# Power and Energy issues on lightweight cryptography

Antonio J. Acosta*, Erica Tena-Sánchez, Carlos J. Jiménez and José M. Mora

Instituto de Microelectrónica de Sevilla, Universidad de Sevilla/CSIC, Spain
{acojim,erica,cjesus,jmiguel}@imse-cnm.csic.es

* corresponding author: Antonio J. Acosta

Address:

Instituto de Microelectrónica de Sevilla
Universidad de Sevilla/CSIC
Av. Americo Vespucio s/n
Sevilla, 41012-Spain

Office : (+34) 954466666
Fax : (+34) 954466600
Email : acojim@imse-cnm.csic.es

Date of Receiving: **to be completed by the Editor**

Date of Acceptance: **to be completed by the Editor**

# Power and Energy issues on lightweight cryptography

Antonio J. Acosta*, Erica Tena-Sánchez, Carlos J. Jiménez and José M. Mora

***Abstract*** *— Portable devices as smartphones, smart cards and other embedded devices need encryption technology to guarantee security. Users store private data daily in electronic devices making use of cryptography to ensure data confidentiality, needing reliable authentication mechanisms. Typical encryption security is based on the usage of algorithms that are mathematically secure, but often requiring expensive computing and power resources. The implementation of security mechanisms on dedicated hardware has been shown as a first-order solution to achieve both required security and low power consumption with reduced resources, in the so-called lightweight cryptography. Upcoming Internet of Thing (IoT) is requiring such solutions extensively. Furthermore, the physical implementation of the encryption algorithm can leak side-channel information that can be used by an attacker to reveal secret key or private data. Therefore, the physical implementations of low-power cryptographic devices have to be carefully considered at algorithmic, circuit and layout levels, in order to be secure against active and passive attacks. A great effort has been recently devoted to the implementation of secure lightweight cryptography, occupying an increasingly large interest from academy and companies, to meet the challenges of IoT. The paper is a survey of i) lightweight cryptography algorithms; ii) techniques to reduce power applied to cryptohardware implementations; iii) vulnerability analysis of low-power techniques against side-channel attacks; and iv) the possibilities opened to emerging technologies and devices in the "More than Moore" scenario.*

***Keywords*** — Cryptography, lightweight cryptohardware, low power, secure hardware, emerging technologies

# 1 INTRODUCTION

In current Information and Communication Techonology (ICT)-based world, cyber-security plays a key-role in everyday life, being recognized as an inalienable right of people. As a foundation of cyber-security, cryptography is widely used for authentication and encryption purposes (smart cards, smartphones, etc), access control (restricted areas, car lock systems, etc), payment (e-commerce), e-voting systems, etc. [1, 2]. In the upcoming Internet of Things (IoT) world, the growing in endpoints takes place from the 12 billion units now installed up to 20 billion "things" that will ship in 2020, with about two-thirds of them consumer applications; whereas hardware spending on networked endpoints will reach 3 trillion USD [3, 4]. These numbers forecast a scenario where cryptographic hardware will provide solutions with an increasing demand of energy efficiency, hardware reliability, system integration, portability and security.

In this scenario, the involved hardware resources will be necessarily forced to operate under extremely low power consumption requirements, in order to accomplish portability and even battery-less autonomous operation in most cases, as for instance RFID tags, sensor nodes and smart cards. In those devices, the implementation of approved conventional cryptographic NIST standards, like the AES block cipher and the SHA-3 hash function, leads to unfeasible solutions in terms of hardware resources, timing performance, power and computing resource consumption [5]. This matter sets the start point for the Lightweight Cryptography, i.e., the subfield of cryptography aiming to provide solutions tailored for resource-constrained devices [5].

Cryptographic algorithms aim to convert secret data into an unreadable code for non authorized persons, protecting secret information from theft or alteration, and also enabling authentication. The encryption process converts plaintexts on ciphertexts using a key, and decryption retrieves plaintext using the same or another key. There are three main categories of encryption mechanisms: Secret/Symmetric Key Cryptography (SKC, the same key is used by sender and receiver), Public/Asymmetric Key Criptography (PKC, different keys are used) and Hash functions (no keys are used). In lightweight cryptography, the SKC mechanism is the most used, because the simplicity of algorithms and reduced cost of implementations. For this reason, in this paper only will be considered SKC solutions, which can be roughly classified in block ciphers and stream ciphers, depending on the way that data are encoded: bit by bit or through data blocks, see Figure 1 for clarification. Stream ciphers generate a keystream that is XORed (XOR operation) with the plaintext (pt) bit by bit. They implement some kind of feedback mechanism so that the keystream is continuously changing producing different ciphertexts (ct) for the same plaintext in each encryption, depending on the key, the initial value, and the encryption cycle. On the other hand, block ciphers encrypt one block of data at a time using the same key on each block.

In last years, a huge amount of references deal with conceptual, algorithmic, software, and hardware solutions that may be taken into account in lightweight cryptography, as it can be stated in some surveys [5-11]. Great effort has been devoted to provide and analyze lightweight solutions at all description levels. In this work we provide a brief overview of the power-related figures of crypto-hardware devices, with a special focus to the power and energy consumption of hardware-implemented lightweight cryptography algorithms, as well as the techniques to reduce power applied to cryptohardware implementations.

There exist several implementations of well known lightweight cryptographic algorithms that are especially conceived to use few resources [12-29]. A key point to select a specific algorithm, built either as a block or stream cipher, is the time needed to perform an encryption/decryption, as well as the energy needed to encrypt/decrypt the plaintext. The relationship between time and energy involved sets an interesting niche for low-power solutions.

Besides hardware resources, the most important requirement in a cipher is security that concerns two different issues. First, security strength is referred to the ability of the algorithm to keep protected the private information. Each existing algorithm has some inherent security according to both the mathematic encryption formulation and the key length, being obviously the cipher more secure as the key length increases. With current computer capabilities, key lengths below 56 bits are not secure at all. For lightweight cryptography, NIST recommends a 112-bit key to provide a good trade-off between hardware complexity and a reasonable level of security [5]. Even if a cryptographic algorithm is mathematically secure, its physical implementation leaks side-channel information that can be used by third parties to reveal secret information. This information can be exploited by the known as side-channel attacks (SCAs) and fault injection attacks, classified in Figure 2. Fault injection attacks are non-invasive active attacks that insert any kind of malfunction on the operation during encryption, using this wrong result to retrieve the secret key of a device. SCAs on cryptographic devices are non-invasive passive attacks that use certain physical information leaked during normal encryption such as power consumption [32], time delay [33], or electromagnetic radiation [34] to find the secret key. SCAs usually require minimal cheap equipment; hence they are easy to carry out and are a big threat for designers, thus being the most studied ones [31-34]. Thus, security concerns both the mathematic algorithm and its physical implementation. Hence, it is necessary to perform vulnerability analysis against side-channel attacks on lightweigth cryptohardware, being easy to understand the influence of low-power design techniques on such aspect.

Finally, to complete the snapshot of power-aware lightweight cryptography, the possibilities opened to emerging technologies and devices in the “More than Moore” scenario will be considered in near future. In parallel to quantum cryptography world, the design of cryptographic circuits using new devices is of maximum interest.

This survey is organized as follows. In Section 2 we revise the state of the art in lightweight power-reduced and energy-reduced stream and block ciphers at algorithmic, architectural and implementation level. Section 4 studies the effect of power reduction on vulnerability of ciphers against side-channel attacks. In Section V a prospection of ciphers based on next generation devices is foreseen. Conclusions and References close the paper.

## 2 POWER AND ENERGY IN LIGHTWEIGHT CRYPTOGRAPHY

In lightweight cryptography, the interest is mostly focused on algorithms combining security and reduced resources, mainly power or energy consumption. The power consumption depends on the algorithm itself, the design architecture and the implementation. Hence, for a selected algorithm, different implementation architectures lead to different power and energy consumptions. Finally, for a selected architecture, the hardware implementation may include techniques that reduce power consumption. In this section, we discuss power consumption at these three levels, considering both stream and block ciphers.

As mentioned in Section 1, stream ciphers are SKC ciphers that generate a keystream that is XORed with the plaintext to obtain the ciphertext (Figure 3). The keystream is generated serially, through a pseudorandom sequence generator fed with a random seed value: the secret Key and an Initialization Vector (IV) using linear and non-linear shift registers. On the other side, block ciphers operate on large blocks of digits with a fixed transformation that combine the plain text and the key with simple operations such as substitutions and permutations in multiple rounds (Figure 3).

Since stream and block ciphers are quite different at algorithmic, architectural and implementation levels, separated analysis of both types of ciphers are needed and considered.

### *2.1 Power consumption issues at algorithmic level*

The main aspects that influence the power consumption in lightweight cryptography at the algorithmic level, are related not only to the selection of the algorithm, but also to the size of the internal state for stream ciphers.

### *2.1.1 Stream ciphers algorithms*

The generation of the pseudorandom bit sequence is usually done using shift registers with linear and non-linear feedbacks [27]. Thus, the power consumption of a stream cipher will have a strong dependence on the size of the shift registers and the complexity of the feedback function.

The eSTREAM Project [28] was an initiative to select the most suited stream cipher for secure applications. A comparison of power consumed by Grain, Mickey and Trivium stream ciphers hardware implementations, finalist of eSTREAM Project, is made in [29]. While the key size for Trivium is 80 bits, for Mickey and Grain there are two different proposals, with key a size of 80 and 128 bits, what involves a different size of the state register. The results shown in Table 1 reflect the power consumption of the different proposals as presented in [29], but adding the number of bits of the state register and the power consumption per bit of the state register. As it can be seen in the table, the main contribution to power consumption comes from the bit count of the state register. The higher number of bits in the state register, the higher power consumption. The second factor influencing power is the complexity of the cipher's feedback function. Trivium has a simpler feedback function, so its power consumption per bit of the state register is smaller, but Mickey, with more complex feedback consumes more power per bit of the state register than the others.

### *2.1.2 Block cipher algorithms*

Block ciphers algorithms are more complex than stream ciphers ones. There are many proposals of block ciphers, which can be grouped in two families: Substitution-Permutation Networks (SPN) and Feistel Networks (FN) [9]. In an SPN, the cipher performs two operations: confusion and diffusion. A layer of Substitution boxes, known as Sboxes, performs confusion, which is simply a permutation of a small subset of data. Diffusion is achieved through the use of a permutation of the whole space, usually linear. In FN ciphers, data block is split into two equal pieces and the encryption is performed in multiple rounds, which implements permutation and combinations derived from the primary function or key. Considering only lightweight block ciphers, within the SPN category are Klein, LED, Present, Prince, Midori, and within FN are Hight, Simeck, Simon, Speck, Misty, Lblock, Piccolo.

The characteristics of proposed block ciphers, including power consumption, have been extensively analyzed. However, a fair comparison between all of them is not possible, by the use of different technologies and design options. In [7], Noekeon, Hight, Iceberg, Katan, Present and AES block ciphers were designed in a 65nm technology, taking the care in designing them with the same interface. In [8], the analysis of [7] was extended to include recent block ciphers, evaluating the area, power consumption and energy of eleven lightweight block ciphers, but using a 130 nm technology. In [9], a compilation of the data offered by several published surveys is made, offering a ranking of ciphers based on different factors. Klein, mCrypton, Prince, Noekeon and Present were selected as the least energy/bit ciphers, being all of them SPN ciphers. From these results, it seems that the SPN based ciphers have the best performance for the energy per bit parameter. However, the power-based classification includes the FN-type Hight cipher, with Katan and Present, in the ultra-low power ciphers category.

## *2.2 Factors related to power consumption at the architecture level*

### *2.2.1 Stream ciphers architectures*

As already mentioned, stream ciphers have an internal structure that is defined by the algorithm. The best way to decrease power consumption and specially, energy per bit, uses multi-bit stream ciphers, that is, stream ciphers which generate several bits in one clock cycle. These architectures maintain the size of the internal state but increments the number of bits used for feedback. So, in each clock cycle *n* bits are generated in parallel. Figure 4 shows a general multi-bit architecture for the Trivium stream cipher.

These architectures only increase the number of logic gates generating the feedback bits, whose power consumption is usually much lower than that of the shift registers. Therefore, in the multi-bit architectures, the power increases slightly, but the energy per bit, the most important merit factor in the lightweight cryptography decreases. [29] presents power results for multi-bit implementations of several stream ciphers summarized in Table II. It can be observed that in multi-bit architectures, although the power consumption increases as the number of bits generated in each clock cycle increases, the value of the energy per bit is reduced.

### *2.2.2 Block ciphers architectures*

Block ciphers perform a set of operations iteratively, carrying out a series of rounds that can be executed in a more parallel or a more serial way. As it is shown in Figure 3.b, implementation of block ciphers can execute each round in a clock cycle, called rolled implementations. But other implementations can execute several rounds in a clock cycle, known as unrolled versions, shown in Figure 5,. In general, rolled implementations need lower resources, but at the cost of more clock cycles to complete an encryption operation. From the point of view of power consumption or energy per bit, results may be different.

In [10], a comparison between different implementations of block ciphers is made, but only in terms of power and energy consumed. Their analysis is also carried out comparing different implementation architectures that involve the realization of circuits that require different numbers of clock cycles, not only comparing the power consumption of different ciphers, but also comparing the power consumption of different architectures for the same cipher, obtaining conclusions about the best architecture of implementation according to different parameters. A power consumption model for ciphers was developed, concluding that the energy consumed by a circuit during an encryption operation depends quadratically with the degree of unrolling. In tests performed on different ciphers, they obtain lower power and energy per bit for those implementations with fewer unrolled rounds and, therefore, a greater number of clock cycles to complete the encryption. The rolled implementations have less area, less power consumption and less energy per bit. But they expend more clock cycles to produce the output.

## *2.3 Factors related to power consumption at the implementation level*

In this subsection, we will concentrate on techniques for semicustom design methodology with optimizations which will be done at RTL and logic level.

The implementation and design aspects that influence power consumption are summarized in [17, 18]. On the one hand, the main parameters affecting dynamic power consumption are nodes capacitances in the implementation, supply voltage, operation frequency and switching activity. These elements play an important role to improve power efficiency. Different techniques that optimize previous parameters to reduce dynamic power consumption are presented in [17-23]. On the other hand, the leakage power is dominant in nanometric technologies, with contributions depending on the size of the circuit and the technology used.

Depending on the chosen cipher and the cryptographic application, several techniques for reducing dynamic and leakage power consumption can be applied, as it is shown below.

### *2.3.1 Low-power stream ciphers implementations*

Clock gating technique (Figure 6) has been applied in Grain and Trivium stream ciphers with radix-16, including some temporary registers to store intermediate results and additional signals to disable clock [17, 24]. The mean power consumption has been reduced significantly, down to 1.2 µW for Grain and 1.02 µW for Trivium, measured at 100 kHz.

Reducing switching activity has been applied in hardware implementation of the Trivium stream cipher [22, 23] with the parallelization technique (Figure 7). In [22] a low power version, synthesized in three technologies (180, 130 and 90 nm), showed that dynamic power consumption decreases in all cases, by a factor about 18-30%, although 4-7% additional standard cells are used, when comparing to the conventional implementation of Trivium. In [23], two versions of low power Trivium implementation using logic parallelization (named as MPLP and FPLP) were presented applying the same technique. Electrical and logical simulations were applied in a 350 nm standard cell technology in order to obtain precise power results. The improvement in dynamic power consumption was quite high (15-25%), at the reduced cost of additional 6% in area occupation.

In literature, few contributions about analyzing and reducing power consumption in ASIC implementations have been published. A summary of them is shown in Table III.

### *2.3.2 Block ciphers implementations*

For block ciphers, the block that plays a dominant role in the power consumption is the implementation of the substitution block S-box [8, 10], because of its size and complexity. Several styles for implementing the S-box are presented in the literature: look-up table (LUT), Canright, Decode Switch-Encode (DSE) and combinations of them, [16-19, 21, 25, 26]. Some of them have been shown more appropriated in terms of low power consumption. In [18] the hardware implementation of AES is optimized for low power using an S-Box implementation with combinational logic and pipelined to lower switching (glitching) activity. Furthermore, in order to reduce the signal activity, an advanced variant of sleep logic technique is applied. Whenever the output of a combinational circuit is not needed, changes of the input data will nevertheless cause switching activity. In order to prevent the undesired switching activity, the inputs of the combinational circuit are masked using AND gates and a sleep signal (Figure 6).

In [25], the DSE S-Box implementation limits the spurious switching activity by one-hot coding. In [21], the mixed design style for the S-box use gating in the inputs to reduce the signal activity. The AES design can save up-to 13 % in power consumption or 20-30% in energy consumption.

In [16], the LUT based S-box consumes much less energy as compared to the Canright S-box. In both the LUT and Canright architectures, the switching activity in the circuit is roughly proportional to the signal delay across the input and output ports. In the case for DSE S-box, it consumes much less energy because the total switching activity in the delay period is much lower. A design using 4-bit S-boxes is more efficient in terms of energy consumed per cycle than a design using 8-bit S-boxes. This is primarily due to the fact that a 4-bit S-box will typically have a lower signal delay as compared to an 8-bit S-box. In [16] when a series of S-boxes are connected sequentially; the energy consumed by each S-box in a given period of time is likely to be more than the previous S-box, as the switching activity of the S-boxes are likely to increase from the first to the last.

In [20], it is shown how clock gating, applied at round function level (Figure 8) can affect and improve the consumption of the most common lightweight block ciphers. Experimental results show that the technique is able to reduce the energy consumption in most block ciphers by over 60% while incurring only a minimal overhead in hardware (around 10-15%). This technique reduces principally the propagation of glitches across the unrolled implementation. In [17] this technique is also applied to block ciphers not specifically conceived to lightweight cryptography, as the case of AES cipher.

The average load capacitance on the chip increase as more gates are placed on the hardware implementation. Minimizing combinational and sequential cells is mandatory for low power concerns. In [19] cells with large driving strengths are minimized and thus power is reduced.

Logic depth in combinational circuits can negativelly affect power consumption, due to the different critical paths and the probability of glitches increases sharply which contribute to the power consumption [44]. In [7] different lightweight ciphers are compared in terms of the impact with the frequency and voltage scaling. The power consumption decreases in a non-linearly way with the supply voltage and the power reduction is also moderated by the critical path length increase.

Summarizing, although stream and block ciphers are quite different, it is possible to apply similar techniques on their hardware applications in order to reduce dynamic power consumption as minimizing combinational and sequential cells, applying clock gating, using sleep logic, minimizing switching activity and reducing depth of combinational logic. Reported improvements in power and energy are considerable, but additional work is needed for future applications.

## 3 SECURITY OF LIGHTWEIGHT CRYPTOGRAPHY AGAINST SIDE-CHANNEL ATTACKS

When designing lightweight cryptocircuits, it should be ensured a tradeoff between performance and resources for a required security level, that designers need to achieve. In this kind of applications, performance are usually expressed in terms of power and energy consumption, latency and throughput, the latter being not as restrictive parameter as the others, because in lightweight applications it is not a design goal. Hardware resources can be expressed as occupied area, equivalent gates, or slices in the case of FPGAs, and the available inputs/outputs for the application. In these cases, designers try to meet three design aspects namely security, cost and performance. As a rule, it is very difficult to achieve the three design goals, but easy to reach two of them. For example, the design techniques that improve the security of the system without performance degradations are always linked to an increase in area and therefore cost increase. In another case, an increase of the security without increasing costs can be achieved with a reduced performance design.

In previous sections, some power consumption reduction techniques for SKC lightweight ciphers have been shown, but it has not been analyzed how such low-power solutions affect the security of the implemented designs. It has been stated that the security against malicious attacks can be determined by the algorithm itself, the key length and the physical implementation of it [5], mostly vulnerable to SCAs. Among SCAs, the Differential Power Analysis (DPA) attacks exploiting the power consumption of the device during encryption have been shown as one of the most challenging threat that designers need to deal with [31]. Since Kocher presented the first DPA attack in 1999 [32], there have been numerous works revealing successful DPA attacks against both ASIC and FPGA hardware implementations of different algorithms either on block or stream ciphers [31, 32, 35-37].

Due to the enormous success of DPA attacks, several countermeasures have been presented to counteract them [30]. These countermeasures try to break the dependency between the processed data and the power consumption of the circuit during encryption and can be applied at different abstraction levels: at cell, gate or algorithm level as shown in Figure 9. At a cell level, depending on the used mechanism to break the data-power, the countermeasures can be classified as masking or hiding, being applicable to any stream or block cipher, because they are independent on the selected algorithm or architecture [30, 31].

Masking techniques try to remove the data dependency with power consumption by using a mask mixed with an intermediate value of the processed data [38, 39]. On the other hand, hiding focuses on raising the noise level in the system or seeks to have the same power consumption independently of the processed data, meaning that the system consumes the same amount of power regardless the processed data [40-43]. Hiding techniques appear to be more efficient than masking regarding security improvement, more specifically those applied at cell level known as Dual Precharge Logic (DPL) styles to achieve the same amount of power consumption per transition [30]. DPL gates compute always the output and its complementary, alternating precharge and evaluation phases, then having in all clock cycles one transition in the output node, achieving thus in all clock cycles the same power consumption independent on the data being processed (Figure 10a).

Among DPL families, there are solutions that can be used with standard-logic cells as for instance Wave Dynamic Differential Logic (WDDL) [40] or Masked Dual-rail Pre-charged Logic (MDPL) [41], applicable for both ASIC or FPGA implementations. Dedicated full-custom solutions for ASIC implementations are the ones that achieve the best results in terms of security, including several logic families as Sense Amplifier Based Logic (SABL) [42] which schematic is shown in Figure 10b or Dynamic Current Mode Logic (DyCML) [43], among others. Current-mode logics are a priori discarded for lightweight cryptography because of static power consumption. For the remaining, the main problem with these countermeasures is still the increase in area and power consumption when compared to standard-cell based ones, which can be alleviated using alternate strategies.

To remedy the high power consumption produced by DPL solutions, there exist some solutions: i) using power-optimized circuit proposals, as the one presented in [44]; ii) making use of alternative architectures, as the adiabatic one in [45, 46], iii) proposing new power-reduced DPL structures [47]. These alternatives achieve a reduction in the power consumption maintaining high security levels against SCAs.

To reduce area, the straightforward solution is the migration to deep nanometric technologies, where the open question [48] is how can be improved the power and area figures without degrading security metrics.

Despite its increment in cost, integrating cryptocircuits in advanced CMOS technologies, some factors may affect negatively or positively the security against DPA of secure cryptographic devices, are appearing. With nanometric technologies, the area and dynamic power consumption can be reduced, but other factors as leakage are becoming more and more important. In 45nm technologies and below, leakage can be greater than the dynamic power, for this reason, several attacks exploiting leakage have been presented [49-51].

The attacks exploiting leakage power during encryption are known as Leakage Differential Power Analysis (LDPA) attacks. These attacks are a real threat for security designers due to the fact that leakage is strongly data dependent. Since 2007, when the first LDPA attack was presented [49], several works with some theoretical and experimental LDPA attacks to different implementations have been presented [49-51]. To counteract LDPA attacks, several countermeasures have been proposed, for example in [52], authors present a LDPA countermeasure using standard cells, based on symmetric dual-rail logic (SDRL). It is shown how the security is improved, performing simulation and experimental based LDPA attacks over Sbox in AES implementations.

As referred, designing cryptocircuits in nanometric technologies has brought new threats, as new weaknesses are appearing. Thus, two significant effects have to be balanced: as technology shrinks, global consumption and delay figures decrease, meaning that secure information could be easier to hide but, in the other hand, leakage power is revealing sensible information. It is not demonstrated that the integration of the same cryptocircuits in two different technologies leads to better or worse security figures, but different. This is an open issue requiring additional work [48, 58].

Even so, we are reaching a point where reducing the dimensions to deep-nanometric technologies is not improving neither the security nor performance of the implemented designs, as we have seen that new attacks appear exploiting the leakage of information that were previously not relevant. For this reason, in last years few works have presented the first implementations of cryptographic circuits using emerging technologies.

## 4 EMERGING TECHNOLOGIES AND DEVICES IN THE "MORE THAN MOORE" SCENARIO

Advances in emerging post-CMOS technologies give new options to the designers to meet the mentioned three major goals that require lightweight applications such as security, cost and performance. While nanometric technologies try to maintain the expected performance of Moore's law by scaling and/or reducing power consumption, new technologies can provide novel devices that can be very beneficial for the development of new cell structures. These new implementations are intended to improve the performance while maintaining or even improving the security metrics against DPA attacks in lightweight cryptography applications.

In last years, several researchers studied the benefits for secure cryptographic applications of the unique I-V characteristics of emerging devices, which are not available with conventional MOSFET devices [53-57]. There are two categories when classifying the I-V characteristics: the first one includes those devices exhibiting tunnelable polarity, which appear in carbon nanotubes, graphene, silicon nanowire transistors (SiNW), and transition metal dichalcogenide (TMD) tunnel FETs (TFETs), being all already experimentally fabricated; in the second group are included devices with atypical switching behaviors like negative capacitance FETs and ionic FETs [53-55]. Among all of them, Tuneling FET devices are of special interest [54-56]. Especially, III-V TFETs appear more promising due to their higher conduction current. Compared to conventional CMOS transistor, the TFET has asymmetric doping where the source and drain are p-type or n-type doped, respectively. In TFET, a sub-60 mV/decade slope in the I-V characteristic can be achieved [55], thus enabling the supply voltage scaling to further address conventional CMOS challenges such as oxide breakdown.

Combining these emerging technologies with DPL-based CML gates as presented in [55,56], the implementation area of the KATAN32 block cipher is maintained equal but reducing the power consumption from 170.19 µW to 9.76 µW, for CMOS CML and TFET CML, respectively. The security evaluation of TFET CML implementation shows a clear DPA resistance when compared with the static TFET implementation, where a successful attack was carried out [55]. Thus both power reduction and security improvement are achieved.

Besides the possible approaches based on emerging technologies, the usage of FinFETs is becoming an appealing solution for lightweight cryptography. FinSAL adiabatic logic using FinFET transistors is presented in [57] as countermeasure against DPA attacks, the generic FinSAL and the FinSAL inverter schematics are shown in Figure 11a and 11b respectively. Authors reduce the energy of the implemented Sbox circuit from 360 pJ (obtained from the conventional FinFET implementation) to 58 pJ for their FinSAL implementation. In the case of the security evaluation, authors retrieve the correct key for the conventional FinFET circuit but not for the FinSAL implementation, achieving higher security level.

With this information is clear that emerging technologies offer advantages due to their I-V characteristics that can be exploited to design new topologies to improve the DPA resilience and performance of lightweight cryptographic devices. The work developed in the future on this topic will be of maximum interest for cryptohardware community.

## 5 CONCLUSIONS

Incorporating cryptography in modern electronics systems is probably the main challenge in security of current Information Society. Data privacy, authentication and confidentiality are recognized between the most valuable rights of people. Low-power electronics plays an irreplaceable role in this topic, through the implementation of cryptographic algorithms in portable circuits and systems, in the so-called lightweight cryptography, mainly in the IoT scenario. This paper has reviewed the state of the art focuses on stream and block ciphers, their implementation and the ways of reducing power and energy. Furthermore, the relationship between security and power reduction has been analyzed and finally, the expected evolution within emerging technologies has been visited. Open issues have been mentioned and opportunities for new investigations have been presented, encouraging the low-power community to participate in.

# REFERENCES

[1] S. Vaudenay, A classical introduction to cryptography. Springer (**2006**).

[2] J. Katz and K. Lindell, Introduction to modern cryptography. CRC Press (**2015**).

[3] Goldman Sachs. (**2017**) The 5G Revolution: The Internet of Things Meets Everything [Online]. Available: www.goldmansachs.com/our-thinking/pages/iot-meets-everything.html. Last accessed March 31, 2017

[4] Gartner, Inc. (**2017**) [Online]. Available: www.gartner.com/technology/research/internet-of-things Last accessed March 31, 2017

[5] K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha, "Report on Lightweight Cryptography," NIST DRAFT NISTIR, 8114 (**2016**).

[6] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and Leif Uhsadel, "A Survey of Lightweight-Cryptography Implementations," IEEE Design and Test of Computers (**2007**), Vol. 24, Nº 6, pp. 522-533.

[7] S. Kerckhoff, F. Durvaux, C. Hocquet, D. Bol, and F-X. Standaert, "Towards Green Cryptography: a Comparison of Lightweight Ciphers from the Energy Viewpoint", International Workshop on Cryptographic Hardware and Embedded Systems **(2012)**, LNCS 7428, pp. 390–407

[8] L. Batina, A. Das, B. Ege, E. B. Kavun, N. Mentens, C. Para, I. Verbauwhede, T. Yalçin, "Dietary Recommendations for Lightweight Block Ciphers: Power, Energy and Area Analysis of Recently Developed Architectures", Workshop on RFID Security **(2013)**, pp. 103-112.

[9] B. J. Mohd, T. Hayajneh, and A. V. Vasilakos, "A Survey on Lightweight Block Ciphers for Low-resource Devices", Journal of Network and Computer Applications **(2015)**, Vol. 58C, pp. 73-93.

[10] S. Banik, A. Bogdanov, F. Regazzoni, “Exploring Energy Efficiency of Lightweight Block Ciphers”, International Conference on Selected Areas in Cryptography **(2015)**, pp. 178-194.

[11] A.J. Acosta, T. Addabbo, and E. Tena-Sánchez, “Embedded electronic circuits for cryptography, hardware security and true random number generation: an overview”, International Journal on Circuit Theory and Applications (**2017**). Vol. 45, Nº 2, pp. 145-169

[12] M. Hell, T. Johansson, and W. Meier, “Grain: a stream cipher for constrained environments”, International Journal of Wireless and Mobile Computing (**2007**), Vol. 2, Nº 1, pp. 86–93.

[13] C. De Canniere, “Trivium: A stream cipher construction inspired by block cipher design principles”, International Conference on Information Security (**2006**), pp. 171–186.

[14] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, “Present: An ultra-lightweight block cipher”, International Workshop on Cryptographic Hardware and Embedded Systems (**2007**), pp. 450–466.

[15] C. De Canniere, O. Dunkelman, and M. Knežević, “KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers”, International Workshop on Cryptographic Hardware and Embedded Systems (**2009**), pp. 272-288.

[16] S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni, “Midori: a block cipher for low energy”, International Conference on the Theory and Application of Cryptology and Information Security (**2014**), pp. 411-436.

[17] M. Feldhofer, and J. Wolkerstorfer, “Hardware implementation of symmetric algorithms for RFID security”, Workshop on RFID Security (**2008**), pp. 373-415.

[18] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, “AES implementation on a grain of sand”, IEE Proceedings-Information Security (**2005**), Vol. 152 No. 1, pp. 13-20.

[19] C. Hocquet, D. Kamel, F. Regazzoni, J. D. Legat, D. Flandre, D. Bol, and F. X. Standaert, “Harvesting the potential of nano-CMOS for lightweight cryptography: an ultra-low-voltage 65 nm AES coprocessor for passive RFID tags”. Journal of Cryptographic Engineering (**2011**), Vol. 1, No. 1, pp. 79-86.

[20] S. Banik, A. Bogdanov, F. Regazzoni, T. Isobe, H. Hiwatari, and T. Akishita, “Round gating for low energy block ciphers”. Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (**2016)**, pp. 55-60.

[21] D. H. Bui, D. Puschini, S. Bacles-Min, E. Beigné, and X. T. Tran, “Ultra low-power and low-energy 32-bit datapath AES architecture for IoT applications”. International Conference on IC Design and Technology **(2016),** pp. 1-4.

[22] J. M. Mora-Gutiérrez, C. J. Jiménez-Fernández, and M. Valencia-Barrero, “Low power implementation of trivium stream cipher”. International Workshop on Power and Timing Modeling, Optimization and Simulation **(2012)**, pp. 113-120.

[23] J. M. Mora-Gutiérrez, C.J. Jiménez-Fernández and M. Valencia-Barrero. "Trivium hardware implementations for power reduction". International Journal of Circuit Theory and Applications **(2017)**. Vol. 45, No. 2, pp. 188-198.

[24] M. Feldhofer, “Comparison of low-power implementations of Trivium and Grain”, Workshop on The State of the Art of Stream Ciphers (**2007**), pp. 236-246.

[25] G. Bertoni, M. Macchetti, L. Negri, and P. Fragneto, “Power-efficient ASIC synthesis of cryptographic sboxes”, Proceedings of the ACM Great Lakes symposium on VLSI **(2004)**, pp. 277-281.

[26] D. Canright, “A very compact S-box for AES”, International Workshop on Cryptographic Hardware and Embedded Systems (**2005**), pp. 441-455.

[27] A. Klein, “Stream Ciphers”, Springer-Verlag, London 2013.

[28] eSTREAM: the ECRYPT Stream Cipher Project. Available: http://www.ecrypt.eu.org/stream/ Last accessed March 31, 2017

[29] T. Good, and M. Benaissa, “ASIC Hardware Performance”, New Stream Cipher Designs **(2008)**, LNCS 4986, pp. 267–293

[30] E. Tena-Sánchez, J. Castro, and A. J. Acosta, “A Methodology for Optimized Design of Secure Differential Logic Gates for DPA Resistant Circuits”, IEEE Journal on Emerging and Selected Topics in Circuits and Systems (**2014**), Vol. 4, Nº 2, pp.203-215.

[31] S. Mangard, E. Oswald, and T. Popp, Power analysis attacks: Revealing the secrets of smart cards, Springer Science & Business Media (**2008**).

[32] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis”, Annual International Cryptology Conference (**1999**), pp. 388-397.

[33] P. Kocher, “Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems”, Annual International Cryptology Conference (**1996**), pp. 104-113.

[34] Y. I. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, L. Sauvage, and J. L. Danger, “Analysis of electromagnetic information leakage from cryptographic devices with different physical structures”, IEEE Transactions on Electromagnetic Compatibility (**2013**), Vol. 55, Nº 3, pp.571-580.

[35] S. Mangard, N. Pramstaller, and E. Oswald, ”Successfully attacking masked AES hardware implementations”, International Workshop on Cryptographic Hardware and Embedded Systems, (**2005**), pp. 157-171.

[36] W. Fischer, B. M. Gammel, O. Kniffler and J. Velten, ”Differential power analysis of stream ciphers”, Topics in Cryptology-CT-RSA, (**2007**), pp. 257-270.

[37] Y. Jia, Y. Hu, F. Wang, and H. Wang, “Correlation power analysis of Trivium”, Security and Communication Networks (**2012**), Vol. 5, Nº 5, pp.479-484.

[38] Y. Ishai, A. Sahai, and D. Wagner, “Private circuits: Securing hardware against probing attacks”, Advances in Cryptology (**2003**), pp. 463–481.

[39] O. Reparaz, B. Bilgin, S. Nikova, B. Gierlichs, and I. Verbauwhede, “Consolidating masking schemes”, Advances in Cryptology (**2015**), pp. 764–783.

[40] K. Tiri and I. Verbauwhede, “A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation”, Proceedings of Design, Automation and Test in Europe (**2004**), pp. 246-251.

[41] T. Popp and S. Mangard, “Implementation aspects of the DPA-resistant logic style MDPL”, Proceedings of IEEE International Symposium on Circuits and Systems (**2006**), pp. 2913-2916.

[42] K. Tiri, M. Akmal, and I. Verbauwhede, “A dynamic and differential cmos logic with signal independent power consumption to withstand differential power analysis on smart cards”, Proceedings of IEEE Solid-State Circuits Conference (**2002**), pp. 403–406.

[43] M. W. Allam, and M. I. Elmasry, “Dynamic current mode logic (DYCML): A new low-power high-performance logic style”, IEEE Journal of Solid-State Circuits (**2001**), Vol. 36, Nº 3, pp. 550–558.

[44] E. Tena-Sánchez, and A. J. Acosta, “Improving Power and Security in DPL-based Cryptocircuits via Logic Optimization”, IEEE Transactions on VLSI Systems, *Under revision*.

[45] M. A. Morrison, N. Ranganathan, and J. Ligatti, "Design of Adiabatic Dynamic Differential Logic for DPA-Resistant Secure Integrated Circuits", IEEE Transactions on VLSI (**2015**), Vol. 23, Nº 8, pp. 1381-1389.

[46] S. D. Kumar, H. Thapliyal, and A. Mohammad, "EE-SPFAL: A Novel Energy-Efficient Secure Positive Feedback Adiabatic Logic for DPA Resistant RFID and Smart Card", IEEE Transactions on Emerging Topics in Computing (**2016**), pp.1-12.

[47] E. Tena-Sánchez, J. Castro, and A. J. Acosta, "Low-Power Differential Logic Gates for DPA Resistant Circuits", Euromicro Conference on Digital System Design, (**2014**), pp. 671-674.

[48] M. Renauld, D. Kamel, F. X. Standaert, and D. Flandre, "Information theoretic and security analysis of a 65-nanometer DDSLL AES S-box", International Workshop on Cryptographic Hardware and Embedded Systems, (**2011**), pp. 223-239.

[49] J. Giorgetti, G. Scotti, A. Simonetti, and A. Trifiletti, "Analysis of data dependence of leakage current in CMOS cryptographic hardware", Proceedings of the ACM Great Lakes symposium on VLSI (**2007**), pp. 78-83.

[50] L. Lin, and W. Burleson, "Leakage-based differential power analysis (LDPA) on sub-90nm CMOS cryptosystems", IEEE International Symposium on Circuits and Systems (**2008**), pp. 252-255.

[51] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, "Leakage Power Analysis Attacks: A Novel Class of Attacks to Nanometer Cryptographic Circuits", IEEE Transactions on Circuits and Systems I (**2010**), Vol. 57, Nº 2, pp. 355-367.

[52] N. H. Zhu, Y. J. Zhou, and H. M. Liu, "Employing symmetric dual-rail logic to thwart LPA attack", IEEE Embedded Systems Letters (**2013**), Vol. 5, Nº 4, pp. 61-64.

[53] A. Chen, X. S. Hu, Y. Jin, M. Niemier, and X. Yin, "Using emerging technologies for hardware security beyond PUFs", Proceedings of Design, Automation & Test in Europe (**2016**), pp. 1544-1549.

[54] Y. Bi, X. S. Hu, Y. Jin, M. Niemier, K. Shamsi, and X. Yin, "Enhancing hardware security with emerging transistor technologies", Proceedings of International Great Lakes Symposium on VLSI , (**2016**), pp. 305-310.

[55] Y. Bi, K. Shamsi, J. S. Yuan, F. X. Standaert, and Y. Jin, “Leverage emerging technologies for dpa-resilient block cipher design”, Proceedings of the Conference on Design, Automation & Test in Europe (**2016**), pp. 1538-1543.

[56] Y. Bi, K. Shamsi, J. S. Yuan, Y. Jin, M. Niemier, and X. S. Hu, "Tunnel FET Current Mode Logic for DPA-Resilient Circuit Designs", IEEE Transactions on Emerging Topics in Computing (**2016**). DOI: 10.1109/TETC.2016.2559159.

[57] S. D. Kumar, H. Thapliyal, and A. Mohammad, "FinSAL: FinFET Based Secure Adiabatic Logic for Energy-Efficient and DPA Resistant IoT Devices", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**2017**). DOI: 10.1109/TCAD.2017.2685588

[58] J. Castro, P. Parra, and A. J. Acosta, “An Improved Differential Pull-Down Network Logic Configuration for DPA Resistant Circuits,” in IEEE International conference on Microelectronics (**2010**), pp. 311-314.

# FIGURES AND TABLES

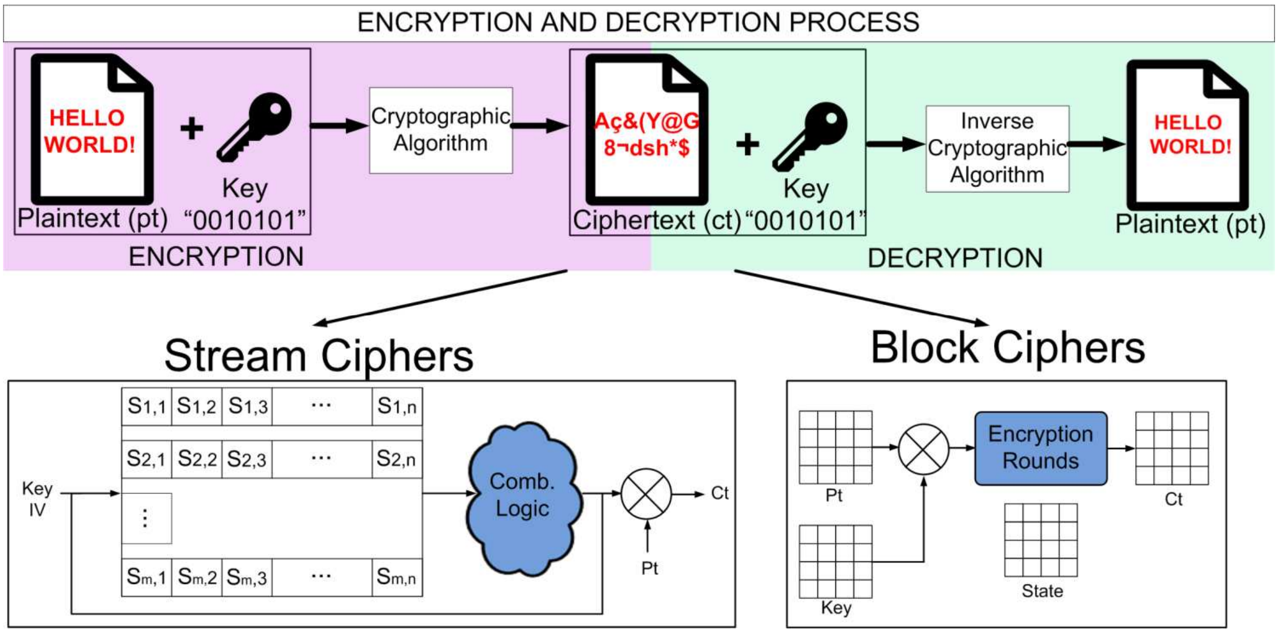

**Figure 1. Encryption and Decryption process for stream and block ciphers**

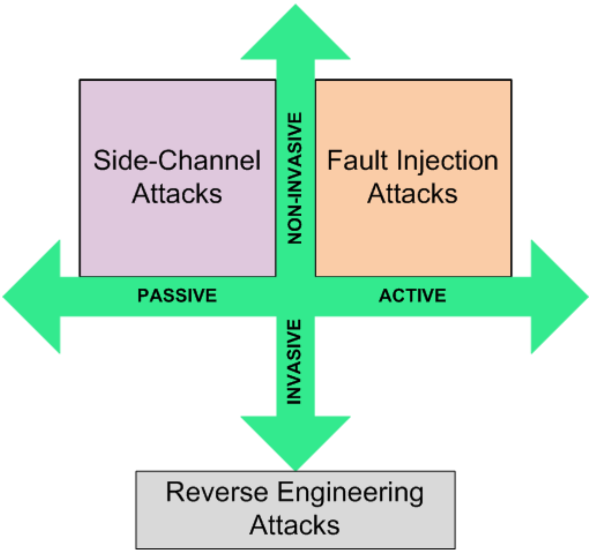

**Figure 2. Attack classification.**

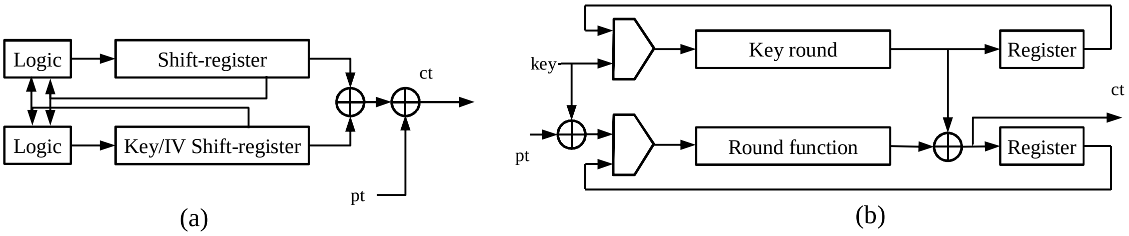

**Figure 3. General structure of a) stream ciphers, b) block ciphers.**

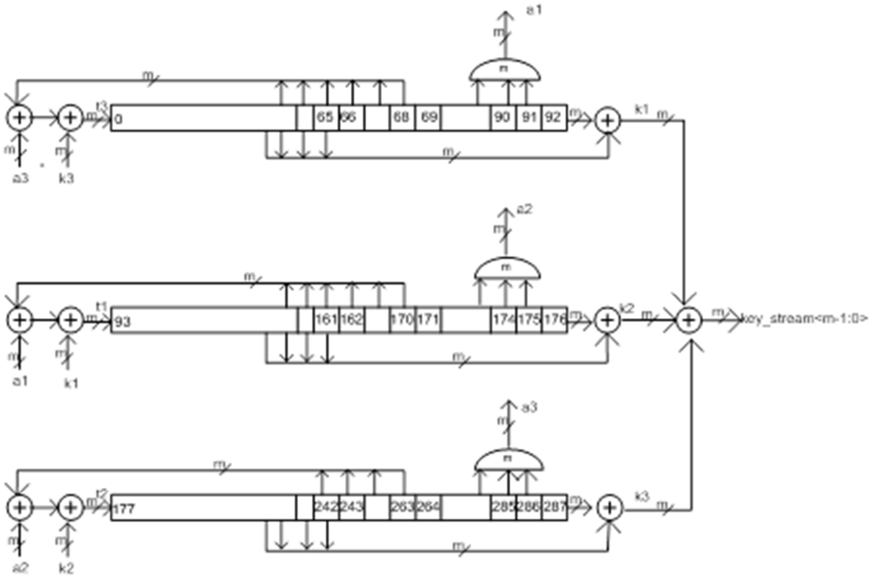

**Figure 4. Multi-bit architecture of Trivium stream cipher.**

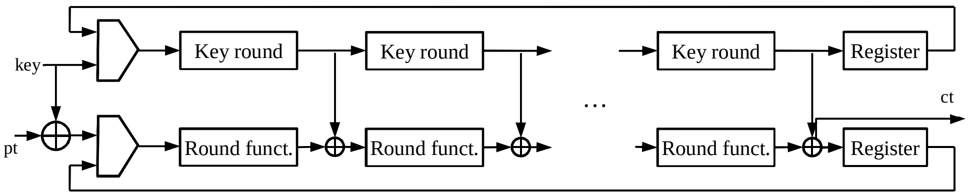

**Figure 5. General unrolling architecture of block ciphers.**

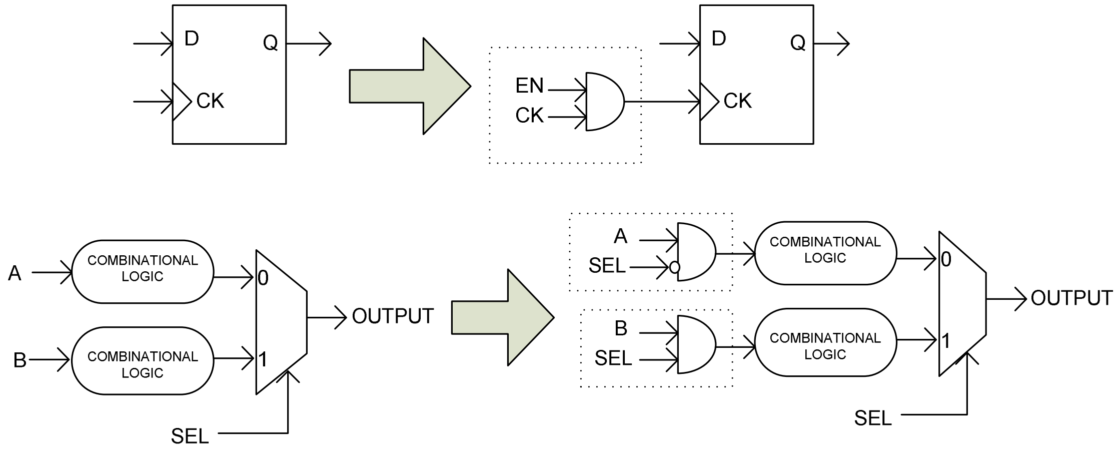

**Figure 6 Clock gating and sleep logic techniques.**

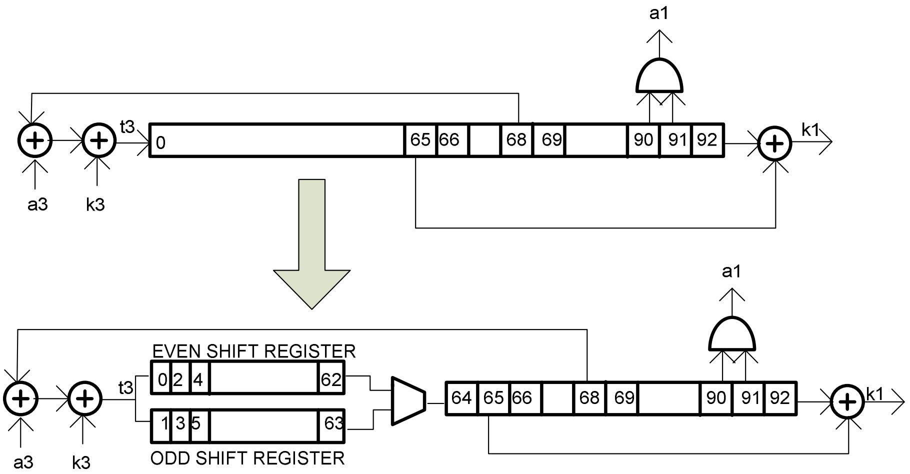

**Figure 7 Schematic for Trivium shift-register with paralellization technique [22]**

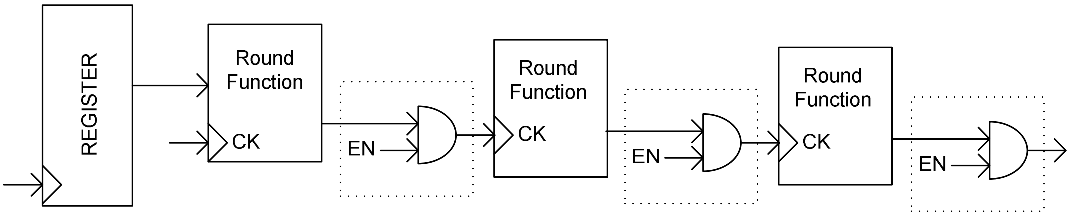

**Figure 8 Round gating [20].**

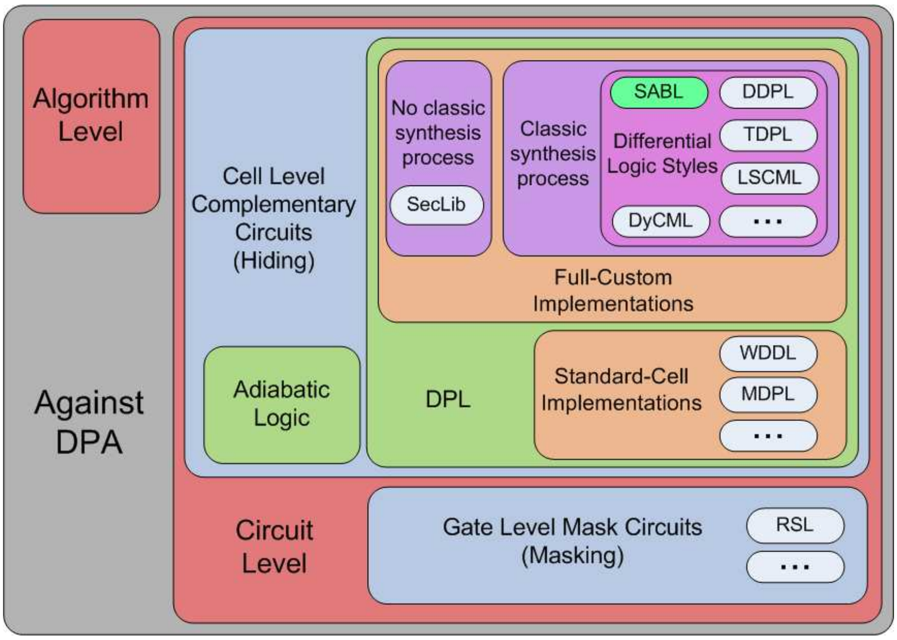
Algorithm Level
Against DPA
Cell Level Complementary Circuits (Hiding)
No classic synthesis process
SecLib
Classic synthesis process
SABL
DDPL
Differential Logic Styles
TDPL
LSCML
DyCML
...
Full-Custom Implementations
Adiabatic Logic
DPL
Standard-Cell Implementations
WDDL
MDPL
...
Circuit Level
Gate Level Mask Circuits (Masking)
RSL
...

**Figure 9. Countermeasure classification at different abstraction levels**

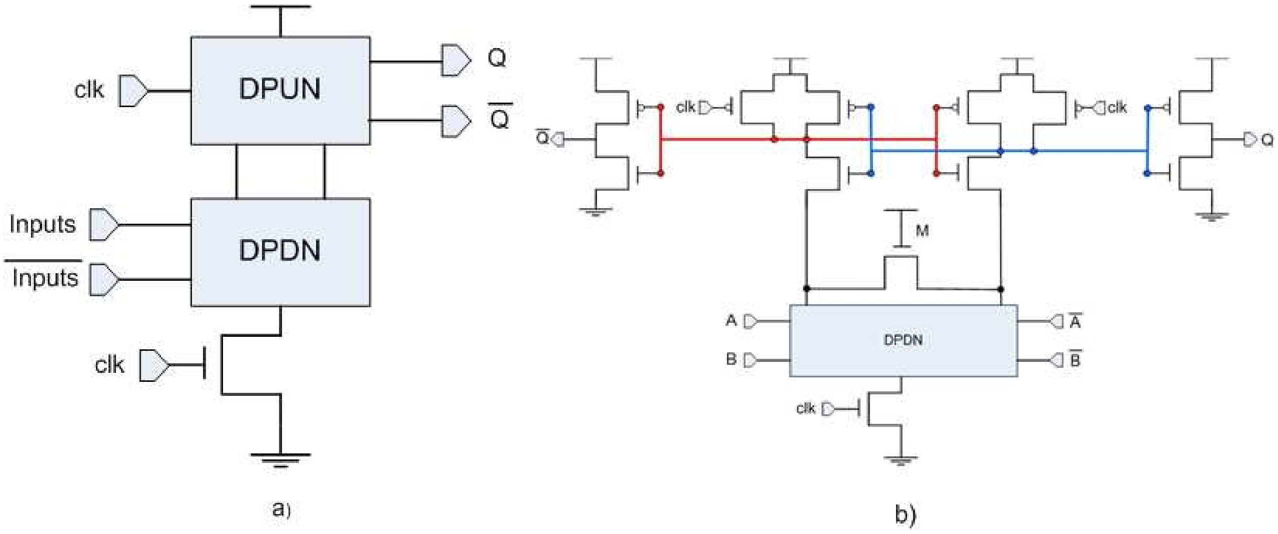

**Figure 10. (a) DPL universal scheme using NMOS transistors to implement the differential pull-down network (DPDN) block logic function. (b) SABL logic style.**

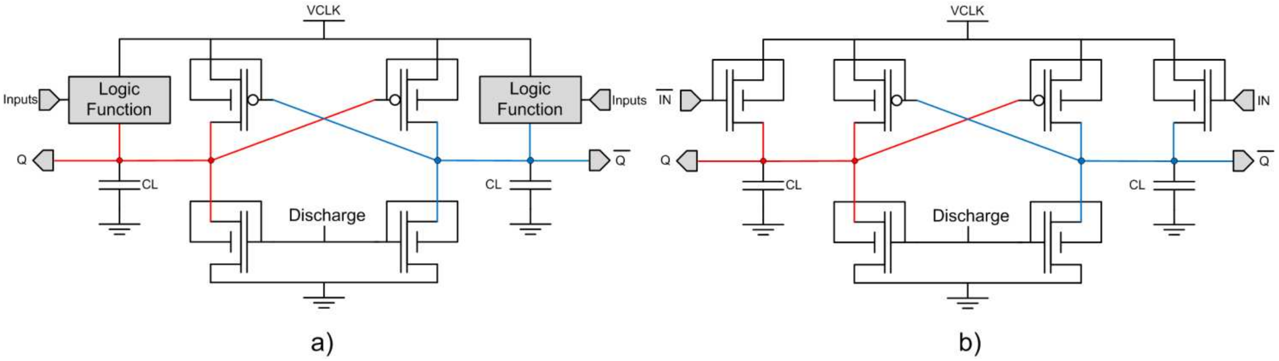

**Figure 11. (a) Generic FinSAL schematic. (b) FinSAL inverter schematic.**

TABLE I
STREAM CIPHER POWER COMPARISON

| **Design** | **Power (uW, @10 Mhz)** | **Bits of state register** | **Power/bit (uW)** |
|---|---|---|---|
| ***Grain80*** | 109.4 | 160 | 0.683 |
| ***Grain128*** | 167.7 | 256 | 0.655 |
| ***Mickey80*** | 196.5 | 200 | 0.982 |
| ***Mickey128*** | 310.7 | 320 | 0.970 |
| ***Trivium*** | 175.1 | 288 | 0.607 |

TABLE II
POWER AND ENERGY FOR MULTI-BIT STREAM CIPHERS

| **Design** | **Grain80** | | | | **Trivium** | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | **x1** | **x4** | **x8** | **x16** | **x1** | **x2** | **x4** | **x8** | **x16** | **x32** | **x64** |
| ***Power (uW)*** | 109.4 | 126.6 | 150.7 | 200.5 | 175.1 | 182.8 | 184.6 | 203.4 | 214.4 | 282.5 | 374.2 |
| ***Energy/bit (pJ)*** | 10.94 | 3.16 | 1.88 | 1.25 | 17.51 | 9.14 | 4.61 | 2.54 | 1.34 | 0.88 | 0.58 |

TABLE III
COMPARATIVE SUMMARY OF REDUCING POWER IN STREAM CIPHERS REFERENCES

| *Trivium* | *Dynamic power or mean current* | *Supply voltage* | *Clock rate* | *Technology* |
|---|---|---|---|---|
| *Grain radix-16 [24]* | 0.80 µA | 1.5 V | 100 KHz | 350 nm |
| *Trivium radix-16 [24]* | 0.68 µA | 1.5 V | 100 KHz | 350 nm |
| *Trivium [22]* | 1007 µW | 1.8 V | 25 MHz | 180 nm |
| *Trivium-FPLP [22]* | 712 µW | 1.8 V | 25 MHz | 180 nm |
| *Trivium [22]* | 236 µW | 1.2 V | 25 MHz | 130 nm |
| *Trivium-FPLP [22]* | 178 µW | 1.2 V | 25 MHz | 130 nm |
| *Trivium [22]* | 219 µW | 1.2 V | 25 MHz | 90 nm |
| *Trivium-FPLP [22]* | 179 µW | 1.2 V | 25 MHz | 90 nm |
| *Trivium [23]* | 5.8 mW | 3.3 V | 25 MHz | 350 nm |
| *Trivium-MPLP [23]* | 4.3 mW | 3.3 V | 25 MHz | 350 nm |
| *Trivium-FPLP [23]* | 4.4 mW | 3.3 V | 25 MHz | 350 nm |

# BIOGRAPHIES

**Antonio J. Acosta** received a B.Sc. and PhD degrees in Physics from the University of Seville, Spain, in 1989 and 1995, respectively. He is Full Professor at the University of Seville and Senior Researcher at the Instituto de Microelectrónica de Sevilla (CSIC/University of Seville). His current research interests are low-power and low-noise CMOS circuits, Digital CMOS and mixed-signal high-performance VLSI Design, and cryptographic circuits. He has co-authored more than 100 international publications and has led numerous R&D projects. Dr. Acosta serves as associate editor at different journals, including JOLPE. He was General Chair of the 2002 PATMOS Workshop.

**Erica Tena-Sánchez** received a B.Sc.degree in Telecomunications in 2010 from the University of Cantabria, Spain, and an Electronics Engineering degree (with honors) and an M.Sc. degree in Microelectronics from the University of Seville, Spain, in 2012 and 2013 respectively. Since 2011, she has been with the Instituto de Microelectrónica de Sevilla (CSIC/University of Seville). Her current research interest lies in the field of CMOS Digital Design of secure cryptographic circuits.

**Carlos J. Jiménez** received B.Sc. and Ph.D. degrees in Physics at the University of Seville, Spain, in 1989 and 2000, respectively. From 1990 to 2001, he was with the Instituto de Microelectrónica de Sevilla (CSIC/University of Seville). Since 2001, he has been Associate Professor at the University of Seville. His current research interests include the design and test of ICs for cryptography, hardware implementations of ciphers for IoT applications, secure communications, design methodologies and CAD tools. He is co-author of 2 books and more than 50 scientific papers, and has participated in more than 20 R+D projects.

**José Miguel Mora** received BSc. and M.Sc. degrees in Telecommunications Engineering (specialization microelectronics) at the Universidad Politécnica de Madrid, Spain, in 1990 and 1992, respectively. Since 1992, he has been a member of the Technical Staff at the Instituto de

Microelectrónica de Sevilla (CSIC/University of Seville), where he is currently Assistant Manager in the R+D section, supporting numerous R+D projects. His main areas of interest include the design and test of digital and mixed-signal ASICs and FPGAs, and ICs for cryptography.