128비트 블록 암호 알고리즘 SEED와 UART의 저비용 FPGA를 이용한 통합 설계 및 구현

박예철° 이강
zangpark@hotmail.com°, yk@handong.edu

An Integrated Design and Implementation of 128-bit block cipher SEED and UART with a low-cost FPGA

Ye Chul Park°, Kang Yi
School of Computer Science and Electronic Engineering, Handong Global University

요 약

본 논문에서는 국내 표준 128비트 블록 암호화 알고리즘인 SEED와 UART를 통합하여 최저가의 FPGA로 구현하는 방법을 제안한다. 논문[1]에서 구현한 면적 요구량이 최소로 구현된 SEED 암호화 모듈의 유용성을 실제 내장형 시스템에 적용하여 그 실효성을 보여주는 것이 본 논문의 목적이다. 우리가 구현한 회로는 SEED를 통해 암호화를 한 후 UART를 이용하여 외부와의 통신할 수도 있고, SEED를 건너뛰고 UART 단독만 이용하여 외부와 통신을 할 수도 있다. 또한, SEED 자체를 coprocessor로 이용하여 암호화/복호화 가능만 사용할 수도 있도록 설계하였다. 구현 결과, 10만 게이트를 갖는 Xilinx 사의 Spartan-II 계열의 xc2s100 시리즈 칩을 사용하였을 때, SEED와 UART와 주변 논리 회로를 합하여 84% 이하의 면적을 차지 하였고, 최대 41.3Mhz 클럭에서 동작하였으며, SEED의 암호화 처리 Througput은 54.55Mbps로서 UART를 이용하여 통신하는데 전혀 문제가 없었다.

1. 서론

통신 및 네트워크의 기술 발달로 인한 인터넷 고속망의 설치는 인터넷 사용의 증가를 가져 왔으며, 그로 인해 전송되는 정보량이 증가 하면서, 정보의 보호 및 보안에 관한 요구 역시 증가 하고 있다. 데이터 전송의 안전성과 신뢰성 등을 보증하기 위해 여러 암호화 알고리즘들이 개발되었으며, 몇몇 알고리즘들은 국내 및 국제 표준으로 선정되어 여러 분야에서 사용되고 있다[2].

SEED는 한국정보보호진흥원에서 1999년 제정 발표한 대한민국 표준 대칭키 블록 암호화 알고리즘으로 128비트의 블록으로 데이터를 읽어서 암호화 혹은 복호화한다. 또한 SEED는 동일한 구조가 반복되는 Feistal 구조이고, 암호화와 복호화에 사용되는 키가 128비트의 같은 키를 사용하는 대칭키 알고리즘이기 때문에 비대칭키 암호화 알고리즘에 비해 처리속도가 빠르며, 하드웨어 구현하기에 용이하다[3].

한편, FPGA(Field programming Gate Array)가 과거에는 복잡한 하드웨어 검증을 목적으로 하드웨어 원형 제작(Prototyping)용으로만 주로 사용되었다. 그러나 근래에는 공정기술의 발달로 게이트 당 단가가 떨어지고,FPGA 내부에 메모리나 표준 입출력을 위한 인터페이스 회로 등 다양한 특수 기능 블록들을 내장함으로써 단일 칩으로 시스템 레벨의 설계 및 구현을 소화해낼 수 있게 되었고 이에 따라 소량 생산의 임베디드 시스템 제품의 부품으로 직접 사용되는 경우도 있다. 따라서 본 논문에서는 임베디드 시스템을 위한 SEED로서 저가의 FPGA를 구현 대상 기술로 정하였다[1].

이 연구는 IDEC의 지원을 받아서 수행되었음.

본 논문에는 기존 연구[1]에서 구현된 SEED 암호화 회로의 내장형 시스템을 위한 효용성을 실제 내장형 시스템에서의 필요로 하는 모듈로의 구현을 통하여 보이기 위해 [1]에서 설계된 SEED와 UART를 함께 집적하였다. 한편, 통신에서는 제3자로부터의 정보 보호를 위해서 데이터에 대한 암호화/복호화가 필요하기 때문에 SEED 암호화 모듈과 UART 통신 모듈을 한 칩으로 구현하는 것은 실용적 용도가 높은 조합이다. 여기서 구현된 칩의 사양은 다음의 3가지의 동작 모드를 가진다 : (1) UART와 SEED암호화 칩을 이용하여 암호화/복호화한 후 외부와 통신하는 모드, (2) 암호화/복호화를 하지 않고 UART만을 이용하여 외부와의 데이터 전송하는 모드, (3) 암호화/복호화만을 위한 보조 프로세서로서의 이용가능한 모드의 3가지 동작 모드가 있다.

본 논문의 구성은 다음과 같다. 2장에서는 SEED 알고리즘과 기존연구를 설명을 하고 3장에서는 UART와 SEED를 통합한 설계를 설명하고 4장에서는 FPGA에서의 구현 결과와 검증 및 성능을 분석하며 5장에서는 결론을 맺는다.

2. 기존연구 : SEED 암호화 모듈 구조

SEED는 대칭 키 블록 암호 알고리즘으로서, 128비트 단위로 데이터를 처리한다. 각 t 비트인 L0, R0 블록으로 이루어진 2t 비트 평문 블록(L0,R0)을 r라운드를 거쳐 암호문(Lr,Rr)을 내는 반복 구조를 말한다. 그림 1은 SEED 암호 알고리즘의 전체 구조 도이다. SEED는 128

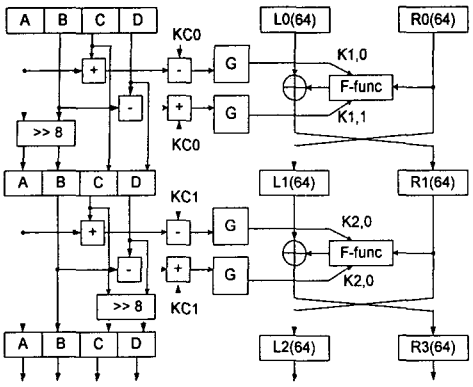

그림 1. SEED 암호 알고리즘 전체 구조도

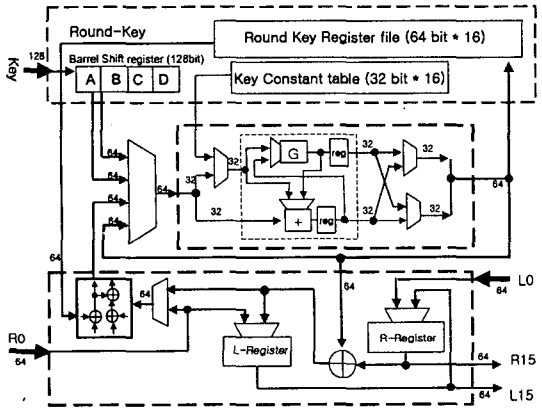

그림 2. SEED의 내부 블록도

비트의 평문을 블록단 위당 128비트 키로부터 생성된 64비트의 라운드 키를 입력으로 받아 총 16라운드를 거쳐 128비트 암호문 블록을 출력으로 낸다. 내부 연산은 Modular adder와 Exclusive-OR 만을 사용하였고 암호화에 사용된 기본함수는 F-함수와 G-함수가 있으며, F-함수는 G-함수 3개로 이루어진다. 라운드 키 생성에도 같은 연산과 함수를 사용한다[4]. 그림 2는 [1]에서 구현한 FPGA를 위한 최소 면적을 가지는 SEED의 내부 블록도이다. 면적을 줄이기 위해 라운드 생성부분과 키 생성부분을 공유하고, G함수 1개와 32-bit addr 한 개를 반복하여 재사용 하도록 설계하였다.

3. 제안된 설계

3.1 UART 구조

UART (Universal Asynchronous Receiver and Transmitter)는 비동기식 직렬 데이터 전송을 위한 인터페이스로서, 통신을 할 때 비동기식 직렬데이터를 병렬데이터로 전환 하거나 그 반대의 일을 한다. 그림 3은 본 논문에서 구현한 UART의 내부 블록도 이다. Transmitter에서는 보낼 데이터 8비트를 입력 받아서 TxD를 통해 한 비트씩 보내 며, Receiver에서는 RxD로부터 받은 데이터를 모아서 8비트로 출력한다.

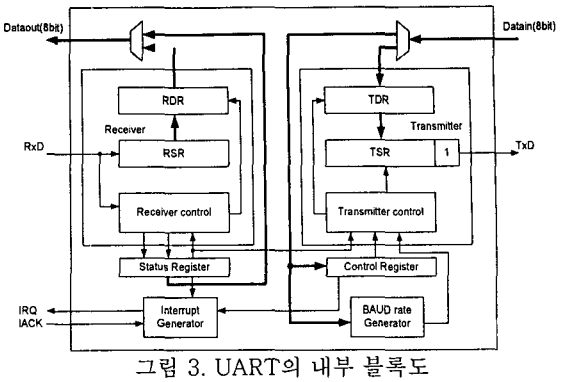

그림 3. UART의 내부 블록도

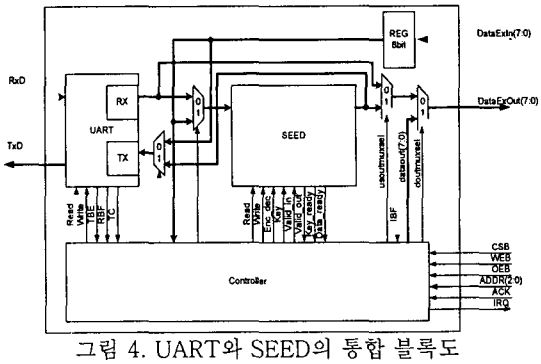

그림 4. UART와 SEED의 통합 블록도

3.2 SEED와 UART의 통합 구조

암호화를 위한 SEED 와 통신을 위한 UART를 통합한 설계를 그림 4에서 보이고 있다. UART는 8비트 단위로 데이터를 주고 받기 때문에 128비트 단위로 작동하는 SEED와의 인터페이스를 위해서 SEED 내부에 있는 128비트와 8비트간의 변환 인터페이스를 이용한다. SEED와 UART를 모두 사용하여 암호화/복호화 한 후 데이터를 송수신 할 수도 있고, UART만 이용하여 데이터를 송수신 할 수도 있고, 시스템 내부에서 암호화 하여 마이크로프로세서와 데이터를 전송할 수도 있게 하는 3가지의 동작 모드 중의 선택을 위하여 데이터 경로를 다양하게 설정할 수 있어야 한다(2:1MUX가 4개가 필요함). 아래쪽의 Controller 박스는 UART 와 SEED의 데이터 교환 및 마이크로컨트롤러와의 인터페이스를 담당한다.

4. 구현 및 검증

본 설계는 VHDL로 작성되고, 10만 게이트를 크기의 최저가 FPGA인 Xilinx SpartanII 시리즈의 xc2s100-pq108를 대상으로 구현하였다. 합성툴은 Xilinx ISE 5.2i를 사용 하였고, 시뮬레이션 툴은 Modelsim XE II v5.6e를 사용하였다. 그림 6은 시뮬레이션 결과의 일부이다. 위 부분의 신호는 전송 모듈의 TxD 신호로서 128비트의 데이터 0 (128비트의 0)값이 SEED로 입력되어 암호화한 결과 값 " C11F22F20140505084483597E40F43" 가 UART의 Transmitter를 통하여 상대방으로 UART로 전송되는 것을 확인 할 수 있다. 맨 아래 신호는 수신 모듈의 UART의 Receiver를 통해 받은 데이터가 복호화를

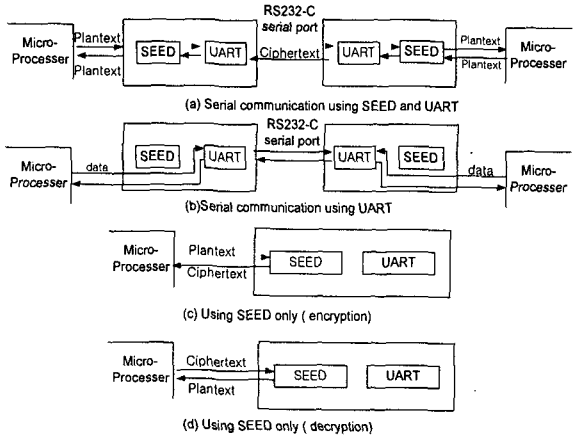

그림 5. 여러가지 통신 모드

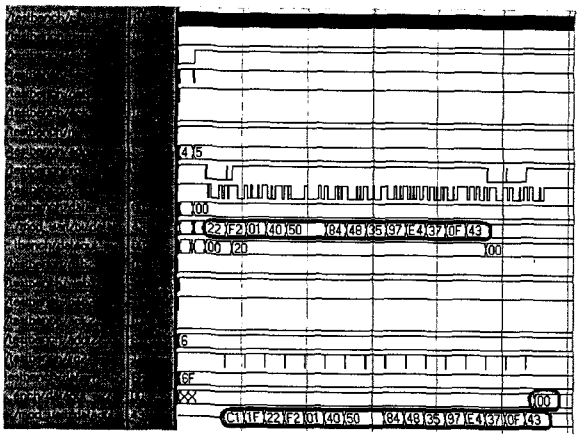

그림 6. 시뮬레이션 결과

위해 SEED에 입력되고 있는 값이며, 그 위의 신호가 원래 값 " 00000000000000000000000000000000" 으로 복호화 되어 8bit 단위로 나뉘어서 출력되고 있다. 합성 결과 FPGA 면적의 84%를 차지하고, 최대 동작 클럭 주파수는 41.3Mhz이다. 이 주파수를 기준으로 계산했을 때, SEED의 암호화 속도는 54.55Mbps 으로서 정상적 UART의 데이터 전송속도에 비해 훨씬 빠르다. 따라서 UART가 데이터를 한 비트 전송 또는 수신하는 동안 128 비트의 데이터를 SEED가 처리 할 수 있으므로 실제 전송 속도는 전적으로 UART의 속도에 따르게 된다. 최종 검증은 FPGA 보드를 통하여 하드웨어 검증을 하였다. 2개의 서두로직 MP3100X FPGA 보드를 RS232-C 시리얼 케이블로 연결하여 그림 5의 (a) 동작 모드에서 상호 동시에 데이터가 제대로 전송되는지를 확인 하였다. 그림 7은 실험할 때 2대의 테스트 보드가 연결된 사진이다.

5. 결론

본 논문에서는 국내 표준 128비트 블록 암호화 알고

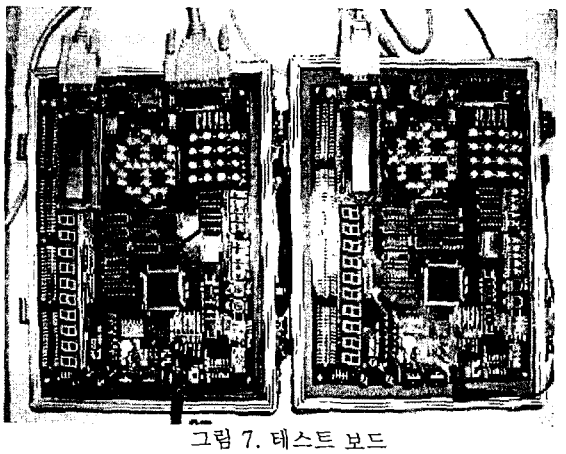

그림 7. 테스트 보드

리즘인 SEED와 UART를 저가의 FPGA에 탑재하는 방법을 제안하였다. [1]에서 제안하였던 SEED 구조를 이용해서 실제 통신이 가능한 칩을 구현하여 기존 연구에서 제시된 SEED 구조의 효용성 시범적으로 보이기 위함이었다. 본 연구에서 구현된 칩은 SEED 와 UART를 동시에 사용하여 암호화/복호화 한 후 외부와의 통신은 물론, UART만 이용하여 외부와 통신을 할 수도 있으며, SEED만 이용하여 내부에서 암호화/복호화도 수행 할 수 있게 하였다. SEED와 UART를 동시에 사용하여 암호화 한 후 데이터를 송신할 때, 암호화에 소요되는 시간은 전체 throughput에 영향을 미치지 않는다. 이것은 UART보다 SEED의 데이터 처리 속도가 훨씬 빠르고, Key생성과 처음 128비트의 데이터를 암호화하는 시간을 제외하고는 데이터를 전송하면서 동시에 암호화/복화화를 할 수 있기 때문이다. 합성 결과 최대 동작 클럭 주파수는 41.3Mhz였으며, Xilinx FPGA SpartanII XC2S100칩 면적의 약 84%를 사용하였다. 따라서 본 논문에서 설계된 칩은 적은 자원을 사용하면서 빠른 데이터처리가 가능하기 때문에 저비용 임베디드 시스템을 위하여 폭 넓게 활용 될 수 있을 것이다. 특히, 저가의 FPGA를 이용한 구현에 적합하도록 설계시에 구조적으로 배려하였다.

참고문헌

[1]Ye-Chul Park and Kang Yi, "A Low Cost Implementation of the 128-bit Block Cipher SEED using FPGAs", Proc. of the 10th Korean Conference on the Semiconductors. pp871-873, 2003. 2.

[2]김종현 "블록 암호알고리즘 SEED의 면적 효율성을 고려한 FPGA 구현", 정보과학회논문지: 컴퓨팅의 실제 제 7권 제 4호, pp372~381, 8월, 2001

[3]권명진 "SEED 암호화 알고리즘의 설계" 대한전자공학회 하계종합학술대회 논문집 제 25권 제 1호, pp313-316, 2002

[4]신종호 "SEED 블록 암호 알고리즘의 단일 칩 연구" 대한전자 공학회 하계종합학술 대회 논문집 제23 권 제 1호 ,pp165-168, 6월, 2000