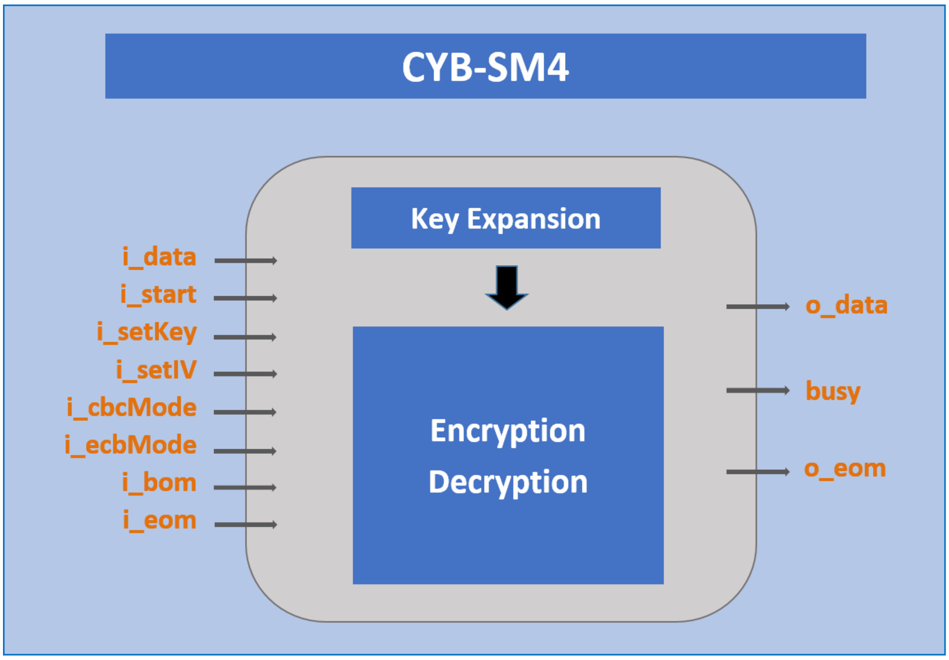
Overview of SM4 IP



SM4 (former name “SMS4”) is a cryptographic standard published by the Office of State Commercial Cryptography Administration (OSCCA) of SCA as an industry cryptographic standard in 2012, and formalized as a Chinese National Standard [GBT.32907-2016] in 2016. SM4 has also been standardized in [ISO.IEC.18033-3.AMD2] by the International Organization for Standardization in 2017 and adopted in TPM2.0 by the Trust Computing Group (TCG). Now SM4 is adopted in architectures Armv8.2-A and later.

Compliant with SM4 specifications, CYB-SM4 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

- Compliant with GBT.32907-2016
- Support both encryption and decryption
- Support ECB, CBC and multiple ciphering modes
- Perform key expansion
- ASIC and FPGA applications
- Flexibly scalable options

Deliverable

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

Application

- Wireless communication
- Payment products
- IoT devices
- FPGA implementations