*URSI AP-RASC, Sydney, Australia, 17 – 22 August 2025*

# H-field probe Detection Method under Supply Voltage Fluctuation using Time Series Variation of Oscillation Frequency Difference of Multiple Ring Oscillators

Koki Abe, Daisuke Fujimoto, and Yuichi Hayashi
Nara Institute of Science and Technology, Nara, Japan

## Abstract

An electromagnetic (EM) analysis attack has been reported to reveal secret keys by measuring and analyzing changes in EM fields generated by the operation of cryptographic circuits. Against such attacks, it is effective to detect the H-field probe in the measurement stage, which is the preliminary stage of the analysis. In response to this, a method has been proposed to detect H-field probes by forming a metallic film directly above the chip that is capacitively coupled to the H-field probe and capturing the capacitance change as a frequency change of the Ring Oscillator (RO). In this method, the sensitivity of the RO to variations in power supply voltage is an issue, and a method that eliminates only DC variations from the frequency difference of multiple ROs has been considered. Therefore, there is a possibility of false detection for voltage fluctuations that vary over time.

In contrast, this paper proposes a method to reduce temporal power supply voltage fluctuations by utilizing the time variation of the frequency difference between multiple ROs. In experiments, it is shown that the effect of power supply voltage fluctuation on the oscillation frequency of ROs for sensors can be reduced in an environment where the power supply voltage fluctuates. As a result, it is shown that it is possible to detect the H-field probe at a distance of 8 mm as stably as in an environment where the power supply does not fluctuate.

## 1. Introduction

Electromagnetic analysis (EMA) attacks are attacks that obtain secret keys by measuring and analyzing changes in electromagnetic (EM) fields caused by the operation of cryptographic circuits. This attack is a realistic threat because it can be performed with a relatively inexpensive setup [1, 2].

Countermeasures against EMA attacks at the algorithm level [3] and at the circuit level [4] have been considered. However, since countermeasures are taken on a specific algorithm or circuit, there is a possibility that they can be revealed when analysis techniques become more accurate for a particular algorithm/circuit. On the other hand, since the EMA attack measures EM fields in the first phase, it is possible to take countermeasures independent of the algorithm/circuit by making the measurement difficult. Measuring difficulties can be achieved by means such as stopping the cryptographic process at the time of the attack or executing a dummy process [5]. To implement this countermeasure, it is necessary to detect EM field measurements which are done by the H-field probe.

As a detection technique for H-field probes, a method for detecting EM coupling with H-field probe has been proposed by including a sensing front end external to the IC in a Ring Oscillator (RO) that can be configured using only digital circuits [6]. In this method, the frequency is calibrated according to the supply voltage value based on the frequency difference between the RO containing the wiring outside the chip and the RO configured inside the chip, which has weak coupling to the outside. This method was shown to be able to detect H-field probes from the oscillation frequency difference even when a DC change in the supply voltage occurs. However, it cannot follow changes in power supply voltage that vary over time. Therefore, an attacker could exploit this to fail to detect the presence of H-field probes or to shut down the system due to false positives.

In this paper, we propose a calibration method that follows the time variation of the power supply voltage by evaluating the frequency difference in time intervals. We show that this frequency calibration enables the detection of H-field probes even under power supply voltages intentionally manipulated by an attacker.

## 2. A method for reducing the effect of power supply fluctuations on RO-based H-field probe detection

### 2.1 Detection of change in parasitic capacitance due to the approach of H-field probe

In measurement using an H-field probe, parasitic capacitance is generated because the H-field probe is capacitively coupled with electronic components and board circuitry when it approaches. In order to directly measure this parasitic capacitance, it is necessary to implement an analog circuit to measure. On the other hand, if the H-field probe is capacitively coupled to the wiring for signal

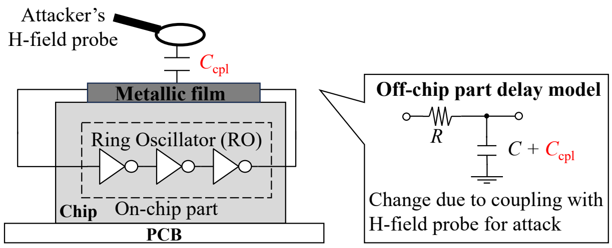


**Figure 1.** Image of detection method using change in delay time due to EM coupling with H-field probe.

transmission, the transmission delay changes. Therefore, it may be possible to detect the approach of the H-field probe from the change in transmission delay. Reference [6] uses the oscillation frequency change of an RO as a detection circuit that does not require a sampling circuit with high time resolution.

Figure 1 shows the principle of H-field probe detection by observing the capacitance coupling between the metallic film outside the chip and the H-field probe as a variation in oscillation frequency. The circuit that constitutes the H-field probe detection is divided into an on-chip part, which is the inverter chain, and an off-chip part, which serves as the sensor for the H-field probe detection. The propagation delay τ that causes the oscillation frequency variation is expressed as follows using the propagation delay $\tau_{\text{on\_chip}}$ of the on-chip part and the propagation delay $\tau_{\text{off\_chip}}$ of the off-chip part.

$$\tau = \tau_{\text{on\_chip}} + \tau_{\text{off\_chip}} \quad (1).$$

The propagation delay $\tau_{\text{off\_chip}}$ is expressed as follows using the resistance $R$, capacitance $C$, and parasitic capacitance $C_{\text{cpl}}$ of the metallic film and H-field probe in the off-chip part [7].

$$\tau_{\text{off\_chip}} = R\left(C + C_{\text{cpl}}\right) \quad (2).$$

The parasitic capacitance $C_{\text{cpl}}$ changes the propagation delay τ and the oscillation frequency of the RO, thus enabling the detection of the H-field probe.

## 2.2 Decrease in detection accuracy due to temporal fluctuations in power supply

On the other hand, other factors that can change the propagation delay of RO include changes in parasitic capacitance as well as fluctuations in the supply voltage. In Reference [6], to address variations in supply voltage, the frequency was calibrated using RO ($RO_{\text{reference}}$), which has a weak coupling to the H-field probe and whose propagation delay changes only with changes in supply voltage, and RO ($RO_{\text{sensor}}$), whose propagation delay changes with changes in supply voltage and parasitic capacitance (Figure. 2(a)). If both $RO_{\text{reference}}$ and $RO_{\text{sensor}}$ propagation delays fluctuate, it can be determined that the supply voltage has fluctuated, and if only $RO_{\text{sensor}}$ propagation delay fluctuates, it can be estimated that the H-field probe is approaching (Figure 2(b)). This enables H-field probe detection even in environments with different supply voltages.

However, this calibration method assumes stable supply voltage differences. Therefore, it may not work in environments with large temporal variations in power supply voltage fluctuations or when an attacker intentionally fluctuates the power supply voltage. As shown in Figure 2(c), when there are temporal power supply voltage fluctuations, the change in the oscillation frequency of the $RO_{\text{reference}}$ has an estimated width in a certain power supply voltage range, resulting in an uncertain estimation. As a result, the H-field probe may not be detected even if it is present, or it may be falsely detected when it is not present.

## 2.3 Methods to improve detection accuracy under time-varying power supply

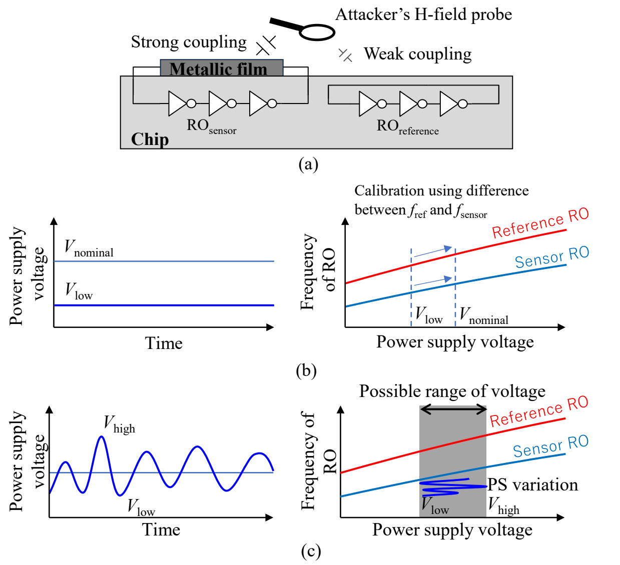


**Figure 2.** Image of a method for reducing supply voltage effects using multiple ROs (a) Configuration of multiple ROs with different electromagnetic coupling to the H-field probe (b) Frequency calibration during DC variation (c) Limitations of conventional calibration methods during time-varying power supply

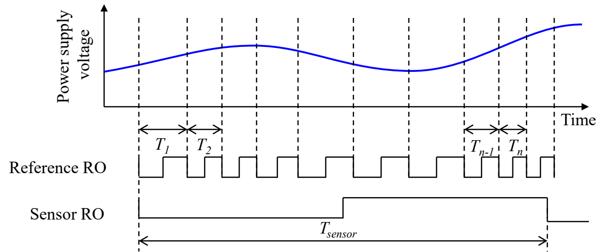


**Figure 3.** Image of estimated power supply effect due to period difference between reference RO and sensor RO.

To address time-varying supply voltage, it is sufficient to be able to estimate time-varying voltage from changes in the oscillation frequency of the $RO_{\text{reference}}$. Since the $RO_{\text{sensor}}$ is an oscillator propagating on a line outside the chip, its frequency is low relative to the $RO_{\text{reference}}$. In other words, there are multiple cycles of $RO_{\text{reference}}$ for each cycle of $RO_{\text{sensor}}$ oscillation. Therefore, as shown in Figure 3, each $RO_{\text{reference}}$ period $T_n$ can be used to reflect the voltage fluctuation in a certain time interval, and by measuring the $RO_{\text{reference}}$ period $T_n$ for one period of the $RO_{\text{sensor}}$, the power supply voltage fluctuation can be predicted, and the frequency when the power supply voltage is stable can be calculated. The frequency when the power supply voltage is stable can be calculated. This eliminates the influence of power supply fluctuations, enabling only the frequency change due to the presence of the H-field probe to be evaluated and the H-field probe to be detected.

# 3. Experiments to reduce the effect of power supply noise

## 3.1 Experimental setup

Figure 4 shows the setup of the H-field probe detection experiment using RO. In Figure 4 (a), the block diagram of the experimental setup is represented. The attacker's setup is a magnetic field probe (Langer EMV RF-U 5-2). The target of the attack was a field-programmable gate array (FPGA) (Xilinx Artix XC7A35T) on an evaluation board. A regulated power supply (GW INSTEK GPD-4303S) was used to supply power to the FPGA. To simulate a fluctuation of power supply, a Function Generator (FG) (NF WF1968) was used to inject a 1 MHz signal into the power line via a DC block to the SMA port connected to the power plane, with an amplitude of 50 mV, which corresponds to 5% of the rated voltage. A single-stage $RO_{sensor}$ connected to the wiring outside the chip and a three-stage $RO_{reference}$ inside the chip are implemented on the FPGA. In order to increase the time constant of propagation delay, $RO_{sensor}$ connects a copper foil that serves as a sensor and a resistor (1.0 kΩ) on the wiring outside the FPGA as in the previous work [6]. The oscillation frequency of $RO_{reference}$ is 233 MHz and that of $RO_{sensor}$ is 27.1 MHz. The oscillation signal generated by the RO is output from the input/output (IO) pin and acquired using an active probe (Keysight N2795A), and oscilloscope (Keysight EXR204A) to measure the oscillation frequency and evaluate the frequency change due to the supply voltage and the approach of the H-field probe. Because the $RO_{reference}$ would exceed the frequency at which the IO pin can transition correctly if the signal is output as is, a divided signal is output to the IO pin. Figure 4 (b) shows a side view of the experimental setup. The copper foil capacitively coupled to the H-field probe is placed over the FPGA, and wiring is drawn from the diagonal of the copper foil and connected to the I/O of the FPGA to form the external wiring of the $RO_{sensor}$. The distance between the H-field probe and the chip was defined to be vertical to the copper foil on the chip. The distance between the H-field probe and the copper foil wiring on the chip was changed from 0 mm (contact) to 16 mm at 2 mm intervals, and the oscillation frequency was measured.

## 3.2 Validation of H-field probe detection method under power fluctuation

Figure 5 shows the power supply line's time-domain waveform when the H-field probe is placed directly above the chip. When FG's output is OFF, random voltage fluctuations with no periodicity are observed. When FG's output is ON, a 1 MHz period is observed with an amplitude of about 90 mV. Figure 6 shows the RO sensor's oscillation frequency distribution under conditions with and without voltage fluctuations. Measurements were taken with the H-field probe directly above the chip. When the FG's output is OFF, the frequency distributions with and without the H-field probe are clearly separated, allowing for H-field probe detection. However, when the FG's output is ON, the frequency distribution increases by about 470% compared to when the FG's output is OFF. As a result, the distinction between the two distributions disappears, making H-field probe detection difficult.

Figure 7 shows the distribution of the oscillation frequency of the $RO_{sensor}$ with and without the probe after calibration. First, the variation of the supply voltage is estimated based on the oscillation frequency of the $RO_{reference}$ and its calibration function. Next, the difference between the

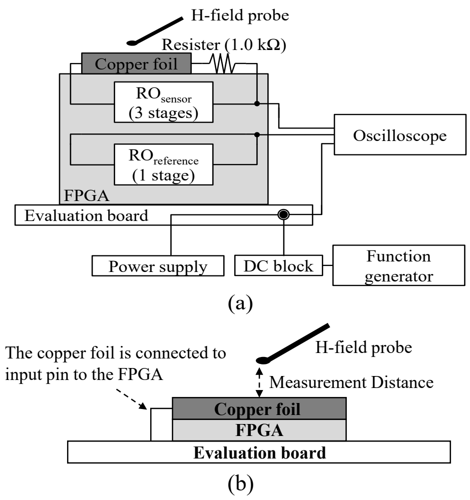


**Figure 4.** Experimental setup (a) Block diagram of the experimental setup (b) Side view of the experimental setup.

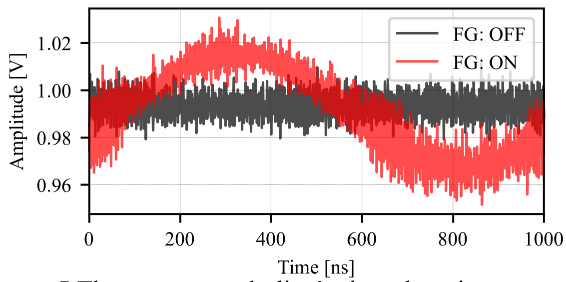


**Figure 5** The power supply line's time-domain waveform.

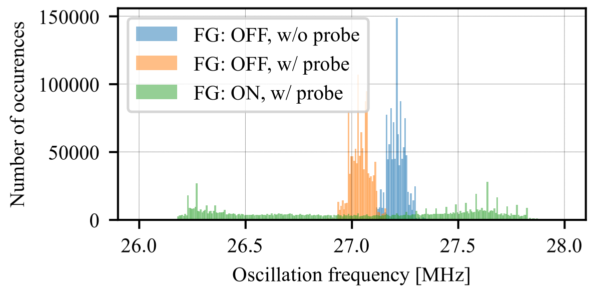


**Figure 6.** The distribution of the oscillation frequency of the $RO_{sensor}$ with and without voltage fluctuations.

estimated voltage value obtained and the nominal voltage (1.000 V) supplied by the regulated power supply is calculated, and this difference is applied to the calibration function of the $RO_{sensor}$ to estimate the amount of variation in the oscillation frequency of the $RO_{sensor}$. Finally, the estimated amount of variation is corrected by subtracting the estimated amount of variation from the actual measured oscillation frequency of the $RO_{sensor}$. The calibration functions of $RO_{reference}$ and $RO_{sensor}$ were obtained by creating regression models from the respective oscillation frequencies and corresponding voltage values. The histograms before and after calibration show that the frequency range is reduced by calibration, and the spread of the distribution is suppressed to about 189% compared to when the FG is OFF. This indicates that calibration suppresses the effect of supply voltage fluctuations on the $RO_{sensor}$. On the other hand, comparing the histograms before calibration while FG's output is ON and OFF, it can be seen that the range of frequencies is wider, and the mode frequency is different when FG's output is ON. The reason for the wider range in the histogram is probably that it is difficult to suppress supply voltage fluctuations below the $RO_{reference}$ period. The reason for the difference in the mode frequency is thought to be that even if 1 V is supplied from the regulated power supply, a voltage drop occurs in the actual system, and the DC value drops below 1.0 V under the condition that FG's output is OFF.

Figure 8 shows the variation of the oscillation frequency of $RO_{sensor}$ when the distance between the H-field probe and the copper tape on the chip is changed. The horizontal axis represents the distance between the chip and the copper tape, and the vertical axis represents the difference (amount of shift) from the oscillation frequency without the H-field probe. When the distance between the copper tape and the H-field probe is between 0 mm and 8 mm, the approach of the H-field probe can be clearly detected because of the large shift in the oscillation frequency. When the distance is 10 mm, the shift is the smallest, and the H-field probe is difficult to detect. When the distance is 12 mm or more, the amount of shift is convergent, and the H-field probe is difficult to detect. These results indicate that the proximity of the H-field probe can be detected within a certain distance range, even in an environment where the voltage fluctuates over time.

In this paper, the period obtained from oscilloscope measurements was used for calibration to demonstrate the feasibility of the proposed method, but the accuracy of period measurement affects the calibration when the sensor is configured closed inside the IC. The impact of the accuracy of the period measurement is future work.

# 4 Conclusion

In this paper, we studied a technique for detecting H-field probes at the measurement stage against side-channel attacks, a realistic attack on cryptographic circuits. The RO-based detection technique has problems with the ROs' sensitivity to supply voltage fluctuation. Therefore, the detection accuracy is degraded for time-varying voltage fluctuations. In contrast, we proposed a technique to calibrate the effect of supply voltage using as a reference the oscillation frequency of RO, which has the same power supply dependence and weak EM coupling to the outside. Using the fact that the oscillation frequency of the RO for sensors is slow due to the wiring delay caused by the connection to the outside circuit, the power supply voltage is estimated and calibrated from multiple reference RO oscillation periods. This makes it possible to estimate the oscillation frequency even under time-varying power supply voltage.

An experimental system using an FPGA was constructed and the supply voltage was varied by a 1 MHz sinusoidal wave that varied 5% from the rated supply voltage. In this environment, it was shown that the frequency estimated without the proposed method widens by 470%, while with the method applied, the estimated oscillation frequency can be suppressed to the extent that it increases by 189% compared to the case without the application of the method. As a result, it was shown that it is possible to stably detect the H-field probe at a distance of 8mm as well as in an environment where the power supply does not fluctuate.

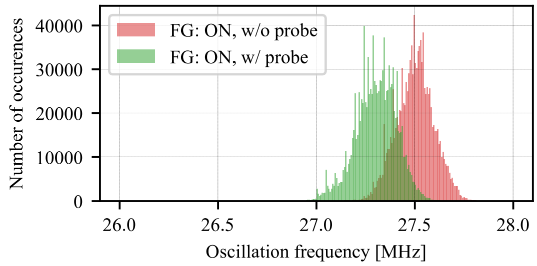


**Figure 7.** Distribution of $RO_{sensor}$ oscillation frequency with and without probe after calibration.

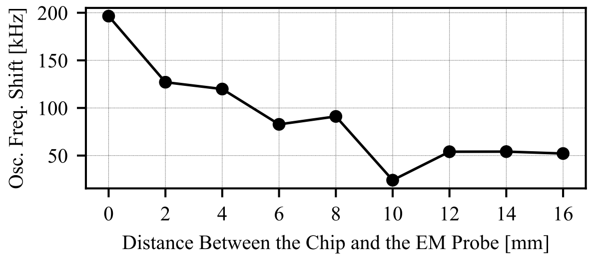


**Figure 8.** Variation of the shift of the oscillation frequency of the $RO_{sensor}$ when the distance between the chip and the H-field probe is varied.


# 5 Acknowledgements

This work was supported by JSPS KAKENHI Grant Number JP23K28087.


# References


[1] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: concrete results," CHES 2001, pp.251-261, 2001.

[2] JJ. Quisquater and D. Samyde, "Electromagnetic analysis (EMA): measures and counter-measures for smart cards," Smart Card Programming and Security, pp.200-210, 2001.

[3] W. Yu and S. Köse, "A lightweight masked AES implementation for securing IoT against CPA attacks," IEEE Trans. Circuits Syst. I: Regular Papers, vol. 64, no. 11, pp. 2934–2944, 2017.

[4]D. Bellizia, S. Bongiovanni, M. Olivieri, and G. Scotti, "SC-DDPL: a novel standard-cell based approach for counteracting power analysis attacks in the presence of unbalanced routing," IEEE Trans. Circuits Syst. I: Regular Papers, vol. 67, no. 7, pp. 2317–2330, 2020.

[5] S. Mangard, E. Oswald, and T. Popp, "Power Analysis Attacks: Revealing the Secrets of Smart Cards," 2007.

[6] D. Fujimoto, T. Sato, K. Abe and Y. Hayashi, "Fundamental Study on Electromagnetic Analysis Attack Detection using Oscillation Shift of Ring Oscillator," 2024 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC), Okinawa, Japan, pp. 53-56, 2024.

[7] SY. Kim and SS. Wong, "Closed-form RC and RLC delay models considering input rise time," IEEE Trans. Circuits Syst. I: Regular Papers, vol. 54, no. 9, pp. 2001–2010, 2007.