2013년 5월 전자공학회 논문지 제 50 권 제 5 호
Journal of The Institute of Electronics Engineers of Korea Vol. 50, NO. 5, May 2013 http://dx.doi.org/10.5573/ieek.2013.50.5.075

논문 2012-50-5-9

전송선의 크로스토크를 이용한 물리적복제방지기능(PUF) 구현

(Implementation of Physical Unclonable Function(PUF) using Transmission Line Crosstalks)

이 관 희*, 김 승 열*, 조 경 록**, 유 영 갑**

(Kwan-Hee Lee©, Seung-Youl Kim, Kyoungrok Cho, and Younggap You)

요 약

본 논문은 인접한 전송선에서 크로스토크의 크기가 임의의 값을 갖는 것을 이용한 PUF 회로를 제안한다. 기존의 PUF는 동작전압과 온도변화와 같은 환경변화에 따라 출력 값이 일정하지 않기 때문에 신뢰성이 보장되지 않는다. 제안된 PUF는 세 개의 전송선으로 구성되고 두 개의 크로스토크를 발생시킨다. 각각의 전송선에서 발생되는 크로스토크의 크기는 서로 다른 임의의 값을 갖는다. 제안된 회로는 전송선간에 발생되는 각각의 크로스토크의 크기가 서로 다르고 그 크기는 항상 일정한 값을 갖고 크로스토크의 특성으로 동작전압과 온도변화와 같은 환경변화에 강하다. 따라서 제안된 PUF 회로는 요청된 값에 대해 신뢰성 있는 응답 값을 제공한다. 이 회로는 인증 및 암호화 등의 보안시스템에 활용 될 수 있다.

Abstract

This paper presents a PUF circuit based on the randomness of crosstalk magnitudes in adjacent transmission lines. Conventional PUF circuitry suffers the reliability problem where a consistent output value is not guaranteed due to environmental changes, such as power supply voltage and operating temperature. The proposed circuit consists of three transmission lines. The crosstalk difference between two transmission line pairs can be arbitrary. The proposed circuit compares the crosstalk differences between two transmission line pairs, and yields consistent responses. The crosstalk differences are immune to operating environment changes. The proposed PUF circuit provides with reliable responses for given challenges. It can be utilized by security systems such as authentication and encryption.

Keywords : crosstalk, PUF, Physical unclonable function, 보안, 전송선

Ⅰ. 서 론

인터넷 및 네트워크의 발전으로 보안의 중요성이 지속적으로 증가하고 있다. 또한 인터넷 뱅킹, 인터넷 쇼핑 및 공공기관의 증명서 등 네트워크상에서 금전 및 개인 정보 등이 거래되고 활용되기 때문에 이와 같은 주요정보를 보호해야하는 보안 시스템이 요구된다.

Physical Unclonable Function(PUF)는 물리적 복제방지 기능으로 새롭게 대두되고 있는 보안시스템이다[1]. PUF는 지문이나 주민등록번호 같은 개인 식별번호를 제조 공정상의 물리적 편차를 이용하여 전자기적으로 제조하는 방법이다. PUF의 입력은 요청(challenge)이라 하고 출력은 응답(response)이라고 한다. 요청-응답 쌍은 비밀 키나 인증 등으로 활용된다. PUF의 출력은 동일한 제조 공정, 동일한 회로로 구현 하더라도 제조 공정상의 편차로 인하여 결과를 예측할 수 없다. 또한 제조 공정상의 편차는 분석하기 어렵고 결과를 복제하기도 어렵다.

PUF는 유일성, 일관성, 다양성을 요구한다. 그림 1은 PUF의 요구사항 중 유일성과 일관성에 대하여 나타낸다. 유일성은 여러 칩에 동일한 요청비트를 입력하면 서로 다른 응답비트를 출력해야한다. 일관성은 동일한

* 학생회원, ** 정회원, 충북대학교 전자정보대학
(College of Electrical and Computer Engineering Chungbuk National University)
※ 본 논문은 2012년도 충북대학교 기성회 교내 연구비의 지원에 의한 연구결과임.
© Corresponding Author(E-mail:kany27@gmail.com)
접수일자 : 2012년12월10일, 수정완료일 2013년5월6일

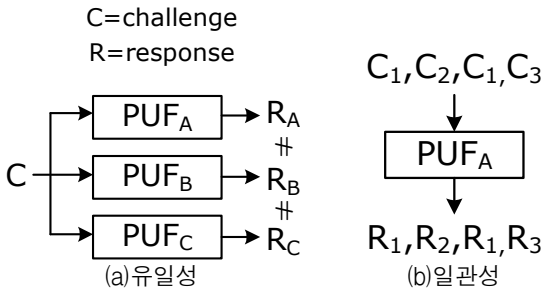


그림 1. PUF의 동작
Fig. 1. Operations of PUF.

칩 내에서 동일한 요청비트를 입력하면 시간이 변해도 동일한 응답비트를 출력해야한다. 다양성은 PUF의 응답비트가 랜덤하게 분포해야한다.

PUF를 이용한 각각의 장치는 동일한 요청에 서로 다른 응답을 갖는 요청-응답 쌍을 가지고 있다. 하나의 장치가 외부의 공격으로 비밀 키가 공개 되더라도 공격당한 장치를 제외하고 다른 장치는 공개된 비밀 키를 사용할 수 있다. 따라서 작은 면적의 회로를 이용하여 원천적으로 복제를 방지할 수 있는 장점이 있다.

기존 PUF의 종류는 크게 메모리 기반, 지연 기반으로 나눌 수 있다. 지연 기반의 아비터 PUF는 두 경로 간의 시간 지연 차이를 이용한다. 길이가 같은 두 개의 경로를 통해 아비터까지 도달하는 신호의 시간 지연 차이에 따라 랜덤 출력 값이 결정된다[2]. 단점은 신호가 환경 변화에 따라 출력 값이 변동되는 것이다. 메모리 기반의 SRAM PUF는 SRAM이 가지고 있는 불안정한 상태를 이용한다. SRAM 내부의 두 인버터의 미세한 비대칭으로 인하여 랜덤 값을 출력한다[3]. 단점으로는 시간과 온도에 따른 환경변화에 따라 출력 값이 변동된다. 기존의 다른 PUF들도 연결선의 신호지연이나 MOSFET의 특성, 회로의 미세한 비대칭성을 이용한다. 최근에 나노스케일의 크로스바 구조를 이용한 PUF가 발표되었다[4].

PUF는 비밀 키 또는 인증 키 등으로 이용되기 때문에 요청-응답 쌍이 항상 일관된 출력을 가져야하고 환경 변화에 둔감해야 한다. 기존의 PUF는 전압과 온도 등 주변 환경 변화에 일관된 출력을 내보내지 못하고 출력 값이 변동되는 문제점을 가지고 있다. 이러한 문제점들로 인하여 PUF의 인증 및 비밀 키 등의 기능이 제대로 수행되지 못한다.

본 논문에서는 크로스토크를 이용한 크로스토크 PUF를 제안한다. 제안된 PUF는 전송선에서 발생하는 제조 공정상의 물리적 편차를 이용한다. 세 개의 전송선 사이에 생기는 두개의 크로스토크는 제조 공정상의 물리적 편차에 의해 크로스토크의 크기가 차이가 발생하도록 만든다. 두 개의 크로스토크의 크기 차이는 센스 앰프를 통하여 비교된다. 제조 후 결정된 전송선의 물리적 구조로 크로스토크는 일관되게 출력된다. 이 회로는 주변 환경 변화에 둔감하여 일관성 있는 출력을 제공하여 안정성이 높은 보안 시스템에 적용할 수 있다.

Ⅱ장에서는 전송선에서 발생하는 크로스토크를 모델링하고 제조 공정상 편차에 따른 크로스토크의 영향을 분석한다. Ⅲ장에서는 크로스토크를 이용한 PUF의 원리와 설계에 대해 설명하고 Ⅳ장에서 결론을 맺는다.

Ⅱ. 크로스토크 모델링 및 영향분석

1. 크로스토크의 모델링

크로스토크는 전송선의 전기 신호가 다른 전송선과 전자기적으로 결합하여 다른 전송선에 악영향을 미치는 것이다. 즉, 다른 회로로부터 바람직하지 않은 에너지 영향을 받음으로써 회로 중에 생기는 간섭으로 잡음 신호를 말한다.

그림 2는 전송선의 구조를 등가 회로로 나타낸 것이다. 전송선의 등가회로의 구성요소는 다음과 같다. 전송선의 구성요소는 저항 R(resistor), 자기 인덕턴스 Ls(self inductor), 자기용량 Cs(self capacitor)가 있다. 그리고 전송선 사이에서 생성되는 상호 인덕턴스 Lm (mutual intuctor)과 상호 용량 Cm(mutual capacitor)이 있다.

제안하는 PUF는 두 개의 크로스토크를 유발시키기 위하여 세 개의 전송선으로 구성된다. 세 개의 전송선은 중간의 트리거선을 중심으로 대칭인 구조이다. 가운데 전송선은 신호를 입력하는 트리거선이고 양 측의 전송선은 크로스토크를 유발시키는 감지선이다. 트리거선

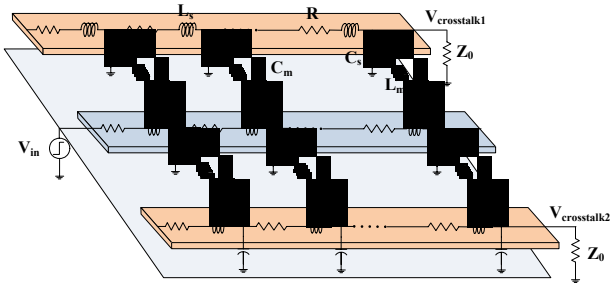


그림 2. 전송선의 등가 회로
Fig. 2. Equivalent circuit of transmission lines.

에 신호를 입력하여 양 측 감지선에 두 개의 크로스토크를 유발시킨다. 양 측 감지선에는 Cm, Cs, Lm, Ls의 영향을 받아 순방향 크로스토크와 역방향 크로스토크가 유발된다. 본 논문에서는 순방향의 크로스토크를 사용하고 순방향 크로스토크 Vcrosstalk1과 Vcrosstalk2를 모델링하였다.

전송선의 특성 파라미터는 다음의 식들을 사용하여 구할 수 있다. 식 (1)은 R, 식 (2)는 Cs[5], 식 (3)은 Cm[6], 식 (4)는 Ls[7], 식 (5)는 Lm[7]을 구하는 수식이다.

수식에 사용된 약어는 다음과 같다. R_{SQ}는 단위길이당 저항, n은 단위 저항의 갯수 , l은 전송선의 길이, W는 전송선의 폭 , H는 전송선의 높이 , T는 전송선의 두께 , S는 전송선 사이의 거리 , ϵ는 유전율, μ는 투자율을 의미한다.

$$R = R_{SQ} * n \tag{1}$$

$$C_s = \epsilon\left[\frac{W}{H} + 0.77 + 1.06\left(\frac{W}{H}\right)^{0.25} + 1.06\left(\frac{T}{H}\right)^{0.5}\right] \tag{2}$$

$$C_m = \epsilon\left[0.03\left(\frac{W}{H}\right) + 0.83\left(\frac{T}{H}\right) - 0.07\left(\frac{T}{H}\right)^{0.222}\right]\left(\frac{H}{S}\right)^{1.34} + \epsilon\left[0.075\left(\frac{W}{H}\right) + 1.4\left(\frac{T}{H}\right)^{0.222}\right] - \epsilon\left[0.075\left(\frac{W}{H}\right) + 1.4\left(\frac{T}{H}\right)^{0.222}\right]\left[1 + \left(\frac{T}{S}\right)\right]^{-1} \tag{3}$$

$$L_s = \frac{\mu_0 l}{2\pi}\left[\ln\left(\frac{2l}{W+T}\right) + \frac{1}{2} + 0.2235\frac{W+T}{l}\right] \tag{4}$$

$$L_m = \frac{\mu_0 l}{2\pi}\left[\ln\left(\frac{2l}{S}\right) - 1 + \frac{S}{l}\right] \tag{5}$$

S 파라미터 매트릭스 식 (6)은 수식 (1)~(5)에서 구한 파라미터들을 단위 길이로 표시하는 방법이다. R, L, C 파라미터들을 다음과 같이 표현할 수 있다[8].

$$[R] = \begin{bmatrix} R & 0 \\ 0 & R \end{bmatrix},$$
$$[L] = \begin{bmatrix} L_s & L_m \\ L_m & L_s \end{bmatrix},$$
$$[C] = \begin{bmatrix} (C_s + C_m) & -C_m \\ -C_m & (C_s + C_m) \end{bmatrix} \tag{6}$$

크로스토크의 크기는 전송선이 가지는 식 (6)의 R, L, C 파라미터에 의하여 결정된다. 파라미터들에 의한 크로스토크의 관계는 식(7)과 같다[9].

$$V_{crosstalk(RLC)} \approx V_{crosstalk(C)} + V_{crosstalk(L)} \tag{7}$$

모든 파라미터들을 고려한 크로스토크 $V_{crosstalk(RLC)}$는 C 성분만을 고려한 $V_{crosstalk(C)}$와 L 성분만을 고려한 $V_{crosstalk(L)}$의 크기의 합과 거의 같다. 크로스토크의 크기에서 R의 영향은 미미하기 때문에 C와 L 성분만을 고려하여 크로스토크를 모델링 한다.

순방향 크로스토크의 진폭은 다음과 같이 구할 수 있다[10]. 식 (8)은 순방향 크로스토크의 최대 전압이고 식 (9)는 순방향 크로스토크의 최소 전압을 구할 수 있다.

$$\alpha = -\frac{VX\sqrt{LC}}{2Tr}\left(\frac{L_m}{L} - \frac{C_m}{C}\right) \tag{8}$$

$$\beta = \frac{V}{4}\left(\frac{L_m}{L} - \frac{C_m}{C}\right) \tag{9}$$

칩에서 환경변화는 주변온도의 변화, 동작 전압의 변화, 습도 및 빛 등의 변화가 있다. 그 중 칩에 가장 큰 영향을 미치는 변화로 온도변화와 동작전압의 변화가 있다. 크로스토크를 이용한 PUF가 환경 변화에 강한 이유는 식 (8), 식 (9)에서 알 수 있다. 두 식에는 온도 파라미터가 없다. 그리고 전압의 경우 동일하게 영향을 받기 때문에 크로스토크의 크기가 환경에 따라 달라질 수 없다.

크로스토크의 크기를 결정하는 W, T, S, H와 같은 물리적 파라미터들은 한번 공정이 제작되면 변하지 않기 때문에 크로스토크의 크기가 변하지 않는다. 그 중 공정에 특히 영향을 많이 받는 W와 S를 이용하여 크로스토크 PUF를 제안한다.

그림 3은 인텔사의 180nm 공정의 구조이다[11]. 실제 공정에서 전송선의 크로스토크를 모델링하기 위한 것이다. 본 논문에서는 크로스토크의 크기를 최대한 크게

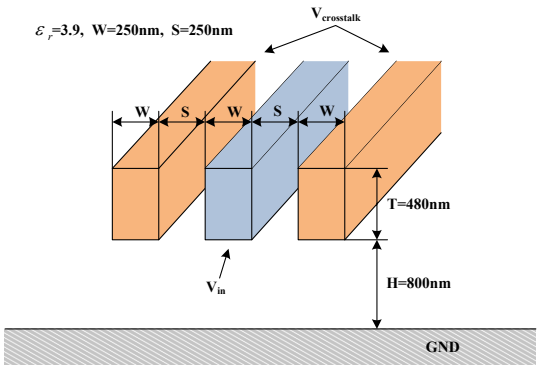


그림 3. 전송선의 구조
Fig. 3. Architecture of transmission lines.

만들어야하기 때문에 전송선과 전송선 사이의 간격을 공정의 최소 크기로 사용하였다. 또한 전송선의 폭도 공정상의 편차를 많이 발생시키기 위해 공정의 최소 크기를 사용하였다.

식 (10)은 전송선이 그림 3의 구조를 가지는 공정에서 두 개의 전송선의 길이가 1mm로 하였을 때를 가정하였다. 두 개의 전송선 사이에서 가지는 R, L, C의 특성 파라미터를 S 파라미터 매트릭스로 구한 것은 다음과 같다.

$$[R]=\begin{bmatrix} 361 & 0 \\ 0 & 361 \end{bmatrix}\begin{bmatrix} \Omega \\ mm \end{bmatrix},$$
$$[L]=\begin{bmatrix} 1.683 & 1.597 \\ 1.597 & 1.683 \end{bmatrix}\begin{bmatrix} nH \\ mm \end{bmatrix},$$
$$[C]=\begin{bmatrix} 189.36 & -96.26 \\ -96.26 & 189.36 \end{bmatrix}\begin{bmatrix} fF \\ mm \end{bmatrix} \quad (10)$$

위의 전송선이 가지는 특성 S 파라미터 매트릭스를 가지고 식 (8)과 식 (9)를 이용하여 그림 4와 같이 크로스토크 모델을 얻었고 시뮬레이션과 비교하였다. 트리거선에 전압 1.8V, 상승시간 10ps의 신호를 입력하였을 때 크로스토크의 최대 진폭은 약 200mV를 얻을 수 있었다.

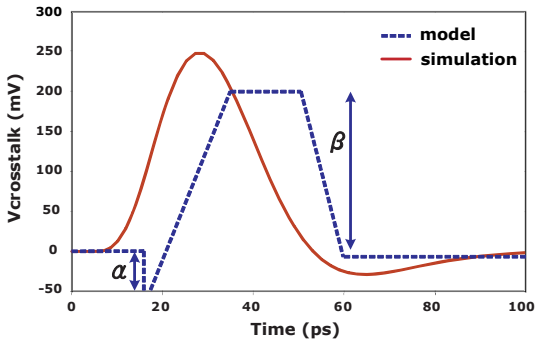
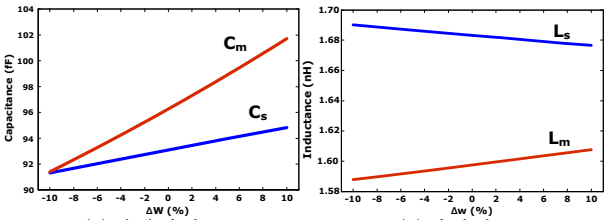


그림 4. 크로스토크 시뮬레이션
Fig. 4. Crosstalk simulation.

2. 공정 편차에 따른 크로스토크 영향 분석

크로스토크 PUF는 전송선이 가지는 제조 공정상의 물리적 편차를 이용한다. 전송선의 폭이 제조 공정상에서 물리적 편차가 발생하게 되면 Cm, Cs, Lm, Ls의 파라미터 값이 변한다. 전송선에서 공정상의 편차는 전송선의 폭이 일정하지 않고 울퉁불퉁하게 편차를 가지므로 모델링하기 어렵다. 따라서 그림 3의 구조를 가지는 전송선에서 전송선 폭의 편차가 평균적으로 일어났을 때를 가정하고 분석하였다. 그림 5는 두 개의 전송선



(a)커패시턴스 (b)인덕턴스

그림 5. 전송선 폭의 편차에 따른 파라미터의 변화
Fig. 5. Paramiter variation reflecting transmission line width deviations.

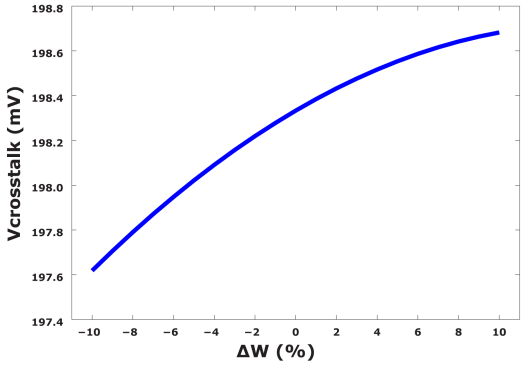


그림 6. 전송선 폭의 편차에 따른 크로스토크의 변화
Fig. 6. Crosstalk variation reflecting transmission line width deviations.

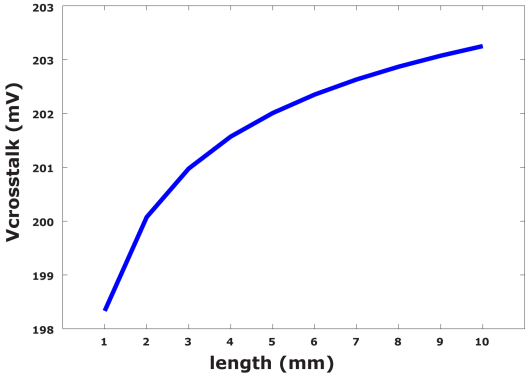


그림 7. 전송선의 길이에 따른 크로스토크의 변화
Fig. 7. Crosstalk variation reflecting transmission line lengths.

중 하나의 전송선 폭이 -10%에서 10%까지의 평균적인 편차를 가질 때 파라미터 값들의 변화를 분석한 그래프이다.

그림 6은 그림 5에서와 같이 전송선의 구조에서 폭이 -10%에서 10%까지의 평균적인 편차를 가질 때 크로스토크의 크기 변화를 분석한 그래프이다.

크로스토크는 전송선의 길이에 따라서도 영향을 받는다. 그림 7은 길이에 따른 크로스토크의 크기를 분석한 그래프이다. 분석 결과를 보면 전송선의 길이가 길

수록 크로스토크의 크기가 증가하는 것을 알 수 있다.

크로스토크 PUF의 특징은 고의로 크로스토크를 유발시켜 이용하기 때문에 길이가 길수록 PUF에 유리한 결과를 갖는다. 하지만 실제 칩 구현에서 10mm의 길이는 매우 크다. 전송선의 길이가 0.1mm의 경우 약 190mV, 0.5mm의 경우 196mV의 크기를 얻을 수 있었다. 전송선의 길이는 클수록 성능엔 유리해지겠지만 전송선의 길이를 1mm로 설정하고 크로스토크 PUF를 구현하면 면적과 성능을 모두 만족시킬 수 있을 것이다.

Ⅲ. 크로스토크 PUF 설계

트리거선과 감지선간의 거리와 길이를 같도록 설계되었을 때 생성된 두 개의 순방향 펄스는 이상적으로 동일 할 가능성이 매우 적다. 칩을 제작할 때 생성되는 전송선의 미세한 공정차이로 인해 트리거선과 감지선사이의 간격이 불규칙하게 되어 두 개의 라인에 유발되는 크로스토크의 영향이 일정하지 않게 된다.

두 개의 크로스토크의 차이는 센스 엠프를 사용하여 두 크로스토크의 차이를 감지한다. 센스 엠프는 전류의 미세한 흐름의 차이도 감지 할 수 있고 대칭적인 구조를 가지고 있기 때문에 온도나 전압의 환경변화에 동시에 영향을 받기 때문에 환경변화에 결과가 변하지 않는다.

그림 8은 제안된 크로스토크 PUF 1 bit 셀의 구조를 나타낸다. 트리거선에 펄스가 인가되면 두 개의 감지선에 크로스토크가 발생한다. 발생된 크로스토크의 진폭은 서로 다른 크기를 갖는다. 서로 다른 크기를 갖는 두 개의 크로스토크 펄스는 센스 앰프의 입력이 되고 펄스의 진폭 차이를 비교하여 출력한다.

두 개의 크로스토크 진폭의 크기를 감지하는 NMOS 센스 엠프의 구조는 그림 9와 같다. 센스 엠프는 이퀄라이저와 센싱회로로 구성된다. 이퀄라이저는 ME1, ME2와 ME3로 구성되고 In1, In2 노드에 입력되는 크로스토크를 정확히 비교하기 위해 양단 노드의 전압을 같게 만들어준다. 크로스토크의 크기는 트랜지스터의 Vth보다 작으므로 센스 앰프를 동작 시킬 수 없기 때문에 In1, In2 노드에 프리차지가 필요하다. 센싱회로는 MS1과 MS2로 구성된다. MS1는 sense1의 신호로 크로스토크 진폭의 차이를 증폭시킨다. MS2는 sence2의 신호를 통해 차이를 극대화 시킨다. MS2의 사이즈는 MS1의 10배이다. 비교된 신호는 각 각의 비대칭 인버터를 통하여 “0”과 “1”로 출력한다.

제안된 크로스토크 PUF의 동작은 그림 10과 같이 시뮬레이션을 거쳐 검증하였다. 크로스토크 입력 양단 노드 In1, In2를 이퀄라이저를 통해 VDD/2의 전압으로 프리차지한다. 다음은 EQ의 신호로 양단의 노드를 플로팅 시킨 상태에서 크로스토크를 입력해준다. 양단 노드는 sense1 신호로 크로스토크의 크기에 따라 미세한 변화를 시작한다. 출력은 sense2 신호로 확실히 구분시킨 뒤 비대칭 인버터를 통해 출력된다. 두 개의 크로스토크 진폭이 차이가 난다면 출력을 “0” 또는 “1”로 만들 수 있다.

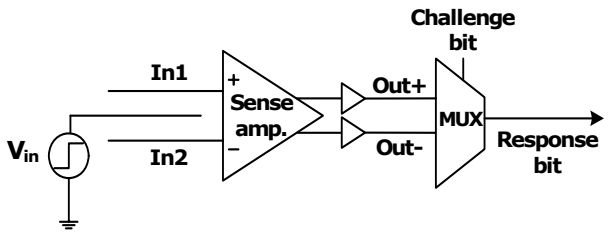


그림 8. 1 bit 크로스토크 PUF 셀 구조
Fig. 8. 1 bit crosstalk PUF cell architecture.

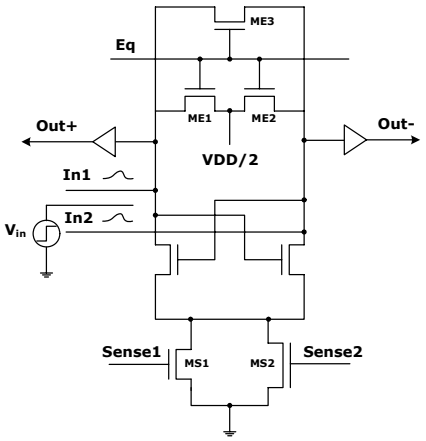


그림 9. 센스 엠프 구조
Fig. 9. Sense amp architecture.

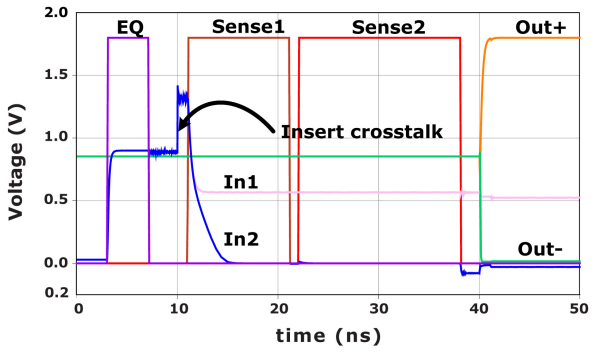


그림 10. 센스 엠프의 시뮬레이션 결과
Fig. 10. Sense amp simulation results.

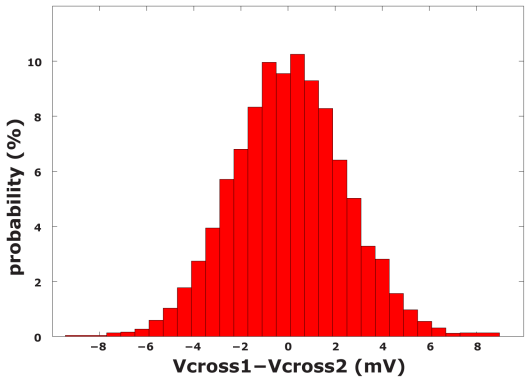


그림 11. 두 크로스토크의 진폭 차
Fig. 11. Amplitude differences between two crosstalk values.

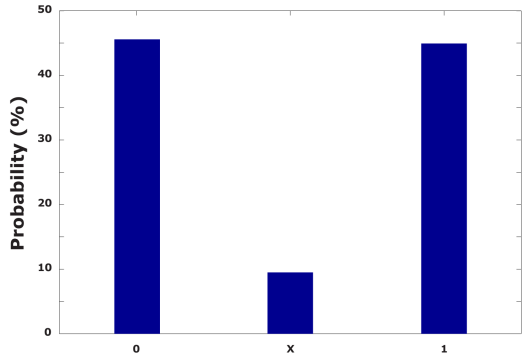


그림 12. 센스 엠프의 예상 출력
Fig. 12. Sense amp expected output.

그림 11은 세 개의 전송선이 공정상의 물리적 편차가 발생하였을 때 두 개의 크로스토크의 진폭 차의 분포를 나타낸다. 세 개의 전송선의 폭이 250nm 일 때 σ=1.5[12] 의 가우시안분포의 편차를 랜덤하게 분포하는 것을 가정하였다. 시뮬레이션은 총 1만회를 진행하였다.

그림 12는 편차가 발생된 전송선에서 두 개의 크로스토크를 감지회로의 입력이 되었을 때 출력 분포를 나타낸다. 크로스토크의 진폭의 차이가 0.25mV이하의 경우 센스 엠프에서 감지하지 한다. 이 경우는 'X'로 표시한다. 'X'의 데이터 출력은 차동 출력이 모두 0이 된다.

그림 13은 크로스토크 PUF를 4 bit로 확장하여 출력의 분포를 분석한 그래프이다. 시뮬레이션은 총 1만회를 진행하였다. 가로축은 출력 패턴이 되고 세로축은 4 bit 크로스토크 PUF의 출력 패턴의 확률이다. 출력 패턴이 고르게 분포하는 것을 알 수 있다. 따라서 크로스토크 PUF가 단일 셀에서 랜덤한 데이터를 가질 뿐 아니라 시스템에서도 출력패턴이 고르게 분포하는 것을 알 수 있다.

이러한 단일 셀의 PUF를 병렬로 구성하면 원하는

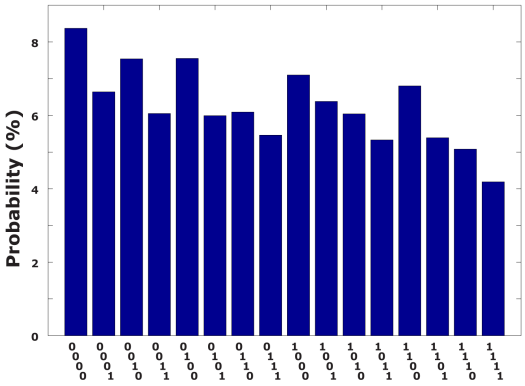


그림 13. 4bit 크로스토크 PUF의 출력 분포
Fig. 13. Output distribution of 4 bit crosstalk PUF.

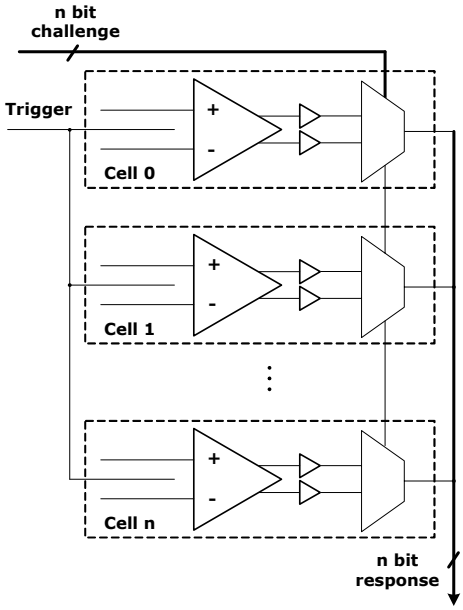


그림 14. PUF 시스템 구조
Fig. 14. The structure of PUF system.

비트의 크기로 확장할 수 있다. 보안 시스템에서 필요로 하는 크기로 비밀 키를 만들 수 있다. 그림 14와 같이 구성하면 n비트의 크로스토크 PUF를 설계할 수 있다. n비트 크로스토크 PUF의 입력은 트리거 신호가 n비트의 요청 비트이다. 출력은 n비트의 요청 비트로 선택된 MUX의 데이터로 n비트의 응답 비트가 된다.

Ⅳ. 결 론

PUF는 물리적 복제가 불가능한 보안 기술이다. 각각의 장치마다 입력 값에 대하여 출력 값의 대응이 모두 다르다. 그 특성을 이용하여 하나의 장치가 외부의 공격으로 비밀 키가 공개 되었을 때 그 장치를 제외한 다른 장치는 안전하다.

기존의 PUF들은 전압과 온도 등의 변화에 따라 대응되는 출력 값이 변할 수 있다. 본 논문에서는 전압과 온도 등의 환경변화에 둔감한 전송선간의 크로스토크를 이용한 PUF를 제안했다.

트리거선과 감지선으로 구성된 전송선들은 제조 공정상에서 오차를 포함하고 있으므로 감지선에 발생하는 크로스토크는 서로 다른 진폭을 갖는다. 크로스토크의 진폭 차이는 센스 앰프를 통해 비교된다. 출력은 MUX를 통하여 요청 비트에 따른 응답 비트를 생성하며 비밀 키로 활용할 수 있다.

제안된 방법으로 PUF를 구현할 경우 환경의 변화에 영향이 적고 안정성이 높은 보안 시스템을 구현할 수 있을 것으로 판단된다.

참 고 문 헌

[1] G. E. Suh, S. Devadas, "Physical unclonable functions for device authentication and secret key generation," *ACM/IEEE 2007*, pp. 9-14, Jun. 2007.

[2] J. W. Lee, L. Daihyun, B. Gassend, G. E. Suh, M. van Dijk and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," *IEEE VLSI Circuits Symposium*, pp. 176-179, Jun. 2004.

[3] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "Physical unclonable functions and public-key crypto for FPGA IP protection," *FPL 2007*, pp. 189-195, Aug. 2007.

[4] P. Lugli, A. Mahmoud, G. Csaba, M. Algasinger, M. Stutzmann and U. Ruhrmair, "Physical unclonable functions based on crossbar arrays for cryptographic applications," *International journal of circuit theory and applications*, 2012.

[5] N. Meijs and J. T. Fokkema, "VLSI circuit reconstruction from mask topology," *Integration*, vol. 2, no. 2, pp. 85-119, 1984.

[6] L. R. Zheng, D. Pamunuwa and H. Tenhunen, "Accurate a priori signal integrity estimation using a dynamic interconnect model for deep submicron VLSI design," *ESSCIRC*, pp. 324-327, sep. 2000.

[7] E. B. Rosa and F. W. Grover, *Formulas and tables for the calculation of mutual and self-inductance*, Washington Government Printing Office, 1916.

[8] T. H. Kim, D. C. Kim and Y. S. Eo, "Signal transient and crosstalk model of capacitively and inductively coupled VLSI interconnect lines," *JSTS*, vol. 7, no. 4, pp. 260-266, Dec. 2007.

[9] J. E. Lorival, D. Deschacht, Y. Quere, T. L. Gouguec and F. Huret, "Additivity of capacitive and inductive coupling in submicronic interconnects," *IEEE DTIS*, pp. 300-304, 2006.

[10] S. H. Hall, G. W. Hall and J. A. McCall, *High-speed digital system design*, John Wiley & Sons New York, pp. 48, 2000.

[11] N. H. E. Weste and D. Harris, *Principle of CMOS VLSI design: A system perspective*, Addison Wesley, 2005.

[12] K. G. Verma, B. K. Kaushik, R. Singh "Effects of process variation in VLSI interconnects - a technical review," *Microelectronics International*, vol. 26, pp. 49-55, 2009.

저 자 소 개

이 관 희(학생회원)

2011년 충북대학교 정보통신공학과 학사 졸업.
2013년 충북대학교 정보통신공학과 석사 졸업.

<주관심분야 : 낸드플래시, PLA, 보안, PUF>

조 경 록(정회원)

1977년 경북대학교 전자공학과 학사 졸업.
1989년 일본 동경대학교 전자공학과 석사 졸업.
1992년 일본 동경대학교 전자공학과 박사 졸업.
1979년～1986년 ㈜금성사TV연구소 선임연구원.
1999년～2005년 Oregon State University 객원교수.
1992년～현재 충북대학교 전자정보대학 교수.
2008년～2011년 World Class University program (충북대학교) 책임.
2010년～현재 IDEC 충북대지역센터장
<주관심분야 : 통신시스템 LSI 설계, 저전력 고속 회로설계, Platform 기반의 SoC 설계>

김 승 열(학생회원)

2002년 충북대학교 정보통신공학과 학사 졸업.
2004년 충북대학교 정보통신공학과 석사 졸업.
2005년 3월～현재 충북대학교 정보통신공학과 박사과정.

<주관심분야 : 디지털 회로설계, Cryptography>

유 영 갑(정회원)

1975년 서강대학교 전자공학과 학사 졸업.
1981년 Univ. of Michigan, Ann Arbor 전기전산학과 석사 졸업.
1986년 Univ. of Michigan, Ann Arbor 전기전산학과 박사 졸업.
1988년～현재 충북대학교 전자정보대학 교수
1986년～1988년 금성반도체(주) 책임 연구원
1993년～1994년 아리조나 대학교 객원 교수
2000년～2001년 오레곤 주립대학교 교환교수
2007년～2008년 일리노이 주립대 객원 연구원
2010년～2011년 충북대학교 전자정보대학장
<주관심분야: VLSI 설계 및 Test, 고속 인쇄회로 설계, Cryptography>