Low-power secure S-box circuit using charge-sharing symmetric adiabatic logic for advanced encryption standard hardware design

Câncio Monteiro¹✉, Yasuhiro Takahashi², Toshikazu Sekine²

¹Graduate School of Engineering, Gifu University, Gifu City, Japan
²Department of Electrical, Electronic and Computer Engineering, Faculty of Engineering, Gifu University, Gifu City, Japan
✉ E-mail: canciotimor@gmail.com

Abstract: The previously proposed charge-sharing symmetric adiabatic logic (CSSAL) in an 8-bit S-box circuit is implemented in this paper using a multi-stage positive polarity Reed–Muller representation with a composite field technique. The CSSAL and other conventional dual-rail adiabatic logics are evaluated from the view point of the transitional power fluctuation and the peak current traces in the 8-bit S-box in order to compare their resistance against side-channel attacks. A method to eliminate unwanted glitch current, the triple power clock supplies are required to collect from the attacking device, CPA only requires while the secret key is embedded within it. Unlike modern cryptology which has been a special threat for algorithm designers, software developers and hardware engineers working to secure private information stored in cryptographic devices such as smart cards, radio frequency ID (RFID) tags, USB tokens and wireless sensors. The SCA can be used to unveil the secret key of cryptographic devices by analysing the side-channel information such as the power consumption, computing time and electromagnetic radiation. Among these SCA attack techniques, differential power analysis (DPA) attack is one of the most threatening type of attacks that reveal the secret information in a cryptosystem. A DPA attack seeks to reveal the secret key of a smart card by statistically analysing the power fluctuations that occur while the device encrypts and decrypts large blocks of data [1]. Since when the DPA attacks reported by Kocher et al. in 1999, it has been widely studied for possible countermeasures against DPA attacks in both algorithm and hardware levels [2–6]. Moreover, an improvement in DPA attack known as correlation power analysis (CPA) attack has been practically implemented in [7, 8]. Unlike the DPA experiment, where the power consumption of all possible keys (including the hypothetical keys and the secret key) are required to collect from the attacking device, CPA only requires the power consumption of the cryptographic device to be collected while the secret key is embedded within it [8]. Apart from the power analysis attacks, the differential electromagnetic radiation attack (DEMA) has been extensively studied [9–11]. DEMA attacks can reveal secret information because the current flow during the switching of the complementary metal–oxide semiconductor (CMOS) gates causes a variation in the surrounding electromagnetic field, which can be monitored by positioning an inductive probe around the microcontroller chip.

On the basis of cryptanalysis knowledge to unveil secure information in the preceding data encryption standard, that is the advanced encryption standard (AES), an efficient algorithm for both hardware and software implementations was standardised by the NIST in 2001 [12]; this standard operates over GF(2⁸) for computational efficiency and exhibits high resistance to cryptanalysis, hardware and software compatibility, and flexibility. Since the new AES was announced, much efforts have been expended [13–16] to simplify a finite field over GF(2⁸) in the S-box transformation to $GF(2^8)$ and $GF((2^8)^2)$ for low cost, low power consumption and low complexity. An optimisation strategy to simplify the complicated circuitry in AES S-box over $GF((2^8)^2)$ have been reported by Wong et al. [17]. They proposed simplified algorithm by employing algebraic normal form and common sub-expression elimination algorithm efficiently optimises the logical expression. Moreover, the low-cost structure-independent fault detection schemes and the gate-level minimisations for the inversion in $GF(2^8)$ were presented in [18, 19]. Mostly, the algorithm-level designs are aimed at low circuit complexity, low area occupancy, enhancing computation time, increasing output data-rate, and so on; however, in our observation, sometimes less attention for AES hardware security against SCA attacks exists.

In an AES-128 hardware platform, there are 10 rounds of iterations, where the first to ninth rounds are composed of four transformation circuits in each round of computation, such as AddRoundKey, Mixcolumn, ShiftRow and SubByte (S-box) transformation, except the Mixcolumn operation is omitted in the final round, as simply depicted in Fig. 1. Among these four transformations, the S-box circuit is the most consuming in terms of area, computation time, high power and serious security treatment, which we highly consider in this contribution work. A typical target point of attackers in a cryptosystem is depicted in Fig. 2. The attackers may have control over the secret information by guessing the secret key values in the statistical analysis from the DPA measurement result in the output of the S-box circuit. Therefore the S-box circuit needs to be accurately designed to maintain the secrecy of the processed private information. As a countermeasure to the problem mentioned above, two types of adoption techniques have been implemented thus far, namely, hiding and masking at the cell level. The objective of hiding countermeasures is to make the power consumption of the cryptographic devices independent of both the intermediate values and the operation that is performed. The hiding technique has been
reported by a sense-amplifier-based logic (SABL) [20], wave dynamic differential logic (WDDL) [21] and three-phase dual-rail pre-charged logic (TDPL) [22]. A thorough investigation on security level of WDDL and SecLib logic styles has been presented by Guilley et al. [23]. The simulation and experimental results [23] proved that SecLib is much more resistive than WDDL. In a masking method reported in [24, 25], the logic technique that is introduced randomises the input signals to avoid input–output data dependency. In addition, a fault rate analysis on masked AES in [26] briefly presents the masking technique to avoid setup time and glitch cycle mismatch during AES execution. Practically, the drawback of this masking technique is that switching from one type of masking to another type often requires significant amount of additional operation.

A majority of the logic styles implemented in cryptographic hardware applied the conventional CMOS logic operation that causes the occurrence of different high spike current and huge energy consumption. For example, peak current transition of a static CMOS (scCMOS) used for security integrated circuits (ICs) consumes different peak current for charging and discharging process, as shown in Fig. 3a. Furthermore, a technique to balance the charging and discharging load for uniform peak current trace, the dual-rail CMOS (DR-CMOS) logic in Fig. 3b become a solution for secure logic designing. Observing the current transition in Figs. 3a and b, generally, transitional power consumption values hold that \( (P_{0\rightarrow0} \approx P_{1\rightarrow1}) \ll (P_{0\rightarrow1}, P_{1\rightarrow0}) \), which is attackable by using Hamming distance (HD) model in power analysis attacks. The idea behind HD model is to count the number of \( P_{0\rightarrow1} \) and \( P_{1\rightarrow0} \), \( P_{0\rightarrow0} \) and \( P_{1\rightarrow1} \) transitions that occur in the digital circuit during a certain time interval with the assumption of \( (P_{0\rightarrow1} \approx P_{1\rightarrow0}) \approx (P_{0\rightarrow0} \approx P_{1\rightarrow1}) \). From the viewpoint of DPA and DEMA attack techniques, the scCMOS and DR-CMOS are vulnerable, because they perform different peak current transition and different large magnitude which cause a sudden variation in the electromagnetic field surrounding the chip.

![Fig. 1 Schematic of the AES encryption circuit](image1)

![Fig. 2 Attack point in partial AES S-box circuit](image2)

![Fig. 3 Logic comparison of the transitional current traces](image3)

---

This is an open access article published by the IET under the Creative Commons Attribution-NonCommercial License (http://creativecommons.org/licenses/by-nc/3.0/)
as reported in [9]. As a result, the DPA and DEMA attacks are a bit difficult to avoid.

In our approach, we have implemented a logic circuit that exhibits uniform peak current for all possible input transition to avoid HD model by an expression \( \left( \frac{P_{0_{\rightarrow}1}}{P_{1_{\rightarrow}0}} \right) \approx \left( \frac{P_{0_{\rightarrow}0}}{P_{1_{\rightarrow}1}} \right) \) as shown on the right side of Fig. 3c. The proposed fundamental logics and their implementation in the multiplier over \( GF(2^4) \) has been presented and published in [27, 28]. In this work, our previously proposed CSSAL is implemented in an 8-bit AES S-box circuit using the positive polarity Reed–Muller (PPRM) representation [14] for low peak current transition and low energy consumption by exploiting an adiabatic switch principle [29]. We have also implemented several dual-rail adiabatic logic styles, such as SyAL [30], 2N-2N2P [31] and a static CMOS circuit [14] in the same S-box circuit and compared the results with each other. All the comparative results described in this work are obtained using the SPICE simulation at the cell level.

2 Low-power S-box circuit using adiabatic logic

2.1 Adiabatic logic technique

Adiabatic switching is commonly used for minimising the energy lost during the charging/discharging period at all nodes of a circuit. The main concept of adiabatic switching is shown in

![Diagram](image1)

**Fig. 5** Proposed CSSAL

| a | Inverter logic structure |
| b | Timing diagram |
| c | Equivalent RC model for each phase |

IET Circuits Devices Syst., 2015, Vol. 9, Iss. 5, pp. 362–369

This is an open access article published by the IET under the Creative Commons Attribution-NonCommercial License (http://creativecommons.org/licenses/by-nc/3.0/).
Fig. 4b: this figure indicates a transition that is considered sufficiently slow such that heat is not significantly emitted. The adiabatic dissipated energy is expressed as $E_{\text{adiabatic}} = 2(RC/\tau)V_{\text{dd}}^2$, where $R$ is the effective resistance in the driven device, $C$ is the output node capacitance to be switched, $\tau$ is the time over which switching occurs and $V_{\text{dd}}$ is the voltage to be switched across. Ideally, the charging energy $E_{\text{adiabatic}}$ tends to zero by increasing the length of $\tau$. Conversely, the conventional CMOS logic operation is shown in Fig. 4a, with the following equation: $E_{\text{conv.}} = CV_{\text{dd}}^2/2$; here, it is possible to reduce the charging energy only by reducing $V_{\text{dd}}$ or capacitor $C$. Fig. 4c shows a comparison of the peak supply current for the equivalent RC models of the conventional CMOS logic and the adiabatic logic. The comparison result in this figure shows that the instantaneous peak supply current of the adiabatic logic is significantly lower than that of the conventional CMOS logic style.

2.2 Charge-sharing symmetric adiabatic logic

The proposed charge-sharing symmetric adiabatic logic (CSSAL) operation was described in details in [27, 28]. We recall the CSSAL inverter logic in this paper for better understanding of the secure logic comparison with Fig. 3, as depicted in Figs. 5a–c. The logic operation is clearly described in Fig. 5b that at $\text{In}, \text{Eval}, \text{Dischg} \geq V_{\text{th}}$ of the MOS transistor in the charge-sharing phase; all

---

Fig. 6  Analysis of the proposed CSSAL, SyAL and the 2N-2N2P PDL

a Transistor schematic of NAND/AND logic of the proposed CSSAL, SyAL and the 2N-2N2P
b Their equivalent RC model at PDL
c Simulated transient response of NAND/AND logic for input (A, B) transition from (0 → 1, 0 → 0) at 12.5 MHz clock frequency, and the supply current graph expresses 16-possible dual-input transitions

Equivalent RC model describes the floating capacitors during the input transition which is indicated by grey colour in the background

---

This is an open access article published by the IET under the Creative Commons Attribution-NonCommercial License (http://creativecommons.org/licenses/by-nc/3.0/)
internal nodes are discharged to ground level before evaluation; hold and recovery phases take place, as shown by the equivalent RC model in Fig. 5c.

The NAND/AND transistor schematic diagram of the proposed CSSAL, SyAL and the 2N-2N2P pull-down logic (PDL) is shown in Fig. 6a, and their respective equivalent RC of PDL is labelled in Fig. 6b, which evidently shows that the proposed CSSAL has always same amount of charges for all possible input transitions. This load balancing is the reason why our proposed logic has uniform energy dissipation for all possible input transitions. 

Input-output voltage signals in Fig. 6c representing dual-input \((A, B)\) condition at \((0 \rightarrow 1, 0 \rightarrow 0)\) transition, and the supply current graph at the bottom of Fig. 6c shows 16-possible dual-input transitions which certifies that the CSSAL’s supply current transition has the same peak values which is able to consume uniformly low power for various input transitions, while the other adiabatic logic styles display large and visible different supply current transitions. It is important to notice that, although only few micro-ampere differ in peak current transition by the individual logics, their implementation in a complex digital circuit, such as in an AES S-box, with the circuit ability for SCA resistance will be degraded, as proved in this work by PPRM S-box current traces in Fig. 9.

2.3 Multi-stage PPRM architecture

The targeting S-box circuit of the multi-stage PPRM architecture has been proposed by Morioka and Satoh [14]. Three sub-components of the conventional composite field S-box circuit were converted into the PPRM form: the pre-inversion section, the inversion section and the post-inversion section, as depicted in Fig. 7. In our proposed CSSAL S-box circuit, we apply three power clock supplies for each section, which completely avoid the glitch current, consume uniform transitional energy and ensure significant energy reduction in our comparative results, even though the transistor counts much higher than other adiabatic logics investigated, as shown in Table 2. Triple power clock \(V_{pc0}, V_{pc1}\) and \(V_{pc2}\) signals are depicted in Fig. 8. The primary input signal and \(V_{pc2}\) shown in Fig. 8 and the input signal and \(V_{pc}\) signal shown in Fig. 7b are identical. The S-box circuit structure presented in the appendix of [14] describes that variables \(x_7 \rightarrow x_0\) denote the primary inputs of an S-box and \(y_7 \rightarrow y_0\) denote primary outputs. The other variables such as \(a, b, c\) and \(d\) denote the internal wires. Therefore in Fig. 8, we apply \(V_{pc0}\) and \(V_{pc1}\) as the power supplies for the internal wires of the circuit architecture shown in Fig. 7b in order to eliminate the unwanted electric hazard voltage at the output signals.

Moreover, we utilise a logic sharing method instead of a multiple logic recurrence method that uses the same input signals; hence, the dual-input logic complexity is reduced to approximately 17% that of Morioka’s design in [14], as an example is shown in Table 1 for internal wires \(a_0 \rightarrow a_7\). In addition, the transistor complexity of the proposed CSSAL is higher than the other adiabatic logic styles; thus, the proposed CSSAL individual logics are an area consumed by our full custom layout design, as shown in Table 2. Furthermore, the proposed CSSAL S-box timing diagram in Fig. 8 shows that the phase delay time of \(V_{pc2}\) is 20 ns from primary input signal; therefore the logic speed is slow in comparing to the other adiabatic logic styles, as summarised in Table 2. Definitions of adiabatic delay time is derived as \(T_{ad, \text{Adiabatic}} = \text{Phase delay time} + \text{Propagation delay time}\). Although the proposed circuit has

| Table 1 | Example of the logic sharing method of S-box stage-1 of internal wires \(a_0 \rightarrow a_7\) |
|---------------------------------|--------------------------------------------------|
| PPROM [14] | This work |
| \(a_0 \rightarrow a_7\) | \(x_7 \rightarrow x_0\) |
| \(a_1 \rightarrow a_7\) | \(x_7 \oplus x_6 \oplus x_5 \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_1\) |
| \(a_2 \rightarrow a_7\) | \(x_7 \oplus x_6 \oplus x_5 \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_1\) |
| \(a_3 \rightarrow a_7\) | \(x_7\) |
| \(a_4 \rightarrow a_7\) | \(x_7 \oplus x_6 \oplus x_5 \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_1\) |
| \(a_5 \rightarrow a_7\) | \(x_7 \oplus x_6 \oplus x_5 \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_1\) |
| \(a_6 \rightarrow a_7\) | \(x_7 \oplus x_6 \oplus x_5 \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_1\) |
| \(a_7 \rightarrow a_7\) | \(0\) |
| sub-total: 13 XORs | sub-total: 8 XORs |

---

Fig. 7 Components of the conventional composite field S-box circuit and PPRM representation

\(a\) Conventional composite field AES S-box architecture

\(b\) Multi-stage PPRM representation with the implementation of the proposed triple \(V_{pc}\) signals in the CSSAL 8-bit S-box circuit

---

Fig. 8 Triple power clock signals for CSSAL S-box circuit shown in Fig. 7b

---

This is an open access article published by the IET under the Creative Commons Attribution-NonCommercial License (http://creativecommons.org/licenses/by-nc/3.0/)
The typical result provided in this paper was obtained using SPICE simulation with a 0.18-μm, 1.8-V standard CMOS technology from ROHM Corporation in collaboration with VLSI Design and Education Centre (VDEC) at the University of Tokyo. To validate the results in this proposal, we have simulated and compared our proposed CSSAL with SyAL, and 2N-2N2P using the same parameters. We attach 10-fF load capacitors to all the output nodes of the buffer, NAND/AND and XNOR/XOR gates in our simulation as an optimal design for future chip measurement comparison. The range of the power clock frequency for all logics investigated in this work varies depending on the active frequency bands. Moreover, the CSSAL S-box has the lowest and uniform peak supply current (about 1.5 mA order) for all instantaneous peak supply current transitions by SPICE simulation result, as shown in Fig. 9, which enables the reduction of electromagnetic radiation for DEMA attacks in a practical measurement.

Furthermore, a histogram of the observed energy per power clock cycle in Fig. 10 indicates that the CSSAL S-box circuit guarantees balanced energy consumption, independent of the processed data. For instance, the variation in transitional energy dissipation for the CSSAL S-box circuit fluctuates between 6.5 and 6.8 pJ (6.5 pJ: $E_{\text{max}}$, 6.8 pJ: $E_{\text{min}}$) for 256 cyclical energy data samples; the CSSAL S-box

We measured NED and NSD that indicate the ability of the logic against a power analysis attack. These parameters indicate how the consumed energy is more constant for different input transitions, but only for small values obtained by these parameters. Hence, by observing the results summarised in Table 3, we can conclude that the proposed CSSAL S-box has a unique ability to withstand the DPA attack, because it has smallest values of NED and NSD for all the active frequency bands. Moreover, the CSSAL S-box has the lowest and uniform peak supply current (about 1.5 mA order for all instantaneous peak supply current transitions by SPICE simulation result), as shown in Fig. 9, which enables the reduction of electromagnetic radiation for DEMA attacks in a practical measurement.

3.2 Results

The simulation results of this comparison study are summarised in Table 3 for all the logics investigated in the 8-bit S-box circuit. The data of power consumption of each circuit are obtained as

$$E_{\text{avg}} = \int_0^T V_{\text{cc}}(t)I_{\text{cc}}(t) \, dt$$

which is adopted as the figure-of-merit to measure the resistance against power analysis attacks. The calculation for the normalised energy deviation (NED) and normalised standard deviation (NSD) is given as

$$\sigma_E = \sqrt{\frac{\sum_{i=1}^n (E_i - \bar{E})^2}{n}}$$

is the average of the energy dissipation over each respective transition, and the standard deviation is defined as

$$E = \frac{\sum_{i=1}^n E_i}{n}$$

of the investigation at these frequency ranges is to verify the logic resistance between the active frequency bands. Furthermore, the DPA attacks analyse different peaks of power consumption to reveal the secret key during encryption and decryption; hence, specific analysis of the various energy consumptions per input transitions and the analysis of the current-to-data dependency are required.

drawbacks in terms of overhead area and latency, it consumes more uniform power than other benchmark methods; thus, the input–output data analysis using peak supply current differences by DPA technique is difficult.

3 Simulation and result

3.1 Condition

The typical result provided in this paper was obtained using SPICE simulation with a 0.18-μm, 1.8-V standard CMOS technology from ROHM Corporation in collaboration with VLSI Design and Education Centre (VDEC) at the University of Tokyo. To validate the results in this proposal, we have simulated and compared our proposed CSSAL with SyAL, and 2N-2N2P using the same parameters. We attach 10-fF load capacitors to all the output nodes of the buffer, NAND/AND and XNOR/XOR gates in our simulation as an optimal design for future chip measurement comparison. The range of the power clock frequency for all logics investigated in this work varies depending on the active frequency bands. Moreover, the CSSAL S-box has the lowest and uniform peak supply current (about 1.5 mA order for all instantaneous peak supply current transitions by SPICE simulation result), as shown in Fig. 9, which enables the reduction of electromagnetic radiation for DEMA attacks in a practical measurement.

Table 2 Gate size, transistor counts, layout area and delay of an 8-bit S-box circuit (0.18-μm 1.8-V CMOS standard cell at 12.5 MHz)

| Circuit          | Buffer | AND  | XOR  | S-box | Delay, ns |
|------------------|--------|------|------|-------|-----------|
| Fig. 7b          | 148    | 141  | 216  |       |           |

Transistor counts and delay

| Circuit          | Buffer | AND  | XOR  | S-box | Delay, ns |
|------------------|--------|------|------|-------|-----------|
| CSSAL            | 9 x 148| 19 x 141| 19 x 216| 8 x 116| 22.41     |
| SyAL             | 5 x 148| 15 x 141| 15 x 216| 6 x 956| 6.28      |
| 2N-2N2P          | 6 x 148| 8 x 141 | 10 x 216| 4 x 176| 15        |
| PPRM [14]        | –      | 8 x 203| 16 x 228| 5 x 272| 3         |

Individual logic and S-box layout area, μm²

| Circuit          | Buffer | AND  | XOR  | CSSAL S-box area |
|------------------|--------|------|------|------------------|
| CSSAL            | 83.82  | 105.82| 142.73| 795 x 614        |
| SyAL             | 48.36  | 122.22| 108.87|                  |
| 2N-2N2P          | 51.99  | 55.54 | 94.84 |                  |

Example of CSSAL S-box: (9 × 148) + (19 × 141) + (19 × 216) = 8115T, where

$$\text{CSSAL buffer: } 9T; \text{CSSAL AND: } 19T; \text{CSSAL XOR: } 19T; (T=\text{transistors}).$$

Fig. 9 Comparison of peak supply current traces of the multi-stage PPRM 8-bit S-box circuit at an operating frequency of 12.5 MHz (at the worst case of the current-to-data dependency) using different logic styles

a S-box circuit using CSSAL
b S-box circuit using SyAL
c S-box circuit using 2N-2N2P
d S-box circuit using Morioka’s circuit

This is an open access article published by the IET under the Creative Commons Attribution-NonCommercial License (http://creativecommons.org/licenses/by-nc/3.0/)

IET Circuits Devices Syst., 2015, Vol. 9, Iss. 5, pp. 362–369
has 184 numbers of observation at 6.7 pJ/cycle. On the other hand, the SyAL S-box gives a distribution of 18 numbers at 13.4 pJ/cycle (between 10.8 and 15.2 pJ); the 2N-2N2P S-box only gives a distribution of 5 numbers at 20 pJ/cycle (between 3.5 and 33.0 pJ) and the CMOS S-box [14] has only a distribution of 4 numbers at 25.3 pJ/cycle (between 3.5 and 44.4 pJ). In addition, it has been recognised that the conventional CMOS logic styles such as TDPL and SABL logics are well known and stronger to DPA attacks in secure logic implementation; however, comparative data are not available in this work because we have found out in our thoroughly SPICE simulation results that they are not suitable to operate in the 8-bit S-box using the PPRM representation.

Apart from the logic’s ability for resistance against SCA attacks, power reduction is also one of the research targets. The graphical information shown in Fig. 11 evidently shows that our proposed CSSAL S-box has significant energy reduction as much as about a half of the other adiabatic S-box circuits investigated in this work. Moreover, the CSSAL S-box reduces energy about 3.3 times smaller than the conventional CMOS logic style in Morioka’s work [14] at 12.5 MHz operating frequency.

By considering the circuit performances in terms of low-power dissipation and logic’s ability to avoid supply current-to-data dependencies, the proposed CSSAL S-box circuit has high potential to be implemented in low-speed and low-power secure devices, such as in wireless sensors, RFID tags or might be applicable for IC-card implementation.

### 4 Conclusion

The investigation and comparison of secure adiabatic logic in a partial 8-bit AES S-box using PPRM representation for countermeasure against SCA attacks have been thoroughly carried out in this work. To the best of our knowledge, the DPA and DEMA attacks reveal the secret information by statistically analysing the power fluctuations and the current amplitude of the attacked hardware such as smart cards. Hence, as an alternative solution for these challenges, the dual-rail adiabatic logic is an interesting approach for reducing the information leakage caused by dynamic power and various high dynamic currents in the CMOS logic operation. The investigation results of low-power adiabatic logic styles have shown that the proposed CSSAL S-box has significant energy reduction; such as 70% smaller than the Morioka’s S-box [14], 31 and 65% power reduction from SyAL and 2N-2N2P, respectively, at 12.5 MHz operating speed. Furthermore, CSSAL S-box consumes uniform transitional energy dissipation and exhibits similar peak current transition which improves the security performance to withstand DPA attacks applicable for low-power and secure devices in low frequency bands, such as contactless smart cards, RFID tags and wireless sensors.

### 5 Acknowledgments

This work is partially supported by Marubun Research Promotion Foundation, in Japan. The custom circuits discussed in this paper have been simulated with Cadence and Synopsys tools through the chip fabrication program of the VLSI Design and Education Centre (VDEC) at the University of Tokyo in collaboration with ROHM Corporation.

### 6 References

1. Kocher, P., Jaffe, J., Jun, B.: ‘Differential power analysis’. Proc. Int. Advances in Cryptology Conf. (CRYPTO), 1999, vol. 1666, pp. 388–397
2. Alioto, M., Giancane, L., Scotti, G., Trifiletti, A.: ‘Leakage power analysis attacks: a novel class of attacks to nanometer cryptographic circuits’, IEEE Trans. Comput. Syst. I: Reg. Pap., 2010, 57, (2), pp. 355–367
3. Homma, N., Miyamoto, A., Aoki, T., Satoh, A., Samir, A.: ‘Comparative power analysis of modular exponentiation algorithms’, IEEE Trans. Comput., 2010, 59, (6), pp. 795–807

---

**Table 3** Simulation and calculation results of 8-bit S-box circuit in PPRM representation using proposed CSSAL, SyAL and 2N-2N2P, respectively at 1.25, 12.5 and 50 MHz input power clock frequencies

| Logic         | Proposed CSSAL | SyAL     | 2N-2N2P | Morioka [14] |
|---------------|---------------|---------|---------|-------------|
| Frequency, MHz | 1.25, 12.5, 50 | 1.25, 12.5 | 12.5, 50 | 1.25, 12.5, 50 |
| $E_{\text{min}}$, pJ | 3.11, 6.5, 13.52 | 4.85, 10.78 | 24.87, 1.83 | 3.49, 6.48 |
| $E_{\text{max}}$, pJ | 3.42, 6.76, 14.04 | 5.87, 15.21 | 36.64, 12.66 | 33.04, 51.79 |
| $E_{\text{avg}}$, pJ | 3.35, 6.67, 13.87 | 5.12, 13.29 | 30.34, 6.94 | 18.86, 27.53 |
| $\sigma_{E_{\text{p}}}$, pJ | 0.05, 0.04, 0.09 | 0.13, 0.79 | 1.85, 1.88 | 5.70, 8.34 |
| NED, % | 9.06, 3.84, 3.70 | 17.38, 29.13 | 32.12, 85.55 | 84.44, 87.49 |
| NSD, % | 1.49, 0.60, 0.65 | 2.54, 5.94 | 6.10, 27.09 | 30.22, 30.29 |

**Fig. 10** Observed amount of energy consumed per input transition: proposed CSSAL, SyAL and 2N-2N2P in the 8-bit S-box for 256 energy data sample

**Fig. 11** Simulated energy dissipation comparison of all the investigated adiabatic logics: CSSAL, SyAL, 2N-2N2P, and Morioka [14] in the multi-stage PPRM 8-bit S-box circuit at each operating frequency range
14 Morioka, S., Satoh, A.: ‘A compact Rijndael hardware architecture with S-box optimisation’. Advances in Cryptology – ASIACRYPT’01, 2001, LNCS, 2248, pp. 239–254, doi: 10.1007/3-540-45082-1-15

15 Chen, J.-H., Huang, S.-J., Lin, W.-C., Lu, Y.-K., Shieh, M.-D.: ‘Computation 2N-2P and 2N-2N2P logic circuits without routing constraints’. Proc. Int. Conf. on Embedded Software and Systems, 2008, pp. 4220–4428

16 Shariy, P.V., Agarwal, A., Kachroo, C.D., Singh, J., Sutaoe, M.S.: ‘A combinational logic implementation of S-box of AES’. Proc. IEEE 54th Int. Midwest Symp. Circuit and System, 2011, pp. 1–4

17 Wong, M.M., Wong, M.L.D., Nandi, A.K., Hizajin, I.: ‘Composite field GF((2^17)^2)’, A logic level design methodology for a masked S-box circuit. Proc. CHES, 2005, pp. 172–186, doi: 10.1007/11535212-1-15

18 Kermani, M.-K., Masoleh, R.-M.: ‘Concurrent structure-independent fault detection schemes for the advanced encryption standard’, IEEE Trans. Comput., 2010, 59 (5), pp. 608–622

19 Kermani, M.-K., Masoleh, R.-M.: ‘Efficient and high-performance parallel hardware architecture for the AES-GCM’, IEEE Trans. Comput., 2012, 61 (8), pp. 1165–1178

20 Tiri, K., Akmal, M., Verbauwede, I.: ‘A dynamical and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards’. Proc. 28th ESSCIRC, 2002, pp. 403–406

21 Tiri, K., Akmal, M., Verbauwede, I.: ‘A logic level design methodology for a secure FPGA resistant ASIC or FPGA implementation’. Proc. Design, Automation and Test in Europe Conf. and Exhibition, 2004, pp. 246–251

22 Bucci, M., Giancane, L., Luzzi, R., Trifiletti, A.: ‘Three-phase dual-rail pre-charge logic’. Proc. CHES’06, 2006, LNCS, 4249, pp. 232–241, doi: 10.1007/11894063_19

23 Guilley, S., Sauvage, L., Flament, F., Vong, V.-N., Hoogvorst, P., Paelet, R.: ‘Evaluation of power constant dual-rail logic circuit against DPA with design time security metrics’, IEEE Trans. Comput., 2010, 59 (9), pp. 1250–1263

24 Mangard, S., Thomas, P., Gimmel, B.M.: ‘Side channel leakage of masked CMOS gates’. Proc. Conf. CT-RSA’05, San Francisco, 2005, pp. 351–356

25 Thomas, P., Mangard, S.: ‘Masked dual-rail pre-charge logic: DPA-resistance without routing constraints’. Proc. CHES, 2005, pp. 172–186

26 Wang, A., Chen, M., Wang, Z., Wang, X.: ‘Fault rate analysis: Breaking masked AES hardware implementation efficiently’, IEEE Trans. Circuit Syst.-II: Express Briefs, 2013, 60 (8), pp. 517–521

27 Monteiro, C., Takahashi, Y., Sekine, T.: ‘DPA resistance of charge-sharing symmetric adiabatic logic’. Proc. of IEEE ISCAS ’13, 2013, pp. 2581–2584

28 Monteiro, C., Takahashi, Y., Sekine, T.: ‘Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level’, Microelectron. J., 2013, 44 (6), pp. 496–503

29 Athas, W.C., Svensson, L.J., Koller, J.G., Tzartzanis, N., Chou, E.Y.C.: ‘Low power digital system based on adiabatic-switching principles’, IEEE Trans. VLSI Syst., 1994, 2 (4), pp. 398–406

30 Chou, B.D., Kim, K.E., Chung, K.S., Kim, D.K.: ‘Symmetric adiabatic logic circuits against differential power analysis’, ETRI J., 2010, 32 (1), pp. 166–168

31 Kramer, A., Denker, J.S., Flower, B., Moroney, J.: ‘Second order adiabatic computation 2N-2P and 2N-2N2P logic circuits’. Proc. of the IEEE Int. Symp. on Low Power Design, 1995, pp. 191–196