Extended Abstracts of the 2020 International Conference on Solid State Devices and Materials, VIRTUAL conference, 2020, pp789-790

A Dual-mode SAR ADC Enabling On-chip Detection of Off-chip Power Noise Measurements by Attackers

Takuya Wadatsumi, Takuji Miki and Makoto Nagata
Kobe University
1-1 Rokkodai, Nada, Kobe 657-8501, Japan
E-mail: {wadatsumi, miki}@cs26.scitec.kobe-u.ac.jp, nagata@cs.kobe-u.ac.jp

Abstract

An on-chip noise monitor using a dual-mode analog to digital converter (ADC) is developed to detect off-chip power noise measurement attacks. A two-step sampling scheme using sync./async. clock enables both real-time monitoring and high-resolution diagnostics of power supply noise. A wide-band ADC with 1 GHz BW also helps to analyze the noise waveform in detail and recognize the injected devices. Fabricated in 65 nm CMOS, the proposed noise monitor detects and identifies the series resistors from 1 Ω inserted on power line of the prototype chip.

1. Introduction

Distributed IoT devices are exposed to malicious interference since they are physically accessed by attackers. Power supply terminals of IC chips are often targeted to cause malfunction by actively injecting a disturbance through the terminals. Moreover, they are also used by attackers to measure the power supply noise and steal a secret key of internal cryptographic core by finding the correlation between them [1]. This side-channel attack affects the fluctuation of the noise waveform due to probe contact or sensing device insertion to power supply lines. Thus, on-chip noise monitoring circuits are required to detect the variation of power supply noise waveform. To monitor the power noise, an on-chip waveform capture circuit using a comparator-based quantizer has been reported [2]. However, it requires multiple clock cycles to obtain the digital value of the noise, which disables real-time monitoring. Though an ADC based monitor has been also proposed [3], its bandwidth is too narrow to precisely analyze the noise waveform and recognize the attacks.

In this paper, we propose an on-chip noise monitoring circuit which detects a malicious interference injection in real time and diagnoses the noise with high accuracy to identify the injections. A two-step clocking scheme enables both detection and analysis of malicious interference. The ADC for noise monitoring achieves wide bandwidth owing to the proposed front-end driver, which contributes to detecting the insertion of malicious devices on the power line.

2. On-chip noise monitor with dual-mode ADC.

The proposed on-chip noise monitoring circuit for malicious interference detection is shown in Fig. 1. The target core by attackers is a large scale digital encryption circuit. The power and ground of the digital circuit, V_{DDD} and V_{SSD}, are externally supplied, thus, the attackers can directly access to the power line and steal the cryptographic key information or tamper the internal data by attaching a measurement hardware to the power/ground terminals. To detect such malicious attempts, a wide-band (WB) SAR ADC array is embedded in

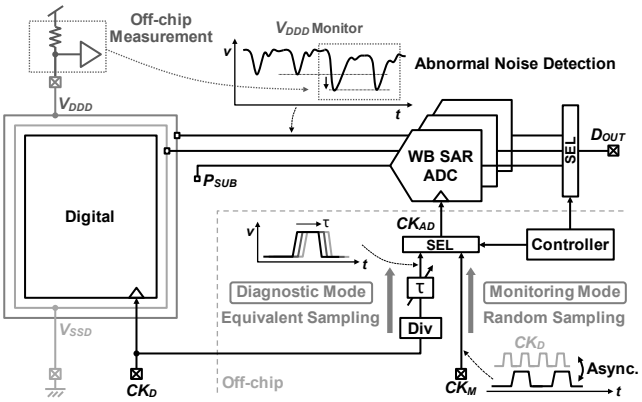

Fig. 1 On-chip noise monitor with dual-mode ADCs.

the same chip. The input nodes of the ADC array are connected to V_{DDD}, V_{SSD} of core rings, and also Si substrate, which enables to probe the voltage bounces of V_{DDD}, V_{SSD} and P_{SUB} during digital circuit operation. The on-chip interference detection circuit with the WB SAR ADC array operates with two modes: monitoring mode and diagnostic mode. In the monitoring mode, the WB SAR ADCs digitize each noise with an external sampling clock CK_M whose frequency is low enough with less than 4 MHz, and is not synchronized with the operation clock of the digital circuit. Since the digital circuit works at the clock frequency CK_D around 100 MHz, the ADCs under-sample the noise waveforms randomly and can detect the abnormal noise level thanks to their wide-band characteristics. After the detection, the circuit goes into diagnostic mode to further analyze the noise waveform and identify the type of disturbance. The CK_D is divided to less than 4 MHz, and its phase is shifted by the variable delay circuit. This clock is selected as a sampling clock and enables the ADCs to digitize with the higher time-resolution using an equivalent sampling technique.

Fig. 2 shows the timing diagram of both monitoring and diagnostic mode when V_{DDD} is monitored as an example. During the monitoring mode, the sampling clock of ADC CK_{AD} is asynchronous to the power noise at V_{DDD}, thus, the ADCs can acquire across the periodical noise waveform without missing the peak points. From the randomly sampled noise values, the characteristics of noise waveform such as the peak-to-peak drop value and average level can be derived. These values are stored as a normal condition, then, compared to them, the ADCs find out an unexpected interference when obtaining an irregular value outside the normal range. After moving to the diagnostic mode, the CK_{AD} starts to be synchronous to the V_{DDD} waveform. By gradually shifting the phase, the V_{DDD} noise can be acquired at equivalently higher sampling frequency. Hence, the noise waveform can be analyzed

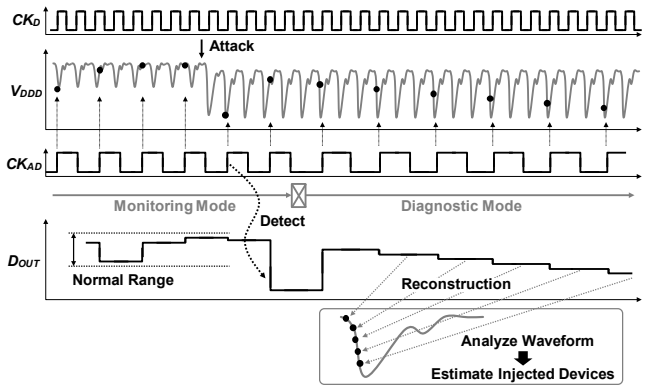

Fig. 2 Timing diagram of monitoring and diagnostic mode.

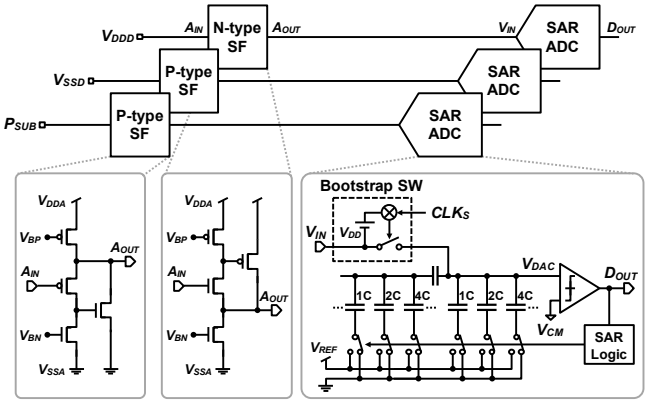

Fig. 3 Circuit schematic of wide-band ADC.

in detail by reconstructing the sampling data, in order to estimate what kind of devices are inserted.

3. Wide-band ADC

The circuit schematic of the wide-band ADCs is depicted in Fig. 3. As front-end buffers, source follower (SF) circuits are employed to drive the noise signals to the ADCs with low output impedance. The V_{DDD} noise is input to the N-type MOS transistor to shift the signal level down to the input range of the following ADC. On the other hand, the noise of V_{SSD} and P_{SUB} are received by the P-type SF with p-MOS transistors. In addition to typical SF configuration, feedback transistors are added to further reduce the output resistance. The ADC is successive approximation register (SAR) architecture for small area and low power consumption. The resolution is 11-bit which is accurate enough for noise analysis. The sampling frequency is up to 4MHz since equivalent sampling is applied. To reduce an on-resistance of the sampling switch and expand the band-width, a boot-strap switch (BSSW) is designed [4]. Moreover, the capacitive DAC is minimized by split structure with series capacitor to reduce the input capacitance of the ADC. As a result, the band width of the monitor circuit is extended to around 1 GHz in AC simulation.

4. Measurement results

A prototype chip was fabricated in 65 nm CMOS. The die photo and the magnified layout view of SAR ADCs are shown in Fig. 4. The area of ADC including SF and BSSW is 160 µm x 50 µm. The integrated ADC array contains 16

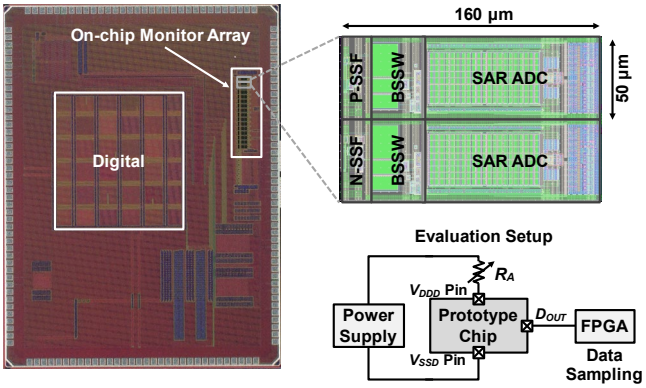

Fig. 4 Die photo and layout image of SAR ADC.

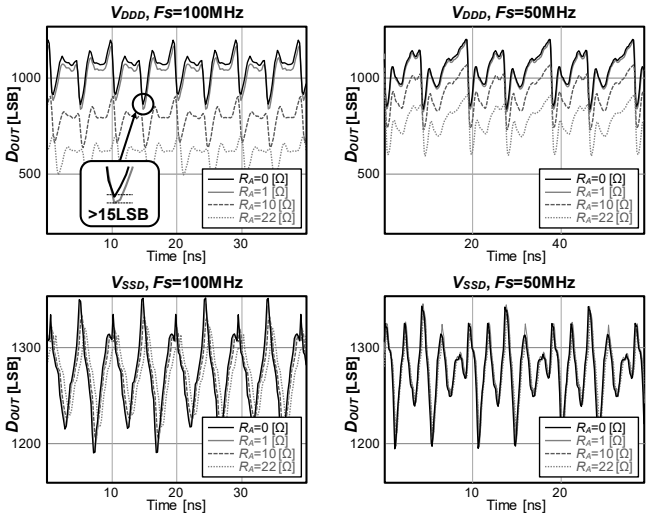

Fig. 5 Measured V_{DDD} and V_{SSD} waveforms.

ADCs, and they probe V_{DDD}, V_{SSD} and P_{SUB} of digital circuits across the entire chip. Fig. 5 shows the measured V_{DDD} and V_{SSD} waveforms acquired by the on-chip monitor with diagnostic mode. The digital circuit operates at 100 MHz and 50 MHz as noise sources. To assume the off-chip measurement attacks, series resistors of 1 Ω to 22 Ω are inserted in the power supply path as illustrated in Fig. 4. From the results, the ADC successfully measures the noise variations due to only 1 Ω insertion with more than 15-LSB resolution, which indicates the proposed on-chip monitor can detect the malicious off-chip noise measurement attacks.

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] S. Chari, *et al*., "Towards sound approaches to counteract power-analysis attacks," in *Advances in Cryptology-CRYPTO 1999.*

[2] T. Hashida, M. Nagata, "An On-chip Waveform Capture and Application to Diagnosis of Power Delivery in SoC Integration," *IEEE JSSC*, Apr. 2011.

[3] J.-E Park, et al., "A 0.5-V Fully Synthesizable SAR ADC for On-Chip Distributed Waveform Monitors," *IEEE Access*, May 2019.

[4] A. M. Abo and P. R. Gray, "A 1.5-V, 10-bit, 14.3-MS/s CMOS pipeline analog-to-digital converter," *IEEE JSSC*, May 1999.