

Side Channel Attack to Magnetic Near Field of Cryptographic LSI and Its Countermeasure by Means of Magnetic Thin Film

M. Yamaguchi^a, H. Toriduka^a, S. Kobayashi^a, T. Sugawara^a, N. Homma^a, A. Satoh^b and T. Aoki^a

^aTohoku University, Sendai, Japan

^bAdvanced Industrial Science and Technology, Tokyo, Japan

Measurement of electromagnetic near-field of a cryptographic LSI provides data on its instantaneous circuit operation. Therefore magnetic near field can be a target for side channel attack to steal secret key of encryption [1]. Current interest is on the effectiveness to attack cryptographic circuit locally rather than to whole LSI chip, which may yield higher correlation to the secret key. In this paper, two types of miniature shielded-loop type magnetic probes were used to analyze RF magnetic near field on the ISO/IEC 18033-3 Standard Cryptographic LSI made by 0.13 μm CMOS process with clock frequency of 24 MHz [2]. Fig. 1 shows 41st harmonic (984 MHz) map of magnetic near field measured by the 180x180 μm^2 -size on-chip shielded loop probe we developed[3]. The targeting cryptographic circuit, AES_Comp, is located bottom left area of the chip as indicated by the rectangle. It employs 16 BITE secret key. Many line images are seen, corresponding to the power and ground lines. Magnetic field is strong not only on the AES_Comp. Such a detailed map was depicted for the first time for cryptographic LSI. Then the differential electromagnetic analysis (DEMA) was performed and summarized in the form of error rate in Fig. 2. This figure means the number of non-decrypting BITEs out of total 16 BITEs of the secret key, as a function of number the magnetic field waveform data measured by the shielded-loop probe (1000 x 500 μm^2 , CP-2S, NEC). It is obvious that all the BITEs of secret key are decrypted by using only 1×10^4 waveform data in case the waveform is measured closely to the AES_Comp (points 1 and 2 in Fig. 1). At the points 3 and 4, magnetic field intensity is as high as point 1 but the error rate does not converge to zero until the waveform number reaches 3×10^4 . This means the meaningful information is much on/closely to the AES_Comp. As the countermeasure against DEMA, 25 μm thick spin-spray NiZn ferrite film ($\mu_r=50$ at 1MHz, NEC Tokin Co, type E25) was attached on top of bare LSI chip to suppress magnetic field intensity by 6 dB as shown in Fig. 3. Thus magnetic film can be a good candidate to protect cryptographic LSI from side channel attack. Grants by SCOPE, JST, and magnetic film provision by NEC Tokin Co. are acknowledged.

- [1] J-J Quisquater, D. Samyde, "Smart Card Programming and Security," pp. 200-210, Springer Berlin/Heidelberg (2001).
 [2] National Institute of Advanced Industrial Science and Technology (Japan), "ISO/IEC 18033-3 Standard Cryptographic LSI Specification- Version 1.0 -" (2008).
 [3] M. Yamaguchi, S. Koya, H. Torizuka, S. Aoyama, S. Kawahito, IEEE Trans. Magn., **43** (2007), 2370-2372.

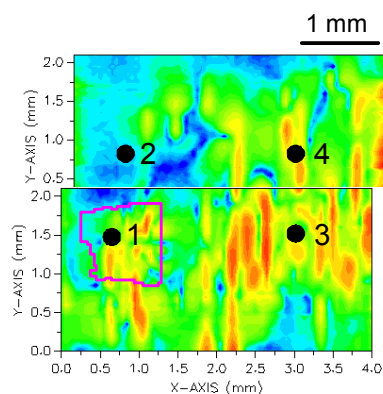


Fig. 1 Magnetic near field map

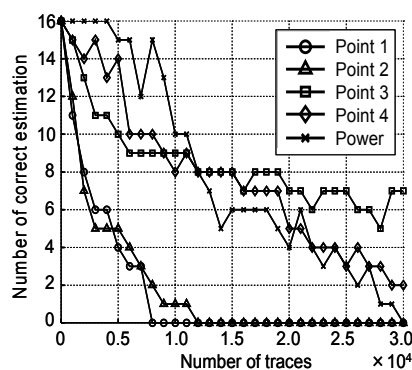
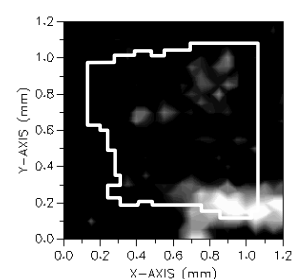
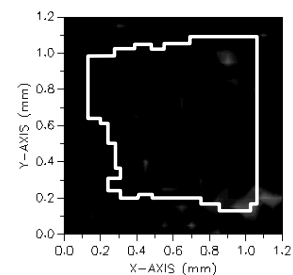


Fig. 2 Error rate



(a) Without magnetic film



(b) With magnetic film

Fig. 3 Magnetic field map on AES_Comp.