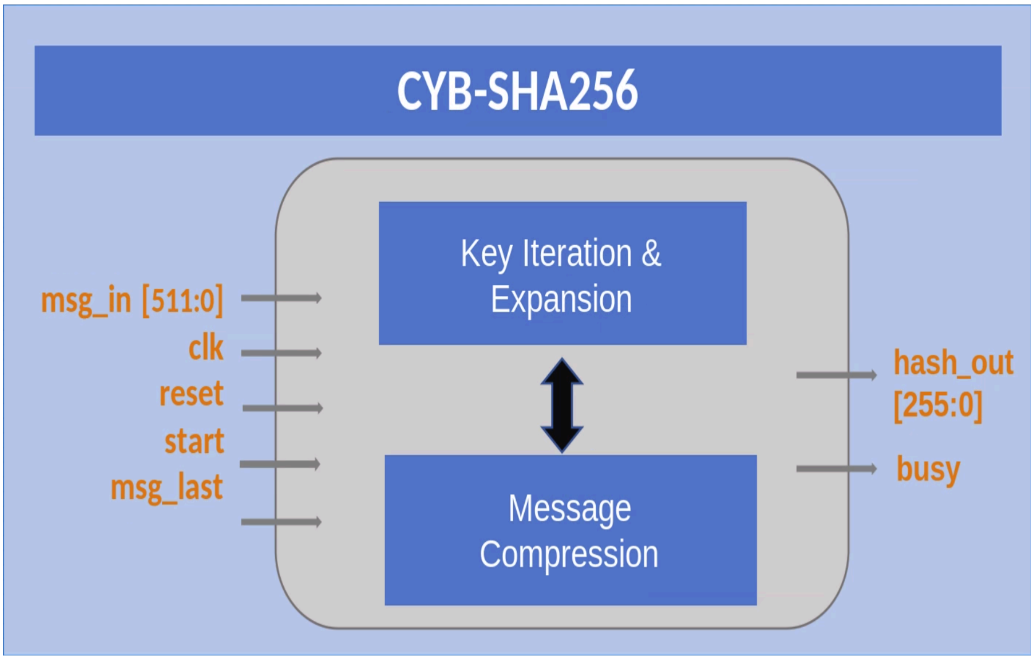
CYBERTEK SOLUTION

CYB-SHA256
Product Brief

Overview of SHA256 IP



SHA256 is a Secure Hash Algorithms which is one of the latest hash functions standarized by the U.S Federal Government. SHA 256 IP Core Algorithm implements one-way hash functions that process a message digest. Such functions enables the determination of a message's integrity and provide 128 bits of security agains collison attacks. CYB-SHA256 IP Core solution can be widely applied in the variety of cryptography designs to protect digital signature and identity authentication in order to avoid the attacks. The implementation is designed with high performance, simple interface that enable easy integration into SOC or FPGA applications.

Feature

- FIPS 180-2 compliance
- Message compression
- Key expansion
- Hash input 512 bit
- Hash output 256 bit
- 68 cycles per 512-bit hash block
- Bit padding

Deliverable

- Flexible licensing
- Documentation
- Source code
- Verilog
- Technical support

Application

- Digital signature
- Password protection
- Message authentication
- Data intergrity check
- Security applications and protocols
- Transcation verification for crypto-currencies