고자 한다.

Ⅰ. 서 론

이동 통신 시스템의 보안 요구사항과 서비스는 사용자와 기지국 사이의 무선 통신 때문에 고정망에서의 통신과는 근본적으로 다르다. 사용자 지역 교환국 사이에 깔린 전화선이 로밍과 과금과 같은 목적을 위한 사용자의 신원 확인을 제공하는 유선망과 달리, 무선 이동 통신에서는 누군가가 다른 사람의 신분으로 위장하는 것을 방지하기 위한 암호학적 인증 절차가 필요하다. 또한 무선 구간의 도청자가 사용자 데이터를 가로채거나 시스널링 데이터를 도청하여 사용자의 위치를 추적하는 것과 같은 위협을 막기 위한 암호학적 암호화 절차가 필요하다.

현재 전세계적으로 가장 광범위하게 이용되고 있는 음성 서비스 위주의 2세대 셀룰러 이동통신 시스템인 GSM은 무선 구간에서 사용자 음성 및 시스널링 데이터의 기밀성을 보호하고 이동단말기 사용자의 신원을 확인하기 위한 보안 관련 서비스를 제공하고 있다. 특히 무선 구간에서 사용자 데이터의 기밀성을 제공하기 위하여 스트림 암호 A5/1 또는 A5/1보다 좀 더 안전성 강도가 약한 A5/2를 사용하고 있다. 하지만 A5 알고리즘은 설계의 취약성이 계속 보고되고 있다.[10, 11] 따라서 GSM의 무선 구간에서 사용자와 시스널링 데이터의 암호화에 사용될 수 있는 강화된 알고리즘의 개발이 필요해 졌다. 또한 유럽 정보통신 표준화 기구인 ETSI에 의해 표준화가 진행 중인 GSM 시스템에서 데이터의 전송률을 향상시키고자 하는 EDGE와 GSM 망에서 packet switching을 구현하는 기술인 GPRS에서도 사용자 데이터에 대한 보호가 요구되고 있다.

이러한 요구에 따라 최근 ETSI의 암호 전문가 그룹 SAGE는 GSM과 EDGE에서 사용될 수 있는 새로운 표준 암호화 알고리즘 A5/3과 GPRS에서 사용되는 암호화 알고리즘 GEA3을 개발하였다. 이들 알고리즘들은 GSM 핵심망에 기반한 WCDMA 방식의 무선 접속기술 규격을 개발하는 3GPP(3rd Generation Partnership Project)에 의해 개발된 3GPP 암호화 알고리즘 f8[7]의 설계 원리와 핵심 블록 암호 알고리즘 KASUMI[8]를 근간으로 개발되었다. 본 고에서는 새로운 표준 암호화 알고리즘 A5/3과 GEA3을 분석하고자 한다.

* 한국전자통신연구원 ({dwhon, hsryu}@etri.re.kr)

II. 블록 암호 KASUMI와 스트림 암호 KGCORE

이 절에서는 먼저 A5/3과 GEA3 알고리즘의 핵심 함수로 사용되는 3GPP f8 함수의 확장이라 할 수 있는 KGCORE 함수[3]와 이 KGCORE 함수의 핵심 블록으로 사용되는 64비트 입출력 길이과 128비트 키를 가진 블록 암호 KASUMI에 대해 간략하게 기술한다.

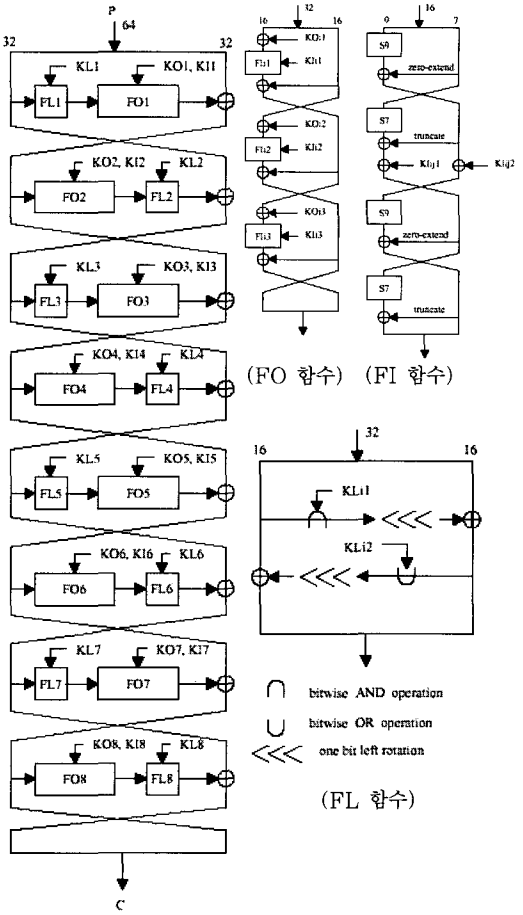
2.1 KASUMI

KASUMI는 64비트 입출력 길이와 128비트의 키 길이를 갖는 블록 암호이다. 전체 구조는 8라운드의 Feistel 구조로 블록도는 〈그림 1〉과 같다.

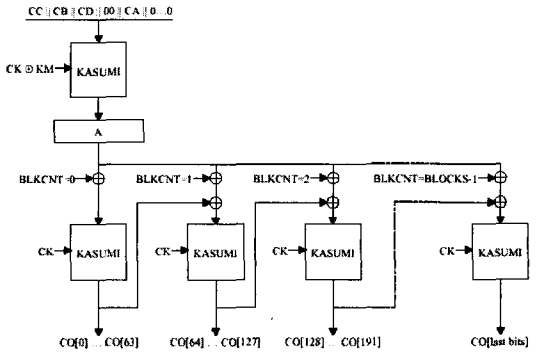
라운드 함수는 32비트 비선형 함수인 FO 함수와 32비트 선형 함수인 FL 함수로 구성된다. FO 함수는 다시 3라운드의 16비트 비선형 함수 FI로 구성되며, FI 함수는 비선형 S-box S7와 S9를 이용한 4라운드 구조이다. 이들 모든 라운드 함수에는 키 스케줄을 통해 생성된 128비트 라운드 키가 입력된다. S-box들의 규격과 라운드 키의 생성은 [8]을 참조하기 바란다.

2.2 KGCORE

A5/3과 GEA3에서 데이터 프레임의 암호화를 위해 사용되는 스트림 암호 KGCORE는 64비트 피드백을 가진 변형된 OFB(Output Feedback Mode) 모드로 KASUMI를 구성한다. 블록도는 〈그림 2〉와 같다. Pre-computation 단계에서 시스템 변수 CC, CB, CD, CA는 모두 0으로 설정되어 유도된 키 $CK \oplus KM$를 가진 KASUMI의 입력 블록이 된다. 여기에서 키 변형 상수 KM은 0x55555555555555555555555555555555이다. 이 KAUMI 알고리즘의 출력값은 64비트 레지스터 값 A이고, 이 값은 계속되는 KASUMI 계산에서 입력의 한 부분으로 이용된다. 입력 변수 CA는 GSM, EDGE, GPRS, UMTS f8 함수에서의 알고리즘 사용을 구분하기 위해 사용된다. 이 단계를 거치면 연속되는 64비트 키스트림 블록들이 output feedback mode로 추가적인 입력값 A와 블록 카운터 BLKCNT를 입력으로 KASUMI를 실행하여 생성된다. 그러면 암호문은 키스트림 비트들과 평문 비트들을 xor하여 구해진다.



〔그림 1〕 KASUMI 블록도



〔그림 2〕 KGCORE 함수

III. A5/3과 GEA3 암호화 알고리즘

A5/3과 GEA3 알고리즘을 설명하기 전에 먼저

GSM 03.20[2]에 명시된 GSM/EDGE에 사용되는 A5 알고리즘의 요구사항과 GSM 01.61[1]에 기술된 GPRS 암호화 알고리즘의 요구사항을 알아보자.

GSM

알고리즘 A5는 MS(Mobile Station)와 BS(Base Station)에서 수행된다. 암호화는 변조 전 인터리빙 후에 취해지며 복호화는 대칭적으로 복조 후에 일어난다. GSM 시스템에서 사용 중인 TDMA 기술 때문에 유용한 데이터는 114비트 블록으로 만들어야 하며, 이때 각 블록은 하나의 타임 슬롯 중 정상적인 버스트와 통합되어 전송된다. 기존 물리 채널을 위한 성공적인 슬롯은 최소한 한 프레임(약 4.615 ms)으로 분리되어야 한다. 따라서 암호화를 위한 A5 알고리즘은 매 4.615 ms마다 114 암호화/복호화 비트(BLOCK라고 불림)를 생성하여, 평문 114비트과 bit-wise 모듈러 2로 결합된다.

각 슬롯을 위해 복호화는 A5에 위해 생성된 처음 114비트 블록(BLOCK1)으로 MS쪽에서 수행되고, 암호화는 두 번째 생성된 블록(BLOCK2)으로 수행된다. 결론적으로 네트워크쪽에서는 BLOCK1이 암호화를 위해 사용되고 복호화를 위해서는 BLOCK2가 사용된다. 그러므로 A5 알고리즘은 매 4.614ms마다 114비트 2 블록을 반드시 생성하여야 한다.

EDGE

EDGE에서 블록 길이는 114비트보다 더 크다. EDGE에서 한 블록에서 유용한 정보는 116개의 심볼에 포함된다. 각 심볼은 3비트이므로 각 블록은 348비트를 포함해야 한다. 따라서 A5 알고리즘을 EDGE에서 사용하기 위해서는 BLOCK1과 BLOCK2가 384비트를 포함하도록 변경한다. 변경된 알고리즘은 TDMA 프레임(4.615ms)동안 348비트의 두 블록을 생성해야 한다.

EDGE은 상향이나 하향링크동안 평문 데이터 블록이 348비트보다 적은 것을 허용한다. 이 경우에는 단지 대응하는 출력 변수 BLOCK의 첫 번째 부분만이 bit-wise 결합으로 이용되고 나머지 비트들은 버려진다.

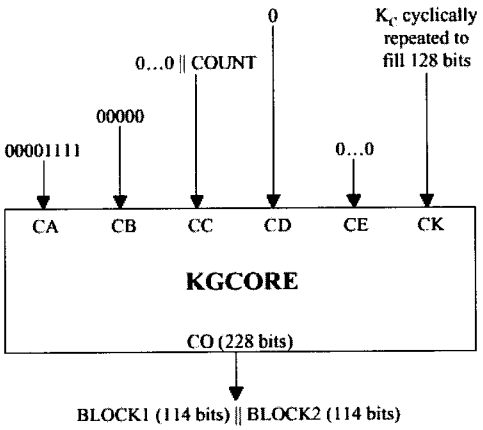
GPRS

알고리즘은 Serving GPRS Support Node (SGSN)과 MS에서 수행된다. 상향과 하향링크 전송은 독립적이다. 따라서 상향과 하향링크를 위한 암호화는 각각 독립적이어야 한다. 이것은 양 방향을 위한 키스트림들이 같은 입력으로 생성되는 A5 알고리즘과 반대이다.

단지 하나의 시간 슬롯 GPRS 통신을 허용하는 MS의 각 방향에서 최대 용량은 21.4 kbit/s(전체 42.8 kbit/s)이고, 500 octet의 패킷 길이를 가정하고 시간당 12 번의 초기화가 가정된다. MS는 양 방향에서 모두 8개의 시간 슬롯의 최대 처리능력을 가져야 하는데 각각은 최대 21.4 kbit/s로 전송하고 수신해야 한다.(전체 342.4 kbit/s) 500 octet의 패킷 길이를 가정하고 시간당 100 번의 초기화가 가정된다.

3.1 GSM 암호화를 위한 A5/3 알고리즘

GSM A5/3 알고리즘은 두 개의 114비트 키스트림 스트링을 생성하며, 하나는 상향링크 암호화/복호화를 위해 사용되고 다른 하나는 하향링크 암호화/복호화를 위해 사용된다. A5/3 알고리즘은 핵심함수 KGCORE를 이용해서 다음 〈그림 3〉과 같이 정의된다.

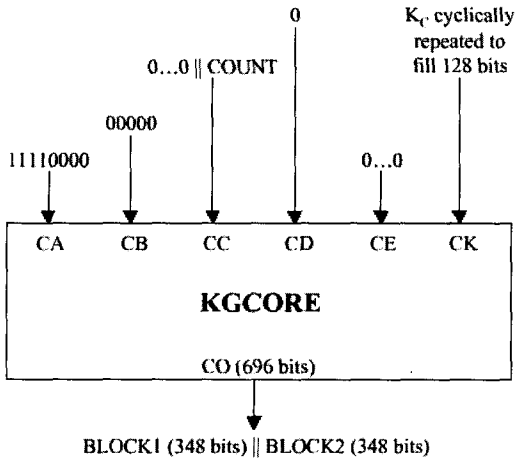


〔그림 3〕 GSM A5/3 키스트림 생성 함수

알고리즘의 입력값은 TDMA 프레임 번호에서 유도되는 22비트의 COUNT와 64-128비트를 가질 수 있는 암호화 키 K_C이다. 현재 GSM 표준은 A8 알고리즘을 이용하여 64비트의 K_C를 생성하지만 강화된 알고리즘을 위해 128비트까지를 허용한다. 시스템 변수들의 값은 그림 3에서와 같은 값으로 정의된다. 알고리즘의 출력값은 각각 114비트의 BLOCK1과 BLOCK2이다.

3.2 EDGE 암호화를 위한 A5/3 알고리즘

EDGE A5/3 알고리즘은 두 개의 348비트 키스트림 스트링을 생성하며, 하나는 상향링크 암호화/복호화를 위해 사용되고 다른 하나는 하향링크 암호화/복호화를 위해 사용된다. A5/3 알고리즘은 핵심 함수 KGCORE를 이용해서 다음 그림 4와 같이 정의된다.



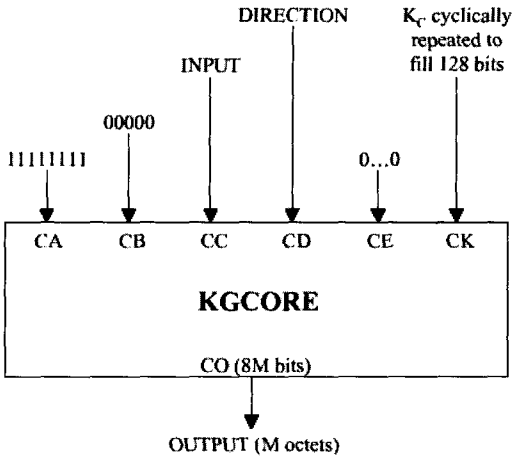
〔그림 4〕 EDGE A5/3 키스트림 생성 함수

알고리즘의 입력값은 GSM A5/3 알고리즘과 같고 사용되는 시스템 변수 값 중 함수를 구별하기 위한 CA값을 제외하고는 모두 GSM A5/3 함수와 같다. 하지만 출력값은 696비트를 가지며 이는 각각 348비트의 BLOCK1과 BLOCK2로 구성된다.

3.3 GPRS 암호화를 위한 GEA3 알고리즘

GPRS GEA3 알고리즘은 M 바이트 키스트림 스트링을 생성한다. M은 가변이며, 규격에서 M은 $2^{16}=65536$을 초과할 수 없다. GEA 알고리즘은 핵심 함수 KGCORE를 이용해서 다음 그림 5와 같이 정의된다.

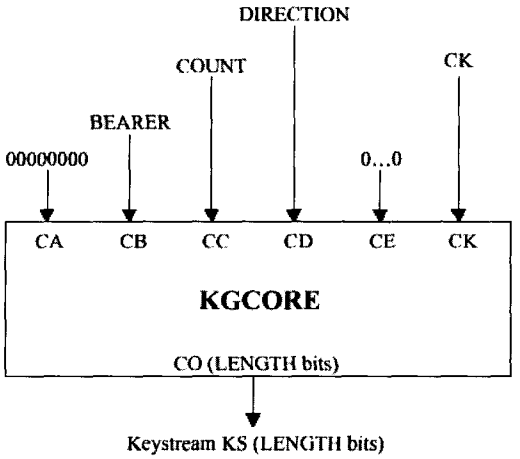
알고리즘의 입력값은 프레임에 의존하는 32비트의 INPUT, 전송 방향을 지시하는 1비트의 DIRECTION, 64-128비트를 가질 수 있는 암호화 키 K_C, 1부터 65536 사이의 요구되는 출력의 octet의 수를 나타내는 M이다. 그리고 사용되는 시스템 변수 값 중 함수를 구별하기 위한 CA값을 제외하고는 모두 GSM A5/3 함수와 같다. 출력값은 8M비트의 OUTPUT 스트링이다.



〔그림 5〕 GEA3 키스트림 생성 함수

3.4 3GPP 암호화 알고리즘 f8

A5/3과 GEA 알고리즘은 이미 개발된 3GPP 암호화 알고리즘 f8[7]과 유사하다. 이점을 분명히 하기 위해 이 절에서는 핵심 함수 KGCORE를 사용하여 〈그림 6〉과 같이 f8 알고리즘을 표현할 수 있음을 보인다.



〔그림 6〕 3GPP f8 키스트림 생성 함수

f8 함수의 입력값은 프레임에 의존하는 32비트 COUNT, 5비트의 BEARER, 전송 방향을 지시하는 1비트의 DIRECTION, 128비트 암호화 키 CK, 암호화/복호화되는 비트의 수를 나타내는

LENGTH이며, f8 함수를 거쳐 키스트림비트 KS를 출력한다. 이 f8함수를 KGCORE 함수로 표현하면 단지 CA와 CE를 0으로 할당하고 나머지 시스템 변수는 〈그림 6〉과 같이 대치하면 된다.

3.5 A5/3과 GEA3 알고리즘의 안전성

A5/3과 GEA3 알고리즘 설계의 이론적 근거와 알고리즘의 안전성에 대한 자세한 분석 및 평가는 [6]을 참고하라. 블록 암호 KASUMI의 안전성과 3GPP f8 함수와 비슷한 핵심 함수 KGCORE의 안전성은 이미 [9]에서도 자세히 분석되어 안전한 것으로 여겨진다. 따라서 A5/3과 GEA3에서 사용된 암호화 모드에 대한 분석이 필요하다.

A5/3과 GEA3 구성에 대한 공격이 고려되었다. 긴 키스트림 수열(2^{38} 비트)이 주어졌을 때, 공격으로 분류될 수 있을 만큼의 키스트림의 일부를 구별할 수 있다. 하지만 GSM/EDGE/GPRS 구조에서, 이와 같은 긴 키스트림 프레임은 발생하지 않으므로 실용적인 관점에서 잘 설계된 것으로 간주된다.

IV. 결 론

본 고에서는 최근에 ETSI SAGE의 task forth 팀에 의해 개발된 GSM 시스템에서의 사용자 음성 및 시스널링 데이터의 기밀성을 보호하는 A5 알고리즘의 강화된 버전인 A5/3 알고리즘을 분석하였다. 또한 현재 표준화가 진행 중인 GSM 시스템에서 데이터 전송률을 향상시키고자 하는 EDGE와 GSM 망에서 packet switching을 구현하는 기술인 GPRS에서의 사용자 데이터를 보호하기 위한 표준 암호화 알고리즘 A5/3과 GEA3에 대하여 살펴봄으로써 표준 규격을 따르는 GSM/EDGE/GPRS 시스템 및 단말기 개발에 참고할 수 있도록 하였다.

참고문헌

[1] GSM 01.61 "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements"

[2] GSM 03.20: "Difital cellular telecommunications system (Phase 2+); Security related network functions"

[3] ETSI/SAGE Specification. Specification of the A5/3 Encryption Algorithms for GSM and EDGE, and the GEA3 Encription Algorithm for GPRS; Document 1: A5/3 and GEA3 Specifications. Version: 1.0; Date: 30th May 2002.

[4] ETSI/SAGE Specification. Specification of the A5/3 Encryption Algorithms for GSM and EDGE, and the GEA3 Encription Algorithm for GPRS; Document 2: Implementors' Test Data. Version: 1.0; Date: 27th May 2002.

[5] ETSI/SAGE Specification. Specification of the A5/3 Encryption Algorithms for GSM and EDGE, and the GEA3 Encription Algorithm for GPRS; Document 3: Design Conformance Test Data. Version: 1.0; Date: 27th May 2002.

[6] ETSI/SAGE Specification. Specification of the A5/3 Encryption Algorithms for GSM and EDGE, and the GEA3 Encription Algorithm for GPRS; Document 4: Design and Evaluation Report. Version: 1.0; Date: 17th May 2002

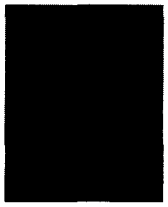
[7] 3GPP TS 35.201: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specification".

[8] 3GPP TS 35.202: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: KASUMI algorithm specification".

[9] 3G TR 33.908: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Report on the Design, Specification and Evaluation of 3GPP Standard

Confidentiality and Integrity Algorithms".
[10] J. D. Golic, "Cryptanalysis of Alleged A5 Stream Cipher", Advances in Cryptology EUROCRYPT '97, pp.239-255, 1997.
[11] A. Biryukov, A. Shamir, D. Wager, "Real Time Cryptanalysis of A5/1 on a PC", FSE 2000, pp. 71-79, 2000.

〈者著紹介〉



홍 도 원 (Do-Won Hong)
정회원
1994년 2월 : 고려대학교 이과대학 수학과(학사)
1996년 2월 : 고려대학교 수학과(석사)
2000년 2월 : 고려대학교 수학과(박사)
2000년 4월~현재 : 한국전자통신연구원 선임연구원
관심분야 : 정보보호 이론, 이동통신 정보보호

류 희 수 (Hee-Soo Yu)
정회원
1990년 2월 : 고려대학교 이과대학 수학과(학사)
1992년 2월 : 고려대학교 수학과(석사)
1999년 5월 : Johns Hopkins University 수학과(박사)
2000년 7월~현재 : 한국전자통신연구원 선임연구원
관심분야 : 정보보호 이론, 이동통신 정보보호