情報保護學會論文誌
第 21 卷 第 5 號, 2011. 10

전력 분석 공격에 안전한 3상 동적 전류 모드 로직*

김 현 민,† 김 희 석, 홍 석 희‡
고려대학교 정보경영공학전문대학원

Three Phase Dynamic Current Mode Logic against Power Analysis Attack*

Hyunmin Kim,† HeeSeok Kim, Seokhee Hong‡
Graduate School of Information Management and Security, Korea University

요 약

암호화 장비에 의해 소비되는 전력이 연산 데이터에 의존하는 특성을 이용한 전력 분석 공격이 제안된 이후, 이러한 연관성을 하드웨어에서 원천적으로 차단할 수 있는 많은 로직들이 개발되었다. 그 중 대부분의 로직들이 채택하고 있는 DRP로직은 전력 소비량을 균형 있게 유지하여, 연산 데이터와 소비 전력 간의 연관성을 제거한다. 하지만, 최근 설계 회로 규모 확장에 따른 semi-custom 디자인 방식의 적용이 불가피하게 되었고, 이러한 디자인 방식은 불균형적인 설계 패턴을 야기하여 DRP로직이 균형적인 전력을 소비하지 않는 문제점을 발생하도록 하였다. 이러한 불균형적인 전력 소비는 전력 분석 공격에 취약점이 된다. 본 논문에서는 이러한 불균형적인 전력 소비 패턴을 제거하기 위하여 양쪽 출력 노드를 동시에 discharge 시켜주는 동작을 추가한 DyCML로직 기반의 새로운 로직을 개발하였다. 본 논문에서는 또한 제안 기법의 성능을 증명하기 위해 1bit fulladder를 구성하여 기존 로직과의 성능을 비교하였다. 제안 로직은 전력 소비량의 균형성을 판단하는 지표인 NED와 NSD값에 대해 최대 60%이상 성능 향상이 있음이 확인되었으며 전력 소비량 또한 다른 로직에 비하여 최대 55%정도 감소하는 것으로 확인되었다.

ABSTRACT

Since power analysis attack which uses a characteristic that power consumed by crypto device depends on processed data has been proposed, many logics that can block these correlation originally have been developed. DRP logic has been adopted by most of logics maintains power consumption balanced and reduces correlation between processed data and power consumption. However, semi-custom design is necessary because recently design circuits become more complex than before. This design method causes unbalanced design pattern that makes DRP logic consumes unbalanced power consumption which is vulnerable to power analysis attack. In this paper, we have developed new logic style which adds another discharge phase to discharge two output nodes at the same time based on DyCML to remove this unbalanced power consumption. Also, we simulated 1bit fulladder to compare proposed logic with other logics to prove improved performance. As a result, proposed logic is improved NED and NSD to 60% and power consumption reduces about 55% than any other logics.

Keywords: Side Channel Attack, Countermeasure, semi-custom design, DyCML

접수일(2011년 1월 28일), 수정일(2011년 4월 26일), 게재확정일(2011년 5월 26일)
* 본 연구는 지식경제부 및 정보통신산업진흥원의 "대학 IT 연구센터 육성, 지원사업"의 연구결과로 수행되었음 (NIPA-2011-C1090-1001-0004)
† 주저자, hmkim8099@cist.korea.ac.kr
‡ 교신저자, hsh@cist.korea.ac.kr

I. 서 론

부채널 공격(side channel attack)은 암호 알고리즘의 구현 시 고려하지 않았던 암호화 장비의 누설 정보 (시간, 전력, 전자기파, 소리 등)를 이용해 비밀 정보를 알아내는 공격 방법이다.

부채널 공격 방법 중, 가장 강력한 것으로 알려진 전력 분석 공격[1]은 전력 소비 패턴이 내부적으로 연산되는 데이터와 밀접한 연관성을 갖는 로직(logic)의 성질에 기반 한 것으로 이를 방어하기 위한 다양한 대응기법(countermeasure)들이 제안되어져 왔다. 하지만, 기존의 대응기법들은 주로 알고리즘적인 대응기법들로 하드웨어 구현 시 구현환경이나 노이즈 등으로 인해 예상치 못한 취약점들이 많이 발견되어지고 있다. 따라서, 최근에는 하드웨어 구현 시 발생할 수 있는 취약점을 원천적으로 제거하기 위해 트랜지스터 로직 레벨에서의 대응기법이 다양하게 제안되어졌다. 이러한 트랜지스터 로직 레벨의 하드웨어 대응기법은 각 기본게이트를 구성하는 트랜지스터들을 재구성하여 각 게이트의 전력소비가 연산데이터에 독립적으로 나타나도록 로직을 설계하는 방법이다.

트랜지스터 레벨 로직의 대표적인 방법으로는 DRP(Dual-Rail Pre-charge logic) 스타일과 CML(Current Mode Logic) 스타일이 존재한다.

DRP 스타일의 로직은 소비 전력을 항상 일정하게 유지하기 위하여 두 상보대칭형 배선(complementary wire)으로 로직을 구성한다. 이러한 스타일의 로직은 동일한 캐패시턴스 로드를 가졌다는 가정 하에 소비 전력을 일정하게 유지할 수 있으며, 대표적인 로직으로는 DCVSL(Differential Cascade Voltage Switch Logic)[2], SABL(Sense Amplifier Based Logic)[3,4], WDDL(Wave Dynamic Differential Logic)[5], dual-spacer DRP[6]이 있다. Dual-rail 형태로 구성된 이러한 로직들은 출력 값이 항상 양측 출력노드에 쌍으로 존재하게 되어 전체적인 게이트출력에서는 항상 일정한 전력 소비를 하게 된다.

반면, CML 스타일의 로직은 트랜지스터 로직 자체가 항상 일정한 전류를 내부적으로 소모하도록 구성된 방식으로서 full-swing이 아닌 small-swing으로 동작한다. 따라서 이러한 로직 스타일은 기존의 DRP 스타일에 비해 60%이상 저 전력으로 구성이 가능하다. 대표적인 CML 스타일의 로직인 MCML(Mos Current Mode Logic)[7,8,9,10,11]은 여러 논문에서 부채널 기능에 대한 검증이 이루어졌지만, precharge 구간에서 pmos 대신에 풀업저항을 사용해야하며 이로 인해 상당한 비용이 소비되는 단점을 가진다. 또한, 한 개의 게이트 트랜지스터의 동작으로 인해 접지로 전류가 흐르기 때문에 정적 소모 전류가 많아 실제로 하드웨어 모듈로 구현하기 어렵다고 알려져 있다[12]. 따라서, 이러한 정적 소모 전류의 문제를 해결하기 위해 DyCML(Dynamic Current Mode Logic)[13,14,15,16] 같은 동적 전류 모드 로직의 사용이 대안으로 제시되어지고 있다.

최근, 빠르게 변화하는 기술흐름에서 실제로 새로운 기술을 기존의 회로에 쉽게 적용하고 대량으로 빠른 시간에 제작할 수 있는 semi-custom 디자인 방식이 일반화되고 있다. 하지만 위에서 살펴본 기존의 DRP, CML 스타일 로직들은 full-custom 디자인 환경에서 고려되어진 방식으로서 semi-custom 디자인 방식의 적용 시 자동배선으로 인해 노드불균형을 초래한다. 이러한 노드불균형은 전력 분석 공격에 취약점이 되며 따라서 암호학적인 측면에서 기존의 로직들의 노드 불균형에 대한 새로운 검증이 필요해졌다. 비록, back annotation작업이나 fat layout[17]을 이용해 디자인 후 대칭적으로 rail을 분리하는 방법 등이 개발되었지만, 회로 디자인 후 추가 작업이 필요하거나, 특별한 툴을 이용해야 하는 단점이 여전히 존재한다. 이러한 semi-custom 디자인에서의 노드불균형을 해결하기 위하여 DRP 스타일에 기반한 TDPL(Three-phase Dual-rail Precharge Logic)이 제안되어졌다[18].

TDPL은 기존의 DRP 스타일에 매 클럭 마지막에 추가로 각 노드에 남아 있는 전류를 discharge 시켜주는 기능을 추가한다. 이러한 기능 추가는 한 클럭 동안 전체 로직의 전력 소비를 일정하도록 만들어 노드 불균형에 대한 문제를 해결해 주었다. 하지만, 소형화된 전자기기와 스마트카드의 사용이 늘어나면서, 저 전력 회로 구성이 필수적인 요소가 되어가고 있는 요즘 TDPL은 기존 DRP 스타일 로직 대비 2배정도의 전력을 더 소모하는 것으로 알려졌고 이로 인해 암호학적 고려 이전에 사용상에 많은 제약을 받고 있다.

본 논문에서는 TDPL에서 사용한 3상(three phase) 디자인 기법을 저 전력 회로를 구성할 수 있는 DyCML에 적용하여 불균형적인 캐패시턴스 로드 상태에 덜 민감한 향상된 로직을 제안하였다. 즉, 상보 대칭형의 배선에 대한 추가적인 제약 없이 semi-custom 디자인 방식을 선택할 수 있고, 소형 전자기기 및 스마트카드에 실제적으로 이용 가능한 로

직을 제안한다.

제안 기법은 DyCML에 discharge 단계를 추가적으로 구성하여 최종적으로 양측 출력 노드의 전류를 discharge 하여 줌으로 인해서, 어떠한 요인에 인해서 발생할 수 있는 노드 불균형에도 항상 일정한 에너지 소비를 할 수 있도록 구성되었다. 이 로직은 비록 몇 개의 트랜지스터가 추가되어 전체적인 구성면적은 기존의 DyCML에 비해 증가하지만, 풀업 저항을 연결하여 구성하는 MCML에 비해서는 효율적이다. 또한, 자동배선 후의 불균형으로 인해 나타나는 전력 소비차이를 크게 줄일 수 있어서, 부채널 공격에 대한 대응기법 측면에서도 기존 로직들에 비하여 기능이 향상되었다.

제안한 로직의 성능 검증을 위해 semi-custom 디자인 후의 노드 불균형을 가정하고 각 게이트 출력에 불균형적인 노드 캐패시턴스를 삽입하여, 기존 로직들과 제안한 로직에 대하여 기본게이트들에 대한 전력 소비를 측정하였다. 또한, 실제 하드웨어 구현 시 동일한 결과를 얻을 수 있는지 확인하기 위해 1bit fulladder를 설계하여 가능한 64가지 입력 값의 변화에 대한 시뮬레이션을 수행하였다. 이 1bit fulladder를 실험을 통해 본 논문에서 제안한 로직이 기존의 로직들에 비해서 최대 60%이상 NED(Normalized Energy Deviation)와 NSD(Normalized Standard Deviation)가 향상됨을 보였다. 전력소모량 측면에서도 역시 최대 55%까지 줄일 수 있음을 검증하였다. 즉, 제안된 로직이 기존 로직들에 비해 저 전력으로 구현 가능한 향상된 하드웨어 대응기법임을 증명하였다.

본 논문에서 중점을 두고 분석한 균형적인 전력소비와 저 전력 문제이외에도 반도체 공정조건이 줄어들면서 암호모듈에 영향을 줄 수 있는 process variation에 대한 관심도 증가하고 있다. 최근 [19]의 논문에서는 scCMOS와 SABL에 대한 process variation의 영향을 분석하였다. 하지만, process variation에 대한 영향은 본 논문의 연구범위를 벗어나기 때문에 본 논문에서는 고려하지 않았다.

본 논문의 구성은 다음과 같다. 2절에서는 관련된 연구에 대한 소개로 DRP 스타일 로직(SABL, TDPL)과 CML 스타일 로직(MCML, DyCML)의 특징을 간단히 설명하였고, 3절에서는 제안된 로직에 대한 설명과 동작특성을 설명하였다. 4절에서는 실험결과를 토대로 기존의 4가지 로직에 대한 기본 게이트들의 성능을 비교하였고, case study로 1bit fulladder를 구성하여 제안된 로직의 향상된 성능을 증명하였다. 마지막으로 5절에서는 결론을 맺고 있다.

II. 기존의 하드웨어 로직 대응기법

2.1 DRP 스타일 로직

가장 기본적인 로직인 scCMOS(Static Complementary CMOS logic)은 스탠다드 셀을 이용하여 쉽게 구현이 가능하여 하드웨어 구현 시 가장 많이 사용하는 로직이다. 하지만, 암호학적 측면에서는 scCMOS로 구현한 암호모듈의 경우 입력 값의 변화에 따라 출력 값의 변화가 일어나고 그 변화에 따라 모듈의 전력 소비량이 변화하게 된다. 따라서, 이러한 전력 소비정보를 이용하여 전력 분석 공격을 하게 되면, 쉽게 비밀 키를 알아낼 수 있는 취약점을 가지고 있다. 이러한 취약점을 극복하기 위해 소비 전력을 항상 일정하게 유지하도록 상보 대칭형 배선을 사용하는 DRP 스타일의 SABL이 소개되었다.

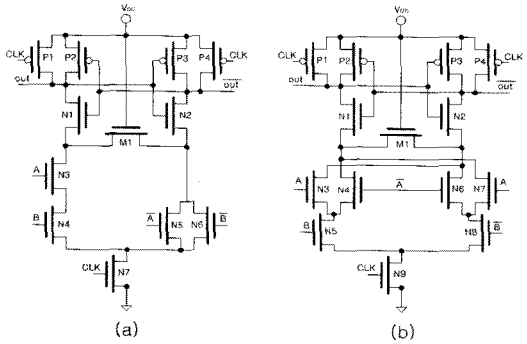
SABL은 게이트 출력 값의 로직을 평가할 때 입력 값에 상관없이 에너지 소비량을 일정하게 유지하게 하여 전력 분석 공격이 어렵게 구현하였다. 하지만, 이 로직 스타일은 full-custom 방식에서는 일정한 에너지가 소비되게 유지할 수 있지만, semi-custom 방식으로 암호 모듈을 구성할 경우 자동적으로 설계되는 레이아웃으로 인하여 에너지 소비량의 불균형이 발생하게 된다. 이러한 semi-custom 설계 시 발생할 수 있는 문제를 해결하기 위하여 TDPL이 제안되었다.

이 TDPL은 SABL의 매 클럭의 마지막에 추가적으로 양측 노드에 남아 있는 에너지를 discharge 시켜줌으로써 매 클럭 소비되는 전력량을 동일하게 만들어 준다. 하지만, TDPL도 추가적인 discharge 모드의 트랜지스터들로 인하여 에너지 소모가 큰 단점이 있다.

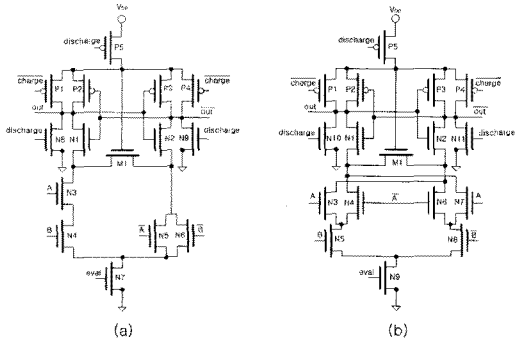
2.1.1 SABL

SABL은 DRP 스타일로 구성이 되어, precharge/evaluation 동작이 클럭 신호에 의해서 일정하게 발생하고, 양측 출력 노드를 연결하는 트랜지스터로 인하여 입력 값에 상관없이 일정한 에너지를 소비하도록 개발된 하드웨어 대응기법이다.

간단히 SABL의 동작을 설명하면, precharge 모드에서 low 클럭이 들어 왔을 때 out과 $\overline{out}$의 출력



〔그림 1〕 SABL의 NAND/AND gate(a)와 XOR/XNOR gate(b)



〔그림 2〕 TDPL의 NAND/AND gate(a)와 XOR/XNOR gete(b)

노드에 에너지가 charge 되게 된다. 또한 high 클럭이 들어 올 때 evaluation 모드가 동작하여 입력 값에 따라 In(A, B) 또는 $\overline{In}(\overline{A}, \overline{B})$가 on이 되어 그 노드를 통해 out 또는 $\overline{out}$에 charge된 전류가 discharge 되지만, SABL은 중간에 삽입된 M1 트랜지스터에 의하여 입력 값에 상관없이 out과 $\overline{out}$에 충전된 전류가 동시에 discharge 되게 구성되어 있다.

〔그림 1〕은 SABL의 NAND/AND 및 XOR/XNOR 게이트의 그림이다.

로직 설계 방식이 full-custom 방식에서 semi-custom 방식으로 변화되어가면서, HDL 디자인 후 자동배선 방식으로 실제 게이트를 설계하게 되었다. 이렇게 자동배선으로 설계를 하게 되면 out과 out의 캐패시턴스 로드에 차이가 발생하게 되어 SABL의 가장 큰 장점이었던, 매 클럭 당 동일한 전력 소비량을 얻을 수 없게 된다.

2.1.2 TDPL

일반적으로 semi-custom 설계 후 자동레이아웃을 하면, 대칭적으로 설계된 로직이라 할지라도 양측 출력 노드의 캐패시턴스의 크기가 서로 달라진다. 이러한 출력 캐패시턴스들의 불균형은 결국 입력 값에 따라 매 클럭마다 다른 전력 소비량을 나타나게 한다.

TDPL은 SABL의 semi-custom 설계 시 발생하는 out과 $\overline{out}$의 캐패시턴스 로드의 불균형으로 인해 전력분석 공격에 취약해지는 문제를 해결하기 위하여 개발된 로직이다.

이 로직은 출력 캐패시턴스의 불균형으로 인한 evaluation 후의 양측 출력노드에 남아있는 에너지를 추가적으로 discharge 모드를 삽입하여 동시에 최종적으로 discharge 해 준다.

〔그림 2〕는 TDPL의 NAND/AND 및 XOR/XNOR 게이트의 그림이다.

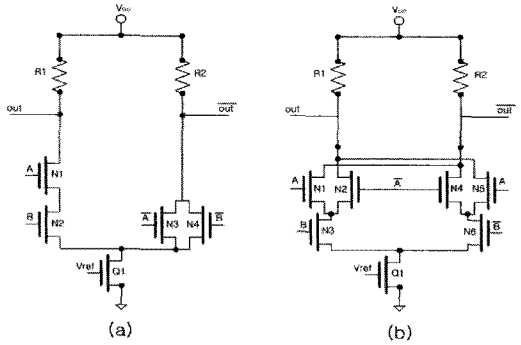
간단히 TDPL의 동작을 설명하면, 전체 동작은 3가지 모드(precharge, evaluation, discharge)로 구성되어진다. precharge 모드에서는 각 출력노드에 전류가 동시에 충전되어지고 evaluation 모드에서는 입력 값에 따라 out 또는 $\overline{out}$가 discharge 되어 진다. 하지만, 항상 에너지 소비량을 동일하게 만들어 주기 위해서 매 클럭의 마지막에 discharge 모드를 추가하여 동시에 출력 노드의 에너지를 discharge 시켜준다. 이렇게 동시에 최종적으로 discharge 시켜주는 부분을 추가함으로써 입력 값에 상관없이 매 클럭마다 항상 일정한 에너지 값을 소비하게 된다.

하지만, 이 TDPL의 경우 discharge 모드의 동작을 위해 추가된 1개의 pmos와 2개의 nmos의 동작은 전체 전력 소모 측면에서 기존의 SABL등의 로직에 비해 50%이상 더 많은 전력 소비를 하게 되어 저전력 회로로 구성되는 소형 전자기기나 스마트카드 등에는 실용적이지 못한 방법이다.

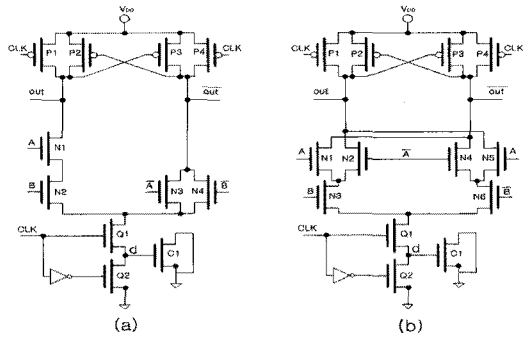
2.2 CML 스타일 로직

다양한 소형 전자기기가 생활화되면서 저 전력 회로의 필요성이 많이 대두되어지고 있다. 특히 CML스타일 로직은 회로의 각 노드의 전압 값이 V_{DD}에서 V_{SS}값으로 변하는 full swing 형태로 동작하지 않고 보다 적은 전압에서 노드출력의 상대적인 전압 값의 비교로 논리 값 1/0을 판단하는 small swing 형태로 동작한다. 이러한 small swing 형태의 동작으로 인해 보다 저 전력으로 회로를 구현할 수 있다.

또한, 암호학적인 측면에서는 항상 일정한 전류가



〔그림 3〕 MCML의 NAND/AND gate(a)와 XOR/XNOR gate(b)



〔그림 4〕 DyCML의 NAND/AND gate(a)와 XOR/XNOR gate(b)

접지를 통해 흘러 나가므로 입력 값의 변화에 관계없이 균형적인 에너지 소비가 가능하게 만들어준다. 따라서, 이러한 전류 모드 로직을 이용한 다양한 전력 분석 공격 대응기법들이 제안되어졌고 실험적으로 그 안전성이 검증되어졌다.

2.2.1 MCML

MCML은 대표적인 전류 모드 로직이다. 전류 모드 로직은 항상 트랜지스터 Q1에 일정한 전류가 흘러서 회로 전체적으로 소모되는 에너지양을 균일하게 만들어주는 로직이다.

〔그림 3〕은 MCML의 NAND/AND 및 XOR/XNOR 게이트의 그림이다.

하지만, MCML은 가장 대표적인 전류 모드 로직임에도 불구하고, 풀업저항을 연결하여 전원이 공급되어지는 동안에 항상 양측 출력노드에 전류가 충전되므로 많은 정적 전류를 소모하게 된다. 실질적으로도 양측 노드의 균형적인 출력 캐패시턴스를 유지하고 적당한 전압 값을 출력 노드에 전달해 주기 위해 풀업 저항 값을 조절해 가며 맞추어 주어야 하므로 하드웨어 모듈구현이 어렵다는 문제점을 가지고 있다.

2.2.2 DyCML

DyCML은 MCML의 과다한 정적 전류 소비문제를 해결하기 위하여 동적으로 전류 모드를 구현한 로직이다. 이 로직은 MCML의 〔그림 3〕의 트랜지스터 Q1에 항상 일정한 전류가 흘러서 발생하게 되는 정적 전류를 감소시키기 위하여, 이 부분을 동적으로 구성하였다. 즉, 〔그림 4〕의 트랜지스터 Q1과 Q2를 클럭 신호를 이용해 각각 동작하게 하여 동시에 on이 되어 소모되는 정적 전류를 최소화하였다.

〔그림 4〕는 DyCML의 NAND/AND 및 XOR/XNOR 게이트의 그림이다.

DyCML의 동작을 간단히 설명하면, 클럭 신호가 low 일 때, 양 측 출력 노드는 각각 charge 되어 진다. 클럭 신호가 high가 되었을 때, 양측 출력 노드의 에너지가 입력 값에 따라 트랜지스터가 on이 되는 rail을 따라 discharge 되고, 〔그림 4〕의 트랜지스터 Q1이 on이 되어 트랜지스터 Q1과 Q2사이의 노드 d에 에너지가 charge 되어 진다. 이 에너지 값이 트랜지스터 C1의 threshold 전압 이상이 되면, 트랜지스터 C1이 on이 되어 이 노드 d에 charge 되어 있던 에너지가 discharge 되어 접지로 흘러나가게 된다. 또한, discharge 가 되는 중 노드 d의 전압 값이 캐패시턴스 C1의 threshold 전압 이하로 떨어지면 C1은 off 되어 더 이상의 discharge가 일어나지 않게 된다. 즉, 매 클럭 동안 노드 d에 연결된 트랜지스터 C1이 가상 캐패시턴스 역할을 해서 트랜지스터 C1의 크기에 따라 노드 d에 charge 되고, discharge 되는 에너지양이 변하게 된다. 이러한 가상 캐패시턴스 C1에 의해서 전체 로직의 출력 전압이 V_{DD}에서 V_{DD}-V_{th}사이에서 변하는 small swing 동작을 하게 된다. 따라서 small swing은 저 전력으로 회로 구성이 가능하게 만들어 준다.

비용 면에 있어서 추가적으로 구성되는 트랜지스터들은 기존의 논문들에서 언급되어진 것처럼 MCML에 사용되는 풀업 저항에 비하여 효율적이어서 실제 암호 모듈에 사용되어 질 수 있다.

하지만, 이 DyCML도 기존의 로직들과 마찬가지로 semi-custom 방식으로 설계되는 환경에서 발생할 수 있는 노드 불균형에 관한 연구는 아직 진행되지 않았다.

III. 제안하는 3상 동적 전류 모드 로직 스타일

본 논문에서는 semi-custom 설계에서 저 전력, 고 성능의 DyCML로 회로를 구성 시 환경적인 요인이나 자동배선으로 인해 노드 캐패시턴스의 불균형과 입력 값에 따른 에너지 소비량의 변화가 발생하는 취약점을 극복하기 위해 3상 전류 모드 로직을 제안한다.

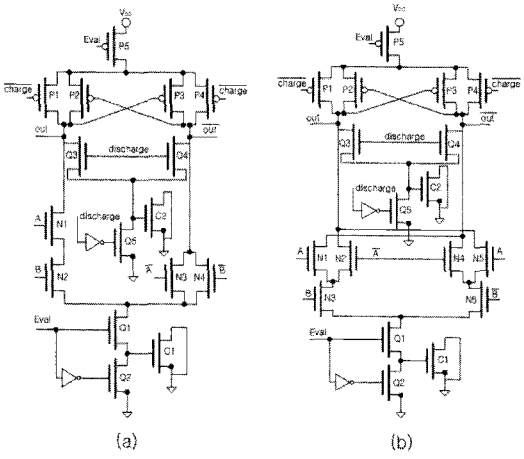
이러한 취약점을 극복하기 위해 제안 기법은 TDPL에서 이용한 3상 모드 기법을 이용하여 구현하였으며 전력 소비가 기존 전력 분석 대응 기법에 비해 적고 전력 분석 공격에 대한 대응기법으로써의 성능도 더 좋다는 장점을 가진다.

〔그림 5〕는 제안하는 3상 동적 전류 모드 로직 TPDyCML(three phase dynamic current mode logic)을 이용한 NAND/AND 및 XOR/XNOR 게이트이다.

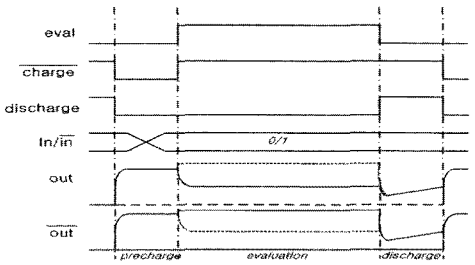
TPDyCML의 동작을 설명하면, 매 클럭마다 pre-charge/evaluation/discharge의 3가지 모드로 동작을 한다.

〔그림 6〕은 TPDyCML의 한 클럭 동안의 동작을 나타낸 timing diagram이다.

첫 번째 모드인 precharge 모드에서 $\overline{charge}$ 신호가 low 일 때 〔그림 5〕의 트랜지스터 P1과 P4가 on이 되어 양 출력 노드에 에너지가 charge 되어 진다. 물론 이때 전원 단에 연결된 게이트 트랜지스터가 on(eval=low)되어 각 노드로 전류가 흐르게 된다. 두 번째 모드인 evaluation 모드에서는 실제로 출력



〔그림 5〕 TPDyCML의 NAND/AND gate(a)와 XOR/XNOR gate(b)



〔그림 6〕 TPDyCML의 timing diagram

의 논리 값이 결정된다. 이 모드에서는 입력 값에 따라 dual rail로 구성된 로직의 한쪽 rail로 출력 노드에 charge 되었던 에너지가 discharge 되게 된다. 이 discharge 된 에너지는 동적 전류 모드로 구성된 〔그림 5〕의 Q1 트랜지스터와 Q2 트랜지스터 사이의 노드까지 흐르게 된다. 이 노드의 전압 값이 가상 캐패시턴스를 구성한 C1 트랜지스터의 threshold 전압 이상이면 C1이 on되어 노드의 에너지가 discharge 되게 된다. 따라서 입력 전압 값과 C1의 threshold 전압 사이의 값으로 small swing이 일어나면서 동작하게 된다. 마지막 단계인 discharge 모드에서는 노드 불균형으로 인한 양측 출력노드에 불균형적으로 남아있는 에너지를 추가적으로 트랜지스터 C2의 게이트에 연결된 노드에 charge 하게 된다. C2도 C1과 같은 크기의 트랜지스터로 구성되어 같은 양의 small swing이 발생하게 된다. 이처럼, 최종적으로 양 출력 노드에 남아있는 에너지를 한 번 더 discharge 함으로 인해 전체적으로 한 클럭 동안에 소모되는 에너지의 양을 일정하게 유지시켜 줄 수 있다.

이 로직을 구현 시 가상 캐패시턴스를 구현하는 〔그림 5〕의 트랜지스터 C1과 C2 트랜지스터의 크기를 조절하여 small swing의 크기를 정하여 준다. 즉, 트랜지스터 C1과 C2의 크기에 따라 각각의 트랜지스터의 threshold 전압이 달라지고, small swing의 크기 범위인 V_{DD}-V_{TH} 값이 달라지게 되어 small swing의 크기를 조절할 수 있다.

IV. 실험 결과 및 분석

실제 TPDyCML을 암호 모듈로 구현 시 정상적인 동작을 하는지 알아보기 위하여, 본 절에서는 각 게이트들에 대한 DUT testbench 회로를 구성하여, 각 논리 게이트의 특성을 기존의 로직들과 비교, 분석하였다. 또한, case study로 각각의 로직들로 1bit

fulladder를 구현하여 제안한 로직이 다른 로직들에 비해 효율적인지 검증하였다. 실험은 1.5V 공급 전압과 200MHz로 동작주파수로 구동하였으며, UMC 0.13㎛ 공정의 BSIM3v3 트랜지스터 모델을 이용하여 HSPICE로 시뮬레이션 하였다. 1bit fulladder에 사용된 트랜지스터는 모두 w=2㎛, l=120㎚로 동일하게 구현하였다.

4.1 DUT

Semi-custom 디자인 후의 불균형적인 캐패시턴스 로드가 발생한 환경을 만들어 주기위하여 논문[18]의 DUT testbench circuit을 동일하게 적용하여 실험하였다.

[그림 7]은 각 게이트들을 테스트하기 위하여 사용한 DUT testbench circuit이고, [표 1]은 각 출력 노드에 연결한 캐패시턴스의 값을 나타내었다.

[그림 7]의 입력단의 인버터는 실제 암호모듈을 구현했을 경우의 이상적인 입력 값이 아닌 실제적인 입력 값과 가까운 값을 만들기 위하여 연결하였다. 이 testbench circuit을 이용해 모든 입력 값의 경우에 대하여 각 게이트들의 소비 전류량을 구하고, 이 소비 전류량을 다음 식(1)에 적용하여 한 클럭 동안의 각 게이트 출력에서의 에너지 값을 구하였다.

$$E = V_{DD}\int_0^T I_{DD}(t)dt \tag{1}$$

모든 입력 값의 변화에 대한 에너지 소모량의 변화를 알아보기 위하여 기존의 로직들에서 부채널 공격에 대한 대응지수 평가를 위해 사용하였던 NED와 NSD 값을 사용하였다[3,18]. 또한, NED와 NSD 값을 구하기 위하여 최소전력(min(E)), 최대전력(max(E)), 평균전력($\overline{E}$), 소비전력의 분산 값(σ_E)을 각각 실험을 통해 구하였다. 식 (2)와 (3)은 NED와 NSD를 계산하기 위한 수식이다.

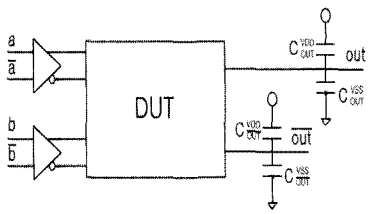
$$NED = \frac{(\max(E) - \min(E))}{\max(E)} \tag{2}$$

$$NSD = \frac{\sigma_E}{\overline{E}} \tag{3}$$

[표 2]는 [그림 7]의 DUT testbench circuit을 통해 얻은 기본 게이트들에 대한 시뮬레이션 결과를 나타낸다.

각 게이트들에 대한 시뮬레이션 결과 본 논문에서 제안한 TPDyCML이 같은 CML 스타일 로직인 DyCML에 비하여 전력 소모량이 50%이상 증가하였지만, SABL과 TDPL 같은 DRP 스타일 로직에 비하여 전력 소모량이 최대 35% 가까이 감소하였다.

하드웨어 대응기법 측면에서는 TPDyCML이 NAND/AND gate의 경우 NED와 NSD값이 2.9%, 0.8%로 TDPL의 2.9%, 0.7%와 비슷하였지만, 같은 CML 스타일 로직인 DyCML에 비하여 NED와 NSD값이 70%이상 향상되었음을 확인 할 수 있었다. 이와 같이 TPDyCML은 각 게이트들에서의 전력 소모량은 DRP 스타일 로직인 SABL과



[그림 7] DUT testbench circuit

[표 1] Capacitive loads

	to V_{DD}	to V_{SS}
from out	Cout = 6fF	Cout = 4fF
from $\overline{out}$	$\overline{Cout}$ = 1fF	$\overline{Cout}$ = 3fF

[표 2] 기본 게이트들에 대한 시뮬레이션 결과

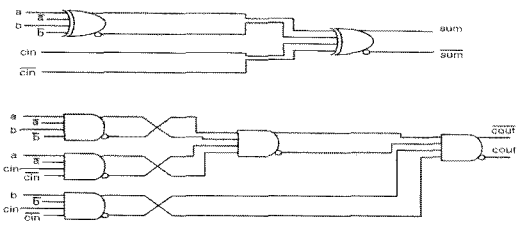
NAND/AND				
logics	SABL	TDPL	DyCML	TPDyCML
min(E) [fJ]	40.27	67.52	17.36	43.19
max(E) [fJ]	54.51	69.38	19.21	44.5
NED [%]	26	2.9	9.6	2.9
$\overline{E}$ [fJ]	44.51	68.72	18.37	43.78
σ_E	5.25	0.5	0.55	0.35
NSD [%]	12	0.7	3	0.8
XOR/XNOR				
logics	SABL	TDPL	DyCML	TPDyCML
min(E) [fJ]	46.93	74.13	17.37	42.46
max(E) [fJ]	61.05	74.53	18.55	42.97
NED [%]	2.3	0.5	6.3	1.2
$\overline{E}$ [fJ]	53.95	74.33	17.9	42.72
σ_E	6.43	0.15	0.45	0.24
NSD [%]	12	0.2	2.5	0.6

TDPL에 비해 감소하고, 하드웨어 대응기법으로써의 성능은 같은 CML 스타일 로직인 DyCML에 비하여 향상되었다. 따라서 본 논문에서 제안한 TPDyCML이 이전의 로직들과는 달리 전력 소모량과 암호학적 성능 모두 효율적인 새로운 하드웨어 대응기법임을 알 수 있었다.

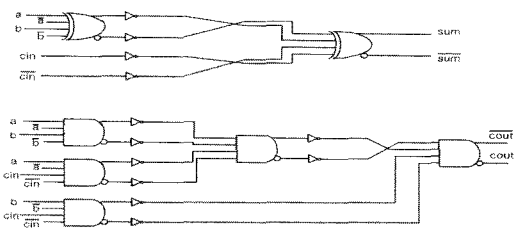
4.2 Case Study

본 논문에서 제안한 TPDyCML 로직의 성능을 검증하기 위하여 [18]에서 적용한 1bit fulladder를 이용하여 DRP스타일 로직과 CML스타일 로직으로 각각 구현하였다. 구현 결과는 [그림 8]와 [그림 9]과 같다.

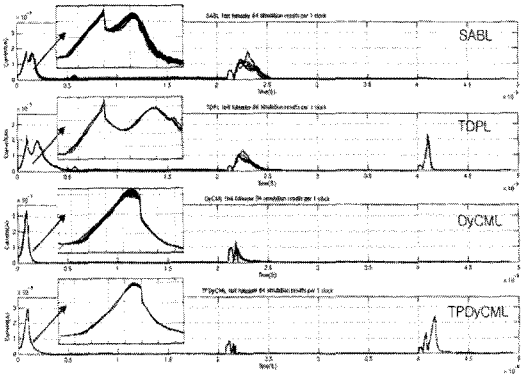
하지만, DRP 스타일 로직과 달리 CML스타일 로직은 각 기본 게이트들을 연결할 경우, 게이트 사이의 static inverter는 연결할 필요가 없다. 왜냐하면, 일반적인 디지털 회로에서 full swing으로 동작하는 기본 게이트들을 연결할 경우 이전 게이트의 입력 값을 static inverter를 연결하여 다음 게이트로 신호를 보내기 전에 완전한 논리 값 0 or 1로 신호 값을 보상해 주게 된다. 이러한 것을 domino rule이나 nora rule이라고 한다. 하지만, CML스타일 로직은 small swing으로 동작하므로 static inverter를 연결하여 domino rule이나 nora rule로 값을 보상할 필요가 없다. 따라서, SABL과 TDPL의 경우는 게이트 출력 단에 inverter를 연결하여 구성한 [그림 8]와 같은 1bit fulladder로 실험 검증하였고, DyCML과 TPDyCML은 [그림 9]과 같이 1bit fulladder를 구성하여 실험을 하여 검증하였다. 중간에 삽입된 static inverter가 전체 에너지 소모량에 미치는 영향이 거의 미비함을 [18]에서 언급하였다. 또한, DUT testbench에서 일정한 노드 불균형을 주기 위하여 추가하였던 캐패시턴스를 각 게이트 출력 부분에 각각 모두 연결하여서 일정한 노드 불균형을 준 1bit fulladder들을 구성하였다.



[그림 8] DyCML과 TPDyCML의 1bit fulladder



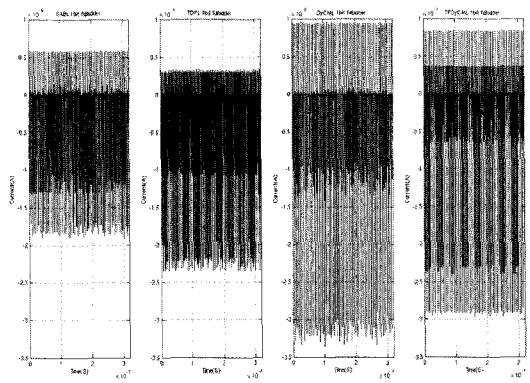
[그림 9] SABL과 TDPL의 1bit fulladder



[그림 10] SABL, TDPL, DyCML, TPDyCML의 매 클럭 당 전류 소비 파형 중첩 그래프

4.3 실험 결과

[그림 10]은 [그림 8]과 [그림 9]에서 구현한 4가지 로직 각각의 1bit fulladder에서 입력 값(a, b, cin)의 모든 64가지 변화의 경우에 대하여 실험한 후 매 클럭 당 소비 전류의 파형을 중첩하여 나타내었다. 이 [그림 10]에서 보는 바와 같이 TPDyCML이 다



[그림 11] SABL, TDPL, DyCML, TPDyCML의 1bit fulladder에 대한 power consumption graphs

〔표 3〕 1bit fulladder에 대한 시뮬레이션 결과

	1bit fulladder			
logics	SABL	TDPL	DyCML	TPDyCML
mix(E) [fJ]	426.1	718..9	133.2	316.3
max(E) [fJ]	500.5	737.2	140.2	320.6
NED [%]	14.87	2.48	4.99	1.34
$\overline{E}$ [fJ]	459.02	727.95	136.40	318.60
σ_E	20.07	6.78	1.43	0.85
NSD [%]	4.37	0.93	1.05	0.27

른 로직에 비하여 한 파형으로 중첩되어 입력 값에 상관없이 균형적인 전류를 소비하는 것을 알 수 있다.

〔그림 11〕은 64가지 모든 입력 값(a, b, cin)의 변화에 대한 1bit fulladder의 전체적인 전력 소비량을 나타낸 그래프이다. 이 그래프에서 확인할 수 있듯이 precharge 구간(중간의 진한선)과 discharge 구간(바깥의 엷은선)이 다른 로직들이 위, 아래로 굴곡이 있는 반면에 본 논문에서 제안한 TPDyCML의 경우 거의 직선 형태로 균일한 전력 소비량을 보임을 확인 할 수 있다.

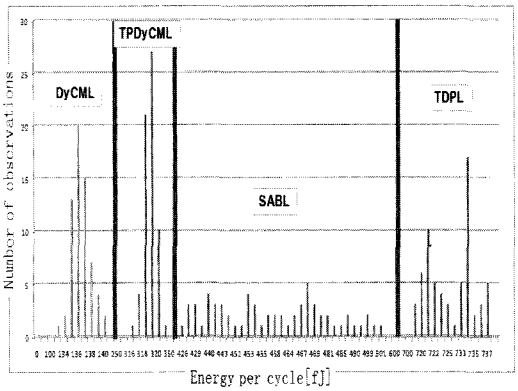
〔표 3〕은 1bit fulladder에 대한 각 로직 별 시뮬레이션 결과를 나타내었다.

〔표 3〕에서 보는바와 같이 1bit fulladder를 구성하여 실험한 결과 CML 스타일 로직을 이용한 회로가 DRP 스타일 로직에 비하여 전력 소모 측면에서 효율성이 있음을 알 수 있고, 비록 제안한 로직이 DyCML에 비하여 전력 소비가 늘어나지만, 다른 DRP 스타일 로직에 비하여 최대 55% 절감 될 수 있다는 것을 확인 할 수 있었다.

전력 분석 대응기법으로써의 효용성을 확인하기 위해 NED와 NSD를 비교한 결과 본 논문에서 제안한 TPDyCML이 SABL과 DyCML에 비해 60%이상 NED와 NSD가 향상 되었으며, 노드 불균형을 개선한 TDPL에 비해서도 30%이상 향상된 것을 알 수 있었다. 〔그림 12〕는 시뮬레이션 결과에 대한 그래프로 제안한 TPDyCML이 전체적인 시뮬레이션 동안 다른 로직들에 비하여 균형적인 에너지 소비량을 나타냄을 확인 보여주고 있다.

V. 결 론

하드웨어 대응기법으로 개발된 많은 로직들도 semi-custom 방식으로 디자인 시 발생할 수 있는 출력 캐패시턴스의 불균형으로 인해 매 클럭 당 전력 소비의 불균형이 발생하게 된다. 이러한 전력 소비의



〔그림 12〕 1bit fulladder simulation results(SABL, TDPL, DyCML, TPDyCML)

불균형은 입력 값과 전력량과의 관련성을 증대시켜 하드웨어 대응기법으로 개발된 로직을 전력 분석 공격에 취약하게 만들게 된다.

본 논문에서는 3상 동적 전류 모드 로직을 이용하여 전력 소비의 불균형을 효과적으로 개선하였다. 이전의 로직들은 back annotation과 같은 회로 설계 후의 추가적인 작업을 통해 전력 소비의 불균형을 유발하는 출력 캐패시턴스의 불균형을 보정하였다. 하지만, 본 논문에서 제안한 TPDyCML은 이러한 추가적인 작업 없이도 매 클럭마다 일정한 에너지를 소비하는 전력 분석 공격에 강한 하드웨어 대응기법이다.

본 논문에서는 각 게이트들과 1bit fulladder를 구현한 case study를 통해 전력 소비 측면에서는 다른 로직들에 비해 최대 55% 절감되고, 전력의 균형 소비량을 검증하는 NED와 NSD값은 최대 60%이상 향상됨을 검증하였다.

본 논문에서 제안한 TPDyCML의 이러한 저 전력과 균형적인 전력 소비의 특성으로 인하여 모바일 전자기기나 스마트카드 같은 암호장비에 실제적으로 응용 가능한 전력 분석 공격에 안전한 하드웨어 대응기법이라 할 수 있겠다.

참고문헌

〔1〕 P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," CRYPTO'99, LNCS, vol. 1666, pp. 388-397, August 1999.
〔2〕 J. Rabaey, Digital Integrated Circuits: A design perspective, Prentice Hall, 1996.
〔3〕 K. Tiri, M. Akmal, and I. Verbauwhede,

"A dynamic and differential cmos logic with signal independent power consumption to withstand differential power analysis on smart cards," ESSCIRC'02, pp. 403-406, September 2002.

[4] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," DATE'04, pp. 246-251, February 2004.

[5] S. Guilley, L. Sauvage, P. Hoogvorst, R. Pacalet, G.M. Bertoni, and S. Chaudhuri, "security evaluation of WDDL and SecLib countermeasures against power attacks," IEEE Transactions on Computers, vol. 57, no. 11, pp. 1482-1497, November 2008.

[6] D. Sokolov, J. Murphy, A. Bystrov, and A. Yakovlev, "Improving the security of dual-rail circuit," CHES'04, LNCS, vol. 3156, pp. 282-297, August 2004.

[7] M.Yamashina and H.Yamada, "Mos current mode logic MCML circuit for low-power GHz processors," NEC research development, vol 36, no. 1, pp. 54-63, January 1995.

[8] F. Regazzoni, A. Cevrero, F.-X. Standaert, S. Badel, T. Kluter, P. Brisk, Y. Leblebici, and P. Ienne, "A design flow and evaluation framework for DPA-resistant instruction set extensions," CHES'09, LNCS, vol. 5747, pp. 205-219, September 2009.

[9] F. Regazzoni, T. Eisenbarth, A. Poschmann, J. G.soßschädl, F. Gurkaynak, M. Macchetti, Z. Toprak, L. Pozzi, C. Paar, Y. Leblebici, and P. Ienne, "Evaluation resistance of MCML technology to power analysis attacks using a simulation-based methodology," Transactions on Computational Science Ⅳ, LNCS, vol. 5430, pp. 230-243, February 2009.

[10] S. Badel, E. Guleyupoglu, O. Inac, A.P. martinez, P. Vietti, F. Gurkaynak, and Y. Leblebici, "A generic standard cell design methodology for differential circuit styles," DATE'08, pp. 843-848, March 2008.

[11] H. Hassan, M. Anis, and M. Elmasry, "Design and optimization of MOS current mode logic for parameter variations," VLSI journal, vol. 38, pp. 417-437, January 2005.

[12] 송진석, 공정택, 공배선, "저 전력 SoC를 위한 저 누설전류 특성을 갖는 Self-Timed Current-Mode Logic Family," 전자공학회 논문지, 제 45권, SD편, 제 8호, pp. 803-809, August 2008.

[13] M.W. Allam and M. Elmasy, "Dynamic Current Mode Logic(DyCML): A new low-power high-performance logic style," IEEE Journal of Solid-State Circuits, vol 36, no. 3, pp. 550-558, March 2001.

[14] F. Ren and D. Markovic, "True energy-performance analysis of the MTJ-based logic-in-memory architecture(1-Bit Full Adder)," IEEE Transactions on Electron Devices, vol. 57, no. 5, pp. 890-895, May 2010.

[15] F. Mace, F.-X. Standaert, I. Hassoune, J.-D. Legat, and J.-J. Quisquater, "A dynamic current mode logic to counteract power analysis attacks," DCIS'04, pp. 186-191, November 2004.

[16] T. Sundstrom and A. Alvandpour, "A comparative analysis of logic styles for secure IC's against DPA attacks," NORCHIP'05, pp. 297-300, November 2005.

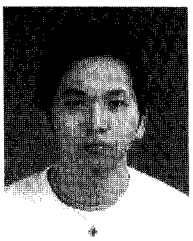
[17] K. Tiri and I. Verbauwhede, "Place and route for secure standard cell design," CARDIS'04, pp. 143-158, August 2004.

[18] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-Phase Dual-Rail Pre-Charge Logic," CHES'06, LNCS, vol. 4249, pp. 232-241, September 2006.

[19] L. Lin and W. Burless, "Analysis and mitigation of process variation impacts on power-analysis tolerance," DAC'09, pp. 238-243, July 2009.

〈著者紹介〉

김 현 민 (Hyunmin Kim) 학생회원
2006년 2월: 동국대학교 전자공학과 졸업(학사)
2005년 12월~2008년 12월: 삼성전자 반도체 총괄 연구원.
2009년 3월~현재: 고려대학교 정보경영공학전문대학원 석사과정
2010년 9월~현재: K.U.Leuven university International Scholar
〈관심분야〉 부채널 공격, 초경량 암호모듈 설계, Secure Logic Design, 보안칩 설계



김 희 석 (HeeSeok Kim) 학생회원
2006년 2월: 연세대학교 수학과 졸업(학사)
2008년 2월: 고려대학교 정보경영공학전문대학원 공학석사
2008년 3월~현재: 고려대학교 정보경영공학전문대학원 박사과정
〈관심분야〉 부채널 공격, 암호시스템 안전성 분석 및 고속구현, 암호칩 설계 기술

홍 석 희 (Seokhie Hong) 종신회원
1995년: 고려대학교 수학과 학사
1997년: 고려대학교 수학과 석사
2001년: 고려대학교 수학과 박사
1999년 8월~2004년 2월: (주) 시큐리티 테크놀로지스 선임연구원
2003년 3월~2004년 2월: 고려대학교 시간강사
2004년 4월~2005년 2월: K.U.Leuven. 박사 후 연구원
2005년 3월~2008년 8월: 고려대학교 정보경영공학전문대학원 조교수
2008년 9월~현재: 고려대학교 정보경영공학전문대학원 부교수
〈관심분야〉 대칭키 암호 알고리즘, 공개키 암호 알고리즘, 포렌식