MERL
Accelerating Engineering Innovation

SuperSHA3

RISCV Based SoCNow Supported Hardware Accelerator for SHA3(256) Algorithm With Generalized Interfaces

Talha Ahmed, Shahzaib Kashif, Abdul Samad, Maira Usman

Project Proposal

Problem:

The calculation of SHA-3 is very computationally intensive, limiting its applicability on RISC V processors used in modern embedded systems and Systems on Chips (SoCs). However, its underlying SHA256 algorithm is computational intensive and thus limits its deployment on IoT systems which are normally equipped with 32-bit resource constrained embedded processors. There is a single verified open-source SHA3 accelerator which is only compatible with ROCC and it is tightly bound that we cannot use it with another SoC as its news diplomacy.

Solution:

To make an accelerator with custom instructions and having custom specified interfaces to achieve generalizability.

Deliverables:

1) Software implementation of SHA3(256) algorithm.
2) SHA3 Computation Unit
3) SHA3 Control Unit
4) Systolic Arrays
5) Accelerator with generalized interfaces.

Success Criteria:

Accelerator compatible with SoCNow generated SoC and passes the benchmarks.

MERL
Accelerating Engineering Innovation

Project Schedule:

S.No.	Tasks	Deadline
1	Software implementation of SHA3(256) algorithm.	September 17, 2022
2	Reflect SHA3 algorithm on hardware from software.	TBD
3	SHA3 Control Unit.	TBD
4	Systolic Arrays	TBD
5	Accelerator with generalized interfaces.	TBD

Future Work:

1) Integrate it with the SoCNow SoC Generator.