정 보 보 호 학 회 지
제28권 제4호, 2018. 8

물리적 복제방지 기능(PUF) 보안 요구사항 및 시험방법 국제표준화 동향

강 유 성*, 오 미 경*, 이 상 재*, 최 두 호*

요 약

다양한 응용이 예상되는 물리적 복제방지 기능(PUF)은 각 디바이스별로 고유하고 복제 불가능한 특징으로 디지털 지문의 역할을 한다. PUF 구현 기법은 다양하게 존재할 수 있지만, 보안 디바이스에 사용하고자 할 때는 공통적으로 만족해야 하는 보안 요구사항이 있다. 기존에는 PUF 출력에 대한 안정성과 유일성의 2개 특성 분석이 주를 이루었으나 최근 ISO/IEC JTC 1/SC 27/WG 3 표준그룹에서는 현실적인 활용상황에 맞게 보다 세분화하여 보안 요구사항을 정의하고 있다. 본 논문에서는 국제표준그룹에서 정의하고 있는 6개의 PUF 보안 요구사항과 시험방법을 소개하고자 한다.

Ⅰ. 서 론

PUF(Physically Unclonable Function, 물리적 복제방지 기능) 기술이 관심을 끌고 있는 이유는 PUF 출력을 이용하여 디바이스 인증, 실시간 키 생성 등을 보다 효율적으로 구현할 수 있을 거란 기대 때문이다[1].

PUF는 반도체 칩의 제조공정 특성에 따라 자연스럽게 나타나는 각 반도체 칩의 물리적인 특성 차이에 기반하여 디바이스의 유일성을 확인할 수 있다는 아이디어에서 출발한 것으로 알려져 있다[2]. 초기 PUF 구현물은 반도체 칩 구현 시 각 소자의 특성에 기반한 아이디어를 FPGA 또는 ASIC으로 구현하여 성능을 확인하는 것이 일반적이었다. 이러한 PUF들은 각 구현대상에 따라 Arbiter-PUF[3], RO(Ring Oscillator)-PUF[4], LoopPUF[5], VIA PUF[6] 등으로 불린다.

이러한 반도체 칩의 물리적 특성을 이용하는 방법 외에 최근에는 상용 디바이스로부터 직접 PUF 출력을 유도하는 기술이 등장하였다. 대표적인 기법은 메모리 기반 PUF 출력 생성 기법으로 SRAM을 사용하는 기법[7]과 DRAM을 사용하는 기법[8] 등이 있다. 상용 디바이스로부터 PUF를 구현하는 기법은 별도의 반도체 칩을 만들 필요가 없기 때문에 기존 디바이스에 바로 적용하여 호환성과 비용절감의 효과를 볼 수 있는 장점이 있다. 그러나 기술 성숙도가 낮아서 PUF 출력이 불안정하여 많은 개선이 필요하다.

PUF 출력을 이용하는 응용 서비스에 관심이 높아지면서 국제표준그룹에서는 PUF 칩 구현 자체보다는 PUF 출력이 보안 시스템에서 사용되기 위해 가져야 하는 보안 요구사항과 PUF 출력에 대한 성능 시험방법을 표준화 주제로 삼고 표준화를 추진 중에 있다. 본 논문에서는 국제표준그룹에서 정의하고 있는 PUF 출력에 대한 보안 요구사항과 시험방법을 소개한다.

이를 위해 본 논문은 다음과 같이 구성되어 있다. 제Ⅱ장은 PUF 관련 국제표준그룹 및 표준문서 현황을 소개하고, 제Ⅲ장은 PUF 입력과 출력을 고려하여 어떤 특성을 분석할 수 있는지 설명한다. 그리고 제 Ⅳ장에서는 국제표준문서에서 정의하고 있는 PUF 보안 요구사항을 항목별로 설명하고, 시험방법은 제Ⅴ장에서 설명한다. 끝으로 제Ⅵ장에서 결론을 맺는다.

Ⅱ. PUF 관련 표준문서 현황

PUF 관련 국제표준화를 진행하고 있는 국제표준그룹은 ISO/IEC JTC 1/SC 27/WG 3이다. SC 27은 IT 보안기술에 대한 국제표준화를 담당하고 있으며 표 1과

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2018-0-00230, (IoT 총괄+1세부) IoT 디바이스 자율 신뢰보장 기술 및 글로벌 표준기반IoT 통합보안 오픈 플랫폼 기술개발 [TrusThingz 프로젝트])
* 한국전자통신연구원 지능보안연구그룹 (youskang, ohmik, leestrike, dhchoi@etri.re.kr)

같이 5개의 작업그룹(WG)으로 구성되어 있다. 이 중 WG 3가 PUF 표준화 그룹이다[9].

SC 27/WG 3에서 표준화가 진행 중인 PUF 관련 표준은 다음 표 2에 보이는 2개 표준문서이다[10]. ISO/IEC 20897-1 표준은 PUF 출력이 가져야 하는 보안 요구사항을 표준화하고 있고[11], ISO/IEC 20897-2 표준은 PUF 출력의 성능 측정을 위한 시험방법을 표준화하고 있다[12].

Ⅲ. PUF 특성 분석 기법

ISO/IEC 20897-1 표준[11]에서는 PUF를 디바이스 안에 구현된 하나의 기능(function)으로 정의하고 있다.

〔표 1〕 SC27 산하 작업그룹(WG)

	영문 명칭	주요 표준화 대상
WG1	Information Security Management Systems	ISMS 관리 기술
WG2	Cryptography and Security Mechanisms	암호 알고리즘, 보안 프로토콜
WG3	Security Evaluation Testing and Specification	보안성 평가, 시험 표준
WG4	Security Controls and Services	보안 서비스
WG5	Identity Management and Privacy Technologies	ID 관리, 프라이버시

〔표 2〕 PUF 관련 표준문서

문서	제목	현단계
ISO/IEC 20897-1	Security requirements, test and evaluation methods for physically unclonable functions for generating non-stored security parameters - Part 1: Security requirements	2nd CD*
ISO/IEC 20897-2	Security requirements, test and evaluation methods for physically unclonable functions for generating non-stored security parameters - Part 2: Test methods	2nd WD**

* CD(Committee Draft):위원회 초안 (위원회 승인은 받았으며, 국가 투표를 진행하는 문서)

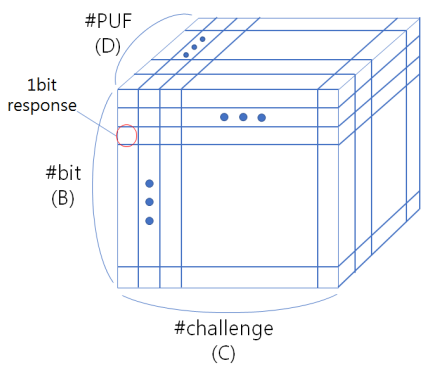
** WD(Working Draft): 작업 초안(위원회 승인 받기 전 작업그룹에서 논의 중인 문서)

이와 함께, PUF는 함수(function)의 의미도 내포하고 있다. 즉 입력을 받고 그 입력에 따라 출력을 내보내는 구조를 가진다. 다음 보이는 식(1) challenge(c)를 입력으로 받아 response(r)를 출력으로 내보내는 PUF를 의미한다.

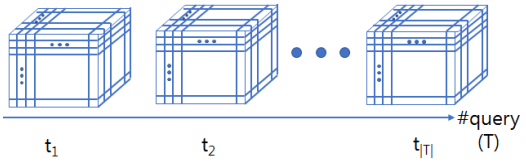
$$r = f(c) \tag{1}$$

표준에서는 PUF를 크게 Extensive PUF와 Confined PUF로 구분하고 있다. PUF는 입력이 되는 challenge, 출력이 되는 response가 쌍을 이루어 구성되는데, 이러한 challenge-response 쌍의 개수가 제한되지 않을 정도로 많은 경우가 Extensive PUF이고, challenge-response 쌍의 개수가 1개 또는 비교적 작게 제한되는 경우가 Confined PUF이다. 기존에 잘 알려진 표현은 Strong PUF와 Weak PUF 이었으나[13], 이는 성능이 좋은 PUF와 성능이 안 좋은 PUF로 오해할 수 있다는 측면이 고려되어 표준에서는 그 표현을 달리 하게 되었다.

PUF 출력의 성능을 평가하기 위한 보안 요구사항을 유도하기 위하여 ISO/IEC 20897-1 표준에서는 디바이스 셋(D), 입력 셋(C), 출력 셋(B)으로 구성된 정육면체 표현도(cube representation)를 사용하며, 추가적으로 시험 셋(T)을 별도로 사용한다. 다음에 보이는 그림 1은 정육면체 표현도이고, 그림 2는 반복 시험을 나타내는 표현도이다. 이는 정육면체 표현도를 사용하여 성능 분석을 시도한 내용[14]을 표준에서 활용한 것으로 각각의 dimension은 다음과 같은 의미를 가진다.



〔그림 1〕 다수 PUF 입력-출력 정육면체 표현도 (D, C, B 관계도)



〔그림 2〕 단일 PUF 반복 시험 표현도 (T, B 관계도)

- Dimension D: “#PUF”는 시험에 사용되는 각기 다른 PUF 디바이스 개수를 나타낸다.
- Dimension C: “#challenge”는 PUF 디바이스에 입력되는 각기 다른 입력 challenge 개수를 나타낸다. 만약 1개의 입력만 허용하는 Confined PUF인 경우에는 Dimension C에서 하나의 블록만 선택되는 것을 의미한다.
- Dimension B: “#bit”는 하나의 challenge로부터 얻어지는 response 비트열을 나타낸다. 만약 128 비트 출력이 요구되는 경우는 Dimension B의 128개 블록이 각각 0 또는 1 값을 가진다.
- Dimension T: “#query”는 단일 PUF 디바이스에서 고정된 하나의 challenge를 반복적으로 시험하는 반복 횟수를 나타낸다.

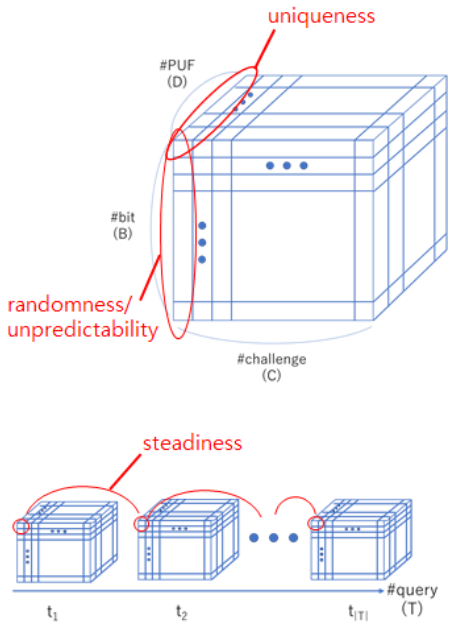
Ⅳ. PUF 보안 요구사항

PUF 출력이 가져야 하는 가장 중요한 특성은 크게 단일 PUF에서의 안정성(Reliability)와 다수 PUF에서의 유일성(Uniqueness)으로 알려져 있다. 그러나 ISO/IEC 20897-1에서는 보다 세분화하고 현실적인 접근을 통해 6가지 보안 요구사항을 정의하고 있다[11]. 이 장에서는 표준에서 정의하고 있는 6개의 보안 요구사항을 설명한다.

표준에서 정의하고 있는 6개의 보안 요구사항 중 정육면체 표현도에서 표현 가능한 특성은 4개이며, 그 관계도는 그림 3에서 보이고 있다.

4.1. Steadiness

Steadiness는 PUF 출력의 안정성 또는 신뢰성을 의미한다. Dimension T에서 PUF 출력의 BER(Bit Error Rate)과 관련된 특성이다. 단일 PUF 디바이스에서 고정된 challenge를 반복적으로 입력하여 동일한 response 비트열이 나오는지 확인하는 척도로 BER이 0



〔그림 3〕 정육면체 표현도와 보안 요구사항 관계도

에 가까울수록 우수한 성능이다. Steadiness라는 표현 외에도 많은 논문에서 Reliability, Robustness, Reproducibility, Stability 등이 동일한 의미로 사용되고 있다.

4.2. Randomness

Randomness는 PUF 출력 자체의 난수성을 의미한다. 특정 PUF 디바이스에서 다수의 challenge 입력에 대해 출력되는 response 비트열이 충분한 난수성을 가져야 한다는 것이다.

4.3. Uniqueness

Uniqueness는 동일한 아이디어로 구현된 다수의 PUF 디바이스들을 구분 지을 수 있는 유일성을 의미한다. 동일한 challenge를 다수의 PUF 디바이스에 입력하여 얻은 출력 response 비트열들이 충분한 엔트로피를 가져야 한다는 것이다. 서로 다른 response 비트열들의 분포는 uniform해야 하며, hamming distance를 계산했을 때 평균이 비트열 크기의 50%에 가까울수록 우수한 성능이다.

4.4. Unpredictability

Unpredictability는 PUF 출력에 대한 예측불가능성을 의미한다. 특정 PUF 구현기법에 대한 설계내용과 구현구조 등이 알려져 있고, 다수의 challenge-response 쌍이 노출되어 있다하더라도 공격자가 임의의 challenge에 대한 response 비트열을 예측할 수 없어야 한다는 것이다. Unpredictability는 Randomness와 유사한 특성으로 볼 수 있으나, 이 요구사항은 머신러닝 기반 모델링 공격 등 다양한 공격에 의한 response 비트열 예측을 방어할 수 있어야 한다는 측면에서 볼 때 보다 더 현실적이고 실용적인 보안 요구사항으로 간주된다.

4.5. Tamper-resistance

Tamper-resistance는 PUF 디바이스 자체에 대한 침투적 또는 비침투적 공격을 포함한 물리적 탬퍼링에 대한 저항성을 의미한다. PUF 디바이스에 대한 부채널 분석과 역공학 분석을 포함한 다양한 물리적 공격으로부터 PUF 출력을 보호할 수 있어야 한다는 것이다.

4.6. Physical unclonability

Physical unclonability는 PUF 고유 특성으로 서로 다른 PUF 디바이스가 동일한 동작 및 동일한 challenge-response 쌍을 가지지 않는 복제불가능성을 의미한다. Unpredictability가 일종의 Mathematical unclonability로 고려될 수 있는 반면, Physical unclonability는 PUF 설계내용, 구현구조 등이 모두 알려져 있다하더라도 동일한 동작과 동일한 출력을 가지는 물리적 복제품을 만들 수 없어야 한다는 것이다.

Ⅴ. PUF 시험방법

ISO/IEC 20897-2 표준에서는 PUF 출력의 성능을 평가할 수 있는 시험방법으로 크게 2개의 수식을 제시하고 있다[12]. 하나는 Intra-Hamming Distance (Intra-HD)이고, 다른 하나는 Inter-Hamming Distance (Inter-HD)이다. Hamming Distance는 2개의 같은 길이를 가진 비트열에서 서로 다른 비트가 몇 개인지를 나타내는 값으로, Intra-HD는 동일한 PUF 디바이스에서 출력된 response 비트열에서의 차이를 의미하며, Inter-HD는 서로 다른 PUF 디바이스로부터 얻은 response 비트열에서의 차이를 의미한다.

5.1. Intra-HD 측정

Intra-HD는 Steadiness 평가와 관련된 측정 메트릭이다. 그림 4는 Intra-HD 측정을 위한 구성도로 단일 PUF에 단일 challenge를 M번 입력하여 M개의 response 비트열을 얻어서 측정함을 보이고 있다.

Intra-HD 측정을 위해 먼저 $\mathbb{D}^{intra}$를 N_{puf}, N_{chal}, N_{query}에 대해 측정된 출력 response로 구성된 3차원 벡터라 하면, 식(1)로부터 다음 식(2)와 같이 유도할 수 있다.

$$\mathbb{D}^{intra} = \left[HD\left(f_i^{(j_1)}(c_k), f_i^{(j_2)}(c_k)\right)\right] \quad (2)$$
$$1 \le i \le N_{puf}, 1 \le k \le N_{chal}, 1 \le j_1 \ne j_2 \le N_{query}$$

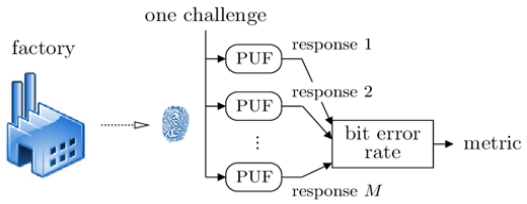
여기서 HD는 Hamming Distance, N_{puf}는 시험대상 PUF 디바이스 최대 개수, N_{chal}은 입력 최대 개수, N_{query}는 시험 반복 최대 횟수를 의미한다.

$\mathbb{D}^{intra}$의 평균 μ^{intra}는 식(3)과 같이 계산된다.

$$\mu^{intra} = E[\mathbb{D}^{intra}] = \frac{2}{N_{puf} * N_{chal} * N_{query} * (N_{query}-1)} \sum\sum\sum \mathbb{D}^{intra} \quad (3)$$

$\mathbb{D}^{intra}$의 표준편차 σ^{intra}는 식(4)와 같다.

$$\sigma^{intra} = \Sigma[\mathbb{D}^{intra}] = \sqrt{\frac{2}{N_{puf} * N_{chal} * N_{query} * (N_{query}-1)-2} \sum\sum\sum (\mathbb{D}^{intra} - \mu^{intra})^2} \quad (4)$$



〔그림 4〕 Intra-HD 측정 구성도

Intra-HD의 평균(μ^{intra})과 표준편차(σ^{intra})가 0에 가까울수록 안정적인 PUF 출력이 나오는 것이며, 이러한 경우에 Steadiness 특성이 우수하다고 평가할 수 있다.

5.2. Inter-HD 측정

Inter-HD는 Uniqueness 평가와 관련된 측정 메트릭이다. 그림 5는 Inter-HD 측정을 위한 구성도로 M개의 PUF 디바이스에 고정된 challenge를 입력하여 M개의 response 비트열을 얻어서 측정함을 보이고 있다.

Inter-HD 측정을 위해 먼저 $\mathbb{D}^{inter}$를 N_{puf}, N_{chal}, N_{query}에 대해 측정된 출력 response로 구성된 3차원 벡터라 하면, 식(1)로부터 다음 식(5)와 같이 유도할 수 있다.

$$\mathbb{D}^{inter} = \left[HD\left(f_{i_1}^{(j)}(c_k), f_{i_2}^{(j)}(c_k)\right)\right] \quad (5)$$
$$1 \le i_1 \ne i_2 \le N_{puf}, 1 \le k \le N_{chal}, 1 \le j \le N_{query}$$

여기서 HD, N_{puf}, N_{chal}, N_{query}는 식(2)에서의 의미와 동일하다.

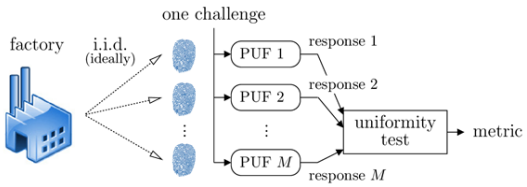
$\mathbb{D}^{inter}$의 평균 μ^{inter}는 식(6)과 같이 계산된다.

$$\mu^{inter} = E[\mathbb{D}^{inter}] = \frac{2}{N_{puf}*(N_{puf}-1)*N_{chal}*N_{query}} \sum\sum\sum \mathbb{D}^{inter} \quad (6)$$

$\mathbb{D}^{inter}$의 표준편차 σ^{inter}는 식(7)과 같다.

$$\sigma^{inter} = \Sigma[\mathbb{D}^{inter}] = \sqrt{\frac{2}{N_{puf}*(N_{puf}-1)*N_{chal}*N_{query}-2} \sum\sum\sum (\mathbb{D}^{inter}-\mu^{inter})^2} \quad (7)$$

Inter-HD의 평균(μ^{inter})은 출력 response 비트열 크기의 절반(예를 들어, 256 비트 출력인 경우 Inter-HD 평균이 128 비트)에 가까울수록 다른 PUF 디바이스들과 차별적인 PUF 출력이 나오는 것이며, 이러한 경우에 Uniqueness 특성이 우수하다고 평가할 수 있다.



〔그림 5〕 Inter-HD 측정 구성도

5.3. 기타 특성 측정

Randomness는 PUF 출력의 엔트로피와 가장 밀접한 관련이 있으며, 이는 미국 NIST의 SP 800-90B[15]와 같은 표준을 준용하여 시험할 수 있다. 측정된 엔트로피가 높을수록 공격자에게 노출되는 PUF 출력 정보가 작아지므로 우수한 성능이라고 판단할 수 있다.

Unpredictability 역시 PUF 출력의 엔트로피와 관련이 있다. 특히 PUF 입력과 출력의 관계인 challenge-response 쌍의 일부가 노출되더라도 공격자가 다른 challenge-response 쌍을 예측할 수 없어야 하는 환경에서는 challenge-response 쌍의 상호상관계수(Cross-correlation coefficient)가 작을수록 우수한 성능이라고 판단할 수 있다.

Tamper-resistance와 Physical unclonability는 물리적 특성과 관련된 보안 요구사항으로 수학적 공식에 기반한 시험이 아닌 실험적 접근이 필요한 측면이 있어서 표준에서는 시험방법에 대한 수학적 계산식을 정의하지 않는다.

Ⅵ. 결 론

본 논문에서는 차세대 하드웨어 보안 솔루션으로 각광받고 있는 물리적 복제방지 기능(PUF) 출력이 가져야 하는 보안 요구사항에 대한 국제표준그룹 활동과 현재 정의된 내용을 살펴보았다. 또한 주요 보안 요구사항의 성능을 평가하기 위하여 국제표준그룹에서 정의하고 있는 계산식을 소개하였다.

국제표준그룹에서 정의하고 있는 PUF 출력에 대한 보안 요구사항은 Steadiness, Randomness, Uniqueness, Unpredictability, Tamper-resistance, Physical unclonability의 6개 항목이며, 이는 기존에 알려져 있는 안정성(Reliability)과 유일성(Uniqueness)을 실제 현실적인 상황에 맞게 세분화하고 확대시킨 것으로 PUF 디바이스에 대한 사이버-물리 공격을 모두 방

어해야 한다는 것을 강조하고 있다. 그리고 주요 계산식으로 Intra-HD와 Inter-HD의 평균과 표준편차를 제시하여 실제 다수의 PUF 디바이스가 사용되는 상황에 적합한 성능 평가 기준이 될 수 있도록 표준화를 진행하고 있다.

본 논문에서 소개하는 국제표준은 PUF 디바이스를 사용하고자 하는 다양한 서비스 환경에 적합한 객관적 보안 요구사항과 시험방법을 제시하고 있기 때문에 향후 PUF 디바이스 상용화를 촉진시키는 긍정적 역할을 할 것으로 기대된다.

참 고 문 헌

[1] G. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation”, In DAC 2007, Proceedings of the 44th annual Design Automation Conference, pp. 9-14. June 2007.

[2] G. Simmons, “A system for verifying user identity and authorization at the point of sale or access”, Cryptologia, vol. 8, no. 1, pp. 1–21, 1984.

[3] D. Lim, J. Lee, B. Gassend, G. 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, 2005.

[4] A Maiti, J. Casarona, L. McHale, and P. Schaumont, “A large scale characterization of RO-PUF”, In HOST 2010, Proceedings of IEEE International Symposium on Hardware-Oriented Security and Trust, pp. 94-99, June 2010.

[5] Z. Cherif, J. Danger, S. Guilley, and L. Bossuet, “An Easy-to-Design PUF based on a single oscillator: the Loop PUF”, In DSD 2012, Proceedings of Euromicro Conference on Digital System Design, September 2012.

[6] 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”, In Electronics Letters, vol. 50, no. 12, pp. 876-877, 2014.

[7] D. Holcomb, W. Burleson, and K. Fu, “Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers”, IEEE Trans. Computers, vol. 58, no. 9, pp. 1198-1210, September 2009.

[8] W. Xiong, A. Schaller, N. Anagnostopoulos, M. Saleem, S. Gabmeyer. S. Katzenbeisser, and J. Szefer, “Run-time Accessible DRAM PUFs in Commodity Devices”, In CHES 2016, Proceedings of Conference on Cryptographic Hardware and Embedded Systems, pp. 432-453, Santa Barbara, August 2016.

[9] ISO/IEC JTC 1/SC 27, https://www.iso.org/committee/45306.html

[10] 강유성, “물리적 복제방지 기능(PUF) 보안 요구사항 국제 표준화 현황”, TTA ICT Standard Weekly, 2018-22(875), May 2018.

[11] ISO/IEC 2nd CD 20897-1, “Security requirements, test and evaluation methods for physically unclonable functions for generating non-stored security parameters – Part 1: Security requirements”, July 2018.

[12] ISO/IEC 2nd WD 20897-2, “Security requirements, test and evaluation methods for physically unclonable functions for generating non-stored security parameters – Part 2: Test methods”, July 2018.

[13] C. Herder, M. Yu, F. Koushanfar, S. Devadas, “Physical Unclonable Functions and Applications: A Tutorial”, Proceedings of IEEE, vol. 102, no. 8, pp. 1126-1141, 2014.

[14] Y. Hori, T. Yoshida, T. Katashita, A. Satoh, “Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs”, In ReConFig 2010, Proceedings of IEEE Conference on Reconfigurable Comput. FPGAs, pp. 298-303, December 2010.

[15] NIST, “Recommendation for the Entropy Sources Used for Random Bit Generation (Second DRAFT)”, NIST Special Publication 800-90B, January 2016.

〈저 자 소 개〉

강 유 성 (Yousung Kang)
종신회원

1997년 2월 : 전남대학교 전자공학과 졸업
1999년 8월 : 전남대학교 전자공학과 석사
2015년 8월 : KAIST 전기및전자공학부 박사
1999년 11월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원/PL
2011년 1월~2012년 4월 : 영국 북아일랜드 QUB 방문연구원
<관심분야> 암호엔지니어링, 키은닉, IoT보안, 드론보안, 부채널 분석 등

오 미 경 (Mi-Kyung Oh)

2000년 2월 : 중앙대학교 전기전자제어공학부 졸업
2002년 2월 : KAIST 전기및전자공학과 석사
2006년 2월 : KAIST 전기및전자공학과 박사
2006년 3월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원
<관심분야> IoT보안, 키은닉, 물리계층 보안, 통신공학 등

이 상 재 (Sangjae Lee)

1999년 2월 : 전북대학교 전자공학과 졸업
2001년 2월 : 전북대학교 전자공학과 석사
2013년 8월 : 충북대학교 정보통신공학부 박사
2000년 12월 ~ 현재 : 한국전자통신연구원 정보보호연구본부 책임연구원
<관심분야> 전자공학, 무선통신 칩, PUF 설계, IoT보안 등

최 두 호 (Dooho Choi)
종신회원

1994년 2월 : 성균관대학교 수학과 졸업
1996년 2월 : KAIST 수학과 석사
2002년 2월 : KAIST 수학과 박사
2002년 1월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원/PL
<관심분야> 암호엔지니어링, 부채널 분석, IoT보안 등