복제 방지용 PUF 모델링을 적용한 전자계 해석

김태용* · 이훈재*

*동서대학교 컴퓨터정보공학부

EM Analysis Applied for Unclonnable PUF Modeling

Tae Yong Kim* · Hoon-jae Lee*

*Division of Information and Computer Engineering, Dongseo University

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

요 약

본 연구에서는 암호 칩의 부식방지를 위해 Si 기판위에 도핑된 산화물질로 구성된 복제 방지용 PUF 모델링 적용을 고려하였다. 이를 통하여 디바이스의 전자계 해석을 위한 정식화 방안을 모색하고 디바이스 복제기술에 대응할 수 있는 안전한PUF를 설계하였다.

ABSTRACT

In this research, the application of PUF modeling which is configured to be doped oxide material on Si substrate and this oxide material is to prevent corrosion of the security chip device. It is to design device replication technology through applying the electromagnetic formulation and its analysis of a device and find ways to PUF design.

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[1-3]. 이와 관련하여 PUF 모델링이 가능한 전자계 해석용 1차원 모델에 대한 그 유효성 검증 및 관련 연구를 진행하고 있다[6-7].

본 연구에서는 이전의 1차원 모델링 과정을 거쳐 보다 현실적인 모델링이 가능하도록 2차원 모델링을 시도하고자 한다. 이를 위해 디지털 칩에 부식방지 계층(passivation layer)으로서 Si, SiO2 등의 재료 특성을 사용하여 절연 및 칩을 보호하는 산화막을 가지는 디바이스를 대상으로 그 물리적 특성을 해석하고 보다 효율적인 PUF 모델링을 통하여 디바이스 보안 설계를 실현하고자 한다.

Ⅱ. EM 해석을 위한 수치 모델링

그림 1에서와 보인바와 같이 디바이스 하부에는 유전체 기판을 가지고, 그 위에 부식방지 계층(분산성 매질 특성을 가짐)을 가지는 디바이스에 대한 해석을 위해서는 일반적인 전자계 해석으로는 어려움이 따른다. 본 연구에서는 부식방지 계층의 매질을 모델링하기 위하여 파동이 전파되는 매질의 특성이 주파수에 따라 상대 유전율이 변하는 Debye 분산[4,5]을 다음 식으로 고려하였다.

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

여기서 ϵ_r은 상대 유전율, σ는 도전율, t_0는 relaxation time, 기타 나머지 항들은 주파수에 관련된 항들이다. 따라서 SiO2와 같은 산화막 물질

에서의 전자계는 디바이스의 동작 주파수에 따라 그 물성이 변화하는 분산 특성을 고려할 필요가 있다.

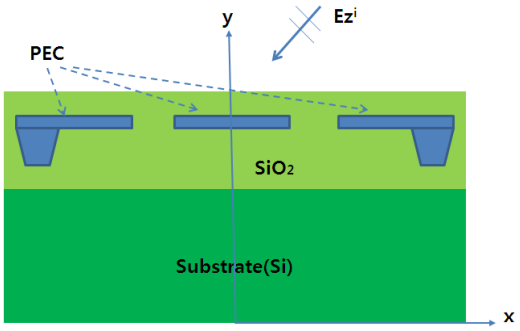

그림 1. PUF 모델링을 고려한 디바이스

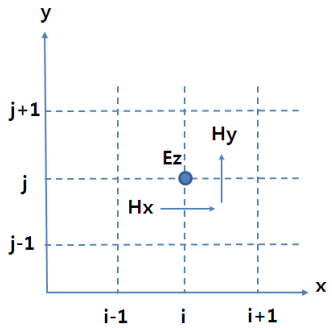

그림 2. 정식화를 위한 전자계 배치

이와 같은 상황에서는 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.

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

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

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

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. 차분법 적용을 위한 전자계 배치는 그림 2를 참고하여 2차원 모델링을 시도하였으며 구체적인 정식화 과정은 참고문헌 [6-7]과 유사하기 때문에 이 문헌을 참고하기 바란다.

그림 1과 같은 디바이스 모델에 대한 전자계 성분은 다음과 같이 일종의 TM(Transverse Magnetic) 모드 해석으로 간주할 수 있다.

$$\begin{aligned}
dz[i][j] &= dz[i][j] \\
&\quad +0.5*(hy[i][j]-hy[i-1][j] \\
&\quad -hx[i][j]+hx[i][j-1]) \\
ez[i][j] &= gaz[i][j]*(dz[i][j]-iz[i][j]) \\
iz[i][j] &= iz[i][j]+gbz[i][j]*ez[i][j] \\
hx[i][j] &= hx[i][j]+05*(ez[i][j]-ez[i][j+1]) \\
hy[i][j] &= hy[i][j]+05*(ez[i+1][j]-ez[i][j])
\end{aligned}$$

위 식들을 이용하여 시간추이에 따른 전계와 자계를 구하게 되며, 필요에 따라 DFT 알고리즘을 이용하여 관심 주파수들에 대한 주파수 응답 특성을 계산 종료와 함께 그 결과를 얻어 디바이스의 특성을 파악할 수 있다.

그림 1에 나타낸 실험 모델을 대상으로 수치실험을 실시하고 주파수 분산특성을 고려한 PUF 모델링에 대한 검증 작업이 필요하다.

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] 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.

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

[7] 김태용, 이훈재, "복제 방지용 PUF 모델링을 위한 전자계 해석", 한국정보통신학회논문지 제16권 제6호, pp. 1141-1147, June, 2012.