Contribution ID: **67**   Type: **ORAL**

Design of a High-Performance 1024-bit Arithmetic Logic Unit for Cryptographic Acceleration

Wednesday, April 1, 2026 3:25 PM (20 minutes)

The project is conducted as a collaborative effort involving undergraduate engineering and physics students, with the dual objectives of achieving a tapeout-ready design and providing hands-on training in modern VLSI workflows. The ALU architecture is optimized for wide-word arithmetic commonly required in public-key cryptography, including modular addition, subtraction, and logic operations.

The design process is organized into several stages: architectural specification and operation selection; register-transfer level (RTL) development and functional verification; pipelined micro-architecture design; synthesis, placement, and routing; and timing, power, and area optimization. A deeply pipelined, systolic approach is employed to overlap input loading, computation, and output generation, enabling high throughput despite the large operand width. The implementation targets the GlobalFoundries 180 nm CMOS (180MCU) technology, with the end goal of participating in an academic tapeout.

Significant challenges were encountered, including the steep learning curve associated with commercial Synopsys design tools, limited or fragmented documentation, and routing congestion arising from the extreme datapath width. These challenges motivated a parallel evaluation of open-source VLSI design flows. Preliminary results indicate that open-source toolchains, such as LibreLane, provide a viable and pedagogically effective alternative for early-stage prototyping and education, while maintaining compatibility with industry-standard design practices.

Academic or Professional Status

Faculty

Authors: VRINCEANU, Daniel (Texas Southern University); Dr THOMAS, Graham (Texas Southern University)

Co-authors: ADAMSON, Adebola (Texas Southern University); Mr WARI, Mustafa (Texas Southern University)

Presenter: Dr THOMAS, Graham (Texas Southern University)

Session Classification: Technical Session 2

Track Classification: AI in Semiconductors