An Analog Side-Channel Attack on a High-Speed Asynchronous SAR ADC Using Dual Neural Network Technique

Takahashi, Ryozo
Miki, Takuji
Nagata, Makoto

(Citation)
IEICE Transactions on Electronics,E106.C(10):565-569

(Issue Date)
2023-10-01

(Resource Type)
journal article

(Version)
Version of Record

(URL)
https://hdl.handle.net/20.500.14094/0100485458

BRIEF PAPER *Special Section on Analog Circuits and Their Application Technologies*

An Analog Side-Channel Attack on a High-Speed Asynchronous SAR ADC Using Dual Neural Network Technique

Ryozo TAKAHASHI[†a)], ***Student Member***, **Takuji MIKI**[†], ***Member***, ***and*** **Makoto NAGATA**[†], ***Senior Member***

SUMMARY This brief presents a side-channel attack (SCA) technique on a high-speed asynchronous successive approximation register (SAR) analog-to-digital converter (ADC). The proposed dual neural network based on multiple noise waveforms separately discloses sign and absolute value information of input signals which are hidden by the differential structure and high-speed asynchronous operation. The target SAR ADC and on-chip noise monitors are designed on a single prototype chip for SCA demonstration. Fabricated in 40 nm, the experimental results show the proposed attack on the asynchronous SAR ADC successfully restores the input data with a competitive accuracy within 300 mV rms error.

key words: *SAR ADC, side-channel attack, neural network, hardware security*

1. Introduction

Sensor edge devices handle confidential and privacy information in various IoT systems such as medical, healthcare and industrial applications. Modern edge devices often contain dedicated cryptographic engines running unbreakable public-key encryption algorithms [1] to protect such sensitive information acquired and digitized by sensor frontend circuits. However, an analog signal before digitization is not yet protected by encryption, which introduces a security hole through which malicious attackers can steal information acquired by the sensors. Thus, analysis of side-channel information such as power supply and ground noise caused by analog circuit activity would allow an estimation of analog signal based on the well-known side-channel attack (SCA) techniques on digital cryptographic circuits [2]–[6].

Among the analog circuit blocks handling unencrypted signals, ADCs are indispensable circuit elements for sensor systems. Successive approximation register (SAR) ADCs are widely used for analog frontend of distributed sensor nodes to benefit from their potential characteristics of small size and low power consumption. The first SCA attempts on ADCs were demonstrated in [7]. It discloses an analog input voltage estimation utilizing reference noise caused by the charge redistribution operation of capacitive digital-to-analog converter (CDAC) in the single-ended SAR ADCs. The reference noise waveforms clearly show the correlation to the input voltages, and the simple template attack [8], [9] reveals them in the work. However, this attack is only effective if the noise waveforms correspond one-to-one with the input voltage, therefore, it cannot be applied to the differential structure that behaves completely opposite ways depending on the sign of the input voltage. Analog SCAs on differential SAR ADC configurations are also reported in [10] and [11]. These attacks exploit neural networks (NNs) to achieve highly accurate estimation of analog input information. However, these works only focus on low-speed synchronous SAR ADCs, and not for high-speed asynchronous SAR ADC architectures. Unlike the synchronous type in which the comparison timing is fixed, the asynchronous type SAR ADC has different timings of internal conversion process, which would make it difficult to classify with normal NN approach. Considering the increase in processing speed and expansion of signal bandwidth in future IoT applications, it is necessary to explore the possibility of security attacks on high-speed asynchronous SAR ADCs and to consider countermeasure techniques against such attacks in advance.

This brief presents a SCA technique targeting on an asynchronous SAR ADC with a newly proposed NN-based power and ground noise analysis. The proposed dual NN (Dual-NN) efficiently discloses sign information of input data hidden by the symmetrical operations of differential circuit structure, enabling highly accurate estimation of the input voltage. The target 11-bit 48-MS/s asynchronous SAR ADC and on-chip monitors for noise observation on power supply and ground nodes were fabricated as a prototype chip in 40 nm process. The measurement results prove that the proposed Dual-NN efficiently exposes the input signal of asynchronous SAR ADC while achieving 89.3 % in sign and 96.7 % in absolute value estimations.

The paper is organized as follows. Section 2 introduces the attacking scheme to asynchronous SAR ADCs. Section 3 presents the proposed Dual-NN to estimate the input data. The measurement results of the proposed SCA will be shown in Sect. 4. Finally, Sect. 5 gives the conclusion.

2. Strategy of Security Attack on Asynchronous SAR ADCs

A block diagram of a sensor system used in general IoT application is shown as Fig. 1. An analog signal acquired by the sensor device is quantized by an ADC after amplification and then encrypted by digital circuit to ensure network security. These processes are executed in a single SoC

Manuscript received November 11, 2022.
Manuscript revised February 26, 2023.
Manuscript publicized April 13, 2023.
[†]The authors are with Kobe University, Kobe-shi, 657–8501 Japan.
a) E-mail: ryozo.takahashi@it1.stin.kobe-u.ac.jp
DOI: 10.1587/transele.2022CTS0002

chip, which makes direct probing on the ADC output before encryption physically impossible. In addition, since the raw sensor signal is relatively sensitive and small amplitude, direct probing on the input signal may affect the original signal, thus the attackers cannot observe the signal path directly. A SCA on a digital circuit disclosing a cryptographic key via a power supply node without degradation of signal integrity, is widely known as a critical threat to break security, however, many countermeasures such as random masking techniques have been reported [12]–[15]. On the other hand, analog circuits have almost no security measures, which introduces a leakage risk of an internal circuit activity correlated with the input signal. Therefore, side-channel information such as power supply noise of analog circuits, especially ADCs, can be a security holes for extracting sensor analog information.

SAR ADCs are widely used in sensor frontends thanks to their low power and small capability. Furthermore, an asynchronous type is popular architecture to meet the recent demands for a high-speed operation. Figure 2 shows the circuit schematic of an asynchronous SAR ADC with their security aspects. It consists of binary-weighted CDACs, sampling switches, a comparator and SAR logic with differential structure. The comparator clock is generated based on the principle of self-oscillation after triggering by the sampling clock. Since the response time of a comparator output depends on the pair of input voltages, the timing of the binary search operation with comparison and charge redistribution varies with the input signal. Moreover, this comparator clock oscillates in a high frequency with N-bit times

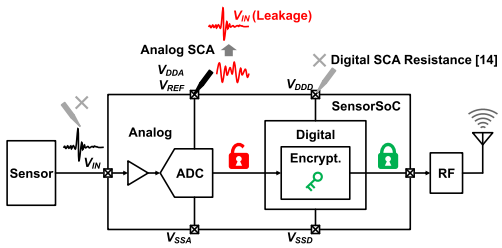

Fig. 1 Security hole of Sensor SoC for IoT edge devices.

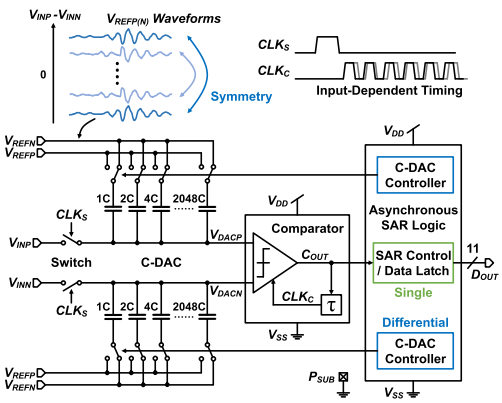

Fig. 2 Side-channel attack on asynchronous SAR ADC.

the sampling clock. These make it difficult to estimate the input-dependent SAR activity via power supply noise from outside, compared to normal synchronous type SAR architecture which accepts easy template attacks because of the fixed timing of comparison and charge redistribution with relatively long recovery time. In addition, the differential structure cancels the current through V_{REFP} and V_{REFN} during charge redistribution, resulting in similar noise waveforms at the same absolute values of $V_{REFP} - V_{REFN}$ as shown in the Fig. 2. It disables the estimation from the input dependent charge flow on V_{REF} nodes. To solve them, the proposed attacking scheme exploits the noise waveforms of power supply V_{DD}, ground V_{SS} and substrate P_{SUB} caused by asynchronous SAR operations. These waveforms contain not only differential circuit noise but also single-end circuit noise such as data latch operations with serial-parallel interface. The attack extracts the profile information included in this single-end motions and performs sign determination to improve the attacking accuracy.

3. Proposed Dual Neural Network Based SCA

3.1 Noise Sources for Learning Data

Figure 3 compares the SCA methods of the conventional template/NN based attacks and the proposed Dual-NN based attack. The conventional methods reported in [7] and [10] acquire noise waveforms of V_{DD} or V_{REF} which indicate the input-dependent activities of the CDAC and comparator inside the ADC, and then construct the template or NN as shown in Fig. 3 (a). The template attacks are only effective on single-ended SAR ADC configuration. The conventional NN attack also becomes difficult to identify sign information when the processing speed is increased by the asynchronous structure. To achieve a successful attack even against high-speed asynchronous SAR ADCs, the proposed attack method adds ground noise and substrate noise as training data to extract single-end activities, and builds a dedicated NN to find sign information of input data. The absolute value, excluding the sign data, is also estimated by constructing another dedicated NN by exploiting all noise data. Ground and substrate nodes have different delay characteristics and frequency responses than power and reference nodes, therefore, it is considered that NNs can extract

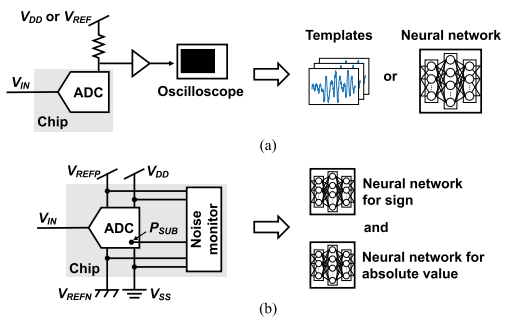

Fig. 3 (a) Conventional and (b) proposed side-channel attack methods.

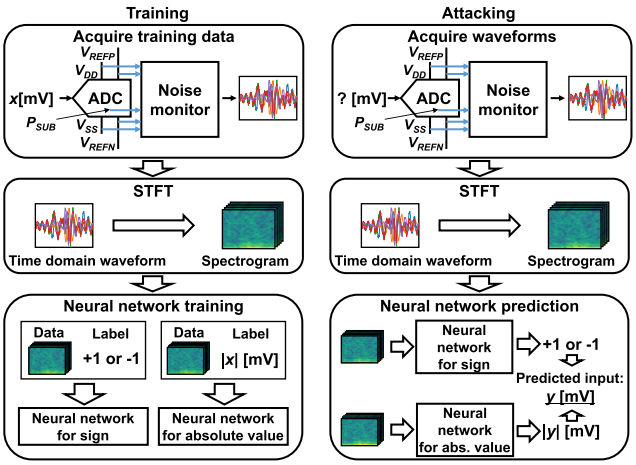

Fig. 4 Flow of proposed SCA method.

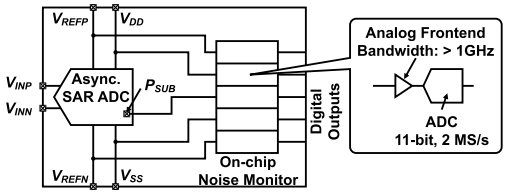

Fig. 5 Block diagram of the test chip.

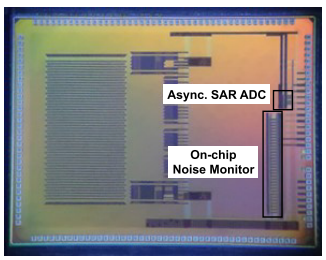

Fig. 6 Chip microphotograph.

more side-channel information when their noise waveforms are added to the input data. This Dual-NN configuration distinguishes the sign and absolute value of the input voltage separately, which improves the accuracy of estimation even in high-speed asynchronous SAR ADCs.

3.2 Dual Neural Network

The sign information of the input data is mainly contained in the noise from the single-ended part of the SAR logic, while the information of the absolute value is largely included in the noise from the comparator and the differential part of the SAR logic. To efficiently extract information which has such different characteristics from the noise waveforms, it is considered to be effective to use two separate neural networks. Figure 4 shows the flow of the Dual-NN side-channel attack. The first step of the Dual-NN SCA is the training step to learn the correlation between the input voltage of the ADC and the noise waveforms. Many pairs of the input voltages and the waveforms are required for the input voltage prediction with neural network. Acquired waveforms are converted into spectrograms by short-time Fourier transform (STFT), which enhances the frequency-domain recognition ability of neural networks, with the window length of 64 samples and then the learning operations of two neural networks are executed. The second step is the attacking phase where the input voltage is predicted using two neural networks from the noise waveforms. The acquisition of the noise waveforms and the STFT is performed in the same way as the learning step except that the actual input voltage is unknown. Two neural networks predict the sign and the absolute value of the SAR ADC's input voltage respectively from the spectrograms.

4. Chip Implementation and Measurement Results

The 11-bit asynchronous SAR ADC with differential structure is designed as a target ADC of the proposed Dual-NN based SCA. The ADC operates at 48 MS/s with the power consumption of 465 μW. To analyze noise waveforms accurately, on-chip noise monitors composed of input buffers and ADCs are also implemented on the same chip as shown in Fig. 5. The monitor circuit acquires the noise waveforms of V_{DD}, V_{SS}, V_{REFP}, V_{REFN} and P_{SUB} nodes with a wide bandwidth of 1 GHz at 2 MS/s with an equivalent sampling technique. Just one substrate contact placed close to the ADC is required to acquire P_{SUB} waveforms. The asynchronous SAR ADC and on-chip noise monitors are fabricated in 40 nm process as shown in the die photo of Fig. 6. The active area of asynchronous SAR ADC is approximately 1.2×10^{-2} mm^2, and the area of the on-chip noise monitor for monitoring one node is approximately 6.3×10^{-3} mm^2.

The experimental results of SCA on the SAR ADCs are shown in Fig. 7. These plots show the predicted voltages by SCA with respect to the actual input voltages. The input signal used in the experiment is DC signal with equally spaced step and random voltages. When the conventional NN is applied only to V_{REFP} and V_{DD} as in [10], there are large discrepancies between the actual input voltages and the predicted voltages with around 400 mV rms errors. The accuracy rates of sign estimation are 73.9 % and 75.6 %, respectively, as shown in Fig. 7 (a) and Fig. 7 (b). On the other hand, the proposed Dual-NN with both of V_{REFP} and V_{DD} achieves sign estimation with higher accuracy rate of 79.8 %, and discloses the absolute value of the input voltage with 29.96 mV rms error as shown in Fig. 7 (c). Moreover, Dual-NN with all waveforms including V_{SS}, V_{REFN}, and P_{SUB} achieves even more accurate precision as shown in Fig. 7 (d). The sign estimation accuracy rate is sufficiently improved to 89.3 % and the rms error of absolute value prediction is also reduced to 29.35 mV. Table 1 shows the comparison to the state-of-the-art analog SCA techniques. This work demonstrates the first successful attack on high-speed asynchronous SAR ADCs to steal data with high accuracy that threatens information security.

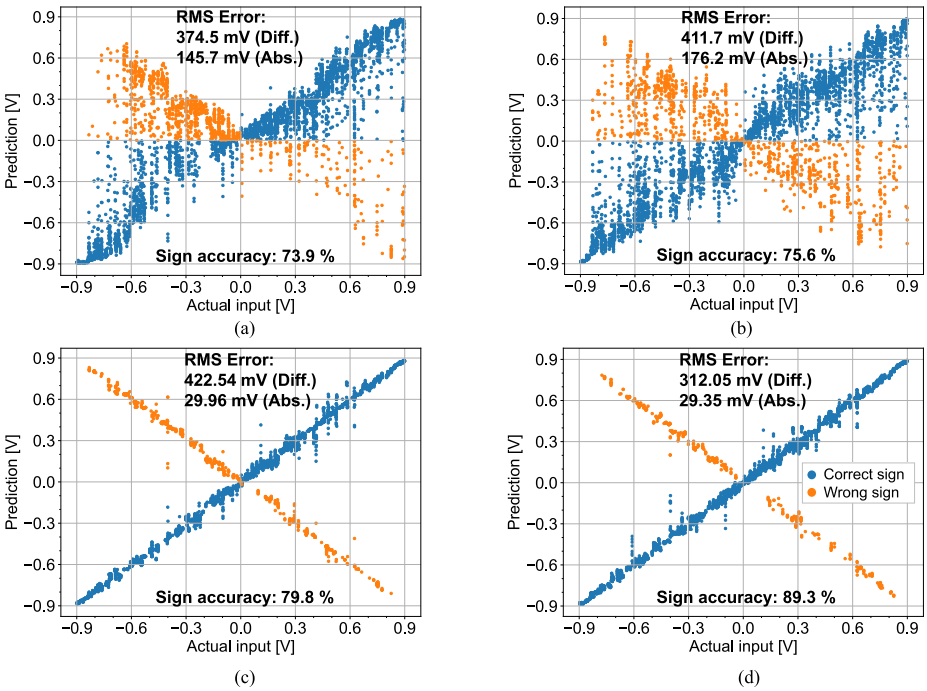

Fig. 7 Prediction results by (a) Conventional NN with V_{REFP}, (b) Conventional NN with V_{DD}, (c) Proposed Dual-NN with V_{REFP} and V_{DD}, and (d) Proposed Dual-NN with all waveforms.

Table 1 SCA performance comparison.

		This work	Jeong SSCS 2021	Miki TCASII 2020
SCA Method		Dual-NN attack	NN attack	Template attack
Target Architecture	Technology	40 nm	65 nm	180 nm
	Speed	48 MS/s	1.25 MS/s	1 MS/s
	Differential	Yes	Yes	No
	Asynchronous	Yes	No	No
Attacking Accuracy		312.1 mV_{RMS} (Async. Diff.) 29.35 mV_{RMS} (Async. Single)	62.91 mV_{RMS} (Sync. Diff.)	74.22mV_{RMS} (Sync. Single)

5. Conclusion

In this brief, the security attack on high-speed asynchronous SAR ADCs was described. To break the symmetry characteristics of supply noise generated by the differential circuit operations, the Dual-NN technique is proposed to construct the dedicated NNs for sign and absolute value estimation respectively. Silicon prototype demonstrates the proposed dual NN-based SCA successfully discloses the input data of asynchronous SAR ADC through multiple power supply and ground nodes with attacking accuracy of 312.05 mV. The discovery of SAR ADC vulnerabilities in this work will promote the development of countermeasures against the SCA in the future. Future work can consider the application of the Dual-NN technique to an ADC integrated to a micro-controller, which generates substrate noise that may affect the performance of the SCA.

Acknowledgements

This paper is based on results obtained from a project, JPNP16007, commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

References

[1] M.A. Khan, M.T. Quasim, N.S. Alghamdi, and M.Y. Khan, "A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data," IEEE Access, vol.8, pp.52018–52027, 2020.
[2] I. Verbauwhede, J. Balasch, S.S. Roy, and A.V. Herrewege, "Circuit challenges from cryptography," IEEE Int. Solid-State Circuits Conf., San Francisco, CA, USA, Dig. Tech. Papers, pp.428–429, Feb. 2015.
[3] Sudeendra Kumar K., S. Sahoo, A. Mahapatra, A.K. Swain, and K.K. Mahapatra, "Analysis of Side-Channel Attack AES Hardware Trojan Benchmarks against Countermeasures," 2017 IEEE Computer Society Annual Symposium on VLSI, Bochum, Germany, pp.574–579, July 2017.
[4] H. Maghrebi, "Assessment of Common Side Channel Countermeasures With Respect To Deep Learning Based Profiled Attacks," 2019 31st International Conference on Microelectronics, Cairo, Egypt, pp.126–129, Dec. 2019.
[5] D. Serpanos, S. Yang, and M. Wolf, "Neural Network-Based Side Channel Attacks and Countermeasures," 2020 57th ACM/IEEE Design Automation Conference, San Francisco, CA, USA, pp.1–2, July 2020.
[6] F. Hu, H. Wang, and J. Wang, "Deep-Learning Side-Channel Attack Against STM32 Implementation of AES," 2021 International Conference on Computational Science and Computational Intelligence, Las Vegas, NV, USA, pp.844–847, Dec. 2021.
[7] T. Miki, N. Miura, H. Sonoda, K. Mizuta, and M. Nagata, "A Random Interrupt Dithering SAR Technique for Secure ADC Against Reference-Charge Side-Channel Attack," IEEE Transactions on Circuits and Systems II: Express Briefs, vol.67, no.1, pp.14–18, 2020.
[8] S. Chari, J.R. Rao, and P. Rohatgi, "Template attacks," Cryptographic Hardware and Embedded Systems 2002, Redwood Shores, CA, USA, pp.13–28, Aug. 2002.

[9] J. Xu and H.M. Heys, "Template Attacks of a Masked S-Box Circuit: A Comparison Between Static and Dynamic Power Analyses," 2018 16th IEEE International New Circuits and Systems Conference, Montreal, QC, Canada, pp.277–281, June 2018.

[10] T. Jeong, A.P. Chandrakasan, and H.-S. Lee, "S2ADC: A 12-bit, 1.25-MS/s Secure SAR ADC With Power Side-Channel Attack Resistance," IEEE Journal of Solid-State Circuits, vol.56, no.3, pp.844–854, 2021.

[11] M. Ashok, E.V. Levine, and A.P. Chandrakasan, "Randomized Switching SAR (RS-SAR) ADC for Power and EM Side-Channel Security," IEEE Solid-State Circuits Letters, vol.5, pp.247–250, 2022.

[12] D. Das, S. Maity, S.B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, "ASNI: Attenuated Signature Noise Injection for Low-Overhead Power Side-Channel Attack Immunity," IEEE Transactions on Circuits and Systems I: Regular Papers, vol.65, no.10, pp.3300–3311, 2018.

[13] M.A. Vosoughi, L. Wang, and S. Köse, "Bus-Invert Coding as a Low-Power Countermeasure Against Correlation Power Analysis Attack," 2019 ACM/IEEE International Workshop on System Level Interconnect Prediction, Las Vegas, NV, USA, pp.1–5, June 2019.

[14] D. Lee, M. Kang, P. Plesznik, J. Cho and D. Park, "Scrambling Technique of Instruction Power Consumption for Side-Channel Attack Protection," 2020 International Conference on Electronics, Information, and Communication, Barcelona, Spain, pp.1–2, Jan. 2020.

[15] Y.-L. Hong, Y.-K. Weng, and S.-H. Huang, "Hardware Implementation for Fending off Side-Channel Attacks," 2021 IEEE International Conference on Consumer Electronics-Taiwan, Penghu, Taiwan, pp.1–2, Sept. 2021.