情 報 保 護 學 會 誌
第 15 卷 第 4 號, 2005. 8

저가의 RFID 태그에 적합한 암호알고리즘 구현 환경에 대한 고찰

장 환 석*, 박 해 룡**, 천 동 현**, 전 길 수**, 송 정 환*

요 약

지금까지 개발된 암호원천기술들이 RFID 태그와 같은 매우 제한된 환경에 맞춰 개발된 사례는 찾기 힘들다. 물론 기존 암호원천기술들이 지향해 온 방향이 초고속화 등에 집중되어 있어, 작은 구현 면적이나 낮은 전력 소비에 맞춰 구현된 시도가 있을 수 있으나, 아직까지는 기존의 알려진 암호원천기술을 RFID 태그와 같은 환경에 적용하기는 어렵다고 보여 진다. 그러므로 현재 활용할 수 있는 태그에 탑재 가능한, 기존 암호원천기술들의 안전성을 유지하며, 경량화되고 저전력을 소비하는 암호원천기술의 개발이 절실히 필요하다. 이를 위한 사전 단계로 본 논문에서는 상업성을 고려한 RFID 태그의 환경에서 보안을 위해 허용되는 구현 면적, 전력 소비량 등과 암호원천기술이 태그에 사용되기 위해 고려되어야 하는 사항들을 도출한다.

Ⅰ. 서 론

물이나 공기처럼 시공을 초월해 '언제 어디에나 존재한다'는 뜻의 라틴어를 어원으로 갖는 '유비쿼터스(Ubiquitous)'는 사용자가 컴퓨터나 네트워크를 의식하지 않고 장소에 상관없이 자유롭게 네트워크에 접속할 수 있는 환경을 말한다. 1988년 Mark Weiser가 '유비쿼터스 컴퓨팅'이라는 용어를 사용하면서 처음으로 등장하였는데, 유비쿼터스 환경이 실현되려면 광대역통신과 컨버전스 기술의 일반화, 정보기술 기기의 저가격화 등 정보기술의 고도화가 전제되어야만 한다. 이러한 제약들로 인해 현재 일반화되어 있지는 않지만, 휴대성과 편의성뿐 아니라 시간과 장소에 구애받지 않고도 네트워크에 접속할 수 있는 장점들 때문에 세계적인 개발 경쟁이 일고 있는 실정이다. 이런 유비쿼터스 환경을 가능하게 해주는 기반구조 중 하나가 USN(Ubiquitous Sensor Network)이다. USN의 개념은 필요한 사물에 전자태그를 부착해 주위 사물의 인식 및 이력정보와 사물을 둘러싸고 변화하는 물리 환경계의 다양한 정보 등을 얻고 네트워크를 통해 실시간 정보를 생성, 구축, 활용토록 하는 것이다. 또한 현재의 인간 중심 정보구축에서 보다 넓은 범위의 사물 중심으로 정보구축을 확대하고 궁극적으로는 광대역망(BcN)과 연계해 유비쿼터스 네트워크로 발전하고자 하는 것이다. 따라서 USN은 전자태그를 통해 단순히 사물을 식별하는 초기 단계에서, 센싱 기능이 첨가되어 환경정보 등을 취득하는 단계, 태그 상호간의 연산 능력과 통신 기능이 추가되어 필요시 Ad-hoc 네트워크를 구축하고 이를 이용해 서로를 제어할 수 있는 단계로까지 발전할 것으로 보인다. 하지만 이런 미래상의 이면에는 해결해야 되는 문제가 있다. 태그가 부착된 모든 기기 및 사물을 통해 정보를 수집·처리하는 과정에서 이들에 대한 보안기술이 확보되지 않을 경우 개인정보 유출 및 프라이버시 문제가 발생할 수 있다는 것이다. 실제로 월마트, 베네통, 질레트사가 RFID 시스템을 도입하려고 하였으나 개인정보 과다 수집 등 프라이버시 침해 논란으로 도입에 차질을 빚기도 하였다.

눈으로 쉽게 확인할 수 없도록 RFID 태그를 부착하거나 RFID 리더가 소형화되고 통신기기에 내장되어, 이들을 통한 개인정보 및 상품정보 등 대량의 데이터 수집이 사용자가 인지하지 못한 채 이루어질 수

* 한양대학교 수학과 (jhs1003@ihanyang.ac.kr, camp123@hanyang.ac.kr)
** 한국정보보호진흥원 암호응용팀 ({hrpark, dhcheon, kschun}@kisa.or.kr)

도 있다. 따라서 태그로부터의 정보가 유출되지 않도록 현재까지 소개된 RSA사의 Bloker Tag기법[1], Auto-ID의 Kill Command 기법[1], MIT의 해쉬-락 기법[2] 등의 보호기술이 반드시 필요하며, 정당한 리더만이 태그 정보를 읽을 수 있도록 하는 태그와 리더간의 상호인증기술이 요구된다. 이런 문제점들을 해결할 수 있는 방법이 암호기술이다. 하지만 기존의 암호기술을 적용하기에는 무리가 따른다. 이는 RFID /USN 시스템이 갖는 특성에 기인하는데, 하부 기반 구조를 구성하는 태그들의 수를 충족하기 위한 태그의 제조 단가가 주된 이유이다. 시스템을 구축하기 위해서는 막대한 양의 태그가 필요하며, 이는 상업적인 측면을 만족시키는 상태에서 태그를 제조하여야 한다는 것을 말한다. 그러므로 현재의 제조 기술 수준에서 제조 단가를 고려하여 태그를 생산하였을 때, 보안을 위해 이용 가능한 하드웨어 사양은 매우 제한적일 수밖에 없다. 일반적으로 받아들여지고 있는 태그 제조 단가는 $0.05 이내로 알려져 있으며, 보안에 할당될 수 있는 게이트(Gate)의 수는 대략 5,000 게이트 이하라고 추정된다.[3] 2002년 CRYPTREC 보고서[4]에 의하면, 일반적인 대칭키 암호알고리즘 구현을 위해서 5,300~18,000 게이트가 소요되는 것을 알 수 있는데, 이는 구현 면적을 최적화하는 것에 목적을 두고 구현된 사례들로 RFID 태그의 하드웨어 환경이 매우 제한적임을 알게 해준다. 표 1은 CRYPTREC 보고서에서 인용한 암호알고리즘의 제조 공정별 게이트 수와 국내 민간암호 표준인 SEED의 제조 공정에 따른 게이트 수를 나타낸 것이다.[16,17]

지금까지 개발된 암호원천기술들이 RFID 태그와 같은 매우 제한된 환경에 맞춰 개발된 사례는 찾기 힘들다. 물론 기존 암호원천기술들이 지향해 온 방향이 초고속화 등에 집중되어 있어, 작은 구현 면적이나 낮은 전력 소비에 맞춰 구현된 시도가 적을 수도 있으나, 아직까지는 기존의 알려진 암호원천기술을 RFID 태그와 같은 환경에 적용하기는 어렵다고 보여진다. 그러므로 현재 활용할 수 있는 태그에 탑재 가능한, 기존 암호원천기술들의 안전성을 유지하며, 경량화되고 저전력을 소비하는 암호원천기술의 개발이 절실히 필요하다. 이를 위한 사전 단계로 본 논문에서는 상업성을 고려한 RFID 태그의 환경에서 보안을 위해 허용되는 구현 면적, 전력소비량 등과 암호원천기술이 태그에 사용되기 위해 갖춰야 하는 조건들을 도출한다.

〔표 1〕 제조 공정에 따른 암호알고리즘의 게이트 수

알고리즘	ASIC process	Throughput (Mbps)	게이트 수 (Kgates)
MISTY1	Misubishi Electric 0.18μm CMOS ASIC Design Library	70.2	5.39
Triple DES	0.18μm CMOS ASIC Design Library	170.3	5.7
	0.13μm CMOS ASIC Design Library	334.2	5.5
AES	0.18μm CMOS ASIC Design Library	235.2	5.3
	0.13μm CMOS ASIC Design Library	311.1	5.4
Camellia	Misubishi Electric 0.18μm CMOS ASIC Design Library	177.7	8.1
	0.18μm CMOS ASIC Design Library	204.6	6.3
	0.13μm CMOS ASIC Design Library	325.8	6.5
Hierocrypt-3	0.25μm CMOS ASIC Design Library	135	18.1
SEED	Fujitsu uc_core_66 FPGA Design Library	35.34	10.6
	0.25μm CMOS ASIC Design Library	237	14.1

Ⅱ. RFID 태그의 하드웨어 환경

RFID 시스템은 기본적으로 다음과 같이 태그(Tag), 리더(Reader), 데이터베이스(Database)로 구성되어 있다.

- **태그** : IC 칩과 안테나 등으로 구성되어 있으며, 무선 신호에 대한 반응으로 RFID 리더에 정보를 보낸다.
- **리더** : 무선 신호를 태그에 보내는 장치로 태그

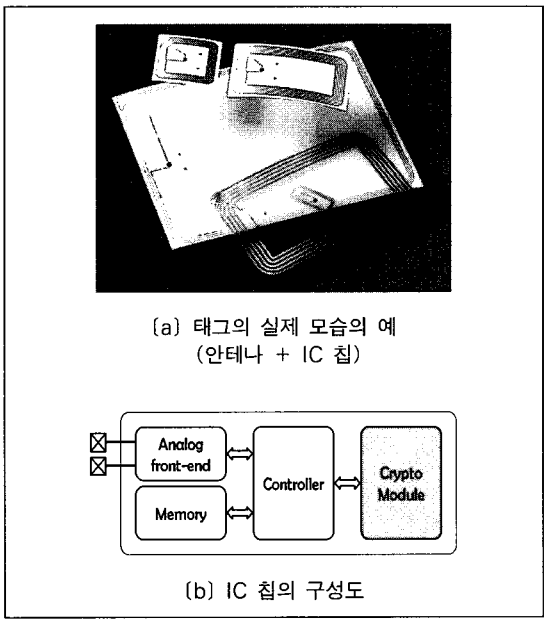
에서 보내는 정보를 수신하여, Back-end 데이터베이스에 정보를 전송한다.

- **Back-End 데이터베이스** : 각각의 태그에 관한 다양한 정보를 관리하는 안전한 데이터베이스로 ID, 리더의 위치정보, 읽혀진 시간 등을 데이터베이스화하여 제공한다.

RFID 태그는 Transponder라고도 불리며 RFID 시스템의 데이터 케리어로서 기본적으로 제품의 ID 정보를 저장하고 있다. 구성은 아래의 그림 1과 같이 데이터를 저장하는 마이크로칩(IC)과 RF통신을 위한 안테나 부(Coiled Antenna)로 구성되며, 본 논문에서의 관심사인 IC칩은 메모리, 제어부, 암호 모듈 등으로 구성되어 있다.

RFID 태그의 분류기준에 주된 요소로 고려되는 것이 배터리의 유무이다. 이를 기준으로 Active, Semi-passive, Passive 태그로 나뉜다. Active 태그는 배터리를 내장하고 있는 형태로 다른 태그와 통신을 할 수 있는 능력을 갖고 있다. Semi- passive 태그는 배터리를 내장하고 있지만, 입력 쿼리가 있어야 이에 반응하여 통신을 할 수 있다.

Passive 태그는 자체전원 없이 리더로부터 전원을 공급받고, 입력 쿼리가 있어야 이에 반응하여 통신 할 수 있다. 태그 전원의 형태는 또한 통신 거리와 비용을 결정하는 요인이 된다. Passive 태그는 리더로부터 전원을 공급받으므로, 제조 단가는 낮지만, 통신 거리는 상대적으로 짧다. Active 태그는 이와 대조적으로 제조 단가는 높지만, 통신 거리가 길다. Semi-passive 태그는 둘의 중간 정도이다. 또한 사용 주파수에 따라, 태그의 크기 및 통신 거리가 상당한 차이를 보인다. 150㎑ 이하 저주파(125㎑ & 134㎑)는 파장이 큼으로 비금속 장애물의 투과성이 우수하고 주파수, 전력 등의 규제에 대해 상대적으로 자유롭다는 점이 장점인 반면 데이터 전송률이 낮으므로 판독속도가 느리고 판독거리가 짧으며, 안테나 또는 코일 크기가 커서 소형화에 한계가 있는 점이 단점이다. 13.56㎒의 주파수는 안테나 코일이 신용카드 크기 정도로 적당하고, 비금속 장애물 투과성이 우수하며 비교적 낮은 가격에 태그용 칩의 수급이 가능하다는 점이 장점인 반면에 이 주파수 대에서 적용되는 상호유도방식의 특성상 판독 거리가 약 0.7m 이내로 제한되며 판독 속도도 낮다는 점이 문제다. UHF(300㎒~1㎓)는 전자기파 방식을 이용하므로 중, 장거리 판독이 가능하고 고속 전송이 가능하며 안테나 크기를 13.56㎒ 태그에 비해 대폭 줄일 수 있다는 점이 큰 장점으로 부각되고 있다. 아직 상용 칩이 다른 주파수대에 비해 적고 장거리용 칩은 단가가 높은 편이다. 2.45㎓는 UHF대와 대체적으로 비슷한 장단점을 갖는데, UHF보다 안테나 크기가 더 작으므로 초소형 RF 태그 구성이 가능하다. 반면 대역이 비슷한 통신 기기(WLAN, Bluetooth 등)가 계속 늘어나고 있어 주파수 간섭 영향을 받기 쉽고 고주파 특성이 우수한 소자를 필요로 하므로 칩 생산 단가가 높아지는 문제가 있다.



(a) 태그의 실제 모습의 예 (안테나 + IC 칩)

(b) IC 칩의 구성도

(그림 1) 태그의 구성(안테나 부 + IC 칩)과 IC 칩의 구성

2.1 RFID 태그의 물리적인 환경

본 논문에서는 근 미래에 수요가 급등할 것이라 예상하는 13.56㎒, 900㎒ 대역에서 작동하는 저가형의 수동형(Passive) 태그에 초점을 맞춘다.

현재 저가 수동형 태그의 가격은 대략 $0.1~$0.2 정도로 추산되며 태그 가격이 개당 $0.05 이하로 떨어져야 경제성이 있다는 것이 일반적인 견해이다.[5,6] 태그의 가격을 개당 $0.05 정도로 제한했을 경우, 안테나 부와 IC 칩과 안테나 부를 패키징하는 부분의 단가를 제외하면, 순수하게 IC 칩을 제조하는데 드는 비용은 $0.02 정도를 초과할 수 없다.[9]

IC 칩의 제조 공정에 따라 집적도가 달리 산출되겠지만, 이런 제한적인 제조단가에서 게이트의 집적도는 7,500~15,000 게이트 정도이다. 예를 들어, 100 비트 정도를 태그의 고유 ID 등의 인증정보를 저장한다

고 한다면 5,000~10,000 정도의 게이트가 요구되며 따라서, 보안을 위해 할당할 수 있는 게이트 수는 2,500~5,000 정도로 예상한다.[3] IC 칩의 크기 또한 제조 공정에 따라 달라질 수 있지만, [7]에 의하면 IC 칩의 크기는 0.4㎜ × 0.4㎜ 이하여야 한다. 현재까지 발표된 태그의 경우 Atmel Corporation의 Atmel TK5552[8]은 1㎜ × 1㎜의 규격을 갖고 있다. 992비트의 저장 공간을 갖고 있으며, 데이터 전송 비율은 약 초당 100kB이다. 또한, 메모리의 내용에 대한 읽기/쓰기를 허용하고 $1.0로 판매가 되고 있다.

13.56㎒와 900㎒z 대역에서의 동작하는 태그의 전송 비율은 대략적으로 다음과 같다. 13.56㎒에서는 50개의 태그 당 26Kbps(즉, 26Kbps/50Tag) 정도이며, 900㎒ 대역에서는 200개의 태그 당 128Kbps (즉, 128Kbps/200Tag)정도이다. 각 태그에 할당된 읽는 시간이 1초를 초과 할 수 없다고 한다면, 태그 당 대략 500비트 정도를 전송할 수 있다고 여겨진다.[9]

전류 소비량 또한 RFID 태그 설계에서 고려되어야 하는 핵심 요소 중 하나이다. 본 논문에서 가정하고 있는 태그의 형태가 Passive형이기 때문에 배터리를 내장하고 있지 않다. Passive 태그는 리더기와 통신하는 동안만, 즉 태그가 리더기의 통신범위(communication range)내에 존재할 때만 전력이 공급되며, 이 전력 또한 전자기장을 통해 무선으로 공급되므로 매우 제한적이어서 자체 계산력은 미약할 수밖에 없다. 반면, 저가형으로 제작이 가능하고, 수명이 반영구적인 장점이 있다. 위의 내용을 정리하면 표 2와 같다. 실제적으로 외부로부터 전원을 공급받는 수동형 RFID 태그의 경우, 전류 소비량은 암호기술을 탑재하기 위한 가장 큰 제약조건이다.

〔표 2〕 태그의 물리적인 환경

물리적 환경	내 용
태그의 형태	Passive
가격	$0.05 이하
보안에 할당된 게이트 수	2,500~5,000 게이트
IC 칩의 크기	0.4mm × 0.4mm 이하
주파수 대역	13.56㎒z, 900㎒
전송률	13.56㎒ : 26Kbps/50Tag 900㎒ : 128Kbps/200Tag
전류 소비량	수십 μA 이하

Ⅲ. 하드웨어 구현 환경

태그에 암호기술을 적용하기 위해서는 앞에서 살펴본 바와 같이 태그에서 허용하는 구현 면적, 전력 소비량 등을 고려해야 한다. 이를 위해서는 암호기술을 하드웨어로 구현하는데 따르는 구성 논리와 그들의 구현 면적, 전력 소비량 등에 대한 이해가 필요하다. 기본적으로 하드웨어는 데이터를 저장하지 않고 산술적인 연산 대부분을 수행하는 조합 논리(Combinational Logic)와 데이터를 저장하고 이어지는 클록에서 이전 결과 값을 이용하여 다시 결과를 계산하는 기능을 수행하는 비조합 논리(Non-combinational Logic)의 두 가지 종류로 구성이 된다.

3.1 조합 논리(Combinational Logic)

조합 논리란 디지털 회로의 가장 기본이 되는 구성 요소로서 회로의 출력이 현재의 입력 값으로부터만 영향을 받는 회로를 말하며 기본 게이트(Gate)에 해당하는 NAND, NOR 등이 조합되어 표현된다. 대부분의 수학적인 연산을 하는 부분은 모두 이 조합 논리 하드웨어로 구성된다. 여기에서 우리가 설계된 하드웨어의 구현 면적을 말할 때 흔히 '게이트 수' 혹은 '하드웨어 사이즈'라는 용어를 사용하게 되는데, 이때 '게이트 수'는 공정에 따라 약간의 차이가 있겠지만 기본적으로는 2개의 입력과 1개의 출력을 가진 NAND 게이트의 수를 의미한다. 즉, NAND 게이트의 크기를 '1'로 기준 하였을 때 나머지 다른 종류 게이트의 크기를 비례 환산하여 표시한 것을 의미한다.

표 3은 삼성전자의 0.13㎛ 라이브러리를 이용하여 디자인 된 것을 참조하여 기본 NAND 게이트 대비 다양한 논리 게이트의 하드웨어 구현면적을 나타낸 것이다. 이는 제조공정에 따라 값이 달라질 수 있다. 표 3에서 보는 바와 같이 산술 덧셈기(Full Adder) 같은 경우나 조금 복잡한 Multiplexer의 경우는 많은 하드

〔표 3〕 논리소자들과 NAND를 기준으로 한 각 논리소자의 비례 게이트 수[12]

논리	게이트 수	논리	게이트 수
AND	1.67	XOR	3
NAND	1	INV	0.67
NOR	1	Full Adder	7.67
OR	1.67	2-to-1 Mux	3
NXOR	3	4-to-1 Mux	7.33

웨어 면적을 차지함을 알 수 있다. 따라서 하드웨어 구현 면적을 줄이기 위해서는 가능한 한 복잡한 계산식을 단순화해야 하며, 경우에 따라 여러 개의 결과 값 중 몇 개를 선택해야 하는 연산의 수를 줄여야 한다.

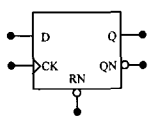
3.2 비조합 논리(Non-combinational Logic)

비조합 논리란 순차 논리(SequentialLogic)라고도 불리는데, 이 회로는 출력이 현재의 입력뿐만 아니라 과거의 입력에도 영향을 받는 회로에 해당한다. 순차 논리는 클록 신호에 의해 입력을 샘플링 하여 출력을 내는 Flip-Flops와 클록 신호와 관계없이 계속해서 입력을 샘플링 하여 출력을 내는 Latches 등이 있다.

일반적으로 암호 알고리즘에서 비밀키나 혹은 평문, 암호문 같은 일련의 데이터를 저장하는 데에는 주로 Flip-Flops가 사용되는데, 통상 "레지스터(Register)"라고 부른다. 여러 가지 종류의 Flip- Flop들이 존재하지만 그 중에 가장 일반적으로 많이 사용되는 D-Flip-Flop을 표 4에서 보여 준다.

암호화 또는 복호화 연산을 수행하기 위해서 초기 입력 데이터를 저장할 레지스터, 매 라운드마다 라운드 함수를 수행하는데 필요한 레지스터, 라운드 함수를 수행하고 난 결과를 저장할 임시 레지스터 등이 존재한다. 물론 암호알고리즘의 성격상 공유 가능한 레지스터가존재할 수도 있지만 반드시 따로 구성되어야 하는 경우도 있다. 표 4와 같이 1 비트를 저장하는 데에는 7.67 게이트가 필요하다. 그러므로 128 비트만을 저장한다고 가정하여도 약 1000 게이트가 요구된다. 이는 조합논리에 비해서는 매우 큰 값이다. 따라서 암호알고리즘의 하드웨어 구현상 필요한 레지스터의 수가 얼마인가 하는 것이 전체 하드웨어 사이즈에 많은 영향을 준다는 것을 알 수 있다.

(표 4) D Flip-Flops와 비례 게이트 수

논리	논리 심볼	게이트 수
D Flip-Flop with Reset		7.67

3.3 저전력 하드웨어

하드웨어 구현에서는 목적하는 바에 따라 고성능 또는 저전력 구현으로 구분해서 접근할 수 있다. 절충되는 부분에 속하는 경우도 있으나, 일반적으로는 고성능 하드웨어 구현과 저전력 하드웨어 구현은 서로 Trade-off 관계에 있다. 이 두 가지 측면의 관점에서 추가적으로 개입되는 것이 구현 면적인데, 고성능 하드웨어 구현 혹은 저전력 하드웨어 구현에 구현 면적까지 작다면 최상의 하드웨어라 할 수 있다. RFID 태그에서는 제약된 구현 면적이 중요 요소로 대두되고 있으므로, 유사 라운드를 반복 적용하는 형태의 일반적인 암호알고리즘에서의 구현 면적에 대해 알아보자.

속도 측면의 고성능 하드웨어를 구현하기 위해서는 기본적으로 라운드 당 1 클록 사이클을 소요하는 것으로 가정한다. 예를 들어, 128 비트 비밀키의 AES[11]를 하드웨어로 구현하고 암호화를 수행하는데, 주어진 제조 공정에서 Critical Path의 연산시간이 40ns 소요되었다고 하자. 1 라운드를 수행하는데, 1 클록이 소요되는 아키텍처에서는 최대 주파수가 25㎒ 이상이 될 수 없으므로 최대 Throughput이 320Mbps 정도 된다. 그러나 1 클록에 여러 라운드를 수행하는 구조로 설계한다면, 그 만큼 Critical Path가 길어져 처리 클록 수는 현저히 줄어들지만 최대 주파수는 낮아지게 때문에 최종 Throughput은 개선되지 않는다. 각 구조에 따른 성능변화를 표 5에 나타내었다.

표 5에서 A0는 라운드 당 클록 수에 영향을 받지 않는 하드웨어 면적을, A1은 라운드 당 클록 수에 영향을 받는 하드웨어 면적을 나타낸 것이다. 위의 표에서 알 수 있듯이 한 클록에 여러 라운드를 연속적으로 수행하는 구조는 A1의 크기가 라운드 수의 배수만큼 증가하게 된다. 반면, 한 라운드를 여러 클록으로 나누어 실행하는 구조는 A1의 크기가 라운드 수의 역수만큼 감소하게 되고, 또한 하드웨어를 분할하여 사용할 수 있기 때문에 전체적인 하드웨어 구현 면적을 줄일 수 있다.

(표 5) 다양한 하드웨어 구조에 따른 성능 변화

클록수 /라운드	Critical Path (클록 주파수)	Throughput	하드웨어 사이즈
1클록/4R	160ns(6.25㎒)	320 Mbps	A0 + 4A1
1클록/2R	80ns(12.5㎒)	320 Mbps	A0 + 2A1
1클록/1R	40ns(25㎒)	320 Mbps	A0 + A1
2클록/1R	20ns(50㎒)	320 Mbps	A0 + $\frac{1}{2}$A1
4클록/1R	10ns(100㎒)	320 Mbps	A0 + $\frac{1}{4}$A1

저전력 하드웨어 구현에 대해서는 하드웨어의 소비 전력(Power)에 대한 이해가 필요하다. CMOS 회로에서 전력 소비는 Static Dissipation(P_s)과 Dynamic Dissipation(P_d)의 두 가지 성분의 합으로 정의할 수 있다. Static Dissipation은 CMOS 자체의 성질에 의해 소비되는 누출(leakage) 전류에 의한 것이며, Dynamic Dissipation은 Switching Transient Current와 Load Capacitance의 충·방전 전류의 합으로 표현할 수 있다. 위에 언급한 두 가지 종류의 전력 소비 중에서 큰 비중을 차지하는 것은 Dynamic Dissipation이다. P_d는 다음과 같은 수식 (1)로 표현이 될 수 있다.

$$P_d = C_L \cdot V_{DD}^2 \cdot f_p \quad (1)$$

위의 수식에서 C_L은 회로가 구동해야 하는 Load Capacitance에 해당하고 V_{DD}는 회로에 걸리는 전압을 말하며 f_p는 회로가 Switching하는 Toggling Rate에 해당한다. 따라서 전체 Dynamic Dissipation의 양을 줄이기 위해서는 회로가 구동해야 하는 Load Capacitance를 줄이고 즉, 다시 말하면 회로의 수와 사이즈를 줄이고 전압을 낮추며 Switching이 최소가 되도록 설계하여야 한다.

위의 결과로 보아 저전력은 하드웨어 사이즈와 클록 주파수와 굉장히 밀접한 관계가 있음을 알 수 있다. 따라서 저전력으로 설계하기 위해서는 최대한 클록 주파수를 낮추고 꼭 필요한 회로만 추가하며 쓸데없는 회로의 switching을 없애는 등의 작은 면적을 차지하는 설계를 하는 것이 관건이다.

3.4 물리적(Physical) 공격에 대한 저항성

암호알고리즘의 소프트웨어 또는 하드웨어 구현은 각각 안전성이나 효율성 등 다양한 면에서 다른 장단점이 있을 수 있다. 저가의 RFID 태그의 경우는 제약된 자원만을 가지므로 소프트웨어적으로 암호알고리즘을 구현하여 탑재하는 것은 불가능해 보이며 간단한 인증 로직이나 암호알고리즘을 하드웨어적으로 구현하는 방안이 적합하다고 보여 진다. 따라서 설계된 암호알고리즘의 이론적인 안전성 이외에도 하드웨어 구현 시 물리적 공격에 대한 저항성이 고려되어야 한다.

암호알고리즘을 탑재한 태그의 경우, 스마트카드에 적용되는 전력해석(Power Analysis), 타이밍 해석(Timing Analysis), 오류주입 공격(Fault Analysis Attack)등의 사이드채널공격(혹은 부채널 공격)[13-15]에 대한 위험요인이 존재할 수 있으며 이에 대한 대응책이 마련되어야 한다.

Ⅳ. 결 론

RFID 시스템에서 개인의 사생활 및 개인 정보를 보호하기 위해 정당한 리더만이 태그 정보를 읽을 수 있도록 하는 태그와 리더간의 상호인증기술, 혹은 정보보호기술은 반드시 필요하며 점차 그 필요성이 높아지고 있다. 이는 암호기술을 사용하여 해결할 수 있는데, 문제는 RFID 태그에 탑재될 수 있는 작은 구현면적, 저전력 등의 제약환경에 맞춰 개발된 암호알고리즘의 부재이다. 비록 고가의 태그에서는 기존의 암호원천기술을 적용하는 것이 가능하다고 하나 이는 유비쿼터스 컴퓨팅 환경이 지향하는 것과 현재로서는 제조기술 및 제조단가 등에서 거리감이 있다. 그러므로 RFID 시스템에서 해결해야 되는 과제 중 선행되어야 하는 것이 저렴한 비용의 RFID 태그에 탑재할 수 있는 안전한 해쉬함수, 블록암호 알고리즘, 스트림암호 알고리즘 등의 암호원천기술 개발 및 구현이다. 또한 점차 RFID 시스템의 시장 규모가 커지고 있으며, RFID 시스템의 보안에 관한 연구가 활발히 시작되고 있는 시점에서 이를 뒷받침할 수 있는 암호원천기술의 개발은 반드시 필요하다.

참 고 문 헌

[1] Juels, A. et al., The Blocker Tag : Selective Blocking of RFID Tags for Consumer Privacy, 10th ACM Conference on Computer and Communications Security, 2003.

[2] S. A. Weis, S. Sarma, R. Rivest, and D. Engels, Security and privacy aspects of low-cost radio frequency identication systems, In First International Conference on Security in Pervasive Computing, 2003.

[3] S.E. Sarma, Towards the five-cent tag, Technical Report MIT-AUTOID-WH-006, MIT Auto ID Center, 2001. Available from http://www.autoidcenter.org.

[4] *CRYPTOREC reports*, published 2002.

[5] *The 5-cent RFID tag*, RFID Journal, Feb.16, 2004.
[6] G..Swamy and S.Sarma, Manufacturing Cost Simulations for Low Cost RFID systems, White Paper, MIT Auto-ID Center, 2003. http://www.autoidlabs.org/whitepapers/mit-autoid-wh017.pdf.
[7] K. Takaragi, M. Usami, R. Imura, R. Itsuki, and T. Satoh, An ultra small individual recognition security chip, IEEE Micro, 21(6):43-49, 2001.
[8] Atmel Corporation. *Atmel TK5552 data sheet, 2001*. Available at http://www.atmel.com/atmel/products/prod227.htm.
[9] Miyako Ohkubo, Koutarou Suzuki and Shingo Kinoshita, Cryptographic Approach to "Privacy-Friendly" Tags, submitted 2003.
[10] Stephen A. Weis, *Security and Privacy in Radio-Frequency Identification Devices*, Masters Thesis. MIT. May, 2003
[11] National Institute of Standards and Technology, *Federal Information Processing Standards Publication 197*, Announcing the Advanced Encryption Standard(AES), 2001.
[12] *Samsung STD150 library databook*, "0.13㎛ 1.2V CMOS Standard Cell Library for Pure Logic Products"
[13] P.C. Kocher. Cryptanalysis of Diffe-Hellman, RSA, DSS, and Other Cryptosystems Using Timing Attacks, In Advances in Cryptology, CRYPTO'95 : 15th Annual Int. Cryptology Conf., D. Coppersmith, Ed., Springer LNCS 963, pp171-183, 1995.
[14] D. Boneh, R. DeMillo, and R. Lipton, On the importance of checking crypto-graphic protocols for faults, Journal of Cryptology, Springer-Verlag, Vol. 14, No. 2, pp. 101-119, 2001. Extended abstract in Proceedings of Eurocrypt '97, Lecture Notes in Computer Science, Vol. 1233, Springer-Verlag, pp. 37-51, 1997.
[15] P. Kocher, J. Jaffe, and B. Jun, *Introduction to Differential Power Analysis and Related Attacks*, http://www.cryptography.com/dpa/technical 1998.
[16] 최병윤, 서정욱, "SEED 알고리즘용 암호 보조 프로세서의 설계," 한국통신학회논문지, 25(9), pp. 1609-1616, 2000.
[17] 최홍묵, 최명렬, "스마트카드용 고성능 SEED 프로세서의 구현," 한국정보보호학회논문지, pp. 37-47, 2004.

〈著 者 紹 介〉

장 환 석 (Hwan Seok Jang)
학생회원

2002년 2월 : 한양대학교 수학과 이학사
2004년 2월 : 한양대학교 대학원 수학과 이학석사
2004년 3월~현재 : 한양대학교 대학원 수학과 박사과정
2004년 11월~현재 : 한국정보보호진흥원 위촉연구원
〈관심분야〉 암호학, 정보보호

박 해 룡 (Haeryong Park)
종신회원

1999년 2월 : 전남대학교 수학과 이학사
2001년 2월 : 서울대학교 수학과 이학석사
2000년 12월~현재 : 한국정보보호진흥원 암호응용팀 연구원
〈관심분야〉 암호프로토콜, 키관리, 정보보호

천 동 현 (DongHyeon Cheon)
종신회원

1995년 2월 : 고려대학교 수학과 이학사
1997년 8월 : 고려대학교 대학원 수학과 이학석사
2001년 2월 : 고려대학교 대학원 수학과 이학박사

2001년 9월~현재 : 한국정보보호진흥원 암호응용팀 선임연구원
〈관심분야〉 암호학, 정보보호

전 길 수 (Kilsoo Chun)
종신회원

1991년 2월 : 서강대학교 수학과 이학사
1993년 2월 : 서강대학교 대학원 수학과 이학석사
1998년 2월 : 서강대학교 대학원 수학과 이학박사
1998년 10월~1999년 9월 : 서강대학교 기초과학연구소 박사후 연구원
2001년 3월~2001년 6월 : 서강대학교 컴퓨터학과 연구교수
2001년 7월~현재 : 한국정보보호진흥원 암호응용팀장
〈관심분야〉 암호학, 정보보호, RFID/USN 정보보호

송 정 환 (Jung Hwan Song)
정회원

1984년 2월 : 한양대학교 수학과 이학사
1989년 5월 : Syracuse University 수학과 이학석사
1993년 5월 : Rensselaer Polytechnic Institute 수학과 이학박사
1999년 3월~현재 : 한양대학교 수학과 부교수
〈관심분야〉 암호학, 수리계획법, 최적론