EM Attack Is Non-invasive? - Design Methodology and Validity Verification of EM Attack Sensor

Naofumi Homma[1], Yu-ichi Hayashi[1], Noriyuki Miura[2], Daisuke Fujimoto[2], Daichi Tanaka[2], Makoto Nagata[2], and Takafumi Aoki[1]

[1] Graduate School of Information Sciences, Tohoku University, Japan
homma@aoki.ecei.tohoku.ac.jp
[2] Graduate School of System Informatics, Kobe University, Japan
miura@cs.kobe-u.ac.jp

Abstract. This paper presents a standard-cell-based semi-automatic design methodology of a new conceptual countermeasure against electromagnetic (EM) analysis and fault-injection attacks. The countermeasure namely EM attack sensor utilizes LC oscillators which detect variations in the EM field around a cryptographic LSI caused by a micro probe brought near the LSI. A dual-coil sensor architecture with an LUT-programming-based digital calibration can prevent a variety of microprobe-based EM attacks that cannot be thwarted by conventional countermeasures. All components of the sensor core are semiautomatically designed by standard EDA tools with a fully-digital standard cell library and hence minimum design cost. This sensor can be therefore scaled together with the cryptographic LSI to be protected. The sensor prototype is designed based on the proposed methodology together with a 128bit-key composite AES processor in 0.18μm CMOS with overheads of only 2respectively. The validity against a variety of EM attack scenarios has been verified successfully.

Keywords: EM analysis attack, EM fault injection attack, countermeasure, attack detection, micro EM probe.

1 Introduction

Side-channel attacks have become a source of major concern in the design and evaluation of cryptographic LSIs. In such attacks, side-channel information, such as power dissipation, electromagnetic (EM) radiation, and/or the timing of internal operations, are observed or manipulated. Two of the best known attacks developed thus far are simple power analysis (SPA) and differential power analysis (DPA), both of which were proposed by Kocher et al. [1][2]. A variety of related attacks and countermeasures have been reported [3]. EM analysis (EMA), which exploits EM radiation from LSIs, is also known as a potentially more versatile alternative of power analysis [4]-[6].

L. Batina and M. Robshaw (Eds.): CHES 2014, LNCS 8731, pp. 1–16, 2014.
© International Association for Cryptologic Research 2014

One of the main characteristics of EMA is that it can perform the precise observation of information leakage from a specific part of the target LSI. Such locally observed EM radiation underlies the effectiveness of EMA [7]. In a semi-invasive context, it enables attacks to be performed at the surface of LSIs beyond the conventional security assumptions (i.e., power/EM models or attackers' capabilities). For example, the study on EMA in [8] showed that the use of micro magnetic field probing makes it possible to obtain more detailed information about an unpacked microcontroller. The authors of [8] first showed that the charge (low-to-high transition) and discharge (high-to-low transition) are distinguishable by EMA. The feasibility and effectiveness of localized EM fault injection exploiting this feature were also demonstrated in [9]. In general, such semi-invasive attacks are feasible since a plastic mold package device can be unpacked easily at low cost. Hereafter, we refer to the above sophisticated EM attack measuring and exploiting local information by micro scale probing as "microprobe-based EM attack."

More surprisingly, the possibility of exploiting leaks inside semi-custom ASICs by such microprobe-based EMA was shown in [10]. This impressive work showed current-path and internal-gate leaks in a standard cell, and geometric leaks in a memory macro were measurable by placing a micro magnetic field probe on its surface. This suggests that most of the conventional countermeasures become ineffective if such leaks are measured by attackers. For example, measuring current-path leaks circumvents conventional gate-level countermeasures involving WDDL [11], RSL [12], and MDPL [3]. Furthermore, measuring internal-gate leaks (e.g., from XOR gates) can be used to exploit, for example, XOR gates for unmasking operations. Conventional ROM-based countermeasures using dual-rail and pre-charge techniques can also be circumvented by measuring geometric leaks in a memory macro. These results still seem to be only in the realm of laboratory case studies. However, there is no doubt that microprobe-based EMA attacks on the surface of LSIs represent one of the most feasible types of attacks that operate by exploiting such critical leaks.

In order to reduce current-path and internal-gate leaks, a transistor-level countermeasure was also discussed in [10]. Such leaks can be reduced using transistor-level balancing (hiding). However, transistor-level countermeasures usually increase the design cost and significantly decrease the circuit performance. In the worst-case scenario, designers are required to prepare many balanced cells for every critical component and to perform the place and route with the utmost care. In addition, the literature does not provide any countermeasures against geometric leaks. Thus, the problem of designing effective countermeasures is still open, and the threat of microprobe-based EM attacks using such leaks is expected to increase in the future with the advancement of measurement instruments and techniques.

A natural approach to counteracting microprobe-based EM attacks is to prevent micro probes from approaching the LSI surface. The detection of package opening might be a possible solution [13], but such detection usually employs special packaging materials, which limits its applicability due to the substantial increase in manufacturing cost. In addition, tailored packaging cannot guarantee

resistance against attacks from the reverse side of the chip. Another possibility is to install an active shield on or around the LSI to be protected [14]-[16]. However, the power needed to drive signals through the shield is non-trivial. A dynamic active shield surrounding an LSI was first presented in [16]. The new concept of 3D LSI integration is designed to counteract EM attacks exploiting all aspects of the LSI. However, such shielding countermeasures inevitably increase power consumption and implementation cost.

With the aim to address the above issues, this paper introduces a new countermeasure against such high-precision EM attacks using micro EM probes. The countermeasure is based on the physical law that any probe (i.e., a looped conductor) is electrically coupled with the measured object when they are placed close to each other. In other words, a probe cannot measure the original EM field without disturbing it. The proposed method detects the invasion by employing a sensor based on LC oscillators and therefore applies to any EM analysis and fault injection attack implemented with an EM probe placed near the target LSI. Such sensing is particularly resistant to attacks performed very near or on the surface of cryptographic cores, which are usually assumed for microprobe-based EM attacks, such as in [10]. In addition, the countermeasure uses a dual-coil sensor architecture and an LUT-programming-based digital sensor calibration in order to thwart a variety of microprobe-based EM attacks.

The original concept and the key sensor circuit block validation were presented in our previous report [17]. This paper proposes a standard-cell-based semi-automatic design methodology using conventional circuit design tools. A demonstrator LSI chip fully integrating a complete set of an AES processor and the sensor is brand-new designed by the proposed systematic design methodology. The sensor is composed of sensor coils and a sensor core integrated into the cryptographic LSI. It can be designed at the circuit level rather than at the transistor level since all components of the sensor, even including the coils, are semi-automatically designed by standard EDA tools with a fully-digital standard cell library, which minimizes the design cost. The validity and performance of the sensor designed based on the proposed methodology are demonstrated through experiments using a prototype integrating a 128bit-key composite AES processor in a 0.18μm CMOS process. We confirm that the prototype sensor successfully detects a variety of microprobe-based EM attacks with overheads of only 2% in area, 9% in power, and 0.2% in performance. Thus, the major contributions of the present paper are establishing a systematic design flow for the sensor using conventional circuit design tools, showing that the sensor can be developed at the circuit level, and demonstrating the validity and performance of the prototype sensor designed by using our design flow through a set of experiments for different attack scenarios.

The remainder of this paper is organized as follows. Section 2 introduces the concept of the countermeasure with the EM attack sensor. In Section 3, the semi-automatic design flow for the sensor is proposed. Section 4 shows the experimental results obtained using the prototype integrated into an AES processor

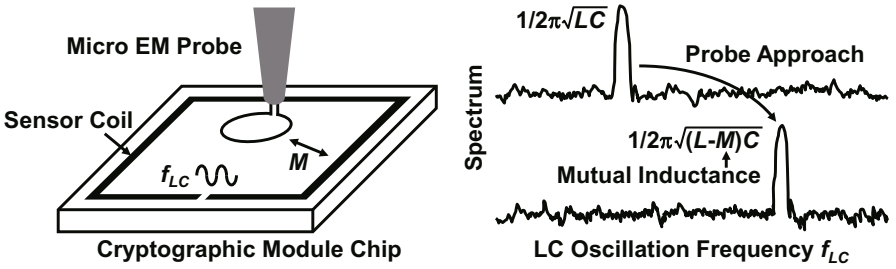

Fig. 1. Basic concept

and discusses its capabilities and limitations. Finally, Section 5 presents some concluding remarks.

2 EM Attack Sensor

Figure 1 illustrates the basic concept of the EM attack sensor. When a probe (i.e., a looped conductor) is brought close to an LSI (i.e., another electric object), mutual inductance increases. This is a physical law that is unavoidable in magnetic field measurement. Assuming current flowing through a coil (i.e., an LC circuit), its frequency shifts due to the mutual inductance M. The original frequency f_{LC} and the shifted frequency $\tilde{f}_{LC}$ are approximately given by

$$f_{LC} \approx \frac{1}{2\pi\sqrt{LC}}, \tag{1}$$

$$\tilde{f}_{LC} \approx \frac{1}{2\pi\sqrt{(L-M)C}}, \tag{2}$$

respectively. Thus, it is possible to detect the presence of a probe that has been placed inside a common LSI package by detecting the frequency shift induced in an LC circuit. Note that the corresponding variation in electric field is also detectable in the equivalent principle by capacitive coupling.

The single-coil sensing scheme in Fig. 1 is simple and straightforward, but it requires a frequency reference generated either inside or outside the LSI for detecting frequency shifts. However, any external clock signal, including a system clock, may be manipulated by the attacker, and therefore cannot be used as a reliable frequency reference. In addition, an on-chip frequency reference requires area- and power-hungry analog circuitry, such as a bandgap reference circuit. These drawbacks of the single-coil scheme are overcome by using a dual- or multi-coil scheme.

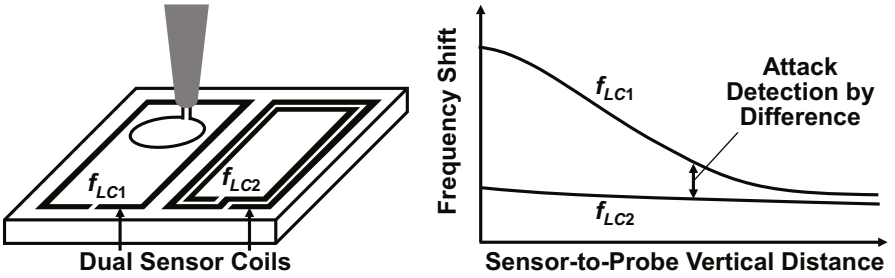

Fig. 2. Dual-coil sensor architecture

Figure 2 illustrates the concept of the dual-coil sensor architecture, where two coils are installed on the cryptographic core to be protected. Using two coils with different shape and number of turns, it is possible to detect an approaching probe by the difference of the oscillation frequencies of the two coils. This dual-coil sensor architecture avoids using any absolute frequency reference that is required in the single-coil scheme. The difference of frequencies is constant and remains detectable even if a frequency reference, such as a system clock, is tampered with. In addition, the difference of the frequencies of the two coils enables probe detection in a variety of probing scenarios (e.g., dual probing and cross-coil probing).

To enhance the attack detection accuracy, PVT (process, voltage, and temperature) variation in f_{LC} should be suppressed. A ring oscillator can be utilized as a PVT monitor for calibrating f_{LC} [17]. The abovementioned LC oscillators do not employ any varactor capacitance as they have a positive temperature coefficient ($k_{TC} > 0$). Instead, small MOS capacitors with low k_{TC} are connected to the oscillator only for calibration. The f_{LC} variation in this design is inversely proportional to the transconductance of a g_m cell in the LC oscillator. As a result, the LC and the ring oscillators have a monotonic inverse dependence on PVT, and thus f_{LC} can be digitally calibrated in one step with only two counters and a small lookup table (LUT) used for converting the difference of clock counts into capacitance values (i.e., the number of capacitors).

In the calibration, first we switch on both the LC and ring oscillators, after which we check the outputs of the counters attached to the oscillators, and finally increase or decrease the number of capacitors in accordance with the difference of counts. Here, a relative frequency difference is utilized, similarly to the attack detection concept. Such digital calibration setup is implemented in a compact and low-power manner since it does not require any analog circuitry for frequency reference. In principle, this calibration only handles f_{LC} shift due to PVT variation, and the shift Δf due to an approaching probe always remains after the calibration. Even if the probe is placed close to the chip before the power supply is switching on, the probe can be detected immediately after wake-up.

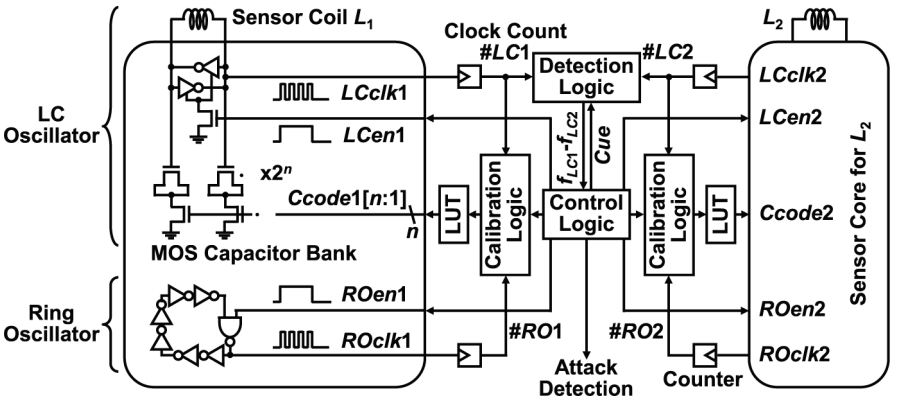

Fig. 3. Circuit diagram

3 Design Methodology

Figure 3 depicts a circuit diagram of the sensor core circuit. It consists of LC oscillators connected to sensor coils L1 and L2, ring oscillators, a detection logic circuit, two calibration logic circuits, and a control logic circuit. For the best compatibility with the standard digital design flow, standard digital cells are assigned to all the circuit components. The g_m cell of the LC oscillator can be realized by using two gated CMOS inverter and the MOS capacitor bank is composed of 2^n sets of unit MOS capacitors with switch controlled by digital binary code Ccode. All other circuit components are of course realized by using the standard digital cell library. The sensor core performs detection of frequency difference, calibration of LC oscillator frequencies, and timing control of the sensor operation.

The detection logic circuit calculates the difference of LC oscillation frequencies by subtracting the clock counts of LCclk1 and LCclk2, which indicate the digitized values of the oscillation frequencies f_{LC1} and f_{LC2}, respectively.

The two calibration logic circuits calculate the difference of clock counts of LCclk1 (LCclk2) and ROclk1 (ROclk2) obtained from the LC and ring oscillators, respectively. Here, note that we know both the frequencies of LC and ring oscillators in advance under typical PVT conditions. The difference is converted into the capacitance value Ccode1 (Ccode2) based on the lookup table (LUT) connected to the calibration logic circuit. The Ccode1 (Ccode2) switches the number of capacitors connected to the LC oscillator and consequently calibrates the LC oscillator frequency.

Figure 4 illustrates the process of calibration, where the LC and ring oscillators have a monotonic inverse dependence on the supply voltage and ΔC indicates the capacitance determined by the difference of LC and ring oscillation frequencies. Although Figure 4 illustrates a case when the supply voltage varies, this calibration method is applicable to variations in process and temperature.

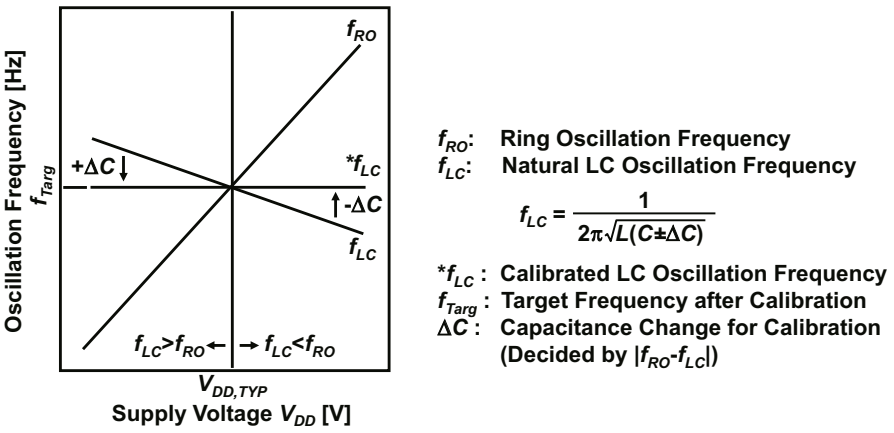

Fig. 4. Calibration scheme

In order to suppress the f_{LC} variation within $\pm 1\%$, a 10-bit Ccode resolution is high enough. The LUT for this calibration is essentially a 10-bit subtracter whose gate count is only around 0.2k gates.

The control logic circuit provides the timings of detection and calibration operations, which are determined depending on the cryptographic operation to be protected. Calibration is performed once before the detection operation, which is performed in a timely fashion before and during cryptographic operation. If a frequency difference is detected, a signal to that effect is generated by the control logic circuit. The cryptographic operation is then changed in accordance with the detection signal.

As described above, all components of the sensor core are implemented as fully digital circuits available as standard cells (including transistor switches and capacitance cells), and therefore the sensor can be scaled together with the cryptographic LSI to be protected. The coil size is also scalable due to transistor performance improvement in device scaling. The sensor monitors for probe approach intermittently and periodically, which saves power and minimizes the performance overhead. In addition, the oscillators do not interfere with the cryptographic core since the sensor is usually activated while the cryptographic core is idle.

Figure 5 shows the proposed design methodology for the above sensor with conventional circuit design tools. The cryptographic and sensor cores are first described by a conventional hardware description language (e.g., Verilog-HDL) at the logic design step and synthesized by a logic synthesizer at the logic synthesis step. Logic synthesis is performed for each functional block since it is assumed that all functional blocks handling sensitive data are protected by sensor coils.

After the logic synthesis step, the sensor coils are designed in accordance with the above design. At the netlist generation step, a netlist of the sensor cores is generated for a SPICE simulation of the sensor core. In parallel, the external

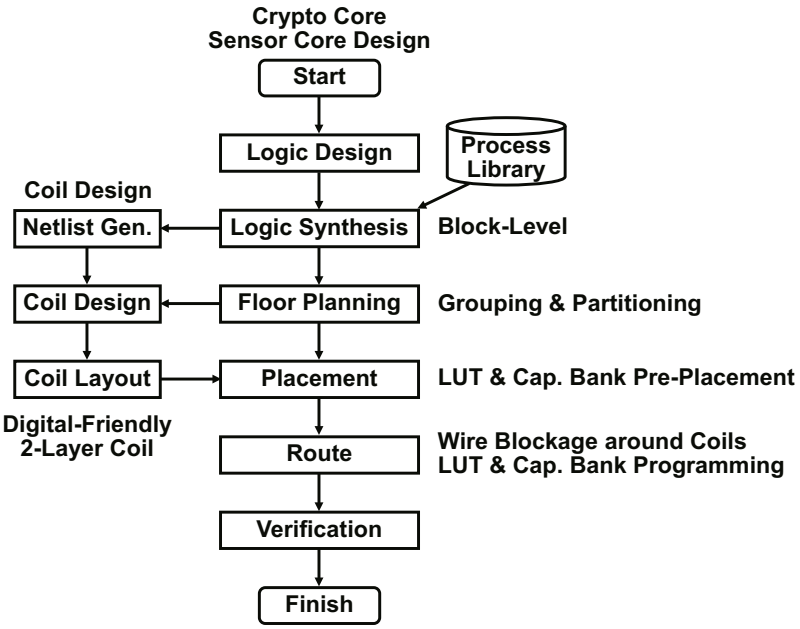

Fig. 5. Design flow

shape of the cryptographic and sensor cores is fixed at the floor planning step, which determines the overall coil size (i.e., length and width).

With the coil length and width fixed, at the coil design step, we determine the number of turns, which determines the oscillation frequency. The gap between the wires is also adjusted to fine-tune the oscillation frequency, and the wire width is adjusted to ensure stable oscillation. A wide wire reduces loss in the coil and hence meets the oscillation requirements, at the expense of using more resources to make the wire. Then, we perform a SPICE simulation with the coil parameters for a range of possible PVT conditions and determine the required capacitor bank structure (i.e., the range and step size of capacitance values). Unit capacitors with some margin are pre-arranged at the placement step, and then the actual bank structure is constructed at the following routing step by hard-wire programming between the capacitor bank and the LUT to convert the frequency difference to capacitance value for sensor calibration.

At the coil layout step, we design the coil layout according to the above parameters. Note here that we can utilize digital layout grids to provide the width and spacing of wires. A digital-friendly 2-layer coil layout style [18] is employing where coil is drawn by two different metal layers for orthogonal edges (Fig. 6). The coil can be hidden in the sea of logic interconnections as it only consumes several tens of logic interconnection tracks. Since a high Q factor is not required, it is also not necessary to have a thick upper layer of metal for the coil since phase noise (jitter) in the LC oscillator has no impact on detection

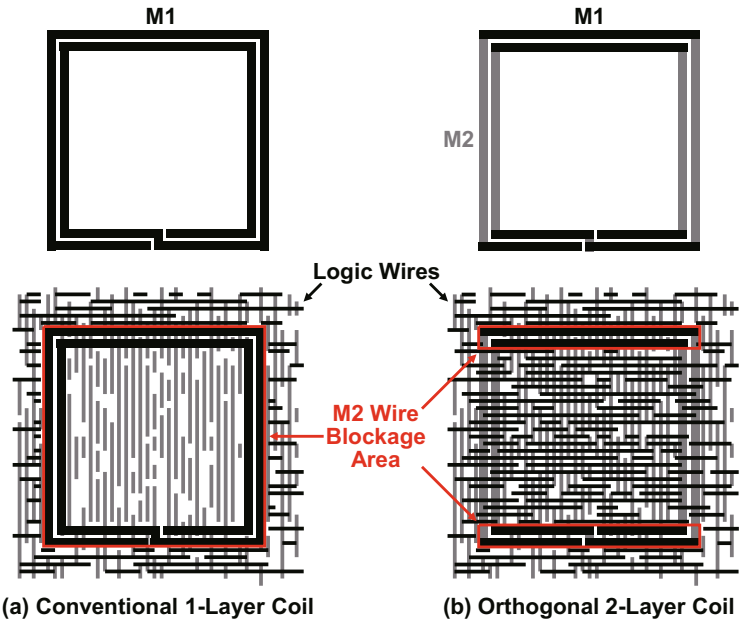

Fig. 6. Coil layout: (a) conventional one-layer coil, and (b) orthogonal two-layer coil

accuracy. Therefore, the coil can be fabricated by a standard digital process without any analog/RF options. Unlike analog LC oscillator such as for RF clock synthesizers, careful dedicated analog design is not necessary for this sensor coil and oscillator design, further lowering the design cost.

Based on the coil layout, at the placement and routing step, we place and route the components of the cryptographic and sensor cores, including the capacitor bank and LUT. The capacitor bank has n capacitors of different sizes, and therefore encodes $2^n - 1$ capacitance values for an n-bit input. Finally, we can verify the overall functionality with a digital verification tool at the verification step since the input and output of the sensor core are digital.

4 Validity Verification

The validity and performance of the proposed sensor were demonstrated through experiments with a newly fabricated chip designed on the basis of the proposed methodology. We assume here four attack scenarios with a single microprobe approaching during the sensing period, a larger micro probe approaching during the sensing period, a single micro probe approaching while the supply voltage was being changed, and a single micro probe approaching before the sensing period (i.e., during the sleep period). The first scenario assumed a conventional microprobe-based EM attack, such as that described in [8] and [10], where attackers move a microprobe close to the core surface while the sensor is working.

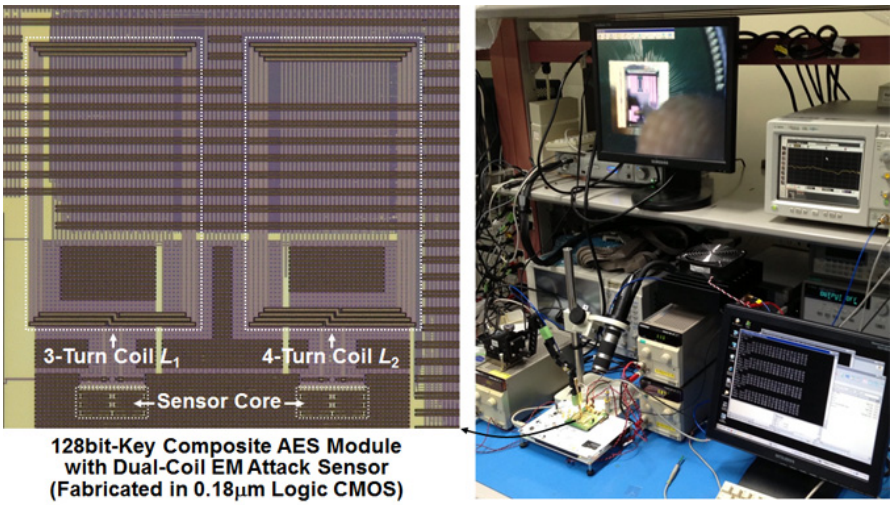

Fig. 7. Die photograph and measurement setup

The second scenario assumed an attempt to avoid detection by a larger probe crossing the two coils. This scenario is equivalent to EMA with two micro probes close to the two coils at the same time. The third scenario assumed that the attacker manipulate the PVT conditions to cheat the sensor. Finally, the fourth scenario assumed that the attacker can place a micro probe on the core surface in advance before the cryptographic and sensor cores are switched on, manipulating the PVT conditions.

The proposed sensor was implemented in a TSMC 0.18μm CMOS process by commercial CAD tools. More precisely, we used Design Compiler (G-2012.06-SP3), IC Compiler (vH-2013.03-SP2), and Virtuoso (6.1.4) for the logic synthesis, the P&R, and the coil design, respectively. Figure 7 shows a die photograph and the measurement setup. Two coils (a 4-turn coil (L1) and a 3-turn coil (L2)) were placed above an AES processor. The L1 (L2) coil had the resistance of 76Ω (55Ω), the capacitance of 68fF (64fF), and the inductance of 13.2nH (8.5nH) according to the EM field simulation with an equivalent circuit model. The AES processor was based on a common loop architecture operating at one round per clock cycle [19]. The test chip was mounted on a side-channel attack standard evaluation board (SASEBO R-II) [20]. A micro EM probe was fixed on a manipulator, and its position was controlled manually by monitoring through a microscope. We conducted successful microprobe-based EMA using EM waveforms observed in the experimental setup, where the EM signal from the probe was amplified by a 100 W +40 dB power amplifier.

Figure 8 shows the frequency spectra of L1 and L2 in the presence and absence of a micro probe. The oscillation frequency of each coil was clearly shifted by the probe, even at a distance of about 100μm. The result indicates that

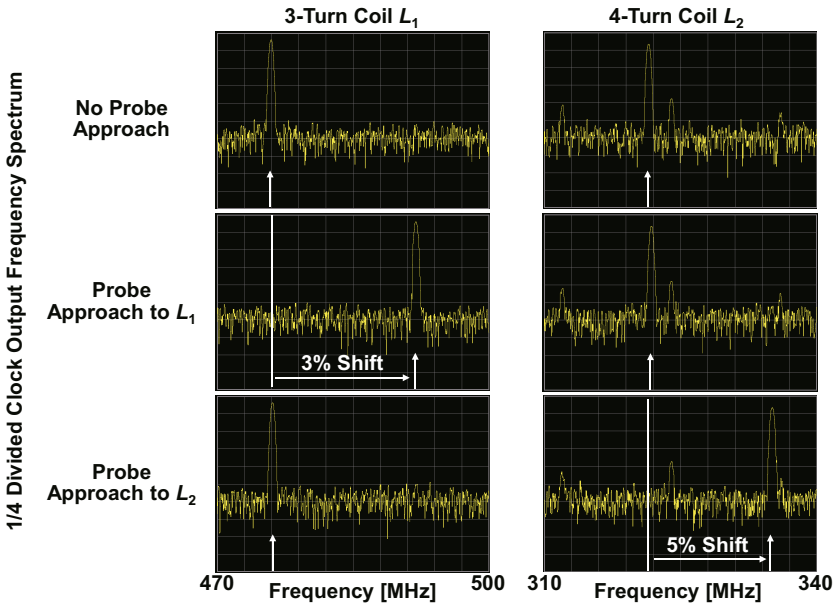

Fig. 8. Frequency shift caused by an approaching probe

microprobe-based EM attacks such as those assumed in the first scenario can be easily detected by the sensor.

Figure 9 shows the difference of the frequency shifts of L1 and L2 for different distances between the coils and the probe. The shift ratio of L1 was clearly different from that of L2 when the same probe was used. This suggests that the second scenario is also thwarted by our dual-coil detection scheme. Even if the attacker can observe the magnitude of the frequency shifts, they would still have substantial difficulty in matching the shifts, which are determined by many coil parameters, while performing high-density EM measurements. This result indicates that EM attacks with two micro probes are also detectable.

Figure 10 (a) presents the frequency shift dependence on the supply voltage VDD, where the left and right hands of the figure are the amount of frequency shifts before and after the calibration, respectively. The proposed one-step digital calibration suppresses the f_{LC} variation to within $\pm 1\%$ over the temperature range of 0-60 °C at a VDD voltage of 1.6-2.0 V which corresponds to a variation greater than $\pm 10\%$ from the nominal VDD voltage of 1.8 V. This result shows that the proposed sensor is robust against PVT variation since the same calibration method is applicable for a range of possible PVT conditions.

Figure 10 (a) also shows that the sensor can thwart the fourth scenario. The frequency shift due to the approaching probe remains after calibration. The result indicates that even if the probe is brought close to the cryptographic core before its power supply is switched on, the probe can be detected immediately after wake-up. Figure 10 (b) presents the result for a sophisticated fourth

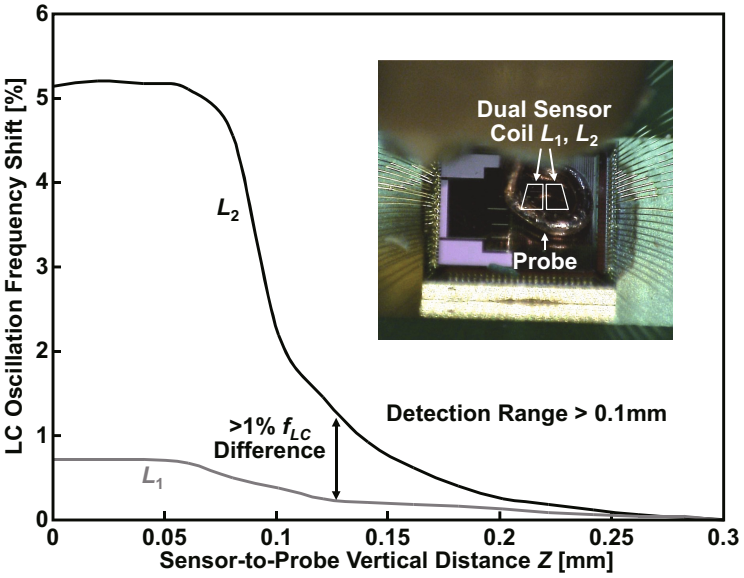

Fig. 9. Difference of frequency shifts of L1 and L2 for different distances

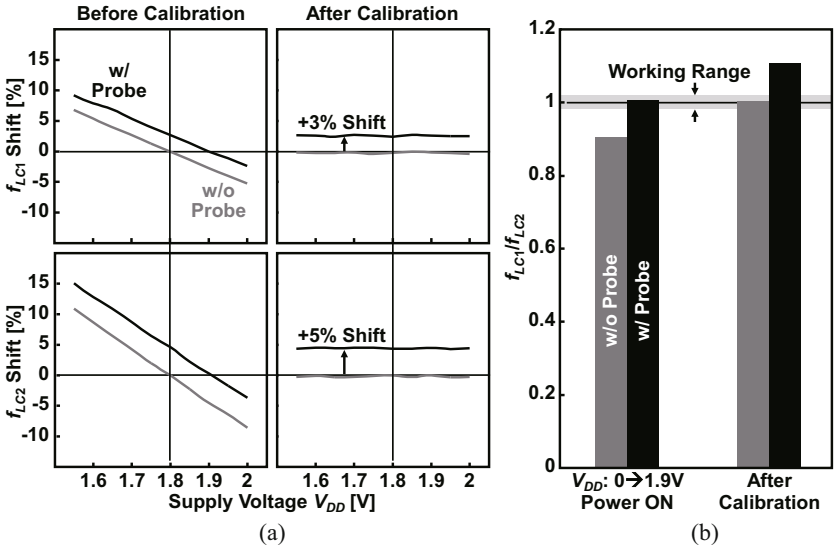

Fig. 10. Frequency shifts before and after calibration

scenario, where the attacker can manipulate the supply voltage and suppress f_{LC} variation to within the working range ($\pm 1\%$) with a micro probe close to the core surface just after the power is switched on. It should be noted that such

Table 1. Overheads caused by sensor

	AES Core	Sensor	Total (Sensor Overhead)
2NAND Gate Count	24.3k	0.3k	24.6k (+1.2%)
Wire Resource	0.40mm^2	0.05mm^2	0.45mm^2 (+11%)
Layout Area	0.48mm^2	0.01mm^2	0.49mm^2 (+2%)
Performance	125μs/Enc	0.3μs/Sense	125.3μs (-0.2%)
Power Consumption	0.23mW	0.02mW	0.25mW (+9%)

cheating was also thwarted by the calibration since the f_{LC} variation is always corrected to within $\pm 1\%$ in the absence of a probe.

Table 1 summarizes the overheads caused by the sensor hardware. The time for a single detection operation (including calibration and sense operations) can be reduced to <1% of the time for one AES encryption operation, including data I/O. Note that the application considered here is a simple device with a few IO pins, such as smartcard, which can be mainly targeted by microprobe-based EMA. Such device usually equips serial IO and outputs the data at each time. This intermittent sensor operation at <1% duty cycle significantly reduces the power and performance overheads of the sensor. The power consumption was estimated from a calibration-and-sense operation before an AES encryption operation. With overheads of only 2% in area and 9% in power, the proposed sensor can be used as a countermeasure against microprobe-based EM attacks, filling a large security hole not covered by conventional countermeasures.

5 Discussion

The experimental results show that the proposed sensor is effective against micro-probe-based EM attacks which cannot be prevented by the conventional algorithmic- and circuit-level countermeasures. EM fault-injection attacks using a micro needle probe, such as that in [9], are also detected by the same principle. Using middle layers to draw sensor coils could also prevent attacks from the backside of the LSI since the magnetic sensing can work through interconnect, transistor and substrate layers. Thus, the proposed countermeasure can detect EM analysis and fault-injection attacks performed close to or on the LSI (front and back) surface in a robust manner.

The proposed sensor would also be invulnerable to frequency injection attacks. First, attackers must measure the original frequency very close to the coil surface but cannot measure it without disturbing the original one. Even if the frequency is known, a significant EM injection power is required to lock an oscillator since each coil is oscillating in a full swing manner. Such powerful EM injection must affect another oscillator. Note again that the oscillation frequencies are different for each other. If both oscillators are locked to the same frequency, the sensor detects it immediately. An attacker might attempt to attach a frequency-injection probe directly to an embedded coil, but it is hard to do it without affecting other wires.

One possible attack on the proposed setup would be to eliminate the difference between oscillation frequencies observed by the sensor by using two probes or similar alternatives. However, performing such a sophisticated attack is extremely difficult, even if the attacker can observe the frequency shifts shown in the above experiments. In addition, it is difficult to identify and disable the sensor prior to the attack since the coils and the sensor core are embedded in the sea of logic gates and wires. Reverse engineering to removing the sensor would also be a rather challenging task when the cryptographic core operation is linked with the sensor operation.

The detectable distance between the probe and the sensor is limited to a maximum of 0.1 mm in the experimental setup. The limited maximum detection distance means that conventional EMAs on the chip package such as DEMA and CEMA are still possible, even if the proposed sensor is installed over the cryptographic core. The extension of the maximum detection distance is an open issue that will be addressed in future work. For example, we could extend the detection distance using larger coils. Extending the maximum distance may enable the sensor to detect chip unpacking as well. On the other hand, the proposed sensor can be combined with any other conventional countermeasures due to the low area and performance overheads. In practice, a combination of conventional countermeasures and the proposed technique would work well in a complementary manner.

The power and performance overheads are further reduced by the optimization of intermittent sensor operation. The sensor should operate continuously during the cryptographic operations for increased security. However, intermittent operation would be sufficient for many applications. For example, one-time calibration and sensing before continuous cryptographic operations might be practical. Designers and users can determine the operation timing according to the target application and intended use. The post-detection operations (e.g., termination or dummy operations) should also be optimized depending on the application. Such optimizations will also be examined in future work.

6 Conclusion

This paper presented the design methodology and validity verification of a new countermeasure against microprobe-based EM analysis and fault-injection attacks. The proposed countermeasure detects variations in the EM field caused by a micro EM probe approaching the cryptographic LSI, and therefore thwarts microprobe-based EMA that cannot be prevented by conventional algorithmic- and circuit-level countermeasures. A dual-coil sensor architecture and an LUT-programming-based digital sensor calibration can prevent such EM attacks in a variety of scenarios where one or more micro EM probes are used under different PVT conditions. All components of the sensor core are implemented in a fully digital circuit and therefore can be scaled together with the cryptographic LSI to be protected.

The proposed systematic design flow for the sensor is based on standard digital circuit design tools. All the sensor circuit components, including the sensor coils,

was semi-automatically designed by the synthesis and placement software once the coil parameters were fixed. The validity and performance of the sensor were demonstrated through experiments using a prototype integrated into an AES processor. The results show that our sensor successfully detects microscale EM probes approaching the AES processor for all assumed attack scenarios.

The sensor was designed based on the proposed design flow and integrated with overheads of only 2% in area, 9% in power, and 0.2% in performance, which are much lower than those of alternative active shield techniques. Such low overheads make it possible to implement the proposed technique together with conventional countermeasures developed for other types of attacks. Although the proposed countermeasure cannot thwart all types of EM attacks, it can significantly reduce the complexity and cost associated with conventional countermeasures against microprobe-based EMA. One direction of future work will be to find the most effective combination of the proposed and conventional countermeasures.

References

1. Kocher, P.C.: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 104–113. Springer, Heidelberg (1996)
2. Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
3. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks - Revealing the Secrets of Smart Cards. Springer (2007)
4. Gandolfi, K., Mourtel, C., Olivier, F.: Electromagnetic analysis: Concrete results. In: Koç, Ç.K., Naccache, D., Paar, C. (eds.) CHES 2001. LNCS, vol. 2162, pp. 251–261. Springer, Heidelberg (2001)
5. Quisquater, J., Samyde, D.: Electromagnetic analysis (EMA): Measures and counter-measures for smart cards. In: Attali, S., Jensen, T. (eds.) E-smart 2001. LNCS, vol. 2140, pp. 200–210. Springer, Heidelberg (2001)
6. Agrawal, D., Archambeault, B., Rao, R., Rohatgi, P.: The EM side-channel(s). In: Kaliski Jr., B.S., Koç, Ç.K., Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp. 29–45. Springer, Heidelberg (2003)
7. Réal, D., Valette, F., Drissi, M.: Enhancing Correlation Electromagnetic Attack Using Planar Near-Field Cartography. In: DATE 2009, pp. 628–633 (2009)
8. Peeters, E., Standaert, X., Quisquater, J.: Power and electromagnetic analysis: Improved model, consequences and comparisons. Integration, the VLSI Journal 40(1), 52–60 (2007)
9. Moro, N., Dehbaoui, A., Heydemann, K., Robisson, B., Encrenaz, E.: Electromagnetic fault injection: towards a fault model on a 32-bit microcontroller. In: FDTC 2013, pp. 77–88 (August 2013)
10. Sugawara, T., Suzuki, D., Saeki, M., Shiozaki, M., Fujino, T.: On Measurable Side-Channel Leaks Inside ASIC Design Primitives. In: Bertoni, G., Coron, J.-S. (eds.) CHES 2013. LNCS, vol. 8086, pp. 159–178. Springer, Heidelberg (2013)
11. Tiri, K., Hwang, D., Hodjat, A., Lai, B.-C., Yang, S., Schaumont, P., Verbauwhede, I.: Prototype IC with WDDL and differential routing – DPA resistance assessment. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 354–365. Springer, Heidelberg (2005)

12. Suzuki, D., Saeki, M., Ichikawa, T.: Random Switching Logic: A Countermeasure against DPA based on Transition Probability, IACR Cryptology ePrint Archive 2004: 346 (2004)
13. Van Geloven, J.A.J., Wolters, R.A.M., Verhaegh, N.: Sensing circuit for devices with protective coating, United States Patent no. US 2010/0090714 Al (2010)
14. Beit-Grogger, A., Riegebauer, J.: Integrated circuit having an active shield. United States Patent no. 6,962,294 (2005)
15. Briais, S., Cioranesco, J.-M., Danger, J.-L., Guilley, S., Jourdan, J.-H., Milchior, A., Naccache, D., Porteboeuf, T.: Random Active Shield. In: FDTC 2012, pp. 103–113 (September 2012)
16. Briais, S., et al.: 3D Hardware Canaries. In: Prouff, E., Schaumont, P. (eds.) CHES 2012. LNCS, vol. 7428, pp. 1–22. Springer, Heidelberg (2012)
17. Miura, N., Fujimoto, D., Tanaka, D., Hayashi, Y., Homma, N., Aoki, T., Nagata, M.: A Local EM-Analysis Attack Resistant Cryptographic Engine with Fully-Digital Oscillator-Based Tamper-Access Sensor. In: 2014 Symposium on VLSI Circuits, Dig. Tech. Papers, pp. 172–173 (June 2014)
18. Saito, M., Kusaga, K., Takeya, T., Miura, N., Kuroda, T.: An Extended XY Coil for Noise Reduction in Inductive-coupling Link. A-SSCC Dig. Tech. Papers, pp. 305–308 (November 2009)
19. Cryptographic Hardware Project (August 2007), `http://www.aoki.ecei.tohoku.ac.jp/crypto/`
20. Side-channel Attack Standard Evaluation Board, SASEBO-RII (2012), `http://www.risec.aist.go.jp/project/sasebo/`