情 報 保 護 學 會 誌
第 14 券 第 2 號, 2004. 4

나노 기술 환경에 적합한 차세대 정보 보호 프로세서 구조와 연산 회로 기술 연구†

최 병 윤*, 이 종 형**, 조 현 숙***

요 약

정보 통신과 반도체 공정 기술의 급격한 발전으로 나노 기술이 가까운 시일 내에 실용화 되고, 유비쿼터스 환경이 도래할 것으로 예측된다. 나노 기술 환경에서 사용되는 디바이스의 고집적도, 낮은 구동 능력, 배선 제약 특성이 정보 보호 분야에 사용되는 프로세서 구조와 회로 설계 기술을 크게 바꿀 것으로 예측된다. 본 연구에서는 이러한 기술 변혁에 대비하기 위해 나노 기술 환경에 적합한 차세대 정보 보호 프로세서 구조와 회로 설계 기술을 분석하였다.

Ⅰ. 서 론

최근 전자 공학과 반도체 관련 공정 기술의 급격한 발전으로 나노 전자(nano-electronics) 기술이 가까운 장래에 실용화 될 것으로 예측되고 있다[1-4]. 나노 기술(nano-technology)은 전자 공학, 물리학, 생물학 분야에서 다양한 방식으로 연구되고 있는데, 나노 기술에 사용하는 나노 디바이스는 정보 통신, 컴퓨터 분야의 프로세서 설계에 있어서, 기존 방식과는 다른 새로운 아키텍처, 회로 구조와 설계 방법을 필요로 한다. 현재 나노 기술 환경에 적합한 컴퓨터 구조에 대한 연구가 활발하게 진행되고 있다[5-10]. 그러나 나노 기술 환경이 정보 보호 프로세서 설계에 미치는 영향을 다룬 연구가 거의 없는 실정이다. 나노 기술이 차세대 마이크로프로세서 구조에 미치는 영향의 많은 부분이 정보 보호 프로세서에게 유사하게 영향을 미칠 것으로 예측된다. 그러나 암호 프로세서는 마이크로프로세서와 다른 구조적인 특성이 존재한다. 즉, 암호 프로세서는 마이크로프로세서와 달리 특수 목적으로 설계되며, 암호 알고리즘은 제어 처리 중심(control-dominated)이 아니라, 데이터 처리 중심(data-dominated) 특성을 갖고 있다. 그 외에도 처리하는 데이터의 길이가 수 백 혹은 수 천 비트의 길이를 갖는다. 또한 암호 디바이스는 외부 공격자에 의한 Tampering 등의 공격에 대한 대비 기능도 고려하여야 한다. 따라서 암호 분야의 특수한 동작 특성과 나노 디바이스의 특성을 고려하여, 나노 기술 환경에 적합한 암호 프로세서의 구조와 연산 회로에 대한 연구가 필요하다. 또한 정보 통신 기술과 나노 기술이 융합되어 유비쿼터스(Ubiquitous) 환경이 도래할 것으로 예측된다. 이러한 유비쿼터스 환경에서는 기존과는 다른 새로운 정보 보호 프로세서 설계 사양이 필요하다. 즉, 극도로 제한된 면적 조건하에 저전력, 저가격 보안 프로세서가 필요하다. 따라서 이러한 유비쿼터스 환경과 나노 기술을 함께 고려하는 암호 프로세서 구조에 대한 연구도 필요하다[11-12].

현재 나노 기술은 암호 프로세서 개발자에게 2가지 상반된 가능성을 열어 주고 있다. 즉, 나노 기술의 발전으로 양자 컴퓨터가 상용화될 경우 자리수가 100이상 큰 수의 소인수 분해를 단 몇 시간 만에 풀 수 있게 되어, RSA 공개키 암호 알고리즘은 안전도를 위협받게 될 것으로 예측된다. 따라서 수학적인 소인수 분해 연산의 난해성에 바탕을 둔 RSA 공개키 암호, 타원 곡선 암호(ECC, Elliptic Curve Crypto-

† 본 연구는 한국 전자 통신 연구원 위탁 연구 및 BB21 사업 지원으로 수행되었습니다.
* 동의대학교 컴퓨터공학과 (bychoi@deu.ac.kr)
** 동의대학교 전자공학과 (jonghlee@deu.ac.kr)
*** 한국 전자 통신 연구원 정보 보호 기반 연구팀 (hscho@etri.re.kr)

graphy)와 같은 공개키 암호와 대칭키 암호 알고리즘을 대체하거나, 보다 안전한 새로운 공개키 및 대칭키 암호 알고리즘 개발이 필요하다. 반면 나노 기술 발전에 따라 단일 칩에 더 많은 디바이스를 내장할 수 있고, 고속 회로를 구현할 수 있게 됨에 따라 RSA, ECC의 키와 평문 블록의 길이를 더욱 확대하여 안전도를 높일 수 있다. 이러한 2가지 상반된 측면이 존재하지만 나노 기술의 발전은 암호 분석 측면 보다는 암호 프로세서 하드웨어 성능 향상 기여에 미치는 효과가 더 크다고 예측되고 있다.

본 논문에서는 현재 정보 보안 프로세서에 널리 사용하는 공정 기술인 CMOS 공정의 미래 전망 분석과 CMOS를 대체할 기술로 평가되는 나노 디바이스를 살펴보고, 이러한 디바이스의 장점과 한계를 분석하였다. 이를 바탕으로 나노 기술 환경에서 암호 프로세서가 갖추어야 할 바람직한 구조와 연산 방식을 전망해 보았으며 논문 구성은 다음과 같다. 2장에서는 CMOS 스케일링에 따른 CMOS 디바이스의 향후 10년 후의 특성을 예측하고, 이를 대신하기 위해 연구되고 있는 나노 소자에 대해 살펴보고, 3장에서는 나노 기술 환경에서 암호 프로세서가 갖추어야 할 구조를 기술하였으며, 4장에서는 나노 기술 환경에서 부각되는 암호 연산 기술을 다루며, 마지막으로 5장과 6장에서는 결과 고찰과 결론을 기술하였다.

II. CMOS 스케일링과 차세대 나노소자

CMOS를 중심으로 하는 실리콘 기술은 더 빠르고 더 많은 기억용량을 가지는 개인용 컴퓨터에 대한 필요성에 의해 주로 발전되어왔다. 이와 같은 추세가 언제까지 지속될지 명확하지 않은 반면 이동통신과 휴대용 기기 등을 중심으로 하는 새로운 응용분야에 대한 요구는 지속적으로 커지고 있다. 따라서 CMOS 기술의 발전은 새로운 응용분야의 확대에 따라 과거와는 달리 다양한 발전경로를 갖게 될 수 있으며, 응용분야에 따라서는 CMOS외의 차세대소자에 대한 필요성이 급격히 대두될 전망이다.

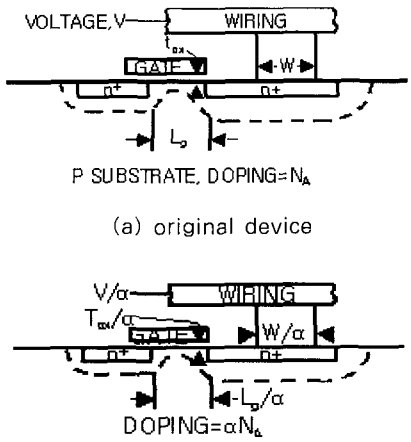
성공적인 컴퓨터 디바이스의 조건은 다음과 같이 정의되고 있다[13].

- 디바이스 입력이 출력과 분리됨
- 잡음이 포함된 신호를 복원하기 위한 큰 이득
- 최소 2개 이상의 fan-out을 갖는 구동 능력
- 비활성 상태에서는 작은 누설 전류

본 장에서는 CMOS 스케일링 기술의 한계와 전망, 또 그 대안으로 떠오르고 있는 새로운 나노 소자들을 소개한다. 현재 나노 디바이스는 위에 기술한 조건을 모두 만족하지 못하는 실정이다.

1. CMOS 스케일링(Scaling) 기술의 한계와 전망

과거 약 30 여 년 동안 CMOS기술은 무어의 법칙에 충실하며 눈부신 발전을 거듭하였으며 곧 100nm 이하 급의 소자가 상용화 될 전망이다[14-15]. 하지만 이와 같은 발전 속도가 계속 지속되기는 어렵다는 전망이 다양하게 논의되고 있으며, 그 중의 하나는 현재의 CMOS소자 스케일링 기술에 많은 제약요인들이 나타나고 있기 때문이다. 그림 1은 스케일링의 기본원리를 나타내는 것으로 이상적으로는 전압과 소자의 크기를 α 배만큼 감소시키고 도핑(doping)농도는 α 배만큼 증가시키는 것이다. 이때 소자내부의 전기장(Electric filed)은 스케일링 전과 동일함으로써 constant field scaling 이라 부르며, 그 결과로 회로의 속도는 α 배, 회로밀도는 α^2 배만큼 증가하게 된다.



(a) original device

(b) scaled device

〔그림 1〕 Constant field scaling의 개략도

그러나 이와 같은 스케일링은 몇 가지 제한요인들에 의해 지속하기 어려운데 그 원인중 하나는 회로의 전압을 채널길이와 같은 비로 낮출 수가 없기 때문이다. 이는 실리콘(Si)의 밴드 갭 에너지에 해당하는 전압은 스케일링하기가 어려워 MOS소자의 중요한 파라미터 중 하나인 문턱전압이 소자크기 비에 따라 스

케일링되지 않기 때문이다. 이와 같은 추세를 완화하기위해 소자내의 전기장이 ε배만큼 증가하는 것을 허용하는, 좀 더 일반적인 스케일링규칙이 사용되기도 한다. 그렇지만, 공정상 도핑농도의 정확한 조절이 힘들고, 이차원적 효과 역시 점점 더 중요하게됨에 따라 스케일링에 따른 소자의 동작이 예측과는 다르게 되는 경우가 많다. 특히 게이트의 산화막이 스케일링으로 점점 얇아지면 게이트의 절연체를 통해 터널링 현상이 발생할 수 있는데 예로 절연 산화막의 두께가 2 nm 일때 1.2V의 전압에서 약 0.1A/cm2 누설전류가 흐른다고 알려져 있다. [2] 이와 같은 누설전류는 저전력용 집적회로에서는 허용될 수 없는 경우가 많다.

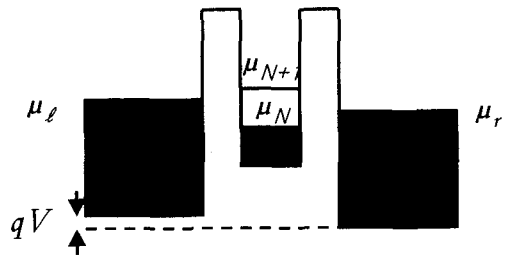
추후 CMOS소자의 스케일링은 응용분야에 따라 서로 다른 최적화 과정을 거칠 것이라 예상되는데 이는 응용분야에 따라 중요시되는 소자의 특성이 다르기 때문이다. 예로 DRAM의 경우는 정보의 손실을 방지하기 위해 낮은 누설전류가 필수적이며, 따라서 높은 문턱전압이 가지도록 소자수준에서 설계되는 것이 필요한 반면, 마이크로프로세서와 같은 논리 회로는 높은 동작주파수가 설계 시 가장 중요한 항목인 경우가 많아 낮은 문턱전압을 가지도록 설계될 것이다. 또한 최근 급격히 늘고 있고 휴대용기기를 목표로 하는 집적회로는 전력소모의 조절이 아주 중요한 설계목표가 될 것이며, 반면 동작속도 역시 중요하다. 따라서 한 칩 내의 CMOS 소자들이 경우에 따라 높은 문턱전압 또는 낮은 문턱전압에서 동작하는 것이 더 유리할 수 있으므로 회로의 동작모드에 따라 몸체전압을 능동적으로 조절하는 방법도 연구되어지고 있다.

따라서 CMOS 스케일링은 각 응용분야에 따라 다른 어려움들을 극복해 나가야 할 것이며, 공통적으로는 게이트 산화막을 대신할 새로운 절연체, 100nm 이하에서의 포토리소그라피 기술, SOI 또는 dual gate 구조와 같은 새로운 소자 개발 등이 필요 할 것이다. 하지만 이와 같은 기술적인 문제 들 외에 새로운 기술에 대한 막대한 투자의 필요성과 같은 경제적인 문제가 CMOS 스케일링의 한계를 결정지을 지도 모른다는 전망이 나오고 있다.

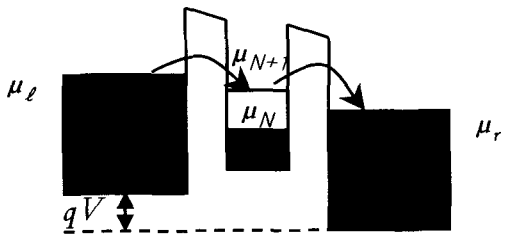
2. 차세대 나노 소자 [2-3]

CMOS를 중심으로 하는 실리콘 기술에 대한 기술적인 한계가 논의되고 있는 한편, 고성능 컴퓨팅과 새로운 통신환경에 필요한 새로운 나노급 소자에 대한 요구는 점점 증가되고 있다. 현재 주목받고 있는 나노소자들은 SET(Single Electron Tunneling), RTDs(Resonant Tunneling Diodes), RSFQ (Rapid Single Flux Quantum), QCA(Quantum Cellular Automata) 등이 있는데, SET는 집적도가 높고 전력소모가 적은 메모리와 같은 분야에 주로 응용될 것으로 보인다. 반면 RTDs는 약 10GHz에서 100GHz 정도의 높은 동작속도가 요구되는 분야에 응용될 것으로 보이며, RSFQ는 고속 동작과 낮은 전력소모를 동시에 얻을 수 있는 소자로 알려져 있으나, 소자의 특성상 냉각장치가 필요하다.

그림 2는 SET의 원리를 나타내고 있다. SET가 동작하기 위해서는 전자 섬 (island of electrons)의 커패시턴스 C가 충분히 작아 전자 섬을 충전할 에너지 (q^2/C)가 열잡음 에너지(kT) 보다 훨씬 커야 한다. 이때 인가된 전압 V가 작아 $\mu_{N+1} > \mu_l$ 상태이면 전자의 흐름이 발생되지 않는데 이를 Coulomb Blockade 라고 부른다. 만약 인가된 전압이 증가하여 $\mu_l > \mu_{N+1} > \mu_r$ 과 같은 조건을 만족시키면 전자가 터널링(tunneling)에 의해 흐를 수 있게 된다. SET는 상온에서 동작되기 어려운 단점이 있는데, 이는 정보의 손실 없이 읽기/쓰기를 하기 위해서는 q^2/C 가 kT보다 훨씬 커야하기 때문이다. 또한 SET소자가 외부부하에 연결되어 있다면 RC 시상수에 의해 동작주파수가 제한됨으로 SET는 논리 회로보다는 기억소자로 응용될 가능성이 더 크다고 알려져 있다.



(a) Coulomb Blockade



(b) Single Electron Tunneling

[그림 2] Single Electron Transistor의 원리

또한 RTDs는 빠른 터널링으로 고속의 소자제조가 가능하다고 알려있다. 또한 I-V 곡선에서 음의 저항을 나타내는 영역이 나타남으로써 필터 및 오실레이터의 설계에 유리하고 다치 논리 소자 제작에 이상적이라 하겠다. 하지만 앞으로 해결해야 할 점도 많은데 첫 번째가 소자 특성이 각 레이어(layer)의 두께변화에 너무 민감함으로써 상업화를 위한 제조공정이 어려운 점이 있고, 두 번째는 I-V 곡선을 조절할 3단자 소자의 제작이 아직은 연구단계로 추후 해결되어야 할 과제 중의 하나이다. 소자특성으로는 출력전력이 μW 범위로 너무 낮은 것도 RTDs의 실용화에 해결해야 할 과제로 남을 것이다. 그러나 현재 가장 상용화에 근접한 다바이스가 RTD 디바이스이다.

마지막으로 RSFQ 소자는 flux quantum을 하나의 비트처럼 정보단위로 이용하는 소자로써 초전도 현상을 이용하는 것으로 알려져 있다. RSFQ는 100GHz이상의 동작이 가능하면서도 게이트 당 1μW 정도의 전력소모가 가능한 유일한 기술로 알려져 있다. 하지만 RSFQ는 기본적으로 초전도현상을 위한 냉각장치가 필수적이어서 그 응용범위가 넓지는 않을 전망이다. 그 외 화학적, 생물학적 반응을 이용하여 자가 조립(self-assembly)이 궁극적으로 가능하게 하는 것을 목표로 하는 분자 나노 전자(Molecular Nanoelectronics)분야와 전자의 마그네틱회전(magnetic spin)을 외부의 전압이나 마그네틱필드로 조절할 수 있는 것을 이용한 스핀소자(Spin devices)분야가 연구되고 있는데 이들 분야는 앞서의 나노 소자들에 비해서는 초보적인 연구단계에 머물고 있는 수준이다.

현재 연구되고 있는 나노 소자들이 CMOS를 전면적으로 대체하리라는 전망보다는 스케일링을 포함한 CMOS의 한계가 다다르는 부분에서 그 틈새시장을 넓혀갈 것으로 전망된다.

Ⅲ. 나노 기술에 적합한 암호 프로세서 구조

본 장에서는 나노 기술 환경에 적합한 암호 프로세서 구조와 차세대 정보 보호 시스템의 기술의 방향을 분석하였다.

1. 나노 기술이 프로세서 설계에 미치는 효과

나노 크기 와 마이크로 크기 디바이스 특성은 표 1과 같이 구분할 수 있다. 표 1에 따르면 마이크로 디바이스에 비해 나노 크기 디바이스가 갖는 장점은 크게 높은 집적도, 높은 동작 주파수, 저전력, 및 다치 논리(multi-valued logic) 연산 가능성이다. 반면 나노 디바이스가 갖는 단점은 신호의 낮은 구동 능력, 백그라운드 전하(background charges)와 공정 오차에 따른 높은 민감도(sensitivity) 문제가 존재한다. 이에 따라 모듈화된 설계, 인접한 연결 배선, 클록 분배가 나노 디바이스 회로 설계에 매우 중요한 요소임을 알 수 있다. 또한 fan-out이 작고 구동 능력이 떨어지므로, 게이트 수준이 아닌 기능 블록(functional block) 레벨의 라이브러리 기반의 설계 방식이 필요하다. 특히 마이크로 디바이스에 비해 단점으로 갖는 특성이 나노 컴퓨터와 정보 보호 프로세서 설계 시 중요하다.

〔표 1〕 나노 크기와 마이크로 크기 디바이스의 주요 특성 비교

Parameter	Micro scale	Nano scale
Minimum dimension	500 - 1000 nm	5-10nm
Power consumption	1 μW	1 pW
Gain	100	≅1
Stable state	2	many
Clock rate(Ghz)	1	1000

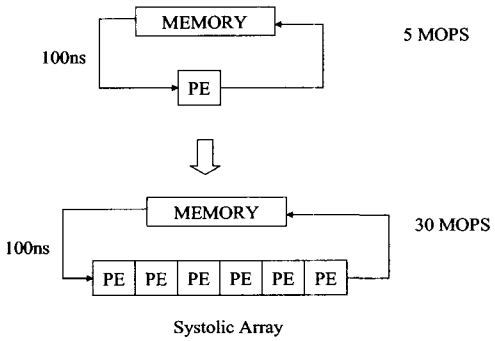
2. Systolic Array와 PIP에 기반을 둔 프로세서 구조[5]

나노 기술 환경에서는 게이트 배선의 지연시간이 시스템 성능에 큰 영향을 미칠 수 있다. 따라서 인접한 연결 배선 구조를 갖는 시스토릭 어레이 구조와 PIP(propagated Instruction Processor) 구조가 바람직하다. 2가지 구조는 제어 신호가 파이프라인으로 전달되는 것과 명령어가 파이프라인으로 전달하는 약간의 차이만 존재하고 유사한 개념이다. 현재 시스토릭 어레이 구조를 이용하는 영상 처리 프로세서가 있지만, 대부분 학술적인 연구 측면에서의 구현이고 실제로는 많은 면적과 많은 입출력 핀에 따른 적절한 입출력 타이밍 제어의 어려움, PE의 추가를 통해서만 기능을 확장할 수 있다는 융통성 제한으로 고속의 동작을 요하는 특수한 목적을 제외하고는, 가격 대비 성능이 중요한 상용 칩에서는 거의 구현되지 않았다. 그러나 나노 기술 환경에서는 암호 알고리즘을 구현하는 프로세서의 경우는 암호 알고리즘을 시스토릭 어레이

구조로 매핑하여, 시스토릭화된 구조로 동작시키는 것이 전역 제어 신호를 제거할 수 있기 때문에 널리 사용될 수 있을 것이라 판단된다.

2. Wavefront Array 기반 프로세서 구조

시스토릭 어레이 구조는 사람의 심장에서 피가 흘러나와 신체 각 부분을 거친 후 다시 심장으로 돌아오는 동작을 연산 구조에 적용한 것으로 H.T. Kung이 제안하였다. 그림 3은 시스토릭 연산의 기본 개념을 나타내며, 그림에서 메모리가 심장(Heart)을 모델링하며, PE(processing element) 또는 셀(cell)은 신체의 각 기관에 대응된다.



〔그림 3〕 시스토릭 어레이 기본 개념

이러한 시스토릭 어레이는 크게 4가지 구조적인 특징을 갖는다.

첫째, 소수의 단순한 셀로 구성된 단순하고 규칙적인 설계를 갖는다. 이러한 구조는 데이터와 제어 흐름이 단순하고 규칙적이다.

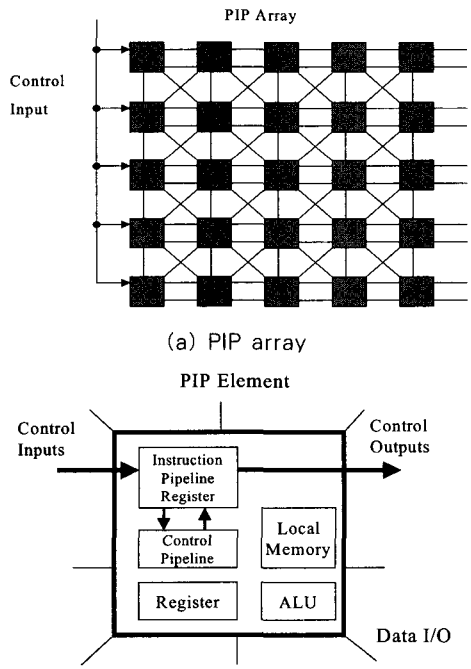
둘째, 데이터 연산에 있어서 높은 병렬성이 존재한다. 시스토릭 구조인 경우 높은 수준의 연산 병렬성, 파이프라인 처리, 인접한 셀 간의 정보 전달(local communication) 특성을 갖고 있다.

셋째, 연산 동작과 입출력 동작사이에 균형이 유지된다. 즉, 외부 셀에서만 입출력이 이루어지고 셀의 확장성이 용이하다.

넷째, 모든 셀이 단일 클록에 동기화되어 동작한다.

이러한 시스토릭 어레이 연산은 알고리즘 내부에 데이터 병렬성이 존재하는 DSP, 영상 처리, Motion Estimation와 같은 연산에 효율적으로 적용가능하다. 그런데 RSA, ECC와 같은 공개키 알고리즘은 데이터 처리에 병렬성이 존재하므로, 나노 기술 환경에서는 시스토릭 어레이로 구현하는 것이 바람직할 것으로 판단된다.

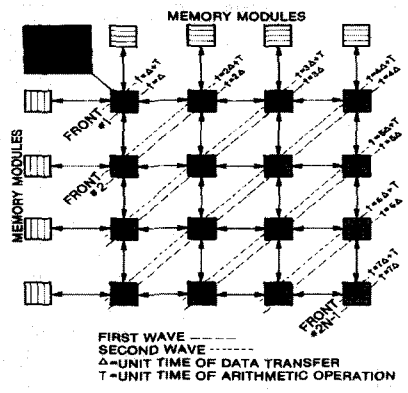
시스토릭 구조는 인접한 PE간의 신호 전달을 통한 데이터 및 제어 신호의 전역 배선 제거, 모듈화된 구조, 데이터의 파이프라인 및 병렬 처리 특성을 갖고 있기 때문에 고속 동작이 가능하다. 그러나 클록 신호가 모든 PE에 동시에 제공되어, 모든 PE가 단일 클록에 의해 동기되어 동작하므로, 클록 배선(routing)과 스큐(clock skew), 클록 신호의 많은 부하(load) 문제가 배열 크기를 제한한다. 이것은 나노 디바이스가 신호 버퍼링 능력이 낮게 때문에 이를 해결하기 위한 클록 버퍼 구조에 대한 연구가 필요하다. 그리고 모든 알고리즘이 시스토릭 구조로 변경하는 것이 가능하지 않기 때문에, PIP와 같이 내부에 범용성을 갖는 연산 장치를 장착하여, 좀더 융통성 있는 구조로 구현하는 방안도 가능하다. 그림 4는 PIP 구조를 나타낸다.



〔그림 4〕 PIP 프로세서

3. Wavefront Array와 Asynchronous Circuit에 기반을 둔 프로세서 구조[16-17]

배선 지연 문제를 해결하기 위해 전역적인(global)



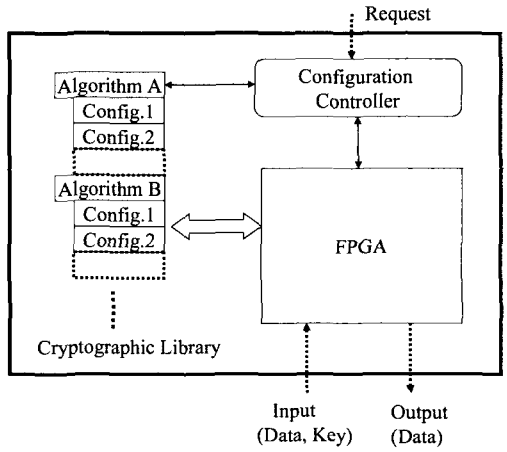
〔그림 5〕 Wavefront Array 구조

클록을 사용을 배제하는 기법으로 비동기 회로 설계 기법이 사용된다. 시스토릭 어레이의 전역 클록 문제를 해결하기 위해 제안된 Wavefront Array 구조는 시스토릭 어레이 구조와 거의 유사한 동작 특성을 갖는다. 다만 PE간의 데이터 전달시 전역 클록을 사용하지 않고 비동기 방식의 handshaking을 사용하는 점만 다르다. 그림 5는 Wavefront Array 구조를 나타내며, PE간에는 데이터 전달을 위해 비동기 회로에서 사용되는 Handshaking 기법이 사용된다. 이러한 Wavefront Array는 시스토릭 어레이의 전역 클록 사용에 따른 클록 스큐 문제를 해결하는 이점은 있지만, 상대적으로 제어가 복잡하다는 결점이 있다.

클록을 사용하지 않는 완전한 비동기 회로는 제어가 복잡하고, 다른 동기 시스템과의 인터페이스가 어렵기 때문에, 동기 회로와 비동기 회로가 함께 사용되는 hybrid 구조가 나노 환경의 암호 프로세서 설계시 널리 사용될 것으로 예측된다.

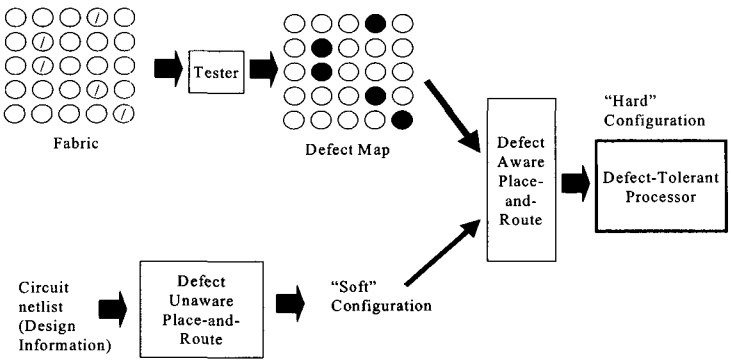
4. Reconfigurable 와 Defect-tolerant 프로세서 구조

최근의 반도체 기술 중 가장 급격한 기술 향상 분야는 Reconfigurable Hardware 분야이다[18-20]. 특히 유비쿼터스 환경에서 사용되는 디바이스는 작은 면적, 적은 전력 소비 등을 필요로 한다. 그런데 모든 암호 알고리즘을 하드웨어로 구현할 경우 면적상 큰 문제가 있다. 이에 대한 해결방안은 하나의 FPGA를 준비하고, 응용 분야 또는 연산 시점에 맞게 Configuration 메모리에 담긴 Configuration 정보로 FPGA를 적절한 알고리즘을 구현하는 대칭키, 공개키, 인증 프로세서로 구성하여 사용하는 방식이다. 이렇게 할 경우 컴퓨터 시스템에서 가상 메모리(virtual memory) 기법을 사용하여 제한된 물리 메모리(physical memory)의 크기에 무관한 프로그램을 작성하는 것과 유사한 효과를 구현할 수 있게 된다. 단, FPGA는 실리콘 ASIC 칩으로 구현하는 방식에 비해 속도가 떨어지므로, 성능보다는 면적이 중시되는 응용 분야에 적합하다. 그림 6은 이러한 기법을 사용하는 Reconfigurable 암호 프로세서 구조를 나타낸다.



〔그림 6〕 Adaptive Reconfigurable 암호 프로세서 구조

나노 공정의 특징은 더 많은 디바이스를 집적할 수 있는 가능성을 제공하지만, 디바이스의 신뢰성이 떨어지므로 현재 CMOS 공정과 같은 높은 수율(yield)을 보장하기 어렵다. 즉 defect density가 10%이상이 될 것으로 예측된다. 그 경우 제작한 대부분의 디바이스는 결점을 가지고 있을 가능성이 있다. 현재 실리콘 공정과 달리 디바이스를 폐기처분 시키는 것은 경제적인 문제로 어렵다. 따라서 나노 공정 환경에서는 경제성을 보장하기 위해 fault-tolerant 기반의 Reconfigurable 프로세서 설계가 필요하다. 이를 위해 각 셀(cell)에 테스트 기능 회로를 내장하고, 외부에서 Reconfigurable 하드웨어의 fault를 감지하고, Configuration과정에서 fault가 존재하는 셀을 사용치 않은 배치 및 배선을 통해 fault-tolerant 구조를 구현할 수 있다. 이러한 fault-tolerant 구조는 reconfigurable 하드웨어 구조에 사용될 수 있다. 현재 FPGA 공정 기술이 급격히 발전하고 있기 때문에 나노 기술 환경에서는 적절한 reconfigurable 기능과 fault-tolerant 기능을 제공해 줄 수 있을 것으로 판단된다. 그림 7은 fault-tolerant를 구현하는

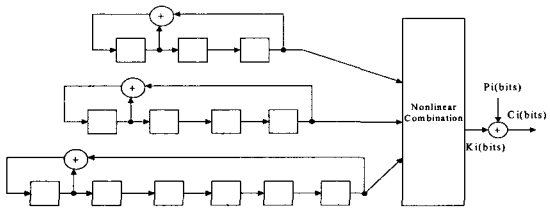


〔그림 7〕 fault-tolerant 구조 구현

기법을 나타낸다. 단, 암호 프로세서의 경우 범용의 프로세서와 달리 tampering에 대한 대비를 해야 한다. 즉, 셀의 테스트를 위한 회로의 경우 내부 셀의 동작을 접근할 수 있는 경로를 제공하므로, Hard Reconfiguration후에는 테스트용 포트는 지동 파괴되도록 하는 기능을 내장하는 것이 바람직하다.

4. Stream Cipher 기반 프로세서 구조

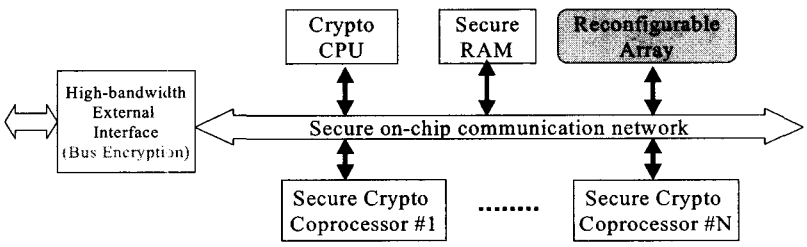
현재 DVD, 무선랜에 사용되고 있는 스트림 암호 알고리즘의 경우 블록 암호에 비해 안전도가 떨어진다는 결점이 있지만, 블록 암호에 비해 채널 잡음에 강하고, 고속 동작, 저전력 동작, 적은 면적의 하드웨어 구현이라는 장점이 존재한다. 따라서 유비쿼터스 환경, 저전력 portable 및 wireless 응용 분야에 스트림 암호가 보다 널리 사용될 것으로 판단된다. 그러나 대부분의 LFSR(linear feedback shift register) 기반 스트림 암호와 IEEE 802.11 표준에 채택된 WEP(wired equivalent privacy)에 사용된 RC4 알고리즘이 안전도에 취약점을 들어내고 있어서, 보다 안전한 새로운 스트림 암호 기법 개발이 필요하다. 그림 8은 현재 널리 사용되고 있는 LFSR 기반의 스트림 암호의 일반적인 키 스트림 생성 회로를 나타낸다.



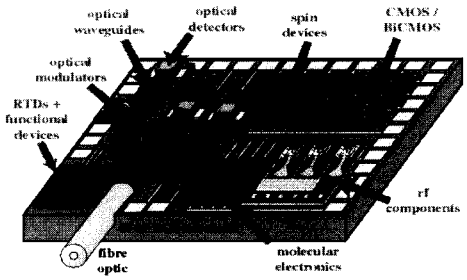
〔그림 8〕 LFSR 기반 스트림 암호

5. CSoC(Cryptographic System on a Chip) 암호 프로세서 구조

나노 공정 기술이 발전함에 따라, 단일 칩에 수십억 개의 트랜지스터가 내장될 수 있게 될 것으로 판단된다. 따라서 고성능을 요하는 암호 프로세서의 경우 단일 칩에 모든 암호 기능을 내장하는 CSoC(Cryptographic System on a Chip)이 구현 가능할 것으로 판단된다. 단, 난수 발생기(random sequence generator)와 같이 아날로그 성격의 회로, RF(radio frequency) 회로와 디지털 회로를 단일 칩에 구현하는 것은 crosstalk, 신호 왜곡 등이 심할 것으로 판단된다. 따라서 단일 칩 보다는 MCM(multi-chip module) 패키징 형태의 CSoC가 구현될 가능성이 크다고 판단된다. 또한 나노 공정 기술의 경우 연산



〔그림 9〕 Cryptographic System on a Chip(CSoC) 구조의 암호 프로세서



〔그림 10〕 CMOS와 차세대 나노 디바이스가 공존하는 SoC 구조[2]

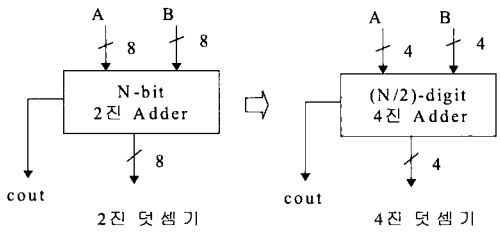
회로 보다는 배선 문제가 심각할 것으로 판단되므로, 블록간의 배선시 현재 네트워크에서 사용되는 통신 프로토콜을 갖는 온 칩 버스 구조가 채택될 가능성이 있다. 암호 프로세서의 경우 통신 네트워크 구조의 온 칩 버스에 Tampering에 대비한 보안 프로토콜을 선택사항으로 구현할 가능성이 있다고 판단된다. 그림 8은 보안 기능 내장 온 칩 버스(통신 네트워크)를 갖는 CSoC를 나타낸다. 그리고 그림 10은 나노 공정 환경에서 실리콘 디바이스와 차세대 나노 디바이스가 함께 사용된 차세대 SoC(System on a Chip) 구조를 나타낸다. 특히 나노 SoC 환경에서는 기존 IRAM (Intelligent RAM) 구조와 달리 non-volatile 메모리가 프로세서와 단일 칩에 구현될 가능성이 크다.

IV. 나노 기술 환경에서 유망한 암호 연산 기술

암호 알고리즘은 오차가 존재하지 않는 정수 연산에 기반을 두고 있는데, 현재 사용되고 있는 대부분의 암호 연산은 나노 기술 환경에서도 사용될 수 있을 것으로 판단된다. 다만 현재 널리 사용되고 있지 않은 연산 기법 중에서 나노 기술 환경에서는 주목을 받을 수 있는 몇 가지 연산 기술을 살펴보았다. 본 연구에서는 나노 디바이스의 3가지 측면, 다치 논리, 나노 공정에서는 고속의 ROM 디바이스 사용 가능성, fan-out 제한 특성을 고려하였다.

1. 다치 논리(multi-valued logic) 연산[21-22]

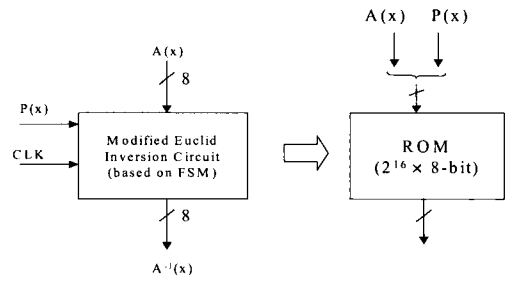
기존 CMOS 실리콘 소자에 비해, 나노 디바이스의 경우 다치 논리 구현이 용이해진다. 다치 논리의 경우 2진 시스템에 비해 다음과 같은 장점이 있다. 첫째, 신호가 다수개의 레벨을 갖고 있기 때문에 배선 수가 작아진다. 둘째, 메모리 셀에 하나 이상의 비트를 저장하기 때문에, 동일한 다이(die)에 더 많은 정보를 저장할 수 있다. 연산 회로의 경우 RNS(Residue Number System) 혹은 RSD(Redundant Signed Digit) 수 체계를 사용하여, 캐리 전달이 없거나, 캐리 전달이 제한되는 연산 회로를 구현할 수 있어서 고속의 회로 구현이 가능하다. 다치 논리의 경우 기존 2진수 기반의 연산에 비해 훨씬 빠른 고속 연산이 가능하므로, 기존 암호 프로세서에 비해 훨씬 빠른 고속 동작이 가능하다. 그림 11은 2진 덧셈기와 4진 덧셈기의 구조를 나타낸다. 4진 덧셈기의 경우 digit 수가 8에서 4로 축소됨에 따라 배선 수가 작고 고속 동작이 가능하다.



〔그림 11〕 2진 덧셈기와 4진 덧셈기 구조

2. ROM을 활용한 연산 구조

RSA와 같은 공개키 암호 알고리즘의 경우, 지수승에 대한 사전 계산 테이블(precomputed lookup table)을 사용할 경우 기존 방식에 비해 훨씬 고속 동작이 가능하다. 실리콘 소자의 경우 ROM이 많은 면적을 차지하고 속도가 느린 결점이 있었지만, 나노 소자의 경우 고속 고밀도 non-volatile memory가 상용화 될 것으로 예측된다. 이렇게 되는 경우 기존의 불규칙한 배선 구조를 가진 많은 연산이 나노 환경에서는 배선 문제로 ROM 형태로 구현될 가능성이 존재한다. 그림 12는 GF(2^8) 역원(inversion) 계산

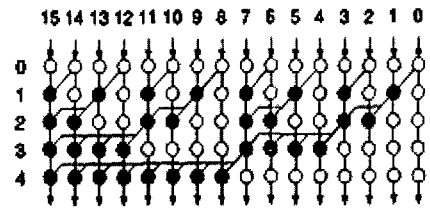


〔그림 12〕 ROM을 이용한 GF(28) 역원 회로

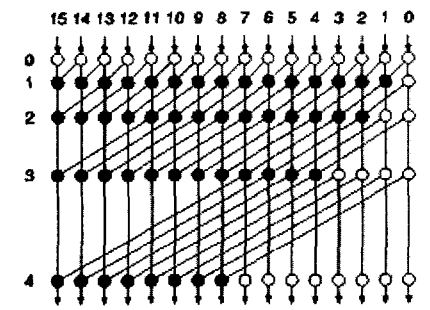
회로를 ROM으로 구현하는 방식을 나타낸다. 그림 12에 보는 바와 같이 기존 순서(sequential) 논리 구조의 역원 회로를 ROM을 사용하여 단일 클록에 조합 회로로 구현할 수 있음을 보여 준다. 단, 이러한 연산 방식은 ROM이 갖는 특성이 면적과 속도 측면에서 기존 논리 구조의 회로에 비해 이점이 있을 때만 타당하다.

3. 작은 수의 팬 아웃을 갖는 모듈화 연산 구조

모든 연산의 기본이 되는 덧셈 연산을 고속으로 구현하기 위한 연구가 Parallel Prefix algorithm 계산 기법[23]을 이용하여 많이 수행되었다. 그러나 기존 Parallel Prefix 기반의 덧셈기의 성능 분석시 팬 아웃의 효과가 크게 고려되지 않았다. 그러나 나노 기술 환경에서는 팬 아웃 수가 작고 모듈화된 연산 방식이 바람직하다. 그림 13은 Parallel Prefix Algorithm을 중심으로 2가지 덧셈기 구조를 분석했다. 첫 번째 방식은 기존 마이크로 CMOS 기술 환경에서는 두 번째 구조에 비해 더 작은 게이트 수를 갖는 우수한 구조로 평가되었지만, 나노 공정 환경에서는 팬 아웃 개수가 2인 2번째 방식의 Brent-Kung Adder가 적합한 구조로 판단될 수 있다.



(a) Sklankey algorithm



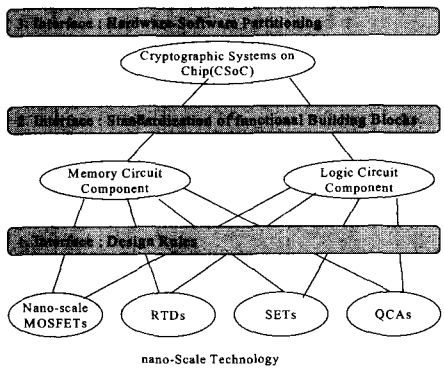
(b) Brent-Kung algorihm

[그림 13] 나노 환경에 적합한 Parallel prefix algorithm 구조

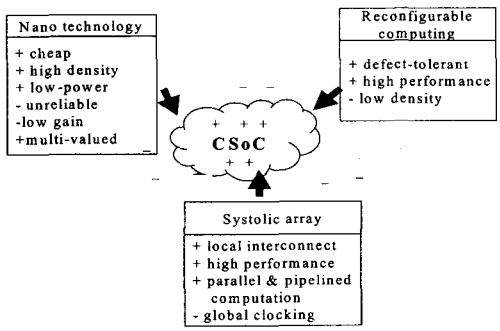
V. 결과 고찰

마이크로 크기에서 나노 크기의 환경으로 바뀜에 따라, 암호 프로세서 및 범용 프로세서 구조의 초점은 연산 처리에서 통신 문제로 바뀌게 됨을 알 수 있었다. 나노 공정 환경에서는 연산 처리는 용이하지만, 배선(interconnection) 문제와 구동 능력이 떨어지는 결점이 있다. 따라서 암호 프로세서 회로 설계시 게이트 수준의 라이브러리(library)가 아닌 기능 블록 수준의 라이브러리가 필요하고, 인접한 배선 구조를 갖는 시스토릭 어레이와 defect tolerant reconfigurable array를 활용하는 구조가 널리 사용될 것으로 예측된다. 그리고 암호 연산 방식으로 다치 논리 연산 방식과 ROM을 사용하는 연산 구조가 증가할 것으로 예측된다. 그림 14는 나노 기술 환경에서 암호 프로세서의 설계 계층 구조를 나타낸다.

그림 15는 암호 프로세서와 관계된 나노 기술, 암호 기술, reconfigurable array, systolic array 기술 사이의 관계를 나타낸다. 그림에서 "+" 기호는 장점을, "-"기호는 단점을 나타낸다.



[그림 14] 나노 공정에서 암호 프로세서 설계 계층 구조



[그림 15] 나노 기술 환경에서 암호 프로세서 구현과 관련된 주요 프로세서 기술

VI. 결 론

나노 기술이 상용화 될 경우 정보 통신, 컴퓨터, 정보 보안 분야는 새로운 기술 변혁을 맞이할 것으로 예측된다. 다른 분야와 달리 정보 보안 분야는 나노 기술 발전에 따라 암호 분석, Tampering 등의 암호 공격 가능성 증대와 암호 프로세서 연산 능력 향상이라는 상반되는 환경에 놓일 가능성이 크다. 따라서 나노 기술 분야에서 예측될 수 있는 여러 가지 정보 보안 문제 위협에 신속하게 대처하고, 이를 해결하기 위한 연구가 다른 분야보다 앞서 추진되어야 한다. 이러한 문제가 해결되어야 유비쿼터스 환경을 구현하기 위한 토대를 마련할 수 있을 것으로 판단된다.

본 연구에서는 차세대 나노 디바이스가 갖는 장단점을 바탕으로 차세대 암호 프로세서의 구조와 암호 연산 방식의 변화를 분석했다. 분석 결과 나노 공정 환경에서는 연산 처리 보다는 배선 문제와 디바이스의 defect 문제가 심각하기 때문에, non-volatile 메모리와 연산 처리부가 통합되고, 지역적인 배선(local connection), 재구성 가능(reconfigurable) 어레이 구조가 암호 프로세서에 적합하다고 판단된다.

참 고 문 헌

[1] Dan DASCALU, "From Micro- To Nano-Technologies", *'98 International Conference of Semiconductors*, vol.2, pp.5-9, Oct., 1998,

[2] ITRS, Technology Roadmap for Nano-electronics, 2nd edition. http://public.itrs.net/ Nov., 2000.

[3] ITRS, Technology Roadmap for Nano-electronics, 1999.

[4] ITRS, International Technology Roadmap for Semiconductors, http:// public.itrs.net/, 2003.

[5] Fountain T.J., D.G. Crawley, M.R.B.Forshaw, S.Spagocci, and D. Berzon, "Novel processor arrays for nanoelectronics," *Ultra electronics program review*, Estes Park, Colorado, pp.34-38, Oct., 1998,

[6] Fountain T.J., M.J.B. Duff, D.G. Crawley, C.D.Tomlinson, and C.D. Moffat, "The use of nano-electronic devices in highly parallel computing systems," *IEEE Trans. On Very Large Scale Integrated Systems*, vol.6, pp.31-38, March 1998.

[7] Montemelo, M., Love, C., Opiteck, G. Goldhaber Gordon, D, Ellenbogen, Technologies and Designs for Electronic Nanocomputers, The Mitre Corporation, http://www.mitre.org/technology/nanotech/.

[8] Paul Becket and Addrew Jennings, "Towards Nanocomputer Architecture," *7th Asia-Pacific Computer Systems Architecture Conference in Research and Practice in Information Technology (ACSAC '2002)*, 2002.

[9] Karl F. Goser and Chrisina Pacha, "System and Circuit Aspect of Nanoelectronics," *24th European Solid-State Circuits Conference (ESSCIRC '98)*, September 1998.

[10] Karl F. Gosner, Christina Pacha, Andreas Kanstein, and Markus L. Rossmann, "Aspect of Systems and Circuits for Nanoelectronics", *Proceedings of the IEEE*, vol.85, no.4, pp.558-573, April 1997.

[11] Christof Paar, "The future of the Art of Cryptographic Implementations", *Position Statement for the STORK (Strategic Roadmap for Cryptography) Workshop*, November 26-27, 2002, Brussels.

[12] R. Reed Taylor and Seth Copen Goldstein, "A High Performance Flexible Architecture for Cryptography," *Proceedings of the Workshop on Cryptographic Hardware and Embedded System 1999(CHES '99)*, pp.231-245, August 1999.

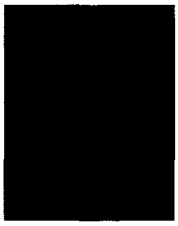
[13] R.W. Keyes, "What makes a good computer device ?", Science, vol. 230, pp.138-144, 1995.

[14] B. Davari, R. H. Dennard, and G. G. Shahidi "CMOS scaling for highperformance and low-power—the next ten years," Proc. IEEE, vol.89, pp.595-606, Apr. 1995.
[15] D. J. Frank, et al. "Device Scaling Limits of si MOSFETs and Their Application Dependencies," *Proc. IEEE*, vol.89, pp.259-288, Mar. 2001.
[16] S.Y. Kung, "VLSI array processor", *IEEE ASSP magazine*, pp.4-22, July, 1985.
[17] D.M. Chapiro, "Globally-aynchronous, locally-synchronous systems", Ph.D dissertation, Stanford University, Stanford, CA, October 1984.
[18] Thomas Wollinger and Christof Parr, "How secure are FPGAs in Cryptographic Applications? (Long Version)", http://www.crypto.ruhr-uni-bochum.de/.
[19] Israel Koren and zahava koren, "Defect tolerance in VLSI circuits: techniques and Yield analysis", *Proceedings of the IEEE*, vol.86, no.9, pp.1819-1836, September 1998.
[20] Christof Paar, Brendon Chetwynd, Thomas Connor, "An Algorithm-Agile Cryptographic Co-Processor based on FPGAs", *SPIE's symposium n voice, and data communications*, September, 1999.
[21] Elena Dubrova, "Multi-valued logic in VLSI : challenge and opportunities," http://www.ele.kth.se/~elena/.
[22] Elena Dubrova, Yusuf Jamal, Jimson Mathew, "Non-silicon non-binary computing: Why not ?", http://www.ele.kth.se/~elena/.
[23] Reto Zimmermann, Binary adder architectures for cell-Based VLSI and their synthesis, ETH Integrated System Laboratory, Ph.D thesis, 1997.

〈著者紹介〉

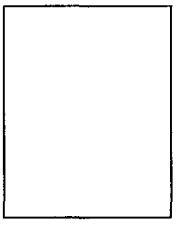
최 병 윤 (Byeong Yoon Choi)

1985년 2월 : 연세대학교 전자공학과 졸업
1987년 2월 : 연세대학교 전자공학과 석사
1992년 8월 : 연세대학교 전자공학과 박사
1997년 8월~1998년 8월 : 미국 University of Illinoia at Urbana-Champaign, 방문 연구교수
1993년 2월~현재 : 동의대학교 컴퓨터공학과 교수
〈관심분야〉 정보 통신용 VLSI 설계, RISC와 암호 프로세서 설계,, 정보보호



이 종 형 (Jong-Hyung Lee)

1987년 2월 : 연세대학교 전자공학과 (공학사)
1990년 2월 : 연세대학교 전자공학과 (공학석사)
2000년 5월 : Ph. D., Electrical & Computer Engineering, Virginia Tech
1990년 1월~1994년 6월 : (주)대우 반도체 사업본부
2000년 5월~2001년 5월 : Principal R&D Engineer, Advanced Technology Lab., Sprint
2001년 5월~2002년 2월 : System Engineer, Opthos, San Carlos, CA
2002년 3월~현재 : 동의대학교 전자공학과 교수
〈관심분야〉 광통신, 나노 디바이스, 정보보호



조 현 숙 (Hyun-Sook Cho)

1998년~2001년 : 충북 대학교 전자 계산 학과 (이학 박사)
1982년~2002년 : 한국 전자 통신 연구원(ETRI) 지상 SW 실장, 한국 전자 통신 연구원(ETRI) 정보 보호 시스템 연구 부장, 한국 전자 통신 연구원(ETRI) 정보 보호 연구 본부장 역임
2003년~현재 : 한국 전자 통신 연구원(ETRI) 차세대 시큐리티 기술 개발 사업 단장
〈관심분야〉 Network Security, 이동인터넷 보안, Conditional Access