Contribution ID: **54**

Type: **POSTER**

BipBip: A Lightweight Crypto Algorithm for Open Source Processors and AI Accelerators

Abstract—Lightweight cryptography is essential in systems constrained by power, performance, and area (PPA), particularly in IoT and embedded applications. To address these challenges,we present a RISC-V implementation of the BipBip algorithm, a symmetric tweakable block cipher tailored for fine-grained protection of pointer and contextual data in the CPU path of an SoC. Unlike larger-block ciphers like Deoxys-BC, PRESENT, Joltik, and Kisau, which are motivated by the need for pointer encryption, BipBip uses 24-bit blocks, a 40-bit tweak,and a 256-bit key to achieve ultra-low latency. This unique configuration supports contextual encryption without the overhead of nonce management, enabling predictable security in resource-limited systems. Our contributions emphasize RTL/FPGA implementation and SoC integration. We demonstrate a 2×2 mm block implementation of BipBip in Intel's 16 nm technology, operating at 300 MHz and with a full encryption-to-decryption path in two cycles.The lightweight primitive can be used in trusted microelectronics, requiring a small footprint, consistent latency, and integration with open-source CPUs and AI acceleration

Academic or Professional Status

Graduate Student

Author: STOYANOV-ROBERTS, Alexander (Morgan State University CAP Center)

Co-authors: JILES, Dranel (Morgan State); Mr OKONKWO, Favour; Mr CONWAY, Jeremiah; DOMINGUEZ, Jose (Morgan State university); Dr KORNEGAY, Kevin (Morgan State CAP Center); Mr RAO, Shameer

Presenter: STOYANOV-ROBERTS, Alexander (Morgan State University CAP Center)

Session Classification: Poster Session

Track Classification: Materials & Devices: Materials & Devices - (a)