

## 부 채널 신호에 대한 박막의 영향

선 용 빈<sup>†</sup>

<sup>†</sup>경기대학교 건설·산업대학원 SDM 전공

### Thin Film Effects on Side Channel Signals

Y.B. Sun<sup>†</sup>

<sup>†</sup>Semiconductor Display Mechatronics Program, GS\_CEI, Kyonggi University

#### Abstract

Even if transmissions through normal channel between ubiquitous devices and terminal readers are encrypted, any extra sources of information retrieved from encrypting module can be exploited to figure out the key parameters, so called side channel attack. Since side channel attacks are based on statistical methods, making side channel signal weak or complex is the proper solution to prevent the attack. Among many countermeasures, shielding the electromagnetic signal and adding noise to the EM signal were examined by applying different thicknesses of thin films of ferroelectric (BTO) and conductors (copper and gold). As a test vehicle, chip antenna was utilized to see the change in radiation characteristics: return loss and gain. As a result, the ferroelectric BTO showed no recognizable effect on both shielding and adding noise. Cu thin film showed increasing shielding effect with thickness. Nanometer Au exhibited possibility in adding noise by widening of bandwidth and red shifting of resonating frequencies.

**Key Words** : Side channel attack, shielding, adding noise, nano film, red shift

## 1. 서 론

유비쿼터스 사회에서 일상적으로 사용되는 스마트 카드, 일회용 비밀번호 생성기, 보안 토큰, 알에프 아이디, 휴대정보단말기, 전자여권 등의 유비쿼터스 기기의 정보는 암호화되어 교환된다. 이렇게 암호화 되어 교환되는 정보는 정규채널을 이용하지만, 이 암호화 과정에서 발생하는 또 다른 정보의 원천으로 암호화 모듈이 생성하는 연산 시기, 전력 소모, 전자기파 신호 등이 있다. 이들에 대한 분석을 통해 암호화 모듈이 사용하는 key를 찾아내는 방법을 부 채널 공격이라고 한다[1-2]. 부 채널 공격은 유선 경로 또는 무선 경로를 따라 얻어지는 정보를 분석할 수 있으나 유비쿼터스 기기라는 단어가 의미하듯이 ‘어디에나 있는’ 기기의 특성 상 무선 경로를 통한 부 채널 공격에 대한 연구가 진행되어 왔다[3-4].

부 채널 공격을 방지하기 위한 대응책으로 지연화, 곱셈과 덧셈의 시간 배분, 전력 소모의 균형화, 신호 감소, 소음화, 차폐, 알고리즘 설계 수정, 그리고 이중 암호화 등이 있다. 이러한 부 채널 공격에 대한 대응책은 회로가 보다 복잡해지고, 비 효율적으로 전력을 사용하게 되어 유비쿼터스 기기의 원가 상승 요인이 될 뿐만 아니라, 완결성 측면에서 볼 때 많은 정보 추출을 통해야만 암호 해독이 가능하므로 완벽한 방법이라고 할 수도 없다[5].

이러한 대응책 중에서 회로를 첨가하지 않고 원가 상승을 최소화 하면서 부 채널 정보의 획득을 어렵게 하고, 획득할 수 있는 정보도 난해하게 하여 정보분석에 소요되는 시간을 길게 할 수 있도록, 박막을 적용한 차폐와 소음화 대응책에 대한 효과를 연구하였다. 차폐는 전자파 신호를 차단하는 것이고, 소음화는 방사 주파수 대역폭이 변경되는 것과 공진 주파수의 적색 편이 또는 청색 편이로 추출되는 정보의 양이 많게 만드는 것이다. 유사한 연구개발로 핸드폰의 전력소비와 안테나

<sup>†</sup>E-mail : ybsun@kgu.ac.kr



는 것을 의미한다.

## 2.2. 칩 안테나 제작

기판은 쿼츠(4 inch, 350  $\mu\text{m}$ )와 실리콘(6 inch)을 사용하였으며, 이는 기판의 유전율에 따른 반사손실과 방사특성에 대한 영향을 보기 위함이다.

칩 안테나 제작은 CMOS 반도체 공정을 이용하여, 알루미늄(Al) 5000 Å, TiN 700 Å을 증착한 후에 패터닝하고, 층간 절연막으로 TEOS 5000 Å을 증착한 후에 패터닝하고, 안테나의 단자 부위를(6.2 × 5.5 mm<sup>2</sup>) 포토 레지스트로 패터닝한 후에 Ti 100 Å과 Au 400 Å을 증착하고 lift-off 공정을 거쳐 단자를 마무리 하였다.

## 2.3. 박막 형성

### 2.3.1. 전도체 Cu 박막과 강유전체 BTO 박막 형성

전도체인 Cu 박막은 실리콘 칩 안테나에 적용하였으며, 급전부위와 접지부위를 제외한 부위에 sputter로 증착하였고, 증착 두께는 sputtering 시간으로 변화를 주어 측정한 결과가 각각 0.5, 1.0, 3.0  $\mu\text{m}$  이었다.

강유전체 세라믹인 BTO(Barium Titanate) 박막은 실리콘 칩 안테나에 적용하였으며, 급전부위와 접지부위를 제외한 부위에, sub-micron 크기의 분말을 기판에 고속 충돌시켜 상온에서 고밀도 막을 형성 하는 aerosol deposition법으로 증착하였고[9], 증착 두께는 증착 시간으로 변화를 주어 측정한 결과가 각각 0.1, 1.1, 9.7  $\mu\text{m}$ 이었다.

### 2.3.2. 나노미터 두께의 Au 박막 형성

나노미터 두께의 Au 박막은 쿼츠 칩 안테나에 적용하였으며, 급전부위와 접지부위를 탄탈륨 메탈로 마스크하고 평판 안테나 부위에 evaporator로 증착하였고, QCM(quartz crystal microbalance)으로 측정한 증착 두께는 15 monolayer (약 5 nm) 이었다.

## 2.4. 칩 안테나 반사손실 및 안테나 이득 측정

쿼츠 칩 안테나의 반사손실은 쿼츠 칩 안테나를 직접 SMA 커넥터에 납땜하여 Agilent E8361C Network Analyzer(10 M ~ 67 GHz)로 측정하였다.

또한 실리콘 칩 안테나의 경우에는 칩 안테나와 SMA 커넥터 사이에 특성 임피던스 50  $\Omega$ 인 CPW PCB를 사용하였다. PCB는 크기가 12.4 × 22.0 mm이고, 접지 단자의 크기는 4.4 × 10.0 mm이고, 단자와 단자 사이의 간격은 0.55 mm이다. 실리콘 칩 안테나를 PCB의 칩의 두께만큼 판 자리에 정렬하여 납땜 연결

하고, PCB 단자와 SMA 커넥터를 납땜하여 Agilent N5230A Network Analyzer(10M~40GHz)로 반사손실을 측정하였다.

칩 안테나 이득은 안테나 챔버에서 측정하였다.

## 3. 결과 및 고찰

부 채널 공격을 방지하기 위한 대응책으로 무선 상으로 발생하는 전자기파의 신호를 차폐하거나 넓은 주파수 대역의 방사 신호가 발생하여 소음화하는 효과를 반사 손실을 측정함으로써 예측하였다.

### 3.1. 박막 증착 전후에 쿼츠 안테나의 반사손실

박막 증착 전후에 쿼츠 칩 안테나의 반사손실을 측정한 결과를 Fig. 4에 비교하였다.

박막 증착 전에는 반사 손실 10 dB 이하인 6.88 ~ 8.3 GHz, 9.6 ~ 10.36 GHz, 11.5 ~ 11.95 GHz, 12.57 ~ 15.42 GHz의 주파수 대역 폭에서 7.51 GHz, 7.71 GHz, 10.0 GHz, 11.7 GHz, 12.8 GHz, 14.0 GHz, 14.2 GHz, 14.5 GHz, 15.1 GHz의 공진을 보였다. 측정 값이 Fig. 2의 시뮬레이션 값과 다른 것은 시뮬레이션의 형상은 반도체 공정으로 제작된 실물의 치수와 상이하고 물질 특성도 한정된 값이어서 당연한 결과로 보여 지나, 측정된 공진 주파수는 시뮬레이션의 9.1 GHz, 12.8 GHz, 그리고 17.5 GHz의 공진 주파수와 비슷한 경향을 보였다.

또한, Fig. 4에서 15 mono-layer(ML), 약 5 nm, 두께의 나노 Au 박막을 증착한 쿼츠 칩 안테나의 반사손실은, 반사손실 10 dB 이하인 6.2 ~ 6.5 GHz, 6.9 ~ 8.3 GHz, 9.5 ~ 10.4 GHz, 11.4 ~ 11.8 GHz, 12.6 ~ 13.4 GHz, 17.9 ~ 18.1 GHz, 18.5 ~ 20.0 GHz의 주파수 대역 폭에서 6.3 GHz, 7.6 GHz, 10.0 GHz, 11.6 GHz, 13.1 GHz, 18.0 GHz,

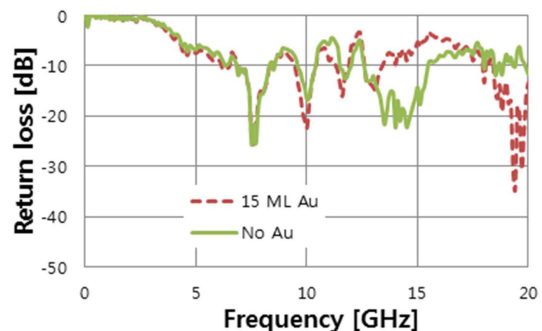


Fig. 4. Measured return losses of quartz antenna before and after 5 nm Au film deposition.

19.4 GHz, 19.7 GHz의 공진을 보였다.

이 또한 측정 값이 Fig. 3의 시뮬레이션과 다른 결과를 보이는데 나노 크기의 형상을 세세하게 구현하는데 한계가 있고, AFM으로 측정한 결과,  $R_a = 15 \sim 18.3$ ,  $R_q = 19.9 \sim 27.8$ 을 보여 이를 뒷받침하였다.

쿼츠 칩 안테나에 나노 Au 박막 증착 전후를 비교하면 나노 Au 박막을 적용한 경우에는 6~13 GHz 구간에서 반사손실 10 dB 이하인 주파수 대역폭이 넓어졌으며, 공진 주파수도 적색 편이하는 경향을 알 수 있었다. 주파수 대역 13 GHz 이상에서는 전혀 다른 공진 특성을 나타내어 나노 박막의 영향이 큰 것을 확인할 수 있었다. 이는 나노 박막의 표면 topology 관점에서 aspect ratio가 커서 메타 물질의 효과를 나타낸 것으로 보여 부채널 공격 방지에 메타물질의 사용 가능성을 볼 수 있었다. 메타 물질의 효과는 무엇보다도, 일반 안테나는 신호 파장의 절반에 해당 하는 크기가 필요한데 반해, 메타 물질 안테나는 일반 안테나의 1/5 정도의 크기로 입력되는 신호의 95% 정도를 방사하여 높은 이득을 얻을 수 있기 때문이다.

### 3.2. 박막 증착 전후에 실리콘 안테나의 반사손실

실리콘 기판은 유전상수 11.8, 전기 전도도 5.5~8.3 S/m로, 유전을 3.78인 쿼츠 기판과 다르나, 박막 증착 전에 실리콘 칩 안테나의 반사손실은 Fig. 5에서처럼 10 dB 이하인 8.5~19.4 GHz의 주파수 대역 폭에서 13.1 GHz, 14.7 GHz, 16.4 GHz의 공진 주파수를 보였다.

BTO 두께를 0.1  $\mu\text{m}$ , 1.1  $\mu\text{m}$ , 9.7  $\mu\text{m}$ 로 변경하면서 실리콘 칩 안테나의 반사손실을 측정한 결과, Fig. 6에서와 같이 BTO 두께가 증가하면서 반사손실 10 dB 이하인 주파수 대역은 9.0~20 GHz, 9.1~19.7 GHz, 8.7~19.8 GHz로 유사한 대역 폭을 보였으며, 공진 주파수도 12.9 GHz와 16.3 GHz, 12.6 GHz와 16.7 GHz, 12.9 GHz와 16.5 GHz로 유사한 공진 특성을 보였다.

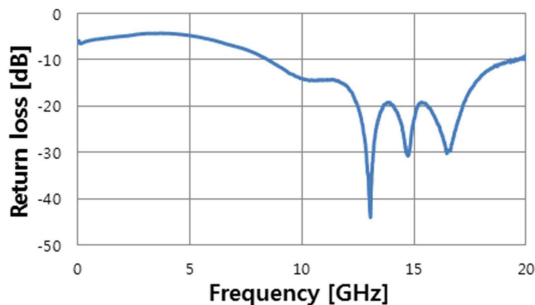


Fig. 5. Measured return loss of Si chip antenna before thin film deposition.

Cu 두께를 0.5  $\mu\text{m}$ , 1.0  $\mu\text{m}$ , 3.0  $\mu\text{m}$ 로 변경하면서 실리콘 칩 안테나의 반사손실을 측정한 결과, Fig. 7에서와 같이 Cu 두께가 증가하면서 반사손실 10 dB 이하인 주파수 대역폭은 각각 12.8~18.6 GHz, 12.6~18.5 GHz, 12.8~14.9 GHz로 Cu 두께 3.0  $\mu\text{m}$ 에서 10dB 이하인 주파수 대역 폭이 현저히 줄었다. 공진 주파수도 Cu 두께의 증가에 따라 각각 13.6 GHz와 17.2 GHz, 13.9 GHz와 17.1 GHz, 13.7 GHz로, 낮은 공진 주파수에서는 Cu 두께에 상관없이 유사한 특성을 보였으나 높은 공진 주파수에서는 Cu 두께 3.0  $\mu\text{m}$ 의 차폐 효과로 공진이 일어나지 않는 것을 알 수 있었다.

실리콘 칩 안테나에 박막 증착 전후와 박막 두께 별로 비교를 한 Fig. 8에서와 같이 BTO를 적용한 경우에는 반사손실 10 dB 이하인 주파수 대역폭은 변화가 적었으나 BTO 두께가 1.0  $\mu\text{m}$ 에서 9.7  $\mu\text{m}$ 로 변함에 따라 공진 주파수에서 반사손실이 커졌다 적어지는 특성을 보였다. 이는 aerosol deposition의 시간에 따른 step coverage의 영향으로 추정할 수 있다. 반면에 Cu를 적용한 경우에는 BTO 대비 상대적인 반사손실이 컸으며 Cu 두께 3.0  $\mu\text{m}$ 에서는 방사 대역 폭이 현저히 줄어든 것을 알 수 있었다.

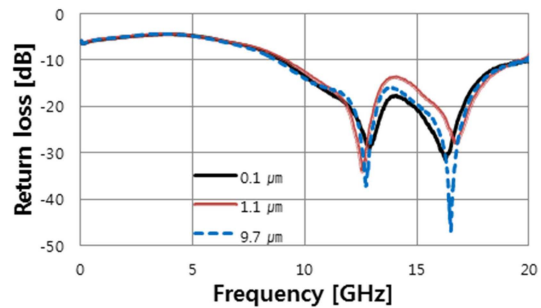


Fig. 6. Measured return loss of Si chip antenna with different BTO thickness.

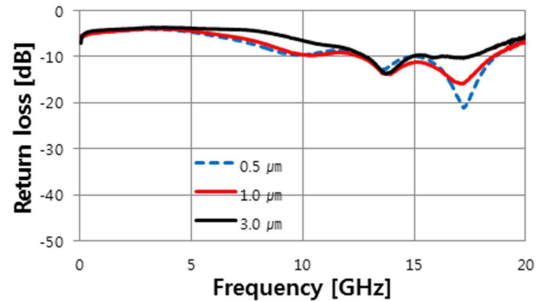


Fig. 7. Measured return loss of Si chip antenna with different Cu thickness.

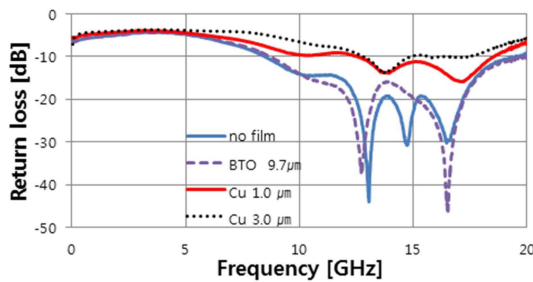


Fig. 8. Measured return loss of Si chip antenna with different film thickness.

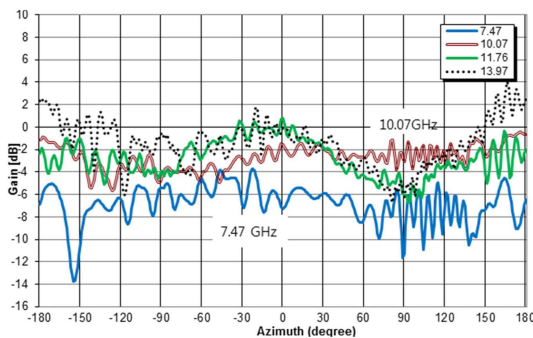


Fig. 9. Measured gain of quartz chip antenna before Au deposition.

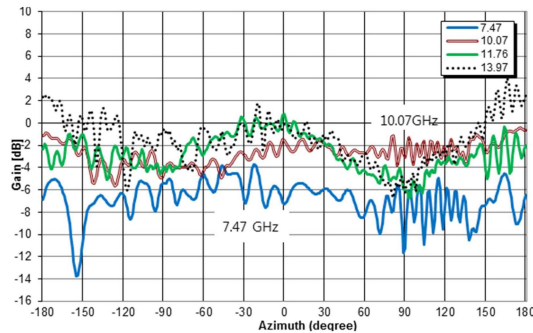


Fig. 10. Measured gain of quartz chip antenna with 15 nm Au film.

### 3.3. 안테나 이득 (gain)

박막의 종류 별로 공진 주파수를 선정하고 전자파의 방사 패턴을 측정하여 칩 안테나의 이득을 비교하였다. 전반적으로 모든 시편에서 E-평면의 이득이 H-평면의 이득보다 크게 나타나 칩 안테나의 패턴이 있는 전면 부위로 주된 방사가 나타남을 알 수 있었다.

쿼츠 칩 안테나의 경우에 주파수 별로 방위각에 따른 이득을 측정한 결과, Fig. 9와 Fig. 10에서 보인 것처럼 주파수가 상승함에 따라 이득이 커졌으며, 나노

크기의 Au를 증착한 경우가 증착하지 않은 경우에 비해 높은 이득을 보였다.

실리콘 칩 안테나의 경우에 13.0 GHz에서 E-field의 이득을 측정한 결과, 박막 증착 전에는  $-0.77$  dB를 보였고,  $9.68 \mu\text{m}$  두께의 BTO 박막을 증착한 경우에는  $-0.62$  dB의 이득을 보였고,  $3.0 \mu\text{m}$  두께의 Cu 박막을 증착한 경우에는  $0.81$  dB의 이득을 보였다. 이는 이중 patch 안테나의 특성을 보이는 것으로, 5 nm Au 박막을 증착한 경우도 이중 patch 안테나의 특성을 갖는다고 할 수 있겠다.

## 4. 결 론

유비쿼터스 기기에서 개인의 정보를 추출할 수 있는 부 채널 신호에 대한 박막의 영향을 칩 안테나를 이용한 방사 패턴 및 세기로 측정하였다.

강유전체인 BTO를 적용한 경우에는 두께 증가에 따라 공진이 깊어짐을 보여 차폐나 소음화에 대한 영향이 없음을 알 수 있었다. 전도체인 Cu의 경우에는 두께 증가에 따른 차폐 현상이 증가되는 것을 볼 수 있었다. 나노 Au를 적용한 경우에는 방사 주파수 대역폭의 확장과 공진 주파수의 적색 편이 경향을 볼 수 있어 소음화의 가능성을 볼 수 있었다.

쿼츠 기판과 실리콘 기판의 다른 유전율은 반사손실과 방사패턴을 비교 분석하는데 영향을 주지 않아 유비쿼터스 기기에서 방사되는 무선 신호에도 영향이 적을 것을 유추할 수 있었다.

## 감사의 글

이 논문은 2010학년도 경기대학교 연구년 수혜로 연구되었음. 또한 토론토 대학의 준 노가미 교수에게 감사의 뜻을 표한다 (This work was supported by Kyonggi University Research Grant 2010. Also I owe thanks to Professor Jun Nogami in University of Toronto).

## 참고문헌

1. "Side Channel Attack", [http://en.wikipedia.org/wiki/Side\\_channel\\_attack](http://en.wikipedia.org/wiki/Side_channel_attack).
2. H.J Lee, "Basic Course for Side Channel Analysis(1)", <http://kowon.dongseo.ac.kr/~hjlee/NETSEC/08DPA-EM A-lecture.pdf>, 2008.
3. Jem E. Berkes, "Side-Channel Monitoring of Contactless Java Cards", Thesis, Electrical Engineering

- and Computer Engineering, U. of Waterloo, 2008.
4. C. Gebotys, "Design of secure cryptography against the threat of power-attacks in DSP-embedded processors", *Trans. On Embedded Computing Sys.*, Vol.3, no.1, pp92-113, 2004.
  5. Hagai Bar-El, "Introduction to Side Channel Attacks", [http://www.discretix.com/images/stories/Introduction\\_to\\_Side\\_Channel\\_Attacks.pdf](http://www.discretix.com/images/stories/Introduction_to_Side_Channel_Attacks.pdf).
  6. K. Hashimoto, Y. Akiyama, T. Kawaguchi, K. Tahara and K. Otsuka, "High-speed Power supply System by Low Characteristic Impedance Transmission Line Using Metamaterials", *ICEP 2009 Proceedings*, pp891-896.
  7. K. Aydin, I. Bulu, *et al.*, "Investigation of magnetic resonances for different split-ring resonator parameters and designs", *New J. of Physics*, 7, pp1-15, 2005, 168.
  8. CST Microwave Studio Technical Specification, <http://www.cst.com/Content/Products/TechnicalSpecification.aspx?product=CST%20MWS>.
  9. Y.J Yoon, S.M. Nam, "Room Temperature Deposition of Ceramic-Polymer Composite Thick Film by Aerosol Deposition", *Ceramist*, Vol.12, No.3, 22-29, June, 2009.
- 
- 접수일: 2013년 5월 24일, 심사일: 2013년 6월 5일,  
2차심사일: 2013년 6월 12일, 게재확정일: 2013년 6월 17일