복제 방지용 PUF의 전자계 해석 방안

김태용* · 이훈재*

*동서대학교 컴퓨터정보공학부

Consideration of EM Analysis for Unclonnable PUF

Tae Yong Kim* · Hoon-jae Lee*

*Division of Information and Computer Engineering, Dongseo University

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

요 약

본 논문에서는 Debye 분산 특성을 가지는 복제 방지용 PUF를 설계하기 위한 전자계 해석 방안을 고려하였다. 공기층과 분산매질(Si)로 구성된 1차원 모델 내에 전파하는 펄스를 모형하기 위해 FDTD 법을 이용하였다. 불연속 경계면에 도달한 펄스는 일부 반사되고 일부는 투과되어 빠르게 감쇠되는 것으로 나타났다. 그 결과 FDTD법에 의한 Debye 분산특성을 가지는 1차원 복제방지용 PUF 설계 및 모델링에 적용 가능한 것을 확인하였다.

ABSTRACT

In this paper, we present electromagnetic modeling to design unclonable PUFs with frequency-dependant materials corresponding to Debye dispersion. To demonstrate FDTD calculations consider that 1-D problem of pulsed plane wave traveling in free space normally incident on air-silicon material interface. The pulse traveling wave at a vacuum-medium interface were reflected, and transmitted wave were dissipated. As a result, 1-D PUF with Debye dispersion material structure can be applied and FDTD calculation for PUF modeling is a good approximation.

키워드

FDTD, Debye 분산, EM 모델링, DFT

Ⅰ. 서 론

최근 암호 칩뿐만 아니라 디지털 기기의 복제 방지를 위한 기술로서 PUF(Physical Unclonnable Functions)에 관련된 기술이 주목을 받고 있다.

PUF는 디지털 기기의 복제 방지 기술로, 동일한 회로라 하더라도 회로를 구현하는 공정에 따라 선로 지연(Wire Delay), 게이트 지연(Gate Delay) 등이 다른 점을 이용하여 복제 여부를 알아내는 기술이다[1,2]. PUF 유형으로는 광학 PUF, 코팅 PUF, PUF 복제, PUF 모델링, 도전-응답모델 구축 등을 들 수 있다. 그리고 PUF를 이용한 RFID 태그와 상호인증 프로토콜 설계에 관한 응용도 그 활용도가 높아지고 있다[3].

본 연구에서는 디지털 칩에 부식방지 계층(passivation layer)으로서 Si, SiO2 등을 사용하여 절연 및 칩을 보호하는 산화막을 가지는 디바이스를 대상으로 그 물리적 특성을 해석하고 보다 효율적인 설계를 목표로 한다.

Ⅱ. EM 모델링 방안

부식방지 계층을 가지는 디바이스에 대한 해석을 위해서는 일반적인 전자계 해석으로는 어려움이 따른다. 그 이유는 파동이 이동하는 매질이 일반적으로 등방성에 국한되는 경우가 많지만, 부식방지 계층을 형성하는 매질은 주파수에 의존하여

전자파의 에너지를 흡수하거나 반사시키는 특성을 가지기 때문이다.

본 연구에서는 부식방지 계층의 매질을 모델링하기 위하여 파동이 전파되는 매질의 특성이 주파수에 따라 상대 유전율이 변하는 것으로 가정하였다. 이와 같은 특성은 Debye 분산[4,5]으로 알려져 있으며 다음과 같은 식으로 그 분산특성을 모델링할 수 있다.

$$\epsilon_r^* = \epsilon_r + \frac{\sigma}{j\omega\epsilon_0} + \frac{\chi_1}{1+j\omega t_0}, \quad \sigma = \omega\epsilon_0\epsilon'' \quad (1)$$

여기서 ϵ_r은 상대 유전율, σ는 도전율, t_0는 relaxation time, 기타 나머지 항들은 주파수에 관련된 항들이다. 본 연구에서 이용한 Debye 분산 특성은 식(1)을 근거로 그림 1과 같은 특성을 가지는 것으로 가정하였다.

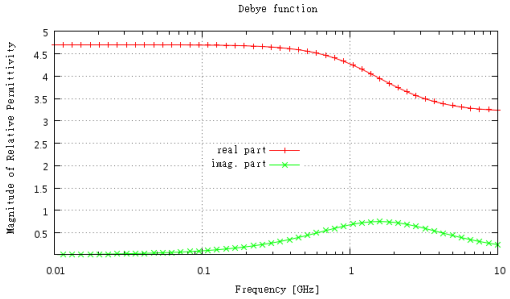


그림 1. 실험을 위한 Debye 분산특성

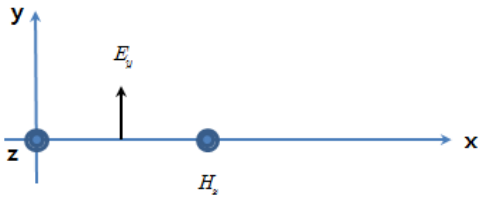


그림 2. 정식화를 위한 전자계 배치

매질의 유전율이 주파수의 함수로 주어지는 분산성 매질에서는 전속밀도 $\boldsymbol{D}$와 전계 $\boldsymbol{E}$가 비례관계를 만족하지 않기 때문에 정식화가 어려움이 따른다. 따라서 분산성 매질을 취급하기 위한 방안으로서 다음과 같은 분극 $\boldsymbol{P}$에 대한 운동방정식을 생각하였다.

$$\frac{d^2\boldsymbol{P}}{dt^2} + \gamma\frac{d\boldsymbol{P}}{dt} + \omega_0^2\boldsymbol{P} = \epsilon_0\omega_p\boldsymbol{E} \quad (2)$$

이와 관련하여 전속밀도 $\boldsymbol{D}$와 전계 $\boldsymbol{E}$는 다음과 같이 주어진다.

$$\boldsymbol{D} = \epsilon_0\boldsymbol{E} + \boldsymbol{P} \quad (3)$$

위에서 언급한바와 같이 분산성 매질을 가지는 전자계 해석을 위해서는 여러 가지 수치해석 방법을 이용할 수 있으나 본 연구에서는 시간영역에서의 차분법으로 알려진 FDTD법[4,5]을 이용하였다. 시간추이에 따른 전계와 자계에 대한 정식화 과정은 다음과 같다. 그리고 정식화와 관련된 전자계 배치는 그림 2와 같다.

$$E_y^{n+1}(i) = coef_1 E_y^n(i) + coef_2 0\Psi^n(i) - coef_3\left[H_z^{n+1/2}(i+1/2) - H_z^{n+1/2}(i-1/2)\right]$$

$$coef_1 = \frac{\epsilon_\infty}{\frac{\sigma\Delta t}{\epsilon_0} + \epsilon_\infty + X^0}$$

$$coef_2 = \frac{1}{\frac{\sigma\Delta t}{\epsilon_0} + \epsilon_\infty + X^0}$$

$$coef_3 = \frac{\Delta t}{\frac{\sigma\Delta t}{\epsilon_0} + \epsilon_\infty + X^0}\frac{1}{\epsilon_0\Delta x}$$

$$H_z^{n+1/2}(i+1/2) = H_z^{n-1/2}(i+1/2) - \frac{\Delta t}{\mu\Delta x}\left[E_y^n(i+1) - E_y^n(i)\right]$$

그림 3. 실험 모델

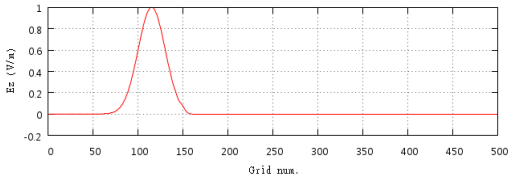
Ⅲ. 실험 및 고찰

실험을 위해서 분산성 매질은 상대 유전율이 10GHz까지의 범위에서 변화하는 것으로 가정하였으며, ϵ_∞는 4.7, σ는 0.01(S/m), t_0는 0.0001로 가정하였다. 또한 계산 공간은 Δ_y=0.13(m) 단위로 전체 500 셀로 이산화하였으며, $250\Delta_y$ 영역부터는 분산성 매질로 설정하였다(그림 3 참조).

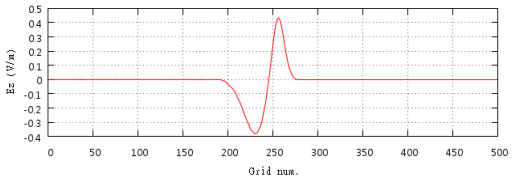
왼편 자유공간 영역에서 가우시안 펄스를 입력하였을 때, 시간 추이에 따른 계산결과는 그림 4에 나타내었다. T=600Δt 시점에서 분산성 매질을 마주하고 일부 펄스는 반사되고 일부는 투과되는 양상을 목격할 수 있다. 이후 T=1000Δt 경과 뒤에는 대부분의 펄스 에너지가 분산성 매질 내에서 소모되어 감쇠되고 있는 것을 알 수 있다.

주파수에 의존하여 분산성 매질 내에서의 펄스 응답을 DFT(Discrete Fourier Transform)를 이용하여 계산한 결과는 그림 5에 나타내었다. 계산

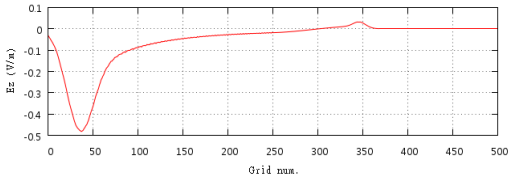
은 T=1500Δt 시점에서 정상상태에 도달하였으며, 각 시간 추이별로 DFT를 수행하였으며 관심 주파수는 800MHz, 2GHz, 5GHz로 설정하였다.



(a) T=300Δt에서의 펄스 전파

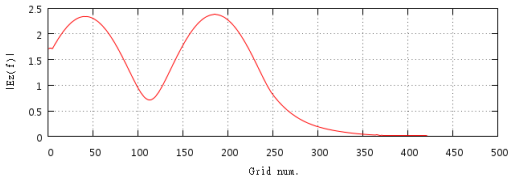


(b) T=600Δt에서의 펄스 전파

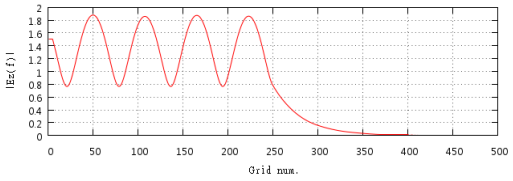


(c) T=1000Δt에서의 펄스 전파

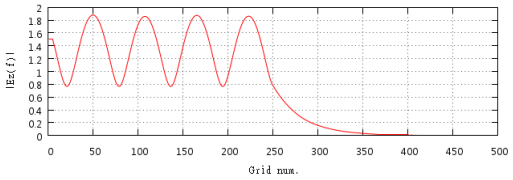
그림 4. 펄스 전파(시간 응답 특성)



(a) 800MHz에서의 주파수 특성



(b) 2GHz에서의 주파수 특성



(c) 5GHz에서의 주파수 특성

그림 5. 정상상태에서의 주파수 응답특성

그림에서 알 수 있듯이, 분산성 매질이 위치한 불연속 경계면에서 일부 펄스들은 반사되고 나머지 펄스는 투과되어 감쇠되고 있는 것을 목격할 수 있다. 특히 5GHz 주파수에서는 투과계수가 0.78이었으며, 분산성 매질이 시작되는 경계면에서 빠르게 감쇠되고 있는 것을 볼 수 있다. 이러한 특성으로 볼 때 EM 공격과 같은 수단을 이용하여 디바이스 내부의 동정을 하거나 디바이스 내부에서의 신호 누설로 인한 신호 해킹 등은 어려울 것으로 판단된다.

본 연구결과를 종합하여 볼 때, EM 공격을 통하여 디바이스 내부의 회로 정보 및 칩 클록 정보 등을 동정하여 수집하는 것은 디바이스를 둘러싼 분산성 매질의 특성으로 인하여 어려울 것으로 보여 그 유효성이 확인되었다고 볼 수 있다.

그러나 실제 디바이스 환경을 고려할 때 2차원 또는 3차원 해석을 통하여 보다 구체적인 모델을 대상으로 연구를 수행할 필요가 있다고 판단된다. 또한 보호 대상으로 볼 수 있는 칩 내부의 회로 패턴 등을 둘러싼 산화막 등이 다층 구조를 하고 있는 복잡한 구조물 등에 대한 해석도 병행할 예정이다.

참고문헌

[1] B. Skori and TU Eindhoven, "Lecture notes: Physical aspects of digital security", 2012.

[2] Ulrich Ruhrmair et al., "Modeling Attacks on Physical Unclonable Functions", CCS'10, October, 2012.

[3] Young Sil Lee, Taeyong Kim, and Hoon Jae Lee, "Mutual Authentication Protocol for Enhanced RFID Security and Anti-Counterfeiting", Proc. of 26th AINA 2012, pp. 558-563, March, 2012.

[4] Matthew N. O. Sadiku, Numerical techniques in electromagnetics (2nd ed.), CRC Press.

[5] K. S. Kunz and R. J. Luebbers, The Finite Difference Time Domain Method for Electromagnetics, CRC Press.