An Adiabatic Quantum-flux-parametron Block Permutation Unit for a Superconductor SHA-3 Cryptoprocessor

Christopher L. Ayala[1], Tomoyuki Tanaka[2], Ro Saito[2], and Nobuyuki Yoshikawa[1]

[1]Institute of Advanced Sciences, Yokohama National University, Japan
[2]Department of Electrical Engineering and Computer Engineering, Yokohama National University, Japan

E-mail: ayala-christopher-pz@ynu.ac.jp

***Abstract* – The computing demands for IoT, Big Data, and social media have been rising rapidly and it is unclear whether conventional CMOS technology can continue to serve as the technological platform to support these services in the long term. Adiabatic quantum-flux-parametron (AQFP) superconductor logic is an alternative technology that can potentially fulfill this role. When using a 10 kA/cm^2 unshunted Nb/AlOx/Nb Josephson junction (JJ) fabrication process available today, AQFP logic can operate with switching energies approaching a zeptojoule per JJ at a clock frequency of 5 GHz. Previously, we successfully demonstrated a 4-bit microprocessor called MANA, an important milestone chip with over 20k JJs. A breakout chip of the execution units operated up to 2.5 GHz. The MANA project helped identify new research areas to improve AQFP technology including the need for more compact logic cells, stronger signal driving capability, and a scalable power-clock network, to name a few.**

We have been seeking new computational areas where our technology can make a major impact, one of which is the cryptoprocessing space. In today's informational society, it is important to ensure the security and privacy of data transmission. One way to achieve this is through hashing algorithms such as the Secure Hash Algorithm-3 (SHA-3). An efficient hardware implementation of SHA-3 for use with high-throughput communication links would be very beneficial. Hashing is also one of the various ways to compute the power intensive "proof-of-work" for cryptocurrencies such as Bitcoin. Towards this, we have investigated the implementation of the core component of SHA-3 known as the block permutation unit. In short, this unit comprises five different permutation stages: θ (theta), ρ (rho), π (pi), χ (chi), and ι (iota), each being a combination of AND, XOR, ROT, and NOT operations.

We implemented the block permutation unit on a 7 mm x 7 mm chip using the AIST four-layer 10 kA/cm^2 High-speed STandard Process (HSTP). The active circuit area is 4.5 mm x 5.5 mm (w x h) containing approximately 13k JJs. Long cyclic AQFP buffer arrays were used to help partially emulate a 25-bit state register of the SHA-3 algorithm. A microwave power-clock binary tree was used to equally distribute clocks horizontally across the chip to manage clock skew. AQFP-based SerDes circuits were designed to help simplify the experimental I/O during measurement. Voltage drivers composed of dc-SQUID stacks were used to readout intermediate results at speed, and a conservative dc-SQUID output driver was used to readout the serialized results at low-speed. Experimental results indicate successful operation up to 7 GHz, making this the largest AQFP circuit to be demonstrated at GHz

speeds to date. This demonstration marks a promising future towards energy-efficient superconductor-based cryptoprocessing.

***Keywords (Index Terms)* — AQFP, adiabatic, parametron, SHA3, crypto, hash**

IEEE CSC & ESAS SUPERCONDUCTIVITY NEWS FORUM (global edition), March 2023. Presentation 1EOr2B-03 given at Applied Superconductivity Conference, Honolulu, HI, USA, October 24, 2022.