情報保護學會論文誌
第18卷 第2號, 2008. 4

FPGA를 이용한 Cdma2000 EV-DO 시큐리티 지원 하드웨어 설계 및 구현*

권 환 우[1†], 이 기 만[1], 양 종 원[1], 서 창 호[1‡], 하 경 주[2]
[1]공주대학교, [2]대구한의대학교

Design and Implementation of the Cdma2000 EV-DO security layer supporting Hardware using FPGA*

Hawn-woo Kwon[1†], Ki-man Lee[1], Jong-won Yang[1], Chang-ho Seo[1‡], Kyung-Ju Ha[2]
[1]Kongju National University, [2]Daegu Haany University

요 약

Cdma2000 1x EV-DO 에서의 보안 계층은 현재 3GPP2를 통해 표준화 규격(C.S0024-A v2.0)을 완성해 나가고 있는 중이며, 이에 따라 cdma2000 1x EV-DO 환경의 AT와 AN 간 전송되는 데이터에 대한 보안 기능을 적용하기 위하여 표준 문서에 명시된 보안 계층 구현요구에 맞는 하드웨어 보안 장치가 요구되고 있다.

본 논문에서는 FPGA 플랫폼을 통해 EV-DO 시큐리티 계층 프로토콜을 시뮬레이션 하여 EV-DO 시큐리티 지원 하드웨어 장치를 설계 하였으며, 패킷 데이터에 대한 인증 및 서비스를 위하여 SHA-1 해쉬 알고리즘과 데이터 암호화를 위한 AES, SEED, ARIA 알고리즘을 탑재했으며, 키교환 프로토콜을 이용한 키 교환을 수행 한 후 데이터에 대한 인증 및 암호화 기능을 선택적으로 적용한 하드웨어를 구현 하였다.

ABSTRACT

Security layer of the Cdma2000 1x EV-DO is currently completing standard (C.S0024-A v2.0). Accordingly, a hardware security devices, that allows to implementation requirement of the security layer described in standard document, is required to apply security function about data transferred between AT and AN of then Cdma2000 1x EV-DO environment.

This paper represents design of hardware device providing EV-DO security with simulation of the security layer protocol via the FPGA platform. The SHA-1 hash algorithm for certification and service of packet data, and the AES, SEED, ARIA algorithms for data encryption are equip in this device. And paper represents implementation of hardware that applies optionally certification and encryption function after executing key-switch using key-switching algorithm.

Keywords : FPGA, Cdma2000 1x EV-DO, AES,

접수일: 2007년 11월 19일; 채택일: 2008년 1월 22일
* 이 논문은 2007년도 한국과학재단 특정기초사업의 지원에 의하여 연구되었음(R01-2007-000-20291-0)
† 주저자, fo187op@empal.com
‡ 교신저자, chseo@kongju.ac.kr

Ⅰ. 서 론

반도체의 소형화, 직접화 및 대량 생산 체제가 이루어지면서 현대 사회에는 휴대용 제품이 대중화가 되었으며, 특히 휴대 전화, 휴대 인터넷, 휴대 게임등 다양한 형태의 단말기들이 앞 다투어 신제품을 개발 생산하는 시대가 되었다. 이러한 휴대용 제품들의 가장 큰 과제중 하나는 저 전력화하는 것이며, 또한 현대 휴대제품의 뚜렷한 경향 중 한 가지는 다기능화 하는 것이다. 휴대폰, PMP, PDA, 네비게이션등의 구분이 갈수록 모호해지고 있어서, 이들 단말기들은 갈수록 더높은 처리 성능을 필요로 하며 이에 사용되는 프로세서도 고성능의 것들이 요구되고 있다. 그러나 고성능의 프로세서 일수록 전력 소모량이 증가하여 휴대용 제품에 장착하기엔 적절하지 않아, 압축(음성, 화상, 동영상) 처리, 암호 알고리즘 처리 등의 기능을 별도의 저전력 ASIC[1]으로 대치하는 것이 휴대 단말기의 추세라 할 수 있다.

CDMA 이동통신 방식은 2G인 IS-95 계열과 3G인 IS-2000[2-5] 계열로 구분되며, IS-95는 초기의 CDMA 무선구간 접속 방식을 정의한 프로토콜이고, IS-2000은 Cdma2000 방식의 무선구간 프로토콜로 IMT-2000을 지향하고 있다. IS-2000 Rev.C 이후의 기술은 Cdma2000 1x EV-DO(Evolution-Data Only)라고 불리 운다.[6]

Cdma2000 1x EV-DO에서는 패킷 데이터 서비스를 위한 전용 보안 프로토콜을 제공하며 기존의 IS-2000 무선 프로토콜과는 달리 무선 인터페이스 계층 구조에 따로 분리된 시큐리티 계층(Security Layer)[7]을 정의하고 있다. 시큐리티 계층에 의해 제어 채널, 엑서스 채널l, Forward 트랙픽 채널l, Reverse 트랙픽 채널l에서 전송되는 패킷 데이터에 대한 인증 및 암호화 서비스를 제공하고 있으며, 인증 및 암호화 기능을 제공하기 위해서 먼저 키 교환 프로토콜을 이용한 키 교환을 수행 후, 패킷 데이터에 대한 인증 및 암호화 기능은 선택적으로 적용가능하다.

현재 이동통신과 관련된 분야에서 국내의 경우 연구 및 개발이 활발하게 이루어지고 있지만, 실제 필드에서 적용한 예는 극히 드물게 존재하는 상태이며, 이제 이동통신 시장에서 기지개를 펴고 있는 상황이라 판단된다. 본 논문에서는 Cdma2000 1x EV-DO 에서의 보안 서비스 제공을 위한 시큐리티 계층(Security Layer)을 고찰하고 시큐리티 계층 지원을 위한 하드웨어 플랫폼을 FPGA 알고리즘[8] 형태로 설계 및 구현하였다.

Ⅱ. Cdma2000 1x EV-DO 프로토콜

2.1 Cdma200 1x EV-DO 개요

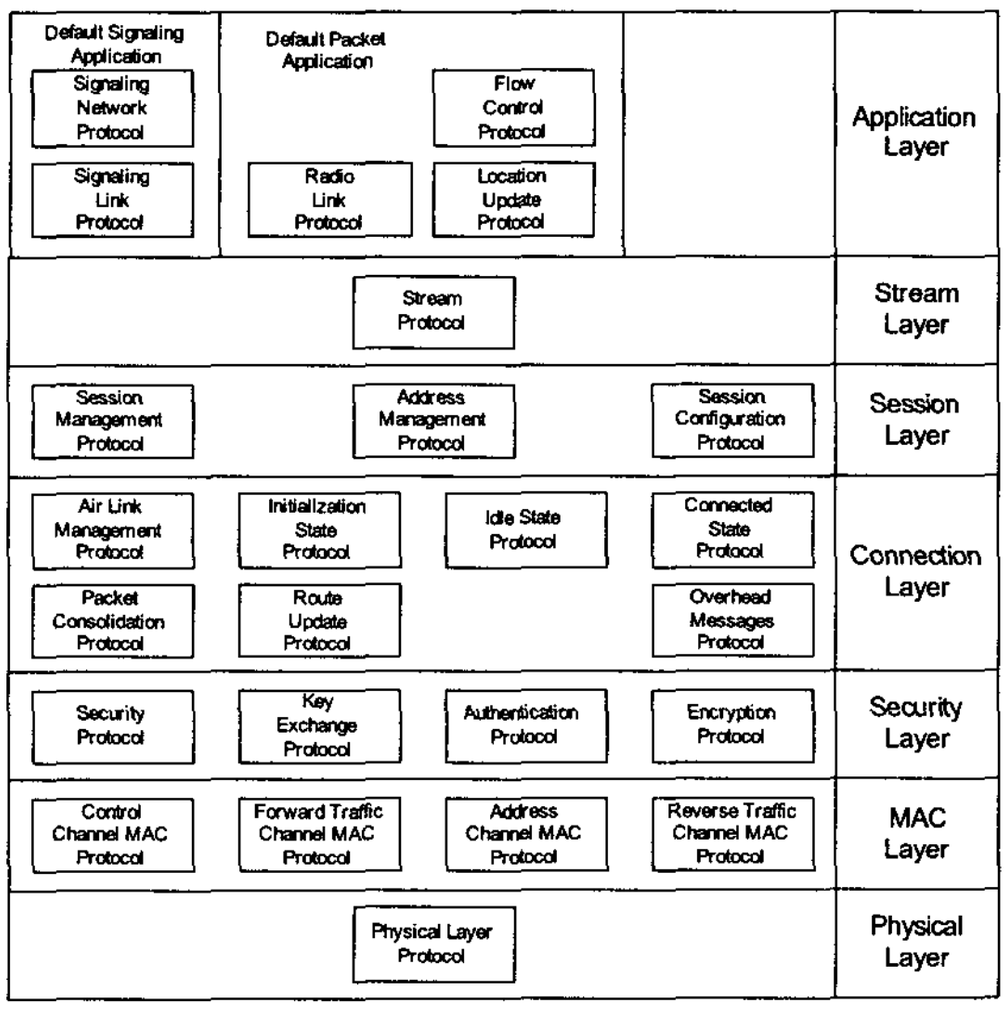
Cdma2000 1x EV-DO 무선 인터페이스는 계층화된 구조를 보이며, 또한 이것은 계층 또는 프로토콜의 수정을 그 계층으로 고립화되며, 각 계층은 하나 이상의 프로토콜로 구성되고 이들 프로토콜 각각은 개별적으로 이루어진다. 또한 프로토콜들은 무선 링크의 peer 개체에게 정보를 전달하기 위해 시그널링 메시지 또는 헤더를 사용한다.

프로토콜들이 메시지를 전송할 때 이들 메시지들을 전송하기 위해 SNP(Signaling Network Protocol)를 사용한다. [그림 1]은 각 계층에 정의된 디폴트 프로토콜들을 보여준다.

2.2 Cdma2000 EV-DO 시큐리티 계층 개요

무선 인터페이스는 제어 채널, 액세스 채널, forward 트래픽 채널, reverse 트래픽 채널에 의해 전송되는 액세스 터미널 트래픽의 인증과 암호화를 위해 사용될 수 있는 시큐리티 계층을 지원한다.

시큐리티 계층은 키 교환(key exchange), 인증



[그림 1] 디폴트 프로토콜

(authentication), 암호화(encryption)기능을 제공하며, 시큐리티 계층은 이들 기능들을 제공하기 위해 키 교환 프로토콜, 인증 프로토콜, 암호화 프로토콜, 시큐리티 프로토콜로 구별된다. 각각의 내용을 보면 다음과 같다.

- 키 교환 프로토콜 : 인증과 암호화를 위한 시큐리티 키 교환을 위해 AN(access network)와 AT(accessterminal)에 의해 수행되는 정차를 제공한다.
- 인증 프로토콜 : 트래픽 인증을 위해 AN와 AT에 의해 수행되는 절차를 제공한다.
- 암호화 프로토콜 : 트래픽 암호화를 위해 AN와 AT에 의해 수행되는 절차를 제공한다.
- 시큐리티 프로토콜 : 인증 프로토콜과 암호화 프로토콜에 의해 사용될 수 있는 cryptosync, timestamp와 같은 공개 파라메타 생성 절차를 제공한다.

[그림 2]은 연결 계층 패킷, 시큐리티 계층 패킷, MAC 계층 패킷들간의 관계를 보여주는 것으로, 세션 구성이 디폴트 시큐리티 계층을 설정하거나 또는 구성된 시큐리티 프로토콜이 헤더 또는 트레일러를 요구하지 않는다면, 시큐리티 계층 헤더 또는 트레일러는 나타나지 않을 수 있다. MAC 계층에 의해 추가되는 필드들이 시큐리티 계층 헤더와 트레일러의 존재를 지시하며, 암호화 프로토콜은 평문의 실제 길이를 숨기기 위해 트레일러를 추가할 수 있고 암호화 알고리즘에 의해 사용되는 패딩을 추가할 수도 있으며, 또한 암호화 프로토콜 헤더는 초기화 벡터와 같은 변수들을 포함할 수 있다. 그리고 인증 프로토콜 세더 또는 트레일러는 인증되는 인증 프로토콜 패킷 부분을 인증하기 위해 사용되는 전자 서명이 가능하며, 시큐리티 프로토콜 헤더 또는 트레일러는 인증과 암호화 프로토콜에 의해 필요한 변수들을 포함할 수 있다. [그림 2]과 같이 인증은 암호화 프로토콜 패킷에 대해 수행되며, 이것은 인증이 실패할 때 불필요한 복호화를 피할 수 있게 해준다.

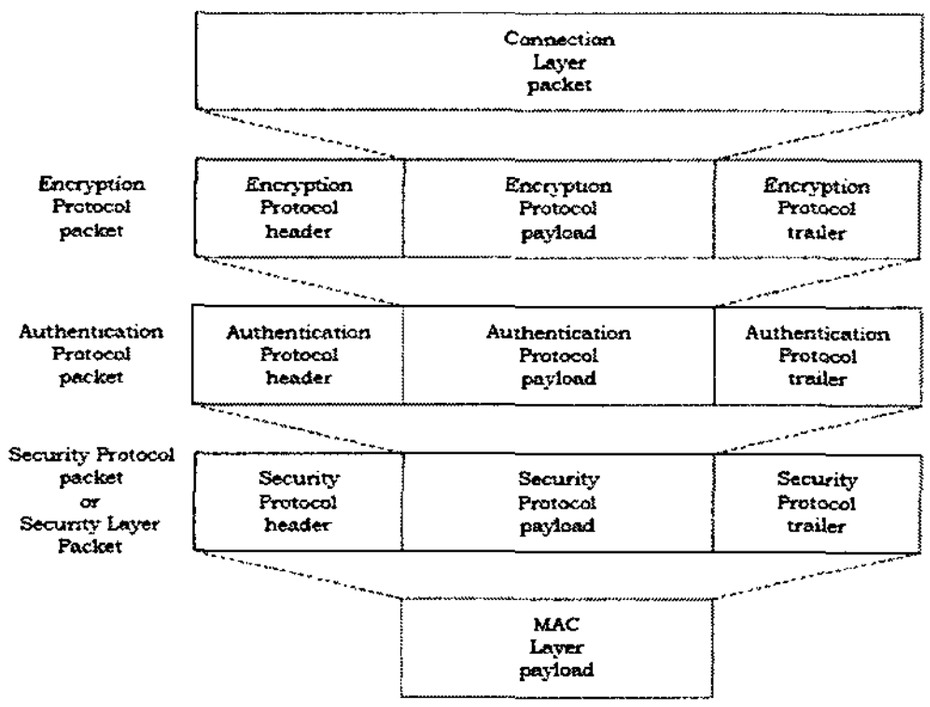
Ⅲ. EV-DO 시큐리티 지원 하드웨어 장치 설계 및 구현

3.1 EV-DO 시큐리티 지원 하드웨어 장치 개요

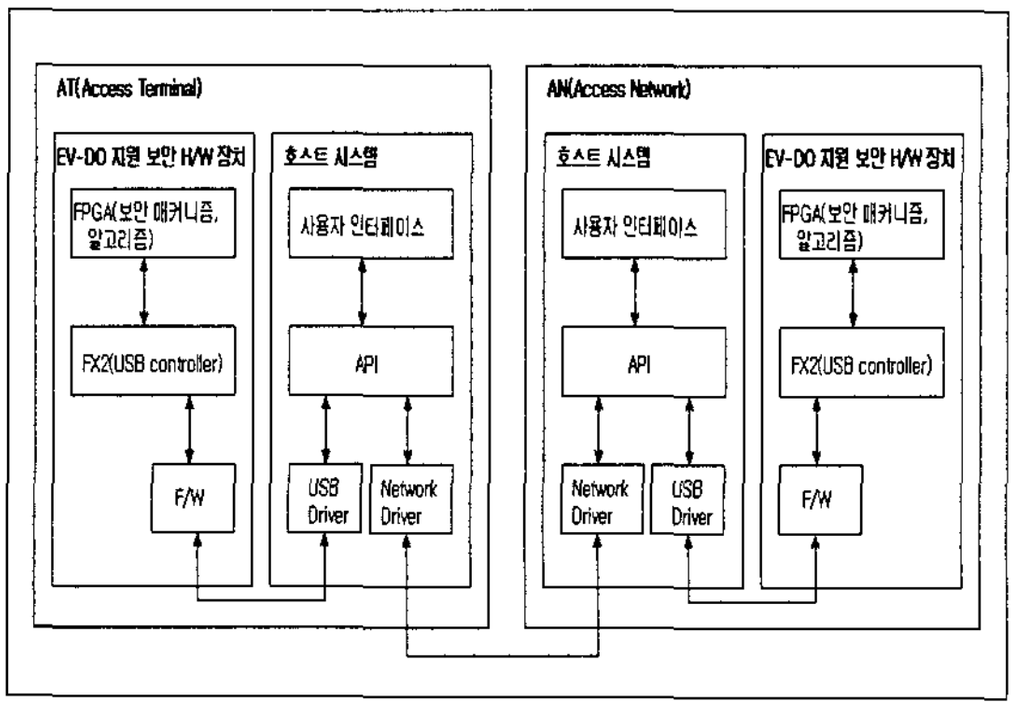
AT와 AN간 빠르고 안전한 데이터 전송 보장을 목적으로 Cdma2000 1x EV-DO 지원 보안 하드웨어 장치를 설계하였으며, [그림 3]과 같은 시스템 구성도를 보여준다.

AT와 AN 으로 구성과 동시에, 각각 EV-DO 지원 보안 하드웨어 장치와 호스트 시스템으로 구성하며, EV-DO 지원 보안 하드웨어 장치는 고속 처리가 필요한 보안 매커니즘 및 보안 알고리즘을 처리하며 호스트 시스템에서는 사용자 인터페이스를 제공하며 소프트웨어 시퀀스를 처리한다.

Cdma2000 1x EV-DO 지원 보안 하드웨어 장치는 호스트 장치와 USB2.0 으로 인터페이스하여 480Mbps로 제어 및 암·복호 데이터를 송수신 하며 암·복호 처리는 자일링스사제품인 XC2V3000 FPGA로서 구현하였다. FPGA 구현 언어는 표준 VHDL을 적용하였으며 ISE7.1 로 컴파일 하였고, 그리고 FX2 F/W는 C-언어로 코딩하여 KEIL 환경에서 컴파일 하였다. 또한 윈도우 환경에서 호환하기 위해 호스트 시스템은 상용 컴퓨터를 사용하여 구성하고 소프트웨어는 C-언어를 사용하였다.



〔그림 2〕 Cdma2000 1x EV-DO 보안계층 패킷 구조



〔그림 3〕 EV-DO 시큐리티 계층 시뮬레이션 시스템 구성도

3.1.1 EV-DO 시큐리티 지원 하드웨어 장치 기능

Cdma2000 1x EV-DO 시큐리티 지원 하드웨어 장치는 시큐리티 처리 기능과 호스트 인터페이스 기능을 가지며, 시큐리티 처리 기능의 구성은 다음과 같다.

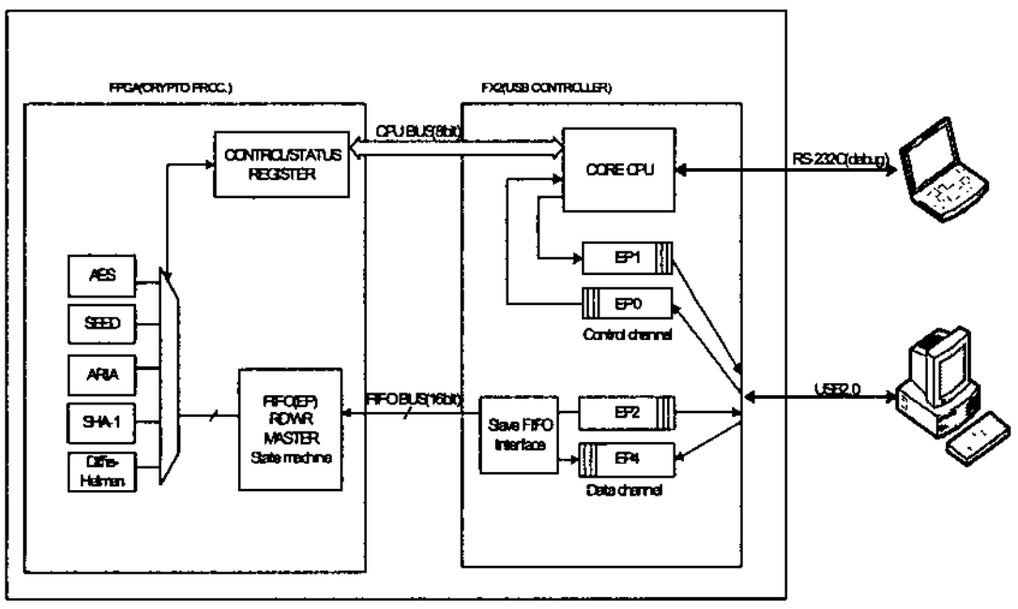
- 키 교환 : 768bit, 1024bit Diffie-Hellman 알고리즘 지원
- 패킷 인증 : SHA1
- 암호 : AES, SEED, ARIA

3.1.2 EV-DO 시큐리티 지원 하드웨어 장치 구조

Cdma2000 1x EV-DO 시큐리티 처리 장치의 하드웨어는 암호 알고리즘을 처리하는 FPGA와 호스트 정합 기능을 하는 USB 컨트롤러(CY7C68013A)로 구성되었으며, 암호 알고리즘을 처리하는 FPGA는 블록암호 알고리즘인 ASE, SEED, ARIA와 키 교환용 Diffie-Hellma, 인증용 SHA-1 으로 구성되며 부가적으로 제어와 USB 컨트롤러의 FIFO 정합을 위한 로직으로 구성된다.

USB 컨트롤러는 cypress사의 USB2.0 FX2를 사용하였으며, FX2는 480Mbps 의 벌크(bulk) 채널로 암·복호 데이터를 송수신하고 제어 채널로 제어 데이터를 송수신한다.

[그림 4]는 EV-DO 지원 보안 하드웨어 장치 구조도이다.

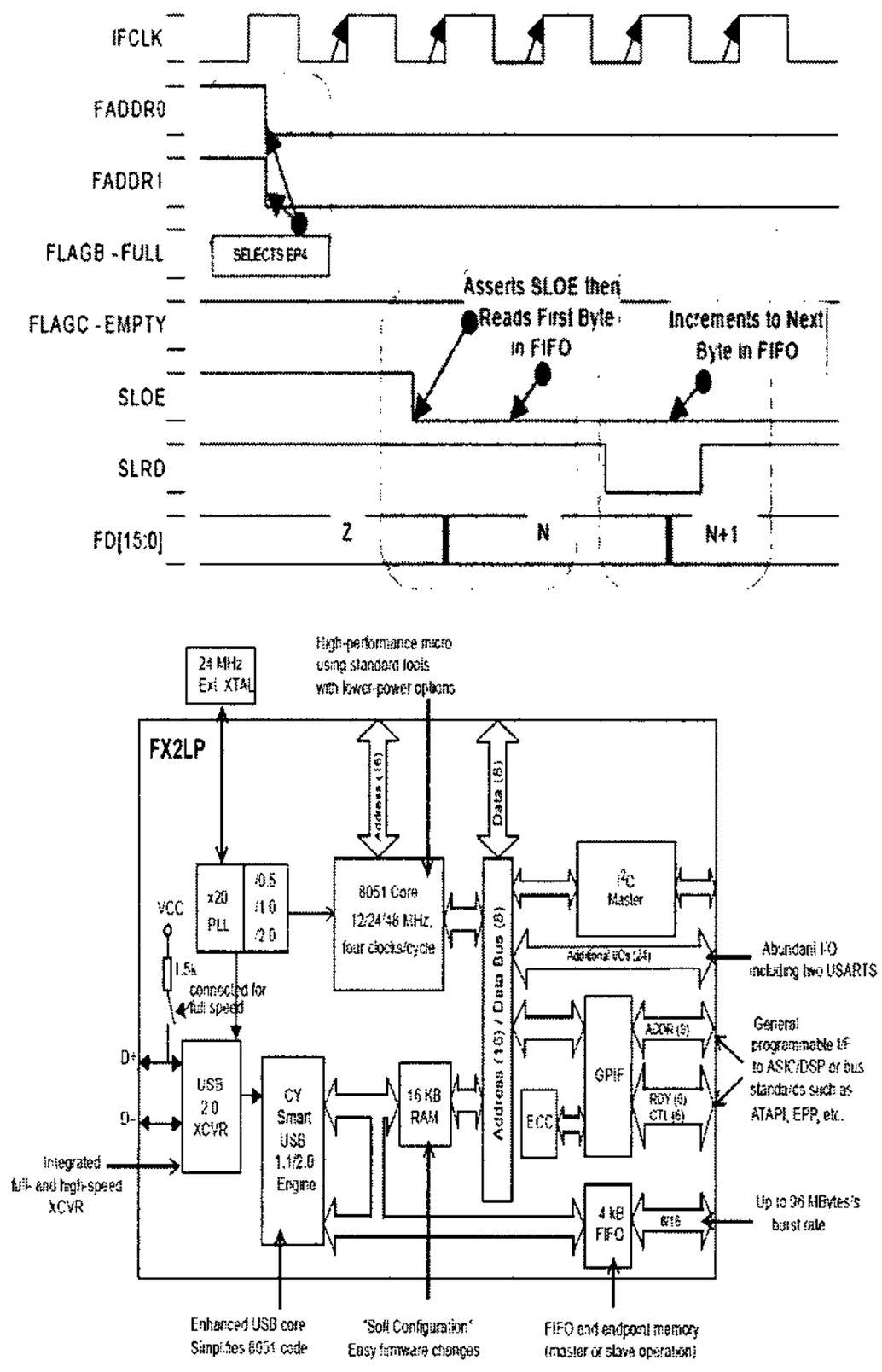


〔그림 4〕 EV-DO 시큐리티 지원 하드웨어 장치 하드웨어 구조도

3.2 EV-DO 시큐리티 지원 하드웨어 장치 세부구조

3.2.1 호스트 정합부

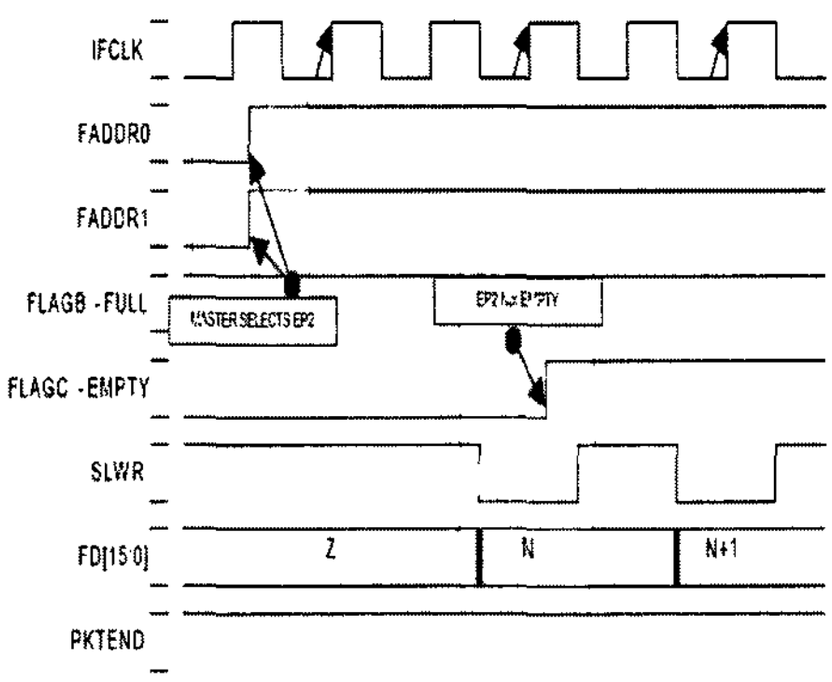
호스트 정합 기능을 하는 FX2는 48MHz 8051 코아



〔그림 5〕 FX2 USB controller 내부 블록도

를 내장한 USB2.0 장치용 컨트롤러 이며, 4개의 데이터 전송용 FIFO, FIFO정합을 별도의 로직없이 가능하게 해주는 GPIF(General Programmable Interface) 와 8051 코아를 내장하고 있다. (그림 5)는 FX2 USB controller 블록도이다.

USB 통신 파이프는 컨트롤에 내장된 FIFO를 사용하며 이 파이프를 Endpoint라고 한다. 그 중 Endpoint1과 Endpoint0는 보드 제어용으로 사용되며 Endpoint 2와 Endpoint 4는 암·복호 데이터 채널로 사용한다. Endpoint0는 호스트에서 EV-DO 시큐리티 처리장치로 제어 데이터를 송신하는데 사용되며, 이 제어 데이터를 8051 코어가 수신하여 FPGA 레지스터에 적용되며, Endpoint1은 8051 코어가 호스트로 보드의 상태를 보고하는 데 사용된다. Endpoint4는 호스트에서 암호화 할 평문을 FPGA로 전송하거나 복호화 할 비문을 FPGA로 전송하는 데 사용되며, 이 때 FPGA는 FIFO 마스터로서 FIFO 상태를 스캔하다가 데이터 있음이 확인되면 읽어



〔그림 6〕 송신 타이밍도(좌), 수신타이밍도(우)

내어 선택된 암호 알고리즘에 입력시킨다. 알고리즘 처리가 완료되고 평문 혹은 암호문이 출력되면 FPGA는 Endpoint2 에 출력 데이터를 전송하며, Endpoint2는 FPGA에서 암호화 한 비문이나 복·호화한 평문을 호스트로 전송하는데 사용되며, Endpoint2와 Endpoint4의 전송에는 8051 코어가 개입되지 않고 FPGA와 호스트간에 고속 벌크 모드로 이루어진다(그림 6).

3.2.2 FPGA 암호처리부

FPGA는 AES, SEED, ARIA 그리고 SHA-1의 암호를 처리하는 각 암호 모듈과, USB FIFO에 송수신 제어를 수행하는 FIFO MASTER STATE MACHINE, 각종 레지스터로 구성된다. 약 30만 게이트(Diffie-Hellman 알고리즘 제외)로 구현 되었으며 [표 1]은 사용된 알고리즘 각각의 소요 게이트 수를 나타낸다.

메인 클록은 40MHz 로 동작되며 각 기능은 모듈 기반의 hierarchy 구조되어 있다.

SHA-1 해쉬함수의 핵심인 라운드 연산은 다음과 같다(그림 7).

SHA-1은 이러한 라운드 연산을 80번 반복함으로써 임의의 데이터를 해쉬하며, 이때 Ft와 Wt는 다음과 같이 정의된 함수이며, Kt는 각 라운드별로 정의되어 있는 상수값이다.

ft(B, C, D) = (B ^ C) _ (~B ^ D) (0 < t < 19)

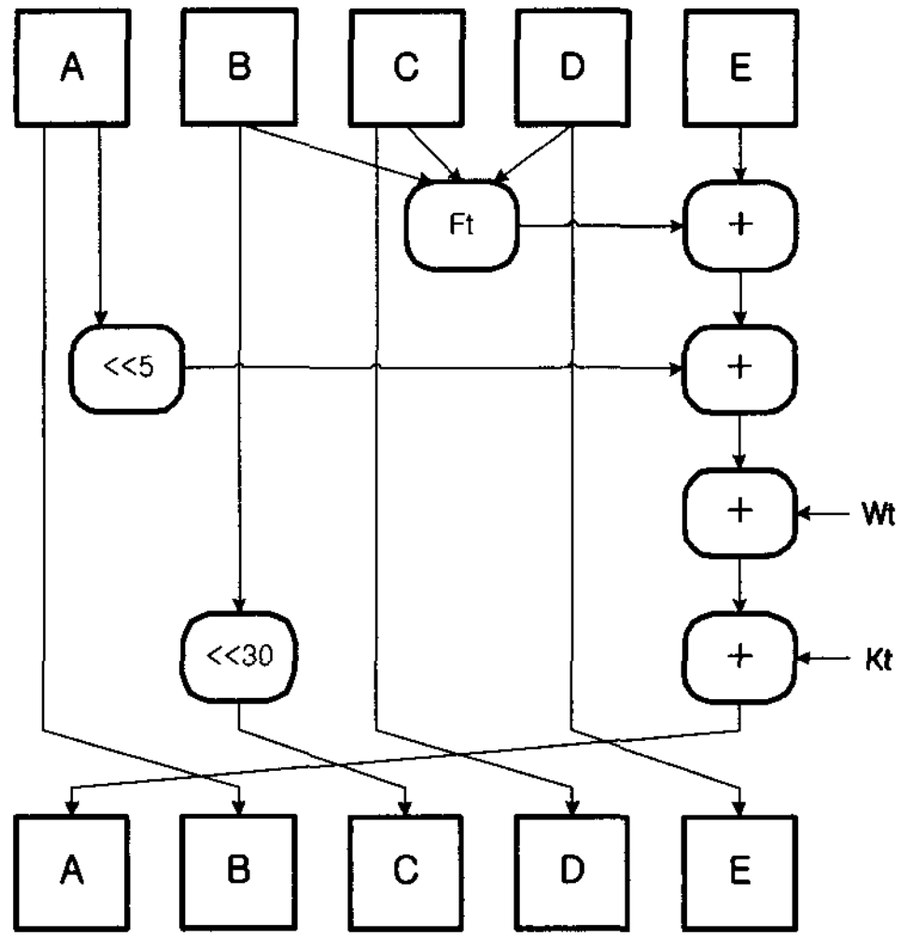
ft(B, C, D) = B xor C xor D (20 < t < 39)

ft(B, C, D) = (B ^ C) _ (B ^ D) _ (C ^ D) (40 < t < 59)

ft(B, C, D) = B xor C xor D (60 < t < 79)

〔표 1〕 암호 알고리즘별 소요 하드웨어 자원

암호 알고리즘	등가 소요 게이트 수
SHA-1	18024
AES	64788
SEED	38800
ARIA	132431



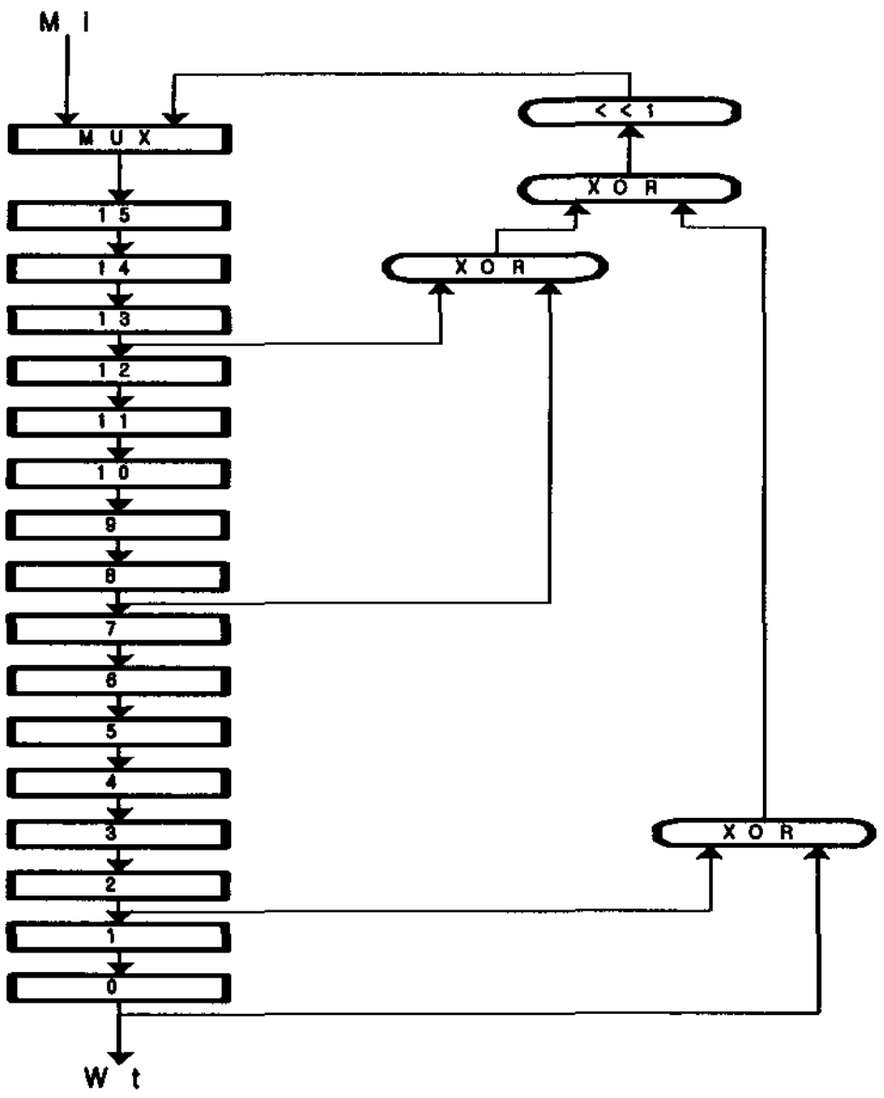
〔그림 7〕 SHA-1 해쉬함수 라운드 연산

Wt = 입력되는 메시지 512비트 데이터를 32비트씩 분할한 값(0 < t < 15)

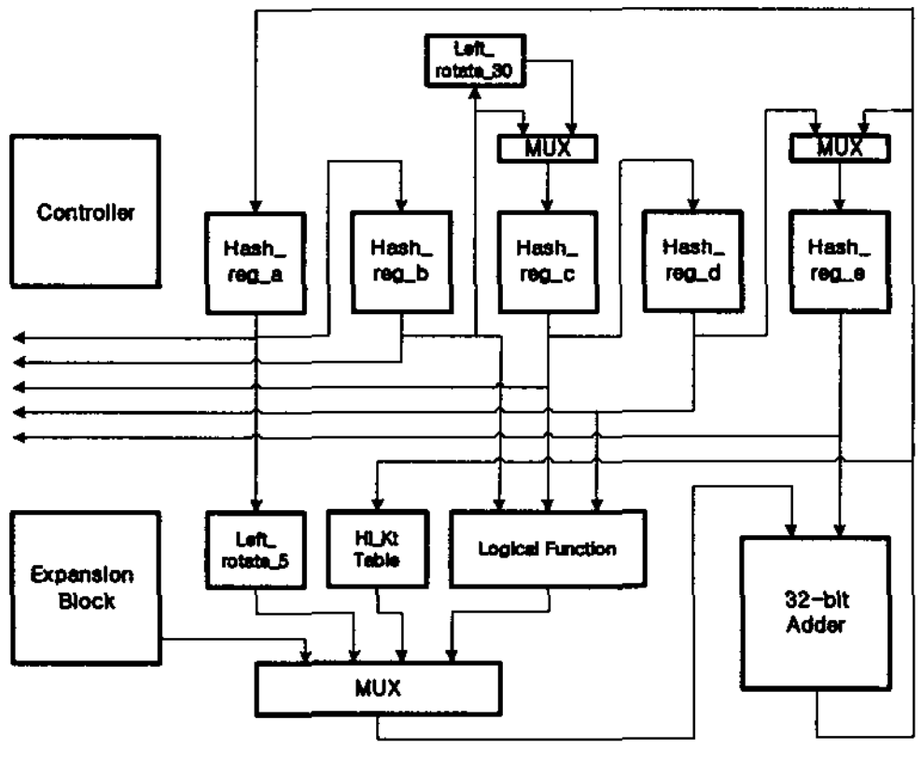
Wt = S1(Wt-3 xor Wt-8 xor Wt-14 xor Wt-16) (16< t < 79)

통상적으로 SHA-1은 32비트 덧셈 연산이 핵심연산인 관계로, 32비트 프로세서 기반에서 소프트웨어 구현에 적합한 것으로 인식되고 있으며, 하드웨어 구현은 고속 연산에 중점을 두어 4개의 덧셈기를 동시에 사용하여 라운드 함수를 한 클럭에 수행하도록 구현하며, 각 라운드에서 필요한 Wt 값을 매 클럭마다 출력하기 위하여 다음과 같이 레지스터를 이용한 구조로 설계 하였다(그림 8).

하지만, 4개의 덧셈 연산과 위와 같은 Wt 값 연산은 많은 전력을 필요로 하며, 이는 RFID나 USN과 같은 시스템에 적합치 않다.. 이에 본 논문에서는 저전력 해쉬함수 구현을 위하여 해쉬 라운드 함수 연산을 위하여 하나의 덧셈기 만을 사용하여 4 클럭에 거쳐 라운드 함수가 연산되도록 설계 및 구현하였다. 한 라운드를 4클럭에 구현함으로써 Wt를 메모리 구조로 바꾸어 연산할



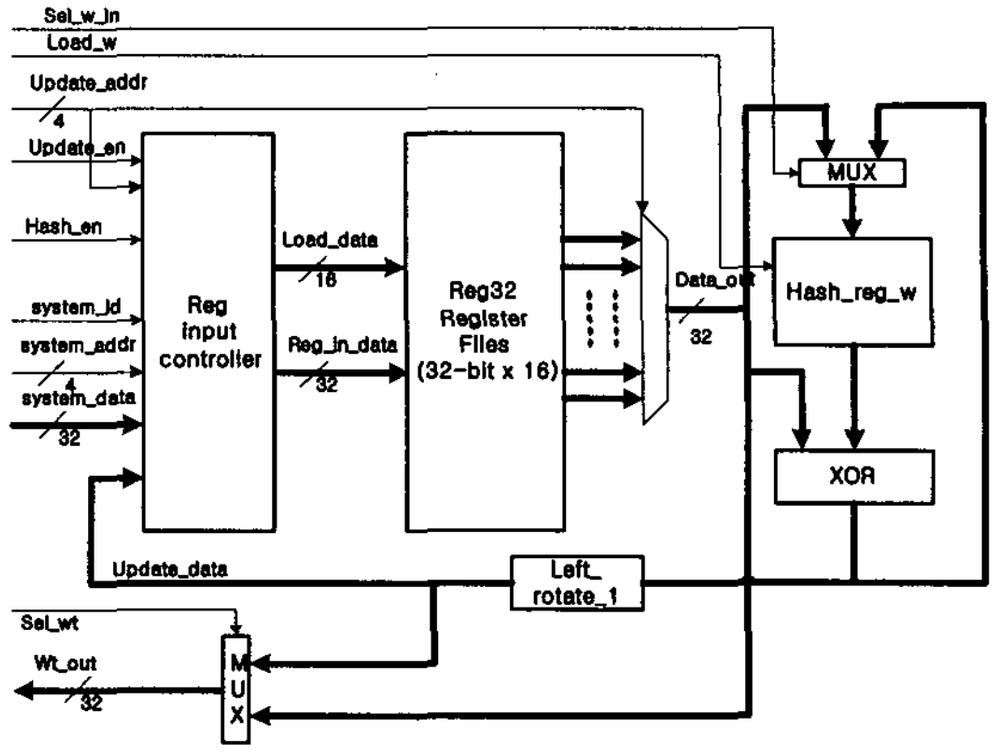
〔그림 8〕 메시지 확장 연산 (Wt)



〔그림 9〕 SHA-1 해쉬함수 암호 모듈 구조

수 있어, Wt 연산을 위한 전력 소모를 1/16로 줄일 수 있으며, 전체 해쉬함수의 데이터 패스 최적화가 가능하게 하였다. [그림 9]는 구현된 SHA-1 해쉬함수 암호 모듈 구조를 보여준다.

위에서 언급한 것과 같이 전력 소모를 최소로 하기 위하여 32비트 덧셈기 하나를 반복 사용하며, 데이터 경로를 유사한 동작에서 그대로 사용할 수 있도록 최적화하였다. 가장 많은 에너지를 소모하는 데이터 확장 블록은 (그림 10, 11)와 같이 설계 및 구현하였다. 가운데의 레지스터 파일은 레지스터로 구성된 32x16 메모리이며, 이는 싱글포트 메모리, 듀얼포트 메모리, synch



〔그림 10〕 데이터 확장 블록

Block 1 has been processed. The values of $\{H_i\}$ are

H_0 = 67452301 + 8CE34517 = F4286818

H_1 = EFCDAB89 + D3AD7C25 = C37B27AE

H_2 = 98BADCFE + 6B4E1883 = 0408F581

H_3 = 10325476 + 74351CD2 = 84677148

H_4 = C3D2E1F0 + 86838382 = 4A566572.

⊞ a_out	F4286818
⊞ b_out	C37B27AE
⊞ c_out	0408F581
⊞ d_out	84677148
⊞ e_out	4A566572

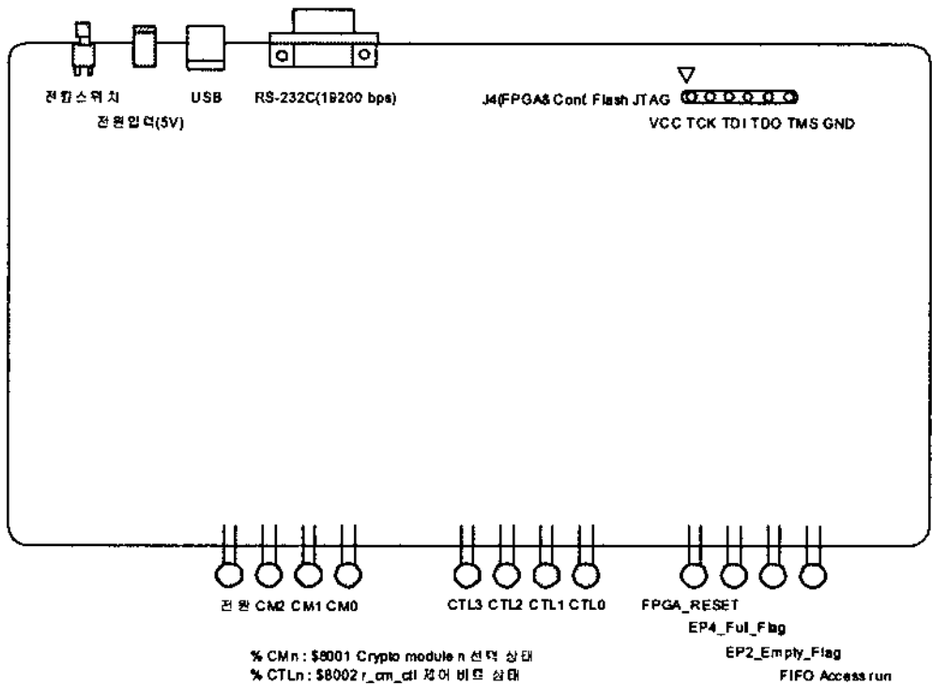
〔그림 11〕 첫 번째 해쉬함수 출력 데이터(좌)와 시뮬레이션 결과(우)

메모리 등 다양한 버전으로 설계 및 구현되었다. (소비전력 측정을 위해서는 레지스터 구조의 메모리가 사용되었다.)

3.3.3 FPGA 제어 레지스터

FPGA 주요 레지스터는 암·복호 모듈을 변경하거나 선택하기 위한 CM_SEL_R 과 암·복호 모듈의 동작 모드 제어를 위한 CM_CTL_R이 있고, 암·복호 모듈의 상태를 읽을 수 있는 CM_STS_R이 있으며, 또 디버깅용으로만 사용하는 128bit 암호모듈 입력 데이터를 출력하는 CM_DAT_IN(n)이 있다.

CM_CTL_R 의 데이터를 업데이트 하기위해 "0xD5 (VR_CRYPTO_CNTL) + Value" 커맨드를 사용하는



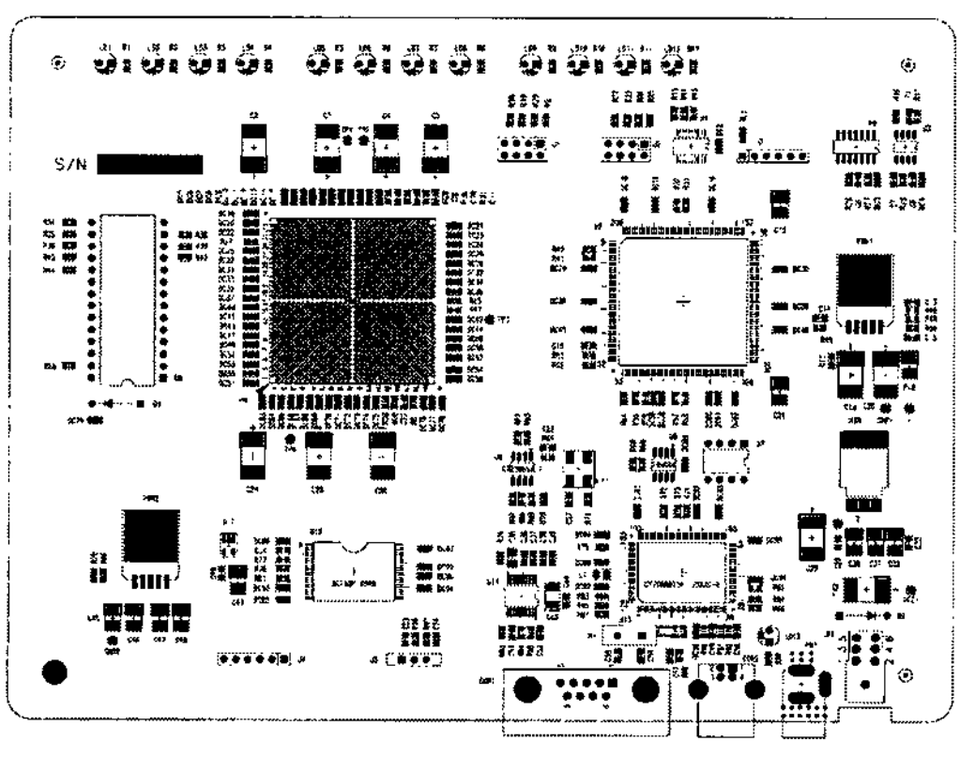
〔그림 12〕 외부 인터페이스 구성도

데 Value에 업데이트하고자 하는 데이터를 주면 된다. CM_SEL_R의 데이터를 업데이트 하기위해 "0xD5 (VR_CRYPTO_SEL) + Value" 커맨드를 사용하고 마찬가지로 Value에 업데이트 하고자 하는 데이터를 주면 된다. FPGA를 Reset 시키기 위해서는 "0xD5 (VR_FPGA_RST)" 커맨드를 사용한다.

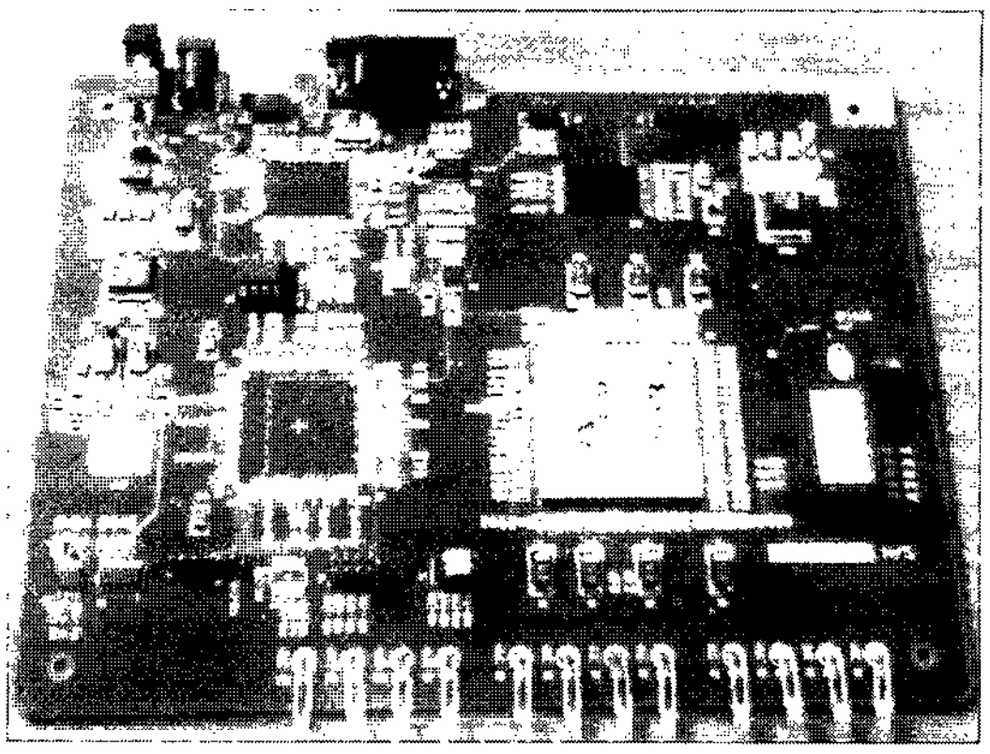
3.3.4 EV-DO 시큐리트 지원 하드웨어 장치 PCB

EV-DO 시큐리티 지원 H/W 장치 PCB는 MENTO TOOL로 CAD 설계되었으며 주요 제원은 다음과 같다.

- 크기 : 150mm x 200mm
- 두께 : 1.5T
- 적층 : 6 Layer
  - Layer1 : COMP(SIGNAL)
  - Layer2 : GROUND(전원)
  - Layer3 : INT1(SIGNAL)
  - Layer4 : INT2(SIGNAL)
  - Layer5 : VCC(전원)
  - Layer6 : SOLD(SIGNAL)
- 재질 : FR4



〔그림 13〕 EV-DO 시큐리티 지원 H/W 장치 PCB TOP-side



〔그림 14〕 구현된 EV-DO 시큐리티 지원 하드웨어 장치

[그림 13, 14]는 EV-DO 시큐리티 지원 하드웨어 장치 PCB TOP - Side설계도와 실제로 구현된 장치를 보여주고 있다.

Ⅳ. 결 론

Cdma2000 1x EV-DO 에서의 보안 계층은 현재 3GPP2를 통해 표준화 규격(C.S0024-A v2.0)을 완성해 나가고 있는 중이다. 본 논문에서는 EV-DO 시큐리티 계층 프로토콜을 시뮬레이션 하기 위하여 EV-DO 시큐리티 지원 하드웨어 장치를 설계 하였으며 패킷 인증을 위한 SHA-1 해쉬 알고리즘과 데이터 암호화를 위한 AES, SEED, ARIA 알고리즘을 탑재하여 설계 및 구현하였다. 또한 키 교환 프로토콜의 시뮬레이션을 일부 적용하였으며, 기지국과 단말 사이에 세션키를 교환하기 위한 Diffier-Hellman 방식의 공개키 알고리즘을 추가 적용하였다.

추후 본 논문은 플랫폼을 보완하여 보다 저 전력의 알고리즘을 개발하고 나아가 상용 수준의 ASIC을 구현하는 데 보탬이 되도록 할 것이며, 또한 암호화 프로토콜에 관하여는 3GPP2에서 자세히 정의하고 있지 않으므로 향후 적절한 암호 알고리즘을 선별하도록 할 예정이다.

참고문헌

[1] D.R. Aadsen. H. N. Scholz. and Y. Zorian. Automated BIST for Regular Strategies Embedd in ASIC Devices. AT&T Technical Journal. May/June. 1990.

[2] 3GGP2 C.S0001. "cdma2000 - Introduction"

[3] 3GGP2 C.S0002. "physical Layer Standard for cdma2000 Spread Spectrum Systems"

[4] 3GGP2 C.S0003. "Medium Access Control (MAC) Standard for cdma2000 Spread Spectrum Systems"

[5] 3GGP2 C.S0004. "Signaling Link Access Control (LAC) Standard for cdma2000 Spread Spectrum Systems"

[6] H. Fathallag, L. A. Rusch and S. LaRochelle, "Passive optical fast frequency-hop CDMA communications system," IEEE J. of Lightwave Tech, Vol.17, No3, 1999.

[7] Frank Quick. "Security in cdma2000". ITU-T Workshop on Security. Seoul(Korea). 13-14 May. 2002

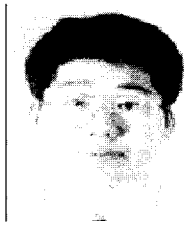
[8] R. J. Francis, J. Rose and Z. Vranesic, "Chortle-crf : Fast Technology Mapping for Lookup Table-based FPGAs," 28th DAC, 1991.

〈著者紹介〉

권 환 우 (Hawn-woo Kwon)
1987년 : 영남대학교 전자공학과(학사)
1987년~1999년 : 대우통신(주) 종합연구소 팀장
1999년~2005년 : 프롬투정보통신(주) 연구소장,전무
2004년 : 공주대학교 일반대학교 수학과(이학석사)
2005년 : 공주대학교 일반대학원 바이오정보학과(정보보호전공) 박사수료
2005년~현재 : (주) 유엠로직스 대표이사
<관심분야> 무선 인터넷 보안, 시스템 보안, 생체인식, 암호 알고리즘,

이 기 만(Ki-man Lee) 학생회원
1986년 : 광주대학교 전자계산학과 (학사)
1990년 : 연세대학교 산업대학원 (석사)
2006년 : 공주대학교 일반대학원 군사정보과학(정보보호전공) 박사과정
<관심분야> 군사정보통신 보안, 네트워크 보안, 생체인식, 암호 알고리즘,

양 종 원 (Jong-won Yang) 학생회원
2003년 : 공주대학교 전자계산학과(학사)
2005년 : 공주대학교 일반대학원 컴퓨터공학과 (공학석사)
2005년 : 공주대학교 일반대학원 바이오정보학과(정보보호전공) 박사과정
2006년~현재 : 한국전자통신연구원 위촉연구원
<관심분야> 무선 인터넷 보안, 시스템 보안, 생체인식, 암호 알고리즘,



서 창 호 (Changho Seo) 종신회원
1990년 : 고려대학교 수학과(학사)
1992년 : 고려대학교 일반대학원 수학과 (이학석사)
1996년 : 고려대학교 일반대학원 수학과 (이학박사)
1996년~1996년 : 국방과학연구소 선임연구원
1996년~2000년 : 한국전자통신연구원 선임연구원, 팀장
2000년~현재 : 공주대학교 응용수학과(정보보호전공) 부교수
2001년~현재 : 공주대학교 바이오정보학과 및 군사정보과학 부교수
<관심분야> 암호 알고리즘, PKI, 무선 인터넷 보안, 시스템 보안 등

하 경 주 (Kyung-ju Ha)
1991년 : 경북대학교 컴퓨터공학과 졸업(공학사)
1993년 : 경북대학교 대학원 컴퓨터공학과 석사과정 졸업(공학석사)
1996년 : 경북대학교 대학원 컴퓨터공학과 박사과정 졸업(공학박사)
1996년 - 1999년 : 한국전자통신기술연구원(ETRI) 부호기술연구부 선임연구원
1999년 ~ : 대구한의대학교 모바일콘텐츠학부 교수
<관심분야> 암호 알고리즘, 무선 인터넷 보안, 시스템 보안, 생체인식,