IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 30, 2021, accepted July 26, 2021, date of publication August 9, 2021, date of current version August 17, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3103183

Synchronous Real-Time Sampling Technique for Side-Channel Analysis Against Randomly Varying Clock-Based Countermeasures

HYEMIN YANG, EUN-GU JUNG, AND CHANGKYUN KIM
Affiliated Institute of Electronics and Telecommunications Research Institute (ETRI), Daejeon 34044, South Korea
Corresponding author: Hyemin Yang (hyang@nsr.re.kr)

ABSTRACT Power analysis attacks pose a significant threat to the security of cryptographic devices as they can reveal a secret key. Performing cryptographic operations based on a randomly varying clock (RVC) is a practical countermeasure against such attacks. The countermeasure makes it difficult to align power traces, which is a prerequisite for power analysis attacks to succeed. This paper introduces a synchronous real-time sampling (SRTS) technique as an advanced hardware-implemented approach to collect traces for a power analysis attack that negates countermeasures involving practical RVCs. By recovering the RVC, the leakage signal corresponding to the recovered clock edge is synchronously sampled in real time. We propose an analog-based hardware system implemented with two circuit blocks for SRTS operations, namely, a clock recovery block and an analog signal-processing block. The target of the power analysis attack is an Advanced Encryption Standard (AES)-128 software-implemented smart card operated at 20 MHz, which is varied in the range of 30% by the RVC countermeasure. The traces captured by the SRTS show that the suboperations of the AES encryption are distinct in contrast to the indistinguishable waveforms captured at a fixed sample rate. The results of the power analysis attack demonstrate that the correct key is successfully extracted with a high correlation coefficient at the S-box output of the AES. The proposed SRTS method improves the relative distinguishing margin by 191.4% and reduces the required number of traces to 2.75% compared with the conventional correlation power analysis attack with a fixed sample clock.

INDEX TERMS Alignment, power analysis attack, randomly varying clock, side-channel analysis, smart card, synchronous real-time sampling.

I. INTRODUCTION

Cryptographic devices implemented in hardware inevitably leak secret information due to unintended physical phenomena resulting from acoustic, thermal, optical, power, and electromagnetic effects [1], [2]. In a complementary metal-oxide-semiconductor (CMOS) device, the switching activity of transistors during cryptographic operations exposes power leakage signals, and power consumption depends on the execution of an instruction [3], [4]. Side-channel analysis (SCA) is an attack technique that involves the extraction of secret information from a cryptographic device with a leaked signal from a side channel and not from the main channel's power flow [5], [6]. A specific behavior related to cryptographic operations can be monitored from power consumption using an oscilloscope [7]. Since Kocher *et al.* [8] first introduced differential power analysis (DPA) in 1999, and since Brier *et al.* [9] introduced correlation power analysis (CPA) in 2004, the risk of exposing cryptographic keys by collecting and analyzing leakage power signals from hardware devices has existed. DPA and CPA have been successfully used to retrieve secret information by modeling side-channel leakages with Hamming weight and Hamming distance models [8]–[10], [12]. While analyzing data encrypted with known plaintexts using statistics with the model, the collection of a large number of power traces is required to obtain a high correlation coefficient.

In order for an attacker to successfully perform a CPA attack with a large number of collected traces, the collected power traces must be aligned [10], [11]. In the cases of misalignment between collected traces, the required number of traces for a successful CPA attack is multiplied several

The associate editor coordinating the review of this manuscript and approving it for publication was Lo'ai A. Tawalbeh.

times [13]. According to this requirement for trace alignment, a time-shifting obfuscation is considered as a strong countermeasure against CPA attacks [20], [23]. Various countermeasures related to the misalignment of traces, such as randomly varying clocks (RVCs), clock-cycle omissions, instruction shuffling, and random delay insertions, have been implemented in cryptographic operations [18]–[22]. Even small fluctuations in the operating clock, such as jitter, can cause CPA attacks to fail despite the starting point being synchronized [28].

Synchronous sampling is a trace acquisition technique that samples a signal in synchronization with the operating clock of a cryptographic device [27], [28]. Collecting traces with synchronous sampling can shorten trace acquisition time and reduce data size without adversely affecting CPA performance. Moreover, for devices to which RVC countermeasures are applied, the use of traces collected by synchronous sampling effectively improves CPA attack performance. O'Flynn and Chen [27], [28] introduced a synchronous sampling using hardware-implemented clock recovery during trace acquisition and showed that synchronous sampling succeeds in CPA attacks when the operating clock frequency changes randomly before the encryption routine call. However, the synchronous sampling method using the existing clock recovery technique is limited to the application of practical time-shifting obfuscation countermeasures in which the clock frequency changes every clock cycle.

In order to collect traces while negating practical RVC countermeasures, we propose an advanced trace acquisition technique of synchronous real-time sampling (SRTS).

The main contributions of this study are:

- We introduce an advanced hardware system that performs synchronous sampling in real time according to a RVC. The proposed SRTS system overcomes the synchronization error, which is a limitation of the synchronization sampling method using the existing clock recovery.
- We provide a design guide for the SRTS hardware system, considering group delay, impedance matching, noise figure, and linearity.
- We perform a practical evaluation of the proposed SRTS method on an actual smart card.
- We only collect points of interest in the power consumption signal by acquiring one signal data per clock edge. The small amount of data can reduce the cost of processing the CPA.

The SRTS system consists of two circuit blocks: a clock recovery block and an analog signal-processing block. The clock recovery block is used to recover a device's clock signal, which is a RVC. The analog signal-processing block is used for the signal processing of leaked power. Both circuit blocks are composed of low-noise amplifiers (LNA), a band-pass filter (BPF), a power splitter, limiters, and an analog-to-digital converter (ADC). The ADC synchronously samples the signal-processed input to the recovered clock. The target is a smart card operating at 20 MHz, and the clock frequency is randomly varied in the range of 30% by the RVC countermeasure. The experimental results demonstrate that suboperations of Advanced Encryption Standard (AES) encryption can be characterized in the traces collected using the proposed hardware system. The CPA attack in a specified suboperation increases the accuracy of the correct key guess with a high correlation coefficient. The SRTS method improves the relative distinguishing margin by 191.4% and reduces the required number of traces to 2.75%, compared with the conventional CPA attack.

The remainder of this paper is organized as follows. Section II presents the background of a CPA attack for misalignment-based countermeasures. We show the operation of a smart card with a RVC countermeasure as the target device. We describe related work on the trace acquisition method using synchronous sampling and discuss its limitation. In Section III, we introduce the operation mechanism of the proposed SRTS method. In Section IV, we describe the design and implementation of the analog-based hardware system in detail. The experiment and the results of the CPA attack are presented in Sections V and VI. We outline the conclusions in Section VII.

II. BACKGROUND AND RELATED WORK

This section describes the prerequisites of trace alignment for CPA attacks and introduces various countermeasures to break the trace alignment. We show signal traces for the smart card with the RVC countermeasure, the target of this study. We briefly discuss related work for synchronous sampling using clock recovery.

A. CPA ATTACK AND TRACE ALIGNMENT

A CPA attack employs Pearson's correlation coefficient to evaluate the linear relationship between the measured power traces and hypothetical power consumption values [10]. The most commonly used power models are the Hamming-weight and Hamming-distance models used to obtain hypothetical power consumption values. The correlation coefficient (ρ) between the Hamming weight matrix (H) and the obtained power traces (T) can be given as

$$\rho(T, H) = \frac{Cov(T, H)}{\sqrt{Var(T) \cdot Var(H)}}, \tag{1}$$

where Cov denotes the covariance matrix, and $Var(T)$ and $Var(H)$ represent the variance of T and H, respectively. If the absolute value of the correlation coefficient is close to one, the result means that the estimated key may be correct with high possibility. The correlation coefficients between the columns of H and T are estimated based on the data elements of these columns. The more elements are in the columns of H and T, the more accurately the attacker can find out the relationship between the columns. To determine the strongest correlation between columns H and T with high precision, the attacker needs to collect a large number of traces. An essential prerequisite of a CPA attack is to align thousands of traces in the time domain [5], [10].

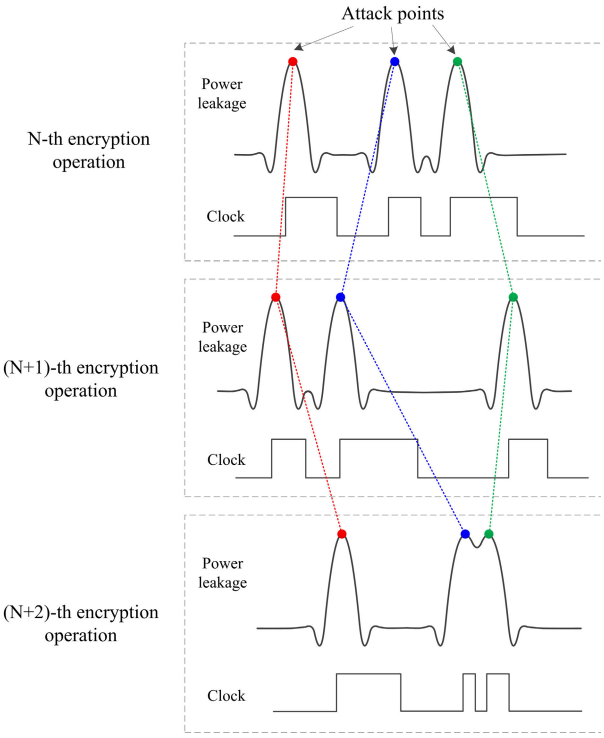

FIGURE 1. Example of misalignment of attack points from power consumption waveform based on a RVC during multiple encryption operations. Each attack point highlighted in a different color is not positioned equivalently on the horizontal axis.

On the defense side, breaking the prerequisites of trace alignment is a practical solution to provide a defense against CPA attacks [14], [20]. Time-shift obfuscation is a countermeasure used to obfuscate the power consumption observed during encryption. If the clock cycle timing is arbitrarily changed, the corresponding attack point shifts at the same encryption operation. Fig. 1 shows an example of the misalignment of attack points in leakage waveforms based on a RVC for multiple encryption operations. Each attack point is not placed in the same position on the horizontal axis by a RVC [15]–[17]. Trace misalignment makes the power profile analysis difficult with traces collected at a fixed sample frequency. For CPA attacks on misaligned power traces, the correlation coefficient between the Hamming weight matrix (H) and the obtained power traces ($\hat{T}$) is dependent on power consumption distribution. The correlation for the correct key hypothesis can be calculated as follows [10]:

$$\rho(H, \hat{T}) = \rho(H, T) \cdot \hat{p} \cdot \sqrt{\frac{Var(T)}{Var(\hat{T})}}, \tag{2}$$

where $\hat{p}$ denotes the maximum distribution of the power consumption at that moment of time which is randomly distributed due to misalignment, and $\hat{T}$ represents the power consumption located at this position. The correlation $\rho(H, \hat{T})$ with the misaligned power traces decreases linearly with the probability p.

B. COUNTERMEASURES USING TIME-SHIFTING OBFUSCATION

Various countermeasures for trace misalignment, such as random clock gating, clock-cycle omission, instruction shuffling, or random delay insertion, have been introduced [18]–[22]. Benini *et al.* [18] employed random clock gating to significantly decrease the signal-to-noise ratio (SNR) for power profile analysis. Bucci *et al.* [21] exploited a random delay insertion in the data path of a cryptographic processor to randomize the power consumption profile for DPA-resistance. In [19], Yang *et al.* suggested a dynamic voltage and frequency scaling technique to improve the resistance of a cryptosystem to DPA attacks. Tanimura and Dutt [20] proposed a time-shifting approach with a latch-based random clock-gating with circuit retiming and clock-gating to prevent power analysis attacks. In [22], Boey *et al.* presented a DPA resistant technique using random clock dummy data. The power analysis resistant methods with the trace misalignment considerably degrade the performance of results due to the randomness of the collected trace distribution.

C. SIGNAL TRACES FOR A SMART CARD WITH A RVC COUNTERMEASURE

We describe the RVC countermeasure characteristics of the actual smart card with the measured waveform. The smart card contains a software implementation of the AES-128 algorithm [24]. When the AES algorithm runs on the smart card, a RVC-based countermeasure is activated. The operating frequency of the smart card is varied from 17 MHz to 23 MHz by the countermeasure. We monitored the power signal traces measured through a small shunt resistor inserted into the bias voltage pin of the smart card. Signal traces were captured by a 250 MHz sampling frequency using a Teledyne Lecroy 204MXi-A digital oscilloscope.

Fig. 2 represents the leakage power signals during the AES encryption operation without a countermeasure (figures on the left) and with a countermeasure (figures on the right). Fig. 2(a) shows a clear distinction of ten rounds of the AES encryption operations. In contrast, ten rounds of the AES encryption based on a RVC are almost indistinguishable by the countermeasure, as shown in Fig. 2(b). The enlarged figures in Figs. 2(a) and (b) show two aligned and overlapping traces for the first round of AES encryption with two different plaintexts. Each trace corresponds to a different randomly chosen-plaintext encrypted with the same unknown key. Figs. 2(c) and (d) represent the differences between these two aligned traces. The difference between the two traces in Fig. 2(c) mostly reflects the signal magnitude difference in the encryption operation by the different plaintexts at the same operation time. Conversely, Fig. 2(d) shows the signal difference with considerable variability in which the power consumption characteristics resulting from different plaintexts are not reflected at the same operation time. Figs. 2(e) and (f) show the leakage power for ten rounds of the AES encryption operations in the frequency domain.

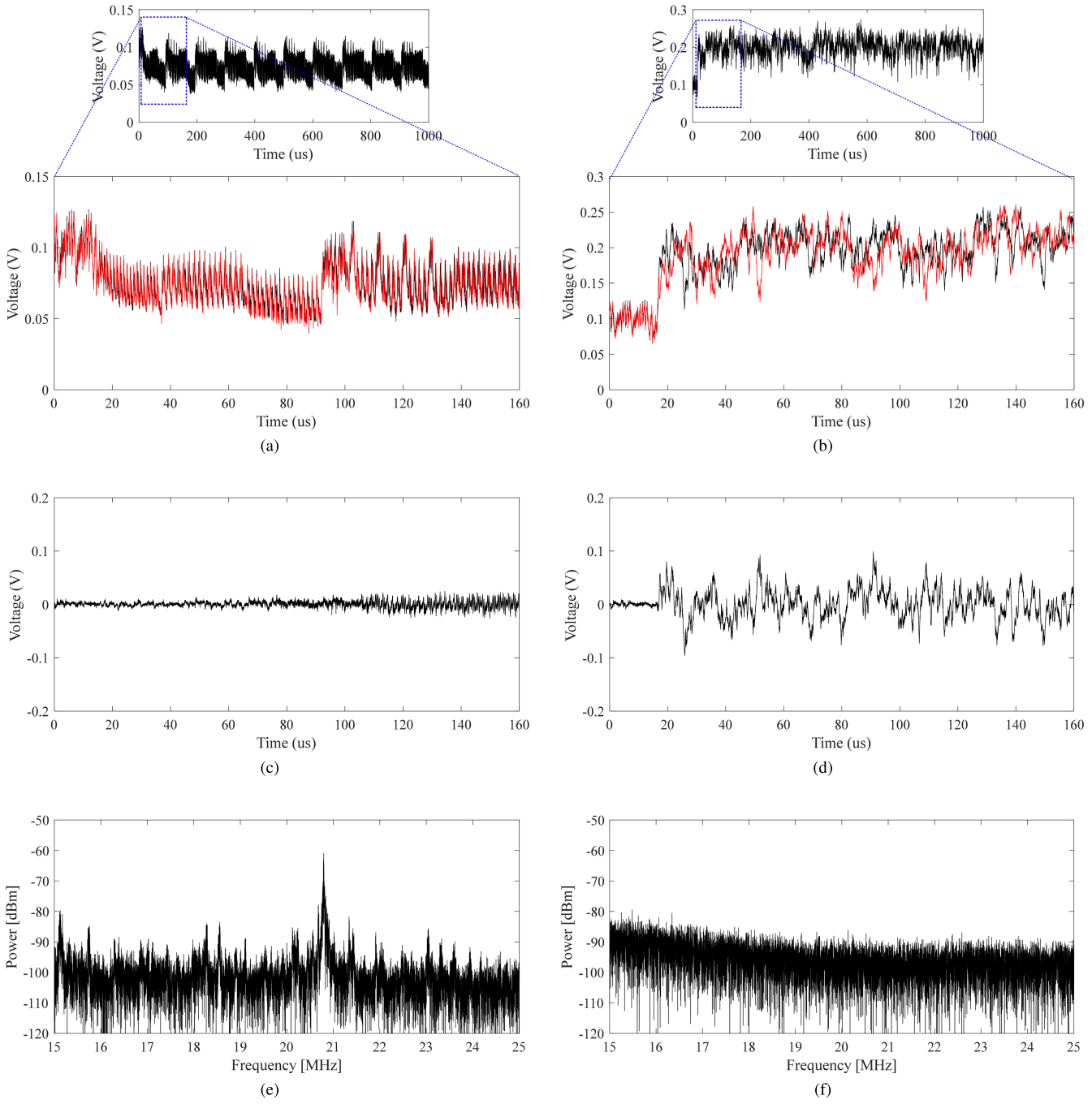

FIGURE 2. Leakage power signals for a smart card captured during AES encryption operation without a countermeasure (figures on the left) and with a countermeasure (figures on the right): (a, b) Two overlapping two traces for the first round among ten rounds of AES encryption with different plaintext. Each trace corresponds to a different randomly-chosen plaintext encrypted with the same unknown key. (c, d) Signal differences in these two traces in the first round. The considerable variability in the signal difference makes a power profile analysis difficult. (e, f) Leakage powers for ten rounds of AES encryption in the frequency domain. For the encryption based on a RVC, a prominent power signal is not observed in the frequency domain.

The power signal in the frequency domain is obtained by calculating the fast Fourier transform in a 50 Ω impedance system. As shown in Fig. 2(e), the dominant power for the clock signal during the encryption operation is observed at 20.78 MHz. In contrast, a prominent power signal is not observed in the frequency domain in Fig. 2(f), because power consumption covers a broad span of the 30% frequency band.

D. RELATED WORK FOR SYNCHRONOUS SAMPLING

Synchronous sampling, a technique that collects traces while synchronizing the sample clock to the device clock, is useful for SCA [27]. It was reported in [26] that the results of a CPA attack using traces collected by synchronous sampling are similar to those of traces collected asynchronously at a high sampling rate. O'Flynn and Chen [28] showed that increasing

the sampling rate does not improve the CPA attack results and demonstrated the enhancement of the CPA results when using traces collected by synchronous sampling. In addition, it has been experimentally determined that the synchronization sampling technique when collecting traces is considerably effective in attacking cryptographic devices that operate based on a variable clock.

A CPA with synchronous sampling using clock recovery for the varying clock was first provided in [27], [28]. The hardware-implemented clock recovery system consists of a LNA, a BPF, and a phase-locked loop and is designed to recover an internally hidden clock signal. The RVC of the target device operates before the encryption routine call. As a result of the CPA attack using synchronous sampling by clock recovery, it has been confirmed that the secret key can be extracted with a small number of trace sampling. However, the BPF of the clock recovery system carries a characteristic that the phase delay varies within frequency ranges. This delay causes synchronization errors between traces, which degrades analysis performance [28]. Moreover, if the clock randomly varies every cycle, such as in the actual smart card with a RVC countermeasure described in the previous subsection, the clock recovery technique of the existing hardware configuration will fail to sample synchronously. That is because sampling timing of the leakage signal does not coincide with the corresponding recovered clock. For synchronous sampling to operate correctly, the leakage signal per clock cycle must correspond to the recovered clock edges at the right time instant.

III. SRTS TECHNIQUE FOR A CPA ATTACK

In this section, we propose a SRTS technique for a power analysis attack and describe its operation mechanism.

A. AIM

For synchronous sampling of devices whose clock frequency randomly varies for each clock cycle, the leakage signal must be sampled at the correct time for each varying clock. A straightforward idea of a SRTS approach involves the synchronous sampling of leakage signals in accordance with the recovered varying clock per cycle. Therefore, the RVC is recovered in real time, and the leakage signal is sampled according to the recovered clock edge. Figs. 3(a) and (b) illustrate a block diagram of the proposed SRTS hardware system and its operating mechanism, respectively.

B. OPERATING MECHANISM

The SRTS system classifies into two processing blocks: a clock recovery block (signal flow indicated by the red-dotted line) and an analog signal-processing block (signal flow indicated by the blue-dotted line) in Fig. 3(a).

We provide the main functions of the hardware system as follows:

- The leakage power signal is synchronously captured by the corresponding RVC.
- The clock recovery block recovers the RVC signal from the leakage power signal.
- The analog signal-processing block amplifies and filters the leakage power signal. The most crucial role of this block is to set the delay time to be exactly the same as the clock recovery block.

The clock recovery block and the analog signal-processing block share two LNAs and one BPF. The power splitter divides the output signal from the two LNAs (LNA1 and LNA2) and one BPF in half. The split signal (in half) is amplified through the analog signal-processing block and is inserted as an input signal to the ADC. The other half of the signal is formed into a clock signal and enters the clock pin of the ADC. Thus, the ADC employs this external clock to sample the input leakage signal. The limiter's role in the clock recovery block is to trim the signal into a square waveform. Therefore, the ADC synchronously samples the analog signal-processed signal (marked with the letter 'A') with the external clock (marked with the letter 'B') recovered from the clock recovery block. All signal information sampled for each trace corresponds to the recovered clock edge. Since each sampled encryption operation data coming out of the ADC's output is placed on the same horizontal axis, trace alignment can be realized.

The most critical factor for the SRTS is sampling at the most appropriate time instant. Thus, the delay time between two block paths must coincide to achieve correct sampling as represented by the following equation:

$$t_{CR} = t_{AS}, \tag{3}$$

where t_{CR} and t_{AS} represent the delay times generated while passing through components corresponding to clock recovery (from LNA1 to Limiter3) and analog signal-processing (from LNA1 to LNA8) in Fig. 3(a), respectively. In this condition, sampling is always performed at the RVC edges, despite the BPF characteristic where the phase delay varies with frequency. Therefore, the proposed system overcomes a limitation of synchronization error due to the group delay in the existing clock recovery system.

IV. DESIGN AND IMPLEMENTATION

In this section, we describe the overall SRTS system design guide. We consider group delay, impedance matching, noise figure, and linearity in implementing the analog-based hardware system.

A. OVERALL DESIGN

In the entire hardware system configured as shown in Fig. 3(a), the number of LNAs to be added depends on the amplitude of the target device's leakage signal. Observing the recovered clock signal with an oscilloscope, we adjust the number and gain of LNAs such that the voltage level meets the level required for the clock input of the ADC. One set of LNA-limiters for the clock recovery block must be paired with the LNA of the analog signal-processing block. For example, if two sets of LNA-limiters are added to increase the

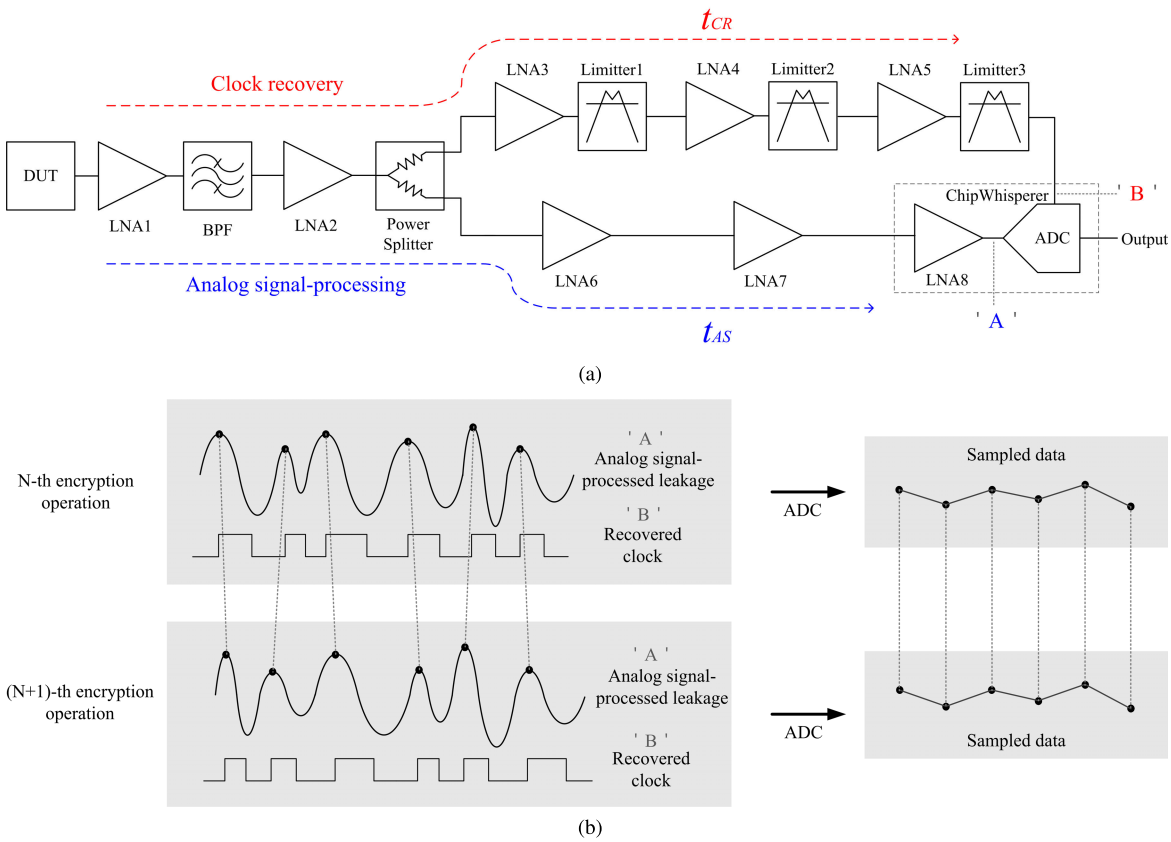

FIGURE 3. (a) Block diagram of the proposed analog-based hardware system for the SRTS approach and (b) signal operating mechanism for SRTS in the hardware system. The hardware system is classified into two processing blocks: a clock recovery block (red-dotted line) and an analog signal-processing block (blue-dotted line). The ADC synchronously samples the analog signal-processed leakage power (marked with the letter 'A') by the recovered-RVC (marked with the letter 'B').

amplitude of an external clock for a stable clock supply to the ADC, two LNAs for the analog signal-processing block must also be added. The key to the clock recovery block is that it should be designed such that no delay time is introduced due to these additional components. Thus, it is recommended that the limiters be replaced with an optional function provided by a LNA. We used an AD8331 LNA from Analog Devices Inc., which could be used as a limiter with an output clamp engaged by a resistor implementation [32]. The two delay times between both processes are almost identical because there is no additional delay due to the integrated function of AD8331.

At the first stage, a LNA with low noise figure and high gain should be placed to improve the SNR of the overall system [25]. A BPF is designed such that the signal passes within the frequency band in which the RVC operates. The power splitter divides the signal in half and sends it to each block. Next, we discuss group delay, impedance matching, noise figure, and linearity in detail for implementing the proposed hardware system.

1) GROUP DELAY

To acquire correct sampling data, it is significant that a datum sampled on the clock edge should not interfere with a datum sampled on the next clock edge. To avoid performing incorrect sampling, we consider a group delay characteristic in the design of the hardware system. The group delay represents the time delay of a signal of devices as a function of frequency, as expressed by the following equation [25]:

$$\tau(\omega) = -\frac{d\phi}{d\omega}, \tag{4}$$

where ϕ is the phase shift in radians, and ω is the angular frequency. The variation of the group delay is the amount of the phase distortion of the device, which is equivalent to a fluctuation of sampling timing. The worst-case scenario in the proposed hardware system is that the group delay fluctuation is greater than one period of the clock cycle, and thus, the sampled data are mixed with other sampled data. To avoid being sampled across, the hardware system should maintain a constant group delay within an operating frequency band. The shortest clock cycle is 43.5 ns, which corresponds to the highest frequency of 23 MHz in the design frequency band. Therefore, we set a design goal with fluctuation ($\Delta\tau$) that is less than half of the shortest clock cycle for stable sample acquisition.

2) DESIGN OF BPF AND IMPEDANCE MATCHING

Since an analog filter characteristic is very closely related to the group delay performance, selecting an appropriate filter

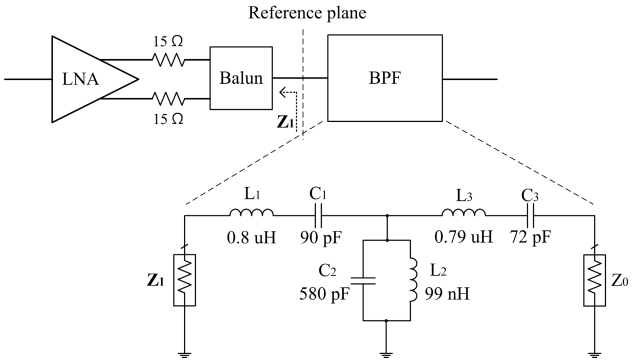

FIGURE 4. Design of the modified third-order Butterworth BPF. The output impedance (Z_1) of the LNA and the input impedance of the BPF are matched within a frequency band that spans 30% of the bandwidth.

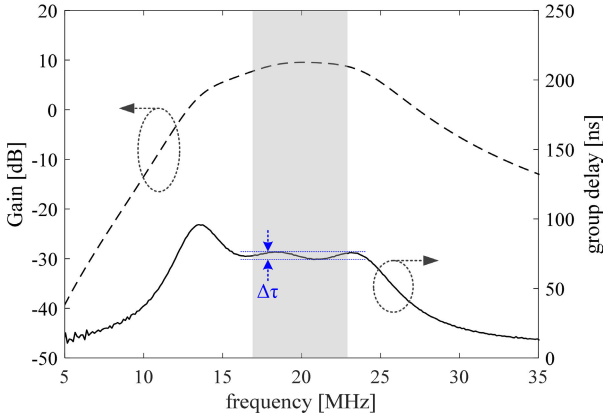

FIGURE 5. The measured results of the gain and the group delay for the LNA and the BPF connected in cascade.

type is important to obtain the desired transfer response. We select a Butterworth filter, referred to as a maximally flat magnitude filter, to ensure a nearly constant group delay. We designed a third-order BPF that considered the tradeoff between the parameters of insertion loss and cutoff sharpness. The values of the reactive elements of the BPF were determined by transforming the low-pass prototype filter design. In a 50 Ω impedance system, the inductance and capacitance values for third-order Butterworth BPF are given by [25]

$$L_1 = L_3 = \frac{g_1 Z_0}{\omega_0 \Delta} \tag{5}$$

$$C_1 = C_3 = \frac{\Delta}{\omega_0 g_1 Z_0} \tag{6}$$

$$L_2 = \frac{\Delta Z_0}{\omega_0 g_2} \tag{7}$$

$$C_2 = \frac{g_2}{\omega_0 \Delta Z_0} \tag{8}$$

where $g_1 = 1$ and $g_2 = 2$ are the prototype element values for the third-order Butterworth low-pass filter, $\omega_0 = 2\pi f_0$ is the angular frequency of the center frequency f_0, Δ is the fractional bandwidth of the passband, and Z_0 is the characteristic impedance.

The response characteristic of a BPF is highly dependent on the impedance of a system because the reactive element values are all determined as a function of the impedance Z_0 as expressed in (5) to (8). If the output impedance of a device connected to a BPF does not match the input impedance of the BPF, both unwanted signal reflection and inefficient power transfer will occur. The measured output impedance of the AD8331 LNA in an evaluation board is 12.6 + j55.6 Ω at 20 MHz. We verified the performance degradation of significant signal loss and large group delay fluctuation as a result of a measurement by connecting the output of the LNA to the BPF designed to have a 50 Ω impedance.

Impedance matching is necessary to transform the complex load impedance to match resistive or complex source impedance [34]. For the best signal transfer between the two devices, the output impedance of the previous device should be the complex conjugate of the following device. However, perfect complex conjugate impedance matching within the entire frequency band is impossible in a wide frequency band. Thus, we designed the BPF that provided adequate matching within the desired frequency band. A common solution to impedance mismatching is to insert a matching circuit between the two components, but it can cause additional loss and delay fluctuations. To avoid the problem caused by the additional circuit, we modified the BPF design to perform impedance matching simultaneously. The modified BPF with the same number of inductor and capacitor elements does not produce additional insertion loss and group delay fluctuations and reduces circuit complexity. Fig. 4 shows the design of the impedance-matched BPF connected in cascade to the output of the LNA. The balun transforms the differential output signal of the LNA into an unbalanced input signal of the BPF. To set the output impedance of the LNA as close to 50 Ω as possible, we connected two 15 Ω resistors in series between the differential output lines of the LNA and the balun. The output impedance (Z_1) when looking leftward from the reference plane is $45.7+j47.4$ Ω at 20 MHz. The output impedance varies slightly within the 30% frequency bandand is equal to $41.9+j40.1$ Ω at 17 MHz and $50.3+j54.9$ Ω at 23 MHz. The impedance Z_1 is set as the input impedance of the BPF, and the values of L_1 and C_1 from (5) and (6) are modified through simulation. We designed an impedance-matched BPF with S-parameter simulation in Keysight Technologies' Advanced Design System simulation tool. The element values used in the BPF design are $L_1 = 0.8\mu$H, $C_1 = 90$ pF, $L_2 = 99$ nH, $C_2 = 0.58$ nF, $L_3 = 0.79\mu$H and $C_3 = 72$ pF.

Fig. 5 shows the measured results of the gain and group delay of the implemented LNA and impedance-matched BPF, connected in cascade. We measured the S-parameters using an E5061B vector network analyzer from Keysight Technology Inc. We verified that within the 30% frequency range (highlighted in gray), the group delay fluctuation ($\Delta\tau$) is approximately 11 ns, which is significantly less than half of the shortest clock. The gain was decreased by −2.5 dB from the LNA's gain of 12.5 dB at 20 MHz due to the insertion loss of the BPF.

3) CASCADE NOISE FIGURE

As the number of analog devices used increases, the noise generated by the entire hardware system will increase. The additional noise adversely affects the signal quality in the power profile analysis based on small leakage signals. Therefore, the additional noise generated in an analog-based hardware system should be considered. A noise figure parameter, defined as the amount of noise a component adds to the overall system, can specify an active device's noise performance, such as an amplifier [34]. The noise figure is calculated as follows:

$$NF = 10\log_{10}(\frac{S_i/N_i}{S_o/N_o}) \tag{9}$$

where S_i and N_i are the signal and noise at the input, and S_o and N_o are the signal and noise at the output, respectively. For passive devices, the noise figure is considered equal to attenuation at a physical temperature of 290 K; thus, the noise figure of the BPF and power divider is equal to the insertion loss.

For N cascade devices, the noise figure formula can be extended according to Friis' formula, as follows:

$$NF = NF_1 + \frac{NF_2 - 1}{G_1} + \frac{NF_3 - 1}{G_1 G_2} + \cdots + \frac{NF_N - 1}{G_1 G_2 \cdots G_{N-1}} \tag{10}$$

where NF_N is the noise figure of stage N and G_N is the linear gain of stage N. The noise figure can be reduced effectively by increasing the gain of the first stage in a cascade system. The overall noise figure of the hardware system is approximated to the noise figure of the first device owing to its high gain. Therefore, LNA1 should have a low noise figure and a high gain in the proposed hardware system, as shown in Fig. 3(a). The noise figure of the AD8331 LNA, which provides a low noise characteristic, is 4.1dB, including the variable gain amplifier noise.

4) LINEARITY

It should be noted that the high gain of an amplifier can adversely affect the linearity of the signal. The linearity characteristic of an amplifier is directly related to the distortion of the output signal. If the output power of an amplifier no longer increases by a gain value as the input power level increases, the output signal becomes distorted. The point at which an amplifier's output power starts to saturate is defined as the 1 dB compression point (P1dB) [34]. To avoid signal distortion, the output power of an amplifier should be below the P1dB. As the gain of an amplifier increases, the P1dB decreases, and the amplifier must thus be operated with an appropriate gain value according to the input power level. We determined the gain of the AD8331 with a root-mean-square input signal with amplitude up to 70 mV by considering the leakage power level and fluctuation of the smart card. The measured input P1dB for a 23 dB gain value at 23 MHz (the highest frequency in the design frequency range) is approximately −10 dBm. Therefore, we set the gain of LNA1 to 22.5 dB, which is slightly lower than 23 dB, to ensure increased linearity. In the proposed hardware system, we set the gain of LNAs low in the analog signal-processing block, wherein signal linearity is important. To form a square wave signal from the clock recovery block, we set the gain of the LNAs to a high value and clamped the output signal to an appropriate voltage level. We optimized the signal performance with the gain of the LNAs by adjusting the voltage with an external power supply. The gain parameters of the LNAs in Fig. 3(a) were set as 22.5 dB, 23 dB, 3.5 dB, 33.5 dB, 29.5 dB, 3.5 dB, 8.5 dB, and 6.4 dB for LNA1, LNA2, LNA3, LNA4, LNA5, LNA6, LNA7, and LNA8, respectively.

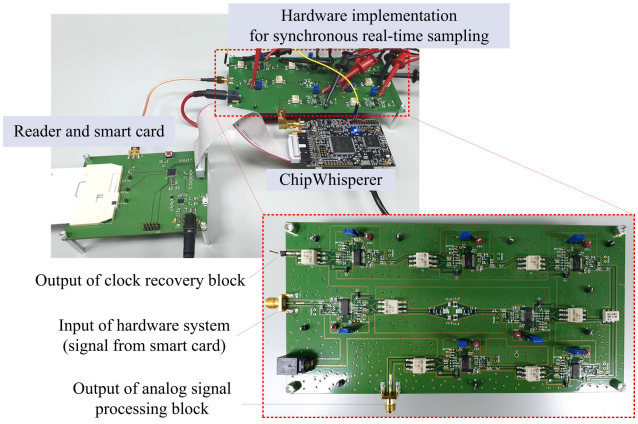

FIGURE 6. Experimental setup for CPA with a hardware implementation of the proposed SRTS technique. The enlarged figure shows the integrated PCB of the analog-based hardware system.

B. DESIGN CONSIDERATION FOR OTHER DEVICES

The SRTS hardware systems can be designed for devices with different operating frequencies or various frequency ranges for which RVC countermeasures operate. The designer requires information on the frequency at which the target device operates and the frequency variable range in which the countermeasure operates. The first step in system design is to select components such as LNAs and a power splitter with a frequency bandwidth that covers the clock frequency band of the device. The number of LNA-limiter sets for the clock recovery block is adjusted according to the amplitude of the target device's leakage signal. Hence, by increasing the number of LNA-limiter sets, the recovery clock signal is within the ADC voltage level requirements. Of course, increasing the number of LNAs in the analog signal-processing block is necessary as the number of LNA-limiter sets increased in the clock recovery block. The BPF should be designed to be impedance-matched as described in the previous subsection, and the order of the BPF can be determined by considering the trade-off between internal loss and the cutoff sharpness characteristic, depending on the leakage signal characteristic of the target device. The design for the group delay performance within the BPF's frequency range is highly dependent on the operating frequency of the device. Accordingly, the higher

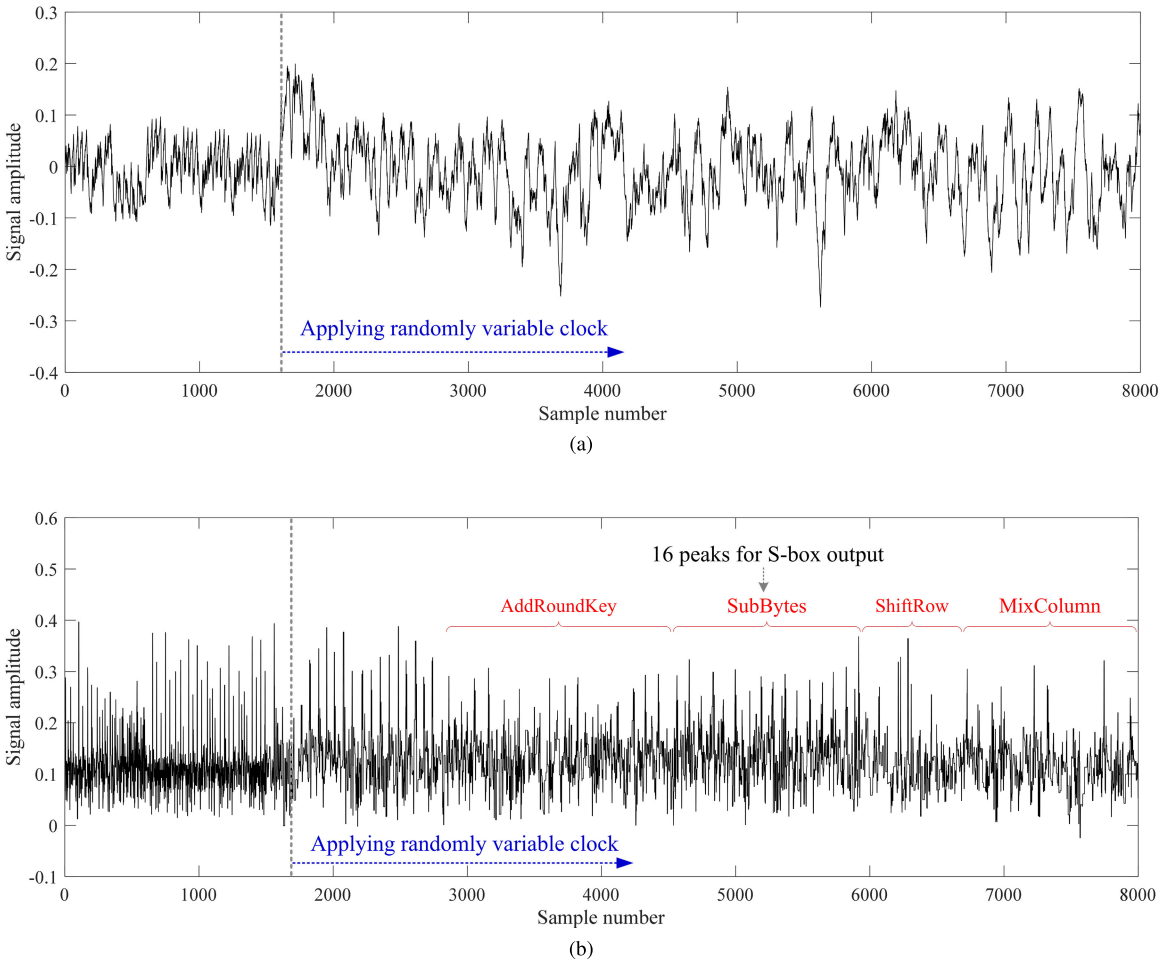

FIGURE 7. Captured leakage signals during AES encryption based on the RVC (a) without and (b) with the proposed SRTS method. The trace obtained using the SRTS method shows that the suboperations of AES encryption can be characterized, and prominent signal peaks corresponding to the 16 subbyte S-box operations are identified.

the target device operating frequency and the wider the countermeasure operating bandwidth, the greater the difficulty in designing this hardware system.

This system is limited in cases where high power signals such as radio frequencies exist within the varying clock frequency range of the target device. In this case, the system does not operate because unexpected signals, not a cryptographic algorithm operation signal, are recovered.

V. EXPERIMENT

We implemented the 8-bit based AES-128 encryption algorithm on a smart card. The smart card operates the AES encryption based on a RVC, which varies within 30% bandwidth of the 20 MHz operating frequency. The clock of the smart card is provided internally, thus making CPA attacks difficult. The reader for communication with the smart card was implemented using a Cortex M4 microcontroller from Microchip Technology Inc. Data communications between the reader and the smart card were performed, according to the T = 0 transmission protocol defined in ISO/IEC 7816 [29]–[31]. We used the ChipWhisperer-Lite to collect the leakage power signal consumed during the AES encryption operation [27]. We modified the ChipWhisperer Capture software and implemented it to send and receive the encryption keys, plaintexts, and ciphertexts necessary for AES encryption based on serial communication via an application protocol data unit.

The proposed analog-based hardware system for SRTS was integrated and implemented on a printed circuit board (PCB). We used AD8331 LNA from Analog Devices Inc. because it has low noise and an adjustable gain. We implemented the limiter with the clamp function of the AD8331 LNA with a shunt resistor. The third-order Butterworth BPF was assembled with surface-mounted-type inductors from Coil Craft Inc. and capacitors from Walsin Technology Inc. The balun was a T1-6T-KK91 from Mini Circuits Inc. An ADP-2-1W from Analog Devices Inc. power splitter that divides the signal in half based on the 50 Ω characteristic impedance was used. Fig. 6 shows the experimental setup for the CPA attack, and the enlarged figure shows the implemented analog-based hardware system. Because one of the LNAs in the analog signal-processing block is already mounted inside the

ChipWhisperer board, it is not represented on the integrated PCB [27]. The clock signal generated from the clock recovery block is directly connected to the clock port of the ADC on the ChipWhisperer board.

The field-programmable gate array (FPGA) on the ChipWhisperer board stores ADC output data according to the FPGA clock at a fixed frequency. Because the ADC outputs data at a variable time, the clock frequency of the FPGA should be set at least twice that of the ADC to avoid data loss.

VI. RESULTS

A. CAPTURED TRACES

We compared the captured traces by SRTS and fixed sampling. Fig. 7 shows the traces captured during AES encryption. RVC countermeasures are applied from the start of the AES encryption operation indicated by the red dotted line. Fig. 7(a) shows the signal waveform captured by the fixed clock frequency, which is identical to the operating frequency of the FPGA. The waveform shows that the suboperations of AES encryption are barely distinguishable because the leakage signal is sampled irrespective of the operating clock frequency. On the other hand, the signal captured by the proposed SRTS, shown in Fig. 7(b), indicates that the suboperations of AddRoundKey, SubBytes, ShiftRow, and MixColumn can be characterized. We can identify the prominent signal peaks corresponding to the 16 subbyte S-box operations for a CPA attack.

B. CPA RESULTS

The ideal SRTS operation enables the alignment of a portion of the captured trace to perform a perfect alignment over the entire signal waveform. However, it is difficult to align the entire trace area at once owing to hardware limitations such as the data acquisition by the fixed clock of the FPGA. Thus, we performed the CPA attack by aligning the peak signals corresponding to 16 subbyte S-box operations. After performing simple signal processing for deleting duplicated data acquired by the FPGA, we performed alignment based on the calculation of Pearson's correlation coefficients between signal peaks that correspond to each subbyte operation [10]. We performed the CPA attack by calculating the correlation coefficient between the Hamming weight of the intermediate value of the S-box output and the collected trace of the first round of the AES encryption. We used 20,000 traces to compare the results of the conventional CPA attack with a fixed sample clock with those of the CPA with the SRTS method.

Fig. 8 shows the correlation coefficient of 16 correct subkey guesses in the S-box operation. For intuitive comparison between the two cases, the vertical axis scales are set to be fixed. Fig. 8(a) shows the correlation coefficient for the conventional CPA attack with a fixed sample frequency of 80 MHz. The 16 correct subkey guesses are revealed, but its correlation coefficient values are low and broadly distributed. The CPA result using the proposed SRTS method shows

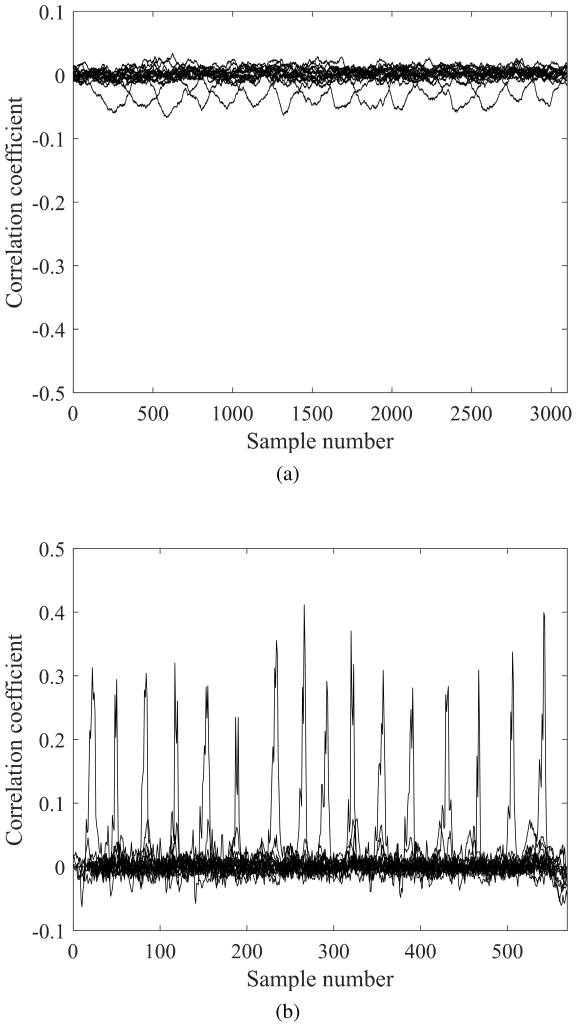

FIGURE 8. Correlation coefficients of the 16 correct subkey guesses in the S-box operation for the CPA attack (a) without and (b) with the proposed SRTS method. The SRTS method improves the result of high and distinctly distributed correlation coefficients for the 16 correct subkey guesses.

that the 16 correct subkey guesses are revealed with high and distinctly distributed correlation coefficients as shown in Fig. 8(b).

A relative distinguishing margin (RDM) measures the extent to which the distinguisher value for the correct key guess stands out over other distinguished values for wrong key guesses in a normalized manner [33]. For a given distinguisher of a subkey that produces the distinguishing vector D, the RDM is defined as

$$\mathrm{RDM}(D) = \frac{D(k^*) - \max[D(k)|k \neq k^*]}{\mathrm{Std}(D)} \tag{11}$$

where k^* is the correct key guess, and Std is the sample's standard deviation. Tables 1 and 2 report the RDM for the results of the conventional CPA and the CPA using the SRTS method, respectively. The average RDM of 16 correct subkey guesses is 5.67 for the conventional CPA, and 10.85 for the CPA using the SRTS method. The SRTS approach improves the RDM value by 191.4%.

TABLE 1. Correlation coefficients of first and second-ranked subkey guesses, standard deviations, RDM, and the required number of traces for 16 subbytes for the conventional CPA attack.

Subbytes	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12	#13	#14	#15	#16	Average
Corr (1^{st}rank)	0.060	0.053	0.067	0.056	0.054	0.054	0.064	0.048	0.054	0.054	0.055	0.040	0.059	0.057	0.043	0.050	**0.054**
Corr (2^{nd}rank)	0.037	0.031	0.034	0.034	0.034	0.033	0.034	0.034	0.034	0.033	0.031	0.037	0.033	0.033	0.034	0.030	**0.030**
Std	0.004	0.003	0.004	0.004	0.003	0.004	0.004	0.003	0.003	0.003	0.004	0.003	0.004	0.004	0.003	0.003	**0.004**
RDM(%)	5.73	6.12	8.18	6.00	5.62	5.81	7.69	4.07	5.61	6.11	6.90	0.82	6.51	6.70	2.75	6.05	**5.67**
Number of traces	7723	9950	6132	8702	9510	9384	6834	12199	9511	9433	8994	17648	7956	8478	14845	11245	**9909**

TABLE 2. Correlation coefficients of first and second-ranked subkey guesses, standard deviations, RDM, and the required number of traces for 16 subbytes for the CPA attack using the proposed SRTS method.

Subbytes	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12	#13	#14	#15	#16	Average
Corr (1^{st}rank)	0.313	0.294	0.304	0.320	0.248	0.238	0.356	0.412	0.291	0.370	0.309	0.281	0.283	0.309	0.338	0.399	**0.319**
Corr (2^{nd}rank)	0.081	0.072	0.071	0.096	0.072	0.065	0.088	0.090	0.078	0.111	0.085	0.081	0.076	0.079	0.090	0.090	**0.083**
Std	0.022	0.020	0.020	0.022	0.019	0.016	0.025	0.028	0.020	0.027	0.021	0.019	0.020	0.021	0.023	0.028	**0.022**
RDM(%)	10.79	11.26	11.56	10.01	11.42	10.94	10.93	11.40	10.81	9.65	10.68	10.48	10.41	11.13	10.88	11.19	**10.85**
Number of traces	267	305	284	255	327	473	203	148	311	186	275	335	330	274	227	158	**272**

The number of traces required for a successful CPA attack can be calculated using the correlation coefficient of the correct subkey guesses. As a rule of thumb, the number of traces, n, that are necessary to ensure a confidence of $1 - \alpha$ such that the two normal distributions $Z_0 \sim \mathcal{N}(0, \sqrt{1/(n-3)})$ and $Z_1 \sim \mathcal{N}(\mu, \sqrt{1/(n-3)})$ are distinguishable, is given by [10]

$$n = 3 + 8\frac{z_{1-\alpha}^2}{\ln^2 \dfrac{1+\rho_{k^*}}{1-\rho_{k^*}}} \tag{12}$$

where ρ_{k^*} is the estimated correlation coefficient for the correct key (k^*), and $z_{1-\alpha}$ is the quantile of a normal distribution for the two-sided confidence interval with the confidence of α. The value of the quantile is $z_{1-\alpha} = 3.719$ with $\alpha = 0.0001$. Tables 1 and 2 show the calculated number of traces required to extract the 16 correct subkey guesses for the conventional CPA attack and those for the CPA attack using the SRTS method, respectively. The average of the number of traces of 16 correct subkey guesses is 9909 for the conventional CPA and is 272 for the CPA using the SRTS method. The proposed SRTS method reduces the average number of traces to 2.75% compared with the conventional CPA.

VII. CONCLUSION

We introduced the SRTS technique, as an advanced trace-collecting method, for a hardware-based power analysis attack that negates countermeasures of a trace misalignment based on an RVC. The SRTS system recovers the RVC from the leakage power signal and synchronously samples the corresponding cryptographic operation leakage signal at the RVC edges. The proposed system configuration overcomes a limitation of synchronization error in synchronous sampling using an existing clock recovery system. We suggested the hardware system, composed of a clock recovery block and an analog signal-processing block for SRTS. We provided the overall design guide and described the implementation with group delay, impedance matching, noise figure, and linearity as the design parameters. The target for the power analysis attack was the AES-128 software-implemented smart card that applied the countermeasure with a RVC operated within a 30% bandwidth with respect to a 20 MHz operating frequency. The trace captured using the SRTS method showed that the suboperations of AES encryption could be distinguishable in contrast to that use the fixed sample rate. We performed the CPA attack with the small amount of sampled data by acquiring one signal data per clock edge and demonstrated that the correct key was successfully revealed with a high correlation coefficient at the S-box output of AES. The CPA results showed that the performance of the RDM was improved by 191.4%, and the required number of traces was reduced to 2.75% compared with the conventional CPA attack. Although the hardware implementation is limited to a specific target of analysis, we believe that the proposed hardware system can be applied to targets operated in various frequency bands by changing the design of a BPF according to the design guide provided.

REFERENCES

[1] J. McNamara. (1999). *The Complete Unofficial TEMPEST Information Page*. [Online]. Available: https://www.jammed.com/ jwa/tempest.html

[2] J. Quisquater and D. Samyde, "ElectroMagnetic analysis (EMA): Measures and countermeasures for smart cards," in *Proc. Int. Conf. Res. Smart Cards, Smart Card Programm. Secur.*, vol. 2140, Sep. 2001, pp. 200–210.

[3] H. J. Mahanta, A. K. Azad, and A. K. Khan, "Power analysis attack: A vulnerability to smart card security," in *Proc. Int. Conf. Signal Process. Commun. Eng. Syst.*, Jan. 2015, pp. 506–510.

[4] R. Mayer-Sommer, "Smartly analyzing the simplicity and the power of simple power analysis on smartcards," *Crypt. Hardw. Embedded Syst.*, vol. 1965, pp. 78—92, Aug. 2000.

[5] F. X. Standaert, "Introduction to side-channel attacks," in *Secure Integrated Circuits and Systems*. New York, NY, USA: Springer, 2010, pp. 27–42.

[6] K. Tiri and I. Verbauwhecle, "Simulation models for side-channel information leaks," in *Proc. 42nd Design Automat. Conf.*, Jun. 2005, pp. 228–233.

[7] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Power analysis attacks of modular exponentiation in smart cards," *Crypt. Hardw. Embedded Syst.*, vol. 1717, pp. 144–157, Aug. 1999.

[8] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology*, 1st ed. Berlin, Germany: Springer, 1999, pp. 388–397.

[9] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Proc. 6th Int. Workshop CHES*, vol. 3156, 2004, pp. 16–29.

[10] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, 1st ed. New York, NY, USA: Springer, 2010.

[11] L. Wu and S. Picek, "Remove some noise: On pre-processing of side-channel measurements with autoencoders," in *Proc. IACR Trans. Cryptograph. Hardw. Embedded Syst.*, Aug. 2020, pp. 389–415.

[12] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Investigations of power analysis attacks on smartcards," in *Proc. USENIX Workshop Smartcard Technol.*, 1999, pp. 1–12.

[13] G. Goodwill, J. Jaffe, and P. Rohatgi, "A testing methodology for side-channel resistance validation," in *Proc. NIST Non-Invasive Attack Testing Workshop*, 2011, pp. 1–15.

[14] Q. Tian, A. Shoufan, M. Stoettinger, and S. A. Huss, "Power trace alignment for cryptosystems featuring random frequency countermeasures," in *Proc. Int. Conf. Digit. Inf. Process. Commun.*, Jul. 2012, pp. 51–55.

[15] Q. Tian and S. A. Huss, "On clock frequency effects in side channel attacks of symmetric block ciphers," in *Proc. Int. Conf. Technol., Mobility Secur.*, May 2012, pp. 1–5.

[16] M. Yoshikawa, Y. Nozaki, T. Asai, and K. Asahi, "Frequency domain aware power analysis attack against random clock LSI for secure automotive embedded systems," in *Proc. IEEE 82nd Veh. Technol. Conf.*, Sep. 2015, pp. 1–5.

[17] P. Hodgers, N. Hanley, and M. O'Neill, "Pre-processing power traces to defeat random clocking countermeasures," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2015, pp. 85–88.

[18] L. Benini, A. Macii, E. Macii, E. Omerbegovic, F. Pro, and M. Poncino, "Energy-aware design techniques for differential power analysis protection," in *Proc. 40th Conf. Design Automat. (DAC)*, Jun. 2003, pp. 36–41.

[19] S. Yang, P. Gupta, M. Wolf, D. Serpanos, V. Narayanan, and Y. Xie, "Power analysis attack resistance engineering by dynamic voltage and frequency scaling," *ACM Trans. Embedded Comput. Syst.*, vol. 11, no. 3, pp. 62:1–62:16, Sep. 2012.

[20] K. Tanimura and N. D. Dutt, "LRCG: latch-based random clock-gating for preventing power analysis side-channel attacks," in *Proc. 8th IEEE/ACM/IFIP Int. Conf. Hardw./Softw. Codesign Syst. Synth.*, Oct. 2012, pp. 453–462.

[21] M. Bucci, R. Luzzi, M. Guglielmo, and A. Trifiletti, "A countermeasure against differential power analysis based on random delay insertion," in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2005, pp. 3547–3550.

[22] K. H. Boey, Y. Lu, M. O'Neill, and R. Woods, "Random clock against differential power analysis," in *Proc. IEEE Asia Pacific Conf. Circuits Syst.*, Dec. 2010, pp. 756–759.

[23] B. Hettwer, K. Das, S. Leger, S. Gehrer, and T. Guneysu, "Lightweight side-channel protection using dynamic clock randomization," in *Proc. 30th Int. Conf. Field-Program. Log. Appl. (FPL)*, Aug. 2020, pp. 200–207.

[24] J. Daemen and V. Rijmen, "C. reference code," in *The Design of Rijndael: The Advanced Encryption Standard*, 2nd ed. Berlin, Germany: Springer, 2020, pp. 259–266.

[25] D. M. Pozar, *Microwave Engineering*, 3rd ed. Hoboken, NJ, USA: Wiley, 2005.

[26] C. O'Flynn and Z. D. Chen, "A case study of side-channel analysis using decoupling capacitor power measurement with the OpenADC," in *Proc. Int. Symp. Found. Pract. Secur.*, vol. 7743, 2012, pp. 341–356.

[27] C. O'Flynn and Z. D. Chen, "ChipWhisperer: An open-source platform for hardware embedded security research," in *Proc. Int. Workshop Constructive Side-Channel Anal. Secure Des.*, vol. 8622, Apr. 2014, pp. 243–260.

[28] C. O'Flynn and Z. Chen, "Synchronous sampling and clock recovery of internal oscillators for side channel analysis and fault injection," *J. Cryptogr. Eng.*, vol. 5, no. 1, pp. 53–69, Apr. 2015.

[29] *Identification Cards–Integrated Circuit Cards—Part 2: Cards With Contacts—Dimensions and Location of the Contacts*, Standard ISO/IEC 7816-2, International Organization for Standardization, 2007.

[30] *Identification Cards—Integrated Circuit Cards—Part 3: Cards With Contacts—Electrical Interface and Transmission Protocols*, Standard ISO/IEC 7816-3, International Organization for Standardization, 2006.

[31] *Identification Cards—Integrated Circuit Cards—Part 4: Organization, Security and Commands for Interchange*, Standard ISO/IEC 7816-4, International Organization for Standardization, 2020.

[32] *AD8331/AD8332/AD8334 Data Sheet*, Analog Devices, Norwood, MA, USA, 2016.

[33] O. Reparaz, B. Gierlichs, and I. Verbauwhede, "A note on the use of margins to compare distinguishers," in *Proc. Int. Workshop Constructive Side-Channel Anal. Secure Des.*, Aug. 2014, pp. 1–8.

[34] G. Gonzalez, *Microwave Transistor Amplifiers—Analysis and Design*, 2nd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 1997.

HYEMIN YANG received the Ph.D. degree in mechatronics from Gwangju Institute of Science and Technology (GIST), Gwangju, South Korea, in 2015. She is currently a Senior Researcher with the Affiliated Institute of Electronics and Telecommunications Research Institute (ETRI), South Korea. Her current research interests include side-channel analysis and hardware security analysis.

EUN-GU JUNG received the Ph.D. degree in information and communications from Gwangju Institute of Science and Technology (GIST), Gwangju, South Korea, in 2006. Since 2008, he has been with the Affiliated Institute of Electronics and Telecommunications Research Institute (ETRI), as a Principal Researcher. His research interests include high speed implementation of cryptography algorithms, IC & PCB reverse engineering, and IC security analysis. He was a recipient of the 2011 IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS Best Paper Award from the IEEE Circuits and Systems (CAS) Society.

CHANGKYUN KIM received the B.S., M.S., and Ph.D. degrees in electronics from Kyungpook National University, Daegu, Republic of Korea, in 2001, 2003, and 2009, respectively. Since 2004, he has been with the Affiliated Institute of Electronics and Telecommunications Research Institute (ETRI), as a Principal Researcher. His current research interests include side-channel analysis on hardware crypto devices and hardware security analysis.