electronics

Article

Charge Based Power Side-Channel Attack Methodology for an Adiabatic Cipher

Krithika Dhananjay * and Emre Salman *

Department of Electrical and Computer Engineering, Stony Brook University, Stony Brook, NY 11794, USA
* Correspondence: krithika.yethiraj@stonybrook.edu (K.D.); emre.salman@stonybrook.edu (E.S.)

Abstract: SIMON is a block cipher developed to provide flexible security options for lightweight hardware applications such as the Internet-of-things (IoT). Safeguarding such resource-constrained hardware from side-channel attacks poses a significant challenge. Adiabatic circuit operation has recently received attention for such applications due to ultra-low power consumption. In this work, a charge-based methodology is developed to mount a correlation power analysis (CPA) based side-channel attack to an adiabatic SIMON core. The charge-based method significantly reduces the attack complexity by reducing the required number of power samples by two orders of magnitude. The CPA results demonstrate that the required measurements-to-disclosure (MTD) to retrieve the secret key of an adiabatic SIMON core is 4× higher compared to a conventional static CMOS based implementation. The effect of increase in the target signal load capacitance on the MTD is also investigated. It is observed that the MTD can be reduced by half if the load driven by the target signal is increased by 2× for an adiabatic SIMON, and by 5× for a static CMOS based SIMON. This sensitivity to target signal capacitance of the adiabatic SIMON can pose a serious concern by facilitating a more efficient CPA attack.

Keywords: adiabatic circuits; application-specific integrated circuit (ASIC); correlation power analysis (CPA); lightweight encryption; side-channel attack; SIMON core

check for updates

Citation: Dhananjay, K.; Salman, E. Charge Based Power Side-Channel Attack Methodology for an Adiabatic Cipher. *Electronics* **2021**, *1*, 0. https://doi.org/

Academic Editor: Paris Kitsos

Received: 26 April 2021
Accepted: 8 June 2021
Published:

1. Introduction

As Internet-of-things (IoT) based devices have become an integral part of everyday life, the corresponding risk for security breaches is rapidly increasing [1]. Ensuring the security and data privacy for lightweight applications (such as radio frequency identification based systems, wireless sensor nodes and energy harvesting IoT devices) is significantly challenging due to highly limited resources in terms of compute capability, power consumption, and physical area. Typically, the area specification for lightweight applications cannot exceed 2000 gate equivalents (GE) [2]. The robust general-purpose encryption algorithms such as the AES are not considered as suitable candidates for lightweight applications because of their high hardware cost. Consequently, research on compact realizations of AES with area less than 2000 GE is gaining attention [3,4]. There is also a growing interest in lightweight cryptographic algorithms that are specifically designed for resource-constrained applications.

Existing lightweight block ciphers include PRESENT-80 [5], PRINCE [6], CLEFIA [7], CAMELLIA [8], SIMON and SPECK [9]. SIMON and SPECK are two sister algorithms developed by the National Security Agency and internationally standardized by ISO/29167-21 [10] as part of radio frequency identification (RFID) air interface standard for use by commercial entities. SIMON was optimized specifically for hardware performance and SPECK for software implementations. The flexibility and simplicity of the SIMON algorithm makes it suitable for diverse lightweight applications based on the power, performance, area, and security requirements. Specifically, the hardware implementation of the smallest configuration of SIMON (with 32-bit plaintext and 64-bit key) achieves an area utilization of only 523 GE, thus enabling encryption for ultra-low area and low power applications, where it is highly challenging to afford an integrated encryption circuitry [9].

Side-channel attacks that target resource-constrained devices have become a feasible form of threat model by adversaries [11]. These attacks retrieve sensitive information (such as the secret key in cryptography hardware) by observing and analyzing the physical information that leaks from the system such as power consumption [12], execution time [13], heat dissipation [14], and electromagnetic emissions [15]. This paper focuses on correlation power analysis (CPA), which is one of the most common power analysis based side-channel attacks [16,17]. The primary contributions of this paper are as follows: (1) a novel charge-based CPA attack methodology is developed for adiabatic hardware, which reduces CPA attack complexity by two orders of magnitude, (2) the vulnerability of adiabatic SIMON architecture to CPA attack is quantified and compared with the static CMOS based SIMON implementation, and (3) the effect of increasing the load capacitance of the target signal on the complexity of a CPA attack is investigated.

The rest of the paper is organized as follows. Existing works on adiabatic circuits and power attacks targeting SIMON encryption core are summarized in Section 2. Background information on adiabatic switching, SIMON encryption core, and CPA attack is provided in Section 3. Details of the proposed methodology including the implementation of the adiabatic SIMON core and establishing a CPA attack using the proposed charge-based measurement are detailed in Section 4. Simulation results are provided in Section 5. Finally, the paper is concluded in Section 6.

2. Related Work

The susceptibility of SIMON encryption core to power side-channel attacks has been demonstrated in existing works. For example, in [18], a successful CPA attack was mounted on an unprotected parallel implementation of SIMON32/64 with a hypothesis complexity of 176. Similarly, a CPA attack on FPGA based parallel implementation of SIMON64/96 was mounted and masking based countermeasures were proposed in [19]. Furthermore, CPA attack resistance of different datapath architectures of SIMON128/128 was analyzed while optimizing the design for minimal power, performance, and area overhead in [20]. The CPA attacks in all of these prior works, however, have been mounted for FPGA based SIMON architectures implemented with conventional static CMOS logic. Alternatively, an adiabatic SIMON architecture was demonstrated in [21], but side-channel attack resistance was not investigated.

Charge-recycling adiabatic logic has recently received attention in resource-constrained applications [22,23]. For example, new charge-recycling logic families have been developed to maximize energy efficiency and increase resistance against power based side-channel attacks [24–26]. Majority of the work related to power side-channel attacks on adiabatic circuits is based on proposing secure logic families such as secure quasi adiabatic logic (SQAL) [27], charge-sharing symmetric adiabatic logic (CSSAL) [28], symmetric pass gate adiabatic logic (SPGAL) [29–31] and 3-Phase adiabatic logic [32]. These logic families are developed to increase resistance against power attacks and are primarily evaluated with conventional S-box based benchmark circuits such as the AES, DES, Rjindael and PRESENT-80.

In all of these works, the measurement of power traces to mount a CPA attack is similar to the conventional static CMOS based CPA attack methodology. In this work, a novel charge-based sampling method is proposed by leveraging some of the unique aspects of adiabatic switching. The proposed method significantly reduces the attack complexity for adiabatic circuits. Furthermore, to the best of the authors' knowledge, none of the existing works have investigated the CPA attack resistance of an adiabatic SIMON core developed for lightweight applications, as described in this paper. The study on the effect of increase in the output load capacitance on the CPA attack resistance is also analyzed for the first time.

3. Background

3.1. Adiabatic Switching

Adiabatic circuits operate with a trapezoidal or sinusoidal power supply signal to maintain a small voltage difference between the power supply and output nodes during charging [22]. As such, adiabatic operation reduces the power consumption by minimizing the current to charge the output node. Furthermore, as the power supply signal falls, the charge stored at the output node is recycled back to the power supply.

Unlike conventional static CMOS based operation where energy does not depend upon transition time, in adiabatic operation, a larger transition time reduces the overall energy. Thus, adiabatic circuits typically favor relatively lower frequency applications. However, the required rise time to ensure high energy efficiency is highly technology dependent. In advanced nanoscale technologies, adiabatic operation can save considerable power even at frequencies in the range of several hundred megahertz [33], which is sufficient for most of the lightweight applications.

Efficient charge recovery logic (ECRL) is adopted in this work for the adiabatic operation due to its robust operation [22,34]. The transistor-level implementation of an ECRL buffer is shown in Figure 1a. ECRL utilizes four power supply signals, each with a 90° phase shift as shown in Figure 1b. Specifically, there is a 90° phase difference in the power supply signal of adjacent logic gates. There are four stages of operation, depending upon the power supply signal:

- Evaluate (E): In this stage, the power supply signal rises and the inputs *in* and *inb* are stable. If $in = 1$, $outb = 0$, $M2$ turns on once power supply reaches the threshold voltage. Thus, *out* follows power supply signal.
- Hold (H): Power signal and the outputs remain stable for the subsequent gate to evaluate.
- Recovery (R): Both inputs are discharged by the previous gate. The power supply falls and *out* follows power supply signal until it reaches the threshold voltage of $M2$. The charge is partially recovered back to the power supply during this stage.
- Wait (W): The gate waits for the next evaluation stage.

This multi-phase operation in an ECRL gate enables the outputs to be evaluated only during the *evaluate* stage when the inputs remain stable (since the preceding gate is at *hold* stage). Thus, adiabatic logic is inherently pipelined where each gate acts as a register and consumes a quarter of a cycle. The power supply signal is also typically referred to as power-clock signal. Inherent pipelining in adiabatic logic acts as a noise generator that decreases the correlation between the power model and the measured current trace [35]. This characteristic is particularly useful in achieving higher resistance to DPA attacks.

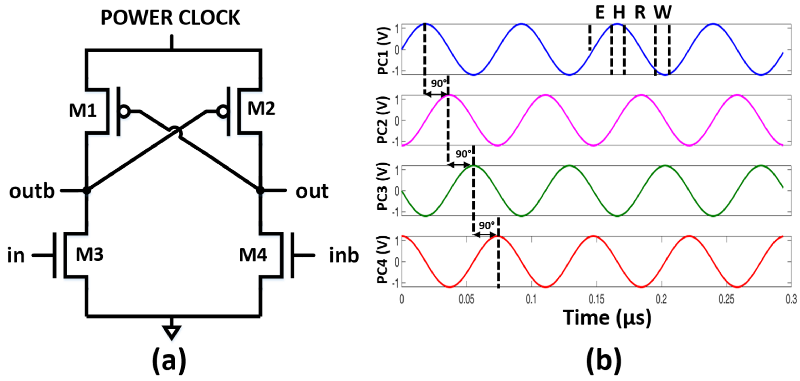


Figure 1. Operation of an ECRL buffer: (**a**) transistor-level schematic, (**b**) four-phase sinusoidal power-clock inputs, each with a 90° phase shift.

3.2. SIMON Encryption Algorithm

SIMON is a lightweight block cipher that has the flexibility to provide reasonable security performance on multiple platforms such as ASICs, microcontrollers, FPGAs, and processors [9]. The algorithm caters to a wide range of block and key sizes that can be chosen depending upon the application and required level of security. A SIMON block cipher with n-bit word plaintext ($2n$-bit block) and m-word key (mn-bit block) is typically referred to as SIMON $2n/mn$ [9]. The configuration adopted for this work is 32-bits of plaintext and 64-bits of key (SIMON 32/64), and 32 rounds of encryption. A typical SIMON algorithm is comprised of a round function and a key expansion function:

3.2.1. Round Function

The SIMON round function uses a two step Fiestel mapping, as shown in Figure 2a and is given by,

$$R(L_{i+1}, R_{i+1}) = (R_i \oplus f(L_i) \oplus K_i, L_i), \tag{1}$$

where i is the current round and $i+1$ is the next round, R is the right word and L is the left word of a block, and K is the key generated by the key expansion module. Function $f(L_i)$ is given by,

$$f(L_i) = ((L_i << 1)\,\&\,(L_i << 8)) \oplus (L_i << 2), \tag{2}$$

where $a << b$ refers to a left-shifted by b bits. This round function is iterated until the desired number of rounds is reached.

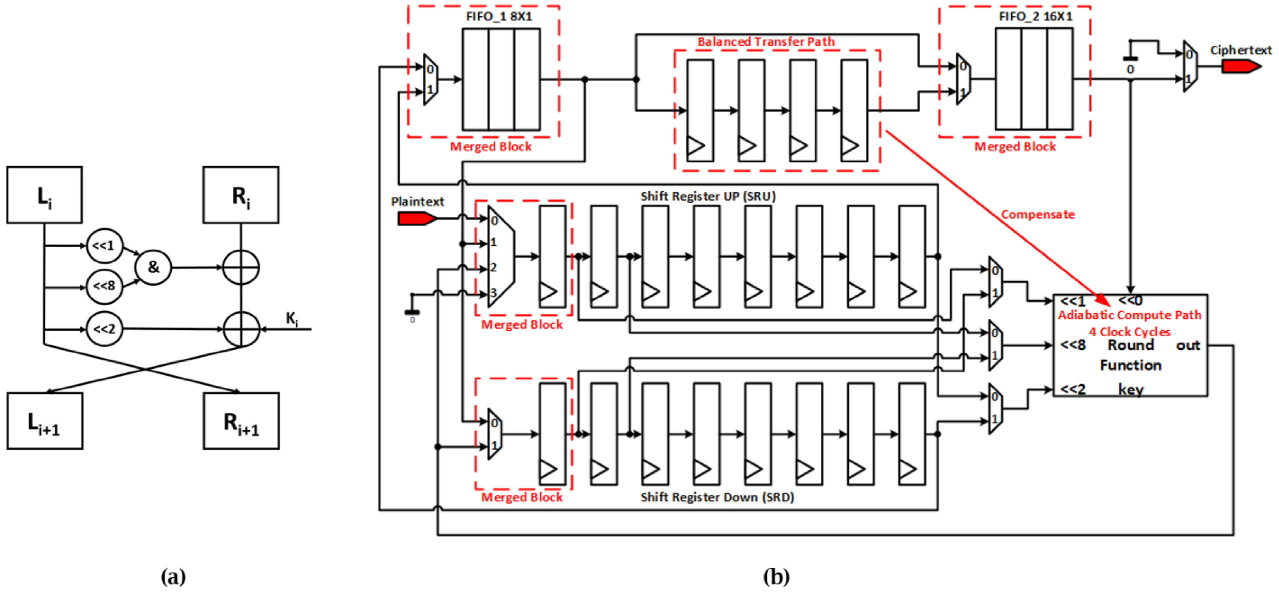


Figure 2. SIMON32/64 round function: (**a**) block-level diagram of the algorithm, (**b**) implementation of the round function in the adiabatic SIMON architecture, illustrating the merged blocks and balanced transfer paths.

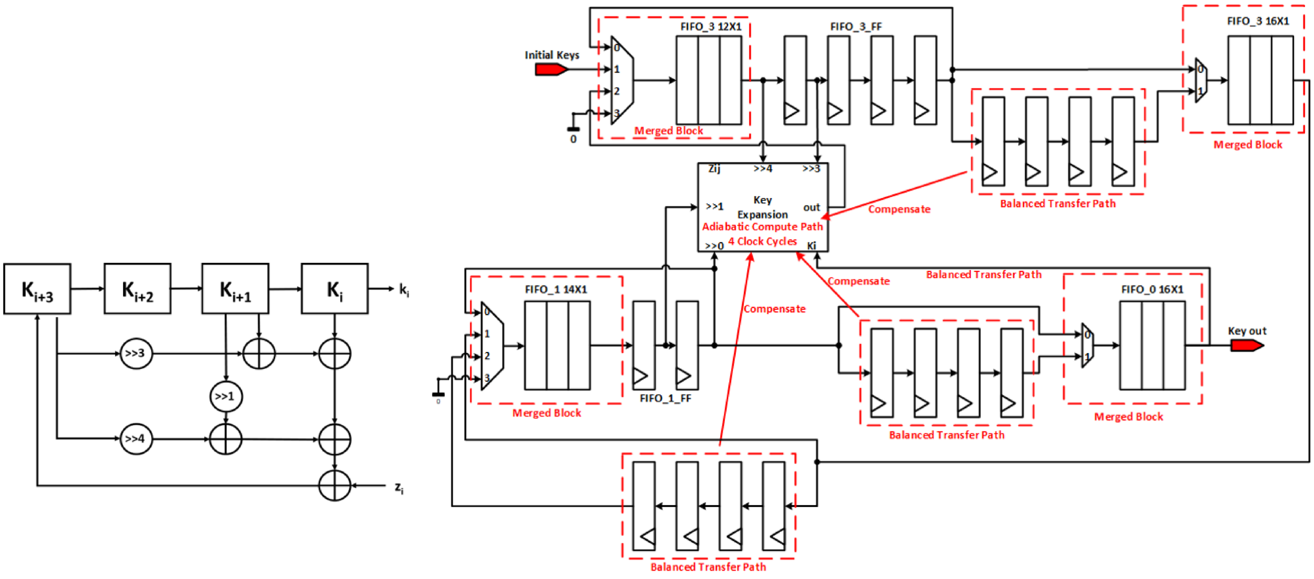
3.2.2. Key Expansion

An input key is used to generate a unique key for each round of encryption. Unlike the round function, the key expansion functions vary depending upon the width of the key word m, which can be 2, 3 or 4. Since the configuration used in this paper is SIMON 32/64, the key expansion algorithm for $m = 4$ is chosen, as illustrated in Figure 3a. The first four rounds use the four words of 64-bit key input and the key used from the fifth round, K_{i+4}, is generated by using the following function,

$$K_{i+4} = (K_i \oplus K_{i+1} \oplus (K_{i+3} >> 3)) \oplus K_{i+1} >> 1) \oplus (K_{i+3} >> 4) \oplus z_i, \tag{3}$$

where $1 <= i <= 28$ and z_i is referred to as the round constant that is used to eliminate slide properties and circular shift symmetries [2].

A key feature of SIMON algorithm is that there is a scope for serialization at every level, unlike *s*-box based algorithms. Depending upon the area constraint and throughput requirement of an application, SIMON algorithm can have a bit-level, round-level or encryption-level parallelism. Since the primary objective of this work is to design and analyze the side-channel resistance of SIMON hardware with minimal area and power constraints, the lowest level of parallelism, i.e., the bit-serial implementation is adopted.



(a)

(b)

Figure 3. SIMON32/64 key expansion: (**a**) block-level diagram of the algorithm, (**b**) implementation of the key expansion in the adiabatic SIMON architecture, illustrating the merged blocks and balanced transfer paths.

3.3. Correlation Power Analysis (CPA) Side-Channel Attack

CPA attacks exploit the statistical theory of Pearson correlation between a chosen hypothetical power model and the actual current consumption for various random plaintexts, to reveal the secret key. Let $h(n,k)$ be the hypothetical power model matrix with $n = 1,2,\ldots,N$, where N is the overall number of random plaintexts and $k = 1,2,\ldots,K$, where K is the overall number of key hypotheses for a portion of the input key. Let $i(n,t)$ be the measured current trace samples, with $t = 1,2,\ldots,T$, where T is the length of the trace. The correlation coefficient $r(k,t)$ is given as,

$$r(k,t) = \frac{\sum_{n=1}^{N}(h_{n,k} - \overline{h_k}).(i_{n,t} - \overline{i_t})}{\sum_{n=1}^{N}(h_{n,k} - \overline{h_k})^2.(i_{n,t} - \overline{i_t})^2}, \quad (4)$$

where $\overline{h_k}$ and $\overline{i_t}$ refer to the average of columns in, respectively, $h_{n,k}$ and $i_{n,t}$. The correct key hypotheses is the row value k, for which the correlation coefficient $r(k,t)$ is maximum. This algorithm is repeated for several key hypotheses until all of the key bits are recovered.

The resistance of an encryption cipher against CPA attack is determined by measurements-to-disclosure (MTD) [36]. MTD is the number of current traces measured at the crossover point between the correlation coefficient of the correct key and the maximum correlation coefficient of all of the incorrect key hypotheses. Higher MTD implies a greater resistance to the attack.

4. Proposed Methodology

The hardware implementation of the adiabatic SIMON architecture is described in Section 4.1. The algorithm used to perform the CPA side-channel attack on the adiabatic SIMON, including the proposed charge-based sampling, is explained in Section 4.2. The effect of increase in the load capacitance of the intermediate target signal on CPA resistance is discussed in Section 4.3.

4.1. Ultra-Low Power Adiabatic SIMON Architecture

The bit-serial static CMOS based SIMON consists of compute and transfer paths in the round function and key expansion modules [37]. In the round function, a compute path is comprised of logical operations that compute each bit of the left word of a round operation and a transfer path consists of logic that shifts bits from the left word of a round operation to the right word of the successive round operation. The ping-pong shift registers, shift register up (SRU) and shift register down (SRD), are used to store the upper half left block output L_{i+1} and to perform the circular left shift operations, alternating their roles in each round [37]. Adapting this static CMOS based architecture for adiabatic operation requires several innovations to ensure timing synchronization [21]. These innovations, illustrated in Figure 2b (adiabatic round function) and Figure 3b (adiabatic key expansion), are described below.

4.1.1. Merged Blocks

Due to inherent pipelining in adiabatic logic, each multiplexer (designed as a single complex gate) in the adiabatic implementation adds an additional clock phase. To compensate for this, multiplexers are merged with the following FIFO blocks [21], referred to as merged block in Figures 2b and 3b. For example, consider the 2-bit multiplexer driving the $FIFO\_1$, as shown in Figure 4. The first flip-flop (FF) in the FIFO is a chain of 4 buffers with the respective power-clock signals, as shown in Figure 4a. Since the multiplexer adds an additional clock (PC4) phase delay, the input of the $FIFO\_1$ cannot be updated in every cycle, thus affecting the left shift operation. Therefore, the multiplexer is merged with the first FF, as shown in Figure 4b to ensure that the bit-wise operation is consecutive. In this case, the merged block functions as a multiplexing flip-flop.

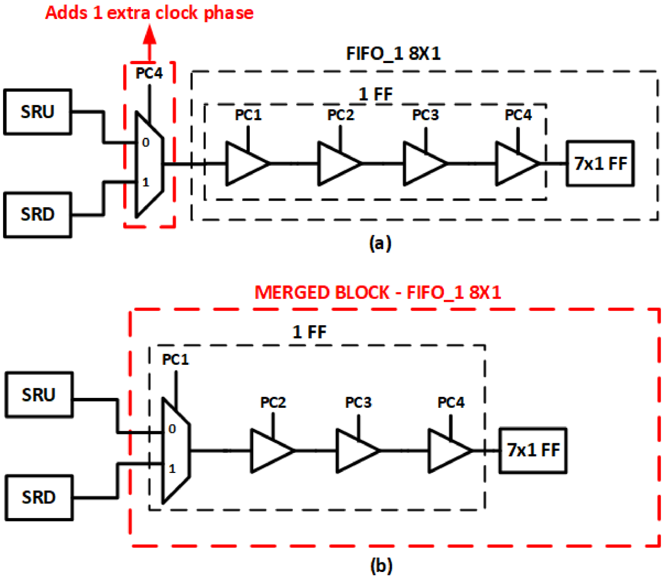


Figure 4. Example of a merged block in the round function: (**a**) multiplexer and $FIFO\_1$ 8 × 1 before merging, (**b**) multiplexer and $FIFO\_1$ 8 × 1 after merging.

4.1.2. Balanced Transfer Paths

In the conventional static CMOS based bit-serial SIMON [37], four additional look-up table registers (LUT_FF) are used to store the output of the key expansion in the first four cycles, so that the four MSBs in the input $FIFO$ can be used for circular right shift operation at the same time. Starting from the fifth cycle, the output is stored back in the $FIFO$. Since adiabatic circuits are inherently pipelined, these four cycles of pipelining are integrated in the combinational logic within the key expansion block. The logic depth of this compute path is chosen according to the maximum number of bits to be shifted, which in this case is 4, thus eliminating the use of the LUT_FF. As a result, each computation takes four additional cycles and therefore the compute and transfer paths are not synchronized. For example, 20 cycles are consumed to compute a new word in the key expansion, whereas only 16 cycles are used to transfer the bits to the next word. In order to bridge this gap, four additional registers are added to balance each transfer path in both round function and key expansion modules [21]. These additional registers are referred to as balanced transfer paths, as shown in Figures 2b and 3b. Note that due to the multi-phase operation of the adiabatic logic where each gate consumes 90° of the power-clock signal, four buffers (see Figure 1a for a single buffer) are cascaded to realize the function of a flip-flop for data synchronization.

4.2. Mounting CPA Attack on Adiabatic SIMON

4.2.1. Power Model

The Hamming distance (HD) based power model [18,38] is used for the adiabatic SIMON core, as illustrated in Figure 5. In this figure, the output voltage simulations of an ECRL buffer with transitions $0 \rightarrow 1 \rightarrow 1 \rightarrow 0 \rightarrow 0$ and the corresponding power supply current are depicted. Note that the output voltage is discharged during the *recovery* phase irrespective of the input since the power-clock signal falls. Unlike static CMOS, the output transition occurs during the $evaluate$ stage of consecutive clock cycles. As indicated, whenever there is a change in the output voltage (i.e., $0 \rightarrow 1$ or $1 \rightarrow 0$), the charging current increases and $HD = 1$. However, when the output remains the same ($0 \rightarrow 0$ or $1 \rightarrow 1$), $HD = 0$ and the current decreases. Thus, the HD based power model is suitable for mounting a CPA attack on an adiabatic SIMON implementation.

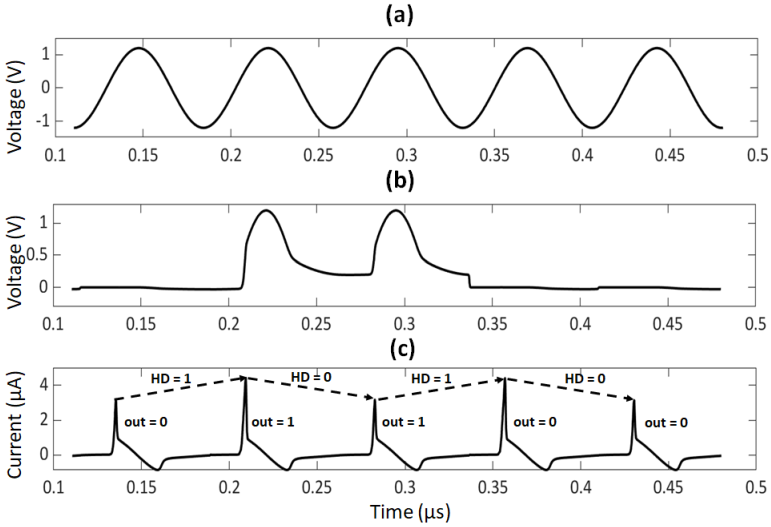


Figure 5. Use of Hamming distance as the power model for adiabatic ECRL circuits: (**a**) power-clock signal, (**b**) output voltage of the ECRL buffer, (**c**) current drawn from the supply by the buffer for output transitions $0 \rightarrow 1 \rightarrow 1 \rightarrow 0 \rightarrow 0$.

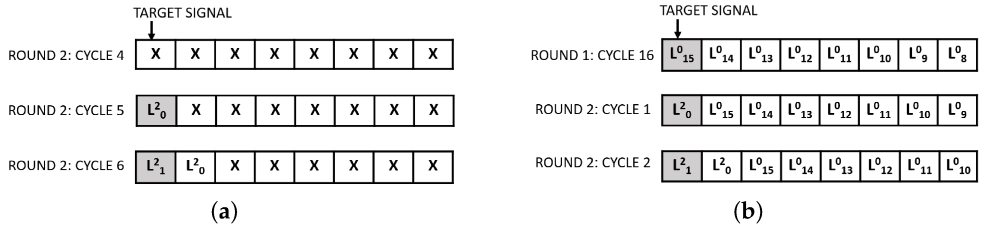
4.2.2. Intermediate Signal for Attack

An intermediate signal should be chosen for the CPA attack where the signal is a function of a non-constant data value and a portion of the key [16]. An immediate choice in SIMON algorithm is the output of a round function since the output of each round operation depends both on the key K_i, and the computed output of the previous round for each random plaintext input, as expressed by (1). The output of the first round operation is a function of the first round key and the known plaintext, thus exhibiting a linear dependency with the key bits. For the attack to be more efficient, the intermediate result should have a non-linear dependency with the key and the key bits should get *diffused* with the state [18]. Therefore, output of the second round operation is chosen as the target intermediate result.

For the proposed adiabatic SIMON implementation, output of the second round operation is stored in shift register SRU starting from the fifth cycle because of the four additional cycles added by the balanced transfer path, as shown in Figure 6b. Consequently, the HD model is constructed starting from L_0^2 and L_1^2 and is given by,

$$HD(L_0^2, L_1^2) = fn(K_8^1, K_{14}^1, K_{15}^1, K_0^2, K_9^1, K_0^1, K_1^2), \tag{5}$$

where, L_0^2 and L_1^2 are the first and second bit of the second round operation output. From (5), it can be seen that the HD is a function of seven bits of the 64-bit input key, $K_8^1, K_{14}^1, K_{15}^1, K_0^2, K_9^1, K_0^1, K_1^2$. Using this model, the matrix $HD(p,k)$ is constructed where $1 <= p <= P$ for P different random plaintexts, and $1 <= k <= 128$ for the 128 hypotheses of the seven key bits in (5). This process is repeated for consecutive cycles until the entire sample space of the 64 key bits is covered, as listed in Table 1. The table is divided into three sub-sections listing the power model for each successive round starting from the second round until all of the key bits are recovered. The total number of hypothesis for the adiabatic SIMON32/64, as seen from the table, is 324.



ROUND 2: CYCLE 4	X	X	X	X	X	X	X	X
ROUND 2: CYCLE 5	L^2_0	X	X	X	X	X	X	X
ROUND 2: CYCLE 6	L^2_1	L^2_0	X	X	X	X	X	X

ROUND 1: CYCLE 16	L^0_{15}	L^0_{14}	L^0_{13}	L^0_{12}	L^0_{11}	L^0_{10}	L^0_9	L^0_8
ROUND 2: CYCLE 1	L^2_0	L^0_{15}	L^0_{14}	L^0_{13}	L^0_{12}	L^0_{11}	L^0_{10}	L^0_9
ROUND 2: CYCLE 2	L^2_1	L^2_0	L^0_{15}	L^0_{14}	L^0_{13}	L^0_{12}	L^0_{11}	L^0_{10}

Figure 6. Contents of the 8-bit SRU loading the target signal at three cycles starting from (**a**) the fourth cycle of second round for the proposed adiabatic SIMON, (**b**) the last cycle of first round for the static CMOS based SIMON.

Alternatively, for the static CMOS based SIMON32/64 implementation, the HD power model can be constructed starting from the sixteenth bit of the plaintext (L_{15}^0), as depicted by Figure 6a. The contents of the shift register SRU at three consecutive cycles starting from the last cycle of first round and the first cycle of the second round are shown in the figure. From (1), the HD of L_{15}^0 and L_0^2 is given by,

$$HD(L_{15}^0, L_0^2) = fn(K_8^1, K_{14}^1, K_{15}^1, K_0^2), \tag{6}$$

where L_{15}^0 is the sixteenth bit of the plaintext and L_0^2 is the first bit of the second round output. The power model matrix is constructed for 16 key hypotheses in order to find the 4 bits $K_8^1, K_{14}^1, K_{15}^1, K_0^2$. Similarly, $HD(p,k)$ is constructed for each key hypotheses, as listed in Table 1, in order to find the correct 64 bits of the secret input key. The total number of key hypothesis for the static CMOS based SIMON32/64 is reduced by approximately half (from 324 to 156) because of the change in the construction of the power model, as listed in Table 1. Note that the correlation model for both implementations begins with different number of key bits (4 bits and 7 bits) due to the differences in their hardware implementations (different synchronization characteristics in adiabatic and static CMOS [21]).

Table 1. Complexity of the CPA attack for static CMOS based SIMON32/64 and adiabatic SIMON32/64 implementations: power model and number of key hypotheses required. L_n^m refers to the n^{th} bit of the left block output of the m^{th} round and K_n^m refers to the n^{th} bit of the m^{th} word of the input 64-bit key.

	Static SIMON			**Adiabatic SIMON**		
Hamming Distance between	**Bits of the Input Key**	**Number of Key Bits**	**Number of Key Hypotheses**	**Bits of the Input Key**	**Number of Key Bits**	**Number of Key Hypotheses**
L_{15}^0 and L_0^2	K_8^1, K_{14}^1, K_{15}^1,K_0^2	4	16			
L_0^2 and L_1^2	K_9^1, K_0^1, K_1^2	3	8	K_8^1, K_{14}^1, K_{15}^1,K_0^2,K_9^1, K_0^1, K_1^2	7	128
L_1^2 and L_2^2	K_{10}^1, K_1^1, K_2^2	3	8	K_{10}^1, K_1^1, K_2^2	3	8
L_2^2 and L_3^2	K_{11}^1, K_2^1, K_3^2	3	8	K_{11}^1, K_2^1, K_3^2	3	8
L_3^2 and L_4^2	K_{12}^1, K_3^1, K_4^2	3	8	K_{12}^1, K_3^1, K_4^2	3	8
L_4^2 and L_5^2	K_{13}^1, K_4^1, K_5^2	3	8	K_{13}^1, K_4^1, K_5^2	3	8
L_5^2 and L_6^2	K_5^1, K_6^2	2	4	K_5^1, K_6^2	2	4
L_6^2 and L_7^2	K_6^1, K_7^2	2	4	K_6^1, K_7^2	2	4
L_7^2 and L_8^2	K_7^1, K_8^2	2	4	K_7^1, K_8^2	2	4
L_{15}^1 and L_0^3	K_{14}^2, K_{15}^2,K_0^3	3	8			
L_0^3 and L_1^3	K_9^2, K_1^3	2	4	K_{14}^2, K_{15}^2,K_0^3,K_9^2, K_1^3	5	32
L_1^3 and L_2^3	K_{10}^2, K_2^3	2	4	K_{10}^2, K_2^3	2	4
L_2^3 and L_3^3	K_{11}^2, K_3^3	2	4	K_{11}^2, K_3^3	2	4
L_3^3 and L_4^3	K_{12}^2, K_4^3	2	4	K_{12}^2, K_4^3	2	4
L_4^3 and L_5^3	K_{13}^2, K_5^3	2	4	K_{13}^2, K_5^3	2	4
L_{15}^2 and L_0^4	K_8^3, K_{14}^3, K_{15}^3,K_0^4	4	16			
L_0^4 and L_1^4	K_9^3, K_1^4	2	4	K_8^3, K_{14}^3, K_{15}^3,K_0^4,K_9^3, K_1^4	6	64
L_1^4 and L_2^4	K_{10}^3, K_2^4	2	4	K_{10}^3, K_2^4	2	4
L_2^4 and L_3^4	K_{11}^3, K_3^4	2	4	K_{11}^3, K_3^4	2	4
L_3^4 and L_4^4	K_{12}^3, K_4^4	2	4	K_{12}^3, K_4^4	2	4
L_4^4 and L_5^4	K_{13}^3, K_5^4	2	4	K_{13}^3, K_5^4	2	4
L_5^4 and L_6^4	K_6^4	1	2	K_6^4	1	2
L_6^4 and L_7^4	K_6^3, K_7^4	2	4	K_6^3, K_7^4	2	4
L_7^4 and L_8^4	K_7^3, K_8^4	2	4	K_7^3, K_8^4	2	4
L_8^4 and L_9^4	K_9^4	1	2	K_9^4	1	2
L_9^4 and L_{10}^4	K_{10}^4	1	2	K_{10}^4	1	2
L_{10}^4 and L_{11}^4	K_{11}^4	1	2	K_{11}^4	1	2
L_{11}^4 and L_{12}^4	K_{12}^4	1	2	K_{12}^4	1	2
L_{12}^4 and L_{13}^4	K_{13}^4	1	2	K_{13}^4	1	2
L_{13}^4 and L_{14}^4	K_{14}^4	1	2	K_{14}^4	1	2
L_{14}^4 and L_{15}^4	K_{15}^4	1	2	K_{15}^4	1	2
TOTAL		64	156		64	324

4.2.3. Proposed Charge Based Sampling

A charge-based method is proposed in this work to significantly reduce the number of samples in adiabatic circuits. Specifically, the traces are measured as an *integral* of current waveform (rather than taking discrete samples) over each *evaluate* stage of the power-clock signal, as illustrated in Figure 7. The shaded portion in this figure indicates the charge obtained in one *evaluate* phase of a clock cycle. The charge traces acquired for the first plaintext can be expressed as,

$$Q(1,n) = \int_{[(n-1)T]}^{[(n-1)T+\frac{T}{4}]} I(t)dt, \tag{7}$$

where T is the time period of the power-clock signal and $1 <= n <= N$ for N number of samples obtained. The lower and upper integration limits of the integral are determined based on the start and end times of the *evaluate* phase, which are known by the attacker via the power-clock signal. Using this approach, the overall number of required samples to be collected is reduced to only 704 (since one charge sample is measured in each clock cycle and the total number of cycles for encryption is 704). In conventional practice, 140.8 K samples would be collected, assuming that an attacker measures approximately 200 current samples in each cycle [19]. Thus, the proposed approach reduces the sample size by two orders of magnitude. Note that this approach is not feasible in conventional static CMOS based operation since the current is drawn from the supply voltage based on the timing characteristics of the internal target signal, which is typically not accessible to the attacker.

The execution times of the attack was measured for both the traditional current sample measurement and the proposed charge based technique for different number of plaintexts. Both approaches were allocated the same set of computation resources. It was observed that the time to mount the attack was 1.5× faster with the proposed approach for up to 8000 plaintexts. This difference in execution time increased to 2× for 10,000 to 14,000 plaintexts. The speedup in the execution times of a CPA attack with the proposed charge based measurement enables a more efficient attack, particularly for protected ciphers, where an attacker would require a larger number of plaintexts to retrieve the key bits.

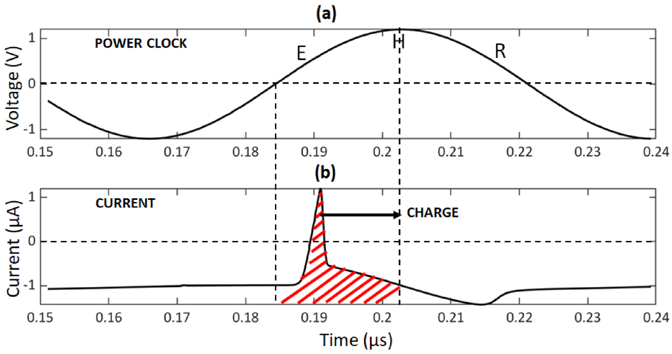


Figure 7. Proposed power sampling method in adiabatic SIMON core: (**a**) power-clock signal, (**b**) charge analysis with respect to the *evaluate* phase of the power-clock signal.

4.3. Effect of Load Capacitance on CPA

For an adiabatic circuit, the overall current consumption during CPA is approximated by,

$$I_{total} \approx \frac{C_{target} V_{dd}}{t_r} + \frac{C_{rem} V_{dd}}{t_r}, \tag{8}$$

where C_{target} is the capacitance of the target CPA signal including the interconnect capacitance, the gate capacitance of the load gate, and intrinsic capacitance. C_{rem} refers to the capacitance of other nodes in the circuit and t_r is the transition time of the power-clock signal. According to (8), an increase in C_{target} amplifies the required current drawn to charge the target signal capacitance, isolating it from current consumed to charge all of the other nodes. This behavior can be observed in Figure 8, where an increase in the width of the load gate increases the signal current without significantly affecting the noise current. The noise current is relatively independent of this change in the C_{target} in adiabatic operation since the load transistors are only n-type (due to the absence of a complementary pull-up network in ECRL circuits). Thus, increasing the width of the nMOS load transistor does not change the current consumed by the load gate. The measured current I_{total} is increased due to an increase in target I_{signal}. Based on (4), this increase contributes to a higher correlation coefficient of the correct key when compared to the incorrect coefficients. This improved correlation of the correct key results in a lower MTD and therefore, lesser resistance to CPA attack. An adversary typically has access to the interface ports of a system. Therefore, if the output ciphertext is chosen as the target signal, the load capacitance at the port can be modified by the attacker and the effect discussed here can cause the encryption core to be more vulnerable to the CPA attack (see results in Section 5.2).

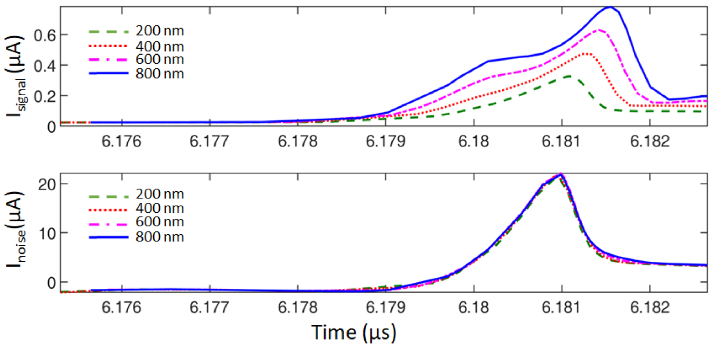


Figure 8. Signal and noise currents drawn from the power supply for different gate widths of the target signal load in adiabatic SIMON core.

5. Results

Both the static CMOS and adiabatic ECRL SIMON core were implemented using a commercial 65 nm CMOS technology. Both circuits operate at the RFID frequency of 13.56 MHz. The charge traces are obtained based on the simulated results using high performance Spectre APS [39]. Power models are constructed and correlated with the charge traces in MATLAB to establish a CPA attack [40]. The correct operation of both implementations is also demonstrated via various test vectors for plaintext and initial keys. Performance characteristics and the results of the proposed CPA attack are described, respectively, in Sections 5.1 and 5.2.

5.1. Performance Characteristics

The post-layout performance characteristics of the bit-serial static CMOS SIMON and the proposed adiabatic ECRL SIMON are listed in Table 2. Average power, latency, energy, throughput, efficiency and area are listed for both static and adiabatic implementations. According to Table 2, the encryption efficiency of the adiabatic core (in Kb/sec/µW) is enhanced by approximately 5×. The average power dissipated by the adiabatic SIMON is approximately 6× less than the static CMOS counterpart. These significant improvements in power and efficiency are achieved at the expense of 1.2× reduction in throughput and approximately 2% increase in overall area. The increase in the latency is due to the balanced transfer path in the proposed SIMON implementation, which takes additional 4 cycles in each round of encryption.

Table 2. Post-layout simulation results of the bit-serialized SIMON32/64 cipher implemented in conventional and proposed adiabatic approaches.

Architecture	**Conventional**	**Proposed**	**Change (%)**
Logic	**Static CMOS**	**Adiabatic ECRL**	
Average power (µW)	22.76	3.84	83.13 ↓
Latency (Clock Cycles)	576	704	22.22 ↑
Energy (pJ)	967	199	79.42 ↓
Throughput (Kbps)	753	616	18.19 ↓
Efficiency (Kb/sec/µW)	33	160	384.8 ↑
Area (µm^2)	4071	4161	2.21 ↑

5.2. Resistance to CPA Attack

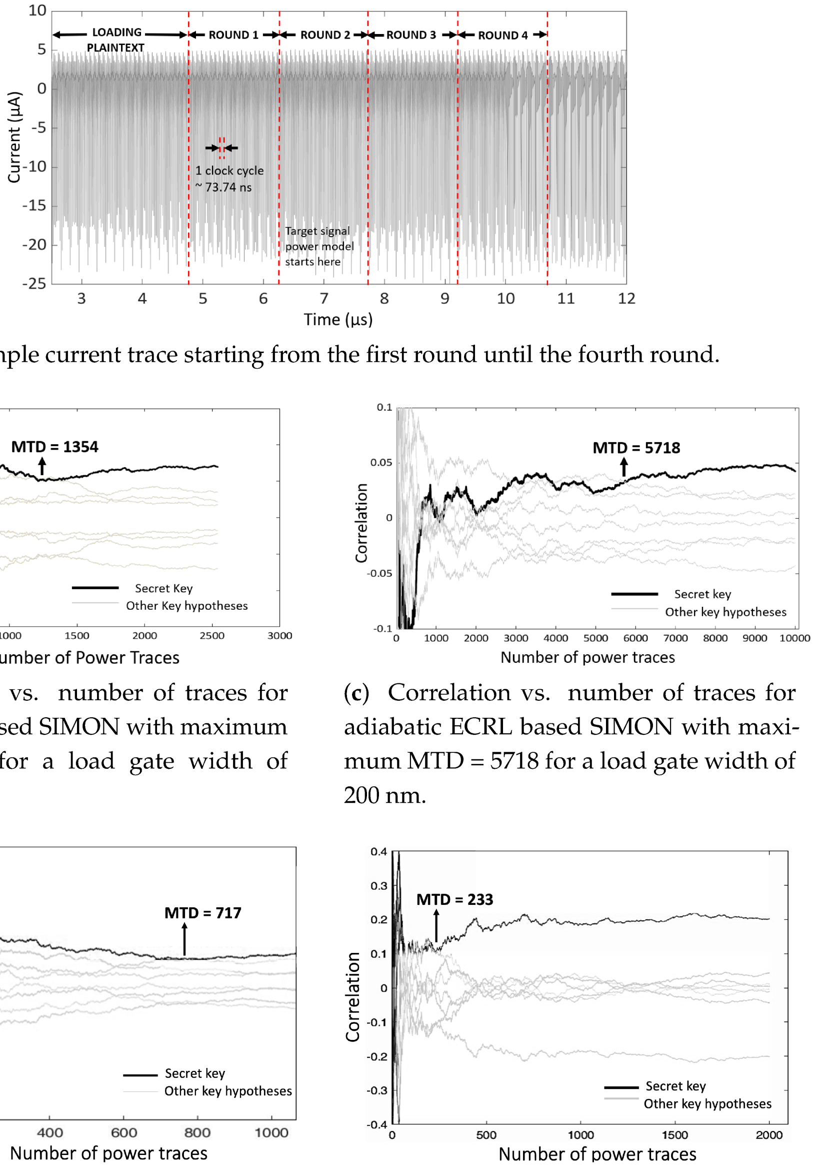
In order to establish a CPA attack, the methodology described in Section 4.2 was utilized. Current (for static CMOS) and charge (for adiabatic) traces were obtained for a large number of encryption scenarios with randomly generated input plaintexts with a key value `16'h 1918 1110 0908 0100`. A sample trace of the overall current consumption starting from loading the plaintext until the fourth round is depicted in Figure 9a.

The CPA algorithm was built in MATLAB [40]. The Hamming distance power model was constructed based on Table 1, for each key hypothesis. All of the key bits were successfully retrieved for both implementations. The correlation coefficient vs. number of current traces for static CMOS based SIMON for the key bits with the maximum MTD (that were the hardest to retrieve), K_8^3, K_{14}^3, K_{15}^3,K_0^4 is illustrated in Figure 9b. The black curve shows the correlation coefficient for the correct key hypotheses `4'b 1000` and the grey curves are the correlation for the other key guesses. As observed from this figure, the highest MTD to retrieve all of the 64 bits of the key is determined as 1354 power traces. Alternatively, for adiabatic ECRL based SIMON, the maximum MTD is 5718 power traces for the key bits K_{11}^1, K_2^1, K_3^2, as depicted in Figure 9c. Note that these plots are symmetrical around the X-axis because complimentary bits in the Hamming distance have equal correlations with opposite signs. The MTD to recover the correct key bits for every key hypothesis for both static CMOS and adiabatic implementations of SIMON is listed in Table 3 and the maximum MTD to recover all the 64 key bits is highlighted in bold. Thus, the SIMON block cipher implemented using adiabatic logic is approximately 4× less vulnerable to power side-channel attack as compared to the conventional static CMOS counterpart.

As a comparison, in [20], a static CMOS based SIMON128/128 has been implemented for various levels of serialization. The MTD of the bit-serial implementation was reported to be 1300, which is similar to the MTD of static CMOS based SIMON in this work. Therefore, the proposed adiabatic implementation is also 4× less susceptible to CPA when compared to [20]. Note however that these results demonstrate the inherent resistance of adiabatic SIMON to CPA attack since the MTD is still relatively low. Furthermore, in this work, the results are obtained for a plaintext-based attack model (see Table 1) and these results can vary depending upon the particular attack model that is used.

Finally, the effect of parasitic capacitance at the target signal node on CPA is quantified. The correlation vs. number of traces for static CMOS based SIMON and adiabatic SIMON for an increased target signal load size is depicted, respectively, in Figure 9d and e. These plots show that for a load gate width of 1200 nm, the MTD of a static CMOS based SIMON is 717, whereas for an adiabatic SIMON, the MTD is only 233 for a load gate width of 800 nm. The dependence of MTD on the size of the load gate is shown in Figure 10 for both static CMOS and adiabatic implementations. According to these results, for static CMOS implementation, if the size of the load transistor is increased by 6× (thereby increasing the capacitance seen by the target signal), MTD is reduced by a factor of 2. Alternatively, for adiabatic implementation, the same reduction in MTD is observed when the size of the load transistor is increased by only 2×. Thus, the CPA attack on adiabatic SIMON is more sensitive to the changes in the capacitance seen by the target signal.

The primary reason for this difference is related to the method of analysis of the current traces. Since the integral of current is used for adiabatic SIMON CPA attack, as explained in Section 4.2.3, the effect of increased load amplifies the charge at a higher rate than the peak current samples used in static CMOS based SIMON. This behavior is depicted in Figure 11 where the dependence of charge and current on the size of load is shown. When the width of the load gate is increased by 4×, the charge consumed by the adiabatic ECRL is doubled whereas the peak current consumed by the static CMOS logic increases by approximately 1.2×. Thus, the correlation is higher for ECRL based SIMON for the same increase in load size, thereby reducing the MTD more.



(**a**) Sample current trace starting from the first round until the fourth round.

(**b**) Correlation vs. number of traces for static CMOS based SIMON with maximum MTD = 1354 for a load gate width of 200 nm.

(**c**) Correlation vs. number of traces for adiabatic ECRL based SIMON with maximum MTD = 5718 for a load gate width of 200 nm.

(**d**) Correlation vs. number of traces for static CMOS based SIMON with maximum MTD = 717 for an increased load gate width of 1200 nm.

(**e**) Correlation vs. number of traces for adiabatic ECRL based SIMON with maximum MTD = 233 for an increased load gate width of 800 nm.

Figure 9. Correlation power analysis (CPA) attack results.

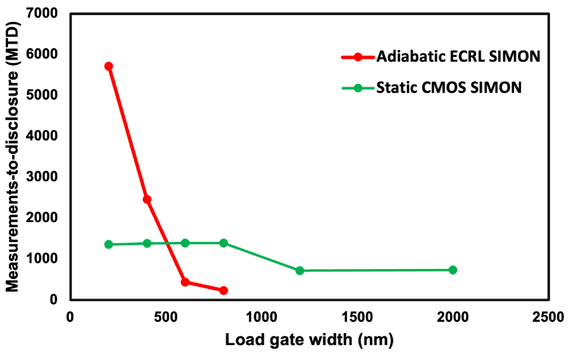


Figure 10. CPA target signal load size vs. MTD for static CMOS based SIMON core and adiabatic SIMON core.

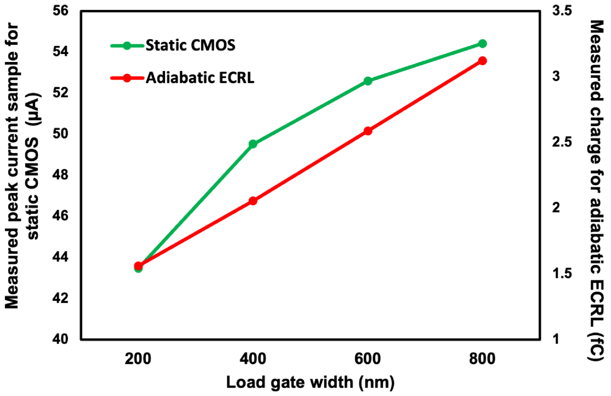


Figure 11. Dependence of peak current and charge drawn by the driving gate on target load capacitance for static CMOS and adiabatic ECRL.

The capacitance at the prospective target signal can be increased by an attacker at the design or foundry level (e.g., as a hardware Trojan) to make CPA attack easier. This capacitance can be increased via various methods that are relatively difficult to detect such as up-sizing the load gate driven by the target signal, increasing the target signal interconnect capacitance, increasing the fanout, or by inserting dummy capacitance at the target signal. Therefore, a reduced MTD by leveraging the dependence of current on this capacitance poses a serious concern, particularly when the output ciphertext is attacked by the adversary where it is easier to modify node capacitance.

Table 3. MTD for each key-bit partition for static CMOS based SIMON32/64 and adiabatic SIMON32/64 implementations where K_n^m refers to the n^{th} bit of the m^{th} word of the input 64-bit key.

Static SIMON		Adiabatic SIMON	
Key Bit Partitions	**MTD**	**Key Bit Partitions**	**MTD**
K_8^1, K_{14}^1, K_{15}^1,K_0^2	145		
K_9^1, K_0^1, K_1^2	114	K_8^1, K_{14}^1, K_{15}^1,K_0^2,K_9^1, K_0^1, K_1^2	720
K_{10}^1, K_1^1, K_2^2	290	K_{10}^1, K_1^1, K_2^2	268
K_{11}^1, K_2^1, K_3^2	409	K_{11}^1, K_2^1, K_3^2	**5718**
K_{12}^1, K_3^1, K_4^2	46	K_{12}^1, K_3^1, K_4^2	2052
K_{13}^1, K_4^1, K_5^2	139	K_{13}^1, K_4^1, K_5^2	1307
K_5^1, K_6^2	116	K_5^1, K_6^2	497
K_6^1, K_7^2	445	K_6^1, K_7^2	2749
K_7^1, K_8^2	55	K_7^1, K_8^2	113
K_{14}^2, K_{15}^2,K_0^3	102		
K_9^2, K_1^3	87	K_{14}^2, K_{15}^2,K_0^3,K_9^2, K_1^3	117
K_{10}^2, K_2^3	27	K_{10}^2, K_2^3	125
K_{11}^2, K_3^3	28	K_{11}^2, K_3^3	11
K_{12}^2, K_4^3	32	K_{12}^2, K_4^3	28
K_{13}^2, K_5^3	364	K_{13}^2, K_5^3	263

Table 3. *Cont.*

Static SIMON		Adiabatic SIMON	
Key Bit Partitions	**MTD**	**Key Bit Partitions**	**MTD**
K^3_8, K^3_{14}, K^3_{15},K^4_0	1354		
K^3_9, K^4_1	2	K^3_8, K^3_{14}, K^3_{15},K^4_0,K^3_9, K^4_1	1078
K^3_{10}, K^4_2	361	K^3_{10}, K^4_2	785
K^3_{11}, K^4_3	197	K^3_{11}, K^4_3	813
K^3_{12}, K^4_4	60	K^3_{12}, K^4_4	1189
K^3_{13}, K^4_5	26	K^3_{13}, K^4_5	267
K^4_6	16	K^4_6	63
K^3_6, K^4_7	27	K^3_6, K^4_7	27
K^3_7, K^4_8	206	K^3_7, K^4_8	2370
K^4_9	52	K^4_9	2
K^4_{10}	2	K^4_{10}	2
K^4_{11}	82	K^4_{11}	84
K^4_{12}	139	K^4_{12}	5454
K^4_{13}	17	K^4_{13}	11
K^4_{14}	95	K^4_{14}	41
K^4_{15}	17	K^4_{15}	172
MTD to recover all key bits	**1354**		**5718**

6. Conclusions

A correlation power analysis (CPA) attack was established on an adiabatic SIMON block cipher. A charge based sampling method was proposed to significantly reduce the attack complexity. It was demonstrated that adiabatic operation enhances encryption efficiency (bit/sec/W) by approximately 5× while also exhibiting approximately 4× higher CPA resistance as compared to static CMOS based SIMON implementation. Despite achieving higher CPA resistance, an unprotected adiabatic SIMON is still susceptible to CPA attacks since the MTD is not sufficiently high. The effect of increasing the target load capacitance on the side-channel resistance was also investigated. The results demonstrate that doubling the capacitance seen by the target signal in the adiabatic SIMON implementation can reduce the MTD by 5×.

Author Contributions: main text.

Funding: This research was supported in part by the National Science Foundation under grant numbers 1717306 and 1646318 and in part by Semiconductor Research Corporation under contract number 2017-TS-2767.

Institutional Review Board Statement: main text.

Informed Consent Statement: main text.

Data Availability Statement: main text.

Conflicts of Interest: main text.

References

1. Sivaraman, V.; Gharakheili, H.H.; Fernandes, C.; Clark, N.; Karliychuk, T. Smart IoT Devices in the Home: Security and Privacy Implications. *IEEE Technol. Soc. Mag.* **2018**, *37*, 71–79, doi:10.1109/MTS.2018.2826079.
2. Beaulieu, R.; Treatman-Clark, S.; Shors, D.; Weeks, B.; Smith, J.; Wingers, L. The SIMON and SPECK lightweight block ciphers. In Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA, 7–11 June 2015; pp. 1–6, doi:10.1145/2744769.2747946.

3. Wamser, M.S.; Sigl, G. Pushing The Limits Further: Sub-atomic AES. In *IFIP/IEEE International Conference on Very Large Scale Integration-System on a Chip*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 220–239.
4. Mathew, S.; Satpathy, S.; Suresh, V.; Anders, M.; Kaul, H.; Agarwal, A.; Hsu, S.; Chen, G.; Krishnamurthy, R. 340 mV–1.1 V, 289 Gbps/W, 2090-Gate NanoAES Hardware Accelerator With Area-Optimized Encrypt/Decrypt GF(2 4) 2 Polynomials in 22 nm Tri-Gate CMOS. *IEEE J. Solid-State Circuits* **2015**, *50*, 1048–1058.
5. Bogdanov, A.; Knudsen, L.R.; Leander, G.; Paar, C.; Poschmann, A.; Robshaw, M.J.; Seurin, Y.; Vikkelsoe, C. PRESENT: An Ultra-lightweight Block Cipher. In *International Workshop on Cryptographic Hardware and Embedded Systems*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 450–466.
6. Borghoff, J.; Canteaut, A.; Güneysu, T.; Kavun, E.B.; Knezevic, M.; Knudsen, L.R.; Leander, G.; Nikov, V.; Paar, C.; Rechberger, C.; et al. PRINCE—A Low-Latency Block Cipher for Pervasive Computing Applications. In *Advances in Cryptology–ASIACRYPT 2012*; Wang, X., Sako, K., Eds.; Springer: Berlin/Heidelberg, Germany, 2012.
7. Akishita, T.; Hiwatari, H. Very compact hardware implementations of the blockcipher CLEFIA. In *International Workshop on Selected Areas in Cryptography*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 278–292.
8. Aoki, K.; Ichikawa, T.; Kanda, M.; Matsui, M.; Moriai, S.; Nakajima, J.; Tokita, T. Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms—Design andAnalysis. In *Selected Areas in Cryptography*; Stinson, D.R., Tavares, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2001; pp. 39–56.
9. Beaulieu, R.; Shors, D.; Smith, J.; Treatman-Clark, S.; Weeks, B.; Wingers, L. The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404. 2013. Available online: https://eprint.iacr.org/2013/404 (accessed on).
10. ISO Security Services for RFID Air Interfaces. *Information Technology—Automatic Identification and Data Capture Techniques*; Standard ISO/IEC TR 29167-21:2018; International Organization for Standardization: Geneva, Switzerland, 2018. Available online: https://www.iso.org/standard/70388.html (accessed on 15 August 2019).
11. Gray-Fow, E. A Brief Peek Into the Fascinating World of Side Channel Attacks. Available online: https://medium.com/swlh/a-brief-peek-into-the-fascinating-world-of-side-channel-attacks-809f96eabea1 (accessed on 15 July 2019).
12. Kocher, P.; Jaffe, J.; Jun, B.; Rohatgi, P. Introduction to differential power analysis. *J. Cryptogr. Eng.* **2011**, *1*, 5–27.
13. Kocher, P.C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other systems. In *Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 1996; pp. 104–113.
14. Hutter, M.; Schmidt, J.M. The Temperature Side-Channel and Heating Fault Attacks. In Proceedings of the International Conference on Smart Card Research and Advanced Applications, Berlin, Germany, 27–29 November 2013.
15. Quisquater, J.J.; Samyde, D. ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards. In *International Conference on Research in Smart Cards: Smart Card Programming and Security*; Springer: Berlin/Heidelberg, Germany, 2001; pp. 200–210.
16. Mangard, S.; Oswald, E.; Popp, T. *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)*; Springer: Berlin/Heidelberg, Germany, 2007; ISBN 0387308571.
17. Kocher, P.C.; Jaffe, J.; Jun, B. Differential Power Analysis. In *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*; Springer: Berlin/Heidelberg, Germany, 1999; pp. 388–397.
18. Shanmugam, D.; Selvam, R.; Annadurai, S. Differential Power Analysis Attack on SIMON and LED Block Ciphers. In *Security, Privacy, and Applied Cryptography Engineering*; Chakraborty, R.S., Matyas, V., Schaumont, P., Eds.; Springer International Publishing: Cham, Switzerland, 2014; pp. 110–125.
19. Bhasin, S.; Graba, T.; Danger, J.; Najm, Z. A Look into SIMON from a Side-channel Perspective. In Proceedings of the 2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Arlington, VA, USA, 6–7 May 2014; pp. 56–59, doi:10.1109/HST.2014.6855568.
20. Singh, A.; Chawla, N.; Ko, J.H.; Kar, M.; Mukhopadhyay, S. Energy Efficient and Side-Channel Secure Cryptographic Hardware for IoT-Edge Nodes. *IEEE Internet Things J.* **2019**, *6*, 421–434, doi:10.1109/JIOT.2018.2861324.
21. Wan, T.; Salman, E. Ultra Low Power SIMON Core for Lightweight Encryption. In Proceedings of the 2018 IEEE International Symposium on Circuits and Systems (ISCAS), Florence, Italy, 27–30 May 2018; pp. 1–5, doi:10.1109/ISCAS.2018.8351163.
22. Teichmann, P. *Adiabatic Logic: Future Trend and System Level Perspective*; Springer: Berlin/Heidelberg, Germany, 2011.
23. Maheshwari, S.; Bartlett, V.A.; Kale, I. A VHDL-based Modelling Approach for Rapid Functional Simulation and Verification of Adiabatic Circuits. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.* **2020**, doi:10.1109/TCAD.2020.3022334.
24. Kumar, S.D.; Thapliyal, H.; Mohammad, A.; Singh, V.; Perumalla, K.S. Energy-Efficient and Secure S-Box Circuit Using Symmetric Pass Gate Adiabatic Logic. In Proceedings of the 2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Pittsburgh, PA, USA, 11–13 July 2016; pp. 308–313, doi:10.1109/ISVLSI.2016.45.
25. Dinesh Kumar, S.; Thapliyal, H.; Mohammad, A. FinSAL: FinFET-Based Secure Adiabatic Logic for Energy-Efficient and DPA Resistant IoT Devices. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.* **2018**, *37*, 110–122.
26. Raghav, H.S.; Kale, I. A Balanced Power Analysis Attack Resilient Adiabatic Logic Using Single Charge Sharing Transistor. *Integration* **2019**, *69*, 147–160, doi:10.1016/j.vlsi.2018.07.010.
27. Avital, M.; Dagan, H.; Levi, I.; Keren, O.; Fish, A. DPA-Secured Quasi-Adiabatic Logic (SQAL) for Low-Power Passive RFID Tags Employing S-Boxes. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2015**, *62*, 149–156, doi:10.1109/TCSI.2014.2359720.

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*, 496–503, doi:10.1016/j.mejo.2013.04.003.
29. Kumar, S.; Thapliyal, H.; Mohammad, A.; Perumalla, K. Design Exploration of a Symmetric Pass Gate Adiabatic Logic for Energy-Efficient and Secure Hardware. *Integr. VLSI J.* **2016**, *58*, doi:10.1016/j.vlsi.2016.08.007.
30. Thapliyal, H.; Varun, T.S.S.; Kumar, S.D. Adiabatic Computing Based Low-Power and DPA-Resistant Lightweight Cryptography for IoT Devices. In Proceedings of the 2017 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Bochum, Germany, 3–5 July 2017; pp. 621–626, doi:10.1109/ISVLSI.2017.115.
31. Kumar, S.D.; Thapliyal, H.; Mohammad, A.; Singh, V.; Perumalla, K.S. Energy-Efficient and Secure S-Box Circuit Using Symmetric Pass Gate Adiabatic Logic. In Proceedings of the 2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Pittsburgh, PA, USA, 11–13 July 2016; pp. 308–313, doi:10.1109/ISVLSI.2016.45.
32. Fadaeinia, B.; Moradi, A. 3-Phase Adiabatic Logic and its Sound SCA Evaluation. *IEEE Trans. Emerg. Top. Comput.* **2020**, doi:10.1109/TETC.2020.2976711.
33. Wan, T.; Karimi, Y.; Stanaćević, M.; Salman, E. Perspective Paper—Can AC Computing Be an Alternative for Wirelessly Powered IoT Devices? *IEEE Embed. Syst. Lett.* **2017**, *9*, 13–16.
34. Moon, Y.; Jeong, D.K. An Efficient Charge Recovery Logic Circuit. *IEEE J. Solid-State Circuits* **1996**, *31*, 514–522, doi:10.1109/4.499727.
35. Khatir, M.; Moradi, A. Secure Adiabatic Logic: A Low-Energy DPA-Resistant Logic Style. 2008. moradi@crypto.rub.de 13955 Received 17 Mar 2008, Last Revised 17 Mar 2008. Available online: https://eprint.iacr.org/2008/123.pdf (accessed on).
36. Hwang, D.D.; Tiri, K.; Hodjat, A.; Lai, B.C.; Yang, S.; Schaumont, P.; Verbauwhede, I. AES-based Security Coprocessor IC in 0.18-μm CMOS with Resistance to Differential Power Analysis Side-channel Attacks. *IEEE J. Solid-State Circuits* **2006**, *41*, 781–790, doi:10.1109/JSSC.2006.870913.
37. Gulcan, E.; Aysu, A.; Schaumont, P. A Flexible and Compact Hardware Architecture for the SIMON Block Cipher. In *Lightweight Cryptography for Security and Privacy*; Eisenbarth, T., Öztürk, E., Eds.; Springer: Cham, Switzerland, 2015; pp. 34–50.
38. Brier, E.; Clavier, C.; Olivier, F. Correlation Power Analysis with a Leakage Model. In *Cryptographic Hardware and Embedded Systems-CHES 2004*; Joye, M., Quisquater, J.J., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 16–29.
39. Cadence Spectre Simulation Platform. Available online: https://www.cadence.com/en_US/home/tools/custom-ic-analog-rf-design/circuit-simulation/spectre-simulation-platform.html (accessed on 27 October 2020).
40. MATLAB. *9.9.0.1467703 (R2020b)*; The MathWorks Inc.: Natick, MA, USA, 2020; Available online: https://www.mathworks.com/products/matlab.html (accessed on 27 October 2020).