복제 방지용 PUF 모델링을 위한 전자계 해석

김태용* · 이훈재**

Electromagnetic Analysis to Design Unclonable PUF Modeling

Tae Yong Kim* · Hoon-Jae Lee**

지식경제부에서 지원하는 동서대학교 유비쿼터스 어플라이언스 지역혁신센터에서 지원받았음
(과제번호. B0008352)

요 약

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

ABSTRACT

Electromagnetic analysis to design unclonable PUFs with frequency-dependant materials with Debye dispersion was considered. To simulate FDTD calculations consider that 1-D problem of pulsed plane wave traveling in free space normally incident on air-silicon material interface on dielectric substrate. The pulse traveling wave at a vacuum-medium interface was reflected, and transmitted wave was dissipated. As a result, 1-D PUF modeling with Debye dispersion on dielectric substrate structure can be applied and FDTD calculation for PUF modeling is a good approximation.

키워드
FDTD, Debye 분산, EM 모델링, DFT

Key word
FDTD, Debye Dispersion, EM Modeling, DFT

* 정회원 : 동서대학교 컴퓨터정보공학부 (주저자, tykimw2k@gdsu.dongseo.ac.kr)
** 정회원 : 동서대학교 컴퓨터정보공학부

접수일자 : 2012. 06. 01
심사완료일자 : 2012. 06. 01

Open Access http://dx.doi.org/10.6109/jkiice.2012.16.6.1141

Ⅰ. 서 론

최근 암호 칩뿐만 아니라 디지털 기기의 복제 방지를 위한 기술로서 PUF(Physical Unclonnable Functions)에 관련된 기술이 주목을 받고 있다[1,4].

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, SiO_2 등을 사용하여 절연 및 칩을 보호하는 산화막을 가지는 디바이스를 대상으로 그 물리적 특성을 해석하고 보다 효율적인 설계를 기초적인 실험을 진행하였다[4]. 이를 통하여 기초적인 PUF 모델링의 가능성을 확인하였으나, 실제 디바이스 환경을 고려할 경우 유전체 기판위에 PUF 모델링을 고려할 필요가 있어 이에 따른 펄스 전파특성을 고려하였다.

Ⅱ. EM 모델링

2.1. 차분법을 이용한 전자계 해석

일반적으로 매질 특성을 고려한 전자계(E: 전계, H: 자계)는 다음과 같은 맥스웰 방정식으로 나타낼 수 있다.

$$\frac{\partial \boldsymbol{D}}{\partial t} = \nabla \times \boldsymbol{H} \tag{1}$$

$$\frac{\partial \boldsymbol{H}}{\partial t} = -\frac{1}{\mu_0} \nabla \times \boldsymbol{E} \tag{2}$$

여기서 $\boldsymbol{D}$는 전속밀도(electric flux density)를 나타내며, μ_0는 자유공간에서의 투자율을 의미한다. 또한 주파수 의존성을 가지는 매질 내에서는 전속밀도를 표현하면 다음과 같다.

$$\boldsymbol{D}(\omega) = \epsilon_0 \epsilon^*(\omega) \boldsymbol{E}(\omega) \tag{3}$$

이와 같은 관계를 이용하여 차분법을 적용하기 전에 편의상 전자계를 다음과 같이 정규화시켜 표현하는 것도 가능하다.

$$\tilde{E} = \sqrt{\frac{\epsilon_0}{\mu_0}}\, E, \quad \tilde{D} = \sqrt{\frac{1}{\epsilon_0 \mu_0}}\, D \tag{4}$$

따라서 식 (4)의 관계를 이용하여 식 (1)과 (2)에 대입하게 되면 다음과 같은 식으로 나타낼 수 있다.

$$\frac{\partial \tilde{\boldsymbol{D}}}{\partial t} = \frac{1}{\sqrt{\epsilon_0 \mu_0}} \nabla \times \boldsymbol{H} \tag{5}$$

$$\frac{\partial \boldsymbol{H}}{\partial t} = -\frac{1}{\sqrt{\epsilon_0 \mu_0}} \nabla \times \tilde{\boldsymbol{E}} \tag{6}$$

$$\tilde{\boldsymbol{D}}(\omega) = \epsilon^*(\omega) \tilde{\boldsymbol{E}}(\omega) \tag{7}$$

이때 손실을 가지는 유전체 매질을 전파하는 전자계를 고려하기 위해서 상대유전율 ϵ^*은 주파수 영역에서 다음과 같이 주어진다.

$$\epsilon^*(\omega) = \epsilon_r + \frac{\sigma}{j\omega\epsilon_0} \tag{8}$$

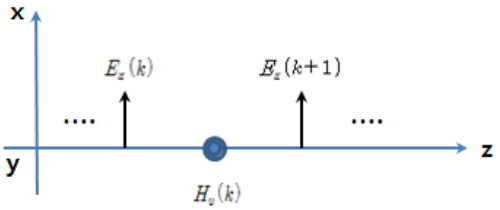


그림 1. 정식화를 위한 전자계 배치
Fig. 1 EM fields for formulation

그림 1을 참고하여 1차원 영역에서의 전자계 정식화를 고려하면, 식 (8)을 식 (7)에 대입했을 때 전속밀도는 다음과 같은 형식으로 표현된다. 여기서 1차원 문제만을 다루기 때문에 전계 및 전속밀도에 대해서는 편의상 아래첨자 x 및 y는 이하 생략하였다.

$$D(\omega) = \epsilon_r E(\omega) + \frac{\sigma}{j\omega\epsilon_0} E(\omega) \quad (9)$$

식 (9)의 경우, Fourier 이론을 적용하면 다음과 같이 시간영역에서의 전속밀도 표현식을 얻을 수 있다.

$$D(t) = \epsilon_r E(t) + \frac{\sigma}{\epsilon_0} \int_0^t E(t')dt' \quad (10)$$

시간영역에서의 차분식을 얻기 위해 시간 샘플 Δt를 이용하여 식 (10)을 변형하면 다음과 같은 축차 연산식을 얻을 수 있다.

$$D^n = \epsilon_r E^n + \frac{\sigma\Delta t}{\epsilon_0} \sum_{i=0}^{n} E^i \quad (11)$$

식 (11)의 경우, 이전 시각에서 얻은 전계 정보를 현 시점에서의 누적연산을 취할 필요가 있으므로 축차연산을 수행하기에는 부적합하므로 다음과 같이 식을 약간 수정할 필요가 있다.

$$D^n = \epsilon_r E^n + \frac{\sigma\Delta t}{\epsilon_0} E^n + \frac{\sigma\Delta t}{\epsilon_0} \sum_{i=0}^{n-1} E^i \quad (12)$$

결과적으로 임의의 시각 $t = n \cdot \Delta t$에서의 전계는 전속밀도를 이용하여 다음과 같이 축차 연산이 가능해진다.

$$E^n = \frac{D^n - I^{n-1}}{\epsilon_r + \sigma\Delta t/\epsilon_0} \quad (13)$$

$$I^n = I^{n-1} + \frac{\sigma\Delta t}{\epsilon_0} E^n \quad (14)$$

마지막으로 자계의 경우는 차분법을 이용하여 다음과 같은 식으로 표현 가능하다.

$$H_y^n(k) = H_y^{n-1}(k) + 0.5(E_x(k) - E_x(k+1)) \quad (15)$$

2.2. 주파수 분산특성을 가지는 매질

앞에서 논의된 시간영역에서의 차분 모델링의 경우는 전자계가 전파하는 매질의 특성은 주파수 분산 특성을 고려하지 않은 경우이다.

본 연구에서는 부식방지 계층을 가지는 디바이스에 대한 해석을 목적으로 하므로 위에서 논의한 정식화 과정만으로는 주파수 분산특성을 고려한 전자계 해석은 어려움이 따른다. 그 이유는 파동이 이동하는 매질이 일반적으로 등방성에 국한되는 경우가 많지만, 부식방지 계층을 형성하는 매질은 주파수에 의존하여 전자기 에너지를 흡수하거나 반사시키는 특성을 가지기 때문이다.

따라서 부식방지 계층의 매질을 모델링하기 위하여 파동이 전파되는 매질의 특성이 주파수에 따라 상대 유전율(ϵ_r^*)이 변하는 것으로 가정할 필요가 있다. 이와 같은 특성은 Debye 분산[4,5]으로 알려져 있으며 다음과 같은 식으로 그 분산특성을 모델링할 수 있다.

$$\epsilon_r^* = \epsilon_r + \frac{\sigma}{j\omega\epsilon_0} + \frac{\chi_1}{1 + j\omega t_0}, \quad \sigma = \omega\epsilon_0\epsilon'' \quad (16)$$

여기서 ϵ_r은 상대 유전율, σ는 도전율, t_0는 relaxation time, 기타 나머지 항들은 주파수에 관련된 항들이다. 본 연구에서 이용한 Debye 분산 특성은 식(16)을 근거로 그림 2와 같은 특성을 가지는 것으로 가정하였다.

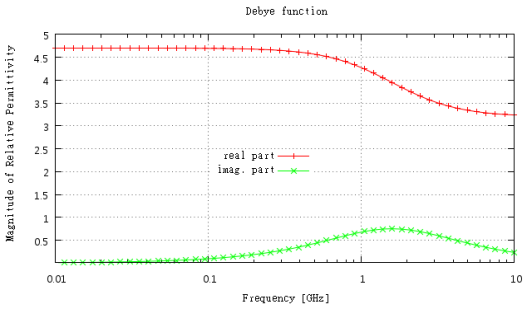


그림 2. 실험을 위한 Debye 분산특성
Fig. 2 Debye dispersion for experiment

매질의 상대유전율이 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.

$$\frac{d^2\boldsymbol{P}}{dt^2}+\gamma\frac{d\boldsymbol{P}}{dt}+\omega_0^2\boldsymbol{P}=\epsilon_0\omega_p\boldsymbol{E} \tag{17}$$

$$\boldsymbol{D}=\epsilon_0\boldsymbol{E}+\boldsymbol{P} \tag{18}$$

위에서 언급한바와 같이 분산성 매질을 가지는 전자계 해석을 위해서는 여러 가지 수치해석 방법을 이용할 수 있으나 본 연구에서는 시간영역에서의 차분법으로 알려진 FDTD법[5,6]을 이용하였다. 시간추이에 따른 전계와 자계에 대한 차분 방정식은 다음과 같다(전자계 배치는 그림 1 참조).

$$E_x^{n+1}(k)=coef_1E_x^n(k)+coef_20\Psi^n(k)$$
$$-coef_3\left[H_y^{n+1/2}(k+1/2)-H_y^{n+1/2}(k-1/2)\right]$$

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

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

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

$$H_y^{n+1/2}(k+1/2)=H_y^{n-1/2}(k+1/2)$$
$$-\frac{\Delta t}{\mu\Delta x}\left[E_x^n(k+1)-E_x^n(k)\right]$$

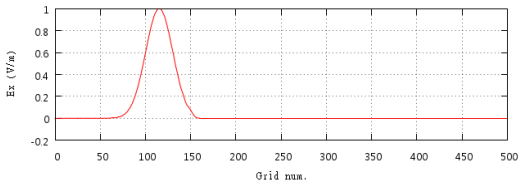
Ⅲ. 실험 결과

3.1. Debye 분산특성을 고려한 전파특성

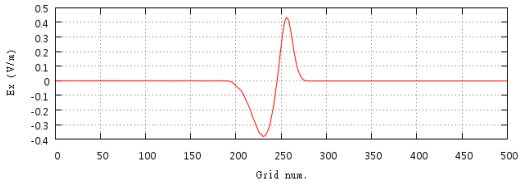
실험을 위해서 분산성 매질은 상대 유전율이 10GHz까지의 범위에서 변화하는 것으로 가정하였으며, ϵ_∞는 4.7, σ는 0.01(S/m), t_0는 0.0001로 가정하였다. 또한 계산 공간은 Δ_z=0.0013(m) 단위로 전체 500 셀로 이산화하였으며, $250\Delta_z$ 영역부터는 분산성 매질로 설정하였다(그림 3 참조).

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.

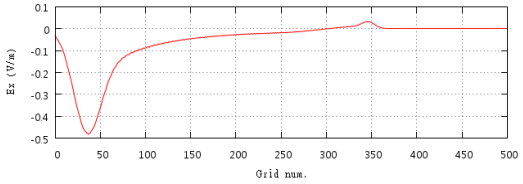
그림 3. Debye 분산특성을 고려한 실험 모델
Fig. 3 Experimental model with Debye dispersion



(a)



(b)



(c)

그림 4. 펄스 전파(시간 응답 특성)
(a) T=300Δt에서의 펄스 전파 (b) T=600Δt에서의 펄스 전파 (c) T=1000Δt에서의 펄스 전파
Fig. 4 Pulse propagation(Time response)
(a) T=300Δt, (b) T=600Δt, (c) T=1000Δt

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, 관심 주파수는 800MHz, 2GHz, 5GHz를 대상으로 각 시간 추이별로 DFT를 계산하여 주파수 응답을 얻었다.

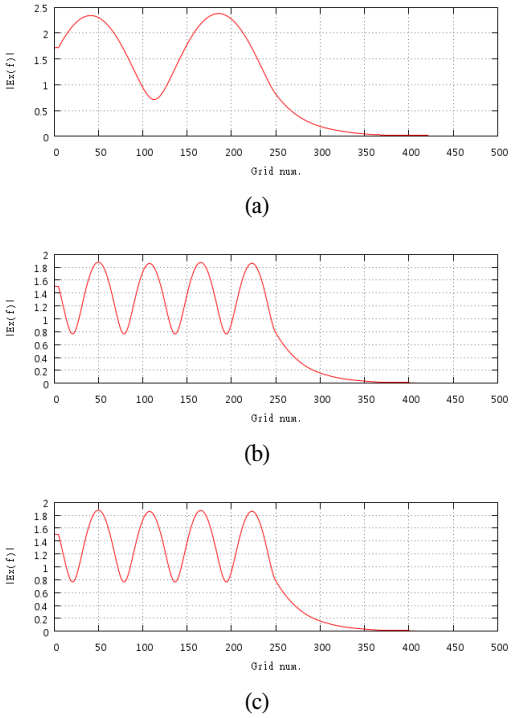


그림 5. 정상상태에서의 주파수 응답특성
(a) 800MHz에서의 주파수 특성 (b) 2GHz에서의 주파수 특성 (c) 5GHz에서의 주파수 특성
Fig. 5 Frequency response in steady state
(a) 800MHz, (b) 2GHz, (c) 5GHz

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.

3.2. 유전체 기판을 고려한 실험결과

그러나 실제 디바이스 환경을 고려할 때 2차원 또는 3차원 해석을 통하여 보다 구체적인 모델을 대상으로 연구를 수행할 필요가 있다고 판단된다.

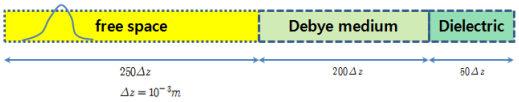


그림 6. 유전체 기판을 포함한 실험 모델
Fig. 6 Experimental model with Debye dispersion including dielectric substrate

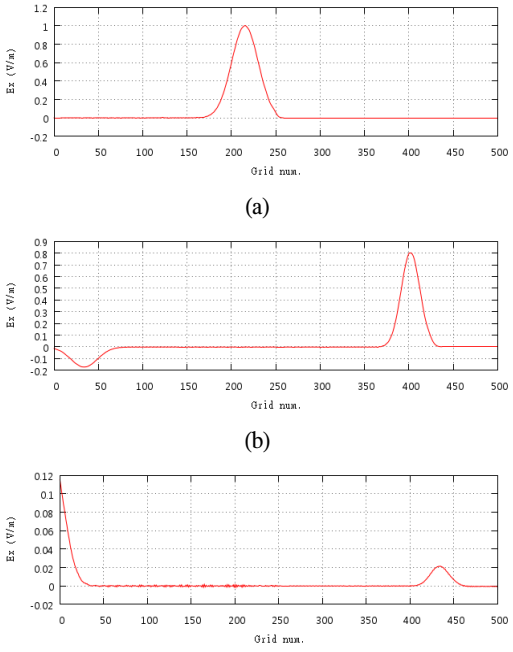
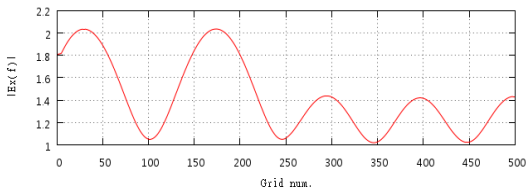


그림 7. 펄스 전파(시간 응답 특성)
(a) T=500Δt에서의 펄스 전파 (b) T=1000Δt에서의 펄스 전파 (c) T=2500Δt에서의 펄스 전파
Fig. 7 Pulse propagation(Time response)
(a) T=500Δt, (b) T=1000Δt, (c) T=2500Δt

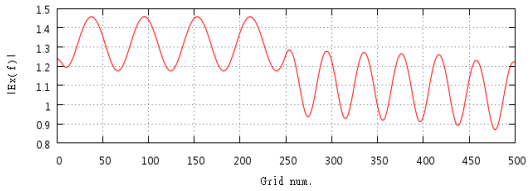
따라서 본 연구에서는 그림 6과 같이 유전체 기판위에 PUF 모델링(Debye 분산특성)을 고려하고 이에 따른 전파특성을 다시 계산하였다. 계산조건은 동일하며, 250Δ_z 영역부터는 분산성 매질로 설정하고 이후 50 Δ_z 영역은 유전체 기판(ϵ_r = 2.6)으로 가정하였다. 또한

이 경우에는 복잡한 매질 특성을 고려하여 전파하는 펄스가 정상상태에 도달하는데 필요한 $2500\Delta t$까지 계산을 수행하였다.

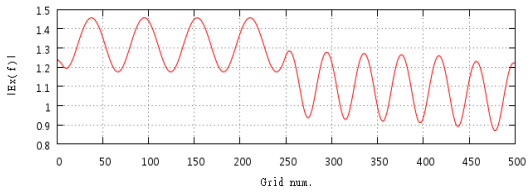
그림 6과 같은 전파 모델을 고려하여 펄스 전파특성을 계산한 결과를 그림 7에 나타내었다. 정상상태에 도달한 경우(그림 (c))를 살펴보면, 분산성 매질 영역에서의 펄스 진폭은 거의 감쇠를 일으켜 내부 디바이스의 상태를 동정하는 것은 어려울 것으로 보이며 이는 비침투형 공격에 유효한 특성으로 판단된다.



(a)



(b)



(c)

그림 8. 정상상태에서의 주파수 응답특성
(a) 800MHz에서의 주파수 특성 (b) 2GHz에서의 주파수 특성 (c) 5GHz에서의 주파수 특성
Fig. 8 Frequency response in steady state
(a) 800MHz, (b) 2GHz, (c) 5GHz

또한 관심 주파수 800MHz, 2GHz, 5GHz에 대해서 동일하게 주파수 응답특성을 계산하였다(그림 8). 그림에서 알 수 있듯이, 높은 주파수에 대해서는 분산성 매질 및 유전체 기판의 매질특성으로 인하여 전계 에너지는 일부 흡수되고 여분의 에너지는 반사되고 있는 것을 볼 수 있다. 이는 그림 5에 나타낸 결과와 비교할 때, Debye 매질 경계면에서의 반사파 진폭은 상대적으로 작아졌지만, 유전체 기판의 특성으로 인하여 전파된 펄스가 일정 진폭의 정재파 형태로 잔류되는 것을 볼 수 있다.

V. 결 론

1차원 영역에서 보호 대상으로 볼 수 있는 칩 내부의 회로 패턴 등을 둘러싼 산화막 등이 다층 구조를 하고 있는 복잡한 구조물을 모델링하고 이에 대한 펄스 전파특성을 계산하였다. 그 결과 디바이스 외부에서 임의로 특정 전자계 신호를 이용한 비침투형 공격에 유효한 PUF 모델링이 가능할 것으로 판단된다.

감사의 글

본 연구는 지식경제부에서 지원하는 동서대학교 유비쿼터스 어플라이언스 지역혁신센터에서 지원받았음(과제번호. B0008352).

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] 김태용, 이훈재, "복제 방지용 PUF의 전자계 해석 방안", 한국정보통신학회 2012년 춘계학술대회논문집, pp. 80-82, April, 2012.

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

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

저자소개

김태용(Tae Yong Kim)

한국정보통신학회 논문지
제12권 제12호 참조

이훈재(Hoon-Jae Lee)

한국정보통신학회 논문지
제15권 제10호 참조