A Random Interrupt Dithering SAR Technique for Secure ADC Against Reference-Charge Side-Channel Attack

Takuji Miki, *Member, IEEE*, Noriyuki Miura, *Member, IEEE*, Hiroki Sonoda, Kento Mizuta, and Makoto Nagata, *Senior Member, IEEE*

***Abstract*—A side-channel attack (SCA) on a reference-charge flow in successive approximation register (SAR) analog-to-digital converters (ADCs) discloses analog information acquired at a sensor frontend. A random interrupt dithering masks the correlation between analog input and reference charge flow by injecting extremely large dither of 1/4 full scale. An internal dither-tracking comparator yet guarantees rail-to-rail operation, resulting in no penalty in conversion accuracy. The comparator functions as a physical-random source for dithering. The unpredictable randomness based on comparator metastable operation by thermal noise enhances the security level while the shared use of the comparator reduces the associated hardware overhead. The additional silicon area penalty for the proposed technique is only 7% of an unprotected ADC core area. A 10-bit 1 MS/s secure SAR ADC was fabricated in 0.18-μm CMOS. The measurement results demonstrate the proposed secure ADC suppresses the information leakage from 4.6 bit to 0.8 bit against reference-charge SCA.**

***Index Terms*—Analog to digital converter, dither, hardware security, SAR, side-channel attack.**

I. Introduction

INFORMATION security is one of the most critical issues in the coming IoT era where malicious attackers exist to steal valuable information handled in critical IoT services. A hardware-domain physical implementation attack on distributed IoT sensor nodes is one serious threat (Fig. 1). Although direct probing of digital and RF information is disabled by cryptography, a Side-Channel Attack (SCA) on a digital hardware block for the cryptography causes information leakage. This digital SCA has been widely discussed and many countermeasures were reported such as in [1]. However, there has not been much discussion on the physical attack on an analog hardware block at the sensor frontend. It is in fact much more critical as the security in the succeeding digital blocks all relies on the security in the analog frontend. The serious security hole exists at the boundary between analog and digital domain, i.e., ADC. Although direct analog probing is almost impossible due to its weak signal strength, SCA on ADC could disclose analog information without disturbing it significantly.

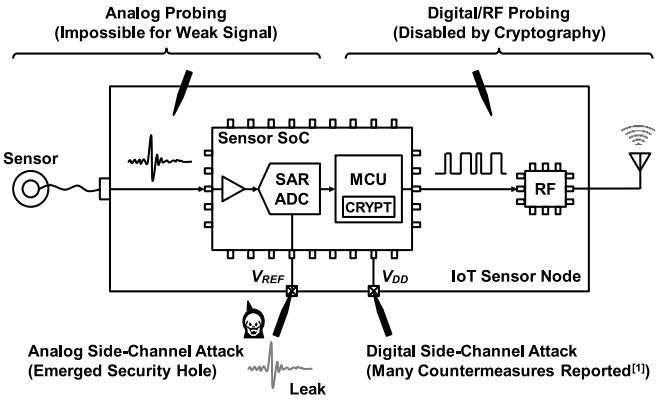

Fig. 1. Security hole of IoT sensor analog frontend.

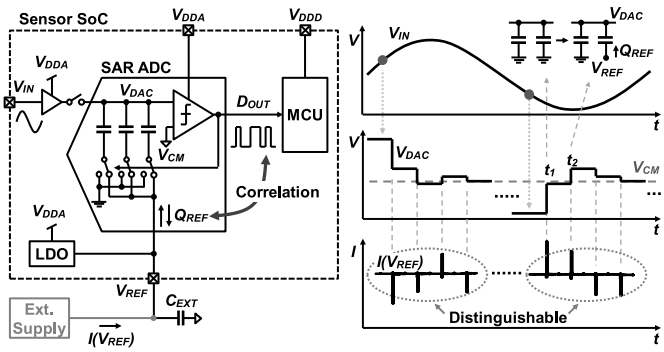

Fig. 2. Reference-charge side-channel attack on SAR ADC.

This brief for the first time demonstrates SCA on ADC. A Successive Approximation Register (SAR) ADC is attacked as it is the most widely used ADC in recent IoT sensor analog frontends such as for compact battery-driven or even battery-less wearable healthcare monitoring SoCs [3], where the SAR architecture currently only meets the stringent demands of low active/standby power, small area, and compatibility with digital-oriented low-voltage scaled process [4]. An effective SCA on SAR ADC is possible by exploiting correlation between analog input and a reference-charge flow via a reference voltage V_{REF} pin. This emerging analog SCA can be

Manuscript received August 23, 2018; revised December 13, 2018 and January 21, 2019; accepted February 17, 2019. Date of publication February 26, 2019; date of current version December 26, 2019. This brief was recommended by Associate Editor H. Shibata. *(Corresponding author: Takuji Miki.)*

The authors are with the Graduate School of Science, Technology and Innovation, Kobe University, Kobe 657-8501 Japan (e-mail: miki@cs26.scitec.kobe-u.ac.jp).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSII.2019.2901534

disabled by dithering technique however the associated overhead becomes huge. In this brief, a secure yet small-overhead circuit solution is presented.

II. Reference-Charge Side-Channel Attack on SAR ADC

Fig. 2 shows a typical SAR ADC configuration in a sensor SoC. In order to acquire relatively high impedance signal V_{IN} such as ECG and EEG with dry electrode, input circuit requires much higher impedance [5]. It makes direct analog probing impossible since the probing on such a sensitive analog node may change the original signal. Thus, a dedicated reference voltage pin V_{REF} for driving a charge redistribution capacitive DAC becomes the first target for stealing the acquired analog signal information without disturbance. Also, the SCA on an analog supply voltage V_{DDA} is very difficult because V_{DDA} is shared among other analog components in the SoC and charge flow at V_{DDA} has small dependency on input signal V_{IN}. The V_{REF} on the other hand is separated from V_{DDA} for noise and crosstalk suppression even though their voltage levels are often the same value. Even if the V_{REF} is driven by an internal LDO regulator, the V_{REF} pin is exposed for the connection to a large external decoupling capacitor C_{EXT} on a board for stability issues. Another reason for providing the external V_{REF} pin is to allow the users to select the dynamic range of the ADC. By supplying the reference charge Q_{REF} to this V_{REF} pin externally and monitoring $I(V_{REF})$ during the charge redistribution operation for AD conversion, the V_{IN} information can be predicted through a correlation analysis between the distinguishable waveform of $I(V_{REF})$ and V_{IN} (Fig. 2). This SCA can be realized by attaching a malicious hardware Trojan on-board to the exposed V_{REF} pin of sensor system. It monitors the Q_{REF} and analyzes the correlation during AD conversion without touching the sensitive analog input. Thus, the attack never sacrifices normal ADC operation, and a confidential sensor analog data can be stolen without application users noticing it.

III. Random Interrupt Dithering SAR ADC

There are mainly two approaches to prevent the side channel leakage of SAR ADC. One is to suppress the input signal dependency of the reference charge. A differential structure can reduce the input dependency but cannot completely eliminate. It only makes the input signal dependency of the reference charge flow to be parabola characteristics, not flat. Hence, the differential structure is not secure enough, even though the layout area is enlarged from a single-end implementation. A circuit concept for the input signal independent operation in SAR ADC was proposed in [6] and [7]. This ADC not only enhances the performance but also can prevent the side channel leakage. However, it requires a dedicated capacitive DAC separately from a sampling capacitor, resulting in non-negligible area overhead.

The second approach is to dynamically disrupt the correlation between the input signal and the reference charge. Dithering, the well-known ADC performance enhancement technique for nonlinearity error [8], can be potentially used. By intentionally injecting a noise to an analog input of ADC and later subtracting in a digital domain, the dithering can hide the correlation between input and internal operation like logic

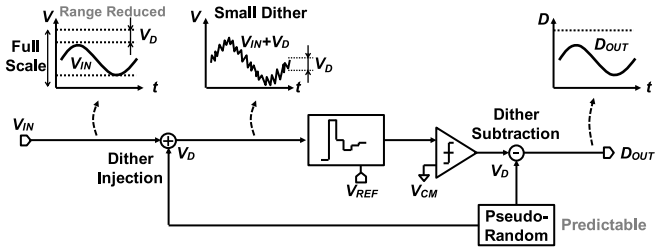

Fig. 3. Conventional dithering.

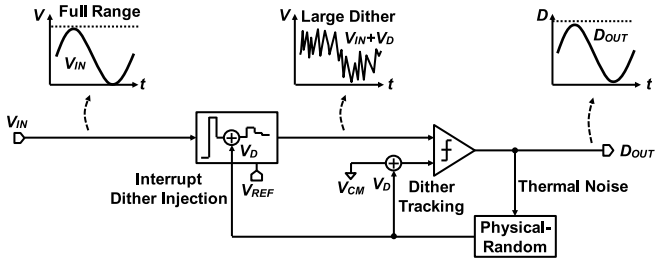

Fig. 4. Proposed random interrupt dithering.

masking resilient against digital SCA [9]. Fig. 3 shows the block diagram of the conventional dithering circuits. The dither voltage V_D generated by pseudo-random binary sequence is intentionally added to the input voltage, and subtracted after quantization by SAR ADC. In the conventional dithering, V_D amplitude is limited since large V_D sacrifices an input range and hence bit resolution (ADC performance). In addition, such small dither can only mask lower bit ADC operation, resulting in data leakage of significant bit by the reference-charge SCA. Furthermore, the pseudo-random binary sequence can be predicted by malicious attackers with long time monitoring of the ADC operation. In this brief, a random interrupt dithering is proposed for the security enhancement without sacrificing the ADC performance (Fig. 4). For dither injection, a comparator noise based random bit sequence is used. The physical-randomness makes it impossible for the attacker to predict the dither (mask) operation. For layout area savings, the existing comparator is utilized to generate the physical-random bit by exploiting its internal thermal noise. The dither is injected interruptedly during the binary search operation of SAR. By injecting the dither after MSB decision and subtracting it in analog domain, an overflow does not occur even if a large amplitude dither of 1/4 full scale is injected. This large dither masks the correlation between input data and internal operation drastically, resulting in the suppression of significant bit information leakage and analog data protection against the reference-charge SCA.

Fig. 5 shows a circuit diagram and operation waveform of the 10-bit secure SAR ADC. It is basically composed of binary-weighted capacitive DAC (CDAC), comparator, sampling switch and digital logic circuitry. Only small few circuit blocks are added to perform the random interrupt dithering. To generate random bit sequence, the existing comparator is used. The penalty is only one extra comparison after LSB judgement equivalent to only 7% speed penalty. The CDAC output V_{DAC} at this extra judgement by necessity approaches very close to the threshold voltage of the comparator V_T. Then, the comparator generates 0 or 1 based on the internal thermal

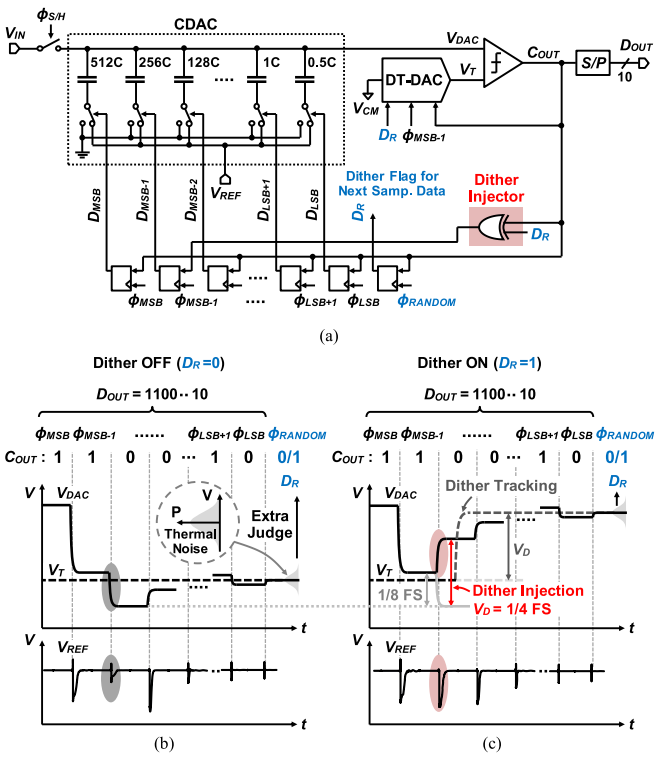

Fig. 5. Secure SAR ADC (a) circuit diagram, operation waveforms (b) without, and (c) with dither injection.

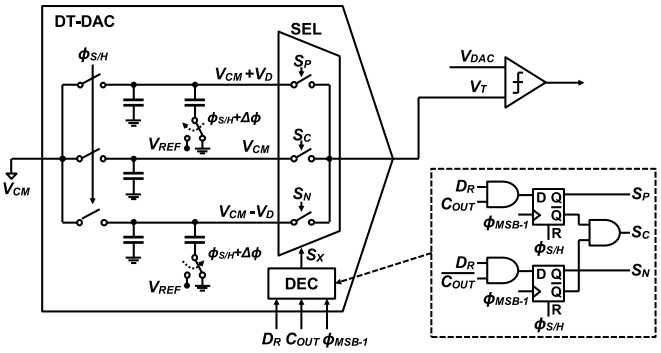

Fig. 6. Circuit details of dither tracking DAC.

noise distribution [10]. The comparator is designed with noise sigma of 0.3 LSB to ensure both accuracy and random generation. However quantization error of $+/-$ 0.5 LSB causes uneven 1/0 occurrence probability. Thus, a half unit capacitor of $0.5C$ is added in the CDAC to move the V_{DAC} further close to mean of the comparator noise distribution by reducing quantization error. As the result, the comparator amplifies the input referred noise and generates high entropy random number at the extra judgement after 0.5C transition. The random bit D_R is latched at the last phase of conversion, and used as a dither enabling flag for the next sampling data. The dither injection is realized by only one additional XOR gate inserted between the comparator output C_{OUT} and CDAC control logic for MSB-1 decision (Fig. 5(a)). When the random bit D_R is 0, the CDAC works normally in the binary search manner and V_{DAC} moves toward V_T (Fig. 5(b)). On the other hand, in the case of $D_R = 1$, the CDAC control signal for MSB-1, D_{MSB-1}, is intentionally inverted by the XOR. The V_{DAC} voltage inversely moves against the decision of the comparator (Fig. 5(c)). This operation corresponds to the dither injection with the amplitude of $V_D = 1/4$ full scale. Since the MSB decision is already given and V_{DAC} transition with 1/4 full scale toward V_T is completed, this large dither injection never causes overflow. A full scale input is therefore acceptable in this interrupt scheme even with the large dither injection. In order to complete the correct conversion after the dither injection, dither tracking DAC (DT-DAC) is implemented on the other input of the comparator. The V_T voltage dynamically shifts according to the polarity of the dither injection V_D. When V_D is positive (Fig. 5(c)), V_T shifts from V_{CM} to $V_{CM} + V_D$, where V_{CM} is an input common mode voltage. When negative, V_T shifts to $V_{CM} - V_D$. This tracking operation is equivalent to dither subtraction in the analog domain. As the result, the same output code D_{OUT} as in normal operation can be obtained, while the V_{REF} waveforms are different due to the charge flow change by the V_{DAC} transition in the opposite direction.

Fig. 6 depicts the circuit details of the DT-DAC. The DT-DAC generates V_{CM}, $V_{CM} + V_D$ and $V_{CM} - V_D$ by using additional CDACs to avoid static power consumption such as in a resistive DAC. However, three dedicated CDACs are needed in parallel to generate three V_T voltages for security purposes. In order to avoid side-channel information leakage whether dither is injected or not, the three V_T voltages are prepared regardless of dither injection and later selected depending on the tracking operation. At the S/H phase $\phi_{S/H}$, all DT-DAC capacitors sample the input common mode voltage V_{CM}. After a short time $\Delta\phi$ from the sampling, the bottom node of some capacitors are switched, which produces the voltages of $V_{CM}+/-V_D$. The output voltage of the DT-DAC V_T are selected from the three voltages according to the selector S_X decoded from the control signals, D_R, C_{OUT} and ϕ_{MSB-1} as shown in the Fig. 6. When the D_R is 1, which is dither injection mode, $V_{CM} + V_D$ or V_{CM}-V_D is selected based on the comparator output C_{OUT} at the phase of ϕ_{MSB-1}. The default value of V_{CM} is selected during normal operation and until dither injection. Unlike the main CDAC, the additional CDACs for DT-DAC is composed of coarse unit capacitors (roughly 8x larger compared to the main CDAC) for compact layout by removing the space and margin between the unit capacitors. The associated mismatch errors ε_P and ε_N in $+/-V_D$ are foreground measured at start up using following equation:

$$D(\varepsilon_{P/N}) = D_{OUT(DR1)} - D_{OUT(DR0)} \quad (1)$$

where $D_{OUT(DR1)}$ and $D_{OUT(DR0)}$ are the digital output values when D_R is fixed to 1 and 0, respectively. Each digital value is obtained utilizing redundant bit technique [11] to recover the tracking errors by additional comparison and V_{DAC} transition with extra capacitor as shown in Fig. 7. The calibration value is selected from $D(\varepsilon_P)$ or $D(\varepsilon_N)$ according to S_X, then, by subtracting it from ADC output, the DT-DAC error can be compensated in digital domain. In this brief, 32x unit capacitor $32C$ is added to $1{,}024C$ total main CDAC. A thorough simulation study estimates ε_P and ε_N to be around $+/-$8LSB at maximum due to mismatch and parasitics. The $32C$ redundancy provides the wide enough error recovery range within $+/-$16LSB. This non-replica DT-DAC implementation with digital calibration suppresses the required

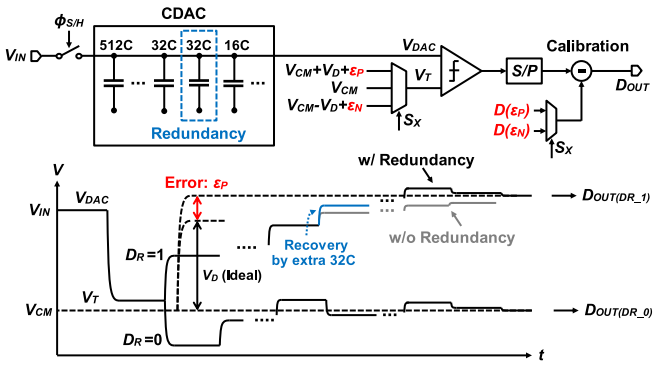

Fig. 7. Calibration for the DT-DAC errors.

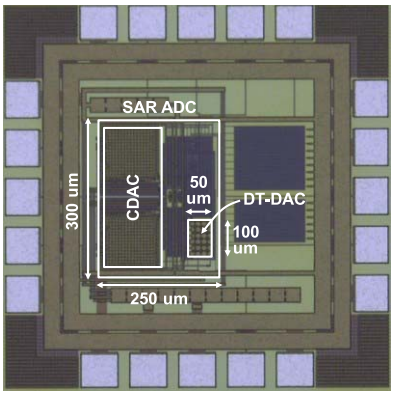

Fig. 8. Die photo.

area penalty by half. Together with the shared comparator utilization for physical-random source, the total area overhead is reduced to be less than 7% of the unprotected ADC core.

IV. Measurement Results

Fig. 8 shows the die photo of the proposed ADC. A 10-bit 1MS/s single-ended secure SAR ADC was fabricated in 0.18 mm CMOS with MIM capacitance. To reduce switching power consumption, the main capacitive DAC is a split-capacitor type architecture [12]. The ADC occupies 300 mm x 250 mm including DT-DAC and other control block for the proposed dithering. Since the accuracy of the DT-DAC capacitor array can be relaxed thanks to the calibration technique, the area of DT-DAC is reduced to 50 mm x 100 mm. The total area overhead is only 7%. Although this prototype SAR ADC is traditional single-ended configuration, the proposed technique can adapt to any switching method of the differential structure such as monotonic switching scheme [13] and single-side switching technique [14].

Fig. 9 shows the measurement setup to evaluate reference-charge SCA. The reference voltage V_{REF} is externally supplied to the ADC via 1 ohm shunt resistance to monitor the reference-charge flow ΔV_{REF} using differential probe and oscilloscope. To solve the correlation between the input data and ΔV_{REF} waveform, template-based attack is employed [15]. In this measurement, upper 6-bit information, D_{LEAK}, is extracted, thus, 64 templates are prepared beforehand. During off-line processing, 64 input voltages within the full range at equal intervals, $V_{Y0} - V_{Y63}$, are given to the

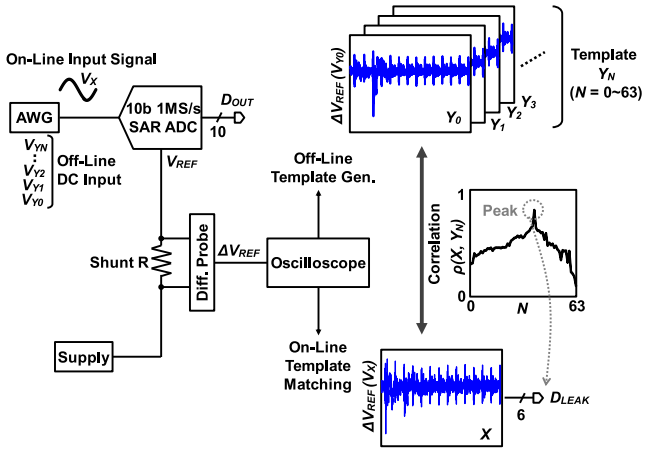

Fig. 9. Measurement setup for reference-charge side-channel attack.

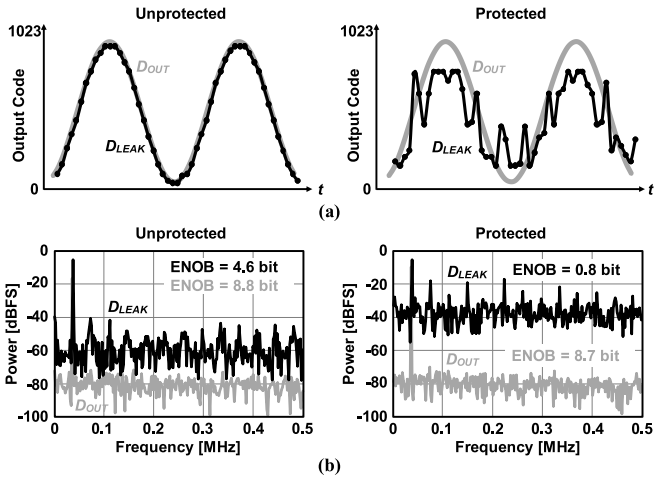

Fig. 10. Measured leakage data with/without protection technique at Fs=1MHz, Fsig=27kHz. (a) Output waveforms, (b) FFT spectrums.

ADC, and each ΔV_{REF} waveform is stored as templates Y_N ($N : 0, 1, \ldots, 63$). Then, the correlation coefficients $\rho(X, Y_N)$ between the ΔV_{REF} waveforms of on-line signal V_X and all templates are solved by the following equation:

$$\rho(X, Y_N) = \frac{\sigma_{X,Y_N}}{\sigma_X \cdot \sigma_{Y_N}} \tag{2}$$

where $\sigma_{X,YN}$ is the covariance between V_X and template waveforms, and σ_X and σ_{YN} are each standard deviation. The index number N of template at the highest correlation $\rho(X, Y_N)$ is considered to be a leak data D_{LEAK} at the input of V_X.

Fig. 10 shows the measurement results of the leakage data using the reference-charge SCA with template matching. The output waveforms of the restored data D_{LEAK} using the template attack before/after applying the protection technique are plotted in Fig. 10(a), and their FFT spectrums are shown in Fig. 10(b). The results of the ADC output data D_{OUT} are also displayed with gray line on the same graphs. The input signal of 27 kHz sine wave is given to the ADC at the sampling rate of 1 MHz. When the proposed dithering is not applied, 4.6-bit ENOB data can be successfully extracted, which indicates most of analog information

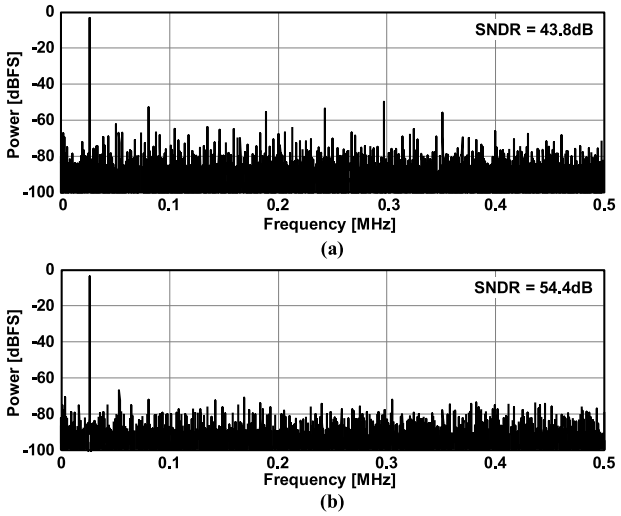

Fig. 11. Measured FFT spectrum, (a) before calibration, (b) after calibration.

is disclosed. On the other hand, the proposed dithering suppresses the data leakage to only 0.8-bit ENOB. This is because the dithering induces the attackers to choose peak correlation at the incorrect code. In addition, dither injection cannot be estimated as the injection is performed based on the physical-random source. Since the proposed dithering affects MSB-1 bit decision, MSB information is leaked. However, more than 90% analog information can be protected against reference charge SCA.

To evaluate randomness of the comparator-based physical random bit, Shannon entropy *H(X)* is introduced as shown in the following equation,

$$H(X) = -\sum_{i} P_i \log P_i \tag{3}$$

where, P_0 and P_1 are the occurrence probabilities of 0 and 1, respectively. The Shannon entropy value of the proposed physical random bit achieves 0.9995 which is high entropy and high quality randomness while keeping unpredictability unlike a pseudo random number generator.

Fig. 11 shows the measured ADC output spectrum with/without the DT-DAC calibration. Without calibration, SNDR is degraded by the error of the dither voltage V_D due to mismatch of coarse DT-DAC capacitors and parasitic elements. However, the calibration improves SNDR by more than 10 dB and achieves 54.4 dB at 30 kHz input. Table I shows the performance summary and overhead for the protection technique. The proposed secure enhancement technique achieves the leakage suppression from 4.6-bit to 0.8-bit with less than 10% speed, power and area overhead.

V. Conclusion

Secure SAR ADC architecture was presented as a countermeasure against reference-charge SCA. The proposed random interrupt dithering can break the correlation between analog input and reference noise without input range reduction. This technique can be realized by adding small circuits with calibration scheme and utilizing internal thermal noise of existing comparator, resulting in less than 10% area overhead. The measurement results indicated this technique achieved over 90% data protection against the reference-charge SCA.

TABLE I
Performance Summary

	Unprotected	Protected
Process [um]	0.18	
Resolution [bit]	10	
Speed [MS/s]	1.07	1
Area [mm^2]	0.07	0.075
Power [uW]	63.6	65.0
ENOB [bit]	8.8	8.7
FoM [fJ/step]	130.8	151.5
INL / DNL [LSB]	±1.2 / ±0.6	±1.2 / ±0.6
SFDR [dB]	64.5	64.3
Leakage [bit]	4.6 (52.3%)	0.8 (9.2%)

Acknowledgment

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

References

[1] I. Verbauwhede, J. Balasch, S. S. Roy, and A. V. Herrewege, "Circuit challenges from cryptography," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2015, pp. 428–429.

[2] N. Verma and A. P. Chandrakasan, "An ultra low energy 12-bit rate-resolution scalable SAR ADC for wireless sensor nodes," *IEEE J. Solid-State Circuits*, vol. 42, no. 6, pp. 1196–1205, Jun. 2007.

[3] Y.-H. Hwang, J.-E. Park, Y. Song, and D.-K. Jeong, "A 20k-to-100kS/s sub-μW 9.5b-ENOB asynchronous SAR ADC for energy-harvesting body sensor node SoCs in 0.18-μm CMOS," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 65, no. 12, pp. 1814–1818, Dec. 2018.

[4] S. Chaput, D. Brooks, and G.-Y. Wei, "An area-efficient 8-bit single-ended ADC with extended input voltage range," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 65, no. 11, pp. 1549–1553, Nov. 2018.

[5] F. N. Guerrero and E. M. Spinelli, "A two-wired ultra-high input impedance active electrode," *IEEE Trans. Biomed. Circuits Syst.*, vol. 12, no. 2, pp. 437–445, Apr. 2018.

[6] R. Kapusta *et al.*, "A 14b 80 MS/s SAR ADC with 73.6 dB SNDR in 65 nm CMOS," *IEEE J. Solid-State Circuits*, vol. 48, no. 12, pp. 3059–3066, Dec. 2013.

[7] J. Craninckx and G. V. der Plas, "A 65fJ/conversion-step 0-to-50MS/s 0-to-0.7mW 9b charge-sharing SAR ADC in 90nm digital CMOS," in *Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2007, pp. 246–247.

[8] H. Pan and A. A. Abidi, "Spectral spurs due to quantization in Nyquist ADCs," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 51, no. 8, pp. 1422–1439, Aug. 2004.

[9] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks," in *Advances in Cryptology-CRYPTO*. Heidelberg, Germany: Springer, 1999, pp. 398–412.

[10] P. Nuzzo, F. D. Bernardinis, P. Terreni, and G. V. der Plas, "Noise analysis of regenerative comparators for reconfigurable ADC architectures," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 55, no. 6, pp. 1441–1454, Jul. 2008.

[11] C.-C. Liu *et al.*, "A 10b 100MS/s 1.13mW SAR ADC with binary-scaled error compensation," in *Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2010, pp. 386–387.

[12] B. P. Ginsburg and A. P. Chandrakasan, "500-MS/s 5-bit ADC in 65-nm CMOS with split capacitor array DAC," *IEEE J. Solid-State Circuits*, vol. 42, no. 4, pp. 739–747, Apr. 2007.

[13] C.-C. Liu, S.-J. Chang, G.-Y. Huang, and Y.-Z. Lin, "A 10-bit 50-MS/s SAR ADC with a monotonic capacitor switching procedure," *IEEE J. Solid-State Circuits*, vol. 45, no. 4, pp. 731–740, Apr. 2010.

[14] L. Chen, A. Sanyal, J. Ma, and N. Sun, "A 24-μW 11-bit 1-MS/s SAR ADC with a bidirectional single-side switching technique," in *Proc. IEEE Eur. Solid-State Circuits Conf. (ESSCIRC)*, Sep. 2014, pp. 219–222.

[15] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *Proc. Cryptograph. Hardw. Embedded Syst. (CHES)*, Feb. 2003, pp. 13–28.