JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 6 : 1283~1288 Jun. 2015

비침투형 공격에 강한 다중 유전체 코팅 설계

김태용* · 이훈재

Design of a Multi Dielectric Coating against Non-invaisive Attack

Tae-Yong Kim* · **HoonJae LEE**

Division of Computer Engineering, Dongseo University, Pusan 617-716, Korea

요 약

일반적으로 암호연산이 수행되는 IC 칩 회로는 강한 전자기 신호를 외부로 방사시키는 경향이 있다. 암호 칩 근방에서 루프 안테나와 같은 전력 수집 계측 장비를 활용하면 계측된 전자기 신호에 의해 암호 키의 동정이 가능하다. 이와 같은 비침투형 공격에 대응하기 위한 한 방법으로서 IC 칩 외부로 방사되는 전자기 신호를 억압하기 위해 칩 상부에 다중 유전체 슬래브 구조를 가지도록 구성하는 방법을 도입하였다. 다중 유전체 슬래브는 Bragg 반사특성을 가지도록 적절하게 구성하여 구현하였고 반사응답 특성을 구하여 그 유효성을 검증하였다. 실험결과로서 유전체 코팅의 두께는 2mm로서 수직 입사파에 대한 반사응답 특성은 91% 수준을 달성하였다.

ABSTRACT

In general, IC chip circuit which is operating a cryptographic computation tends to radiate stronger electromagnetic signal to the outside. By using a power detecter such as a loop antenna near cryptographic device, the encryption key can be identified by probing a electromagnetic signal. To implement a method against non-invasive type attack, multi dielectric slab structure on IC chip to suppress radiated electromagnetic signal was introduced. Multiple dielectric slab was implemented by suitably configured to have the Bragg reflection characteristics, and then the reflection response was computed and verified its effectiveness. As a result, the thickness of the dielectric coating was 2mm and the reflection response characteristics for the vertical incidence was achieved to be 91% level.

키워드 : Bragg 반사, 유전체 코팅, PUF, 반사응답 특성

Key word : Bragg reflective, Dielectric coating, PUF, Reflection response

Received 01 May 2015, **Revised** 30 May 2015, **Accepted** 08 June 2015

* **Corresponding Author** Tae Yong Kim(E-mail:tykimw2k@gdsu.dongseo.ac.kr, Tel:+82-51-320-1738)
Div. of Computer Engineering, Dongseo University, Pusan 617-716, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2015.19.6.1283 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

정보통신 기술의 발달에 힘입어 세계적인 도시화, 문서의 디지털화, 금융 보안 강화, NFC 기반 스마트카드 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.

비침투형 공격[4]에는 여러 가지 유형이 있으나 전력 분석 공격에서 SPA(Simple Power Analysis) 또는 DPA (Differential Power Analysis) 공격 대신에 칩의 전자파 방사를 활용하는 전자파분석 공격 기법을 생각할 수 있다. 일반적으로 암호연산이 수행되는 IC 칩 회로는 강한 전자기 신호를 외부로 방사시키는 경향이 있다. 이 경우 암호 칩 근방에서 루프 안테나와 같은 전력 수집 측정 장비를 활용하여 전자기 신호를 검출하여 암호 키를 추정하는 시도를 하게 된다[2,3].

비침투형 공격에 대응하기 위한 한 방법으로서 IC 칩 외부로 방사되는 전자기 신호를 억압하기 위해 칩 상부에 다중 유전체 슬래브 구조를 가지도록 구성하는 방법을 도입할 수 있다[5-8]. 이 경우에는 칩 상부에 위치하는 다중 유전체 슬래브의 두께 및 상대 유전율 등의 선택에 따라 원하는 반사응답 특성을 얻을 수 있다.

본 연구에서는 암호연산이 수행되는 프린트 기판 회로 위에 다중 유전체 슬래브 구조를 형성시키고 암호연산이 수행되는 과정에서 외부로 방사되는 강한 전자기 신호를 억압하기 위한 수단을 연구하였다. 다중 유전체 슬래브는 Bragg 반사특성[9]을 적절하게 구성하여 칩 외부로 방사되는 신호가 대부분 억압될 수 있도록 하였으며 다중 유전체 슬래브의 반사응답 특성을 구하여 그 유효성을 검증하였다.

Ⅱ. 다중 유전체 슬래브

먼저 비침투형 공격에 강한 유전체 코팅을 실현하기 위해 그림 1과 같이 IC 회로 기판위에 n개의 유전체 슬래브가 놓인 것으로 가정하였다. 칩 외부로 방사되는 신호를 억압하는 특성을 얻기 위해 IC 칩 위에 놓이는 n개의 유전체 슬래브의 두께 및 상대 유전율을 적절히 결정할 필요가 있다.

2.1. 다중 유전체 슬래브

우선 다중 유전체 슬래브 구조에 대한 반사계수 특성을 계산하기 위해서 그림 2와 같은 구조를 생각한다. 여기서 상대 유전율의 차이에 의해 굴절률 $n_i = \sqrt{\epsilon_{r,i}}$에 따라 스넬의 법칙을 만족한다. 각 인터페이스 면에서의 반사계수 ρ_i는 다음 식을 이용하여 계산할 수 있다[4,5].

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

여기서 파동 임피던스는 $\eta_i = \eta_0 / n_i = \eta_0 / \epsilon_{r,i}$의 관계를 만족하며, 인터페이스면 i와 $i+1$에서의 전계는 다음과 같이 계산할 수 있다.

$$\begin{bmatrix} E_{i+} \\ E_{i-} \end{bmatrix} = \frac{1}{\tau_i} \begin{bmatrix} e^{jk_i l_i} & \rho_i e^{-jk_i l_i} \\ \rho_i e^{jk_i l_i} & e^{-jk_i l_i} \end{bmatrix} = \begin{bmatrix} E_{i+1,+} \\ E_{i+1,-} \end{bmatrix},\ i = M,\cdots,1 \quad (2)$$

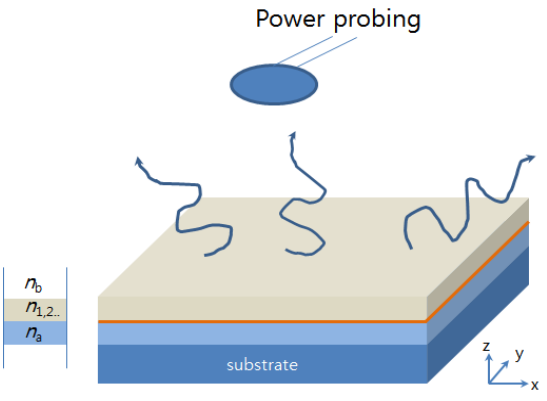

그림 1. PUF 층을 가지는 IC 회로
Fig. 1 IC circuit with a PUF layer

식 (2)에서 $\tau_i = 1+\rho_i$의 관계를 만족하며 그림 2의 우측면에서 어떠한 입사파도 도래하지 않는 것으로 가정하였다. 따라서 $(M+1)$차 인터페이스 면에서의 전계는 결국 식 (3)과 같이 표현 가능하다.

$$\begin{bmatrix} E_{M+1,+} \\ E_{M+1,-} \end{bmatrix} = \frac{1}{\tau_{M+1}} \begin{bmatrix} 1 \\ \rho_{M+1} \end{bmatrix} E'_{M+1,+} \quad (3)$$

그림 2의 유전체 슬래브 구조의 왼편에서 입사파가 여기되고, 이에 따라 각 인터페이스 면에서는 반사파와 투과되는 파가 생기므로 이 관계를 이용하면 반사 특성 응답은 $\Gamma_i = E_{i-}/E_{i+}$와 같이 계산할 수 있다. 따라서 각 유전체 슬래브의 특성 길이 l_i 등에 의해 반사 응답 특성은 다음 식을 이용하여 재귀적으로 계산 가능하다.

$$\Gamma_i = \frac{\rho_i + \Gamma_{i+1} e^{-2jk_i l_i}}{1+\rho_i \Gamma_{i+1} e^{-2jk_i l_i}}, \quad i = M, M-1, \cdots, 1 \quad (4)$$

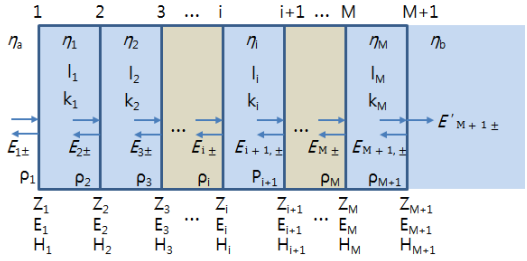

그림 2. 다중 유전체 슬래브 구조
Fig. 2 Structure of multi dielectric slab

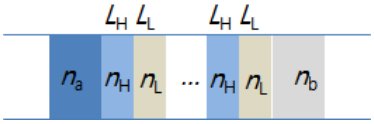

그림 3. Bragg 반사 구조
Fig. 3 Structure of Bragg reflectors

2.2. 비침투 공격의 대응

그림 1에서 유전체 기판 위에 인쇄된 프린트 회로가 암호 연산을 수행하는 경우에는 기판 외부 방향으로 강한 전자기 신호를 방사하게 된다. 공격자의 입장에서는 기판 상부에서 이러한 신호를 루프 안테나와 같은 계측 장비를 이용하여 신호를 캡처하고 역으로 회로 기판 내부에서의 연산 값(암호 키 등)을 추정하는 등의 공격 수법 등이 잘 알려져 있다.

본 연구에서 기판 위 프린트 회로에서 연산되는 과정에서 발생하는 신호를 외부로 유출되지 않도록 기판 상부를 그림 3에 나타낸 Bragg 반사 코팅을 시도함으로써 다중 유전체 슬래브를 통과하는 신호가 억압될 수 있도록 설계하였다. Bragg 반사는 굴절률의 차이에 따라 각 인터페이스 면에서 Fresnel 반사[9]가 발생하고 각 인터페이스 면에서 반사된 모든 파동들이 상호 보강간섭을 가지도록 유도할 수 있다. 그림 3에서 (n_H, n_L)로 구성되는 굴절률 차이를 가지는 유전체 슬래브 구조가 반복하여 여러 층으로 구성되고 각 슬래브의 두께를 적절히 선택함으로써 기판 상부에 있는 회로가 동작하는 과정에서 발생되는 전자기파가 외부로 방출되는 것을 억압할 수 있다. 본 연구에서는 각 인터페이스 면에서의 굴절률의 값은 $n_a = 1.52$, $n_b = 1.0$, $n_H = 1.38$, $n_L = 2.32$로 선택하고 유전체 슬래브의 두께는 $L_H = L_L = 0.25$ mm로 두고 반사응답 특성을 구하였다. 반사응답 특성은 첫 번째 인터페이스 면을 기준으로 식 (4)를 이용하여 다음과 같이 계산하였다.

$$G = |\Gamma_1|^2 \times 100\ [\%] \quad (5)$$

Ⅲ. 실험 결과

최근 스마트카드 및 NFC 통신을 이용한 보안 솔루션 도입이 보편화되고 있는 점을 고려하고, 암호키가 동작하는 IC 칩은 ISM 밴드(2.4-2.48GHz)에서 주로 동작하는 것으로 가정하였다. 이 경우 신호대역의 파장 범위는 120-125mm가 되며, 각 유전체 슬래브의 굴절률에 따른 반사 응답특성을 식 (5)를 이용하여 계산한 결과를 그림 4와 5에 나타내었다.

그림 4와 5의 경우는 다중 유전체 슬래브에 TE (Transverse Electric) 및 TM(Transverse Magnetic)파가 수직 또는 경사 입사하였을 때의 반사응답 특성을 나타낸다. 수직 입사(θ=0도)인 경우 관심 주파수대역에서는 입사파가 다중 유전체 슬래브 구조를 그대로 통과하고 있다. 반면에 입사각이 40도인 경우에는 투과 경로가 수직 입사에 비교하여 상대적으로 길어지는 효과로 인

하여 유전체 내부를 통과하면서 입사파의 전력이 TM파의 경우는 37%, TE파의 경우는 17.5% 정도가 입사파 반대 방향으로 되돌아오는 것을 알 수 있다. 유전체 회로 기판의 상부가 굴절률 $n_a = 1.52$에 해당하는 단순 물질로 구성된 경우에는 회로에서 발생하는 신호가 대부분 회로 외부 방향으로 누출되는 것으로 생각할 수 있어 신호 억압 성능이 달성된 것으로 보기 힘들다.

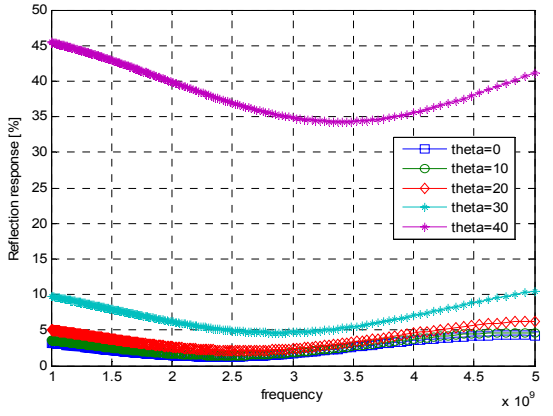

그림 4. 반사응답 특성(입사파: TE wave, Bragg층 없음)
Fig. 4 Reflection response(TE wave incidence without Bragg layers)

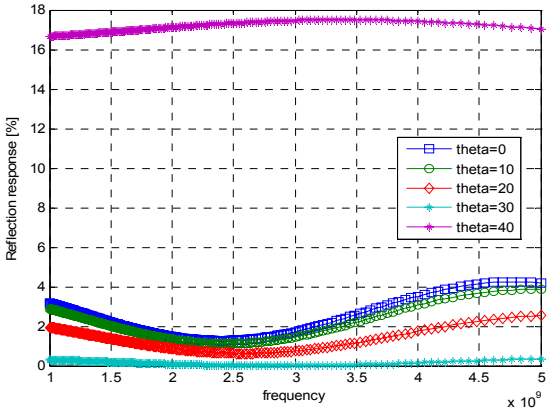

그림 5. 반사응답 특성(입사파: TM wave, Bragg층 없음)
Fig. 5 Reflection response(TM wave incidence without Bragg layers)

다음 실험으로 회로 기판 상부에 이중 Bragg 반사층 $(n_H{:}n_L{:}n_H{:}n_L)$을 삽입한 경우에 대한 반사응답 특성을 계산한 결과를 그림 6과 7에 나타내었다. TE파가 수직 입사한 경우에는 52% 반사, 48% 투과 특성을 보였으며, 경사 입사의 경우에는 최대 89%에 해당하는 반사특성을 달성하였다. 마찬가지로 TM파가 수직 방향으로 입사한 경우에도 관심 주파수 대역에서 53%의 반사특성을 보였다. 그러나 경사 입사의 경우에는 반사특성이 점진적으로 나빠지는 경향을 보였다.

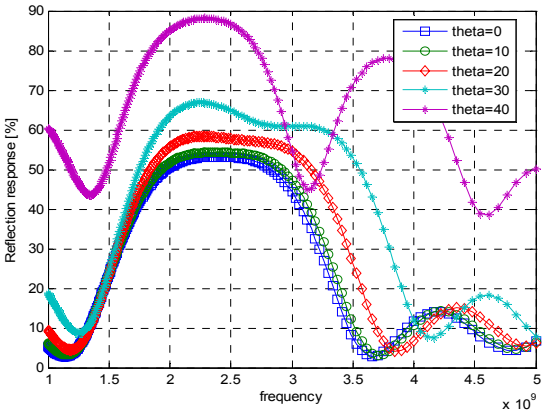

그림 6. 반사응답 특성(입사파: TE wave, 이중 Bragg층 가짐)
Fig. 6 Reflection response(TE wave incidence with double Bragg layers)

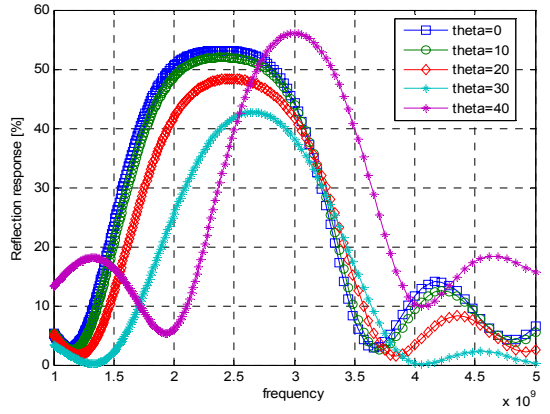

그림 7. 반사응답 특성(입사파: TM wave, 이중 Bragg층 가짐)
Fig. 7 Reflection response(TM wave incidence with Bragg 2-layers)

마지막으로 인쇄 회로 기판 상부에 4중 Bragg 반사층$(n_H{:}n_L{:}n_H{:}n_L{:}n_H{:}n_L{:}n_H{:}n_L)$을 삽입한 경우에 대한 반사응답 특성을 계산한 결과를 그림 8과 9에 나타내었다.

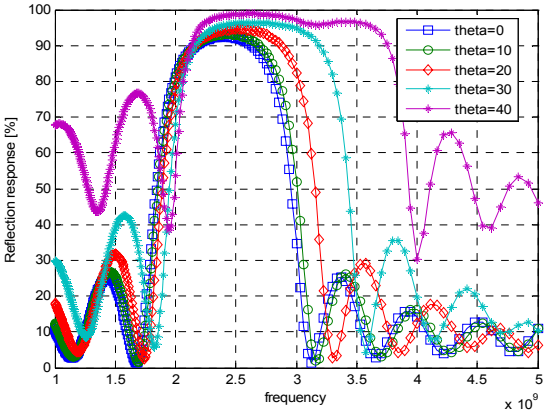

그림 8. 반사응답 특성(입사파: TE wave, 4중 Bragg층 가짐)
Fig. 8 Reflection response(TE wave incidence with Bragg 4-layers)

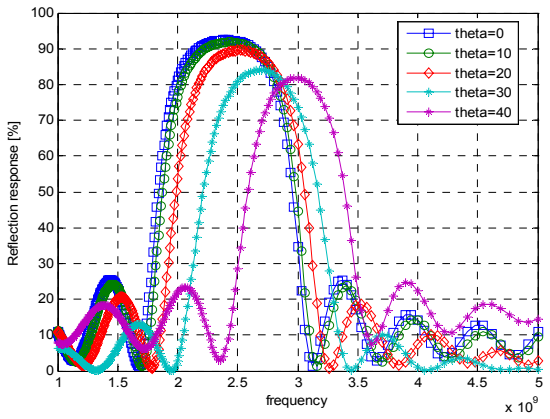

그림 9. 반사응답 특성(입사파: TM wave, 4중 Bragg층 가짐)
Fig. 9 Reflection response(TM wave incidence with Bragg 4-layers)

TE파가 입사한 경우에는 경사 입사를 포함하여 반사 특성이 최소 91%를 보장하는 특성을 보였다. 동일하게 TM파가 입사한 경우에도 수직 입사의 경우에는 91%의 반사특성을 보였지만, 경사 입사(θ=40도)의 경우에는 대부분의 입사파가 외부로 누출되는 것으로 나타났다. 그러나 인쇄회로 기판 바로 위 상부에서 탐침을 이용한 계측장비를 이용한다는 점을 고려하면 매우 양호한 반사응답 특성이 실현된 것으로 생각된다. 4중 Bragge 반사층의 두께는 2mm 수준으로서 비침투형 공격에 대한 효과적인 대안이 될 수 있을 것으로 판단된다.

Ⅳ. 결 론

스마트카드와 같은 ISM 밴드에서 동작하는 IC 칩이 연산되는 과정에서 강하게 방사되는 신호를 억압하기 위한 유전체 코팅을 다중 유전체 슬래브 구조를 통하여 실현하였다.

유전체 코팅을 구성하는 다중 유전체 슬래브의 반복 구조 특성은 Bragg 반사특성을 가지도록 형성시킴으로써 외부로 방사되는 반사응답 특성은 약 90%의 억압특성을 나타냈으며 유전체 코팅의 두께는 2mm로서 실장 가능한 수준으로서 비침투형 공격에 대한 유효한 방법으로 볼 수 있다.

ACKNOWLEDGMENTS

For only the 2nd Author, this research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology. (grant number: NRF-2011-0023076). And it also supported by the BB21 project of Busan Metropolitan City.

REFERENCES

[1] NXP Semiconductors offical site. PUF-Physically Unclonable Functions [Internet]. Available: http://www.nxp.com/.

[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] Tae Yong Kim and Hoon-Jae Lee, “Source identification in 2-dimensional scattering field based on inverse problem,” *Journal of the Korea Institute of Information and Communication Engineering*, Vol. 18, No. 6, pp. 1262-1268, 2014.

[4] Sergei P. Skorobogatov, “Semi-invasive attacks-A new approach to hardware security analysis,” University of Cambridge, Technical Report No. 630(UCAM-CL-TR-630), 2005.
[5] Tae Yong Kim and Hoon-Jae Lee, “Reflection characterics from multiple dielectric slabs for PUF modeling,” in *Proceeding of the Korea Institute of Information and Communication Engineering*, vol. 19, no. 1, pp. 211, 2015.
[6] Sophocles J. Orfanidis, Electromagnetic waves and antenans, No Published ed., 2014.
[7] D. M. Pozar, *Micro Engineering*, Addison-Wesley Pub., 1990.
[8] Matthew N. O. Sadiku, Numerical techniques in electro-magnetics (2nd ed.), CRC Press.
[9] F. A. Jenkins and H. E. White, *Fundamentals of Optics*, 4th ed. Singapore: McGraw-Hill, 1976.

김태용(Tae Yong Kim)

1993년 부경대학교(공학사)
1997년 오카야마대학(공학석사)
2001년 오카야마대학(공학박사)
2002년 ~ 현재 동서대학교 컴퓨터공학부 교수
※관심분야 : 위성통신, 마이크로파 회로해석 및 설계, 마이크로 센서 응용, 센서 네트워크

이훈재(Hoon Jae Lee)

1985년 경북대학교(공학사)
1987년 경북대학교(공학석사)
1998년 경북대학교(공학박사)
1987년 ~ 1998년 국방과학연구소
2002년 ~ 현재 동서대학교 컴퓨터공학부 교수
※관심분야 : secure communication system, side-channel attack, USN RFID security