2000年度 大韓電子工學會 秋季綜合學術大會 論文集 第23卷 第2號 2000/11

VHDL을 이용한 GSM 시스템의 A3 알고리즘 구현

엄 세 욱, 김 규 철
단국대학교 컴퓨터공학과
전화 : 02-709-2860 / 핸드폰 : 017-725-7489

Implementation of A3 Algorithm for GSM System Using VHDL

Se-Wook Eom, Kyu-Chull Kim
Dept. of Computer Engineering, Dankook University
E-mail : eomse99@dankook.ac.kr

Abstract

GSM(Global System for Mobile Communication) system which is being used in Europe is composed A3, A5 and A8 algorithms. In this paper we implement A3 algorithm using VHDL, and verify the design by simulation. The A3 algorihm is divided into 3 parts, the encryption part, in which F-function encrypts 64 bit block data; the key generation part, which produces 32 bit subkeys; the control part, which produces the control code.

I. 서론

무선통신 기술의 발달로 언제 어디서나 원하는 사람과 통신이 가능하게 되어가고 있다. 이러한 이동 통신망은 기존의 공중 전화망이나 데이터망과 연결되고, 점차적으로 ISDN과도 접속이 가능하도록 발전되어 가고 있다. 그러나 이동 통신망에서는 무선 채널을 통하여 정보가 전달되므로 정보가 도청될 가능성이 크고, 조작될 가능성이 있으므로 안전한 정보 교환을 위해서 통신망 차원의 정보보안 대책이 필요하다.[7]

GSM은 유럽의 ETSI에 의해 제안된 TDMA 이동통신 방식으로, 보안 기능 실현에 인증 알고리즘인 A3와 키생성 알고리즘인 A5, 그리고 암호화 알고리즘인 A8의 세 가지 알고리즘을 사용한다. 이 중 A3, A8 알고리즘은 표준화되어 있지 않으므로 자국에 맞는 암호 알고리즘을 사용하여도 된다.[1,7]

본 논문에서는 GSM 시스템의 보안에 관련된 기능들과 암호 알고리즘, 그리고 암호 알고리즘인 A3, A8에 대용할 수 있는 알고리즘을 살펴보고, A3 알고리즘의 하드웨어 구현에 관하여 설명한다. A3 알고리즘은 암호화부, 키생성부, 제어부의 세 가지로 나누어 탑다운 방식으로 구현되었으며, 각 부분들은 하드웨어의 크기를 줄이기 위하여 직렬(serial) 방식으로 바꾸어 순차회로로 구현하였다.

II. GSM 시스템

2.1 GSM 시스템의 보안 기능

GSM 시스템의 보안 기능은 가입자 ID 인증 및 가입자 ID 보호 그리고 무선 구간에서의 데이터 기밀성 등 3가지로 구분된다.

가입자 ID 인증은 불법 가입자가 통신망으로부터 정보를 획득하는 것을 방지하기 위한 것이며, 가입자 ID 보호는 등록된 가입자 ID 정보 누출을 방지하고, 무선 구간에서의 데이터 보호는 무선 채널 특성상 노출되는 정보의 보호를 위한 것이다.[1,4,7]

2.2 GSM 시스템의 보안 구조

GSM 시스템에서는 보안 기능 실현에 인증 알고리즘인 A3와 키생성 알고리즘인 A5 그리고 암/복호화 알고리즘인 A8의 세 가지 알고리즘이 사용된다.

(1)A3 알고리즘

A3 알고리즘을 사용한 인증절차는 그림 2와 같다. 기지국에서 128 비트의 난수 RAND가 발생되어 이동국으로 전달되면, 이동국에서는 RAND와 128 비트의 키를 사용해 32 비트의 SRES'를 계산하고 결과를 기지국으로 보낸다. 기지국에서는 이 SRES'와 기지국에서 계산된 SRES 값을 비교해 같을 경우에만 가입자 인증이 완료된다.

A3 알고리즘은 GSM에서 표준화되어 있지 않은 관계로 통신망 관리자가 적당한 알고리즘을 선택해 주어진 RAND와 SRES로부터 인증키를 유출하기가 불가능하도록 설계되어야 한다.[4,7]

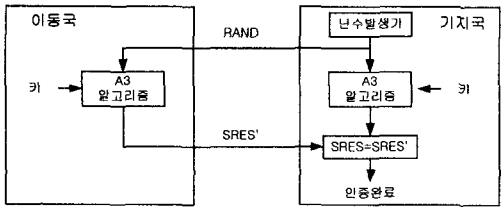

그림 2. 가입자 인증 절차

(2) A8 알고리즘

A8 알고리즘은 A3와 동일한 입력 파라미터를 사용하여 암호키를 생성하는 데 이용된다. 이 알고리즘은 인증 절차가 완료된 후에 사용되며, 표준화되어 있지 않다.

(3) A5 알고리즘

A5/0, A5/1, A5/2를 사용하도록 표준화가 이루어져 있으며, 데이터의 암/복호화시 사용된다. A5 알고리즘의 입력으로는 A8 알고리즘으로 생성된 64 비트 암호키와 TDMA 프레임 번호가 사용되며, 4.615 msec 마다 114 개의 PN(pseudo noise)비트 수열을 생성한다. 생성된 PN비트 수열과 데이터가 XOR 연산을 수행함으로써 암호문이 생성된다.[4,7]

Ⅲ. 새로운 블록 암호알고리즘

본 논문에서 구현하고자 하는 A3 알고리즘에서 사용되는 블록 암호 알고리즘은 64 비트의 평문을 64 비트 암호문으로 바꾸는 암호 알고리즘으로 A3, A5, A8 알고리즘 모두에서 사용이 가능하도록 64 비트와 128 비트의 키를 모두 사용할 수 있게 설계되었다. 이 알고리즘의 구조는 Feistel 구조이며, F함수는 32 비트 블록을 4 개의 8 비트 블록으로 나누어 기본연산을 수행한다. F함수에 입력되는 부분키는 Key-scheduling에 의해 생성된 32 비트 키이다. F함수의 블록도가 그림 3에 나타나 있다.[4]

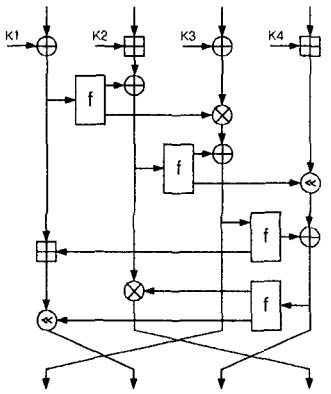

그림 3. F함수의 블록도

3.1 새로운 블록 암호 알고리즘을 이용한 A3 알고리즘

새로운 블록 암호 알고리즘을 이용한 A3 알고리즘은 128 비트의 난수를 2 개의 64 비트 블록으로 나누어 그림 4와 같이 각 블록을 연쇄적으로 암호화하여 그 결과인 64 비트 해쉬 값을 다시 2 개의 32 비트 블록으로 나누어 XOR한 32 비트의 해쉬 값을 생성하는 해쉬 함수이다.

이런 형태의 해쉬 함수는 블록 암호 알고리즘이 안전하다면 안전한 해쉬 함수라는 것이 알려져 있다.[4]

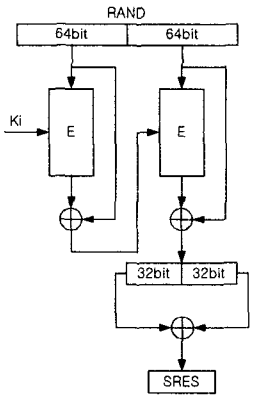

그림 4. A3 알고리즘의 블록도

Ⅳ. A3 알고리즘의 구현 및 검증

A3 알고리즘은 VHDL과 자동 합성기법을 기본으로 탑다운 설계방식에 따라 구현된다. 탑다운 설계방식이란 회로의 특성을 가장 개괄적인 측면으로부터 시작해 가장 기본적인 회로 구성 요소까지 점점 세분화된 서브 블록들을 통해 단계적으로 표현하는 기법이다.[2,6]

A3 알고리즘의 하드웨어 설계를 기능별로 나누면, 데이터를 암호화시키는 암호화부와, 암호화 과정 중 필요한 부분키를 생성하는 키생성부, 그리고 이들을 제어하는 제어부로 나눌 수 있다.

4.1 암호화부

암호화부는 그림 3과 같이 두 개의 mux와, 64 비트 XOR, 32 비트 XOR 및 f_blk와 중간값을 저장하기 위한 레지스터로 구성된다. F_blk는 F함수와 32 비트 XOR로 구성된다.

A3 알고리즘에서는 두 번의 암호화 과정이 있는데, 첫 번째 암호화 과정에서는 mux1의 sel 신호가 '0', mux2의 sel 신호가 '1'이 되어 RAND의 상위 64 비트가 F함수 블록의 입력으로 들어간 후, mux2의 sel 신호가 '1'이 되어 F함수 블록의 출력값이 다시 F함수 블록의 입력으로 들어가는 과정을 15번 반복하게 되고, enc1으로 64 비트의 결과를 출력한다.

두 번째 암호화 과정에서는 mux1의 sel 신호가 '1'이 되어 RAND의 하위 64 비트가 들어온 후, 첫 번째 암호화 과정과 같이 15번 반복된다가 결과값을 32 비트씩 나누어 XOR 연산을 수행해 최종 SRES를 생성한다.

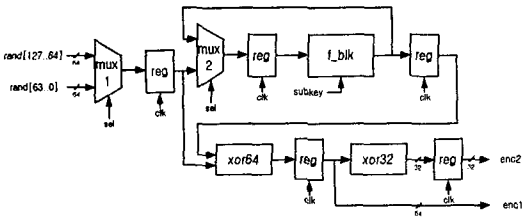

그림 5. 암호화부의 블록도

(1) F함수

하드웨어 구현시 많은 면적을 차지하는 f_table과 f_mul 부분을 mux41과 mux21 및 5 개의 register를 추가하여 각각 하나씩만을 사용하도록 순차회로로 구성하였다. 그림 4에 F함수의 블록도가 나와 있다. F함수에 사용된 각 블록들의 기능은 아래와 같다.

-f_table

$GF(2^8)$에서의 역원을 미리 구한 후 십육진수 'a5'와 XOR 한 값들을 저장해 테이블화 하였다.

-f_adder

두 개의 8 비트 입력을 받아 더한 후 modulo 2^8 연산을 수행한다.

-f_mul

Tool에서 지원하는 곱셈 operator를 사용하였다. 8 비트로 들어오는 두 개의 입력에 대하여 곱셈 연산을 한 후 modulo 2^8+1을 수행한다.[3,4]

-f_shift

두 개의 입력중 한 입력을 다른 입력의 하위 3 비트만큼 쉬프트 한다.

-f_xor

두 개의 입력을 xor 한다.

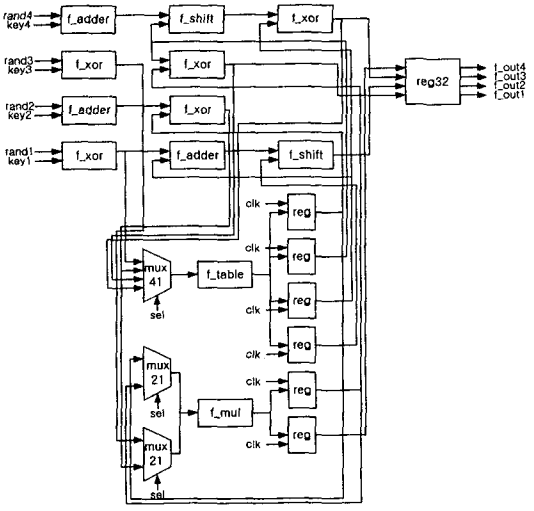

그림6. F함수의 블록도

4.2 키생성부

A3 알고리즘에는 128 비트의 키를 입력으로 16 개의 32 비트 부분키를 생성하는 SETKEY128과 64 비트의 키를 입력으로 16 개의 32 비트 부분키를 생성하는 SETKEY64가 있다. 본 논문에서는 이 두 가지 키생성부분에서 공통적으로 쓰이는 부분을 공유하여 키생성부 하나로 구현하였다. 키생성부는 그림 7과 같이 shifter128, shifter64, rot128, rot64, f_함수, shift_blk 및 두 개의 mux와 레지스터들로 구성된다.

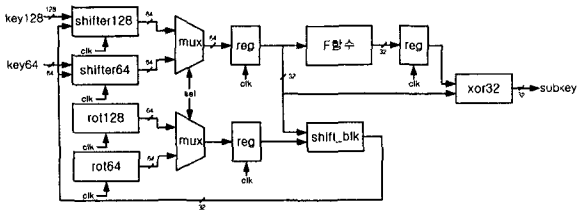

그림 7. 키생성부의 블록도

(1) shifter128, shifter64

shifter128에서는 en_key128이 '1'일 경우 128 비트의 키 값이 저장되고, 저장된 값의 상위 32 비트를 출력한다. en_key128이 '0'이고 클럭이 들어올 경우에는 저장된 값을 8 비트 왼쪽으로 쉬프트하고, shift_blk의 출력이 저장된 값의 95~64번째 비트로 들어가 상위 32 비트 값을 출력한다.

(2) rot128, rot64

클럭 신호가 들어오면, 저장되어 있는 128 비트와 64 비트 값의 상위 32 비트가 출력되고, 저장된 값이 8 비트 왼쪽으로 쉬프트 된다.

(3) F함수

암호화부의 F함수와 비슷한 구조로, 입력부분의 두 개의 f_adde와 f_xor가 없고, 출력부에 4 개의 f_xor가 추가된 구조이다.

4.3 제어부

제어부에서는 암호화부와 키생성부에 쓰일 제어 신호를 만들어 내는 부분으로 sel_gen, st_gen, sig_logic으로 구성된다.

st_gen은 암호화부와 키생성부의 레지스터에 들어가는 클럭 신호를 생성하는 부분으로 주 클럭의 하강 에지가 들어 올 때마다 t1~ t18 제어 신호를 순서대로 내보낸다. sel_gen은 주 클럭의 상승 에지에서 작동하여 F함수에서 쓰이는 mux의 sel 신호를 생성한다. 그리고 sig_logic은 sel_gen으로부터 생성된 신호 c_in을 받아 '1'일 경우 카운터를 하나씩 증가시키고 카운터의 수에 따라 키의 입력 신호와 F함수 이외의 mux의 sel 신호를 생성한다.

4.4 결과

구현된 A3 알고리즘을 검증하기 위하여 Altera사의 MAX-PLUSⅡ를 이용해 시뮬레이션을 수행하였다. 그림 8은 A3 알고리즘에 대한 시뮬레이션 결과로 128 비트의 입력 RAND(0123456789abcdeffedcba98765432 10)와 KEY(00112233445566778899aabbccddeeff)를 받아 32 비트의 인증키(eca9f4e5)를 얻는 것을 확인했다.

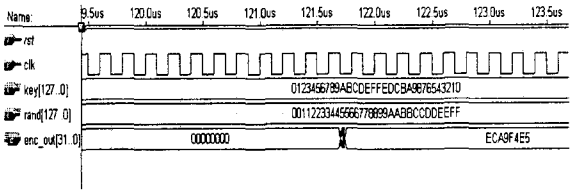

그림 8. A3 알고리즘에 대한 시뮬레이션 결과

V. 결론

본 논문에서는 GSM에서의 인증 알고리즘인 A3 알고리즘을 VHDL을 이용해 구현, 검증하였다.

Target Device로는 Altera사의 EPF10K100GC503-3 device를 사용하여 3,856 개의 Logic cell을 이용해 약 77%의 자원을 사용함을 확인하였고, 동작 주파수는 16.89MHz로 암호화가 이루어지는 시간은 34 usec 정도 걸렸다. 이것은 F함수를 순차회로로 구현하지 않았을 때보다 2,565 개의 logic cell을 적게 사용하는 것으로, 암호화가 이루어지는 시간은 F함수에 추가된 레지스터들로 인하여 약 3 배정도 더 걸리는 단점이 있으나 A3 알고리즘 같은 경우는 인증시 한 번만 사용하는 알고리즘이므로 속도가 크게 문제가 되지는 않는다. 본 논문에서 구현한 암호기는 인증을 필요로 하는 부분에 직접 적용될 수 있을 것으로 기대된다.

참고문헌(또는 Reference)

[1] Asha Mehrotra, "GSM System Enginnering", Artech House, 1996.

[2] Kevin Skahill, "VHDL for Programmable Logic", Addison Wesley, 1996.

[3] 김영철 외, "디지탈 시스템 설계를 위한 VHDL", 홍릉과학 출판사.

[4] 신인철, 김규철, 송영상, "GSM에 적합한 인증 알고리즘의 VHDL 구현", 단국대학교 논문집 제35집, 2000.

[6] 오행수, 한승조, "VHDL을 이용한 확장된 DES (HDES) 설계", 한국통신학회논문지 제20권, 9호, 1995. 9.

[7] 오현서, 이홍섭, 이대기, "GSM 시스템의 Security 특성에 관한 고찰", 통신정보보호학회 논문집 제3권, 4호, 1993. 12.