소프트웨어/하드웨어 최적화된 타원곡선 유한체 연산 알고리즘의 개발과 이를 이용한 고성능 정보보호 SoC 설계

문상국*

Design of a High-Performance Information Security System-On-a-Chip using Software/Hardware Optimized Elliptic Curve Finite Field Computational Algorithms

Sangook Moon*

이 논문은 2006년도 한국학술진흥재단 연구비를 지원받았음 (KRF-2006-331-D00401)

요 약

본 연구에서는 193비트 타원곡선 암호화프로세서를 보조프로세서 형태로 제작하여 FPGA에 구현하였다. 프로그램 레벨에서 최적화된 알고리즘과 수식을 제안하여 증명하였고, 검증을 위해 Verilog와 같은 하드웨어 기술언어를 통하여 다시 한번 분석 하여 하드웨어 구현에 적합하도록 수정하여 최적화 하였다. 그 이유는 프로그래밍 언어의 순차적으로 컴파일되고 실행되는 특성이 하드웨어를 직접 구현 하는 데에 본질적으로 틀리기 때문이다.

알고리즘적인 접근과 더불어 하드웨어적으로 2중적으로 검증된 하드웨어 보조프로세서를 Altera 임베디드 시스템을 활용하여, ARM9이 내장되어 있는 Altera CycloneII FPGA 보드에 매핑하여 실제 칩 프로토타입 IP로 구현하였다. 구현된 유한체 연산 알고리즘과 하드웨어 IP들은 실제적인 암호 시스템에 응용되기 위하여, 193 비트 이상의 타원 곡선 암호 연산 IP를 구성하는 라이브러리 모듈로 사용될 수 있다.

ABSTRACT

In this contribution, a 193-bit elliptic curve cryptography coprocessor was implemented on an FPGA board. 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 which was double-checked in view of hardware structure together with algorithmic verification, was implemented on the Altera CycloneII 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, 타원곡선, FPGA, Altera

* 목원대학교

접수일자 2008. 07. 16

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, 전자메일 등을 통해서 악의적인 소프트웨어를 고의로 배포하거나, 웹서버에 대한 서비스 거부 공격이나 해킹이 빈번히 발생하여 사회적으로도 심각한 혼란을 야기 시킨다. 이러한 상황으로 인해 보안 분야는 통신망 분야에서 가장 주목을 받고 있는 분야 중 하나가 되고 있는 추세이다. 네트워크에서의 안정적인 서비스 운용 뿐 아니라, 전자 상거래에서의 인증, 휴대 전화 통신망에서의 과금 문제와 관련된 인증, 무선 통신망에서의 사생활 보호를 위한 안전한 데이터 전송 등 보안은 정보통신 전반에 걸쳐 반드시 고려되어야 할 이슈 사항이다.

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

본 논문에서는 193비트 타원곡선 암호화프로세서를 FPGA를 사용하여 구현한다. 소프트웨어적으로 유한체 곱셈, 유한체나눗셈, 타원곡선곱셈 알고리즘을 최적화 후 HDL로 재검증한 후 FPGA로 구현하였다. 제안된 알고리즘은 FPGA에 내장된 메모리를 LUT로 활용하여 LUT와 연산모듈을 이용한 반복계산 구조를 가지고 있다. 이러한 구조는 메모리와 연산IP를 내장한 FPGA에서 소요 게이트 수를 최소화 할 수 있으며, 또한 고속의 연산을 가능하게 한다.

본 논문의 Ⅱ장에서는 FPGA에 구현하기 위한 이슈 및 구현에 관한 기존 연구를 살펴보고, Ⅲ장에서는 BUS 마키텍쳐에 대해 알아본다. Ⅳ장에서 타원곡선암호용 보조 프로세서의 설계와 구현에 대해서 논하고, Ⅴ장에서 결론을 맺는다.

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 sequential한 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 CycloneII 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 것이다.

칩 상의 시스템을 구현하기 위하여, 마이크로프로세서와 암호 시스템 블록 간의 데이터 교환을 위한 상호 규약이 필요하다. CycloneII FPGA와 ARM9 마이크로프로세서를 연동하기 위해서는 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 고성능 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 사용하

여 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 CycloneII 디바이스에 로드 시키고, 전체 시스템을 시뮬레이션 하면서 JTAG을 활용하여 디버깅한다 [3].

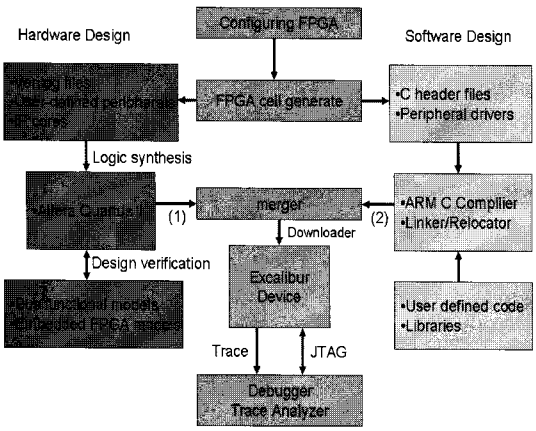

그림 1. 전체 시스템 하드웨어 설계 흐름도
Fig. 1. Hardware design flow of the system

Ⅲ. AMBA BUS 시스템

16/32-bit 임베디드 RISC 프로세서 업계를 선점한 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.

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 타원곡선 시스템을 구현하였다.

Ⅳ. 유한체 연산 알고리즘

GF(2^m)를 기본으로 하는 유한체 연산에서 덧셈과 뺄셈은 그 구현이 단순하지만, 곱셈, 나눗셈이나 역원을 구하는 데에는 수학적으로 복잡한 수식을 간략화하는 과정이 필수적이다. 유한체 연산은 기본적으로 normal basis와 polynomial basis 두 가지 측면에서 접근할 수 있고 이 두 방법은 각각 장단점을 가지고 있다 [4]. 본 연구에서는 두 가지 basis 중에서 수학적인 접근이 용이한 polynomial basis 를 사용한 접근방식을 채택하여 수학적인 원리를 이용한 수식의 간략화를 꾀하고 최적화 하는 방법을 제시한다. 이는 알고리즘의 측면에서 수학적인 증명이 가능한, 다시 말하여 현대 알고리즘 설계 추세에 맞도록 "본질적으로 신뢰할 수 있는 (Inherently reliable)" 알고리즘이 될 것이다.

제안하여 적용한 유한체 연산 알고리즘은 유한체 곱셈, 유한체 나눗셈에 대한 것이며, 아래에 제시한다.

1. 유한체 곱셈

polynomial 방식의 유한체 곱셈은 주어진 유한체의 임의의 두 원소를 각각 $A(x) = \sum_{i=0}^{m-1} a_i x^i$, $B(x) = \sum_{i=0}^{m-1} b_i x^i$ 라고 가정할 경우, 유한체 곱셈의 결과값인 $Z(x)$에 해

당하는 수식은 다음과 같이 표현된다.

$$Z(x) = A(x)\sum_{i=0}^{m-1} b_i x^i = \sum_{i=0}^{m-1} b_i (x^i A(x)) \bmod P(x)$$
$$= [b_0 A(x) + \ldots + b_{m-1} x^{m-1} A(x)] \bmod P(x)$$

이에 대한 기 수행 연구 결과는 α^2-multiplying circuit을 사용한 IEEE 논문에 제안자의 제시 구조와 타 아키텍쳐를 비교하여 자세히 나타내어 보였으며 [5], 본 연구에서는 α의 차수와 하드웨어 자원에 대한 트레이드-오프에 대한 분석을 수행하여 최적화할 수 있는 구조를 찾아 검증하였다. 제안한 방법은 유한체 곱셈 연산 수식을 변형하여 변형된 수식을 위한 α^k-multiplying circuit을 제안하고 k 값에 따른 자원 소모와 속도를 비교해 보면서 결정된 최적의 유한체 곱셈기 구조를 적용한 것이다. 제안하는 곱셈는, k 값이 커질 수록 자원이 많이 들면서 고속의 연산이 가능하다.

2. 유한체 나눗셈

주어진 유한체의 임의의 두 원소를 각각 $A(x) = \sum_{i=0}^{m-1} a_i x^i$, $B(x) = \sum_{i=0}^{m-1} b_i x^i$ 라고 가정할 경우, 유한체 나눗셈의 결과값인 $Z(x)$에 해당하는 수식은 다음과 같이 표현할 수 있다.

$$Z(x) = A(x)/B(x)$$
$$= A(x) \cdot B(x)^{-1} \bmod P(x)$$

즉, $B(x)$의 유한체 역원을 빠르고 효율적으로 구현하는 것이 핵심이 된다. 이 역원을 구하는 데 사용되는 기 연구된 알고리즘은 페르마의 정리, 유클리드의 알고리즘, Almost Inverse 알고리즘이 있으며, 유클리드 알고리즘과 AI 알고리즘이 변형되어 구현이 되고 있다 [6]. 본 연구에서는 loop unrolling과 table lookup 방식을 혼합하여 최적의 구조로 유한체 곱셈에 대한 역원을 구하는 효율적인 방식을 제안하여 타원곡선 암호용 보조 프로세서에 적용하였다.

V. 타원 곡선 암호 시스템의 FPGA 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 알고리즘의 성능을 평가하고 기존의 알고리즘들과 비교하기 위하여 알고리즘을 Verilog HDL [7] 로 코딩한 후 코드레벨에서의 기능을 ModelSim을 [8] 사용하여 시뮬레이션 및 디버깅을 수행하였고, FPGA에 구현하여 논리분석기로 결과를 측정하였다. FPGA는 Altera의 CycloneII 디바이스를 사용하였으며 코드의 합성,

표 1. SEG-2에서 제안하는 GF(2193) 상의 타원 곡선과 관련 변수
Table 1. Recommended EC and related parameters on GF(2193) 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

표 2. 구현 알고리즘 간 유한체연산의 수와 연산단계 수 비교
Table 2. Comparison of number (#) of GF operations and steps between algorithms

	♯ of steps	add( )	double( )	neg( )	quad( )
Double-and-add	m	$\frac{1}{2}m$	m	0	0
Quad-and-add	$\lceil \frac{m}{2} \rceil + 1$	$\frac{6}{8}\cdot\frac{1}{2}\cdot\frac{1}{2}m = \frac{3}{16}m$	1	2	$\lceil \frac{m}{2} \rceil + 1$

Mapping, P&R을 위한 소프트웨어로는 QuartusII를 사용하였다. 코드들은 모두 100MHz 이상의 클럭에서 동작하도록 설계되었으며 동작속도를 보장하기 위해서 버퍼 레지스터들을 추가하였다. 제안된 구조는 기존 구조의 타원 곡선 연산 계층 (double-and-add)에 네배점 (quad-and-add), 8배점 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.

표 3. 타원곡선연산 수행사이클 비교
Table 3. Comparison of EC operation cycles

	스칼라 곱셈 수행 시간		
	사이클 수	20MHz 환산 수행 시간	예상 면적
$GF(2^{167})$ standard basis implementation[9]	526,718 cycles	26.335 msec	20k gates
163 bit cryptoprocessor[10]	258,000 cycles	12.9 msec	24k gates
proposed 193 bit architecture	83,268 cycles	4.163 msec	59k gates

사용된 표준 타원곡선은 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. 타원곡선 곱셈연산을 수행할 때 적용한 알고리즘에 대한 연산단계 수 비교는 표 2와 같고, 스칼라 곱셈을 수행하였을 때 타 연구와의 성능비교는 표 3에 제시하였다.

VI. 결론

본 연구를 수행함에 있어서, 연구에 대한 주안 목표는 복잡한 계산 처리를 요하는 고성능 정보보호 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.

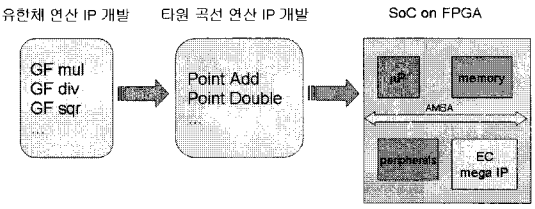

그림 2. 타원곡선 보조프로세서 구현 단계
Fig. 2. Design flow of EC Coprocessor

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 성능평가하고 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 같고, 타원곡선 연산보조프로세서의 전체 블록도는 그림 4와 같다.

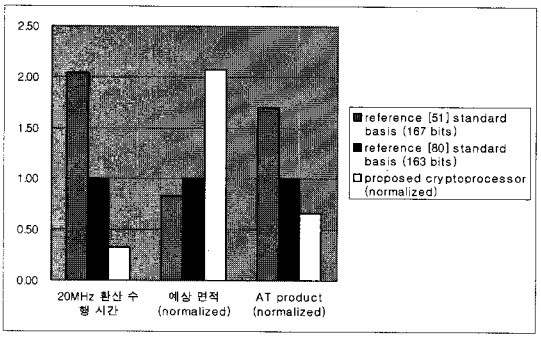

그림 3. 설계된 암호용 프로세서들의 시간, 면적 곱
Fig. 3. A*T product of designed crypto processors

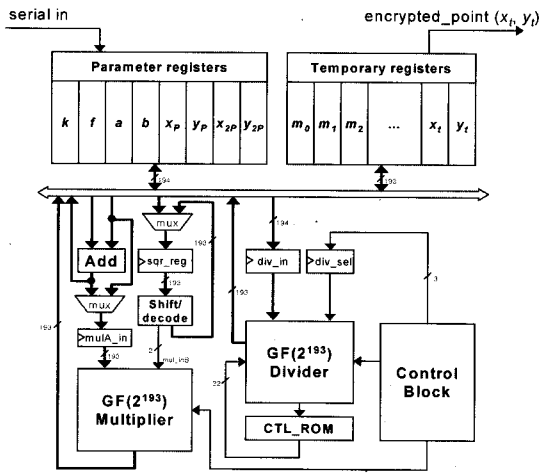

그림 4. 구현된 타원곡선연산 보조프로세서 블록도
Fig. 4. Implemented EC Coprocessor block diagram

감사의 글

이 논문은 2006년 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임 (KRF-2006-331-D00401)

참고문헌

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

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

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

[4] 문상국, "타원 곡선 암호용 프로세서를 위한 고속 VLSI 알고리즘의 연구와 구현," 연세대학교 대학원 박사학위논문집, 2002.

[5] Sangook Moon, Jaemin Park and Yongsurk Lee, "Fast VLSI Arithmetic Algorithms for High-Security Elliptic Curve Cryptographic Applications", IEEE Transactions on Consumer Electronics, Vol. 47, No. 3, pp. 700~708, August 2001

[6] Min-Sup Kang, et. al., "Hardware Implementation of Fast Division Algorithm for GF(2m)", The 8th International Conference of Advanced Communication Technology (ICACT), Vol. 1, Issue 20-22, Feb. 2006.

[7] Samir Palnitkar, 장훈 역, *Verilog HDL 디지털 설계와 합성의 길잡이*, 홍릉과학출판사, 2005.

[8] http://www.modelsim.com, ModelSim SE Tutorial, Jul. 2004.

[9] G. Orlando, C. Paar, "A Super-Serial Galois Fields Multiplier for FPGAs and its Application to Public-Key Algorithms," Proceedings of 7th Annual IEEE Symposium on Field-Programmable Custom Computing Machines, pp. 232-239, 1999.

[10] 최용제, 김호원, 김무섭, 박영수, "IC 카드를 위한 polynomial 기반의 타원 곡선 암호시스템 연산기 설계," 2001년도 대한전자공학회 하계종합학술대회 논문지 제 24권 제 1호, pp. 305-308, 2001.

저자소개

문상국 (Sangook Moon)

1995 연세대학교 전자공학 학사
1997 연세대학교 전자공학 석사
2002 연세대학교 전자공학 박사
2002~2004 하이닉스반도체 선임연구원
2004~현재 목원대학교 전자공학과 조교수
※관심분야 : 정보보호 VLSI 설계, Data encryption, 임베디드 SoC