타원곡선 암호연산 IP의 FPGA 구현

(FPGA Implementation of Elliptic Curve Cryptography Processor as Intellectual Property)

문상국

목원대학교 전자공학과

Sangook Moon

Mokwon University, Department of Electronic Engineering

E-mail : smoon@mokwon.ac.kr

요 약

C 프로그램을 사용하여 증명된 최적화된 알고리즘과 수식은 검증을 위해 Verilog와 같은 hardware description language를 통하여 다시 한번 분석 하여 하드웨어 구현에 적합하도록 수정하여 최적화 하여야 한다. 그 이유는 C 언어의 sequential한 특성이 하드웨어를 직접 구현 하는 데에 본질적으로 틀리기 때문이다.

알고리즘적인 접근과 더불어 하드웨어적으로 2중적으로 검증된 하드웨어 IP는 Altera 임베디드 시스템을 활용하여, ARM9이 내장되어 있는 Altera Excalibur FPGA에 매핑되어 실제 칩 프로토타입 IP로 구현한다. 구현된 유한체 연산 IP들은 실제적인 암호 시스템으로 구현되기 위하여, 193 비트 이상의 타원 곡선 암호 연산 IP를 구성하는 라이브러리 모듈로 사용될 수 있다.

ABSTRACT

Optimized algorithms and numerical expressions which had been verified through C program simulation, should be analyzed again with HDL (hardware description language) such as Verilog, so that the verified ones could be modified to be applied directly to hardware implementation. The reason is that the characteristics of C programming language design is intrinsically different from the hardware design structure.

The hardware IP verified doubly in view of hardware structure together with algorithmic verification, was implemented on the Altera Excalibur FPGA device equipped with ARM9 microprocessor core, to a real chip prototype, using Altera embedded system development tool kit. The implemented finite field calculation IPs can be used as library modules as Elliptic Curve Cryptography finite field operations which has more than 193 bit key length.

키워드

GF, 타원곡선암호, FPGA, Altera

Ⅰ. 서 론

유한체 연산과 이에 대한 SoC 설계 결과가 사용될 수 있는 분야는 소규모 정보보호 어플리케이션에는 물론, 거시적으로는 정보통신분야 전반에 걸쳐서 다양하다. 정보의 보호 문제는 통신망의 발달과 더불어 점점 더 중요한 문제로 부각되고 있다. 인터넷의 예를 들면, 전자 메일 등을 통해서 악의적인 소프트웨어를 고의로 배포하거나, 웹서버에 대한 서비스 거부 공격이나 해킹이 빈번히 발생하여 사회적으로도 심각한 혼란을 야기시킨다. 이러한 상황으로 인해 보안 분야는 통신망 분야에서 가장 주목을 받고 있는 분야 중 하나가 되고 있는 추세이다. 네트워크에서의 안정적

인 서비스 운용 뿐 아니라, 전자 상거래에서의 인증, 휴대 전화 통신망에서의 과금 문제과 관련된 인증, 무선 통신망에서의 사생활 보호를 위한 안전한 데이터 전송 등 보안은 정보통신 전반에 걸쳐 반드시 고려되어야 할 이슈 사항이다.

타원곡선 암호알고리즘에 대한 하드웨어 적용 방은으로는 다양한 규모의 컴퓨터 시스템, 네트워크 관리 및 운영분야, 전자보안 및 개인정보보호 시스템 등에 사용되며, 시장 규모로 본다면 PC와 워크스테이션 분야, 서버 및 네트워크 장비, 전자 상거래 시스템 및 IC 카드 등이 가장 큰 규모를 차지할 것이다. [1]

HDL로 하드웨어를 기술하는 방식은 크게 알고리즘 수준, RTL (Register Transfer Level) 수준 그리고 게이트 수준으로 나눌 수 있는데, 알고리즘 수준은 하드웨어 동작을 알고리즘 수준에서 기술하므로 빠르고 쉽게 원하는 하드웨어를 표현할 수 있는 반면 실제 하드웨어로 합성을 수행할 경우 많은 문제점을 나타낸다. 게이트 수준 기술은 하드웨어를 구성하는 모든 게이트를 실제로 기술하는 방식으로 일반적으로 사람이 기술하기 보다는 이미 기술된 상위 수준의 HDL을 합성하고 최적화하여 얻을 결과로 변환하는 경우에 얻어진다. RTL 수준은 하드웨어의 모든 동작을 레지스터와 그 외의 로직으로 구분하여 기술하는 방식으로 구현하고자 하는 동작을 가장 효율적으로 기술할 수 있으며, 합성 시에도 최적의 결과를 얻을 수 있다. 이렇게 알고리즘적으로, HDL 기술 시뮬레이션으로 이중적으로 검증된 IP의 실제 칩으로의 구현은 또다른 이슈들을 유발시킨다. 본 논문에서는 설계된 IP를 실제 FPGA와같은 하드웨어 칩으로 구현 시 실제로 발생할 수 있는 문제점과 고려사항들에 대해 논하고 실제로 FPGA로 구현하여 본다.

II. FPGA 구현

C 프로그램을 사용하여 증명된 최적화된 수식은 다시한번 Verilog와 같은 hardware description language를 통하여 다시 한번 검증을 하여 하드웨어 구현에 적합하도록 수정하여 최적화 하여야 한다. 그 이유는 C 언어의 sequential 한 특성이 하드웨어를 직접 구현 하는 데에 본질적으로 틀리기 때문이다.

알고리즘적인 접근과 더불어 하드웨어적으로 2중적으로 검증된 하드웨어 IP는 임베디드 시스템 개발 키트와 같은 장비를 활용하여, ARM9이 내장되어 있는 Altera Excalibur FPGA에 매핑되어 실제 칩 프로토타입 IP로 구현될 수 있다. 구현된 유한체 연산 IP들은 실제적인 암호 시스템으로 구현되기 위하여, 193 비트 이상의 타원 곡선 암호 연산 IP를 구성하는 라이브러리 모듈로 사용될 것이다.

칩 상의 시스템을 구현하기 위하여, 마이크로프로세서와 암호 시스템 블록 간의 데이터 교환을 위한 상호 규약이 필요하다. Excalibur FPGA의 버스 구조는 ARM9 마이크로프로세서와 주변 버스 마스터들 간에 AMBA (Advanced Microcontroller Bus Architecture)라는 버스 프로토콜로 설계하여야 하고, 그의 설계에 대한 몫은 버스 마스터를 설계하는 사람이 담당하여야 한다. [2] 따라서 마이크로프로세서와 연동하는 타원 곡선 암호 연산 IP를 구현하기 위해서는 AMBA 버스 아키텍쳐에 대한 선행 연구가 필수적이다. AMBA 버스 프로토콜은 주변 장치와 통신을 위해 APB (AMBA Peripheral Bus), AHB (AMBA Hi-performance Bus)를 사용하는데 특히 Excalibur 디바이스에서는 AHB 버스 프로토콜을 사용하기 때문에 AHB 아키텍쳐에 대한 연구가 필요하다.

하드웨어 설계까지의 전체 디자인 흐름은 그림 1과 같다. 먼저 PLL이나 인터럽트, 메모리 영역 할당을 위한 FPGA의 세팅을 해 주고, 타원 곡선 암호 연산 하드웨어를 기술하기 위한 Verilog 파일과 시스템을 위한 주변 블록, 라이브러리에서 제공하는 IP 코어를 사용하여 하드웨어를 기술하고, 그를 합성 툴을 이용하여 자동 합성 (logic synthesis)을 수행한다. 합성된 게이트 레벨의 모델은 FPGA의 bus functional model과 맞물려서 시뮬레이션이 수행되고, 타이밍에 오류가 없을 때까지 시뮬레이션을 반복한다. 설계에 필요한 디자인 시뮬레이션 툴을 이용하여 시뮬레이션을 수행하며, 자동 합성 툴을 사용하여 회로를 합성한다. 최종 검증된 IP들을 FPGA에 구현하기 위해 소프트웨어 측면에서 고려해야 할 사항은 타겟 FPGA에서 C 헤더 파일 정보와 내장된 주변기기들에 해당하는 디바이스 드라이버들, 제공되는 라이브러리들을 포함하여 테스트를 프로그램 등을 작성하여 ARM 컴파일러를 사용하여 컴파일 시킨 다음, 컴파일된 결과물을 (2) 하드웨어 결과물 (1)과 합병하여 Excalibur 디바이스에 로드 시키고, 전체 시스템을 시뮬레이션 하면서 JTAG을 활용하여 디버깅한다. [3]

III. AMBA BUS 시스템

16/32-bit 임베디드 RISC 프로세서 업계에서 선두주자인 ARM사가 선보인 AMBA (Advanced Microcontroller Bus Architecture)는 오픈 표준 버스 규격이다. AMBA는 SOC를 구성하는 기능 블럭들간의 연결 및 관리 방법으로서 하나 또는 이상의 CPU/ DSP를 내장한 임베디드 제품의 다양한 설계를 가능하게 한다. 또한, AMBA 버스는 SOC 내부 모듈들을 위한 공통 시스템 버스 (backbone)를 정의함로써 디자인의 재사용을 한층 강화시키는 장점을 제공한다.

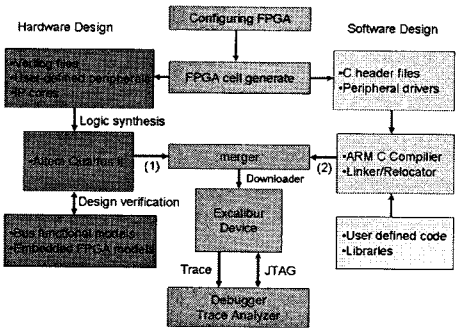

그림 1. 전체 시스템 하드웨어 설계 흐름도
Fig. 1.Hardware design flow of the system

AMBA (버전 2.0) 버스는 내부적으로 AHB와 APB 버스로 구성된다. 일반적으로 AHB 버스는 CPU에 대하여 고속의 엑세스를 요구하는 기능 블록들에, APB 버스는 저속의 기능 블럭들을 위하여 사용된다. 이들은 AHB-to-APB 브릿지에 의해서 AHB 버스로 연결된다. 한편 Multi-layer AHB는 여러개의 버스 마스터가 존재하는 시스템에서 각 버스 마스터들에 대한 Latency와 Bus bandwidth를 크게 개선한 향상된 AMBA 버스 연결 방법이다. AHB (버전 2.0) 버스 규격과 완벽하게 호환되는 Multi-layer AHB 버스로 다양한 버스 구조를 선택할 수 있다. AHB-Lite는 AHB 버스 규격의 부분집합으로서 버스 마스터가 하나뿐인 디자인을 위한 것이다.여기서 AHB-Lite는 버스 마스터가 하나인 시스템과 각 layer에 버스 마스터가 하나뿐인 Multi-layer AHB가 될 수 있다. 일반적으로 ARM 프로세서 기반의 임베디스 SOC 디자인은 다양한 IP와 전용 모듈 그리고 응용 소프트웨어로 동작한다. 그러므로 SOC 디자인의 설계 시간 단축 및 신뢰도를 증대 시키기 위해서는 AMBA AHB(또는 AHB-Lite) 또는 APB 버스 규격에 맞게 설계된 모듈들을 사용해야 한다. 본 논문에서는 AMBA AHB를 사용하여 타원 곡선 시스템을 구현하였다.

IV. 타원 곡선 암호 시스템 구현

본 논문에서는 제안된 유한체 곱셈기와 유한체 나눗셈기, 그리고 스칼라 곱셈 연산 알고리즘의 성능을 평가하기 위하여 193 비트 유한체 $GF(2^{193})$ 위에서 동작하는 타원 곡선 암호용 프로세서를 구현하였다. 제안된 구조는 기존 구조의 타원 곡선 연산 계층에 네배점 연산이라는 새로운 연산 단계와 산술연산인 점 역원 연산을 추가한 것이다. 193 비트의 타원 곡선 암호 기반의 암호 키는 2020년까지 안전하여 이에 필요한 암호 공격 계산량은 인텔 펜티엄 PC 450MHz를 이용하여 계산할 경우 6.54 x 1011 년이 걸린다고 알려져 있기 때문에 이를 구현 대상으로 선택하였다. SEG 2에서 제안하는 193 비트의 타원 곡선은 두 가지가 있는데, 표 1과 같다. 본 논문에서는 두 가지 경우를 모두 모의 실험하였으며 결과로서 두 가지 경우 모두 $n \cdot G$를 계산하였을 때 무한 원점 O가 구해지는 것을 확인하였다.

표 1. SEG-2에서 제안하는 GF(2^{193}) 상의 타원 곡선과 관련 변수
Table 1. Recommended EC and related parameters on GF(2^{193}) by SEG-2

	sect193r1	sect193r2
$p(x)$	$x^{193}+x^{15}+1$	$x^{193}+x^{15}+1$
Coefficient a	00_17858FEB_7A989751_69E171F7_ 7B4087DE_098AC8A9_11DF7B01	01_63F35A51_37C2CE3E_A6ED8667_ 190B0BC4_3ECD6997_7702709B
Coefficient b	00_FDFB49BF_E6C3A89F_ACADAA7A_ 1E5BBC7C_C1C2E5D8_31478814	00_C9BB9E89_27D4D64C_377E2AB2_ 856A5B16_E3EFB7F6_1D4316AE
Base point $G(x)$	01_F481BC5F_0FF84A74_AD6CDF6F_ DEF4BF61_79625372_D8C0C5E1	0D_9B67D192_E0367C80_3F39E1A7_ E82CA14A_651350AA_E617E8F
Base point $G(y)$	00_25E399F2_903712CC_F3EA9E3A_ 1AD17FB0_B3201B6A_F7CE1B05	01_CE943356_07C304AC_29E7DEFB_ D9CA01F5_96F92722_4CDECF6C
Order n	01_00000000_00000000_00000000_ C7F34A77_8F443ACC_920EBA49	01_00000000_00000000_00000001_ 5AAB561B_005413CC_D4EE99D5

V. 결론

본 연구를 수행함에 있어서, 연구에 대한 주안 목표는 복잡한 계산 처리를 요하는 고성능 정보 보호 암호 시스템 중, 특히 차세대 공개키 암호 시스템에서 사용되는 타원 곡선 암호 알고리즘에서의 핵심 처리 연산인 유한체 (GF; Galois Field) 사칙 연산들을 처리하는 알고리즘 측면에서의 최적화되어 이를 응용한 타원 곡선 암호 연산 IP를 SoC 형태로 통합한 시스템을 FPGA 형태로 구현하는가에 대한 것이다. 그림 2에서 보이는 오른쪽 블록의 항목들이 구체적으로 구현된 부분이다.

소프트웨어적으로 검증된 여러가지 알고리즘들을 ARM 마이크로프로세서와 연동되는 하드웨어 IP로 구현하여, 하나의 System-On-a-Chip 형태의 타원 곡선 암호화 프로세서를 설계하고 구현함으로써 또한 하드웨어면에서 유한체 연산 알고리즘에 대한 최적화를 성능 평가하고 검증하였다.

구현 결과는 제안된 곱셈기 및 나눗셈기 모두 소형 정보보호 어플리케이션의 핵심인 IC 카드의 구동에 사용되는 낮은 범위의 주파수 대에서는 물론 동작하였고, 100MHz 이상에서도 동작하였다. FPGA에서 프로토타입으로 구현된 프로세서의 시간, 면적 비교결과는 그림 3과 같았다.

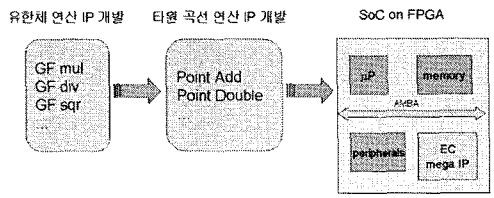

그림 2. 연구 목표 체계도
Fig. 2. Design flow diagram

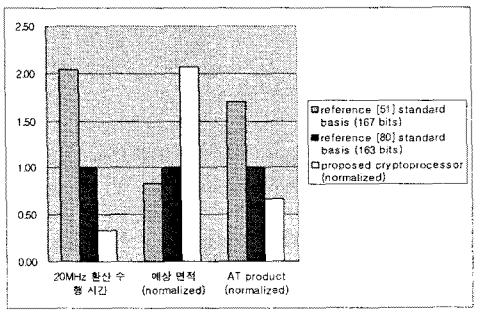

그림 3. 설계된 암호용 프로세서들의 시간, 면적 곱
Fig. 3. AT product of designed crypto processors

IV. 참고문헌

[1] B. Schneier, Applied Cryptography, second edition, John Wiley & Sons, Inc., 1996.

[2] http://www.arm.com

[3] http://www.altera.com