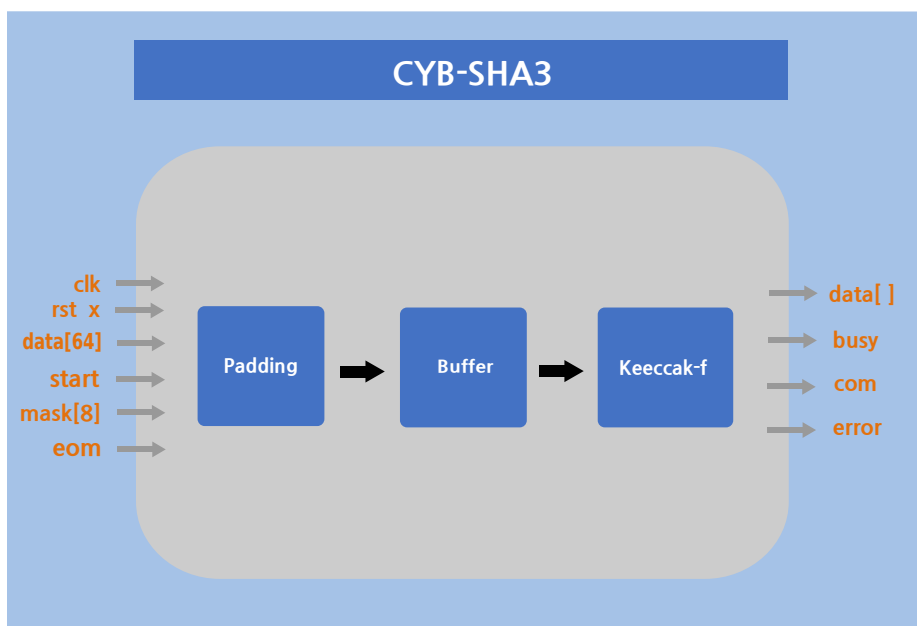


## Overview of SHA3 IP



CYB-SHA3 implements Secure Hash Algorithm-3 (SHA-3) family of functions on binary data with the NIST FIPS 202 Standard. It supports cryptographic hash functions (SHA3-224, SHA3-256, SHA3-384, and SHA3-512). SHA-3 can be directly substituted for SHA-2 in current applications and significantly improve the robustness of NIST's overall hash algorithm toolkit. It provides two versions of SHA3 IP: SHA3 hash engine and SHA3 hash engine with input buffer and padding logic. It is flexible to select different versions based on various requirements.

CYB-SHA3 is an ideal solution for wireless communication, payment products and IoT devices with high implementation performance. It is fastly and easily integrated into ASIC and FPGA applications.

## Feature

- Support NIST FIPS 202 standard
- Pass NIST FIPS 202 test vectors
- Support four cryptographic hash functions: SHA3-224, SHA3-256, SHA3-384, and SHA3-512
- Padding and buffer of input data
- High throughput
- ASIC and FPGA applications

## Deliverable

- Flexible licensing
- Documentation
- Netlist
- Verilog or VHDL
- Testbench
- Technical support

## Application

- IoT devices
- Secure encryption
- Data validation
- Unique identification