J Cryptol (2017) 30:373–391
DOI: 10.1007/s00145-015-9223-3

Journal of
CRYPTOLOGY

Design Methodology and Validity Verification for a Reactive Countermeasure Against EM Attacks

Naofumi Homma · Yu-ichi Hayashi · Takafumi Aoki
Graduate School of Information Sciences, Tohoku University, Sendai, Japan
homma@aoki.ecei.tohoku.ac.jp

Noriyuki Miura · Daisuke Fujimoto · Makoto Nagata
Graduate School of System Informatics, Kobe University, Kobe, Japan
miura@cs.kobe-u.ac.jp

Communicated by François-Xavier Standaert.

Received 30 January 2015
Online publication 17 December 2015

Abstract. This paper presents a standard-cell-based semiautomatic design methodology for a new conceptual countermeasure against electromagnetic (EM) analysis and fault-injection attacks. The countermeasure, called the EM attack sensor, utilizes LC oscillators that react to variations in the EM field around a cryptographic LSI caused by a microprobe brought near the LSI. A dual-coil sensor architecture with digital calibration based on lookup table programming can prevent various microprobe-based EM attacks that cannot be thwarted by conventional countermeasures. All components of the sensor core are semiautomatically designed by standard electronic design automation tools with a fully digital standard cell library and hence minimum design cost. This sensor can therefore be scaled together with the cryptographic LSI to be protected. The sensor prototype is designed based on the proposed methodology together with a 128-bit-key composite AES processor in 0.18-μm CMOS with overheads of only 2 % in area, 9 % in power, and 0.2 % in performance, respectively. The countermeasure has been validated against a variety of EM attack scenarios. In particular, some further experimental results are shown for a detailed discussion.

Keywords. EM analysis attack, EM fault-injection attack, Countermeasure, Attack detection, Microprobe.

1. Introduction

Side-channel attacks have become a 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 are simple power analysis and differential power analysis, both of which were proposed by Kocher et al. [10,11]. A variety of related attacks and countermeasures have been reported [12]. EM analysis (EMA), which

exploits EM radiation from LSIs, is also known as a potentially more versatile alternative to power analysis [1,8,16].

One of the main characteristics of EMA is that information leakage can be precisely observed from a specific part of the target cryptographic LSI. Such locally observed EM radiation underlies the effectiveness of EMA [17]. In a semi-invasive context, it enables attacks to be performed at the surface of LSIs beyond the conventional security assumptions (power/EM models, attackers' capabilities, etc.). For example, a study on EMA [15] showed that the use of magnetic field microprobing makes it possible to obtain more finely detailed information about an unpacked microcontroller. The authors of that study 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 has also been demonstrated [2,7,14,19]. In general, such semi-invasive attacks are feasible since a plastic mold package device can be unpacked easily at low cost. Hereinafter, we refer to the above sophisticated EM attack measuring and exploiting local information by microscale probing as microprobe-based EM attack.

More surprisingly, the possibility of exploiting leaks inside semi-custom ASICs by such microprobe-based EMA was demonstrated in [21]. 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 magnetic field microprobe on the chip surface. This suggests that most conventional countermeasures become ineffective when such leaks are measured by attackers. For example, measuring current path leaks circumvents conventional gate-level countermeasures involving WDDL [23], RSL [22], and MDPL [12]. 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 which indicate the geometric layout of the memory matrix structure. These results still appear to be limited to 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.

To reduce current path and internal gate leaks, a transistor-level countermeasure has also been discussed [21]. Such leaks can be reduced by 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 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 exploiting such leaks is expected to increase in the future with the advancement of measurement instruments and techniques. Even if improved process technology makes such attacks more difficult, legacy and low-cost systems with the conventional process would remain and an imbalance between advanced measurement techniques and such systems would sometimes arise.

A natural approach to counteracting microprobe-based EM attacks is to prevent microprobes from approaching the LSI surface. The detection of package opening might be a

possible solution [24], 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 [3–5]. However, the power needed to drive signals through the shield is non-trivial. A dynamic active shield surrounding an LSI was first presented in [4]. 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 that use EM microprobes. 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 invading it. The proposed method reacts to such invasion through the use of 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. When the sensor detects an invasion by a probe, the protected cryptographic core immediately moves to an arbitrary safe mode to prevent information leakage. 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 [21]. In addition, the countermeasure uses a dual-coil sensor architecture and digital sensor calibration based on lookup table (LUT) programming in order to thwart a variety of microprobe-based EM attacks.

The original concept and preliminary validation of this countermeasure were presented in our previous report [13]. This paper is an extended account of our work presented at CHES 2014 [9]. Here we present a standard-cell-based semiautomatic design methodology using conventional circuit design tools and shows some further experimental results for a detailed discussion. A demonstrator LSI chip that fully integrates an AES processor and the sensor as a complete set is newly designed by the proposed systematic design methodology. The sensor consists 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, including even the coils, are semiautomatically designed by standard electronic design automation 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 128-bit-key composite AES processor in a 0.18 μm CMOS process. We confirmed that the prototype sensor can detect 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 this paper are establishing a systematic design flow for the sensor by means of 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 on 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 Sect. 3, the semiautomatic design flow for the sensor is proposed. Section 4 shows the experimental results obtained using the

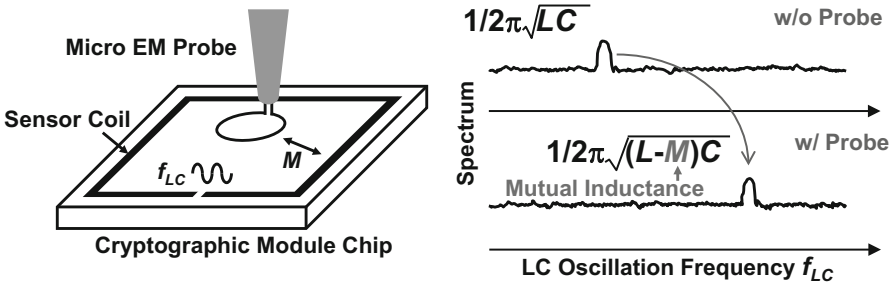

Fig. 1. Basic concept.

prototype integrated into an AES processor and discusses its capabilities and limitations. Finally, Sect. 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 (another electrical 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 by the equivalent principle of 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.

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 the use of any absolute frequency reference as would be required in the single-coil scheme.

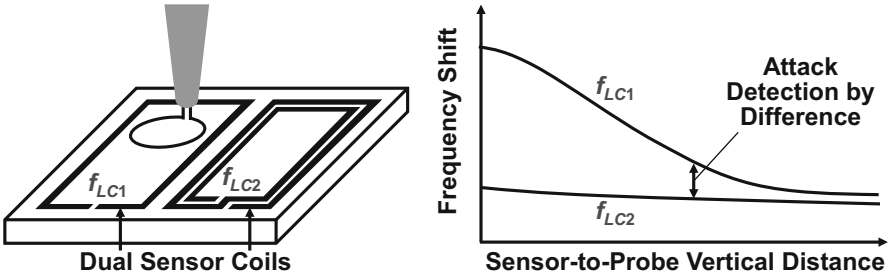

Fig. 2. Dual-coil sensor architecture.

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 between the frequencies of the two coils enables probe detection in various 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 by a calibration technique. A ring oscillator can be utilized as a PVT monitor for calibrating f_{LC} [13]. In our design, f_{LC} can be digitally calibrated in one step with only two counters and a small LUT used for converting the difference between 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. This 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 handles only an 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 switched on, the probe can be detected immediately after wakeup.

3. Design Methodology

Figure 3 shows 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 inverters, and the MOS capacitor bank is composed of 2^n sets of unit MOS capacitors with a switch controlled by a digital binary code Ccode. All other circuit components are pure digital circuits and are 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 between LC oscillation frequencies by subtracting the clock counts of LCclk1 and LCclk2, which represent the digitized values of the oscillation frequencies f_{LC1} and f_{LC2}, respectively.

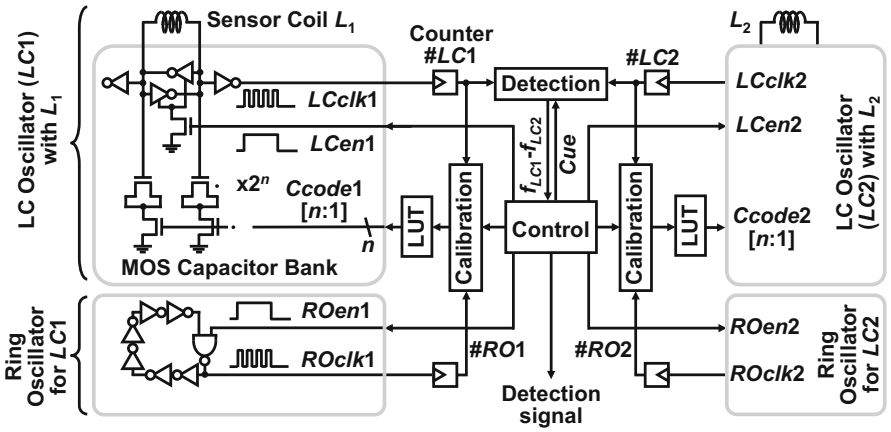

Fig. 3. Circuit diagram.

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, both the LC and ring oscillators are initially designed to have the same basic frequency under typical PVT conditions. The difference is converted into the capacitance value Ccode1 (Ccode2) based on the 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. Note that the above 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 for calibration only. 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.

Figure 4 illustrates the process of calibration, where the LC and ring 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 Fig. 4 illustrates a case when the supply voltage varies, this calibration method is applicable to variations in process and temperature. 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 subtractor whose gate count is only around 200. An important property of this design is that the cross point (i.e., the calibrated frequency) of the two frequencies must be constant even for different PVT conditions as shown in Fig. 4.

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 mainly performed before each detection operation, and each detection operation is performed in a timely fashion before and during cryptographic operation. If a sufficiently large frequency difference is detected, a detection signal is generated by the control logic circuit.

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

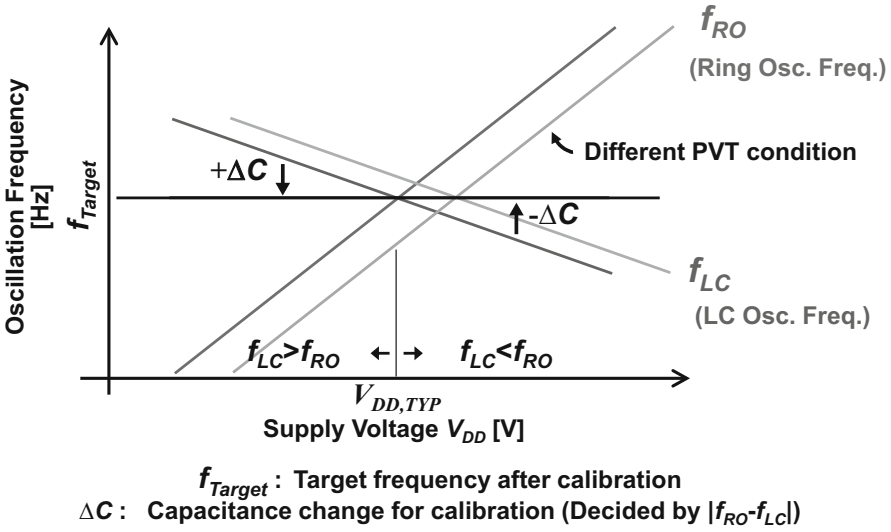

Fig. 4. Calibration scheme.

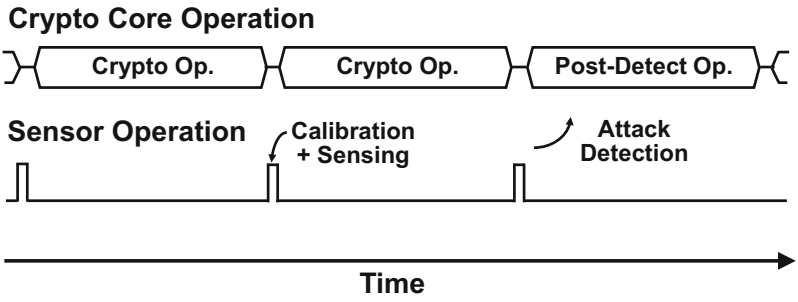

Fig. 5. Intermittent sensor operation.

protected. The coil size is also scalable due to transistor performance improvement in device scaling because the operation frequency of the transistor is increased to reduce the required self-inductance of the coil and hence the physical coil size.

We assume that the sensor monitors for probe approach intermittently and periodically as shown Fig. 5, which saves power overhead and also minimizes the performance overhead due to this additional sensor circuits. In addition, the LC oscillators do not interfere with the cryptographic core since the sensor is usually activated while the cryptographic core is idle. No correlation between the cryptographic core operation and the EM field is generated by the LC oscillator. When the sensor detects a probe approach, the cryptographic core operation can then be changed to, for example, a lock mode to simply stop the cryptographic operation or a dummy key mode using a fake secret key to protect the actual secret key.

Figure 6 shows the proposed design flow using conventional circuit and physical layout design tools for the sensor described above. The cryptographic and sensor cores are first described by a conventional hardware description language (e.g., Verilog HDL

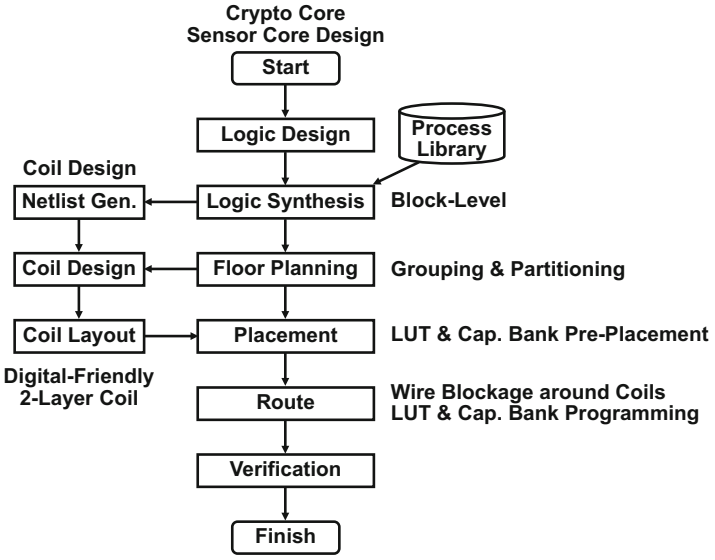

Fig. 6. Design flow.

or VHDL) 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 the 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 shape of the total layout including the cryptographic and sensor cores is fixed at the floor planning step, which determines the overall coil size (i.e., length and width) to cover all the circuit blocks by the coils.

The coil design starts with the fixed coil length and width. First, we determine the number of coil turns N, which approximately determines the oscillation frequency since the self-inductance of the coil is proportional to N^2 and hence has strong dependence on N. Also, because N is basically a discrete number and therefore difficult to use for parameter adjustment, it should be determined initially. The wire width is then adjusted to ensure stable oscillation. A wide wire reduces the parasitic resistance R of the coil and so reduces the electrical loss in the coil. The wire should be wide enough to meets the oscillation condition $R < 1/g_m$, but increased wire width comes at the expense of using more interconnection resources to make the coil wire. This overhead can be mitigated by providing more power consumption because $1/g_m$ can be increased by increasing the current dissipation in the g_m cell. Finally, the gap between the coil wires is adjusted to fine-tune the oscillation frequency. Then, SPICE, Spectre, or other circuit simulator is used to perform a circuit simulation with the coil parameters for a range of possible PVT conditions. Then, we determine the required capacitor bank structure (i.e., the range and step size of capacitance values). Unit capacitors with some margin are prearranged at the placement step, and then the actual bank structure is constructed at the following routing

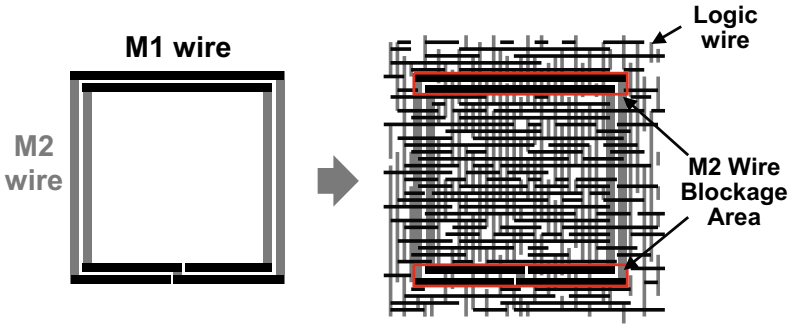

Fig. 7. Orthogonal two-layer coil layout.

step by hardwire 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 layout parameters determined in the previous coil design stage. Note here that we can utilize digital layout grids to provide the width and spacing of wires. An extremely fine minimum layout grid is not necessary for the coil layout parameter design. Stable oscillation can be guaranteed by additional power consumption in the g_m cell. To reduce the interconnection resources required for the coil, a digital-friendly two-layer coil layout style [18] is employed, where the coil is drawn by two different metal layers for orthogonal edges (Fig. 7). For example, an odd-numbered metal layer is used for the vertical edges, and even-numbered metal layer is used for the horizontal edges in order to follow the layout rule with the digital logic interconnections in an automatic routing tool. This layout style enables the coil to be hidden in the sea of logic interconnections for enhanced security and also greatly reduces the required interconnection resources by allowing the logic interconnections to go through the coil. The coil consumes only interconnection resources at the coil edges, requiring only several tens of logic interconnection tracks. Electrical loss, which governs the Q factor of the on-chip coil, is a crucial factor in a conventional analog coil design, such as a design for high-frequency low-jitter clock generation by an LC oscillator or an on-chip RF band-pass filter with sharp cutoff characteristics. The on-chip coil used for this sensor does not require a high Q factor since the jitter (phase noise) in the LC oscillator for the sensor has no impact on detection accuracy. The large jitter causes only instantaneous variation in the oscillation frequency not averaged oscillation frequency. This sensor counts the number of clock pulses for a relatively long time and considers only the averaged oscillation frequency. A thick upper metal layer is therefore not necessary for the coil to reduce the loss and thereby enhance the Q factor. Thus, the coil can be designed and fabricated by a standard digital process without any analog/RF options, further lowering the design and fabrication costs.

At the final place and route step, the only design constraint is a wiring blockage for the coil edges to place the sensor coil drawn in the two-layer coil layout style [18]. At first, we determine the placement of the cryptographic and sensor cores, including the capacitor bank and LUT. Next, the sensor coils are placed to cover the circuit components to be protected. Finally, automatic routing is done with the wiring blockage for only the coil edges. In this routing process, the capacitor bank structure (the range and step of

the capacitance value for calibration) is finally constructed by hardwire programming between the capacitor bank and the LUT. The capacitor bank generated here has n capacitor blocks of different binary-weighted capacitance sizes, and therefore encodes $2^n - 1$ capacitance values for the n-bit digital Ccode input. Finally, we can verify the overall functionality with a digital verification tool because the input and output of the sensor core are digital. The sensor performance is accurately verified by the analog circuit simulation including the extracted parasitic resistance and capacitance in the post-layout simulation.

4. Validity Verification

4.1. *Setup*

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: a single microprobe approaching during the sensing period, a larger microprobe approaching during the sensing period, a single microprobe approaching while the supply voltage is being changed, and a single microprobe approaching before the sensing period (i.e., during the sleep period). The first scenario assumes a conventional microprobe-based EM attack, such as the ones described in [15] and [21], where attackers move a microprobe close to the core surface while the sensor is working. The second scenario assumes an attempt to avoid detection by a larger probe crossing the two coils. This scenario is equivalent to EMA with two microprobes close to the two coils at the same time. The third scenario assumes that the attacker manipulates the PVT conditions to confuse the sensor. The fourth scenario assumes that the attacker can place a microprobe 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 0.18-μm CMOS process by commercial CAD tools. More precisely, we used Design Compiler (G-2012.06-SP3) for logic synthesis, IC Compiler (vH-2013.03-SP2) for place and route, and Virtuoso (6.1.4) for coil design. Figure 8 shows a die photograph and the measurement setup. Two coils [a four-turn coil (L1) and a three-turn coil (L2)] were placed above an AES processor. The L1 (L2) coil had resistance of 76 Ω (55 Ω), capacitance of 68 fF (64 fF), inductance of 13.2 nH (8.5 nH), and oscillation frequency of 5.4 GHz (6.8 GHz) 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 [6]. The test chip was mounted on a side-channel attack standard evaluation board (SASEBO R-II) [20]. An EM microprobe was fixed on a manipulator, and its position was controlled manually under a microscope. We conducted microprobe-based EMA using EM waveforms observed in the experimental setup, where the EM signal from the probe was amplified by a 100 W power amplifier with 40 dB gain.

4.2. *Results*

Figure 9 shows the frequency spectra of L1 and L2 in the presence and absence of a microprobe of 1.0 mm in diameter. The oscillation frequency of each coil was clearly

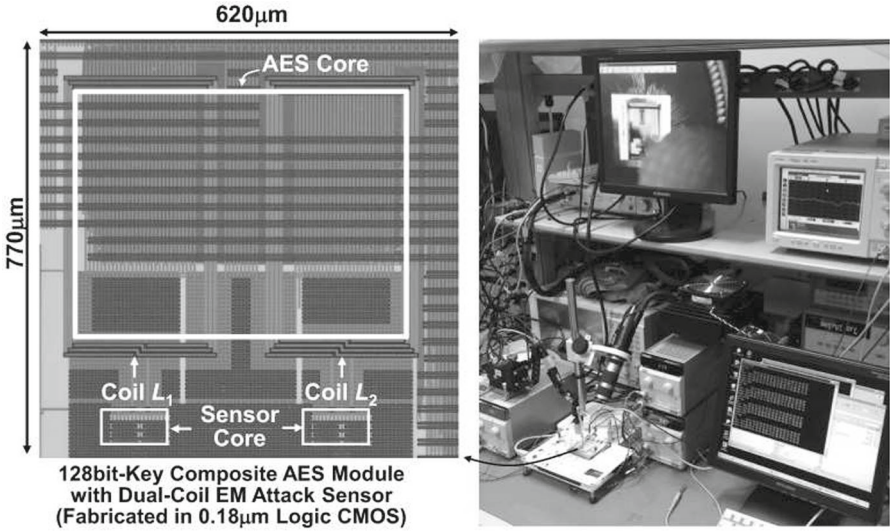

Fig. 8. Die photograph and measurement setup.

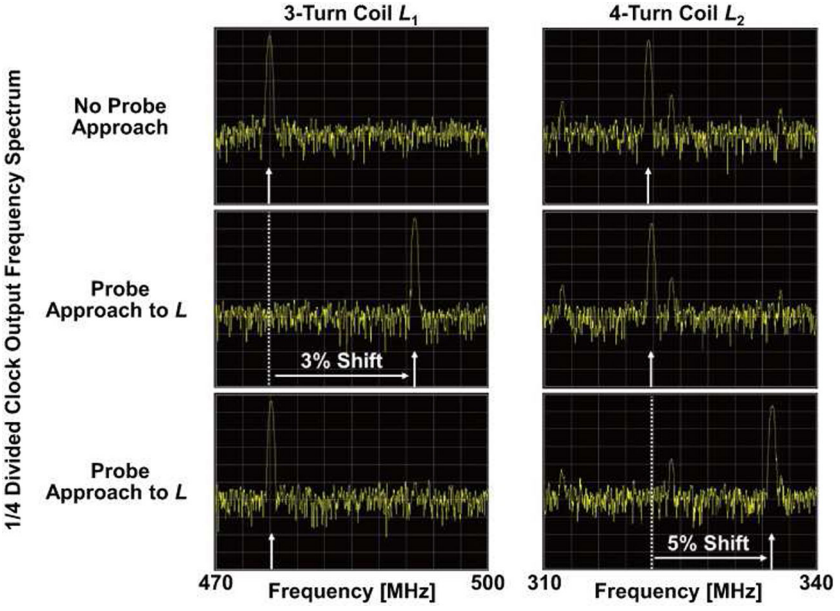

Fig. 9. Frequency shift caused by an approaching probe.

shifted by the probe, even at a distance of about 100 μm. In addition, Fig. 10 shows maps of absolute shift rates when smaller probes were moved on the chip surface. The upper and lower maps were generated from the results using two pseudo probes (conductive wires) of 0.2 and 0.3 mm in diameter. The shift rate at each point was measured by

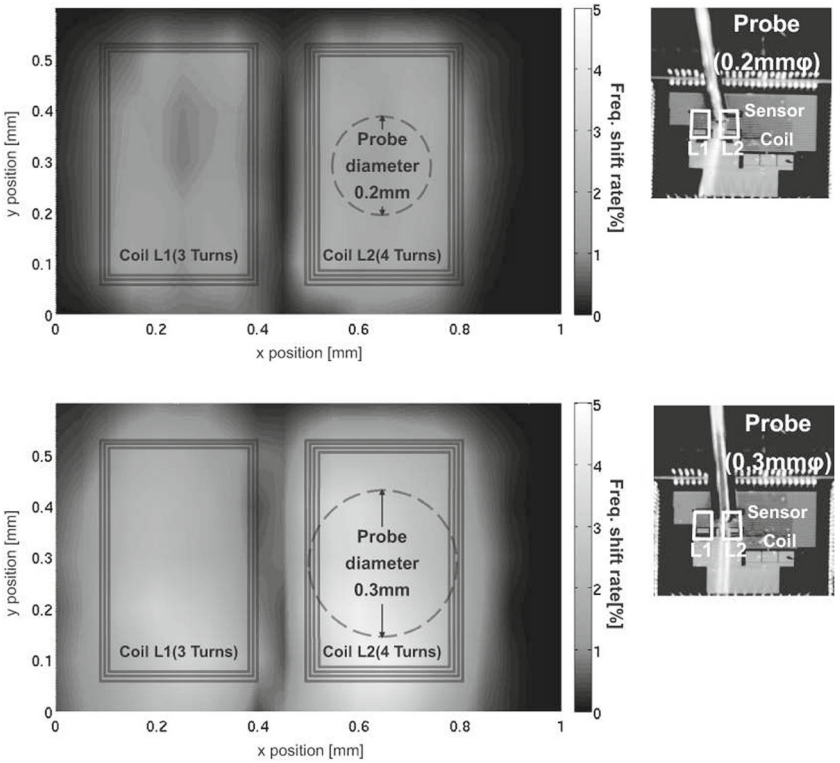

Fig. 10. Shift rate maps for probes of **a** 0.2 mm and **b** 0.3 mm in diameter.

positioning the center of the probe head at the point on the chip surface. Note that, basically, only one coil was affected by these small probes. We confirmed that a shift rate of at least about 1 % can be observed inside and on the coils, even in the case of the 0.2-mm probe. The results indicate that microprobe-based EM attacks such as those assumed in the first scenario can be easily detected by the sensor and also that the most critical components (e.g., S-boxes) should be located near or under the coil wire in order to detect a probe approach with certainty.

Figure 11 shows the difference in frequency shift between L1 and L2 for various distances between the coils and the probe with diameter of about 1.0 mm. The shift rate 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, there would still be substantial difficulty matching the shifts, which are determined by many coil parameters, while performing high-density EM measurements. These results indicate that EM attacks with two microprobes are also detectable.

Figure 12 shows the difference in frequency shift between L1 and L2 for various probe positions in the horizontal direction, where the probe position was moved in 50 μm steps. We confirmed that the frequency shifts of the two oscillators changed with probe position

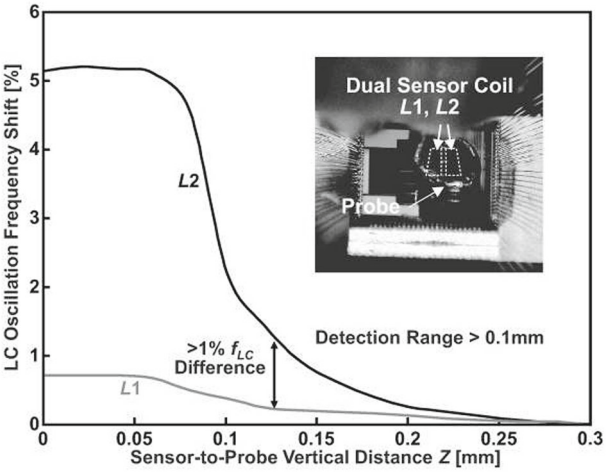

Fig. 11. Difference in frequency shift between L1 and L2 for different probe distances in the *vertical direction*.

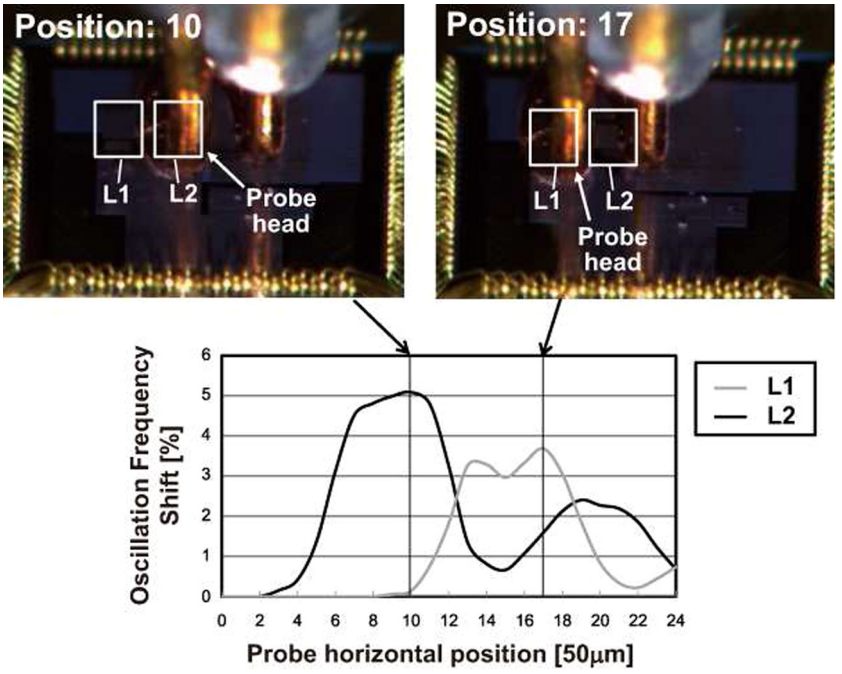

Fig. 12. Difference in frequency shift between L1 and L2 for different probe positions in the *horizontal direction*.

in a complementary fashion. Figure 12 also shows photos of the probe positions 10 and 17. Here, too, the results indicate that the shift amount is larger when the probe head is located just above the coil wire. Note that it is difficult for attackers to measure such shift amounts though both shift amounts are balanced at around positions 12 and 18.

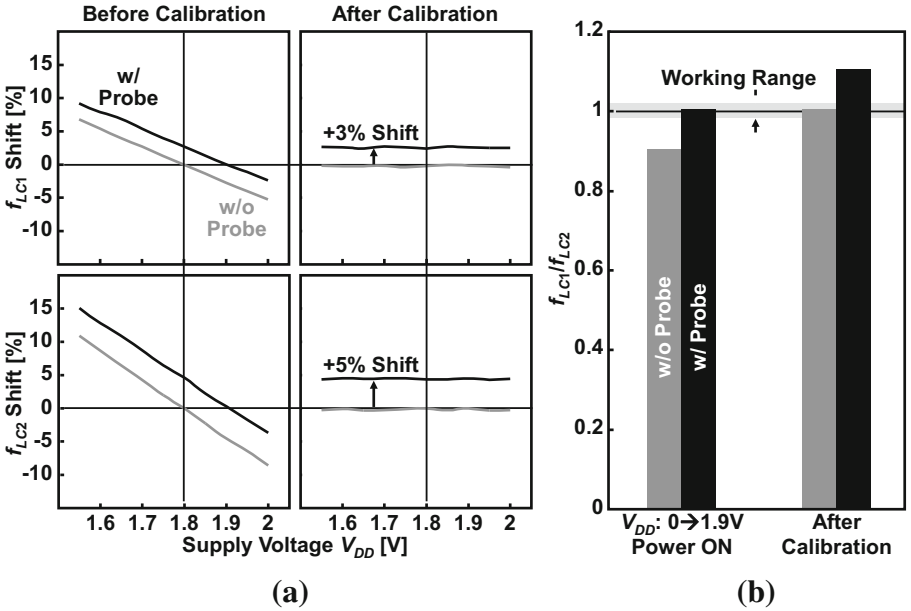

Fig. 13. Frequency shifts before and after calibration.

Figure 13a presents the frequency shift dependence on the supply voltage VDD, where the left and right panels of the figure show the magnitude of frequency shifts before and after the calibration, respectively. The proposed one-step digital calibration suppresses f_{LC} variation to within $\pm 1\,\%$ over the temperature range of 0–60 °C at VDD voltage of 1.6–2.0 V; this f_{LC} variation corresponds to variation exceeding $\pm 10\,\%$ from the nominal VDD voltage of 1.8 V. These results show that the proposed sensor is robust against PVT variation since the same calibration method is applicable to a range of possible PVT conditions.

Figure 13a also shows that the sensor can thwart an attack under the third/fourth scenario. The frequency shift due to the approaching probe remains after calibration. The results indicate 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 wakeup. Figure 13b presents the results for a sophisticated case under the third/fourth scenario, where the attacker can manipulate the supply voltage and suppress f_{LC} variation to within the working range ($\pm 1\,\%$) with a microprobe close to the core surface just after the power is switched on. This attack 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 I/O pins, such as a smartcard, which can be targeted by microprobe-based EMA. Such device usually equips serial I/O and outputs the data at each time. This intermittent sensor operation at $<1\,\%$ duty

Table 1. Overheads caused by sensor.

	AES core	Sensor	Total (sensor overhead)
2NAND gate count	24.3 k	0.3 k	24.6 k (+1.2 %)
Wire resource	0.40 mm^2	0.05 mm^2	0.45 mm^2 (+11 %)
Layout area	0.48 mm^2	0.01 mm^2	0.49 mm^2 (+2 %)
Performance	125 µs/Enc	0.3 µs/Sense	125.3 µs (−0.2 %)
Power consumption	0.23 mW	0.02 mW	0.25 mW (+9 %)

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.

5. Discussion

The experimental results show that 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 algorithmic- and circuit-level countermeasures. EM fault-injection attacks using a microneedle probe, such as those in [2,7,14,19], 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 robustly detect EM analysis and fault-injection attacks performed close to or on the LSI surface.

The proposed sensor is also invulnerable to frequency-injection attacks. First, attackers must measure the original frequency very close to the coil surface but cannot measure it without disturbing it. 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 would affect another oscillator. Note again that the oscillation frequencies are different from one another. 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 this 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. For example, such reverse engineering would easily be recognized by the cryptographic core if the oscillation frequency of the LC oscillator or its substitute signal were supplied to the cryptographic core as an enable signal.

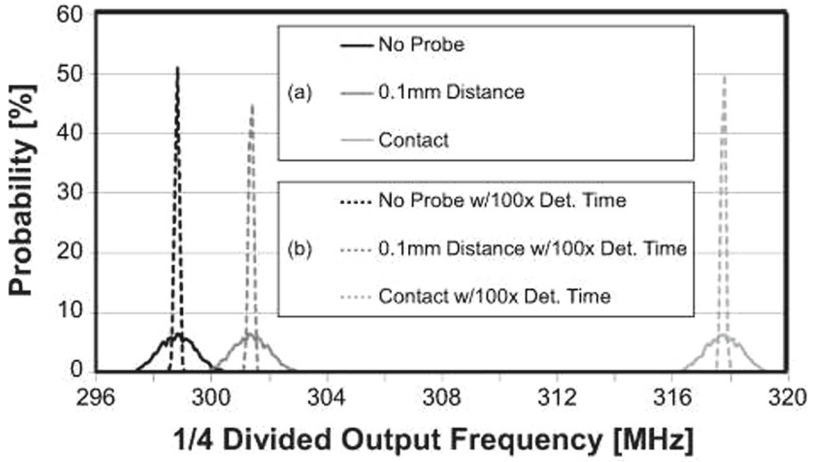

Fig. 14. Distribution of shift amounts: (*a*) 100 single measurements and (*b*) 100 averaged measurements.

The detection distance between the probe and the sensor is limited to a maximum of 0.1 mm in our experimental setup. The limited maximum detection distance means that conventional EMAs on the chip package such as differential EMA and correlation EMA 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. This could be accomplished in several ways. For example, we could use a longer detection time. Figure 14 shows the shift amounts of (a) 100 single measurements and (b) 100 averaged measurements, where each value in (a) indicates an oscillation frequency at a single observation time, and each value in (b) indicates an average frequency of 100 observations. In other words, we used a 100-fold longer time to obtain each value in (b). The probe-to-chip distances are 0 (i.e., contact) and 0.1 mm. For comparison, the figure also shows the original frequencies without any probe. The sensor is required to distinguish the original frequency and the shifted frequency. It is interesting to note that though a frequency shift due to the presence of a probe at a distance of 0.1 mm can be recognized even in the case of (a), it is more clearly recognized in the case (b) because of the lower variance. Thus, a longer detection time has the potential to extend the maximum detection distance. Another possibility is to change the size of coils for detection. Larger coils, a greater number of turns, or both would increase the effects of inductance coupling. Extending the maximum distance may enable the sensor to detect a wider variety of attacks including chip unpacking as well. For example, we plan to study detection of backside attacks in future studies. At the same time, the proposed sensor can be combined with any other conventional countermeasures because of its low area and performance overheads. In practice, conventional countermeasures and the proposed technique would work well in combination and would complement each other.

As shown above, the trade-off between detection capability and performance overheads is adjusted by changing the timing of sensor operation. The sensor can operate continuously during cryptographic operations for increased security. Figure 15 shows the frequency shifts with and without AES operation for different distances between

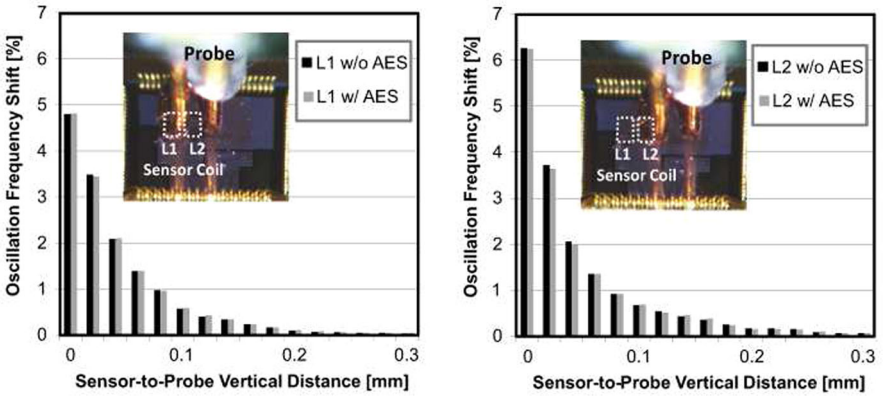

Fig. 15. Frequency shifts with and without AES operations for different probe distances.

the coils and the probe (diameter: 1.0 mm), where the experimental setup was the same as in the above experiments. We found that the effects of EM radiation from the AES processor were trivial, and the above intermittent sensor operation was not required if the performance overhead was critical and should be reduced. On the other hand, intermittent operation to reduce the power consumption 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 be examined in future work.

The general EMC of the resulting IC is not decreased by the sensor. This is because the sensor coils constitutes a part of the upper-level wire mesh and work at a close distance within the IC package. The immunity to EM injection is basically the same as the corresponding IC without the sensor. It is worth noting again that the sensor detects the change in mutual inductance and does not directly detect the change in the surrounding power. On the other hand, it would be a fail-safe operation to detect a conductive wire very close to a bare chip surface without any package.

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 an EM microprobe 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 digital sensor calibration based on LUT programming can prevent such EM attacks in various scenarios where one or more EM microprobes 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, were semiautomatically designed by 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 the 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. Though the overheads were given for the case of an AES processor with a loop architecture, the proposed sensor would still be effective in a smaller architecture. This is because the coil size can be scaled depending on the protected cryptographic core, and the gate count of the sensor core is only 300 which is equivalent to that of a single AES S-box circuit. 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.

Acknowledgements

The authors are deeply grateful to Mr. Daichi Tanaka and Mr. Daisuke Ishihata for their valuable help. This work has been supported by JSPS KAKENHI Grant No. 26240005.

References

[1] D. Agrawal, B. Archambeault, R. Rao, and P. Rohatgi. The EM side-channel(s), in *CHES 2002, Lecture Notes in Computer Science*, vol. 2523 (Aug. 2002), pp. 29–45.

[2] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robisson, and P. Maurine. Contactless electromagnetic active attack on ring oscillator based true random number generator, in *COSADE 2012* (May 2012), pp. 151–166.

[3] A. Beit-Grogger, and J. Riegebauer. Integrated circuit having an active shield. *United States Patent* no. 6,962,294, 2005.

[4] S. Briais, S. Caron, J.-M. Cioranesco, J.-L. Danger, S. Guilley, D. Naccache, and T. Porteboeuf. 3D Hardware Canaries, in *CHES 2012, Lecture Notes in Computer Science*, vol. 7428 (Sept. 2012), pp. 1–22.

[5] S. Briais, J.-M. Cioranesco, J.-L. Danger, S. Guilley, J.-H. Jourdan, A. Milchior, D. Naccache, and T. Porteboeuf. Random active shield, in *FDTC 2012* (Sept. 2012), pp. 103–113.

[6] Cryptographic Hardware Project, http://www.aoki.ecei.tohoku.ac.jp/crypto/, Aug. 2007.

[7] A. Dehbaoui, J.-M. Dutertre, B. Robisson, P. Orsatelli, P. Maurine, and A. Tria. Injection of transient faults using electromagnetic pulses—practical results on a cryptographic system, ePrint, 2012/123, 2012.

[8] K. Gandolfi, C. Mourtel, and F. Olivier. Electromagnetic analysis: Concrete results, in *CHES 2001, Lecture Notes in Computer Science*, vol. 2162 (May 2001), pp. 251–261.

[9] N. Homma, Y. Hayashi, N. Miura, D. Fujimoto, D. Tanaka, M. Nagata, and T. Aoki. EM attack is non-invasive? Design methodology and validity verification of EM attack sensor, in *CHES 2014, Lecture Notes in Computer Science*, vol. 8731 (Sept. 2014), pp.1–16.

[10] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis, in *CRYPTO 1999, Lecture Notes in Computer Science*, vol. 1666 (Aug. 1999), pp. 388–397.

[11] P. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems, in *CRYPTO 1996, Lecture Notes in Computer Science*, vol. 1109 (Aug. 1996), pp. 104–113.

[12] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks - Revealing the Secrets of Smart Cards*. (Springer, 2007).

[13] N. Miura, D. Fujimoto, D. Tanaka, Y. Hayashi, N. Homma, T. Aoki, and M. Nagata. 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* (June 2014), pp. 172–173.

[14] N. Moro, A. Dehbaoui, K. Heydemann, B. Robisson, and E. Encrenaz. Electromagnetic fault injection: towards a fault model on a 32-bit microcontroller, in *FDTC 2013* (Aug. 2013), pp. 77–88.

[15] E. Peeters, X. Standaert, and J. Quisquater. Power and electromagnetic analysis: improved model, consequences and comparisons. *Integr. VLSI J.*, 40(1):52–60, 2007.

[16] J. Quisquater, and D. Samyde. Electromagnetic analysis (EMA): Measures and counter-measures for smart cards, im *E-Smart 2001, Lecture Notes in Computer Science*, vol. 2140 (Sept. 2001), pp. 200–210.

[17] D. Réal, F. Valette, and M. Drissi. Enhancing Correlation Electromagnetic Attack Using Planar Near-Field Cartography, in *DATE 2009* (2009), pp. 628–633.

[18] M. Saito, K. Kusaga, T. Takeya, N. Miura, and T. Kuroda. An Extended XY Coil for Noise Reduction in Inductive-coupling Link, *A-SSCC Dig. Tech. Papers* (Nov. 2009), pp. 305–308.

[19] J.-M. Schmidt, and M. Hutter. Optical and EM fault-attacks on CRT-based RSA: concrete results, in *Austrochip 2007* (Oct. 2007), pp. 61–67.

[20] Side-channel Attack Standard Evaluation Board (SASEBO-RII), http://www.risec.aist.go.jp/project/sasebo/, 2012.

[21] T. Sugawara, D. Suzuki, M. Saeki, M. Shiozaki, and T. Fujino. Measurable side-channel leaks inside ASIC design primitives, in *CHES 2013, Lecture Notes in Computer Science*, vol. 8086 (Aug. 2013), pp. 159–178.

[22] D. Suzuki, M. Saeki, and T. Ichikawa. Random switching logic: a countermeasure against DPA based on transition probability. *IACR Cryptol. ePrint Arch.* 2004:346, 2004.

[23] K. Tiri, D. Hwang, A. Hodjat, B.-C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede. Prototype IC with WDDL and differential routing - DPA resistance assessment, in *CHES 2005, Lecture Notes in Computer Science*, vol. 3659 (May 2005), pp. 354–365.

[24] J.A.J. Van Geloven, R.A.M. Wolters, and N. Verhaegh. Sensing circuit for devices with protective coating. *United States Patent* no. US 2010/0090714 Al, 2010.