AC Computing Methodology for RF Powered IoT Security

Tutu Wan, Emre Salman and Milutin Stanacevic
Department of Electrical and Computer Engineering
Stony Brook University (SUNY), Stony Brook, NY 11794–2350
Email: tutu.wan@stonybrook.edu

***Abstract*—Hardware security is a critical challenge for various emerging applications in the massive deployment of IoT devices due to lack of computing resources. In this paper, an energy-efficient AC computing methodology is proposed to facilitate lightweight encryption in RF powered devices such as RFIDs. Contrary to conventional methods that rely on rectification and regulation, the wirelessly harvested AC signal is directly used to drive the data processing circuity by leveraging charge-recycling mechanism. To quantify the advantages of the proposed framework, SIMON block cipher, a lightweight cryptography algorithm, is implemented in both AC computing and conventional methods. The simulation results demonstrate that the proposed methodology achieves up to 34 times reduction in power and enables a relatively powerful encryption core to be embedded within resource-constrained IoT devices.**

***Keywords*—IoT Security; Lightweight Encryption; Charge-recycling; RF Power**

I. Introduction

Internet of things (IoT) has emerged as a highly dynamic and radically distributed networked system, bringing smart electronics into everyday physical objects and thereby producing a cyber-physical infrastructure [1]. This novel computing paradigm is expected to have significant impact on various fields such as transportation, health care, military and smart environments [2].

Security poses a significant challenge to the widespread deployment of IoT devices since the exchanged data among the devices should be protected. The encryption/decryption of these data is difficult due to lack of resources, primarily the power budget [3]. Conventional RF powered IoT devices (such as RFIDs) are constrained by low power efficiencies of the AC-DC converter, particularly at low input power levels [4]. Even with the state-of-the-art RF-DC converters, approximately 70% of the power is lost during this stage [5]. Furthermore, traditional cryptography algorithms such as advanced encryption standard (AES), though secure and robust, are not suitable for IoT devices due to high energy cost.

Motivated by these limitations in IoT security, a novel AC computing methodology is proposed in the research, as depicted in Fig. 1. The rectifier and regulator of the existing approach are eliminated. The harvested AC signal is directly used to power the computational block. A bit-serialized SIMON cipher (a recently published lightweight cryptographic algorithm [6]) with 64-bit key is developed based on the proposed methodology. The proposed SIMON cipher relies on AC computing and ensures the integrity of exchanged data while enhancing the overall efficiency (Kb/sec/μW) by approximately 27 times.

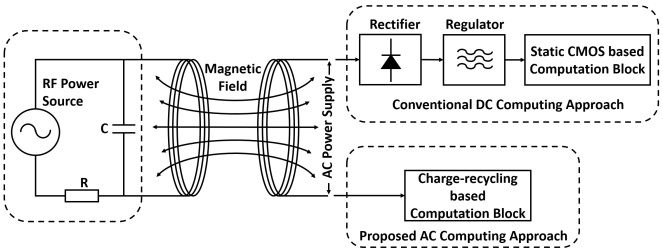

Fig. 1: Proposed AC computing methodology for RF powered IoT devices versus conventional method with rectifier and regulator.

The rest of the paper is organized as follows. In Section II, principles of charge-recycling operation are reviewed. The proposed AC computing methodology for RF powered IoT devices is described in Section III. Simulation results are presented in Section IV. Finally, the paper is concluded in the final section.

II. Background

A. Adiabatic Switching

The underlying principle of the proposed approach is the existing charge-recycling or adiabatic switching mechanism, as illustrated in Fig. 2. Consider this equivalent circuit for an adiabatic logic gate, where C is the load capacitance and R is the on-resistance of transistors along the charging path [7]. Contrary to the conventional charging that is achieved by a constant DC voltage, a time-varying voltage source is used as the power supply. If the transition time t_r is sufficiently long, capacitance voltage $v_C(t)$ approximately follows the input signal $v(t)$ [*i.e.*, $v_C(t) \approx v(t)$)]. Therefore the charging current is

$$i(t) = C\frac{dv(t)}{dt} = \frac{CV_{DD}}{t_r}. \quad (1)$$

This research is supported by the National Science Foundation (NSF) under grant number 1646318 and Simons Foundation through Stony Brook Foundation.

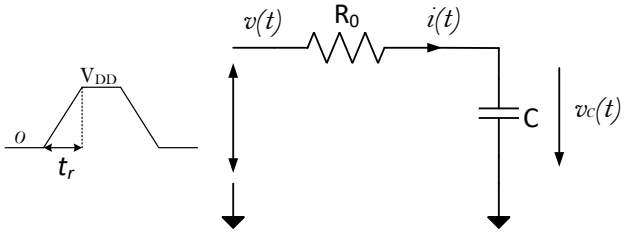

Fig. 2: Equivalent RC circuit to determine the energy loss in charge-recycling adiabatic logic.

The energy dissipated during a charging event is calculated by integrating the instantaneous power $p(t)$ during the transition time t_r,

$$E = \int_0^{t_r} [v_R(t) + v_C(t)] \cdot i(t)dt = \frac{RC}{t_r} CV_{DD}^2. \quad (2)$$

A complete cycle consists of charging and recovering. Since the recovery process consumes the same amount of energy, the overall dissipation in one adiabatic logic during a cycle is expressed by

$$E_{AL} = 2\frac{RC}{t_r} CV_{DD}^2. \quad (3)$$

As indicated by (3), energy dissipation can be significantly reduced by increasing the transition time, particularly in the low-frequency applications. Historically, generation of the AC signal from the input DC voltage has been one of the primary limitations for adiabatic logic systems due to low efficiency of the DC-to-AC conversion, typically in the range of 10% to 30% [8], [9]. Thus, wireless power harvesting can be considered as a niche application for adiabatic circuits since the harvested signal is already in the form of AC signal.

B. Background on SIMON Block Cipher

SIMON is a Feistel network based lightweight block cipher published by NSA, targeting highly resource-constrained applications [6]. It provides a flexible level of security in ten configurations optimized for different block size $2n$ and key size mn, where n is the word size and m is the number of keys [10]. This paper is focused on SIMON32/64, which encrypts 32-bit plaintext with a 64-bit key in 32 rounds ($m = 4$, $n = 16$).

When designing a block cipher, parallelism can be achieved at different levels such as bit level, round level, and encryption level [11]. In this work, the lowest parallelism level of one bit, one round, and one encryption engine, also known as the bit-serial architecture [12], is adopted considering highly resource-constrained IoT devices.

III. Proposed Methodology

In the proposed method, the wirelessly harvested AC signal is directly used to power charge-recycling/adiabatic circuits, while eliminating the rectifier and regulator that exist in conventional method. Existing adiabatic circuits, however, cannot be directly use since the harvested AC signal has negative voltage components, which does not work with most of the existing adiabatic logic families. In the following subsections, two separate implementations are developed, each leveraging a different adiabatic logic and exhibiting different characteristics.

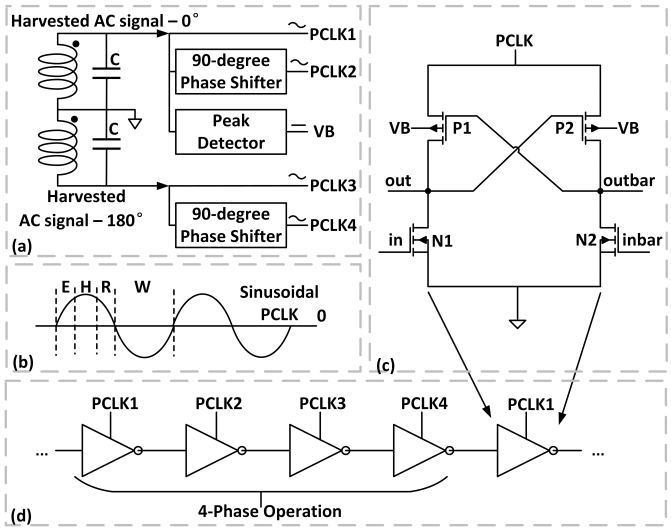

Fig. 3: Proposed ECRL based AC computing system: (a) 4-phase power-clock generation, (b) power-clock signal waveform and 4 operation intervals, (c) schematic of ECRL based inverter, (d) chains of ECRL logic gates.

A. Wirelessly Powered Efficient Charge Recovery Logic (WP-ECRL)

The primary components of the wirelessly powered (WP) efficient charge recover logic (ECRL) based approach are depicted in Fig. 3 [13]. ECRL is a quasi adiabatic logic with complementary functional blocks (f and $\overline{f}$) consisting of nMOS transistors, and a pair of cross-coupled pMOS transistors [see Fig. 3(c)]. The operation of ECRL logic requires four power-clock signals with 90° phase difference. Power-clock (PCLK) signal is typically a trapezoidal waveform and divided into four phases/intervals: evaluation (E), hold (H), recovery (R), and wait (W), as illustrated in Fig. 3(b). Initially, PCLK signal starts to rise from 0 to V_{DD}. Once it reaches the threshold voltage of P2, $outbar$ starts to follow PCLK signal, assuming that signal in is at logic high (so that out is at logic low). During the hold phase, the output node stays above a fixed voltage level so that the next stage can properly evaluate. Then, during the recovery phase, PCLK gradually decreases, partially recycling the charge stored on the load capacitance. For symmetry, a wait phase is inserted to complete the four-phase operation. The PCLK signals of any two adjacent gates have 90° phase difference. To guarantee the proper operation, the WP-ECRL approach requires a peak detector and phase shifter, as shown in Fig. 3(a) and described below:

1) Peak Detector: Biasing the nWELL of the cross-coupled pMOS transistors is challenging due to lack of rectifier (DC voltage). If these bulk nodes are connected to the AC power-clock signal (with negative voltage components), the bulk-to-

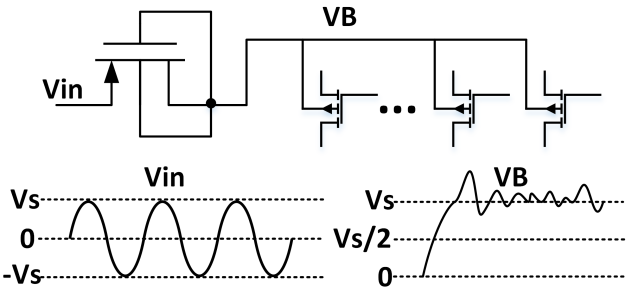

Fig. 4: Schematic of a diode-connected MOS peak detector.

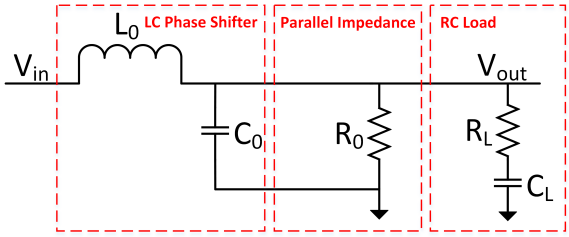

Fig. 5: An RLC model of an LC phase shifter with load.

drain junction diodes are turned on when the junction voltage exceeds the forward-on threshold, dissipating unnecessary power due to significant forward bias diode current. Thus, a peak detector is introduced to avoid the power loss.

A peak detector is a serial connection of a diode-connected transistor and a capacitance (at the bulk terminals of the pMOS devices), producing an unregulated DC voltage equal to the peak value of the applied AC signal, as depicted in Fig. 4.

The output of the peak detector is used to properly bias the bulk nodes of the pMOS devices. Note that unlike a conventional rectifier that provides sufficient current at the output, the current across the peak detector is negligible. Thus, the peak detector is more power efficient as compared to conventional rectifiers that need to drive resistive loads. This issue is further discussed in Section IV-A.

2) Phase Shifter: As shown in Fig. 3(a), the two inductors within the secondary coupling circuit are configured such that the two harvested AC signals have 180° phase difference, thereby providing a pair of complementary power-clock signals (0° and 180°). A phase shifter is required to generate the remaining two power-clock signals (90° and 270°).

Phase shifters generate a fixed phase angle along a transmission line driven by an electromagnetic wave of a certain frequency. Switched low pass and high pass topologies are commonly used in monolithic microwave ICs for achieving a flat band of 180° phase shift [14]. Inspired by this topology, the low pass arm is extracted from the switched line phase shifter to generate the four-phase power-clock signals. The proposed phase shift circuitry can be modeled as a π-LC low pass network, as shown in Fig. 5.

The values of inductor (L) and capacitor (C) that generate

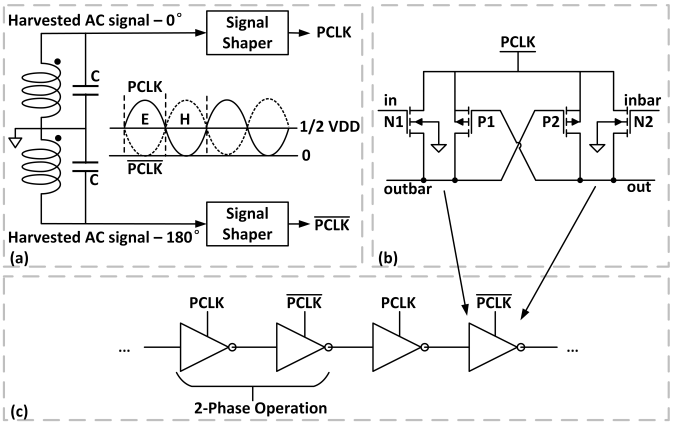

Fig. 6: Proposed PAL based AC computing system: (a) 2-phase power-clock generation and signal waveform, (b) schematic of PAL based inverter, (c) chains of PAL logic gates.

a phase shift of θ are determined from

$$L = \frac{Z_0 \sin\theta}{\omega} \quad \text{and} \quad C = \frac{1-\cos\theta}{\omega Z_0 \sin\theta}, \tag{4}$$

where Z_0 is the parallel impedance to alleviate the effect of varying load impedance on the output of the phase shifter. In the RLC model of phase shifter, Z_0 is given by,

$$Z_0 = R_0 \parallel (R_L + \frac{1}{sC_L}). \tag{5}$$

B. Wirelessly Powered Pass Transistor Adiabatic Logic (WP-PAL)

The primary components of the wirelessly powered (WP) pass transistor adiabatic logic (PAL) based approach is depicted in Fig. 6 [15], [16]. Contrary to ECRL where the nMOS transistors are grounded, in PAL, nMOS transistors are connected to the AC power-clock signal, as shown in Fig. 6(b). Thus, full charge recycling (rather than partial) can be achieved since nMOS transistors can fully discharge the output capacitance [17]. A PAL inverter consists of two pass-transistors N1, N2 for the logic function, and a pair of charging/recovering transistors P1, P2. The operation of the PAL inverter can be summarized as follows. Assume that initially, input signal in is at logic high and AC supply $PCLK$ is rising. A conducting path is formed between $outbar$ and $PCLK$ since N1 is on. Thus, node $outbar$ follows the $PCLK$ whereas node out is floating. As the $PCLK$ reaches the threshold voltage, transistor P1 turns on and fully charges $outbar$. Finally, when the $PCLK$ is falling, the charge stored at $outbar$ node is fully recovered through both N1 and P1.

Note that PAL is a two-phase logic where the AC supply of each consecutive gate is 180° out-of-phase, as illustrated in Fig. 6(c). Thus, when one of the gates is at the "evaluation" phase, the preceding gate is at the "hold" phase, maintaining the input signals stable for the evaluating gate. This behavior is also a significant advantage over ECRL that requires four-phase operation. Thus, contrary to ECRL, in PAL based AC computing for wireless devices, a phase shifter is not needed

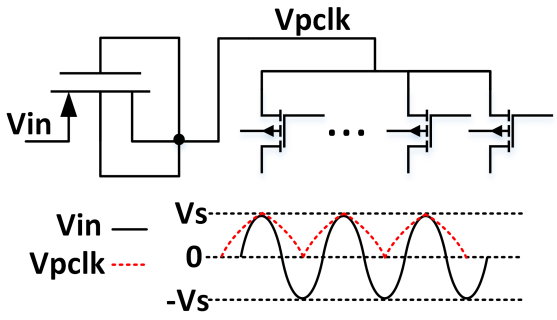

Fig. 7: Schematic of a diode-connected MOS signal shaper.

within the receiver, thereby reducing the overhead power consumption. Note that the two inductors within the receiver are configured such that the two harvested AC signals have 180° phase difference, which is sufficient for PAL operation.

Despite these advantages, PAL cannot correctly operate with the harvested AC signal that has both positive and negative voltage components. To mitigate this limitation, a low complexity signal shaper is proposed, as described below:

1) Signal Shaper: The proposed signal shaper, as shown in Fig. 7, consists of a pMOS transistor with the bulk, gate, and one of the junctions shorted together. The input is the wirelessly harvested AC signal with -1 V to 1 V whereas the output is from 0 to around 1 V. The signal shaper lets the output approximately follow the shape of the input AC signal, but does not let the output fall below zero volt (thereby eliminating the negative voltage component). Specifically, the transistor is sized to act as a voltage divider where the output signal is always positive.

IV. Results

To quantify the benefits of AC computing methodology, a bit-serialized SIMON32/64 block cipher is developed using 65 nm CMOS technology in both conventional and proposed methods. The proposed implementation of SIMON is intended for data encryption within RF-powered IoT devices with limited resources. The simulation results are presented in the following sections.

A. Auxiliary Circuits

Auxiliary circuits refer to the supporting circuitry required for each approach (such as phase shifter, peak detector and signal shaper for the proposed approaches). A low-complexity RF-DC converter/regulator is designed for the conventional approach. Typical maximum power conversion efficiencies at low input power levels are in the range of 30 to 40% due to voltage drop across the diodes [18]–[21]. To ensure a fair comparison between conventional and proposed approaches, the RF-DC converter/regulator is designed to achieve a power efficiency of 32.9%. The output voltage is regulated at approximately 1 V. For WP-ECRL, the output of the phase shifter is illustrated in Fig. 10, demonstrating 90° phase difference. The peak detector and signal shaper are also designed to maximize power efficiency.

TABLE I: Performance of the bit-serialized SIMON32/64 cipher implemented in proposed and conventional approaches.

Architecture	Conventional	Proposed	
Logic	Static Logic	ECRL	PAL
Average Power (μW)	9.12	0.91	0.27
Throughput (Kbps)	753	616	616
Efficiency (Kb/sec/μW)	83	677	2281
Transistor (#)	2966	2258	1242

B. Bit-serialized SIMON32/64 Cipher with AC Computing

ECRL and PAL based encryption circuits are supplied with a sinusoidal signal with an amplitude of 1.2 V. The conventional static logic is powered by a DC supply of 1.2 V. All of the circuits run at 13.56 MHz, the standard frequency for silicon based item-level RF identification [22].

Since adiabatic logic is inherently pipelined, additional clock phases are introduced within combinational logic. To guarantee proper functionality, the conventional FIFO-based SIMON block cipher architecture should be modified, as illustrated in Figs. 8 and 9 for, respectively, round and key expansion functions. The dashed-line boxes denote the modifications/additions in the proposed architecture, as further described below.

First, the FIFO-based bit-serial implementation uses conventional registers as the memory elements. Due to the multi-phase operation of selected adiabatic logic, a certain number of inverters are cascaded to realize the function of registers for data synchronization.The second modification is merging the multiplexers with the FIFO blocks, referred to as merged blocks in Figs. 8 and 9, to ensure that the operation is completed in one clock cycle. Assume that the round function is running the first round in Fig. 8. The output of $FIFO\_1$ is an input for the 4-to-1 multiplexer. Shift register up (SRU) and $FIFO\_1$ store the upper 16-bit word block in the current state. When the MSB of the upper block is shifted right by one bit, the LSB in $FIFO\_1$ should be ready for the computation of the next bit. To achieve this and maintain the consecutiveness of bitwise computation, multiplexer is merged with the first register of FIFO. Otherwise, the LSB in $FIFO\_1$ would only arrive to the output of the multiplexer since an adiabatic multiplexor introduces one clock phase. Finally, the additional clock phases in computing path are compensated by adding the balanced transfer paths, as depicted in Fig. 8 and Fig 9.

A software implementation of SIMON32/64 in MATLAB is also developed to verify the correctness of encryption. The input vectors of SIMON32/64 used in the simulation consists of initial keys `16'h 1918 1110 0908 0100`, plaintext `8'h 6565 6877`. The correct ciphertext is `8'h c69b e9bb`. The simulated output waveforms of three implementations are shown in Fig. 11, demonstrating the correct encryption operation.

The simulation results comparing the proposed implementation with the conventional approach are listed in Table I where average power, throughput, and efficiency are listed. According to the simulation results, the proposed methodology reduces the average power consumption by up to 34 times at

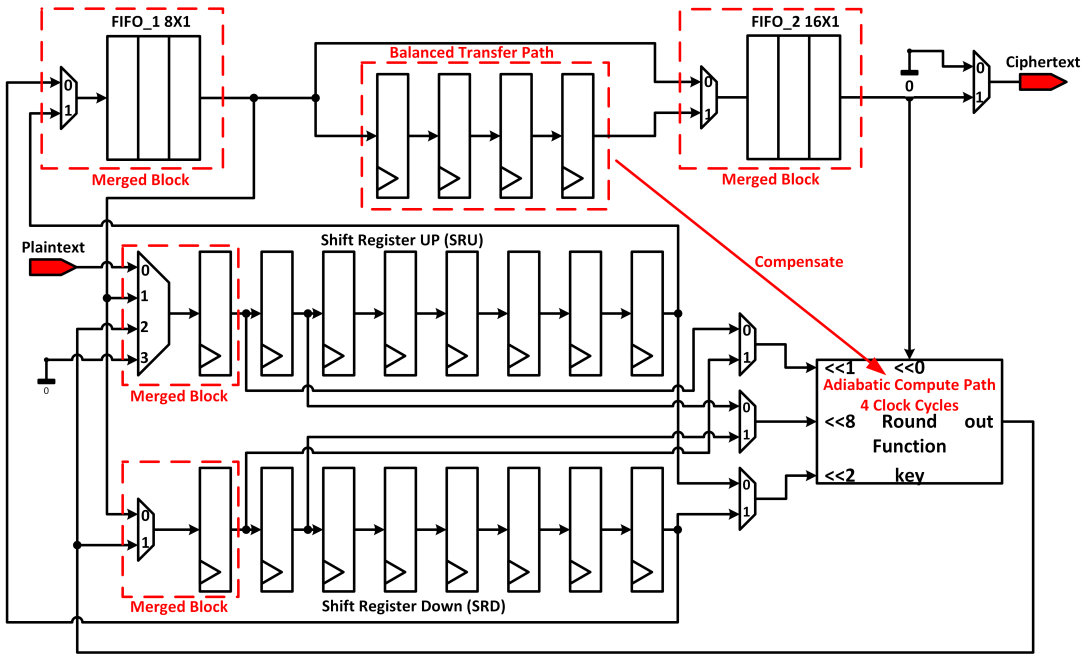

Fig. 8: Proposed adiabatic architecture for round function of the bit-serialized SIMON32/64 cipher.

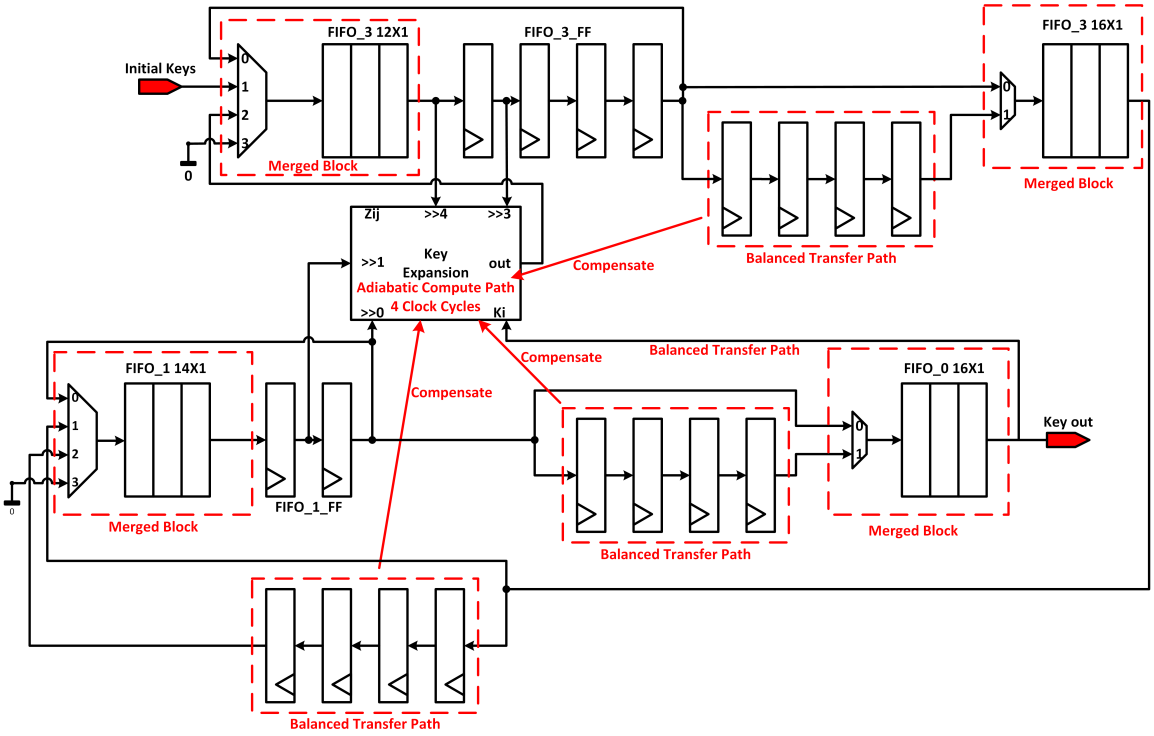

Fig. 9: Proposed adiabatic architecture for key expansion of the bit-serialized SIMON32/64 cipher.

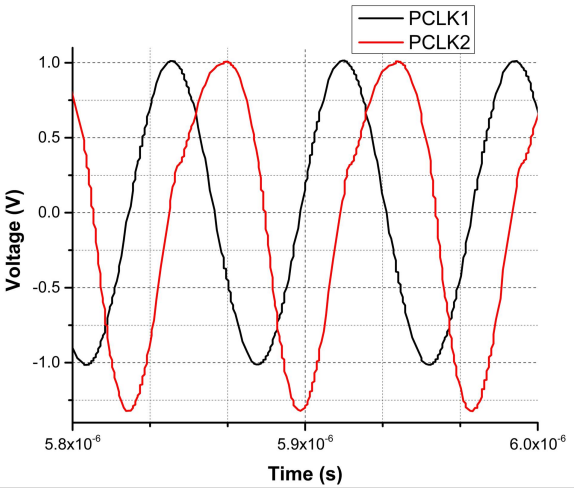

Fig. 10: Simulated output waveforms of the LC phase shifter, illustrating the 90° phase difference.

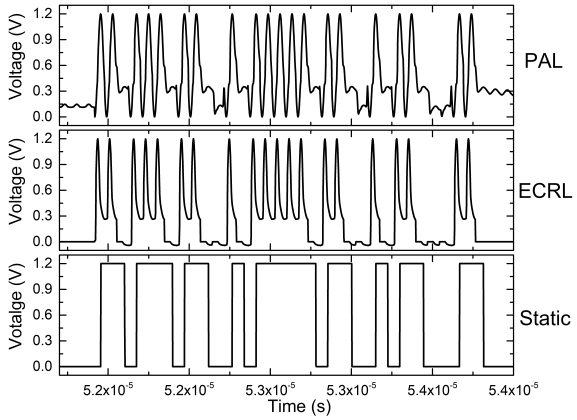

Fig. 11: Simulated output waveforms of the SIMON32/64 cipher blocks in each approach, demonstrating functional verification.

the expense of 1.2 times reduction in throughput. The encryption efficiency (Kb/sec/μW) is increased by up to 27 times. Furthermore, the overall number of transistors is reduced by up to 2.4 times.

Conclusion

A novel AC computing methodology is proposed to facilitate lightweight encryption in RF powered IoT devices. The proposed method leverages the existing charge-recycling principle and eliminates the inefficient AC-to-DC conversion stage that exists in existing methods. Several circuit structures are introduced to ensure interoperability with wireless power harvesting. To evaluate the benefits of the proposed framework, a bit-serialized SIMON32/64 cipher is developed with application to resource-constrained IoT devices. The simulation results demonstrate significant advantages in efficiency, facilitating a cryptographic algorithm to be embedded into future RF powered IoT devices.

References

[1] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[4] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with rf energy harvesting: A contemporary survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 757–789, 2015.

[5] T. Soyata, L. Copeland, and W. Heinzelman, "Rf energy harvesting for embedded systems: A survey of tradeoffs and methodology," *IEEE Circuits and Systems Magazine*, vol. 16, no. 1, pp. 22–57, 2016.

[6] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The simon and speck families of lightweight block ciphers," Cryptology ePrint Archive, Report 2013/404, 2013, http://eprint.iacr.org/2013/404.

[7] P. Teichmann, *Adiabatic logic: future trend and system level perspective*. Springer Science & Business Media, 2011, vol. 34.

[8] P. Ranjith, S. K. Mandal, and D. Nagchoudhuri, "An efficient power clock generation circuit for complementary pass-transistor adiabatic logic carry-save multiplier," in *International Conference on Computers and Devices for Communication*, 2009, pp. 1–4.

[9] A. Blotti and R. Saletti, "Ultralow-power adiabatic circuit semi-custom design," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 12, no. 11, pp. 1248–1253, 2004.

[10] R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith, and L. Wingers, "The simon and speck lightweight block ciphers," in *Proc. of ACM/IEEE DAC*, 2015, pp. 1–6.

[11] A. Aysu, E. Gulcan, and P. Schaumont, "Simon says: Break area records of block ciphers on fpgas," *IEEE Embedded Systems Letters*, vol. 6, no. 2, pp. 37–40, 2014.

[12] E. Gulcan, A. Aysu, and P. Schaumont, "A flexible and compact hardware architecture for the simon block cipher," in *International Workshop on Lightweight Cryptography for Security and Privacy*, 2014, pp. 34–50.

[13] T. Wan, E. Salman, and M. Stanacevic, "A new circuit design framework for iot devices: Charge-recycling with wireless power harvesting," in *Proc. of IEEE ISCAS*, 2016, pp. 2046–2049.

[14] I. J. Bahl, *Lumped elements for RF and microwave circuits*. Artech house, 2003.

[15] T. Wan, Y. Karimi, M. Stanacevic, and E. Salman, "Energy efficient AC computing methodology for wirelessly powered IoT devices," in *Proc. of IEEE ISCAS*, 2017, pp. 1–4.

[16] T. Wan, Y. Karimi, M. Stanacevic, and E. Salman, "Perspective Paper: Can AC Computing Be an Alternative for Wirelessly Powered IoT Devices?" *IEEE Embedded Systems Letters*, vol. 9, no. 1, pp. 13–16, 2017.

[17] V. Oklobdzija, D. Maksimovic, and F. Lin, "Pass-transistor adiabatic logic using single power-clock supply," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 44, no. 10, pp. 842–846, 1997.

[18] M. Stoopman, S. Keyrouz, H. J. Visser, K. Philips, and W. A. Serdijn, "Co-design of a cmos rectifier and small loop antenna for highly sensitive rf energy harvesters," *IEEE Journal of Solid-State Circuits*, vol. 49, no. 3, pp. 622–634, 2014.

[19] L. G. de Carli, Y. Juppa, A. J. Cardoso, C. Galup-Montoro, and M. C. Schneider, "Maximizing the power conversion efficiency of ultra-low-voltage cmos multi-stage rectifiers," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 4, pp. 967–975, 2015.

[20] T. Le, K. Mayaram, and T. Fiez, "Efficient far-field radio frequency energy harvesting for passively powered sensor networks," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 5, pp. 1287–1302, 2008.

[21] Y. Lu, H. Dai, M. Huang, M.-K. Law, S.-W. Sin, U. Seng-Pan, and R. P. Martins, "A wide input range dual-path cmos rectifier for rf energy harvesting," *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2016.

[22] E. Cantatore *et al.*, "A 13.56-mhz rfid system based on organic transponders," *IEEE Journal of Solid-State Circuits*, vol. 42, no. 1, pp. 84–92, 2007.