Are QCA Cryptographic Circuits Resistant to Power Analysis Attack?

Weiqiang Liu, *Student Member, IEEE*, Saket Srivastava, Liang Lu, Máire O'Neill (née McLoone), *Senior Member, IEEE*, and Earl E. Swartzlander, Jr., *Life Fellow, IEEE*

***Abstract*—Quantum-dot cellular automata (QCA) technology is expected to offer fast computation performance, high density, and low power consumption. Thus, researchers believe that QCA may be an attractive alternative to CMOS for future digital designs. Side channel attacks, such as power analysis attacks, have become a significant threat to the security of CMOS cryptographic circuits. A power analysis attack can reveal the secret key from measurements of the power consumption during the encryption and decryption process. As there is no electric current flow in QCA technology, the power consumption of QCA circuits is extremely low when compared to their CMOS counterparts. Therefore, in this paper an investigation into both the best and worst case scenarios for attackers is carried out to ascertain if QCA circuits are immune to power analysis attack. A QCA design of a submodule of the Serpent cipher is proposed. In comparison to a previous design, the proposed design is more efficient in terms of complexity, area, and latency. By using an upper bound power model, the first power analysis attack of a QCA cryptographic circuit is presented. The simulation results show that even though the power consumption is low, it can still be correlated with the correct key guess, and all possible subkeys applied to the Serpent submodule can be revealed in the best case scenario. Therefore, in theory QCA cryptographic circuits would be vulnerable to power analysis attack. However, the security of practical QCA devices can be greatly improved by applying a smoother clock. Moreover, in the worst case scenario, the design of logically reversible QCA circuits with Bennett clocking could be used as a natural countermeasure to power analysis attack. Therefore, it is believed that QCA could be a niche technology in the future for the implementation of security architectures resistant to power analysis attack.**

***Index Terms*—Cryptography, power analysis attack, quantum-dot cellular automata (QCA) power model, S-box, serpent cipher.**

Manuscript received July 31, 2012; accepted September 25, 2012. Date of publication October 4, 2012; date of current version November 16, 2012. This work was supported by the Engineering and Physical Sciences Research Council leadership fellowship grant (EP/G007586/1). The work of E. E. Swartzlander, Jr., was supported in part by a grant from the Advanced Micro Devices. The review of this paper was arranged by Associate Editor F. Lombardi.

W. Liu and M. O'Neill (née McLoone) are with the Institute of Electronics, Communications and Information Technology, Queen's University Belfast, Belfast BT3 9DT, U.K. (e-mail: wliu05@qub.ac.uk; m.oneill@ecit.qub.ac.uk).

S. Srivastava is with the Indraprastha Institute of Information Technology, New Delhi 110078, India (e-mail: saket@iiitd.ac.in).

L. Lu was with the Institute of Electronics, Communications and Information Technology, Queen's University Belfast, Belfast BT3 9DT, U.K. He is now with Imagination Technologies, Hertfordshire WD4 8LZ, U.K. (e-mail: l.lu@ecit.qub.ac.uk).

E. E. Swartzlander, Jr., is with the Department of Electrical and Computer Engineering, University of Texas at Austin, Austin, TX 78712 USA (e-mail: eswartzla@aol.com).

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

Digital Object Identifier 10.1109/TNANO.2012.2222663

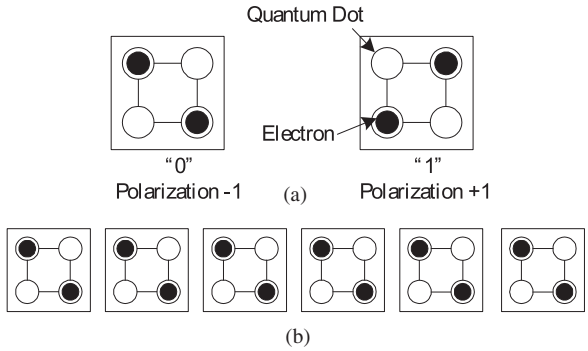


Fig. 1. Schematics of QCA cells and wires.

I. Introduction

QUANTUM-DOT cellular automata (QCA) [1], [2] is a promising alternative to CMOS technology. It can offer significant advantages including fast speed, high density, and low power consumption, which can maintain the trend of Moore's Law. QCA cells are the elementary units. This paper assumes the use of semiconductor QCAs which consist of square nanostructures with a quantum dot in each corner as shown schematically in Fig. 1(a). The cell is populated with two electrons that can tunnel among the four quantum dots. When the barriers between dots are low enough to free the electrons under the control of the clocking scheme, these two electrons tend to occupy antipodal sites within the cell due to Coulombic repulsion. The tunneling action only occurs within, and not between cells. Thus, two ground states with polarizations of -1 and 1 are available to represent binary "0" and "1," respectively. In contrast to a physical wire, a QCA "wire" is a chain of cells where the cells are adjacent to each other as shown in Fig. 1(b). The basic logic components in QCA are inverters and three-input majority gates. Three-input majority gates realize the logic function

$$M(a, b, c) = ab + ac + bc \tag{1}$$

where a, b, and c are inputs. Majority gates can be easily converted to two-input AND or OR gates by fixing one of the inputs to "0" or "1," respectively. The clock typically used for semiconductor QCAs is a four-phase clocking scheme [2] to reduce metastability issues and enable deep pipelines. To apply this clocking scheme, QCA circuits are divided into four clocking zones and each zone contains four phases with a 90° phase shift between adjacent zones. A latched clocking zone is used as the input to the subsequent zone and cells in the other two zones do

not affect these computing zones as they are in inactive states. Since the cells in one clocking zone become latched and remain in this state until the cells are latched in the next clocking zone, information is transferred and processed in a pipelined manner. QCA technology not only provides a fundamentally novel physical structure, but also offers a new kind of computing architecture for a digital design. Simple QCA components have been fabricated and demonstrated [3]–[5] and more complex circuits [6]–[12] have been designed and verified by simulation tools. Digital design methods for QCA circuits [13]–[17] have also been explored to achieve more efficient designs.

As QCA technology is expected to offer ultralow power, the power consumption of designs is not expected to be significant. However, side channel analysis (SCA) attacks [18], [19] based on power analysis have emerged as a significant threat to cryptographic circuits implemented in CMOS in the past decade. These attacks exploit information leaked by the physical implementation of a cryptographic cipher and typically the amount of side-channel information required to break the cipher is very small [19]. One of the most powerful SCA techniques is a power analysis attack [20]–[22]. This attack can extract the secret key of an electronic security device by measuring the power consumption of cryptographic operations inside the device that is highly data dependent. Since QCA is a field-coupled computing paradigm which only involves changing the position of electrons in the cells, the power consumption is ultralow. Therefore, it is appropriate to ask if QCA cryptographic circuits are resistant to power analysis attack.

Some previous research has been carried out into the power dissipation of QCA circuits. Based on the density matrix formalism, a quantum mechanical power model was proposed by Timler and Lent [23], [24]. Although this model provides an accurate estimation of the power in QCA circuits, it is computationally expensive to evaluate a large-scale design. A case study of the energy dissipated in a two-cell chain was investigated via an RC model by Bond and Macucci [25]. Based on the research by Timler and Lent [23], a power model to compute the upper bound of the power consumed in QCA circuits in one clock cycle was proposed by Srivastava *et al.* [26]. This power model can provide a tight upper bound of the power consumption in QCA circuits for quasi-adiabatic (smooth) switching. The lower bound power dissipation for QCA circuits was also studied by Lent *et al.* [27]. The lower bound power dissipation was derived by changing the typical four-phase quasi-adiabatic clock to a Bennett clock.

To evaluate the security of QCA cryptographic circuits in terms of power analysis attacks, both the best case and the worst case scenarios for an attacker can be considered. Power dissipation during quasi-adiabatic switching will be very low [23]. However, a more realistic scenario of switching is more abrupt and hence will introduce more power dissipation. Generally, the greater the power dissipation, the easier to perform a power analysis attack [20], [28]. The best case scenario for attackers involves upper bound power dissipation with nonadiabatic clocking. Therefore, the upper bound power model [26] can be used to assess the performance of QCA cryptographic circuits under power analysis attack. To fully address the issues related to power analysis attack, the worst case scenario (for attackers) should also be considered with a lower bound power model. Lower bound power dissipation is related to Bennett-clocked QCA circuits. The power dissipation under Bennett clocking is arbitrarily low, even lower than the bit erasure energy $k_B T ln(2)$ [27]. The lower bound power model proposed by Lent *et al.* [27] is used to study this scenario.

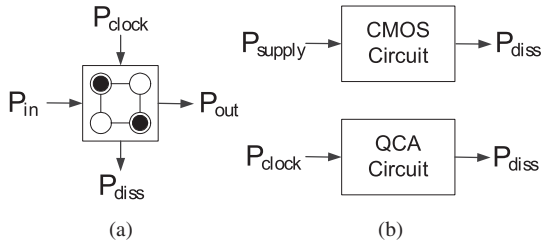


Fig. 2. Power dissipation in QCA. (a) Power flow in a QCA cell. (b) Power dissipation in CMOS and QCA circuits.

The best case scenario is considered first. The power dependence on the Hamming distance (HD) of inputs in QCA gates is demonstrated as a fundamental step in the power analysis attack. As a case study, a submodule of the Serpent cryptographic block cipher with its 4-bit $\times$ 4-bit S_0-box is designed in QCA. It is verified using QCAPro, which is a fast power estimation tool for a QCA circuit design [29]. The power consumption of the Serpent submodule is also simulated in QCAPro based on the upper bound power model. A power analysis attack procedure for QCA is proposed to reveal the secret key by statistically comparing the power consumption and all hypothetical key guesses. The first power analysis attack results show that QCA cryptographic circuits could be at risk of being attacked under typical quasi-adiabatic clocking. Then, a more realistic scenario is discussed for practical QCA devices. Finally, the worst case scenario for attackers is also studied based on a Bennett-clocked QCA gate.

This paper is organized as follows: Section II presents an overview of the upper bound power model for QCA circuits and the power dependence on HD in basic QCA gates. The design of the Serpent submodule with its 4-bit $\times$ 4-bit S_0-box is provided in Section III. Section IV presents the proposed procedure of performing a power analysis attack on QCA circuits using the upper bound power model and provides the first power analysis results in QCA. A discussion of practical QCA devices is given in Section V. The vulnerability of Bennett-clocked QCA circuits to power analysis attack is studied in Section VI and Section VII concludes this paper.

II. Upper Bound Power Model and Power Dependence on HD

QCA technology promises ultralow power computing which can accommodate high densities. The power flow of a QCA cell is shown in Fig. 2(a), where $P_{\rm in}$ is the signal power from the neighboring cell on its left, $P_{\rm out}$ is the signal power transferred to the cell on its right, $P_{\rm clock}$ is the energy provided by the clock, and $P_{\rm diss}$ is the power dissipated. The signal powers $P_{\rm in}$ and $P_{\rm out}$ are generally equal as demonstrated in [23]. A considerable amount of energy is drawn into the cell from the

clock as the barriers are being raised. Most of that energy is returned to the clock as the barriers are lowered. The difference between the powers in and out of the clock is $P_{\rm diss}$. Since $P_{\rm diss}$ is of interest in this research, it is not necessary to include other parts of the cell's power flow in the simulation of power dissipation. Power is only dissipated in a QCA cell when actual computation is performed.

As shown in Fig. 2(b), the power dissipation of a CMOS circuit can be measured by monitoring the power supply, *i.e.*, $P_{\rm supply}$. Similarly, since the power of a QCA circuit is provided by its clock [23], the dissipated power can be measured by the power provided by the clock, *i.e.*, $P_{\rm clock}$. Previous research [30] has shown that the power dissipated in the clocking wires is fairly small and that dissipation in the QCA devices themselves will dominate the power dissipation. Even if the power losses in the clock wire are large, these power losses are not data dependent; thus, they will not affect the results of a power analysis attack [28]. As the best case scenario for attackers is considered here, only the power dissipated by the QCA cells is considered.

Power consumption occurs in QCA circuits when the instantaneous coherence vector cannot track the steady-state vector in an instant of time [26]. Except for pure adiabatic switching, the lag between these two vectors is unavoidable. As typical switching is quasi-adiabatic, power consumption is unavoidable. The upper bound of quasi-adiabatic power dissipation is reached with nonadiabatic clocking. The best case scenario for attackers is considered to determine if QCA circuits are vulnerable to power analysis attack. An upper bound power dissipation model [26] is used, which has been derived from a quasi-adiabatic model [23]. In this section, an overview of the upper bound power model is presented. The validity of the upper bound power is confirmed by calculating the actual power dissipated for various levels of clock smoothness in a QCA cell. Then, the power dependence on the HD in QCA cells and basic components under different tunneling energy levels and temperatures is illustrated.

A. Upper Bound Power Model

A Hamiltonian matrix can be used to describe the total energy of a QCA cell. Using the Hartree-Fock approximation [31] and assuming that only Coulombic interactions apply between cells, the matrix representation of the Hamiltonian for an array of cells is [23], [26]

$$H = \begin{bmatrix} -\frac{1}{2}\sum_i E_k x_i f_i & -\gamma \\ -\gamma & \frac{1}{2}\sum_i E_k x_i f_i \end{bmatrix} = \begin{bmatrix} -\frac{1}{2}G & -\gamma \\ -\gamma & \frac{1}{2}G \end{bmatrix} \tag{2}$$

where

$\sum_i$	the sum over the cells;
E_k	the kink energy;
f_i	the geometric factor that specifies the electronic falloff with distance between cells;
x_i	the polarization of the ith neighbor cell;
γ	the tunneling energy between two logic states of a cell which is controlled by the clock;
G	used to denote the total kink energy caused by neighboring polarized cells.

The energy of a QCA cell at each clock cycle is the expected value of the Hamiltonian, which is given by [23], [26]

$$E = \langle H \rangle = \frac{\hbar}{2}\vec{\Gamma}\cdot\vec{\lambda} \tag{3}$$

where $\hbar$ is the reduced Planck constant, $\vec{\lambda}$ is the coherence vector, and $\vec{\Gamma}$ is the 3-D energy vector

$$\vec{\Gamma} = \frac{1}{\hbar}\left[-2\gamma, 0, G\right]. \tag{4}$$

The equation for the instantaneous power can then be derived as follows:

$$P_{\rm total} = \frac{{\rm d}E}{{\rm d}t} = \frac{\hbar}{2}\frac{\rm d}{{\rm d}t}\left(\vec{\Gamma}\cdot\vec{\lambda}\right) = \frac{\hbar}{2}\left(\frac{{\rm d}\vec{\Gamma}}{{\rm d}t}\right)\cdot\vec{\lambda} + \frac{\hbar}{2}\vec{\Gamma}\cdot\left(\frac{{\rm d}\vec{\lambda}}{{\rm d}t}\right). \tag{5}$$

The first term represents the power in and out of the clock and the intercell power flow. It is the second term, namely $P_{\rm diss}$, that refers to the dissipated power. Therefore, the power dissipation of a QCA cell can be calculated as

$$P_{\rm diss} = \frac{\hbar}{2}\vec{\Gamma}\cdot\left(\frac{{\rm d}\vec{\lambda}}{{\rm d}t}\right). \tag{6}$$

Energy dissipated in one clock cycle $T_c = [-D, D]$ can be computed by [26]

$$\begin{aligned} E_{\rm diss} &= \frac{\hbar}{2}\int_{-D}^{D}\vec{\Gamma}\cdot\frac{d\vec{\lambda}}{{\rm d}t}{\rm d}t = \frac{\hbar}{2}\left(\left[\vec{\Gamma}\cdot\vec{\lambda}\right]_{-D}^{D} - \int_{-D}^{D}\vec{\lambda}\cdot\frac{{\rm d}\vec{\Gamma}}{{\rm d}t}{\rm d}t\right) \\ &= \frac{\hbar}{2}\left(\vec{\Gamma}_+\cdot\vec{\lambda}_+ - \vec{\Gamma}_-\cdot\vec{\lambda}_- - \int_{-D}^{D}\vec{\lambda}\cdot\frac{{\rm d}\vec{\Gamma}}{{\rm d}t}{\rm d}t\right) \end{aligned} \tag{7}$$

where $\vec{\Gamma}_-$ and $\vec{\Gamma}_+$ are used to denote $\vec{\Gamma}\,(-D)$ and $\vec{\Gamma}\,(D)$ and the same notation is used for $\vec{\lambda}$. The maximum power will be dissipated when the change of $\vec{\Gamma}$ is a maximum under nonadiabatic switching. By modeling a step change with a delta function, the upper bound of power dissipation for a QCA cell is derived as follows [26]:

$$\begin{aligned} P_{\rm diss} = \frac{E_{\rm diss}}{T_c} &< \frac{\hbar}{2T_c}\vec{\Gamma}_+ \\ &\times\left[-\frac{\vec{\Gamma}_+}{\left|\vec{\Gamma}_+\right|}\tanh\left(\frac{\hbar\left|\vec{\Gamma}_+\right|}{kT}\right) + \frac{\vec{\Gamma}_-}{\left|\vec{\Gamma}_-\right|}\tanh\left(\frac{\hbar\left|\vec{\Gamma}_-\right|}{kT}\right)\right] \end{aligned} \tag{8}$$

where $\vec{\Gamma}_+$ and $\vec{\Gamma}_-$ are the values of the Hamiltonian before and after the transition, k is the Boltzmann constant, and T is the temperature. Once the pretransition and posttransition Hamiltonians are known, the upper bound of power dissipation for a QCA cell can be calculated. The power model is derived by including the effects of dissipative coupling to a heat bath.

The power dissipation model for each QCA cell is similar; therefore, the total power for one clock cycle can be computed by summing up the power consumed by each cell. The cells interact via the electronic kink energy between them. Power can be computed by tracking the polarization of the cells before and after the switching of the input cells, where next-near-neighbor coupling is ignored since the interaction between cells falls off by the fifth power of the distance [23]. Using the values of cell

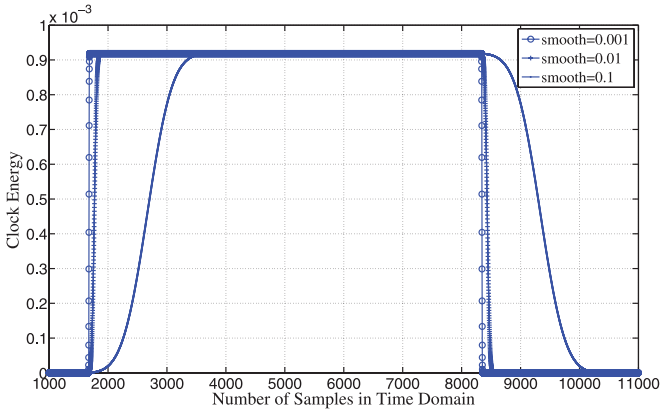


Fig. 3. Clock signals under smoothing of 0.1, 0.01, and 0.001.

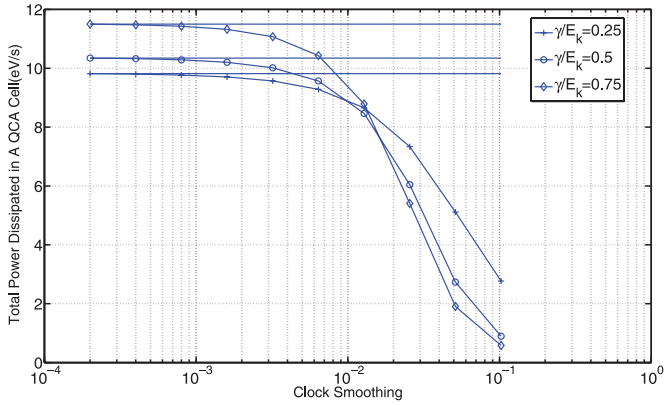


Fig. 4. Total power consumption in a QCA cell under various clock smoothing levels for different tunneling energy γ values ($T = 5.0K$). Adiabaticity of the switching process is controlled by smoothness of the clock. The horizontal line shows the upper bounds for each case.

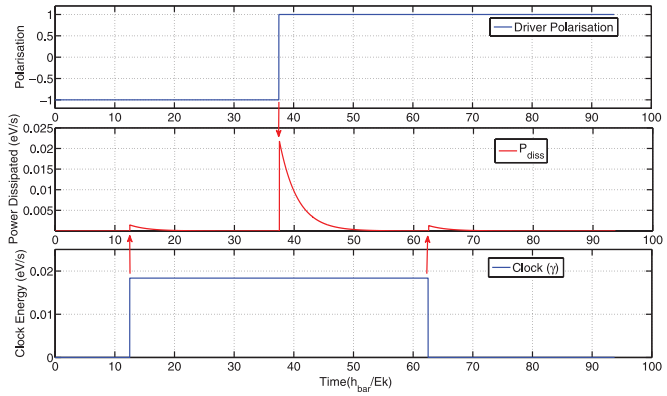


Fig. 5. Power consumption ($T = 2.0K, T_c = 75\frac{\hbar}{E_k}$) in a QCA cell under nonadiabatic switching during driver polarization changing from -1 to 1.

polarization and clock energy, the total power consumption in a QCA circuit for the transition from a current input to the next input can be calculated.

To perform a power analysis attack of a QCA circuit, a power tool for large circuits is required. Based on the upper bound power model discussed earlier, a power tool called QCAPro was developed [29]. QCAPro also offers a quick design check to verify the correct polarization of a design. The input required for the QCAPro tool is the layout file generated by QCADesigner [32] which is a widely used design and simulation tool for QCA. The current version of QCAPro [29] only provides the average, maximum, and minimum power consumption of a QCA circuit during the input switching. For this research, it was necessary to modify the tool to compute and provide the power consumption in one clock cycle according to every input change.

B. Power Consumption in a Cell

The power dissipated in each cell is a function of the rate of change of the clock and the tunneling energy. The adiabaticity of the system is directly proportional to the amount of clock smoothing which can be implemented by a Gaussian function [26]. Clock signals with smoothing from 0.1 to 0.001 are shown in Fig. 3. The actual power dissipated using the quantum model for various values of these parameters was calculated and compared with the upper bound power, which is shown in Fig. 4. The results show that the upper bounds do indeed hold and are reached when the clock smoothing is zero, i.e., nonadiabatic switching. Therefore, it confirms the validity of the upper bound power assumption in this research. Note that, as can be seen from Fig. 4, for a smoother clock, for higher tunneling energies, less power is dissipated, while for a less smooth clock, for higher tunneling energies, more power is dissipated.

To compute the power consumption of a QCA cell under a nonadiabatic clock when its polarization changes from -1 (logic "0") to 1 (logic "1"), the upper bound power model is used. There are three parts to the power consumption of a cell whenever the Hamiltonian changes, as shown in Fig. 5. The first part occurs when the clock goes from low to high (γ_L to γ_H) to depolarize a cell. The second part happens when the driven cell changes state (G_- to G_+), and the third part is produced by changing the clock from high to low (γ_H to γ_L), which latches the cell to the new state. The first and third parts of the power consumption occur even if there are no changes to the cell's polarization. Thus, these can be considered as static power. The second part of the power consumption is dependent on the changes to the cell's polarization, which can be considered as dynamic power. It is clear from Fig. 5 that the dynamic power is significantly larger than the static power in a QCA cell. Since the dynamic power is dependent on the polarization changes, the total power loss in a QCA cell can possibly provide information about its inputs.

Note that the absolute value of the power consumption is on the order of a few hundredths of an electron volt, i.e., eV, which is extremely low. However, a power analysis attack exploits the difference between the static power and dynamic power rather than the absolute value of the power.

C. Power Dependence on HD in Basic QCA Components

The power consumption of a QCA inverter, as shown in Fig. 6, is provided in Table I under different tunneling energy levels. The power consumption does not vary as the temperature range is small, from 1.0 to 8.0 K. From the tables, it can be seen that

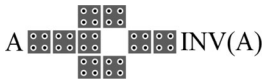


Fig. 6. QCA layout of an inverter.

TABLE I
POWER CONSUMPTION OF AN INVERTER WITH DIFFERENT TUNNELING ENERGY LEVELS ($T = 2.0$ K)

Input Switching	Hamming Distance	Power Dissipated			
		$\gamma = 0.25E_k$	$\gamma = 0.5E_k$	$\gamma = 0.75E_k$	$\gamma = 1.0E_k$
$0 \rightarrow 0$	0	0.8 meV	2.7 meV	5.2 meV	8.0 meV
$1 \rightarrow 1$		0.8 meV	2.7 meV	5.0 meV	8.0 meV
$0 \rightarrow 1$	1	28.4 meV	28.6 meV	29.3 meV	30.2 meV
$1 \rightarrow 0$		28.4 meV	28.6 meV	29.3 meV	30.2 meV

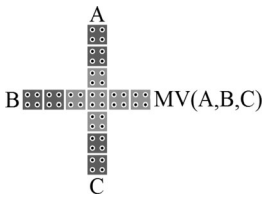


Fig. 7. QCA layout of a majority gate.

TABLE II
POWER CONSUMPTION OF A MAJORITY GATE WITH DIFFERENT TUNNELING ENERGY LEVELS ($T = 2.0$ K)

Switching (A, B, C)	Hamming Distance	Power Dissipated			
		$\gamma = 0.25E_k$	$\gamma = 0.5E_k$	$\gamma = 0.75E_k$	$\gamma = 1.0E_k$
$000 \rightarrow 000$ (0)	0	0.8 meV	2.8 meV	5.3 meV	8.1 meV
$000 \rightarrow 001$ (1)	1	2.3 meV	4.2 meV	6.8 meV	9.8 meV
$000 \rightarrow 010$ (2)		2.3 meV	4.2 meV	6.8 meV	9.8 meV
$000 \rightarrow 100$ (4)		2.3 meV	4.2 meV	6.8 meV	9.7 meV
$000 \rightarrow 011$ (3)	2	25.3 meV	26.4 meV	27.9 meV	29.8 meV
$000 \rightarrow 101$ (5)		25.3 meV	26.4 meV	28.0 meV	29.8 meV
$000 \rightarrow 110$ (6)		25.3 meV	26.4 meV	28.0 meV	29.8 meV
$000 \rightarrow 111$ (7)	3	41.0 meV	41.2 meV	41.9 meV	42.9 meV

in the case of transitions from $0 \rightarrow 0$ and $1 \rightarrow 1$, little static power is dissipated, while for transitions from $0 \rightarrow 1$ and $1 \rightarrow 0$ significantly more power is consumed due to the input changes which produce high dynamic power loss. It is clear that the power consumption of a QCA inverter is dependent on the HD of the inputs. The HD of two inputs X_1 and X_2 is the Hamming weight (HW) of $X_1 \oplus X_2$, where HW is the number of binary "1"s and $\oplus$ represents XOR

$$\text{HD}(X_1, X_2) = \text{HW}(X_1 \oplus X_2). \tag{9}$$

The other fundamental component used in a QCA design is the majority gate, the layout of which is shown in Fig. 7. Its power consumption for input switching from 0 ("000") to 7 ("111") is provided in Table II under different tunneling energy levels. As with the inverters, the power consumption does not vary as the temperature range is small. For HD $= 1$, only one input of the majority gate changes its polarization. Thus, only a little power is consumed. In the case of HD > 1, more cell inputs change and the output polarization changes, which increases the power consumption. It is apparent that increased switching with higher HD results in higher power consumption. Fig. 8 illustrates

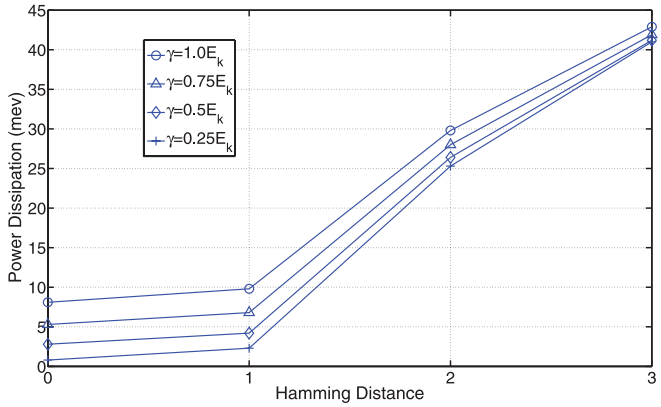


Fig. 8. Power consumption ($T = 2.0$ K) in majority gate versus HD with various tunneling energy γ levels.

clearly the strong dependence between the HD and the power consumption under various tunneling energy levels. Since the functional temperature range of current semiconductor QCA devices is limited, there is little power consumption difference for the different temperatures.

Since power analysis attacks exploit the fact that the power consumption of a cryptographic circuit is correlated with the processed data, such as the HD of inputs [28], from the analysis outlined previously, QCA cryptographic circuits may be vulnerable to attack. However, since QCA architectures are very different from equivalent CMOS architectures, a submodule of the Serpent cryptographic algorithm has been designed in QCA and attacked using a power analysis attack to determine its vulnerability.

III. DESIGN OF THE QCA CRYPTOGRAPHIC CIRCUIT: SERPENT SUBMODULE

Cryptographic block ciphers such as advanced encryption standard (AES) and data encryption standard (DES) are widely used to encrypt confidential information; however, they are vulnerable to power analysis attack which typically targets the substitution boxes (S-boxes) [21], [33]–[35]. S-boxes are at the heart of most block ciphers and are the only nonlinear parts of the ciphers. They are typically used to hide the relationship between the key and the ciphertext following Shannon's property of confusion to resist differential and linear mathematical cryptanalysis. In general, an S-box takes an n-bit input and transforms it into an m-bit output, namely an $n \times m$ S-box.

In this paper, the QCA design of a submodule of the Serpent cipher [36], which includes its S-box, is presented. The Serpent cipher is chosen because the presently available QCA design and simulation tools are currently limited in their support for large circuit designs. Serpent is a well-designed modern block cipher that offers a large security margin. It was a finalist in the AES contest [37]. The 32 rounds in the Serpent cipher provide an even higher security margin than the Rijndael cipher which is the current AES. It uses eight 4×4 S-boxes which are strongly secure against all known mathematical attacks [36]. However, similar to AES and DES, Serpent can be attacked using a power analysis attack. The essential idea of a power analysis attack is

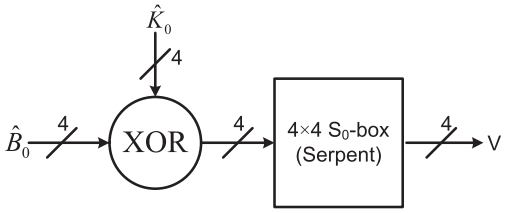


Fig. 9. Submodule of Serpent cipher.

to attack a small part of the whole key to reduce the computational complexity. More specifically, it can be used to target a key-dependent submodule of a cipher (usually the S-boxes for block ciphers) to uncover a small subkey (SK) [28]. The whole key can then be revealed by attacking each of the SKs. A successful power analysis attack of the 4×4 Serpent S-box has been demonstrated on 65-nm CMOS cryptographic circuits [38]. Therefore, Serpent is an appropriate example for demonstrating a power analysis attack on QCA cryptographic circuits.

A. Submodule of Serpent Cipher

Serpent [36] is a 32-round substitution–permutation network that operates on four 32-bit words. It encrypts a 128-bit plaintext to a 128-bit ciphertext in 32 rounds under the control of 33 128-bit SKs $\hat{K}_0, \ldots, \hat{K}_{32}$. An initial permutation is applied to a plaintext before the first round. A set of eight 4×4 S-boxes is used four times. In each round, only a single replicated S-box is used with a SK. The last round is slightly different from the others and uses two SKs, $\hat{K}_{31}$ and $\hat{K}_{32}$.

The submodule implemented in this paper is expressed as follows:

$$V = \hat{S}_0 \left(\hat{B}_0 \oplus \hat{K}_0 \right) \tag{10}$$

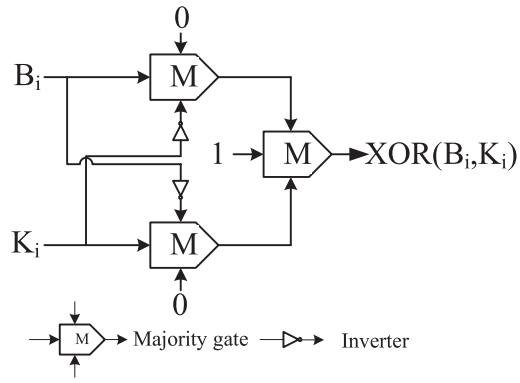
where

V an intermediate value;
$\hat{S}_0$ the first Serpent S-box, namely the S_0-box;
$\hat{B}_0$ the permutated plaintext used as the input to the first round;
$\hat{K}_0$ the first SK.

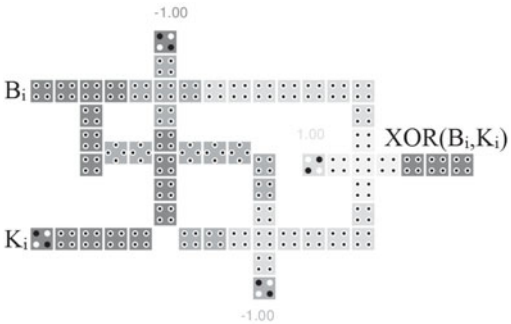
Thus, the function of the submodule as shown in Fig. 9 is to produce the first four bits of an intermediate vector by taking bits $0, 1, 2, 3$ of $\hat{B}_0 \oplus \hat{K}_0$ as the input to the S_0-box, which is chosen without loss of generality. As a replicated S-box is used in each round, the next S_0-box takes bits $4, 5, 6, 7$ of $\hat{B}_0 \oplus \hat{K}_0$ and returns the next four bits of the intermediate vector, and so on. Every four bits of the SK related to the S-box will be attacked. In this way, the SK can be revealed by the power analysis attack. If each SK is revealed, the whole secret key of the Serpent cipher can be obtained.

B. QCA Implementation of the Serpent Submodule

The submodule of the Serpent cipher contains two parts: one is the 4-bit XOR operation and the other is the S_0-box. A XOR gate is designed in QCA and its schematic and layout are shown in Fig. 10.



(a)



(b)

Fig. 10. Design of QCA XOR gate. (a) Schematic of a XOR gate. (b) QCA layout of a XOR gate.

TABLE III
TRUTH TABLE OF S_0-BOX IN FORM OF KARNAUGH MAP

x_4, x_3 \ x_2, x_1	00	01	11	10
00	3 (0011)	8 (1000)	1 (0001)	15 (1111)
01	10 (1010)	6 (0110)	11 (1011)	5 (0101)
11	7 (0111)	0 (0000)	12 (1100)	9 (1001)
10	14 (1110)	13 (1101)	2 (0010)	4 (0100)

The S_0-box is the first Serpent S-box and comprises four inputs and four outputs. Its truth table is shown in Table III. There are two methods to implement the S-box. One is to emulate a lookup table (LUT); however, memory architectures in QCA require many cells and introduce high latency. The second technique is to design a logic-based S-box. This method will occupy less area and introduce low latency. In this paper, the logic-based QCA S_0-box is designed by using majority logic reduction.

Let X denote the input and Y denote the output of the S_0-box. First, by using the Karnaugh map, the minimized logic expressions for $Y = y_4 y_3 y_2 y_1$ can be obtained with AND and OR gates as follows:

$$\begin{aligned} y_1 &= \bar{x}_4 \bar{x}_3 \bar{x}_1 + \bar{x}_4 x_2 + x_4 x_3 \bar{x}_1 + x_4 \bar{x}_3 \bar{x}_2 x_1 \\ &= \bar{x}_4 \left(\bar{x}_3 \bar{x}_1 + x_2 \right) + x_4 \left(x_3 \bar{x}_1 + \bar{x}_3 \bar{x}_2 x_1 \right) \end{aligned} \tag{11}$$

$$\begin{aligned} y_2 &= \bar{x}_4 \bar{x}_3 x_1 + \bar{x}_4 x_3 x_1 + x_4 \bar{x}_3 x_2 x_1 + \bar{x}_2 \bar{x}_1 \\ &= \bar{x}_4 \left(\bar{x}_3 x_1 + x_3 x_1 \right) + x_4 \left(\bar{x}_3 x_2 x_1 \right) + \bar{x}_2 \bar{x}_1 \end{aligned} \tag{12}$$

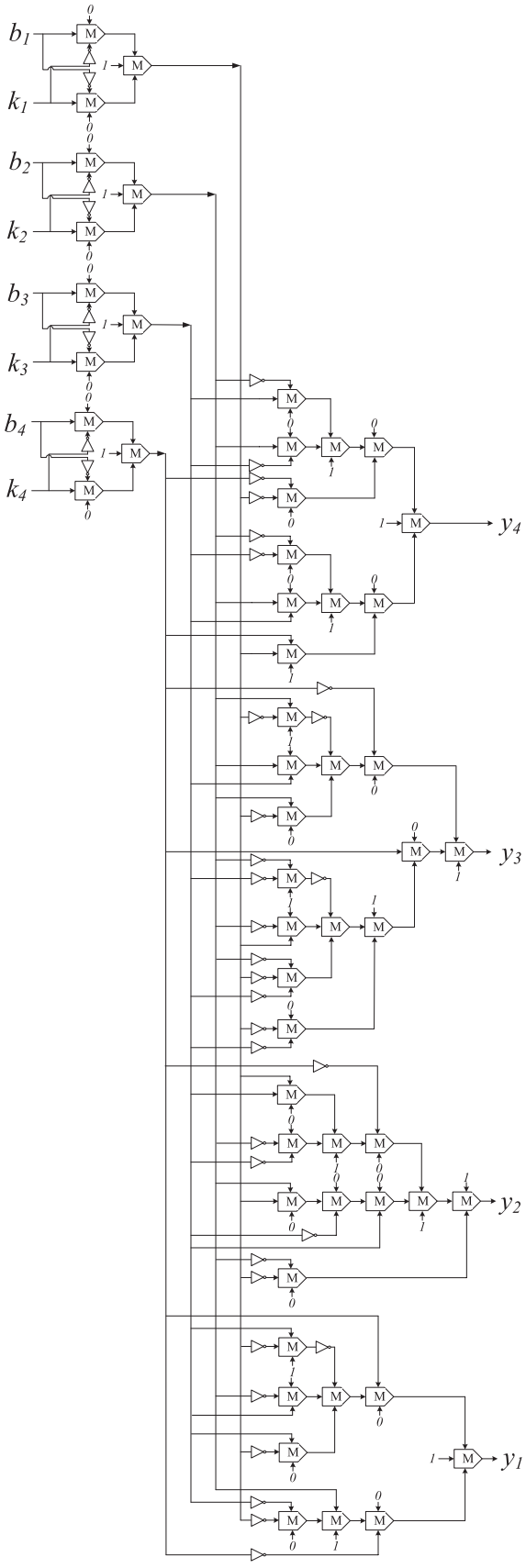


Fig. 11. Schematic of Serpent submodule based on majority gates and inverters.

$$y_3 = \bar{x}_4 x_2 \bar{x}_1 + \bar{x_4} x_3 \bar{x}_2 x_1 + x_4 \bar{x}_3 \bar{x}_1 + x_4 \bar{x}_2 \bar{x}_1 + x_4 \bar{x}_3 \bar{x}_2 + x_4 x_3 x_2 x_1 = \bar{x}_4 \left(x_2 \bar{x}_1 + x_3 \bar{x}_2 x_1\right) + x_4 \left[\bar{x}_3 \bar{x}_1 + \left(\bar{x}_2 \bar{x}_1 + \bar{x}_3 \bar{x}_2 + x_3 x_2 x_1\right)\right] \quad (13)$$

$$y_4 = \bar{x}_4 x_3 \bar{x}_2 \bar{x}_1 + \bar{x_4} \bar{x}_3 x_2 \bar{x}_1 + x_4 x_3 x_2 + x_4 \bar{x}_3 \bar{x}_2 + \bar{x}_3 \bar{x}_2 x_1 + x_3 x_2 x_1 = \bar{x}_4 \bar{x}_1 \left(x_3 \bar{x}_2 + \bar{x}_3 x_2\right) + \left(x_4 + x_1\right)\left(x_3 x_2 + \bar{x}_3 \bar{x}_2\right). \quad (14)$$

By using the majority logic reduction method [39], the previous expressions can be further minimized. y_1 and y_3 can be optimized by the following logic reduction expression:

$$F = ab + \bar{a}\bar{b}c = M(M(a, 0, b), \bar{M}(a, 1, b), M(a, 1, c)). \quad (15)$$

y_2 can be optimized by

$$F = ab + \bar{b}c = M(M(a, 0, b), 1, M(\bar{b}, 0, c)). \quad (16)$$

y_3 can be further optimized by

$$F = ab + bc + \bar{a}\bar{b}\bar{c} = M(M(\bar{a}, 1, b), \bar{M}(b, 1, c), M(a, b, c)). \quad (17)$$

The majority gate-based schematic of the Serpent submodule is shown in Fig. 11. By integrating the XOR gates and S_0-box, the QCA design of the Serpent submodule has been implemented in QCADesigner with appropriately assigned clocking zones as shown in Fig. 12 (different shades of cells show different clocking zones). The design has been checked with QCAPro, which verified that the outputs are correct for all given inputs.

A QCA design of the Serpent S_0-box based on majority logic was previously proposed [40]. In that design, each term of the logic expressions is implemented by AND and OR gates which are directly mapped from the CMOS design. However, since majority-based logic reduction was not applied, the design incurs a much higher cell count and delay [41]. A comparison between the previous work and this design is presented in Table IV. In terms of area, the QCA cell size used in both designs is 18 nm with a center-to-center cell distance of 20 nm. It can be seen from the comparison table that a much more efficient design of the Serpent S_0-box is achieved in this paper, with a reduction of 45%, 42%, and 59% in terms of number of cells, area, and latency, respectively.

IV. Power Analysis Attack of QCA Circuits

The most effective power analysis attack is differential power analysis (DPA) [20]. DPA attacks do not require a detailed knowledge of the target device or the circuit architecture and the adversary does not need to know when a particular operation is actually computed by the cryptographic circuit. Power data that have been measured while a circuit encrypts or decrypts data can be statistically analyzed to reveal the secret key. The attack process focuses exclusively on the data dependency of the power consumption. A large number of power measurements are used to analyze the power consumption that is dependent on the processed data at a fixed moment in time. For a block cipher under DPA, the S-boxes are the main target and they have been shown to be vulnerable to this kind of attack in CMOS

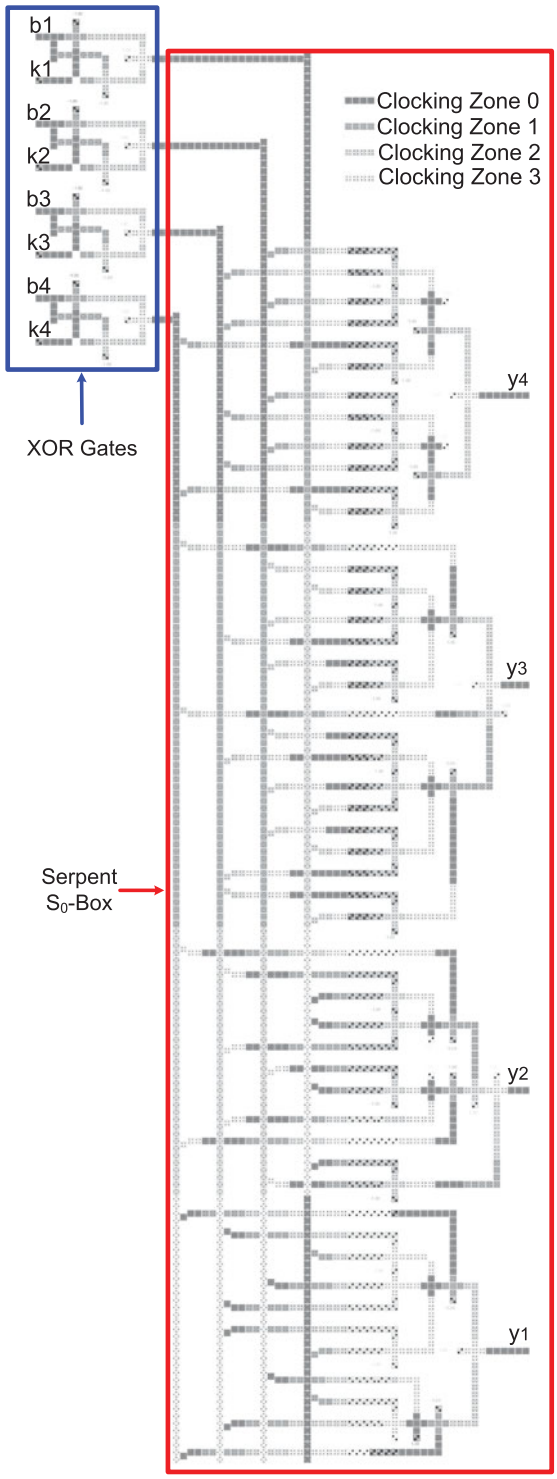


Fig. 12. QCA layout of the Serpent submodule.

technology. In this section, the first DPA attack of a QCA cryptographic circuit is presented with a proposed DPA attack procedure for QCA circuits.

A. DPA Attack Procedure for QCA Circuits

As discussed in Section II, the power consumption in basic QCA circuits depends on the HD of the input switching. Therefore, this power data of QCA circuits could be used to uncover the secret key. In a DPA attack, the power consumption of a circuit is correlated with a hypothetical power model that targets a key-dependent cryptographic operation. By comparing the hypothetical power values with the real power consumption by statistical tests, the key can be revealed. As the power consumed at a fixed moment of time is used in CMOS-based DPA attacks, the total power consumed by a QCA circuit during a full clock cycle is considered and simulated in this paper.

TABLE IV
COMPARISON OF TWO DESIGNS OF THE SERPENT S_0-BOX

Compared Items	Previous Design [40]	This Design	Improvement
Complexity	3965 cells	2186 cells	45 %
Area	5.75 μm^2	3.35 μm^2	42 %
Latency	8 cycles	3.25 cycles	59 %

A DPA procedure for QCA circuits is proposed, which has been adapted from the process used for CMOS-based devices. The proposed DPA procedure consists of the following five steps:

Step 1: The first step is to choose a target key-dependent intermediate result which is generated by the cryptographic circuit. This intermediate signal should be a function of a known non-constant data value (the plaintext or the ciphertext) and a small part of the key. In a block cipher, a submodule which includes the S-boxes is usually chosen. In this paper, the intermediate result under attack is a submodule of the Serpent cipher with its S_0-box, which is

$$\text{Intermediate Result} = \hat{S}_0\left(\hat{B}_0 \oplus \hat{K}_0\right). \tag{18}$$

Step 2: The second step is to measure the power consumption while the cryptographic circuit encrypts the plaintext or decrypts the ciphertext. To perform this step in this paper, $n+1$ random inputs, $\vec{B}$, are applied to the implemented Serpent submodule

$$\vec{B} = (b_0, b_1, \ldots, b_n)' \tag{19}$$

where b_i denotes the data value in the ith encryption or decryption process. For each switching between two inputs, the power consumption $\vec{P}$ is measured by QCAPro and stored as

$$\vec{P} = (p_0, p_1, \ldots, p_{n-1})'. \tag{20}$$

Step 3: The third step is to calculate a hypothetical intermediate value for every possible choice of the key vector $\vec{K}$. In this paper, all possible keys in the key vector are expressed as $\vec{K} = (0, 1, 2, \ldots, 15)$. Each possible key element in the key vector is referred to as a key guess or a key hypothesis. An attacker can calculate hypothetical values for the intermediate result chosen in Step 1 for all random inputs and for all key guesses. The calculation results in a matrix $\boldsymbol{V}_{(n+1)\times(16)}$ with each element calculated as

$$v_{i,j} = \hat{S}_0\left(b_i \oplus k_j\right), i = 0, 1, \ldots, n; j = 0, 1, \ldots, 15. \tag{21}$$

The jth column of $\boldsymbol{V}$ includes the intermediate results calculated with the key guess k_j. As $\vec{K}$ contains all possible keys, the real key used in the cryptographic circuit is one element of the key vector $\vec{K}$. The aim of DPA is to find out which column of the

matrix $\boldsymbol{V}$ has actually been processed during the encryption or decryption. Therefore, one column of $\boldsymbol{V}$ will be most highly correlated with the correct key guess.

Step 4: The next step is to map the hypothetical intermediate values in $\boldsymbol{V}$ to a matrix $\boldsymbol{H}_{(n)\times(16)}$ of hypothetical power consumption values. The elements in the hypothetical power consumption matrix $\boldsymbol{H}_{(n)\times(16)}$ are usually the HW or HD of the hypothetical intermediate values in matrix $\boldsymbol{V}$. The HD is used in this paper, as the total power of QCA circuits heavily depends on the HD between two consecutive inputs, which has been clearly shown in Section II-C. The HD model requires both previous and current values of the target intermediate result. Therefore, the calculation of the hypothetical power from hypothetical intermediate values is expressed as follows:

$$h_{i,j} = \mathrm{HW}\left(v_{i,j} \oplus v_{i+1,j}\right), i = 0, 1, \ldots, n-1; j = 0, 1, \ldots, 15. \tag{22}$$

A larger HD usually leads to higher power consumption.

Step 5: In the last step, the hypothetical power values are compared with the measured power data. The attacker compares the hypothetical power values of each key guess with the measured power data at every position by comparing each column $\vec{\boldsymbol{h}}_j$ of matrix $\boldsymbol{H}$ with the measured power $\vec{P}$. Pearson's correlation function [42] is applied to calculate the correlation coefficient between the hypothesis and the more accurate power data. The comparison result is a vector $\vec{R}$ of correlation coefficients with each element calculated as follows:

$$r_j = \frac{\sum_{i=0}^{n-1}\left(h_{i,j} - \bar{h_j}\right) \times \left(p_i - \bar{p}\right)}{\sqrt{\sum_{i=0}^{n-1}\left(h_{i,j} - \bar{h_j}\right)^2 \times \sum_{i=0}^{n-1}\left(p_i - \bar{p}\right)^2}}, j = 0, 1, \ldots, 15 \tag{23}$$

where $\bar{h_j}$ and $\bar{p}$ denote the mean values of column $\vec{\boldsymbol{h}}_j$ and the power vector $\vec{P}$, respectively. In a successful attack, the highest value of correlation coefficient corresponds to the correct key guess.

A diagram of the DPA procedure for QCA circuits is shown in Fig. 13. For more information on DPA, please refer to [28].

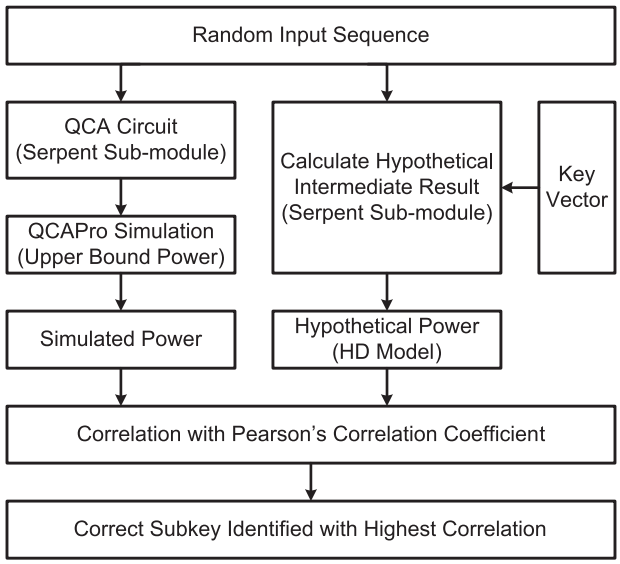


Fig. 13. Outline of the DPA procedure for QCA circuits.

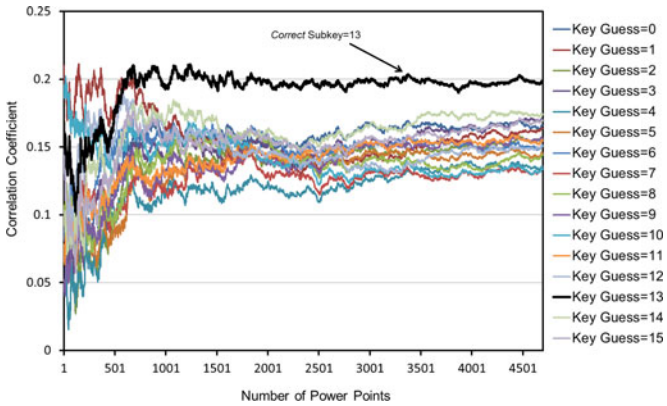


Fig. 14. Correlation results for DPA attack of Serpent submodule ($T = 2.0$ K, $\gamma = 1.0\,E_k$).

B. DPA Attack of the Serpent Submodule

Here, the results of the first power analysis attack of a QCA cryptographic circuit using the upper bound power model are presented. The Serpent submodule inputs and a SK are XORed before being passed to the S-box transformation. All possible combinations of S_0-box inputs are simulated by QCAPro and the corresponding power consumption values are shown in Appendix I. Following the DPA attack steps, the Serpent submodule is attacked and the correlation results are shown in Fig. 14. It can be seen that the correct key guess 13 is clearly distinguishable from wrong key guesses after 1000 inputs. Therefore, since one SK can be revealed, the whole Serpent key set can also be revealed using this power analysis attack.

To illustrate that all of the possible SKs from "0000" to "1111" will result in a distinguishable correlation coefficient, they were applied to the Serpent submodule and DPA attacks were carried out. The results are shown in Fig. 15. All SK correlation coefficients vary between 0.16 and 0.25 and the number of power points required to reveal the SK from the incorrect key guesses varies between 200 and 2000. Therefore, with just 2000 power points, all of the Serpent SKs can be revealed. In Fig. 15, for each SK applied to the submodule, the correlation coefficients of all key guesses are shown in the vertical direction, which are chosen when the number of power points is 2000. For example, the correlation coefficients for all key guesses when the correct SK is 13 in Fig. 15 are a cross section of Fig. 14 taken at 2000 power points. For every case, each correct key guess may have a different correlation coefficient value, but it will be significantly higher than the correlation coefficients of the wrong key guesses.

An observation is that all of the correlation coefficients are much lower than 1. The reason for this is that the power data simulated by QCAPro are the total power consumed by the submodule over one clock cycle. Therefore, some power information that is not related to the target intermediate value is also included in the total power.

The vulnerability of the circuit is due to the close relationship between the processed key-related information and the

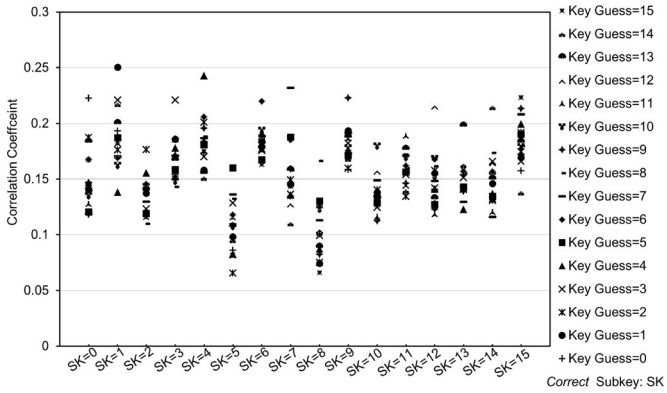


Fig. 15. Correlation of *Correct* SK with all possible key guesses applied to the Serpent submodule ($T = 2.0$ K, $\gamma = 1.0\,E_k$). The results in each column can be visualized as a cross section of results equivalent to that shown in Fig. 14 for each *correct* SK at 2000 power points.

corresponding power dissipation. Generally, if more cells or gates are involved in this processing, it is easier for an attacker to perform a power analysis attack.

V. Discussion of Practical QCA Devices

The upper bound power model has been derived for semiconductor QCAs; however, it can be extended for molecular and magnetic QCAs by using the appropriate Hamiltonian in the derivation [26]. Therefore, the best case scenario of power analysis attack results obtained in this paper can also be applied to other QCA implementations. Although the power consumption in QCA is very low in terms of its absolute value, for power analysis attacks, it is the power difference between transitions from "0" → "0" (or "1" → "1") and "0" → "1" (or "1" → "0") that is important since it indicates a power dependence on the processed data. It has been shown that cryptographic algorithms implemented in QCA with typical four-phase clocking could be vulnerable to power analysis attack. However, this result is for a best case scenario for attackers which assumes nonadiabatic switching.

In a more typical scenario, a smoother clock would be used, which would reduce the power consumption of transitions from $0 \rightarrow 1$ (or $1 \rightarrow 0$) significantly [26]. As shown in Fig. 4, the real power consumption will be lower than the upper bound. The difference between the dynamic power and static power is less and the power dependence on the HD of the inputs is also reduced. This will require more power data to reveal the key, which would enhance the security. Also, no noise is considered in this paper. In a practical situation, noise will be present when measuring the power consumption, which will affect the power analysis attack. Therefore, in practice using a smoother clock, the security of QCA cryptographic circuits would be greatly enhanced in comparison to CMOS-based equivalent circuits. Also, even if the power dependence on processed data is still measurable under a smoother clock, the measurement of power consumption with a magnitude of a fraction of an electron volt is very difficult and expensive. Power analysis attacks were proposed as a cheap attack technique using readily accessible equipment. Therefore, this may not be the case for future QCA devices.

VI. Worst Case Scenario for Attackers-Bennett Clocking

QCA circuits which use typical quasi-adiabatic clocking are performing irreversible computing. Landauer has shown that any logically irreversible operation must dissipate at least $K_B T ln(2)$ per bit, independent of the operation speed [43]. However, if a copy of the bit to be erased is reserved, the operation can dissipate an arbitrarily small amount of energy [44]. Furthermore, Bennett extended Landauer's theory by showing that any computation could be implemented as a logically reversible operation [45]. In this research, the logically irreversible clocking is referred to as Landauer clocking which is the typical quasi-adiabatic four-phase clocking and the logically reversible clocking is referred to as Bennett clocking. Although the reversible computing theory has been proposed for almost four decades, no concrete circuits exist as they are infeasible to implement in CMOS due to the complexity involved in their design. However, QCA technology provides a practical platform for the realization of reversible computing without the requirement for additional circuit complexity [27], [46], [47]. Here, the vulnerability of QCA circuits under Bennett clocking [45] to power analysis attack is considered as the worst case scenario for attackers.

The wave of Bennett clocking used in this study is described as follows [27]:

$$E_c(x,t) = E_C^0 \min\left[\left(1 - \frac{x}{\lambda_c}\right) + sin\left(\frac{t}{T_c}\right), 1\right] \qquad (24)$$

where x is the position of the bit information, t is the time, λ_c is the spatial width of the Bennett-clocked region, and T_c is the temporal clocking period. The lower bound power is modeled by describing the relevant physics of QCA switching in a thermal environment, which is illustrated in detail by Lent *et al.* [27]. To implement QCA circuits with Bennett clocking as shown in (24), only the timing of the clocking signals needs to be altered, in order to keep the bit information in place using the clock until a computational block is finished; then, the information is erased during the reverse order of computation.

It has already been demonstrated that a QCA OR gate using Bennett clocking produces very low and very similar power consumption values for inputs with different HDs [27], which is shown in Fig. 16. From this figure, it is clear that the power dissipated in the Bennett-clocked QCA OR gate during input changes is extremely low, even lower than the bit erasure energy, i.e., $K_B T ln(2)$. Compared with the Landauer-clocked OR gate, the most important point is that there is almost no power difference for a Bennett-clocked OR gate between the input changes from "1" to "1" and "1" to "0.' Therefore, by using Bennett clocking, the power dependence of basic gates on the inputs is effectively removed making it impossible to perform a power analysis attack albeit at the cost of speed. As a result, a cryptographic circuit design using Bennett clocking in QCA would act as a natural countermeasure to power analysis attacks.

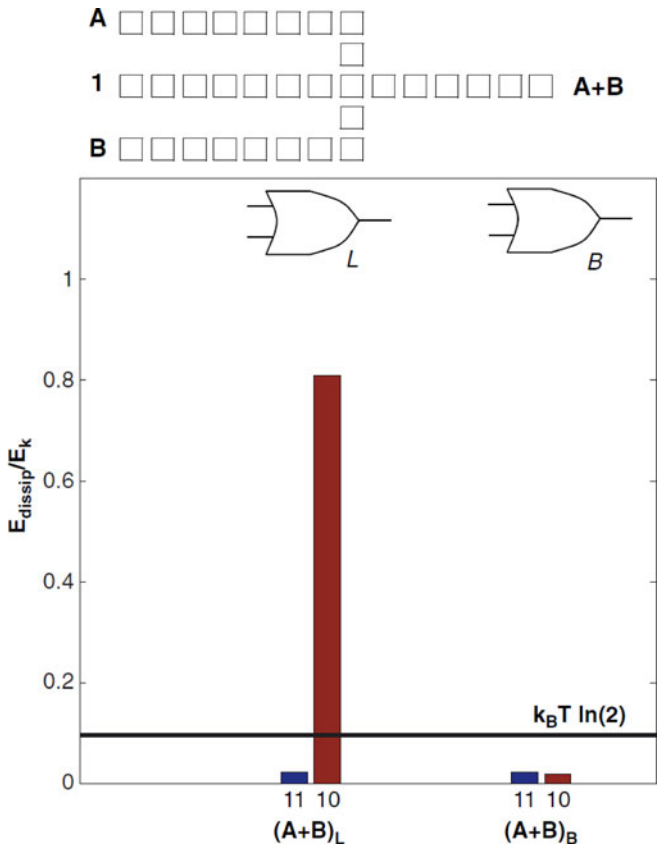


Fig. 16. Calculated power dissipation of QCA OR gate for Landauer-clocked (L) and Bennett-clocked (B) OR gates [27].

VII. Conclusion

An investigation into the resistance of QCA cryptographic circuits to power analysis attacks is presented under both the best case and the worst case scenarios from an attackers' point of view.

Based on the upper bound power model, the power dependence on HD in basic QCA gates including majority gates and inverters has been shown. An efficient design of the Serpent S_0-box is presented with a reduction of 45%, 42%, and 59% in terms of number of cells, area, and latency, respectively, over previous work. The power consumption of the Serpent submodule is simulated using QCAPro based on the upper bound power model. A power analysis attack procedure for QCA is proposed to reveal the secret key by statistically comparing the power consumption and all hypothetical key guesses. The first power analysis attack of a QCA cryptographic circuit is presented under a best case scenario (for the attacker). A DPA attack of the Serpent submodule is performed and the results show that all possible SKs of Serpent can be revealed by power analysis attacks. Therefore, QCA cryptographic circuits under quasi-adiabatic switching could be vulnerable to power analysis attack. However, the security of QCA circuits can be improved greatly by applying a smoother clock.

In the worst case scenario (for the attacker), QCA cryptographic circuits can be designed with reversible computing using Bennett clocking, which removes the power dependence on the basic gates, making power analysis attack impossible. Therefore, a Bennett-clocked QCA circuit design could be used to prevent power analysis attacks. It is believed that QCA could be attractive for the implementation of security architectures resistant to power analysis attack in the future.

TABLE V
Power Consumption of S_0-Box for All Possible Input Switching ($T = 2.0$ K, $\gamma = 1.0\,E_k$, Unit of Power Consumption: eV)

Input	0	1	2	3	4	5	6	7
0	3.54	5.01	5.06	6.05	5.58	6.59	6.93	7.31
1	5.04	3.55	6.15	4.93	6.02	5.44	7.31	6.47
2	5.10	6.15	3.55	4.97	6.83	7.30	5.47	6.34
3	14.40	13.79	12.09	11.45	7.25	6.49	6.13	5.23
4	14.08	13.58	14.19	13.73	3.55	4.90	5.20	5.95
5	11.62	11.48	13.71	13.54	4.90	3.54	5.86	4.91
6	13.19	12.36	12.63	12.33	5.20	5.88	3.55	4.82
7	13.95	13.65	11.48	11.37	5.94	4.92	4.82	3.55
8	12.37	12.29	12.71	12.37	6.84	7.76	8.34	8.76
9	11.93	11.29	14.38	13.56	7.40	6.84	8.63	7.80
10	12.53	12.32	12.26	12.38	7.94	8.60	6.96	7.64
11	14.14	13.29	11.83	11.15	8.46	7.66	7.61	6.61
12	14.19	13.52	14.37	13.64	5.03	6.20	6.62	7.19
13	11.47	11.23	13.76	13.30	6.02	5.04	7.14	6.20
14	13.14	11.93	12.77	12.04	6.46	7.17	5.18	6.05
15	13.82	13.17	11.38	11.10	7.06	6.21	6.10	5.05

TABLE VI
Power Consumption of S_0-Box for All Possible Input Switching (Continued)

Input	8	9	10	11	12	13	14	15
0	5.17	6.39	6.56	7.46	7.03	7.92	8.35	8.84
1	6.06	4.92	7.00	6.16	7.29	6.50	8.36	7.52
2	6.68	7.54	5.26	6.40	14.40	13.79	12.09	11.45
3	7.34	6.27	6.03	5.01	14.08	13.58	14.19	13.73
4	6.83	7.42	7.93	8.44	11.62	11.48	13.71	13.54
5	7.77	6.84	8.54	7.63	13.19	12.36	12.63	12.33
6	8.37	8.69	6.95	7.61	13.95	13.65	11.48	11.37
7	8.74	7.81	7.59	6.61	12.37	12.29	12.71	12.37
8	3.55	4.87	5.04	5.93	11.93	11.29	14.38	13.56
9	4.88	3.55	5.82	4.97	12.53	12.32	12.26	12.38
10	5.08	5.82	3.56	4.72	14.14	13.29	11.83	11.15
11	5.97	4.98	4.71	3.55	14.19	13.52	14.37	13.64
12	5.55	5.91	6.66	7.12	11.47	11.23	13.76	13.30
13	6.37	5.31	7.05	6.19	13.14	11.93	12.77	12.04
14	6.92	7.01	5.47	6.07	13.82	13.17	11.38	11.10
15	7.29	6.33	6.10	5.18	5.77	4.71	4.60	3.55

Appendix

The power consumption of the Serpent S_0-box for all possible input switching is shown in Tables V and VI. The left vertical column of the table represents the current input and the top horizontal row represents the next input.

References

[1] C. S. Lent, P. D. Tougaw, W. Porod, and G. H. Bernstein, "Quantum cellular automata," *Nanotechnology*, vol. 4, no. 1, pp. 49–57, 1993.
[2] C. S. Lent and P. D. Tougaw, "A device architecture for computing with quantum dots," *Proc. IEEE*, vol. 85, no. 4, pp. 541–557, Apr. 1997.

[3] A. O. Orlov, I. Amlani, G. H. Bernstein, C. S. Lent, and G. L. Snider, "Realization of a functional cell for quantum-dot cellular automata," *Science*, vol. 277, no. 5328, pp. 928–930, 1997.
[4] I. Amlani, A. O. Orlov, G. Toth, G. H. Bernstein, C. S. Lent, and G. L. Snider, "Digital logic gate using quantum-dot cellular automata," *Science*, vol. 284, no. 5412, pp. 289–291, 1999.
[5] V. Arima, M. Iurlo, L. Zoli, S. Kumar, M. Piacenza, F. Della Sala, F. Matino, G. Maruccio, R. Rinaldi, F. Paolucci, M. Marcaccio, P. G. Cozzi, and A. P. Bramanti, "Toward quantum-dot cellular automata units: Thiolated-carbazole linked bisferrocenes," *Nanoscale*, vol. 4, no. 3, pp. 813–823, 2012.
[6] S. E. Frost, A. F. Rodrigues, A. W. Janiszewski, R. T. Rausch, and P. M. Kogge, "Memory in motion: A study of storage structures in QCA," in *Proc. 1st Workshop Non-Silicon Comput.*, 2002, vol. 2, pp. 30–37.
[7] V. Vankamamidi, M. Ottavi, and F. Lombardi, "A line-based parallel memory for QCA implementation," *IEEE Trans. Nanotechnol.*, vol. 4, no. 6, pp. 690–698, Nov. 2005.
[8] K. Walus, M. Mazur, G. Schulhof, and G. A. Jullien, "Simple 4-bit processor based on quantum-dot cellular automata (QCA)," in *Proc. 16th IEEE Int. Conf. Appl.–Specific Syst., Archit. Process.*, Jul. 2005, pp. 288–293.
[9] I. Hanninen and J. Takala, "Pipelined array multiplier based on quantum-dot cellular automata," in *Proc. 18th Eur. Conf. Circuit Theory Design*, 2007, pp. 938–941.
[10] H. Cho and E. E. Swartzlander, Jr., "Adder and multiplier design in quantum-dot cellular automata," *IEEE Trans. Comput.*, vol. 58, no. 6, pp. 721–727, Jun. 2009.
[11] E. E. Swartzlander, Jr., H. Cho, I. Kong, and S. W. Kim, "Computer arithmetic implemented with QCA: A progress report," in *Proc. Conf. Rec. 44th Asilomar Conf. Signals, Syst. Comput.*, 2010, pp. 1392–1398.
[12] L. Lu, W. Liu, M. O'Neill, and E. E. Swartzlander, Jr., "QCA systolic matrix multiplier," in *Proc. IEEE Annu. Symp. VLSI*, Jul. 2010, pp. 149–154.
[13] M. T. Niemier and P. M. Kogge, "Problems in designing with QCAs: Layout= timing," *Int. J. Circuit Theory Appl.*, vol. 29, no. 1, pp. 49–62, 2001.
[14] R. Zhang, K. Walus, W. Wang, and G. A. Jullien, "A method of majority logic reduction for quantum cellular automata," *IEEE Trans. Nanotechnol.*, vol. 3, no. 4, pp. 443–450, Dec. 2004.
[15] S. Srivastava, S. Bhanja, "Hierarchical probabilistic macromodeling for QCA circuits," *IEEE Trans. Comput.*, vol. 56, no. 2, pp. 174–190, Feb. 2007.
[16] M. Choi, Z. Patitz, B. Jin, F. Tao, N. Park, and M. Choi, "Designing layout-timing independent quantum-dot cellular automata (QCA) circuits by global asynchrony," *J. Syst. Archit.*, vol. 53, no. 9, pp. 551–567, 2007.
[17] W. Liu, L. Lu, M. O'Neill, E. E. Swartzlander, Jr., and R. Woods, "Design of quantum-dot cellular automata circuits using cut-set retiming," *IEEE Trans. Nanotechnol.*, vol. 10, no. 5, pp. 1150–1160, Sep. 2011.
[18] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Proc. Annu. Int. Cryptol. Conf. Adv. Cryptol.*, 1996, pp. 104–113.
[19] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Side channel cryptanalysis of product ciphers," in *Proc. Eur. Symp. Res. Comput. Security*, 1998, pp. 97–110.
[20] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Int. Cryptol. Conf. Adv. Cryptol.*, 1999, pp. 789–789.
[21] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.
[22] O. X. Standaert, E. Peeters, G. Rouvroy, and J. J. Quisquater, "An overview of power analysis attacks against field programmable gate arrays," *Proc. IEEE*, vol. 94, no. 2, pp. 383–394, Feb. 2006.
[23] J. Timler and C. S. Lent, "Power gain and dissipation in quantum-dot cellular automata," *J. Appl. Phys.*, vol. 91, no. 2, pp. 823–830, 2002.
[24] J. Timler and C. S. Lent, "Maxwell's demon and quantum-dot cellular automata," *J. Appl. Phys.*, vol. 94, no. 2, pp. 1050–1060, 2003.
[25] L. Bond and M. Macucci, "Analysis of power dissipation in clocked quantum cellular automaton circuits," in *Proc. 36th Eur. Solid-State Device Res. Conf.*, 2006, pp. 57–60.
[26] S. Srivastava, S. Sarkar, and S. Bhanja, "Estimation of upper bound of power dissipation in QCA circuits," *IEEE Trans. Nanotechnol.*, vol. 8, no. 1, pp. 116–127, Jan. 2009.
[27] C. S. Lent, M. Liu, and Y. Lu, "Bennett clocking of quantum-dot cellular automata and the limits to binary logic scaling," *Nanotechnology*, vol. 17, pp. 4240–4251, 2006.
[28] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. New York: Springer-Verlag, 2007.
[29] S. Srivastava, A. Asthana, S. Bhanja, and S. Sarkar, "QCAPro-an error-power estimation tool for QCA circuit design," in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2011, pp. 2377–2380.
[30] E. P. Blair, E. Yost, and C. S. Lent, "Power dissipation in clocking wires for clocked molecular quantum-dot cellular automata," *J. Comput. Electron.*, vol. 9, no. 1, pp. 49–55, 2010.
[31] C. S. Lent and P. D. Tougaw, "Lines of interacting quantum-dot cells: A binary wire," *J. Appl. Phys.*, vol. 74, no. 10, pp. 6227–6233, 1993.
[32] K. Walus, T. J. Dysart, G. A. Jullien, and R. A. Budiman, "QCADesigner: A rapid design and simulation tool for quantum-dot cellular automata," *IEEE Trans. Nanotechnol.*, vol. 3, no. 1, pp. 26–31, Mar. 2004.
[33] S. Morioka and A. Satoh, "An optimized S-Box circuit architecture for low power AES design," in *Proc. Int. Workshop Cryptograph. Hardware Embedded Syst.*, 2003, pp. 271–295.
[34] E. Prouff, "DPA attacks and S-boxes," in *Proc. Int. Conf. Fast Software Encryption*, 2005, pp. 424–441.
[35] K. H. Boey, P. Hodgers, Y. Lu, M. O'Neill, and R. Woods, "Security of AES S-box designs to power analysis," in *Proc. 17th IEEE Int. Conf. Electron., Circuits, Syst.*, 2010, pp. 1232–1235.
[36] R. Anderson, E. Biham, and L. Knudsen, "Serpent: A proposal for the advanced encryption standard," in *Proc. 1st Adv. Encrypt. Stand. (AES) Candidate Conf.*, Ventura, CA, Aug. 20–22, 1998. [Online]. Available: http://www.cl.cam.ac.uk/∼rja14/serpent.html
[37] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, and E. Roback, "Report on the development of the advanced encryption standard (AES)," *J. Res.—Nat. Inst. Stand. Technol.*, vol. 106, no. 3, pp. 511–576, 2001.
[38] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, "Leakage power analysis attacks: A novel class of attacks to nanometer cryptographic circuits," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 57, no. 2, pp. 355–367, Feb. 2010.
[39] K. Kong, Y. Shang, and R. Lu, "An optimized majority logic synthesis methodology for quantum-dot cellular automata," *IEEE Trans. Nanotechnol.*, vol. 9, no. 2, pp. 170–183, Mar. 2010.
[40] M. Amiri, M. Mahdavi, and S. Mirzakuchaki, "Logic-based QCA realization of a 4× 4 S-Box," in *Proc. Int. Conf. Comput. Appl. Ind. Electron.*, 2010, pp. 415–420.
[41] W. Liu, L. Lu, M. O'Neill, and E. E. Swartzlander, Jr., "Design rules for quantum-dot cellular automata," in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2011, pp. 2361–2364.
[42] J. L. Rodgers and W. A. Nicewander, "Thirteen ways to look at the correlation coefficient," *Amer. Statist.*, vol. 42, no. 1, pp. 59–66, 1988.
[43] R. Landauer, "Irreversibility and heat generation in the computing process," *IBM J. Res. Develop.*, vol. 5, no. 3, pp. 183–191, 1961.
[44] R. W. Keyes and R. Landauer, "Minimal energy dissipation in logic," *IBM J. Res. Develop.*, vol. 14, no. 2, pp. 152–157, 1970.
[45] C. H. Bennett, "Logical reversibility of computation," *IBM J. Res. Develop.*, vol. 17, no. 6, pp. 525–532, 1973.
[46] M. Ottavi, S. Pontarelli, E. DeBenedictis, A. Salsano, P. Kogge, and F. Lombardi, "High throughput and low power dissipation in QCA pipelines using Bennett clocking," in *Proc. IEEE/ACM Int. Symp. Nanoscale Archit.*, Jun. 2010, pp. 17–22.
[47] M. Ottavi, S. Pontarelli, E. DeBenedictis, A. Salsano, S. Frost-Murphy, P. Kogge, and F. Lombardi, "Partially reversible pipelined QCA circuits: Combining low power with high throughput," *IEEE Trans. Nanotechnol.*, vol. 10, no. 6, pp. 1383–1393, Nov. 2011.

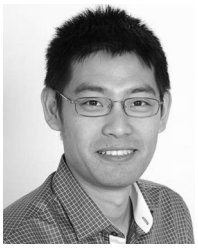
Weiqiang Liu (S'10) received the Bachelor's degree in electronic engineering (information engineering) from the Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing, China, and the Ph.D. degree in electronic engineering from Queen's University Belfast (QUB), Belfast, U.K., in 2006 and 2012, respectively.

He is currently a Research Fellow in the Institute of Electronics, Communications and Information Technology, QUB. He was a Postgraudate Student and Research Assistant with the DSP Solution Lab in NUAA from 2006 to 2009, where he was working on field-programmable gate array, Microcontroller, and DSP hardware design for signal processing. His research interests include quantum-dot cellular automata circuit designs, very large scale integration circuit designs for signal processing, and cryptographic applications.

Saket Srivastava received the B.E. degree in electrical and electronics engineering from the National Institute of Technology, Trichy, Tiruchirappalli, India, in 2003, and the Ph.D. degree in electrical engineering from the University of South Florida, Tampa, in 2008.

Since 2010, he has been an Assistant Professor at the Indraprastha Institute of Information Technology, Delhi (IIITD), Delhi, India. Prior to that, he was a Postdoctoral Research Fellow in the School of Electronics and Computer Science, University of Southampton, U.K., from 2008 to 2010. His current research interests include probabilistic modeling of emerging nanoelectronic devices, computer-aided design tools for nano/molecular circuit design, and software-defined radios.

Dr. Srivastava serves on the technical program committee for International Symposium on Electronic System Design and IEEE Computer Society Annual Symposium on VLSI. He has also served on the technical program committees of Frontiers in Education Conference and Design Automation and Test in Europe and is a reviewer for leading international journals and conferences.



Liang Lu received the B.Sc. degree in telecommunication engineering and M.Sc. degree in signal processing both from Zhejiang University, Hangzhou, China, in 2001 and 2004, respectively, and the Ph.D. degree in electronic engineering from Queen's University Belfast (QUB), Belfast, U.K., in 2008.

He is currently a Leading Design Engineer in Imagination Technologies, Kings Langley, U.K. He was a Research Fellow in the Institute of Electronics, Communications and Information Technology, QUB, from 2008 to 2012. His research interests include quantum-dot cellular automata system design, very large scale integration architecture design in video, and cryptographic applications.

Máire O'Neill (née McLoone) (M'03–SM'11) received the M.Eng. degree with distinction and the Ph.D. degree in electrical and electronic engineering from Queen's University Belfast, Belfast, U.K., in 1999 and 2002, respectively.

She is currently a Chair of Information Security at Queen's University Belfast and holds an EPSRC Leadership fellowship to conduct research into next-generation data security architectures. She previously held the U.K. Royal Academy of Engineering research fellowship from 2003 to 2008. She has authored a research book and has more than 90 peer-reviewed conference and journal publications. Her research interests include hardware cryptographic architectures, lightweight cryptography, side channel attacks and countermeasures, physical unclonable function, and quantum-dot cellular automata circuit design.

Prof. O'Neill was the Guest Editor of the launch issue of IET Information Security in 2005 and is currently an Editorial Board member for the *International Journal of Reconfigurable Computing*. She is an IEEE Circuits and Systems for Communications Technical committee member and was a Treasurer of the Executive Committee of the IEEE UKRI Section from 2008 to 2009. She is a Fellow of the Higher Education Academy (HEA) and a member of the IET and the International Association for Cryptologic Research. She has received numerous awards for her research and in 2007 was named the British Female Inventor of the Year at the British Female Inventors and Innovators Network awards.

Earl E. Swartzlander, Jr. (S'64–M'72–SM'79–F'88–LF'11) received the B.S. degree from Purdue University, West Lafayette, IN, in 1967, the M.S. degree from the University of Colorado, Boulder, in 1969, and the Ph.D. degree from the University of Southern California, Los Angeles, in 1972, all in electrical engineering.

He is a Professor of electrical and computer engineering at the University of Texas at Austin, Austin. In his current position, he and his students conduct research in computer engineering with emphasis on application-specific processor design, including high-speed computer arithmetic, embedded processor architecture, very large scale integration (VLSI) technology, and nanotechnology. As of May 2012, he has supervised 35 Ph.D. students. From 1975 to 1990, he held a variety of positions at TRW including the Director of Independent Research and Development in the TRW Defense Systems Group, the Manager of the Digital Processing Laboratory in the Electronics and Technology Division, and the Manager of the Advanced Development Office in the System Development Division. He is the author of one book, editor of seven books, and the author or coauthor of 72 refereed journal papers, 35 book chapters, and 282 conference papers.

Dr. Swartzlander was the Editor-in-Chief of the IEEE TRANSACTIONS ON COMPUTERS from 1990 to 1994 and was the founding Editor-in-Chief of the *Journal of VLSI Signal Processing*. In addition, he has served as an Associate Editor for the IEEE TRANSACTIONS ON COMPUTERS, the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, and the IEEE JOURNAL OF SOLID-STATE CIRCUITS. He has been a member of the Board of Governors of the IEEE Computer Society from 1987 to 1991, the IEEE Signal Processing Society from 1992 to 1994, and the IEEE Solid-State Circuits Council/Society from 1986 to 1991. He has been a member of the IEEE History Committee from 1996 to 2004, the IEEE Fellows Committee from 2000 to 2003, the IEEE James H. Mulligan, Jr., Education Medal Committee from 2007 to 2011, and the IEEE Awards Planning and Policy Committee since 2011. He has chaired a number of conferences. He has been honored with the IEEE Third Millennium Medal, the Distinguished Engineering Alumnus Award from the University of Colorado, the Outstanding Electrical Engineer and Distinguished Engineering Alumnus Awards from Purdue University, and the IEEE Computer Society Golden Core Award.