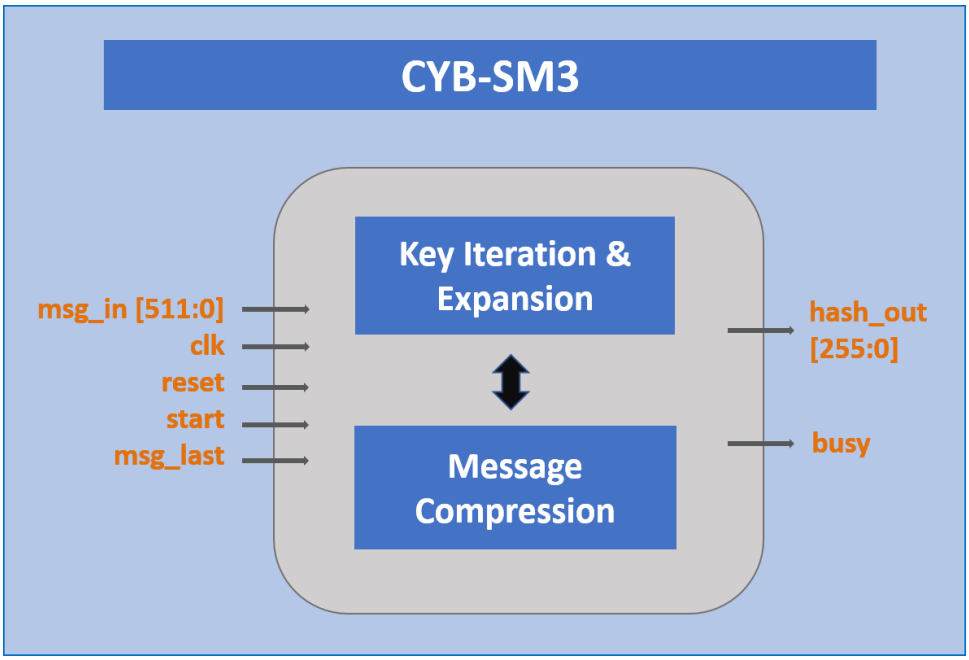
Overview of SM3 IP



SM3 is a hash algorithm initially published by the Office of State Commercial Cryptography Administration (OSCCA) of SCA in 2010, then as a China industry standard in 2012 [GMT-0004-2012], and finally recognized as a Chinese National Standard [GBT.32905-2016] in 2016. SM3 has been also standardized in [ISO.IEC.10118-3] by the International Organization for Standardization in 2017. Now SM3 is adopted in architectures Armv8.2-A and later.

CYB-SM3 provides a reliable and cost-effective SM3 IP solution that can be widely applied in the variety of cryptography designs to protect digital signature and identity authentication in order to avoid the attacks. It is designed with high performance and fast integration into ASIC and FPGA applications.

Feature

- Compliant with GBT.32905-2016
- OSCCA compliance
- Key expansion
- Hash input 512 bits
- Hash output 256 bits
- Synthesis pass
- Prevent bit tracing
- Iterative compression function

Deliverable

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

Application

- Digital signature
- ID authentication
- IoT devices
- IP networking
- FPGA implementations

矽泰科技

www.cybertek-solution.com
sales@cybertek-solution.com

+886-3-668-6603 (TW)
+86-21-5308-5993 (SH)