A Systematic Performance Comparison of Ultra Low-Power AES S-Boxes

Thomas Vandenabeele*, Roel Uytterhoeven[†], Wim Dehaene[†] and Nele Mentens*

*ES&S and imec-COSIC/ESAT, KU Leuven

Wetenschapspark 21, B-3590 Diepenbeek, Belgium

[†]MICAS/ESAT, KU Leuven

Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium

Email: firstname.lastname@esat.kuleuven.be

Abstract—This paper elaborates on the results of a thorough comparison between different AES S-box circuits in 28nm Fully Depleted Silicon-On-Insulator (FD-SOI) technology of STMicroelectronics. The three evaluated S-boxes are strategically chosen to provide a maximum coverage of the design space. Simulation results regarding area, speed, power and energy are presented and analyzed. Further, ultra low-power implementations are considered by simulating the circuits in the sub-threshold region. The presented performance comparison allows cryptographic hardware designers to select the most suitable S-box design for their resource-limited AES implementation.

I. INTRODUCTION

Lowering the power consumption of electronic circuits is essential for the internet of things (IoT) and modern day systems-on-chip (SoCs). The ever increasing demand from the consumer market drives a trend to make smart-phones, smart-watches, tablets etc. even smaller whilst increasing their computation power. This results in a strong focus on creating extremely compact, ultra low-power designs that enable small sensors and actuators to operate independently.

Furthermore, the massive rise of IoT applications has led to a widespread adoption of embedded devices. Hereby, the risk of malicious attacks on the security of these devices increases. It is most likely the case that an adversary has physical access to these devices, creating a hostile environment. Hence, research on "lightweight" cryptography for constrained silicon devices is gaining importance. Depending on the application, the term lightweight refers to different constraints. For most lightweight devices, minimizing the surface area is desirable since this positively impacts several device properties such as production costs, mobility and portability. Besides being restricted in area, battery-fed devices are limited in energy consumption, as the energy determines the lifetime, the cost and the size of the battery.

The purpose of the investigation at hand is to perform a comprehensive area, power and energy analysis of different implementations of the Advanced Encryption Standard (AES) substitution box. AES [1] is the most widely used encryption standard. This analysis is helpful for both the engineering and theoretical communities concerned with lightweight cryptography, as the considered AES substitution box is the most area-, power- and energy-consuming component of AES.

A. Related Work

Abinaya Kamaraj presented in [2] a comparison of the power requirements for different S-box designs. She analyzed and evaluated area-optimized S-boxes in terms of power, logic elements and other resources on an FPGA (Altera Cyclone II). In the related work of Batina et al. [3], a comprehensive area, power and energy analysis of lightweight block ciphers is performed. Their results are based on post-synthesis power simulations using a UMC 130 nm low-leakage Faraday technology. The work of Tillich et al. [4] is to our knowledge the most profound comprehensive survey of various AES S-box implementations. They analyzed and compared various cost metrics of the implementations like the critical path delay, the silicon area and the power consumption based on post-synthesis results using a 0.35 μm CMOS standard cell library.

B. Contribution

This paper goes beyond the aforementioned work by focusing on the newest technologies, design strategies and S-box architectures. In particular, the ultra low-power 28nm FD-SOI technology of STMicroelectronics is used for the comparison. Further, sub-threshold designs based on a re-characterized library are evaluated in comparison to traditional super-threshold designs. Finally, our third contribution is to include the newly introduced and extremely small serial S-box architecture [5] in the evaluation, and to compare it to traditional lookup-table-based and composite-field-based S-boxes.

The paper is organized as follows. Section II gives background information on the considered technology, design strategies and algorithms. In Sect. III, the different AES S-box architectures are discussed. Finally, Sect. IV presents and analyzes the results, and Sect. V concludes the paper.

II. BACKGROUND

In this section, we provide background information on ultra low-power design using a sub-threshold power supply, on ST's 28nm FD-SOI technology and on AES.

A. Ultra low-power design

An important focus of today's digital circuits is on creating extremely compact, ultra low-power designs. The digital power

dissipation P_{dig} can be divided into a dynamic and a static component, P_{dyn} and P_{stat} respectively, and can be expressed as follows:

$$\begin{aligned} P_{dig} &= P_{dyn} + P_{stat} \\ &= \alpha f_{clk} C V_{dd}^2 + V_{dd} I_{leak}, \end{aligned} \quad (1)$$

where V_{dd} is the supply voltage, C is the switching capacity and f_{clk} is the clock frequency. Furthermore, I_{leak} and α are the leakage current and switching activity, respectively [6].

According to Equation 1, the most effective way to lower the power consumption is to downscale the supply voltage V_{dd} , since it influences all the terms in the equation and has a quadratic influence on the dynamic power consumption. Operating circuits in the sub-threshold region is the extreme case of power supply reduction. However, downscaling the supply voltage degrades circuit performance in terms of speed. This creates a challenge as MHz-speeds are preferable for industrial applications. Further, low-power digital circuit design in the sub-threshold region concentrates on overcoming two main issues compromising the functionality of these circuits. First, by lowering the supply voltage, the ratio between the on-current I_{on} and the leakage current I_{off} decreases dramatically. Secondly, sub-threshold circuits are more sensitive to variations, resulting in deteriorated functionality and in highly variable gate delays. Nevertheless, research results show that these problems can be overcome in order to obtain robust digital circuits in the sub-threshold region [7–11]. For the performance comparison in the paper at hand, an existing standard cell library was re-characterized at 300mV supply voltage, resulting in building blocks for ultra low-voltage circuits functioning at MHz-speed.

B. 28nm UTBB FD-SOI

In this work, we implement the experiments in 28nm Ultra Thin Buried-Box Fully Depleted Silicon-On-Insulator (UTBB FD-SOI). In contrast to a conventional bulk planar transistor, a FD-SOI transistor relies on an ultra-thin layer of silicon over a Buried Oxide (BOX) layer (25nm). Considering FD-SOI is fully depleted, random dopant fluctuations are limited. In bulk technologies these random dopant fluctuations have a strong effect on V_t [12]. This makes FD-SOI, with its reduced variability, exceptionally suitable for low-voltage circuits. A cross-section of an UTBB FD-SOI transistor is shown in Fig. 1. The figure shows the ultra-thin (25nm) buried oxide (BOX) that dielectrically isolates the transistor from the back-gate. Hence, FD-SOI enables control of the behaviour of transistors not only through the gate, but also by polarizing the substrate underneath the device (back-gate), similarly to the body bias available in bulk technology. The presence of the buried oxide allows the application of higher biasing voltages, resulting in breakthrough dynamic control of the transistor. By choosing optimal combinations of the gate and back-gate voltages, the transistors characteristics can be transformed from those of a very high-performance transistor to those of a very low-power transistor. By varying these voltages, the V_t is actively lowered (forward body biasing) or raised (reversed

Fig. 1: UTBB FD-SOI transistor cross-section [9].

Fig. 2: AES encryption block diagram. The round block is repeated $Nr - 1$ times before executing the last round block. This paper focuses on the S-box inside the SubBytes layer.

body biasing), resulting in higher performance and less static leakage current, respectively.

C. The Advanced Encryption Standard

To protect sensitive data in a hostile environment, the Advanced Encryption Standard (AES) is the de facto symmetric-key block cipher [1]. It was standardized by the National Institute of Standards and Technology (NIST). The AES algorithm consists of four transformations, i.e. AddRoundKey, SubBytes, ShiftRows, and MixColumns, as is shown in Fig. 2. Using a shared (symmetric) secret key, the AES algorithm encrypts and decrypts data from plaintext to ciphertext by applying 10 rounds (for a 128-bit key length), of which every round consist of the four transformations (excluding the MixColumn transformation in the last round). The encrypted data can in turn safely be transmitted over an insecure channel.

The SubBytes transformation (substitution box or S-box) is the only nonlinear element of the AES algorithm. In software, the most optimal way to implement the S-box is through a 256-by-8 bit lookup table. But the S-box can also be viewed as a mathematical transformation, as is shown in Fig. 3. The $GF(2^8)$ inverse is the computation of an inverse over a binary extension field, in which each element is represented as an 8-bit vector of $GF(2)$ elements. The affine mapping is a linear operation that performs a matrix transformation on

the $GF(2^8)$ inverse. The mathematical representation of the $GF(2^8)$ inverse gives rise to different implementation options in hardware, as discussed in Sect. III.

III. SUBSTITUTION BOXES

The mathematical structure of the S-box, shown in Fig. 3, allows the implementation of different architectural variants in hardware. The lookup-table-based approach (also used in software) results in the lowest logical depth and is thus expected to feature the lowest combinatorial delay and the highest throughput. Another approach, that is specifically interesting for hardware implementations with low area (and low power/energy) as the design goal, is to implement the $GF(2^8)$ inverse as a digital circuit consisting of components that compute operations in the subfields $GF(2^4)$ and $GF(2^2)$ and $GF(2)$; this is called the composite field approach. A third approach that recently gained interest is to serialize the computation in order to both reduce the area and the peak power consumption of the S-box. Depending on the optimization goal, i.e. high throughput, low area, low power consumption and/or low energy consumption, a specific architecture

needs to be chosen. We believe that by evaluating lookup-table-based, composite-field-based and serialized S-boxes, we sufficiently cover the design space, so we concentrate on these three types of S-box architectures in the remainder of this paper. This section gives an overview of the three considered architectures.

A. Lookup-table-based Architecture

The most straightforward way of implementing the S-box is through a lookup table with 8 input bits, that are used as address bits, as is shown in Fig. 4. The lookup table consists of 256 entries with 8 bits each and can be implemented either as volatile embedded memory or as a logical circuit. In this paper, we synthesize the lookup table description into a logical circuit. This approach will be denoted as **LUT**.

B. Composite-field-based Architecture

The inversion in $GF(2^8)$ can be decomposed into a sequence of subfield operations (addition, multiplication and inversion) in $GF(2^4)$. Furthermore, operations in $GF(2^4)$ can be expressed in terms of operations in $GF(2^2)$, and operations in $GF(2^2)$ in terms of operations in $GF(2)$. At the lowest

Fig. 3: The 2 operations of the AES SubBytes layer.

Fig. 4: Diagram of the look-up-table based S-box with an 8-bit input and 8-bit output.

Fig. 5: Diagram of the composite-field-based S-box proposed by Canright [13]. The $GF(2^4)$ blocks are internally decomposed into operations in $GF(2^2)$ and $GF(2)$.

Fig. 6: Diagram of the S-box based on rotational symmetry proposed by [5]. T_0 is the nonlinear part of the S-box and A represents the AES affine transformation.

level, operations in the field $GF(2)$ are XOR gates for addition and AND gates for multiplication. In $GF(2)$, the inverse of 1 is 1 and the inverse of 0 does not exist.

David Canright [13] examined different choices of basis for each subfield, covering both polynomial and normal bases, resulting in 432 explored cases. The case leading to the smallest implementation is used in this paper. Our implementation of this solution is denoted as **Canright** and a diagram of the S-box is shown in Fig. 5.

C. Bit-serialized Architecture

De Meyer et al. [5] proposed two new ways for implementing the AES S-box: linear redundancy and rotational symmetry implementation. Linear redundancy was proposed by Jean et al. in [14] without a serialized S-box. In [5], the linear redundancy technique was extended to construct a bit-serialized S-box based on rotational symmetry. This is based on the fact that the inversion in $GF(2^8)$ is a power map (x^{254}) and can be seen as a linear and nonlinear rotation-symmetric function with a bit-serialized input and an 8-bit parallel output, also shown in Fig. 6. Due to the serial processing of the input, the S-box computation takes 8 cycles. This implementation is called **Serial** in the remainder of this work.

IV. RESULTS

In this section, we elaborate on the analysis strategy and the design properties for the different S-box implementations. Finally we make a systematic performance comparison of the S-box implementations.

A. Analysis Strategy

Using *Synopsys Design Compiler*, each S-box is synthesized with low area as an optimization goal. RTL synthesis is carried out for two different libraries: (1) 28nm UTBB FD-SOI low-leakage technology library of STMicroelectronics with a supply voltage of 1.1V and (2) a re-characterized technology library based on the same technology for sub-threshold design with a supply voltage of 300mV. The 28nm UTBB FD-SOI technology has the nice feature to perform body-biasing efficiently in comparison with regular bulk technology. However, for this power comparison, the body-biasing is not exploited; the designs are simulated using 0V bias voltages. The used standard cell libraries are characterized with an operating temperature of 25°C. This analysis strategy results in six netlists (three different architectures, each synthesized for two different libraries). The generated netlists are then used to simulate the actual S-box behaviour with *Synopsys VCS-MX*. To simulate the behaviour, we implemented two 8-bit counters, both counting from 0 to 255, in a testbench module, also shown in Fig. 7. The first counter is only increased when the second counter has reached 255. Every clock cycle, the input of the S-box under test is switched between counter 1 and counter 2, resulting in an applied stimulus that simulates all possible 8-bit transitions. From these simulations, waveform files are generated, annotating the switching activity in the simulations. In the last step, the waveform files are used in

Synopsys Primetime-PX together with the generated netlists from the initial synthesis to run power analysis.

The power results in this paper reflect the average power consumption per clock cycle (in Watt). The area numbers are given in terms of two-input NAND gate equivalents (GEs) and are obtained from the synthesis area reports. The total power consumption of the S-boxes consists of the internal power, the switching power and the leakage power. The dynamic power of the S-box implementation is the sum of the internal power and switching power, while the leakage power represents the static power. The internal power is estimated by the tool using the technology library as the total power consumed within the gates; it is calculated for each standard cell as a function of the input transition time. Short-circuit power occurs due to the currents flowing from the supply to the ground for a short period of time during switching. As a result, cells with a longer input transition time have a larger short-circuit current flowing through the gate, which results in a larger internal power for the specific cell. The switching power is a result of the charging and discharging of the nodes that connect the gates, influenced by the load capacitance at the output of each gate. The leakage power is mainly determined by the sub-threshold leakage current of the transistors that is present even if the transistor is switched off. The reported energy consumption corresponds to the average power consumption divided by the clock frequency, multiplied by the number of clock cycles needed for the complete S-box computation.

B. Comparison

Table Ia shows a comparison of the area and maximum frequency for the S-box implementations in super- and sub-threshold design. The S-boxes in sub-threshold design are indicated by a supply voltage of 300mV. The super-threshold designs are simulated using a 1.1V power supply. The maximum clock frequency is derived from the critical path in the netlist. The critical path is minimized by iteratively searching for the most strict timing constraint that can be met by the circuit. The results in the table are as expected, i.e. the LUT-based architecture results in the largest silicon area, while the Canright S-box and the serialized S-box are much smaller. Similar to the related work done on older technologies, the serialized S-box is slightly smaller than the Canright S-box. The serialized S-box also features the smallest critical path (corresponding to the highest operating frequency), but needs 8 clock cycles to complete the S-box computation. Therefore, the LUT-based S-box is by far the fastest architecture in terms

Fig. 7: Testbench for the S-boxes in which the input for the S-box under test is switched between the two counters each cycle (counters are 8-bit counters).

	300mV		1.1V	
	Area GE	$f_{\max}$ MHz	Area GE	$f_{\max}$ GHz
Canright	282	6.6	283	1.21
LUT	500	16.0	500	3.54
Serial	245	31.7	245	5.87

(a) Area and $f_{\max}$

Power (W)	300mV			1.1V		
	Canright	LUT	Serial	Canright	LUT	Serial
Internal	3.05E-08	2.53E-08	5.24E-08	5.84E-07	4.33E-07	9.84E-07
Switching	3.20E-08	2.67E-08	1.96E-08	5.91E-07	4.58E-07	3.47E-07
Leakage	8.83E-08	2.27E-07	8.00E-08	3.61E-06	7.83E-06	2.41E-06
Total	1.51E-07	2.79E-07	1.52E-07	4.78E-06	8.72E-06	3.74E-06

(b) Power @ 6.6 MHz

Power (W)	300mV		1.1V		
	LUT	Serial	Canright	LUT	Serial
Internal	6.17E-08	1.28E-07	1.42E-06	1.05E-06	2.39E-06
Switching	6.49E-08	4.76E-08	1.44E-06	1.11E-06	8.46E-07
Leakage	2.27E-07	8.00E-08	3.61E-06	7.83E-06	2.41E-06
Total	3.54E-07	2.55E-07	6.47E-06	1.00E-05	5.65E-06

(c) Power @ 16 MHz

Power (W)	300mV	1.1V		
	Serial	Canright	LUT	Serial
Internal	2.52E-07	2.81E-06	2.08E-06	2.73E-06
Switching	9.41E-08	2.84E-06	2.20E-06	1.67E-06
Leakage	8.00E-08	3.61E-06	7.83E-06	2.41E-06
Total	4.26E-07	9.26E-06	1.21E-05	8.81E-06

(d) Power @ 31.7 MHz

Power (W)	1.1V		
	Canright	LUT	Serial
Internal	1.08E-04	7.98E-05	1.81E-04
Switching	1.09E-04	8.44E-05	6.40E-05
Leakage	3.61E-06	7.83E-06	2.41E-06
Total	2.20E-04	1.72E-04	2.48E-04

(e) Power @ 1.21 GHz

Power (W)	1.1V	
	LUT	Serial
Internal	2.33E-04	5.30E-04
Switching	2.47E-04	1.87E-04
Leakage	7.83E-06	2.41E-06
Total	4.88E-04	7.19E-04

(f) Power @ 3.54 GHz

Power (W)	1.1V
	Serial
Internal	8.78E-04
Switching	3.10E-04
Leakage	2.41E-06
Total	1.19E-03

(g) Power @ 5.87 GHz

TABLE I: Area, speed and power simulation results of different AES S-box implementations at different clock frequencies. Results for sub-threshold designs are annotated by the 300 mV supply voltage and by a supply voltage of 1.1 V for the super-threshold designs.

Fig. 8: Results of the power consumption simulation. The asterisk annotated next to an implementation's name marks the simulation results in the sub-threshold region, otherwise the circuit operates in the super-threshold region.

of computational latency. When we compare the sub-threshold designs to their super-threshold counterparts, we see a drastic degradation in performance.

Table I and Fig. 8 show a comparison of the six designs in terms of the average power consumption per clock cycle at different operating frequencies. The designs are simulated

at six different operating frequencies, corresponding to the maximum clock frequencies of the six evaluated netlists. When no results are reported for a specific design at a specific operating frequency, this means that the design did not meet the timing constraints. A comparison of the sub-threshold implementations shows what we would expect in terms of

	Energy per bit (fJ)	Energy (fJ)
Canright	2.86	22.88
LUT	5.28	42.27
Serial	23.03	184.24

(a) Sub-Threshold @ 6.6 MHz

	Energy per bit (fJ)	Energy (fJ)
Canright	22.73	181.82
LUT	17.77	142.15
Serial	204.96	1639.67

(b) Super-Threshold @ 1.21 GHz

TABLE II: Energy simulation results

power consumption: the S-box with the largest area also consumes the largest total power. This is also the case for the super-threshold implementations operating at the three lowest speeds (6.6 MHz, 16 MHz and 31.7 MHz), also shown in Tables Ib to Id. However, an anomaly occurs when comparing the S-boxes in super-threshold at higher speeds (1.21 GHz, 3.54 GHz and 5.87 GHz), as can be seen in Tables Ie to Ig. The results do not correspond to our expectation that the dynamic power consumption is larger for the designs with a larger area. The most plausible explanation for this behaviour is the following. The amount of conducting transistors (affecting the static power consumption) and the number of nodes that switch (affecting the dynamic power consumption) are different in each implementation. On the one hand, the switching activity of the LUT-based S-box will be significantly lower than the activity of the calculating S-box implementations, meaning that voltage scaling has a significantly lower impact on the power consumption. The serial S-box, on the other hand, has a much larger switching activity, resulting in a strong impact from voltage scaling. Ultimately, this difference in activity causes LUT to be more beneficial at faster clock speeds and thus higher supply voltage. The calculating S-box implementations are more beneficial at lower clock speeds and low voltage. Table II shows this effect clearly.

Table II compares the energy consumption of the evaluated S-boxes. It shows that the serialized S-box, which has the lowest area, consumes the most energy due to the cycle count of 8 cycles to complete the computation; the other S-boxes are purely combinatorial. The energy per bit is calculated by dividing the total power by the clock frequency and then multiplying by the cycle count, followed by dividing by the input length (8 bits).

In summary, Tables I and II show that the architectural differences in the S-boxes cause significant differences in area, power, energy and critical path.

V. CONCLUSION

In this paper, 3 different AES S-box implementations are evaluated based on the area, power consumption and energy consumption in super-threshold and sub-threshold design. This allows designers of cryptographic hardware to choose the most optimal S-box for a specific application.

Note that the resulting figures from the previous simulations are estimates and will differ significantly from real-life measurement results. Nonetheless, as all numbers are generated using the same flow they still provide highly relevant information when compared to each other, as demonstrated by this work.

In future work, we will evaluate these S-boxes in complete cryptographic algorithms. This will result in cryptographic circuits with exceptional low-power features in 28nm FD-SOI. In addition, we will redo the systematic comparison based on post-layout results. Finally, we will investigate the influence of the back-gate bias in FD-SOI technology on the critical path and the power and energy consumption of the designs.

ACKNOWLEDGEMENTS

We would like to thank STMicroelectronics for the 28nm FD-SOI technology donation and support. We also thank Lauren De Meyer for her input on the bit-serialized S-box architecture.

REFERENCES

- [1] FIPS PUB 197, "Advanced Encryption Standard (AES)," *National Institute of Standards and Technology, U.S. Department of Commerce*.
- [2] A. Kamaraj, "Efficient Implementation and Power Estimation of Substitute-Box in Advanced Encryption Standard," Ph.D. dissertation, 2016.
- [3] L. Batina, A. Das, B. Ege, E. B. Kavun, N. Mentens, C. Paar, I. Verbauwhede, and T. Yalçın, "Dietary Recommendations for Lightweight Block Ciphers: Power, Energy and Area Analysis of Recently Developed Architectures," Springer, Berlin, Heidelberg, 2013, pp. 103–112.
- [4] S. Tillich, M. Feldhofer, and J. Großschädl, "Area, Delay, and Power Characteristics of Standard-Cell Implementations of the AES S-Box," Springer, Berlin, Heidelberg, 2006, pp. 457–466.
- [5] L. De Meyer and B. Bilgin, "Can A Bit-Serialized AES S-Box Be Small?" *CHES 2017 - Taipei*.
- [6] M. Pedram, "Power minimization in IC design: principles and applications," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 1, no. 1, pp. 3 – 56, 1996.
- [7] A. Wang and A. P. Chandrakasan, "A 180-mV Subthreshold FFT Processor Using a Minimum Energy Design Methodology," *IEEE Journal of Solid-State Circuits*, vol. 40, no. 1, pp. 310–319, 2005.
- [8] L. Lin, D. Holcomb, D. K. Krishnappa, P. Shabadi, and W. Burleson, "Low-power sub-threshold design of secure physical unclonable functions," *Proceedings of the 16th ACM/IEEE international symposium on Low power electronics and design - ISLPED '10*, p. 43, 2010.
- [9] H. Reyserhove, N. Reynders, and W. Dehaene, "Ultra-low voltage datapath blocks in 28nm UTBB FD-SOI," *Proceedings - 2014 IEEE Asian Solid-State Circuits Conference, A-SSCC 2014*, vol. 32, pp. 49–52, 2015.
- [10] H. Reyserhove and W. Dehaene, "Design margin elimination in a near-threshold timing error masking-aware 32-bit arm cortex m0 in 40nm cmos," in *ESSCIRC 2017 - 43rd IEEE European Solid State Circuits Conference*, Sept 2017, pp. 155–158.
- [11] —, "A Differential Transmission Gate Design Flow for Minimum Energy Sub-10-pJ/Cycle ARM Cortex-M0 MCUs," *IEEE Journal of Solid-State Circuits*, vol. 52, no. 7, pp. 1904–1914, 2017.
- [12] R. Rithe, S. Chou, J. Gu, A. Wang, S. Datla, G. Gammie, D. Buss, and A. Chandrakasan, "The effect of random dopant fluctuations on logic timing at low voltage," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 20, no. 5, pp. 911–924, 2012.
- [13] D. Canright, "A Very Compact S-Box for AES," in *Cryptographic Hardware and Embedded Systems - CHES 2005*. Berlin, Heidelberg: Springer, Berlin, Heidelberg, 2005, pp. 441–455.
- [14] J. Jean, A. Moradi, T. Peyrin, and P. Sasdrich, "Bit-Sliding: A Generic Technique for Bit-Serial Implementations of SPN-based Primitives," in *Cryptographic Hardware and Embedded Systems - CHES 2017*. Springer, Cham, sep 2017, pp. 687–707.