SM4

SM4 Cipher Engine

AMD

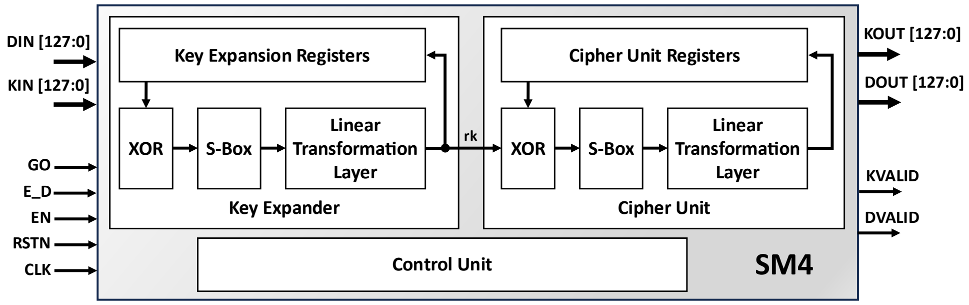
The SM4 IP core implements a custom hardware accelerator for the SM4 symmetric block cipher, specified in Chinese national standard GB/T 32907-2016, and ISO/IEC 18033-3:2010/Amd 1:2021.

Designed for easy integration, the core, internally expanding the 128-bit key, is capable of both encryption and decryption and features a simple handshake input and output data interface. To further simplify integration, CAST separately offers interface bridges to AMBA™ AXI4-Stream and integration with DMA engines to facilitate operation as a memory-mapped peripheral.

The core is available in a **Fast** version (SM4-F), offering a throughput of 4 bits/cycle, while a **High-throughput** version (SM4-X) operating at 128 bits/cycle is optionally available. Variants supporting different cipher modes provisioned by NIST SP 800-38 recommendations (i.e. ECB, CBC, CFB, OFB, CTR, GCM, CCM, XTS) are optionally available for both versions.

The SM4 is rigorously verified, LINT-clean and scan-ready. It is straightforward to implement on any technology as it is a strictly synchronous design using only rising clock edges, an asynchronous reset line and requires no special timing constraints.

Block Diagram



FEATURES

Security Mechanism Support

- Encryption/Decryption per:
  - Chinese national standard GB/T 32907-2016, and
  - ISO/IEC 18033-3:2010/Amd 1:2021

Versions and Variants

- Versions:
  - SM4-F: 4-bits/cycle
  - SM4-X: 128-bits/cycle
- Variants (different cipher modes):
  - ECB, CBC, CFB, OFB, CTR, GCM, CCM, XTS

Fast & Compact

- 2.6Gbps with less than 905 LUTs on modern AMD FPGAs (SM4-F)

Easy Integration and Trouble-Free Technology Mapping

- Simple handshake interface
- Bridges to AXI4 Stream and DMA integration separately available
- Fully synchronous, single-clock domain, re-usable design
- No false or multicycle timing paths, scan-ready, LINT-clean

Deliverables

- RTL source code (VHDL or Verilog) or targeted FPGA netlist
- HDL testbench
- C model and test-vector generator
- Simulation and synthesis scripts
- Documentation

Applications

The SM4 IP core is a versatile symmetric block cipher engine that can be deployed across diverse security-critical domains, which require compact solutions with high-throughput. Application areas include: IoT devices, Wireless Networking (WAPI), Secure communications (encrypted messaging, VoIP, VPNs), Trusted Platform Modules (TPMs), Mobile baseband processors, Data storage security (flash memory, SSDs, and encrypted storage solutions), Digital Payment Systems (e-payment terminals, smart cards, mobile payment apps).

Export Permits

This core implements encryption functions and as such it is subject to export control regulations. Export to your country may or may not require a special export license. Please contact CAST to determine what applies in your specific case.

Implementation Results

The SM4 core can be mapped to any AMD ® FPGA device (provided sufficient silicon resources). The following are sample results with all core I/Os assumed to be routed on-chip.

Family (Speed Grade)	Logic Resources	Memory Resources	Frequency	Throughput
Kintex 7 (-3)	900 LUTs	0 RAMB18	400 MHz	1.6 Gbps
Virtex 7 (-3)	900 LUTs	0 RAMB18	400 MHz	1.6 Gbps
Kintex US (-3)	894 LUTs	0 RAMB18	500 MHz	2.0 Gbps
Kintex US+ (-3)	904 LUTs	0 RAMB18	650 MHz	2.6 Gbps
Zynq US+ (-1)	901 LUTs	0 RAMB18	650 MHz	2.6 Gbps

The provided figures do not represent the higher speed or smaller area for the core. Please contact CAST to get characterization data for your target configuration and technology.