Energy and Side-channel Security Evaluation of Near-threshold Cryptographic Circuits in 28nm FD-SOI Technology

Arthur Beckers
imec-COSIC, ESAT, KU Leuven
Leuven, Belgium
arthur.beckers@kuleuven.be

Roel Uytterhoeven
MICAS, ESAT, KU Leuven
Leuven, Belgium
roel.uytterhoeven@kuleuven.be

Thomas Vandenabeele
imec-COSIC, ESAT, KU Leuven
Leuven, Belgium
thomas.vandenabeele@kuleuven.be

Jo Vliegen
imec-COSIC, ESAT, KU Leuven
Leuven, Belgium
jo.vliegen@kuleuven.be

Lennert Wouters
imec-COSIC, ESAT, KU Leuven
Leuven, Belgium
lennert.wouters@kuleuven.be

Joan Daemen
Digital Security Group
Radboud University
Nijmegen, The Netherlands
joan@cs.ru.nl

Wim Dehaene
MICAS, ESAT, KU Leuven
Leuven, Belgium
wim.dehaene@kuleuven.be

Benedikt Gierlichs
imec-COSIC, ESAT, KU Leuven
Leuven, Belgium
benedikt.gierlichs@kuleuven.be

Nele Mentens
LIACS, Leiden University
Leiden, The Netherlands
imec-COSIC, ESAT, KU Leuven
Leuven, Belgium
n.mentens@liacs.leidenuniv.nl

ABSTRACT

This paper is the first to present an implementation of a cryptographic circuit in 28nm FD-SOI using near-threshold design. The implemented cipher, Ketje Jr, is a lightweight authenticated encryption algorithm. The energy consumption of representative authenticated encryption operations as well as the information leakage through the power consumption side-channel are evaluated. The results show that an ultra-low energy implementation can be achieved, and that the near-threshold design has little influence on the Signal to Noise Ratio in the power measurements of our chip.

CCS CONCEPTS

• **Hardware** → **Integrated circuits**; • **Security and privacy** → **Hardware attacks and countermeasures**.

KEYWORDS

28nm FD-SOI, authenticated encryption, Ketje Jr, near-threshold design, cryptographic circuit, low-power design, power analysis, side-channel analysis, energy evaluation

ACM Reference Format:
Arthur Beckers, Roel Uytterhoeven, Thomas Vandenabeele, Jo Vliegen, Lennert Wouters, Joan Daemen, Wim Dehaene, Benedikt Gierlichs, and Nele Mentens. 2022. Energy and Side-channel Security Evaluation of Near-threshold Cryptographic Circuits in 28nm FD-SOI Technology. In *19th ACM International Conference on Computing Frontiers (CF'22), May 17–19, 2022, Torino, Italy*. ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3528416.3530992

CF'22, May 17–19, 2022, Torino, Italy

ACM ISBN 978-1-4503-9338-6/22/05.
https://doi.org/10.1145/3528416.3530992

1 INTRODUCTION

Battery-powered or energy-harvesting systems are in need of low-power computing. In order to deal with this challenge, low-power techniques for the design of integrated circuits have been introduced at different levels, e.g. at the technology level, the circuit level, the architecture level and the system level. In this paper, we evaluate circuits that are implemented using near-threshold design [12] in FD-SOI technology.

When energy-constrained systems process sensitive data, cryptographic algorithms are needed for encryption and authentication. That is why the circuits presented in this work are implementing an authenticated encryption algorithm. Authenticated encryption takes a plaintext (that needs to be authenticated and encrypted) and associated data (that only need to be authenticated) as an input, and generates a ciphertext and an authentication tag. The authenticated encryption algorithm we consider in this paper, is Ketje Jr, proposed by Bertoni et al. in [2], with low area footprint as a design goal.

Our contributions are the following. We demonstrate two fully functional Ketje Jr cores, based on traditional super-threshold design and near-threshold design. Our comparative empirical evaluation consists of (1) an analysis of the minimal VDD and energy consumption as a function of the operating frequency; and (2) an analysis of the impact on the Signal to Noise Ratio of power measurements for side-channel attacks.

2 RELATED WORK

Existing work on security primitives in 28nm FD-SOI technology (excluding research based on simulations only) is limited. The work

of Danger et al. [5] concentrates on the implementation and evaluation of Physically Unclonable Functions (PUFs) and True Random Number Generators (TRNGs). In [6], Dutertre et al. compare the vulnerability to laser attacks of CMOS FD-SOI versus CMOS bulk technology. Their experiments are based on an implementation of the Advanced Encrypton Standard (AES), an encryption algorithm that is sought to be replaced in lightweight applications by novel authenticated encryption algorithms. Kamel et al. [8] present the implementation and side-channel evaluation of a Learning Parity with Physical Noise (LPPN) processor, which is a component on which authentication protocols can be built. In [9], the intrinsic noise of MOSFETs is simulated and security evaluation metrics are discussed based on the simulation results. None of the aforementioned papers apply a near-threshold design strategy, and none of these papers tackle authenticated encryption. Our fabricated chip gives us the unique opportunity to present the first energy consumption and side-channel analysis results of a lightweight authenticated encryption algorithm in 28nm FD-SOI, based on near-treshold design.

3 IMPLEMENTATION

Our chip is fabricated in 28nm FD-SOI technology. The floorplan in Fig. 1 shows the positions of the super-threshold core (Core0) and the near-threshold core (Core1), as well as the 2048x16-bit RAM blocks used for writing and reading data to and from the cores. The control logic operates based on custom instructions that are written into the RAM write block. It can initiate a single as well as batch tests. The other blocks in the chip are not considered in this paper. The supply voltages of the cryptographic cores are isolated from each other and from the supply voltage of the control logic and the RAM blocks. The control logic and the RAM blocks are always powered at 1V.

Core0 is designed with the standard cell library provided by the semiconductor manufacturer, with a target VDD of 1V. Core1 is designed with a standard cell library that was re-characterized at 0.4V, just like the microprocessor chip presented in [10] and the simulation-based energy evaluation of different implementations of the S-box in AES in [11]. The circuits have a density of 65.4% versus 34.4%, and 10280 versus 5410 equivalent NAND gates, for Core0 and Core1, respectively. We expect that this difference in area can be attributed to a difference in operating regime. Fig. 2 shows a photo of the die. The test setup shown in Fig. 3 consists of a Xilinx ZedBoard, which hosts a Zynq-7000 SoC FPGA with Python test code running on the embedded ARM processor. The choice of core under test is made by physical connections.

We did not apply any power optimization techniques at the circuit or architecture level – both cores are based on a straightforward round-based architecture that operates at one cycle per round, as

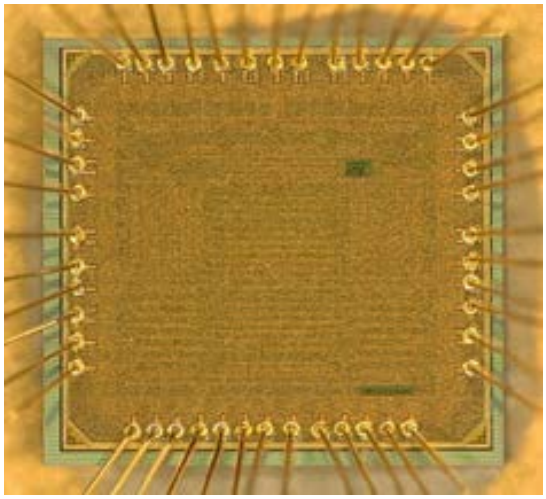

Figure 2: Photograph of the chip.

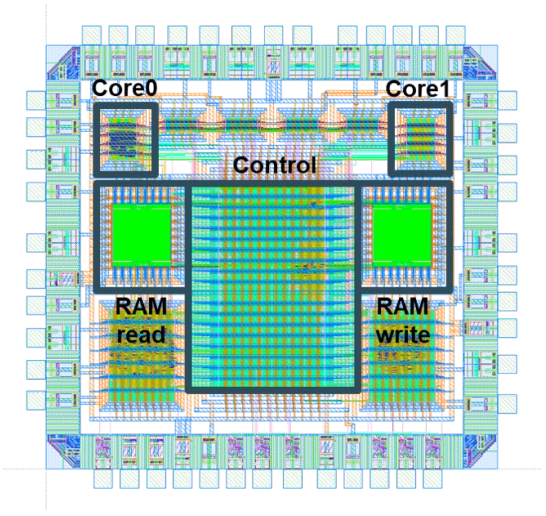

Figure 1: Floorplan of the chip with super-threshold (Core0) and near-threshold (Core1) cores.

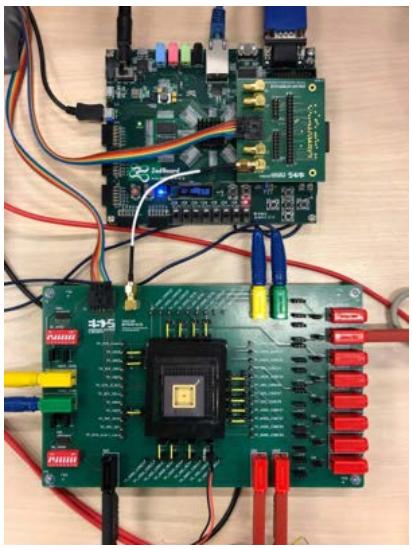

Figure 3: Measurement setup with the chip on a custom PCB at the bottom and the Xilinx ZedBoard at the top.

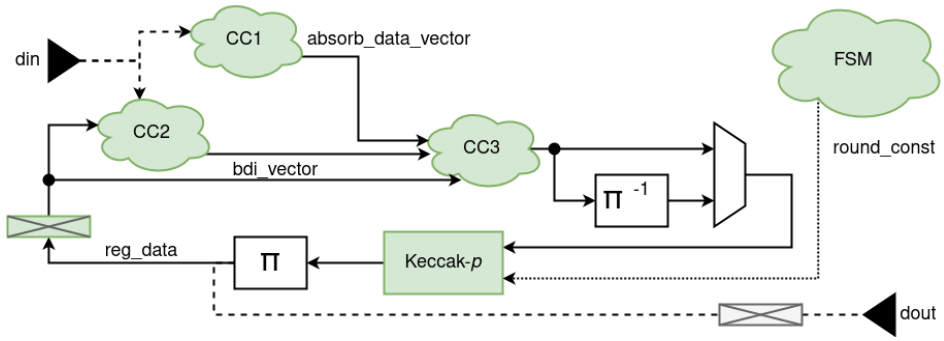

Figure 4: Hardware architecture of the Ketje Jr cores.

shown in Fig. 4. Data arrive at the top left corner in 16-bit chunks and are fed into two combinational clouds (CC1 and CC2). CC1 generates a 200-bit vector (absorb_data_vector) based on the input data and the configuration parameters provided by the FSM. CC2 generates a 200-bit vector (bdi_vector), which is also based on the internal state. The two vectors are merged with the internal state in a third combinatorial cloud (CC3). Then, the updated state is passing the round function which implements the twisted permutation Keccak-p, followed by the π function [2]. In some rounds, these operations are preceded by the $\pi - 1$ function. With one register in the loop, the resulting architecture executes one round per cycle.

4 MEASUREMENTS

4.1 Energy consumption

To obtain the designs' current consumption, we measure the voltage drop across a 1Ω resistor in the VDD line. VDD is supplied using a standard (low-noise) bench supply and the output of the measurement circuit is sampled by a digital storage oscilloscope. Measurements are done at the lowest possible VDD for which the chip operation is reliable. We evaluate the energy consumption in three different use cases that differ in how many reads and writes to and from memory are performed. The predominating number of bytes in the three use cases are (1) in the associated data, (2) in the plaintext/ciphertext, and (3) in the authentication tag, respectively. When the data bytes are transferred from the memory to the core, the processing of the data starts simultaneously. Therefore, our measurements cover both the data transfer and the processing. We take the average over the three use cases to generate the energy results shown in Fig. 5 and Fig. 6. The blue lines show that the energy per cycle is significantly higher for Core0. The first reason is the difference in area, reported in Section 3. The second reason is related to the difference in minimal VDD that can be observed in Fig. 5 and Fig. 6. The red lines show the minimal VDD at which the cores function correctly. Core0 reaches its minimal energy point at 0.48V, while Core1 goes down to 0.44V. Although the absence of level shifters between Core0 and the rest of the chip limits the minimal VDD at lower frequencies, Fig. 6 shows that our near-threshold design pays off, because the minimal VDD of Core0 clearly rises above the minimal VDD of Core1 for higher frequencies. The minimal energy points for Core0 and Core1 are 5.58pJ/cycle at 25MHz and 1.55pJ/cycle at 40MHz, respectively.

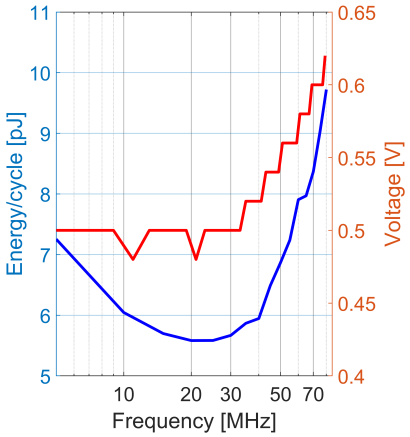

Figure 5: Energy/cycle (blue line) and minimal VDD (red line) for Core0.

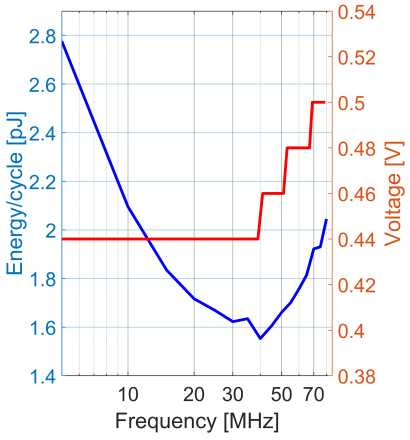

Figure 6: Energy/cycle (blue line) and minimal VDD (red line) for Core1.

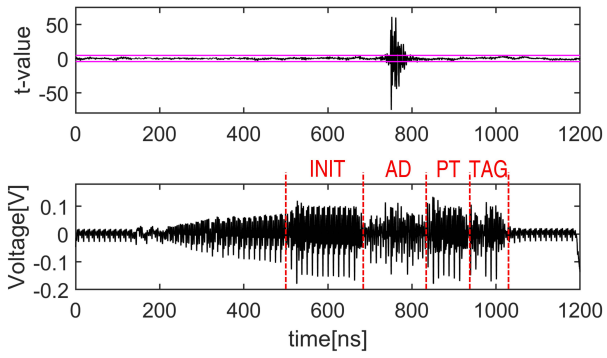

Figure 7: t-test plot (top) and instantaneous current consumption (bottom) of Core0.

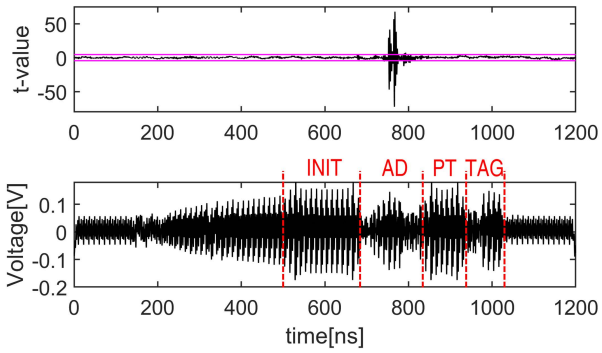

Figure 8: t-test plot (top) and instantaneous current consumption (bottom) of Core1.

Table 1 compares the energy consumption of our cryptographic cores at near- and super-threshold with other related cryptographic implementations. Note that [1] and [3] are based on circuit-level optimizations, use only post-synthesis simulation and exclude memory transfers. We are not aware of any (authenticated) encryption chips in recent technologies that report the energy consumption.

4.2 Side-channel Analysis

To analyze the side-channel resistance of the cores, we perform Test Vector Leakage Assessment with a specific t-test [4, 7] as well as measurements of the Signal-to-Noise Ratio (SNR). Power traces are acquired using a custom carrier board and a Tektronix CT-1 current probe inserted in the core supply. To compare the cores, we acquire two sets of measurements for each core: one at nominal VDD (1V) and one at minimal VDD. All measurements are done at a frequency of 40 MHz.

We only perform a specific t-test, because a non-specific t-test would show leakage over the entire execution, as inputs are processed throughout the execution of Ketje. We perform a specific t-test to make sure we see leakage caused by the operation and not simply input/output leakage.

Fig. 7 (bottom) shows the instantaneous power consumption of Core0 while performing an authenticated encryption. One can clearly distinguish the different phases of the authenticated encryption algorithm in the power trace. First data is loaded into the core in the initialization phase (INIT), then the associated data (AD) is fed into the algorithm, followed by the encryption of the plaintext (PT) and the generation of the tag (TAG).

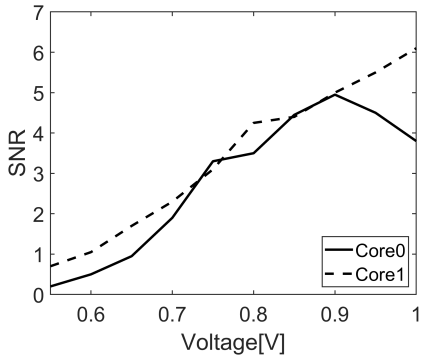

Figure 9: Signal-to-Noise Ratio (SNR) as a function of VDD for the power measurements of Core0 and Core1.

Fig. 7 (top) shows the result of the specific t-test based on 1000 measurement traces. The targeted intermediate state occurs at approximately 750 ns. In Fig. 8, similar results are shown for Core1. The inputs to the algorithm where chosen such that the state register was either random or contained all zeros at the second to last round of the AD being fed into the algorithm. The t-test is a statistical test which tells us whether or not the means of two distributions are significantly different. The power traces are grouped based on the state register being either zero or random before the t-test is applied.

If the t-value passes the 4.5 threshold, the evaluator has a high confidence that the implementation leaks information related to the secret state. The 750 ns sample is used to calculate the SNR reported in Fig. 9. Each point in the plot is based on 1000 traces. We show that near-threshold design does not result in a reduced SNR although it consumes less power for a given voltage. On average the SNR of the sub-threshold design is even higher than traditional super-threshold design. Near-threshold designs in 28nm FD-SOI by themselves thus do not add any side-channel leakage in our test chip. A possible reason could be that the higher density in the near-threshold cores in our chip influences the SNR. The figure also shows that VDD has a significant impact on the SNR.

5 CONCLUSION

We presented a chip in 28nm FD-SOI technology, implementing two Ketje Jr cores for authenticated encryption, one based on regular super-threshold design and the other one based on near-threshold design. The energy measurements show that the near-threshold core is more efficient than the super-threshold core, and that both cores consume significantly less energy than existing work. The side-channel evaluation, based on Test Vector Leakage Assessment and the calculation of the Signal-to-Noise Ratio, shows no significant difference between the two cores.

Table 1: Comparison of the energy per cycle of (authenticated) encryption circuits.

Reference	E/cycle	Algorithm	Technology	Remarks
[1]	> 34pJ	Encryption	90nm	Simulated post-synthesis results, energy-optimized circuits, data transfer not included
[3]	> 55pJ	Authenticated encryption		
Our super	5.58pJ		28nm FD-SOI	Measured results on fabricated chip, fully parallel implementation, data transfer included
Our near	1.55pJ			

ACKNOWLEDGMENT

This work is supported by CyberSecurity Research Flanders with reference number VR20192203 and ERC-ADG 695305 CATHEDRAL. Joan Daemen is supported by ERC-ADG 788980 ESCADA. This work is also supported by NWO through the PROACT project with reference number NWA.1215.18.014. We thank Andreia Cathelin, Sylvain Clerc and Bernard Kasser of STMicroelectronics for their help.

REFERENCES

[1] Subhadeep Banik, Vasily Mikhalev, Frederik Armknecht, Takanori Isobe, Willi Meier, Andrey Bogdanov, Yuhei Watanabe, and Francesco Regazzoni. 2018. Towards low energy stream ciphers. *IACR Transactions on Symmetric Cryptology* (2018), 1–19.

[2] Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer. 2016. CAESAR submission: Ketje v2. *Candidate of CAESAR Competition* (2016).

[3] Andrea Caforio, Fatih Balli, and Subhadeep Banik. 2020. Energy analysis of lightweight aead circuits. In *International Conference on Cryptology and Network Security*. Springer, 23–42.

[4] Jeremy Cooper, Elke DeMulder, Gilbert Goodwill, Joshua Jaffe, Gary Kenworthy, and Pankaj Rohatgi. 2013. Test Vector Leakage Assessment (TVLA) methodology in practice. International Cryptographic Module Conference. http://icmc-2013.org/wp/wp-content/uploads/2013/09/goodwillkenworthtestvector.pdf.

[5] Jean-Luc Danger, Risa Yashiro, Tarik Graba, Yves Mathieu, Abdelmalek Si-Merabet, Kazuo Sakiyama, Noriyuki Miura, and Makoto Nagata. 2018. Analysis of mixed puf-trng circuit based on sr-latches in fd-soi technology. In *2018 21st Euromicro Conference on Digital System Design (DSD)*. IEEE, 508–515.

[6] Jean-Max Dutertre, Vincent Beroulle, Philippe Candelier, Stephan De Castro, Louis-Barthelemy Faber, Marie-Lise Flottes, Philippe Gendrier, David Hély, Régis Leveugle, Paolo Maistri, et al. 2018. Sensitivity to Laser Fault Injection: CMOS FD-SOI vs. CMOS Bulk. *IEEE Transactions on Device and Materials Reliability* 19, 1 (2018), 6–15.

[7] Gilbert Goodwill, Benjamin Jun, Josh Jaffe, and Pankaj Rohatgi. 2011. A testing methodology for side channel resistance validation. NIST non-invasive attack testing workshop. http://csrc.nist.gov/news_events/non-invasive-attack-testing-workshop/papers/08_Goodwill.pdf.

[8] Dina Kamel, Davide Bellizia, Olivier Bronchain, and François-Xavier Standaert. 2020. Side-channel analysis of a learning parity with physical noise processor. *Journal of Cryptographic Engineering* (2020), 1–9.

[9] Kashif Nawaz, Léopold Van Brandt, Itamar Levi, François-Xavier Standaert, and Denis Flandre. 2019. A security oriented transient-noise simulation methodology: Evaluation of intrinsic physical noise of cryptographic designs. *Integration* 68 (2019), 71–79. https://doi.org/10.1016/j.vlsi.2019.06.006

[10] Roel Uytterhoeven and Wim Dehaene. 2018. A sub 10 pJ/Cycle Over a 2 to 200 MHz Performance Range RISC- V Microprocessor in 28 nm FDSOI. In *ESSCIRC 2018 - IEEE 44th European Solid State Circuits Conference (ESSCIRC)*. 236–239. https://doi.org/10.1109/ESSCIRC.2018.8494259

[11] Thomas Vandenabeele, Roel Uytterhoeven, Wim Dehaene, and Nele Mentens. 2018. A Systematic Performance Comparison of Ultra Low-Power AES S-Boxes. In *2018 28th International Symposium on Power and Timing Modeling, Optimization and Simulation (PATMOS)*. IEEE, 248–253.

[12] Alice Wang, Benton H Calhoun, and Anantha P Chandrakasan. 2006. *Sub-threshold design for ultra low-power systems*. Vol. 95. Springer.