PUF 모델링을 위한 다중 유전체 슬래브의 반사 특성

김태용* · 이훈재*

*동서대학교

Reflection Characteristics from Multiple Dielectric Slabs for PUF Modeling

Tae Yong Kim* · Hoon-Jae Lee*

*Div. of Computer Engineering, Dongseo University

E-mail : tykimw2k@gdsu.dongseo.ac.kr

요 약

PUF는 디지털 기기의 복제 방지 기술로서 동일한 회로라도 회로를 구현하는 공정에 따라 선로지연, 게이트 지연 등이 다른 점을 이용하여 복제 여부를 알아내는 기술이다. 본 연구에서는 코팅 PUF 형태의 물리적 보안 디바이스 구현을 위해 해당 디바이스를 다중 유전체 슬래브로 코팅하고, 그 특성을 확인하기 위해 반사 특성을 계산하여 그 유효성을 검증하였다.

ABSTRACT

PUF technology is to prevent a copy of information from digital device and it can be seen whether cloning through its difference for process of implementation corresponding to wire and gate delay, etc. In this paper, multiple dielectric slabs on digital device is investigated to implement physical crypto device based on coating PUF type and its reflection characteristics is analyzed.

키워드

복제 기술, PUF, 반사 특성, 다중 유전체

Ⅰ. 서 론

정보통신 기술의 발달에 힘입어 세계적인 도시화, 문서의 디지털화, 금융 보안 강화, NFC 도입 증가 등으로 인해 보안용 칩의 도입이 절실히 요구되고 있다[1]. 그러나 보안칩의 기능을 저해하고 정보 침해 공격 또한 정교해지고 있는 추세이다. 주로 데이터 복제, 조작 및 절도 방지를 위해 사용되는 비밀 키와 암호 키를 알아내려는 정교한 도구들과 기법들이 광범위하게 사용되고 있어 스마트카드 보안에 대한 우려도 증대되고 있다[2,3].

PUF(Physically Unclonable Function)[1]는 반도체 공정 편차를 이용해 물리적으로 복제 불가능한 키를 생성하고 시스템 안정성을 높이는 차세대 보안기술이다. 이 기술을 활용하면 역설계, 반 침투형(semi-invasive) 공격 및 비침투형(non-invasive) 공격으로부터 칩을 보호할 수 있다.

일반적으로 암호키가 동작하는 IC 칩 회로는 강한 전자기 신호를 외부로 노출시키는 경향이 있다. 이 경우 암호 칩 근방에서 센서를 활용하여 전자기 신호를 검출하여 암호키를 추정하는 시도를 하게 된다[2,3]. 본 연구에서는 IC 칩 외부로 유출되는 전자기 신호를 억압하기 위한 방안으로서 다중 유전체 슬래브 구조를 가지도록 IC 칩 상부를 코팅하는 방법을 시도하였다.

Ⅱ. 정식화

다중 유전체 슬래브 구조에 대한 반사계수 특성을 계산하기 위해서 그림 1과 같은 구조를 생각한다. 여기서 상대 유전율의 차이에 의해 굴절

율 $n_i = \sqrt{\epsilon_{r,i}}$에 따라 스넬의 법칙을 만족한다. 각 인터페이스 면에서의 반사계수 ρ_i는 다음 식을 이용하여 계산할 수 있다[4,5].

$$\rho_i = \frac{\eta_i - \eta_{i-1}}{\eta_i + \eta_{i-1}} = \frac{n_{i-1} - n_i}{n_{i-1} + n_i},\ i = 1,2,\cdots,M+1 \quad (1)$$

그림 1의 유전체 슬래브 구조의 왼편에서 입사파가 여기되고, 이에 따라 각 인터페이스면에서는 반사파와 투과되는 파가 생기므로 이 관계를 이용하면 반사 특성응답은 $\Gamma_i = E_{i-}/E_{i+}$와 같이 계산할 수 있다. 따라서 각 유전체 슬래브의 특성길이 l_i 등에 의해 반사 응답특성은 다음 식을 이용하여 재귀적으로 계산 가능하다.

$$\Gamma_i = \frac{\rho_i + \Gamma_{i+1} e^{-2jk_i l_i}}{1 + \rho_i \Gamma_{i+1} e^{-2jk_i l_i}},\ i = M, M-1,\cdots,1 \quad (2)$$

본 연구에서는 PUF의 간편 설계를 위하여 그림 2와 같이 IC 회로 기판위에 2개의 유전체 슬래브가 놓인 것으로 가정하였다. PUF 특성을 실현하기 위해서는 IC 위에 놓이는 2개의 유전체 슬래브의 두께 및 상대 유전율을 적절히 결정할 필요가 있다. 본 연구에서는 유전체 슬래브의 두께를 1/4파장 길이로 선택하고, 유전체 슬래브의 상대 유전율의 변화에 따른 반사 응답 특성을 계산하였다.

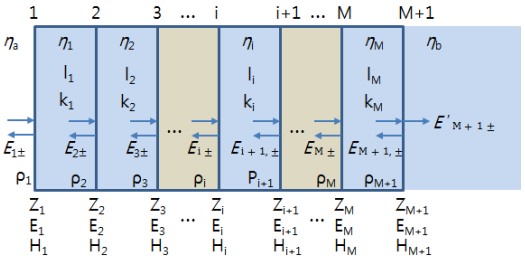

그림 1. 다중 유전체 슬래브 구조

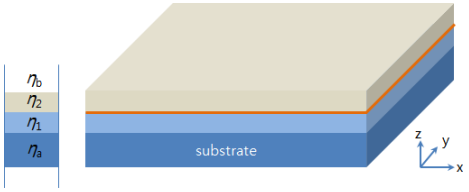

그림 2. PUF를 배치한 IC

III. 계산 결과

최근 NFC 통신을 이용한 보안 솔루션 도입을 고려하여 암호키가 동작하는 IC 칩은 ISM 밴드(2.4-2.48GHz)에서 동작하는 것으로 가정하였다. 이 경우 신호대역의 파장 범위는 120-125mm가 되며, 유전체 슬래브의 상대 유전율에 따른 반사 응답특성을 식 (2)를 이용하여 계산한 결과를 그림 3에 나타내었다.

반사 응답특성을 나타내기 위하여 그래프의 수직 축의 값은 식 (2)와 관련하여 $|\Gamma_1(\lambda)|^2$의 값으로 표시하였다. PUF 특성을 확인하기 위해 일반적으로 많이 사용되는 FR-4 기판으로 구성된 IC 칩 위에 산화 티타늄과 실리콘층을 적재한 경우에는 신호 대역폭에서의 반사 응답특성이 약 40.5%로 나타났다. 이것은 IC 칩에서 발생하는 전자기 신호를 약 40% 정도 억압 가능한 것으로 볼 수 있다.

또 다른 예로서 IC 칩(실리콘 기판) 위에 산화규소와 산화티타늄층을 올린 경우에 대한 반사 응답특성을 계산한 결과를 그림 4에 나타내었다. 이 경우에는 신호 대역 내에서 약 15.5%의 신호 억압 특성을 보여준다.

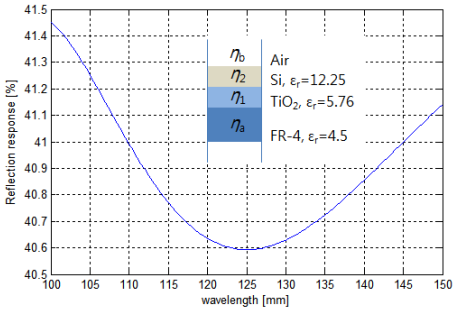

그림 3. 이중 PUF 구조를 가지는 반사 응답특성

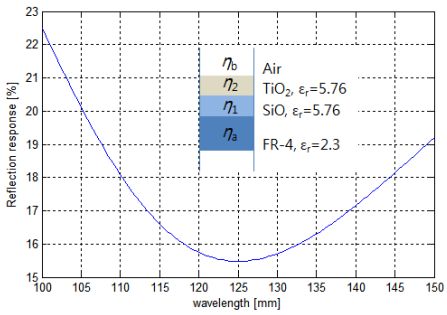

그림 4. 이중 PUF 구조를 가지는 반사 응답특성

IV. 결 론

ISM 밴드에서 동작하는 IC 칩을 대상으로 이중 PUF 층 설계를 하였다. 특히 실리콘 기판위에 적절한 PUF 층을 적재한 경우에는 신호 대역에서 투과 신호를 억압 가능한 것을 확인하였으며, 이는 침투형 공격에 대한 유효한 대안책이 될 수 있다. 향후 최적화 기법을 통해 보다 억압 성능이 높은 PUF층 설계가 가능할 것으로 판단된다.

참고문헌

[1] NXP Semiconductors offical site, PUF-Physically Unclonable Functions, http://www.nxp.com, 2015.
[2] Young Jin Kang et al., "An Experimental CPA Attack for Arduino Cryptographic Module and Analysis in Software-based CPA Countermeasures", International Journal of Security and Its Applications, Vol. 8, No.2, pp. 261-270, Apr. 2014.
[3] 김태용, 이훈재, "역문제를 이용한 2차원 산란장에서의 소스 추정," 한국정보통신학회 논문지, Vol. 18, No. 6, pp. 1262-1268, 2014.
[4] Sophocles J. Orfanidis, Electromagnetic waves and antenns, No Published ed., 2014.
[5] Matthew N. O. Sadiku, Numerical techniques in electromagnetics (2nd ed.), CRC Press.