RISC-V Day Tokyo 2024 Summer, Tokyo, 1st August 2024

RISC-V System-on-a-Chip with ASCON Cryptography for IoT applications on 180nm CMOS

Khai-Duy Nguyen[1], Tuan-Kiet Dang[1], Binh Kieu-Do-Nguyen[1], Cong-Kha Pham[1], and Trong-Thuc Hoang[1]
[1]University of Electro-Communications (UEC), Tokyo, Japan

I. INTRODUCTION

The number of IoT devices has grown significantly in recent years, and edge computing in IoT is considered a new and growing trend in the technology industry. While cryptography is widely used to enhance the security of IoT devices, it also carries limitations such as resource constraints or latency. Therefore, lightweight cryptography (LWC) balances commensurate resource usage and maintaining security while minimizing system costs. The ASCON stands out among the LWC algorithms as a potential target for implementation and cryptoanalysis. It provides authenticated encryption with associated data (AEAD) and hashing functionalities in many variants, aiming for various applications. In this brief, we present an implementation of ASCON cryptography as a peripheral of a RISC-V System-on-a-Chip (SoC). The ASCON crypto core occupies 1,424 LUTs in FPGA and 17.4kGE in 180nm CMOS technology while achieving 417Gbits/J energy efficiency at a supply voltage of 1.0V and frequency of 2MHz.

II . PROPOSED ARCHITECTURE

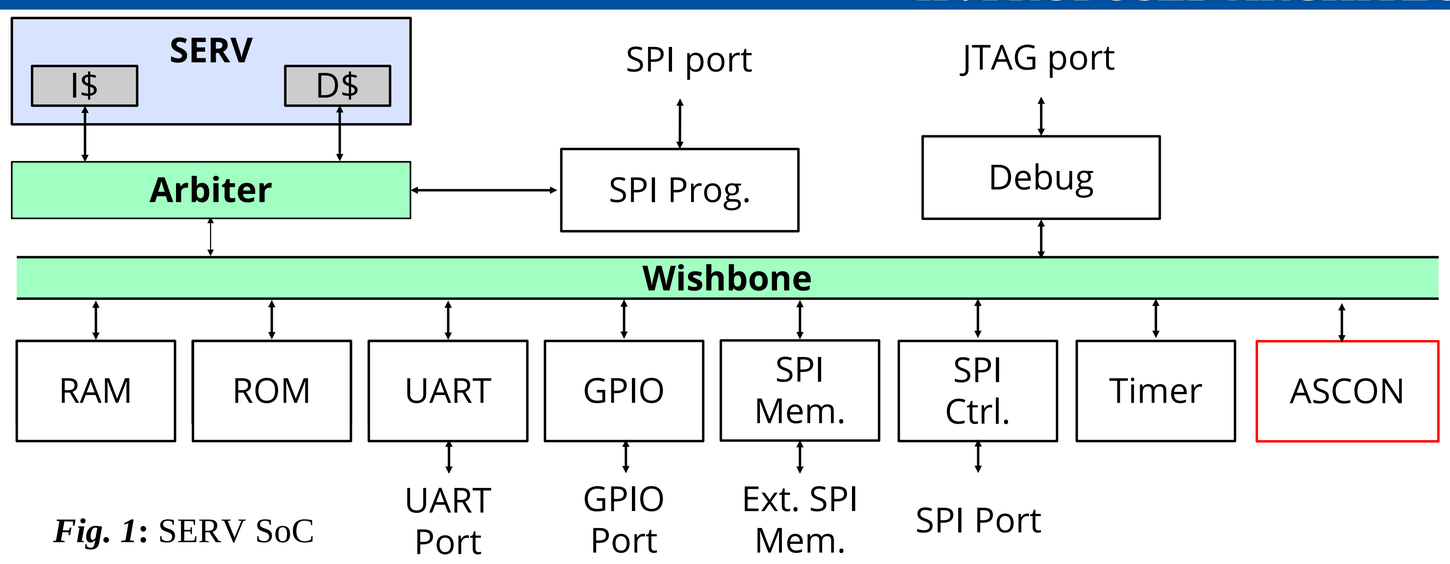


***Fig. 1*:** SERV SoC

The architecture shows the implementation of both the ASCON-128 and ASCON-Hash variants. This design revolves around a 320-bit register containing the state of ASCON and a permutation block to be implemented. There is only one transformation per clock cycle without using a pipelined architecture. Given that this crypto core is integrated with a 32-bit processor and bus system, the data input and output for the ASCON implementation are fixed at 32 bits. A shift register converts the input data from 32 to 128 bits, accommodating fixed-sized parameters larger than 32 bits.

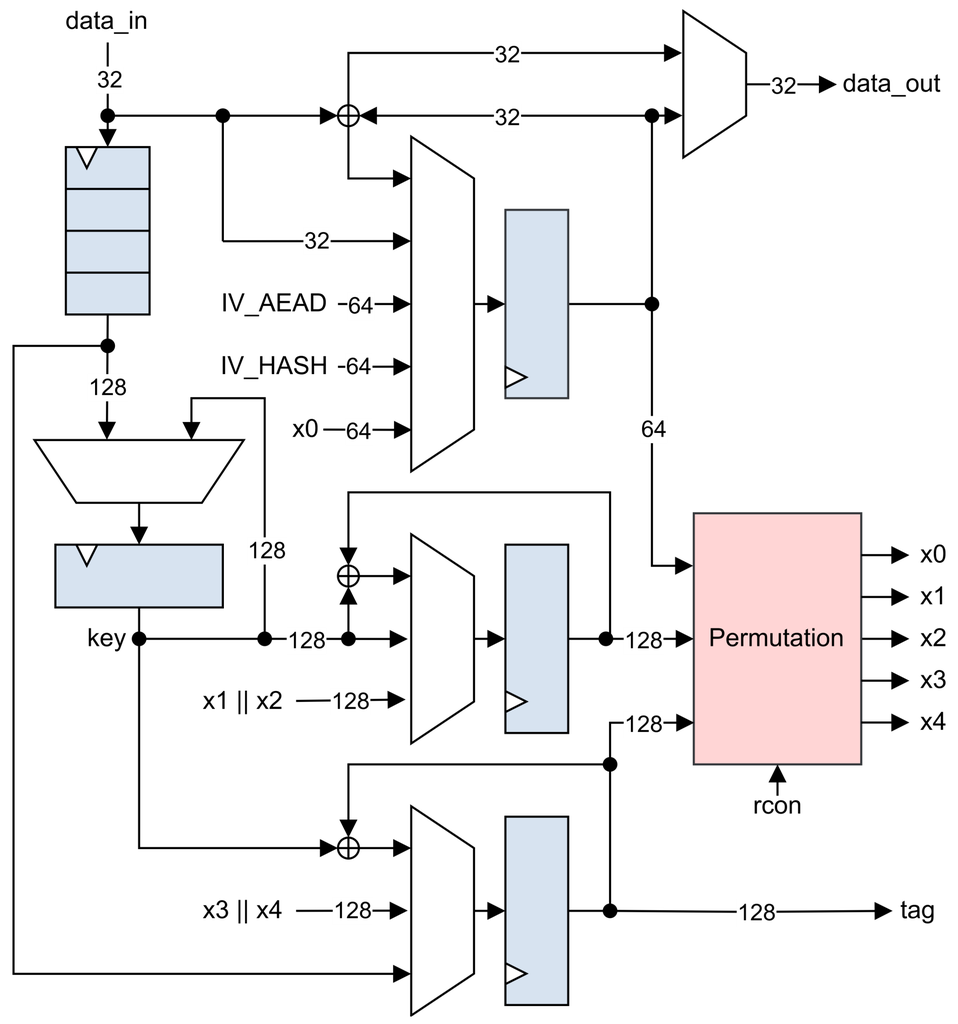
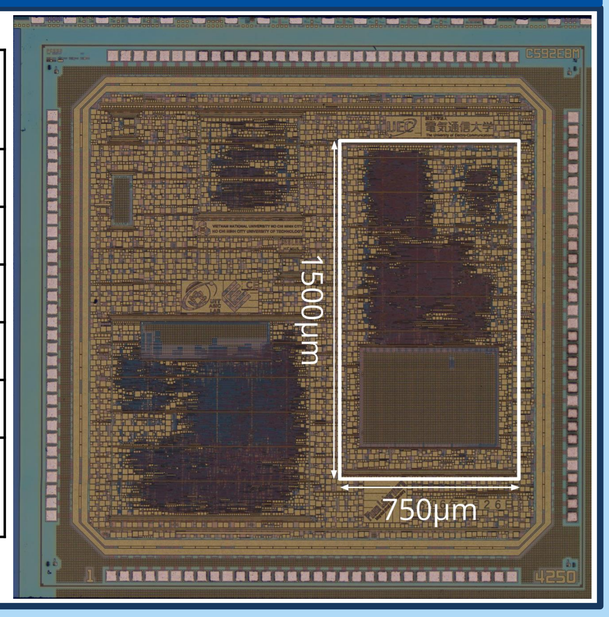


***Fig. 2*:** ASCON crypto core architecture

III . CHIP MICROGRAPH

Operating Voltage	1.0V~2.0V
Area[µm2]	1,125,000
Gate Count	86kGE
Frequency	32kHz~40MHz
Processor	SERV-32E
Memory	4kB
ASCON variant	ASCON-128+ ASCON-Hash



IV . MEASUREMENT RESULTS

Table I. FPGA AEAD in comparison.

	LUTs	Variant	Frequency [MHz]	FPGA	TP [Mbps]	TP/Area [Mbps/LUT]
iSES'22[1]	1,330	ASCON-128	107	Artix-7	457	0.343
IoT'22[2]	2,060	ASCON-128/a	206	Spartan-6	315.2*	0.153
SOCC'22[3]	1,548	ASCON-128/a ASCON-Hash/a	244	Artix-7	-	-
ICECS'22[4]	1,324	ASCON-128	280	Artix-7	2,560	1.93
FCCM'18[5]	1,402	ASCON-128	208	Spartan-6	1,906	1.36
This work	1,277	ASCON-128 ASCON-Hash	294	Artix-7	2,233	1.75

*Throughput value of ASCON-128

- Lowest resource consumption with the highest maximum frequency
- Support both AEAD and hash function

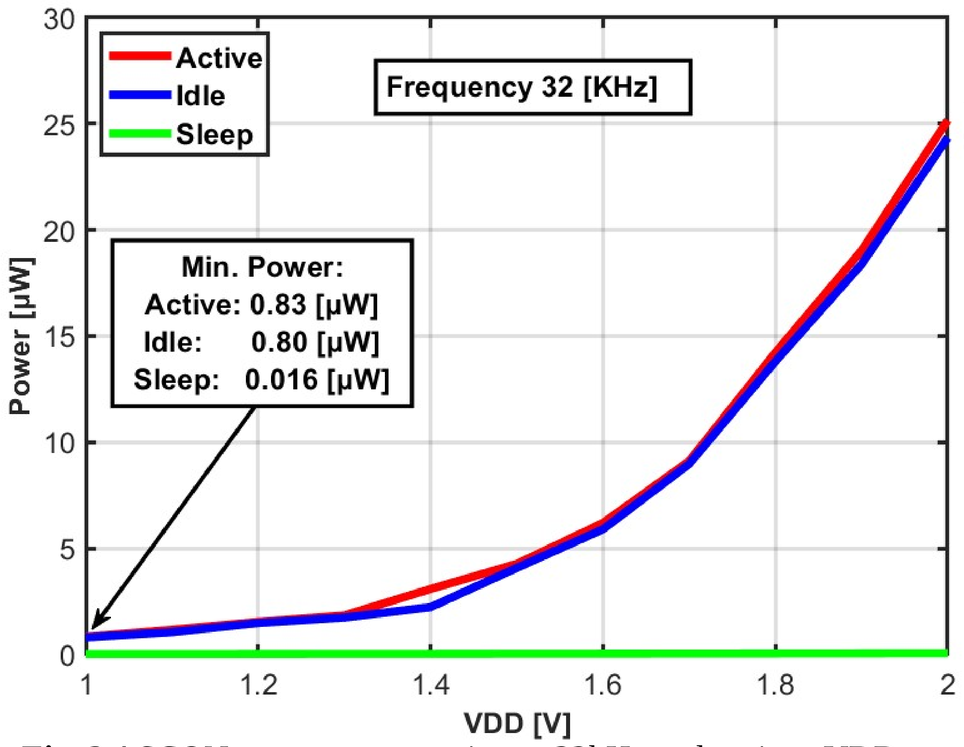


Fig. 3 ASCON power consumption at 32kHz and various VDD

First implementation of ASCON on real silicon with sub-µW power consumption

Table II. ASIC implementation in comparison.

	Tech.	Measure	Area (µm2)	Gate Eq. [kGE]	Energy Efficiency [Gbits/J]
ISDFS'24[6]	22nm	Simulation	2,206	-	2,223
	130nm		41,821	-	179
ISCAS'22[7]	22nm		2,193	11	1,528
ICECS'22[8]	28nm		4,971	10.1	134
SOCC'22[3]	28/32nm		-	25.1	3,628
This work	180nm	Silicon	166,802	17.4	417 3,628*

*Scaled to 32nm [9]

REFERENCES

[1] K. Raj, and S. Bodapati, "FPGA Based Light Weight Encryption of Medical Data for IoMT Devices using ASCON Cipher," iSES, 2022.
[2] S. Khan *et al.*, "Scalable and Efficient Hardware Architectures for Authenticated Encryption in IoT Applications," IEEE Internet of Things Journal, 2021.
[3] X. Wei *et al.*, "RECO-HCON: A High-Throughput Reconfigurable Compact ASCON Processor for Trusted IoT," SOCC, 2022 .
[4] C. Guo *et al.*, "Unified Lightweight Authenticated Encryption for Resource-Constrained Electronic Control Unit," ICECS, 2022.
[5] F. Farahmand *et al.*, "Improved Lightweight Implementations of CAESAR Authenticated Ciphers," FCCM, 2018.
[6] I. Elsadek, and E. Y. Tawfik, "Efficient Programable Architecture for LWC NIST FIPS Standard ASCON," ISDFS, 2024.
[7] I. Elsadek *et al.*, "Hardware and Energy Efficiency Evaluation of NIST Lightweight Cryptography Standardization Finalists," ISCAS, 2022.
[8] N. Roussel *et al.*, "CMOS/STT-MRAM Based Ascon LWC: a Power Efficient Hardware Implementation," ICECS, 2022.
[9] A. Stillmaker and B. Baas, "Scaling Equations for the Accurate Predic- tion of CMOS Device Performance from 180nm to 7nm," Integration, 2017.

ACKNOWLEDGEMENT

The VLSI chip in this study has been fabricated through the activities of VLSI Design and Education Center (VDEC), the University of Tokyo with the collaboration by Rohm Corporation and Toppan Printing Corporation.

Email: khaiduy@vlsilab.ee.uec.ac.jp