PUF 기술을 활용한 보안 칩 기술 개발 과 그 응용 분야

백종학
ICTK

신광조
ICTK

Ⅰ. 서 론

최근 다양한 스마트 기기가 보급되고 그 중 스마트폰의 대중화는 이를 이용한 금융 거래나 무인 자동차 분야에 활용되는 등 새롭고 다양한 서비스와 사용 환경을 만들어 내고 있다. 이러한 IoT 환경의 확산은 해킹에 대한 위험성도 높아져 개인 정보 유출등 많은 보안 사고를 유발하게 되어 보다 안전한 보안에 대한 요구가 높아지기 시작했다. 특히 기존의 소프트웨어 기반의 암호화 Key 관리 기술에 대한 보안 우려로, 보다 안전한 Key 관리와 경량 IoT 기기에 적합한 가볍고 간단한 암호화 Key 관리를 할 수 있는 하드웨어를 이용한 보안방식에 대한 요구도 나타나고 있다.

이러한 요구사항을 해결하기 위해 연구되고 있는 기술 중 하나가 "물리적 복제 방지 기능"이라 불리는 PUF (Physical Unclonable Function)기술이다. 본 기고문에서는 하드웨어 또는 반도체의 고유 지문이라 표현되고 있는 PUF가 무엇인지 살펴 보고 이를 적용한 chip 개발 내용을 설명하며 마지막으로 개발된 chip을 활용하여 정품 인증 및 firmware protection등 실제 field application 에 적용 되는 예를 살펴 보는 것으로 글을 마무리 하고자 한다.

Ⅱ. PUF 란?

하드웨어 보안 분야에서 chip의 고유 정보인 ID 또는 보안 Key 등의 주요 정보는 전원이 공급되지 않더라도 그 값이 없어지지 않아야 하며, 사용할 때마다 항상 같은 값을 유지해야 한다. 이 때문에 현재까지 주로 사용되는 방법은 EEPROM과 같은 NVM (Non-Volatile Memory; 비휘발성 메모리)에 저장하여 사용하는 것이다. 그러나 NVM에 data를

저장하는 경우는 저장되는 data에 대한 관리가 따로 필요하고 관리 소홀시 data가 유출될 수 있는 위험이 있다. 또한 저장된 후에도 다양한 물리적 보안 공격으로 메모리의 값을 읽어낼 수 있기 때문에 보안 위험에 늘 노출되게 된다. 이러한 문제 해결을 위해 접근하고 있는 방법 중 하나가 PUF (Physical Unclonable Function;물리적 복제 방지 기능) 기술이다.

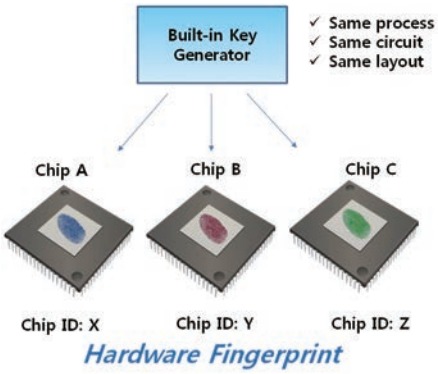
이러한 PUF에 대해서 이제 알아 보고자 한다.

1. PUF 정의

PUF란 반도체 제조 공정에서 발생하는 공정편차를 이용하여 chip 내부에 구현된 예측하기 어려운 랜덤한 디지털 값을 생성하는 시스템을 의미한다. 하드웨어적으로 예측 불가능한 값이 출력되므로 복제가 불가능하다.

좀더 자세히 살펴 보면 〈그림 1〉에서 보듯이 동일한 회로와 동일한 마스크 레이아웃을 가지고, 동일한 공정과정을 진행하더라도 반도체 제조 과정 특성상 발생하는 공정편차에 의해 트랜지스터, 커패시터, 저항 등과 같은 소자 특성에서부터 게이트 지연시간과 같은 회로 특성까지 많은 부분에서 차이가 나게 된다. PUF는 이러한 특성 때문에 chip 마다 서로 다른 0 또는 1의 비트 값을 갖게 되고, 이렇게 결정된 값은 랜덤 수 생성 장치와 달리 매번 생성 시마다 동일한 값을 출력하기 때문에 chip 고유의 정보로 활용할 수 있다. 또한 생성되는 값은 chip 내부에서 생성 되는 값이기 때문에 외부에서 주입 없이 자체적으로 data 생성이 가능하여 chip 외부로의 유출을 근본적으로 차단할 수 있고, 기존 NVM과 달리 침입 공격 등과 같은 물리적 보안 공격에 대해서도 그 값을 읽기가 어렵다. 이렇게 생성된 디지털 값은 chip의 ID, 인증 회로, 암호 알고리즘의 대칭 key 또는 비밀 key 등과 같이 다양한 영역에서 사용될 수 있다.[1-5]

PUF란 반도체 제조 공정에서 발생하는 공정 편차를 이용하여 chip 내부에 구현된 예측 어려운 랜덤한 디지털 값을 생성하는 시스템이다.



〈그림 1〉 PUF 개념도

2. PUF 평가 지표

PUF의 성능을 평가하는 지표에는 대표적으로 랜덤성(randomness)과 신뢰성(Reliability)이 있다. 두 특성 모두 PUF 기술를 평가하는 중요한 항목이 된다.

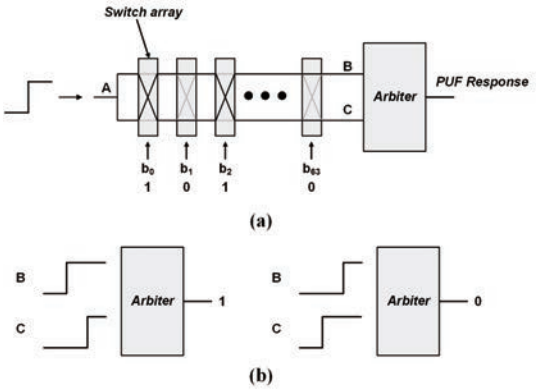
랜덤성이란, 동일하게 제조되어 만들어지는 서로 다른 chip에서 PUF 값은 모두 달라야 하며, 또한 그 값은 예측 불가능하다는 것을 보여 주는 특성을 말한다. 세부적으로는 출력 비트 0 또는 1 값이 random하게 생성되는지에 대한 randomness 지표와 서로 다른 두 칩의 출력 비트가 얼마나 다른지를 나타내는 uniqueness 지표가 있다.

신뢰성이란, 제작된 chip에서 PUF값이 얼마나 동일한 출력 값을 유지하는지를 나타내는 지표를 말한다. 작은 공정 편차를 이용하는 PUF는 시간이 지나거나 외부 노이즈 및 온도와 같은 주변 환경 특성에 따라 값이 쉽게 변할 수 있기 때문이다. 신뢰성은 보안 key로 사용되는 분야에서 매우 중요한 평가 지표가 된다. 제작된 PUF값이 변할 경우 그 변하는 것을 막거나 보상해 주기 위해 pre-selection 및 error correction 등 PUF 구현 방식과 더불어 같이 연구되고 있다.[2,5]

3. PUF의 종류

PUF는 구현하는 방식에 따라 두 가지로 구분 할 수 있다. 소자 또는 회로의 mismatch를 이용한 mismatch-based PUF와 반도체 공정 진행에 따라 물리적으로 형성 여부를 이용한 physical-based PUF이다[6].

Mismatch-based PUF는 제작되는 마스크의 레이아웃은 동일하나 소자 또는 회로의 특성이 반도체 제조 공



〈그림 2〉 Arbiter PUF
(a) Schematic (b) response

정을 진행 하면서 발생하는 공정 편차 (mismatch)에 의해 특성이 달라지는 것을 이용한 것이다. 기존에 연구된 방식인 Arbiter PUF[7], Ring-oscillator PUF, SRAM PUF 등은 대부분 이러한 공정 mismatch를 이용하는 방법으로 연구되었다.

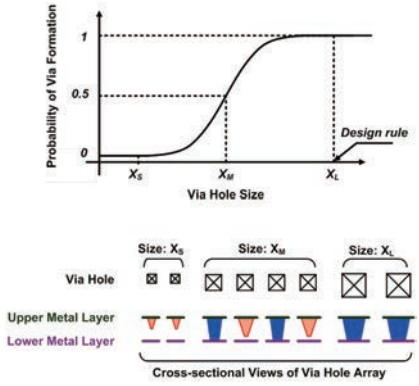
대표적인 mismatch-based PUF는 Arbiter PUF이다. 〈그림 2 (a)〉는 Arbiter PUF의 회로를 도식화한 것으로 동작 원리를 살펴보면 bi 신호에 따라서 switch array의 연결이 달라지게 되고, 달라진 신호 전달 경로는 공정 편차에 의해 지연시간이 달라진다. 따라서 A 점에서 상승 신호가 발생 했을 때 동일한 회로임에도 불구하고 Arbiter 회로의 두 입력인 B, C에는 경우에 따라 서로 다른 도착 시간을 갖게 된다. Arbiter 회로는 어떤 신호가 먼저 도착 했는지를 결정하고 PUF response를 결정한다. 〈그림 2 (b)〉는 B, C의 신호가 각기 달리 도착 했을 때 "1" 또는 "0"의 디지털 값을 Arbiter 결과값으로 내보내는 예를 보여 주고 있다.

그러나 제작이 완료된 Arbiter PUF는 동작 시 전원 전압이나 온도등 환경에 의해서도 지연시간이 변경 될 수 있다. 만약 게이트 지연시간에 미치는 영향이 공정 편차에 의한 것이 다른 외부 환경 노이즈에 의한 영향보다 크다면 문제가 되지 않겠지만, 공정 편차에 의한 지연시간이 작을 경우에는 외부 환경 노이즈에 의한 영향으로 PUF 값이 변할 수 있게 된다. 최초 제작된 디지털 값이 환경에 의해서 변경이 된다면 PUF의 신뢰도에 문제가 생겨 그 역할을 제대로 할 수 가 없다. 이러한 취약한 특성을 보완 하기 위해 대부분의 mismatch-based PUF는 error correction code와 같이 별도의 data 후처리 작업을 통해 값이 바뀌는 현상을 보상하는 회로를 함께 연구하고 있다.

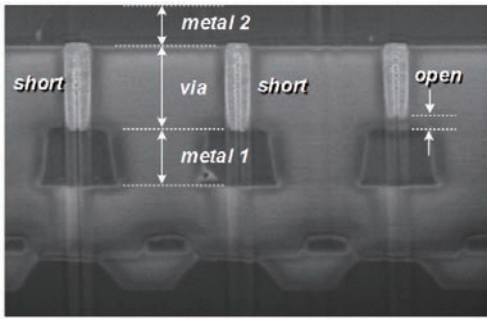
PUF를 구현 하는 또 다른 방식은 physical-based PUF 이다. 이는 메탈, VIA, 폴리실리콘 등과 같은 전도성 레이어가 형성 되는 물리적 상태에 의해 출력 값이 결정되는 PUF를 말한다. 즉 physical-based PUF는 제작 과정중 하나 또은 두 레이어 사이에서 서로 연결되거나 연결되지 않는 물리적 특성을 이용하여 PUF 값을 결정한다. 이러한 점은 PUF 신뢰성 측면에서 매우 큰 장점을 가질 수 있다. 한번 결정된 물리적 특성은 온도나 전원 전압 등 외부의 환경 노이즈가 발생하더라도 그 특성이 바뀌지 않기 때문이다. Physical-based PUF에는 대표적으로 VIA PUF가 있다.

4. VIA_PUF

VIA-PUF는 반도체 제조 공정을 진행하면서 VIA가 형성될 확률을 기반으로 랜덤 값을 생성하는 PUF이다[8]. VIA는 반도체 제조 공정에서 인접한 두 메탈 레이어를 연결하는 공정을 말한다. 일반적으로 VIA의 크기는 해당 process와 공정 recipe를 고려하여 VIA가 항상 형성되는 것을 보장하기 위해 그 크기가 디자인 룰로 정해진다. 만일 VIA의 크기가 디자인 룰보다 작아지면 VIA가 형성이 안되 연결 여부가 불확실해 질 수 있다. 즉 VIA 크기가 작아질 수록 VIA의 형성 확률도 함께 감소한다. 〈그림 3〉은 VIA PUF에 있어 VIA size에 따른VIA 형성 확률



〈그림 3〉 VIA 크기 별 형성 확률



〈그림 4〉 VIA 단면 분석

(Probability of VIA formation)을 나타낸 것이다. 그래프에서 보듯이 design rule size인 X_L인 경우는 모든 VIA가 형성이 되고, size가 X_M으로 design rule 보다 작아지면 형성 확률도 줄어 들게 된다. 그러다 어느 특정 size인 X_S 보다 작아지면 더 이상 VIA는 형성이 되지 않는다. VIA size X_M인경우 동일한 size임에도 불구하고 그 단면을 보면 VIA가 형성되는 경우와 그렇지 않은 경우가 50%에 가까워지며, 이는 PUF 값을 이용해 어떤 디지털 값을 만들 때 높은 randomness 특성을 가지게 할 수 있다.

〈그림 4〉은 실제 반도체 공정을 통해 제작된 VIA_PUF의 단면 사진이다. 동일한 VIA size임에도 불구하고 일부 VIA는 상위 메탈과 하위 메탈을 연결하고 있으며, 어떤 VIA는 연결되지 않고 open 된 것을 확인 할 수 있다. VIA 레이어를 통한 물리적인 연결은 노이즈 및 주변 환경이 달라지더라도 그 연결 상태가 변하지 않아 동일한 상태를 계속 유지한다. 따라서 높은 신뢰성을 보장할 수 있기 때문에 error correction code와 같은 별도의 후처리 작업을 하지 않더라도, 암호 알고리즘의 보안 key로 사용할 수 있다. 이러한 신뢰성은 JEDEC 기준의 1000hr 신뢰도 평가 이후에도 PUF 값이 변하지 않는 것을 확인하였다. 따라서 VIA-PUF는 암호 key를 기반으로 하는 다양한 어플리케이션에 적용하는데 매우 적합한 PUF라고 할 수 있다.

다음 장에서는 연구된 PUF를 이용하여 실제 chip에 적용하는 방법에 대해서 자세히 고찰해 보겠다.

PUF를 활용한 Secure IC 개발 방법은 암호 Key로 사용 하는 방법과 내부 memory에 data를 기입할 때 그 값을 암호화 하는 secure-memory로 사용하는 방법이 있다.

Ⅲ. PUF를 활용한 Chip 개발

PUF를 활용한 Secure IC를 개발하는 데 있어 그 적용 방법은 크게 2가지로 구분하여 이야기 할 수 있다. 암호화 알고리즘에 필요한 암호 key로 사용하는 방법과 다른 하나는 내부 memory에 data를 기입할 때 그 값을 암호화 하는 secure-memory로 사용하는 방법이다.

1. Crypto algorithm의 direct-key

RSA, ECC, AES 및 SEED등 다양한 암호 알고리즘이 현재 사용 되고 있다. 이러한 암호 알고리즘을 사용하기 위해서는 key가 반드시 필요하게 되는데 이 역할을 PUF가 함으로써 안전한 보안을 얻을 수 있다. 그러나 PUF를 적용했다고 해서 무조건 안전하다 할 수 없다. 적용 된 PUF key 관리를 안전하게 설계해야 비로소 안전하다 할 수 있다. PUF를 Key로써 활용하는 데는 적용하는 방식에 따라 weak-PUF와 strong-PUF로 구분할 수 있다.

Weak-PUF[9]는 VIA_PUF와 같은 type으로 static 한 challenge만을 사용하거나 challenge가 하나인 PUF로 한번 결정된 Key값은 다시 변경이 불가능 하기 때문에 이를 외부에서 알아낼 수 없어야 안전하다. 안전한 형태로 존재한다고 해도 key값이 밖으로 나오는 순간 안전하지 않게 된다. 따라서 PUF key 값은 외부로 나오지 않고 chip 내부에만 유지되어 crypto 연산 시에만 사용해야 한다. 고정된 PUF값과 crypto algorithm을 동시에 구현함으로써 안전성을 확보할 수 있다. 또한 side channel attack등을 통해 공격 되는 것을 대비하여 설계해야 한다. 특히 Chip 내부 bus에 probe 공격하는 것에 대한 대비도 필요하다.

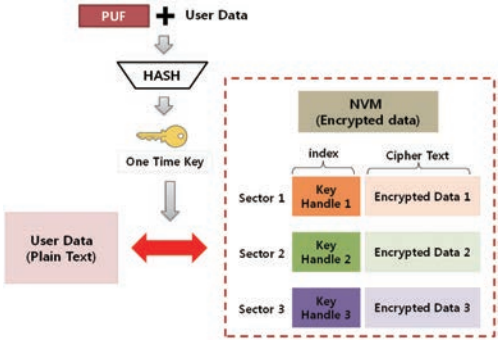
Strong-PUF는 Arbiter PUF와 같은 type으로 challenge-response 방식을 이용하여 challenge에 따라 계속 변경되는 값을 생성하여 이를 key로써 이용하는 것으로 해당 session에만 임시적인 key로 활용한다. 발급 시 challenge-response쌍을 미리 받아 저장했다가 인증 시 challenge에 대한 response를 맞추면 인증되는

방식이다. 따라서 인증서버는 많은 challenge-response 쌍을 안전하게 저장 관리해야 한다. 사용된 challenge-response쌍은 삭제하여 재 사용을 방지한다. 공격자가 인증 과정에 대한 도청과 일정 기간 많은 challenge-response쌍을 알아내도 서버의 challenge-response쌍에 대한 response는 알아낼 수 없다고 정의하여 사용되었으나 요즘 한창 issue가 되고 있는 deep learning 등 여러 공격 방법에 의해 분석이 되고 있어 신뢰성 문제를 차치하고도 Strong-PUF 이름이 무색하게 안정성에 위협을 받고 있는 실정이다.

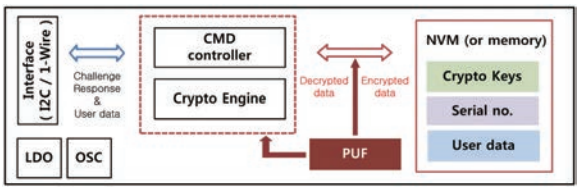
2. Secure-memory

SOC chip 개발시 대부분의 IC는 embedded memory 형태로 개발 된다. 이때 NVM에 기록된 중요한 data가 해커의 물리적 보안 공격에 의해 그 내용이 유출 될 수 있다. 이를 방어하기 위해 chip 설계시 NVM의 memory address를 scrambling 하여 NVM에 쓰여지는 data가 순차적 data가 아닌 형태로 저장하여 memory의 data가 유출되더라도 그 내용을 쉽게 알아 보지 못하게 처리를 한다. 그러나 이 방어는 생각 보다 쉽게 뚫릴 수 있다.

이를 보완하여 보다 안정적인 memory를 사용하기 위해 PUF를 사용할 수 있다.



〈그림 5〉 Secure-memory



〈그림 6〉 IL005 Block diagram

〈그림 5〉는 PUF를 이용하여 secure-memory를 구현하는 방식을 나타낸 것이다. 외부에서 주입된 user data를 PUF를 이용하여 암호화한 이후에 memory에 data를 저장한다[10]. 이를 secure-memory라고 한다. Secure-memory의 경우 공격자가 user data 값을 알아내기 위해서는 chip 내에 NVM에 저장된 data를 알아내는 데서 끝나는 것이 아니라 암호화시 Key로 사용된 PUF값도 알아내야 한다. PUF 값을 모르고 공격하는 방법은 NVM에 저장된 값을 알아낸 후 crypto algorithm을 공격하여 값을 알아내는 방법을 생각할 수 있지만 공인된 crypto algorithm을 cipher-text-only attack 방법만 가지고 분석하는 것은 불가능하다고 알려져 있다. 만일의 경우 한 chip에 대해 공격자가 PUF Key대신에 Key로써 가능한 모든 조합의 data를 넣어 그 chip의 NVM data 값을 알아 낸다 하여도 chip 별로 암호화 key로 사용된 PUF 값이 다르기 때문에 한 chip이 공격을 당해도 다른 chip을 공격하는 데는 도움이 되지 않는다.

3. 실제 적용 개발 사례

PUF를 이용하여 chip을 설계한 경우의 실제 적용 사례를 통해 살펴 보고자 한다.

〈그림 6〉은 ICTK에서 설계한 IL005라는 PUF를 기반으로 하는 secure IC의 block diagram이다. 전원 공급을 위한 LDO와 clock 제공을 위한 oscillator를 내장하고 있고 interface는 I2C 및 1-wire 를 지원한다. Mobile 제품 적용을 위해 대기 전력 소모를 150nA 이하로 설계하여 사용 하지 않을 경우 전원을 off 하지 않아도 chip에서 소모되는 leakage current를 최소화 하였다. VIA-PUF를 적용하여 보안 강도를 높였으며 SHA2-256 algorithm을 hardware로 구현하였다. 구현된 crypto algorithm과 PUF key를 이용하여 '인증' 에 적용 가능하다. PUF값을 cryptographic hash 함수 (h=hash(m)에서 h를 알아도 m을 유추하기 어려운 함수, hash(m) = hash(m')을 만족하는 m, m'을 찾기 어려운 함수)를 이용하여 외부 PUF key[index] = hash(index, PUF)로 계산하여 사용한다. Cryptographic hash 함수의 특성에 따라 나중에 PUF key가 노출되어도 PUF값은 알 수 없어 다른 key에 대

〈표 1〉 IL005 주요 명령어

Name	Code	Description
Read	0x02	Sector Data 읽기
GenMAC	0x08	Key를 이용한 MAC 생성
Write	0x12	Sector Data 쓰기
VerifyMAC	0x28	Key를 이용한 MAC 검증
Encrypt	0x44	PUF/key를 이용한 암호화
Decrypt	0x46	PUF/key를 이용한 복호화

한 안전성을 유지할 수 있다. 내장된 EEPROM은 Chip의 configuration을 정리하는 setup area와 user가 data를 저장할 수 있는 data area로 구분하여 사용의 편의성을 높였다. 이때 data area에 저장되는 data는 VIA-PUF로 암호화가 되어 저장되는 secure-memory 구조를 채택하였다.

Data의 경우 암호화하여 읽기 또는 쓰기 기능을 제공하는데 이는 SHA2-256 algorithm을 사용하여 random한 stream data을 생성한 후 생성된 값과 data를 XOR하여 암호화하는 stream cipher 방식으로 수행한다.

PUF 기반의 Secure IC의 Field application으로는 정품 인증, Firmware 복제방지 등이 있다.

Cipher-text = SHA2-256(Nonce || parameter || counter || Key) xor Plain-text

Plain-text = SHA2-256(Nonce || parameter || counter || Key) xor Cipher-text

일반적으로 SHA와 같은 crypto hash algorithm은 one-way방식의 함수이기 때문에 암/복호화를 수행할 수 없는 것으로 알려져 있지만 random stream을 사용하면 암/복호화가 가능하다[11]. 다만 random stream을 만들 때 사용되는 Nonce(random)는 같은 것을 사용하면 known-plain-text attack, replay attack등 공격에 취약하게 되므로 반드시 다른 것을 사용해야 한다. IL005는 TRNG(true-random-number-generator)를 사용하여 Nonce를 항상 새로 생성하므로 안전성을 확보할 수 있다.

IL005의 주요 명령 체계는 〈표 1〉과 같다

주요 적용 application은 authentication 및 anti-counterfeit로 정품 인증분야에 적용할 수 있고 secure data storage 및 secure boot and secure download등 firmware protection에도 사용 가능 하다. Secure IC로써 다양한 용도로 사용할 수 있도록 확장성도 고려되어 구현되었다. 이를 이용하면 다른 key나 data를 access하기 위한 access condition으로 사용할 수 있다.

Ⅳ. Field Application

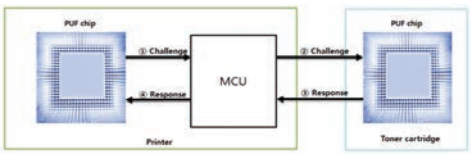
마지막으로 PUF를 적용하여 개발된 Secure IC를 이용하여 적용 가능한 field application을 살펴 보고자 한다.

1. 정품인증

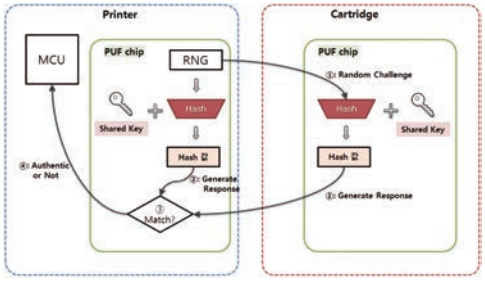
정품인증은 PUF로 보안 안전성을 강화한 chip에 가장 적합한 application으로 printer toner cartridge, printer ink, 공기 청정기 필터, e-cigarette cartridge, mobile phone battery 등에 사용될 수 있다. 사용자의 안전과 제조사의 이익을 위해 가짜 제품을 사용하지 못 하도록 보안 chip이 부착되어 정품 인증을 성공한 경우만 사용할 수 있도록 제한한다.

Printer toner cartridge의 경우 불법 복제/위조카트리지 유통 시장이 수천억 달러 이상으로 보고 있다. 세계 프린터 업계는 불법 복제에 의한 손실을 막기 위해 보안 장치의 대명사인 smart card chip을 적용하여 정품인증을 하고 있으나 결국 key가 노출이 되어 불법 복제를 막지 못하고 있다. 특히 NVM에 대한 공격이 점점 더 짧은 시간 내에 이루어지는 추세여서 key 관리가 점점 더 어려워지고 있다.

Printer는 off-line으로 사용될 수 있으므로 server의



〈그림 7〉 Printer에 사용되는 cartridge 인증



〈그림 8〉 PUF가 적용된 Printer– Cartridge 정품인증 protocol

도움을 받는 on-line 인증을 할 수 없다. 또한 제조사의 카트리지는 자신의 제품 printer에 모두 동작해야 하므로 같은 key를 카트리지에 장착된 chip에 넣어야 한다.

〈그림 7〉은 기존에 적용 되고 있는 printer-cartridge의 인증 방식을 도식화 한 것이다. 그림에서처럼 제품 인증을 위해서는 같은 key를 printer와 카트리지에 넣어야 한다. 따라서 하나의 chip에서 key가 유출되면 가짜 카트리지가 생산 유통될 수 있다.

이를 방지하기 위해 PUF를 적용할 수 있다. 그러나 PUF를 적용함에 있어 direct key 방식으로 사용하려면 모든 카트리지에 PUF Key를 넣어야 하는데 이것은 불가능한 일이다. 따라서 Printer 생산 업체에서 만든 Shared key를 secure-memory 방식으로 주입하고 이때 PUF key를 이용하여 암호화하여 보호한다. 저장된 Shared key를 알아내려면 EEPROM값과 PUF값을 모두 알아내야 한다 〈그림 8〉은 PUF가 적용된 보안 chip을 이용한 Printer– Cartridge 정품인증 protocol을 설명한 것이다. Printer에 PUF chip을 embedding 하고 카트리지에도 chip을 설치하여 상호 인증을 수행해야 인쇄가 되도록 한다. Printer 내의 chip과 카트리지의 chip이 같은 Shared Key를 저장하고 있고 Printer 에서 생성된 challenge에 대한 MAC(message authentication code)을 카트리지에서 생성하고 이를 Printer에서 검증하여 MAC이 일치할 때만 인쇄가 되도록 제한한다.

$$MAC = SHA2\text{-}256(challenge, Key)$$

이 과정이 실행되면 PUF chip 내부에서 PUF key로 암호화된 Shared Key를 복호화 하여 인증을 수행한다.

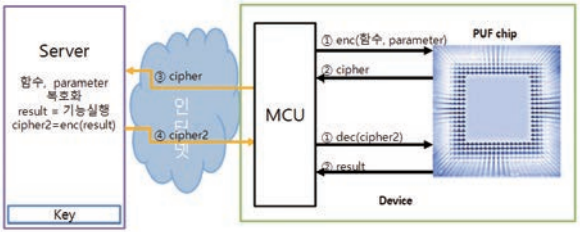
이러한 방식을 보통 challenge-response 방식이라 부르는데 쉽게 표현하면 암구호 방식이라 말할 수 있다. 일반적 암구호는 하루에 하나가 사용되지만 이 방식은 key만 알면 무한히 많은 암구호인 challenage-response pair (CRP)를 만들 수 있다. Random하게 challenge-문어를 생성하여 상대방에게 전달하면 key를 알고 있으면 response-답어를 만들어 전달하고 key를 모르면 이에 대한 연산을 수행할 수 없어 response-답어를 통한 인증에 실패하게 된다. 암구호는 한 번 엿들으면 하루 동안 사용할 수 있지만 PUF 기반의 challenge-response 방식에서는 매 protocol에서 새로운 CRP를 사용한다. 따라서 문어가 계속 변하므로 엿듣기 공격(replay attack)에 안전하다. Challenge-문어와 response-답어가 계속 노출되어도 key를 보호할 수 있는 것은 cryptographic hash 함수의 특성 때문이다.

2. Firmware 복제 방지

두 번째 application은 firmware 복제 방지 분야 이다. Firmware 복제는 많은 제품에서 빈번히 일어나는 것으로 쉬운 불법 복제는 연구 개발자의 제품 개발 의지를 떨어 뜨리는 일이 된다. Re-engineering을 통해 생산된 제품을 분석하여 제품에 사용된 대부분의 부품을 시장에서 구할 수 있고 PCB를 copy한 뒤 복제한 firmware를 올려 그대로 복제품을 생산하는 경우가 많다.

복제 방지 역할을 수행하는 chip이 key를 가지고 있어 key 값을 모르면 복제품을 생산하여 실행할 수 없도록 만드는 일이 firmware 복제 방지의 개념이다. PUF를 적용한 secure IC를 사용한 firmware 복제 방지 방법 중 하나는 on-line server를 이용하는 것이다.

〈그림 9〉는 PUF chip과 on-line server를 이용한 복제방지를 수행하는 과정을 도식화한것이다. On-line



〈그림 9〉 on-line server를 이용한 복제 방지

server에 firmware의 일부 기능을 넣고 chip을 이용하여 암호화된 함수 index와 parameter를 전달하면 on-line server가 기능을 수행하여 결과를 다시 암호화하여 전달하고 chip을 이용하여 복호화하여 함수의 결과로 사용하는 방식이다. 공격자는 on-line server가 어떻게 구성되어 있는지 확인할 방법이 없으므로 함수와 parameter만을 사용하여 함수의 기능을 유추해야 chip과 on-line server없이 firmware를 만들 수 있다. 주요 기능의 함수를 on-line server로 옮겨 놓으면 유추를 통해 복제하는 것은 불가능하다. 결국 chip에 내장된 암호용 key를 알아내지 못 하면 firmware를 복제하여 사용할 수 없다.

이 응용에서는 PUF Key를 direct로 이용하거나 제품 개발 업체에서 만든 key를 주입하여 secure-memory 방식으로 PUF Key를 이용하여 보호하는 방식 모두 사용이 가능하다. 하지만 모든 PUF Key를 on-line server가 저장하는 것은 번거로워 많이 사용되진 않는다.

Ⅴ. 향후 전망 및 결론

요즘은 쉽게 IoT (Internet of Things; 사물 인터넷)이라는 말을 듣게 된다. 이러한 사물 인터넷은 인간의 삶에 편리함을 주는 만큼 한편으로는 위험한 환경에 노출되게 된다. 이러한 위험으로부터 안전해지기 위해서는 점점 더 보안에 대한 중요성이 이야기 될 것이다. 특히 IoT관련해서 논의 되는 많은 기술들은 결국 사람의 개입 없이 사물과 사물간의 communication을 근간으로 하는 기술을 이야기하는 것이기 때문에, IoT 보안의 핵심은 기기간 또는 기기와 서버간의 안전한 '인증'을 의미하는 것이다. 그러나 현재까지 검토되고 사용되는 소프트웨어 기반의 인증 솔루션은 IoT에 있어 보안 취약점으로 논의가 되고 있어 하드웨어 기반의 보안 기술 및 인증 솔루션을 연구 개발하여 더 강력한 보안환경이 적용 될 수 있도록 검토 되어야 할 것이다.

본 글에서는 하드웨어 기반의 보안 기술 중 향후 핵심이 될 수 있는 PUF 기술과 그 기술을 활용한 chip 개발 방법 및 개발된 chip을 이용한 application에 대해 소개하면서 향후 안전한 IoT 환경을 구축 할 수 있는 한 예를 소개하였다. 현재 무인 자동차 시장으로 주목 받고 있는 Automobile 시장에서도 PUF의 사용을 업계 표준으로 정하고 진행 하고 있는 만큼 PUF를 활용한 보안칩 기술 개발과 그 응용분야는 우리나라 System LSI 반도체 시장에 새로운 먹거리로 자리 매김 할 수 있을 것이라 기대한다.

참 고 문 헌

[1] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in Cryptographic Hardware and Embedded Systems-CHES 2007, 2007.

[2] B. Karpinskyy, Y. Lee, Y. Choi, Y. Kim, M. Noh, and S. Lee, "Physically unclonable function for secure key generation with a key error rate of 2E-38 in 45nm smart-card chips," in 2016 IEEE International Solid-State Circuits Conference - (ISSCC) Digest of Technical Papers, 2016, pp. 158-160.

[3] Y. Su, J. Holleman, and B. P. Otis, "A Digital 1.6 pJ/bit Chip Identification Circuit Using Process Variations," IEEE J. Solid-State Circuits, vol. 43, no. 1, pp. 69-77, Jan. 2008.

[4] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, "A physically unclonable function with BER <10-8 for robust chip authentication using oscillator collapse in 40nm CMOS," in 2015 IEEE International Solid-State Circuits Conference - (ISSCC) Digest of Technical Papers, 2015, pp. 1-3.

[5] S. K. Mathew, S. K. Satpathy, M. A. Anders, H. Kaul, S. K. Hsu, A. Agarwal, G. K. Chen, R. J. Parker, R. K. Krishnamurthy, and V. De, "A 0.19pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm CMOS," in 2014 IEEE International Solid-State Circuits Conference - (ISSCC) Digest of Technical Papers, 2014, pp. 278-279.

[6] D. Jeon, J. H. Baek, D. K. Kim, and B.-D. Choi, "Towards Zero Bit-Error-Rate Physical Unclonable Function: Mismatch-Based vs. Physical-Based Approaches in Standard CMOS Technology," in Digital System Design (DSD), 2015 Euromicro Conference on, 2015, pp. 407-414.

[7] Daihyun Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk,

and S. Devadas, "Extracting secret keys from integrated circuits," IEEE Trans. Very Large Scale Integr. VLSI Syst., vol. 13, no. 10, pp. 1200–1205, Oct. 2005.

[8] T. W. Kim, B. D. Choi, and D. K. Kim, "Zero bit error rate ID generation circuit using via formation probability in 0.18 μm CMOS process," Electron. Lett., vol. 50, no. 12, pp. 876–877, 2014.

[9] Ulrich Rü hrmair, Frank Sehnke, Jan Sö lter "Modeling Attacks on Physical Unclonable Functions"

[10] Christoph Bohm, Maximilian Hofer "Physical Unclonable Functions in Theory and Practice"

[11] Jun–cao Li, Chun–ming Li "Research on a Novel Hashing Stream Cipher"

[12] http://wikipedia.org/wiki/Copy_protection

백 종 학

- 1996년 2월 한양대학교 전자공학과 학사
- 2014년 9월~현재 한양대학교 전자컴퓨터통신공학과 석 · 박사과정
- 2004년 7월~2014년 3월 삼성전자 수석연구원
- 2014년 4월~현재 ICTK 연구2실 실장

〈관심분야〉
PUF, Hardware security, Side channel attack

신 광 조

- 994년 2월 광운대학교 이학사(수학)
- 1996년 8월 광운대학교 이학석사(수학, 대수학)
- 1996년 3월 ~ 1998년 7월 백두정보기술 연구원
- 1999년 9월 ~ 2004년 1월 재익정보통신 선임 연구원
- 2004년 2월 ~ 2004년 9월 하이스마텍 선임 연구원
- 2005년 1월 ~ 2006년 12월 한마로 책임 연구원
- 2007년 1월 ~ 2009년 6월 유비닉스 책임 연구원
- 2009년 7월 ~ 현재 ICTK 수석 연구원

〈관심분야〉
Cryptography, Security, PUF, smart card, NFC