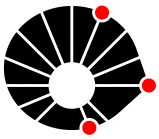

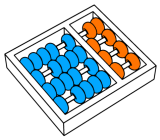

Exploring ASCON on RISC-V

Paulo Pacitti *Julio López*

Technical Report - IC-23-14 - Relatório Técnico
November - 2023 - Novembro

UNIVERSIDADE ESTADUAL DE CAMPINAS
INSTITUTO DE COMPUTAÇÃO

Exploring ASCON on RISC-V

Paulo Pacitti* Julio López†

Abstract

Sed quis lorem magna. Sed sit amet ullamcorper massa, sit amet placerat lectus. Suspendisse pulvinar ipsum sed enim commodo, ac malesuada lectus finibus. Aliquam eu eros eleifend, interdum nisi faucibus, viverra sapien. Vivamus lobortis a lectus eu rutrum. Quisque in est sit amet libero sollicitudin ornare a sed ipsum. Suspendisse potenti. Aliquam sit amet nisi sed nulla tincidunt imperdiet. Pellentesque elementum lacus eget dolor gravida lobortis. Sed placerat lacinia nisi, sed varius turpis facilisis ac.

1 Introduction

Sed quis lorem magna. Sed sit amet ullamcorper massa, sit amet placerat lectus. Suspendisse pulvinar ipsum sed enim commodo, ac malesuada lectus finibus. Aliquam eu eros eleifend, interdum nisi faucibus, viverra sapien. Vivamus lobortis a lectus eu rutrum. Quisque in est sit amet libero sollicitudin ornare a sed ipsum. Suspendisse potenti. Aliquam sit amet nisi sed nulla tincidunt imperdiet. Pellentesque elementum lacus eget dolor gravida lobortis. Sed placerat lacinia nisi, sed varius turpis facilisis ac.

2 Background

2.1 Ascon

Ascon is a family of algorithms for lighweight cryptography, designed to be used in constrained environments, like embedding computing. Designed by cryptographers from Graz University of Technology, Infineon Technologies, Intel Labs, and Radboud University, Ascon has been selected as the new standard for lightweight cryptography in the new NIST Lightweight Cryptography competition (2019–2023).

2.2 RISC-V

3 Implementation

The device used for this research is the MangoPi MQ-Pro, a SBC powered with a Allwinner D1 chip and 1GB DDR3 of RAM, with Wi-Fi, Bluetooth and HDMI video output. The Allwinner D1 chip contains a T-Head Xuantie C906 core, a RISC-V 64-bit 1GHz CPU supporting RV64GC ISA. The board runs Ubuntu Server 23.04, running the latest Linux kernel.

*Computer Engineering Undergraduate, Institute of Computing, UNICAMP. p185447@dac.unicamp.br
†Associate Professor, Institute of Computing, UNICAMP. jlopez@ic.unicamp.br

4 Results

5 Discussion

6 Conclusions

References

[1] A. V. Aho, J. E. Hopcroft and J. D. Ullman, *The Design and Analysis of Computer Algorithms,* Addison-Wesley (1901).

[2] D. E. Knuth and L. Lamport, *A structural analysis of the role of gnus and gnats in the post-modernistic, crypto-existential Weltanschauung of neo-liberal Tibeto-Vietnamese leaf blower operators as manifest in the sexual symbology of the Los Angeles Phone Directory.* Journal of Gnu Technology, **23** (6), 12–87 (March 1996).