SNOW-V

SNOW-V Stream Cipher Engine

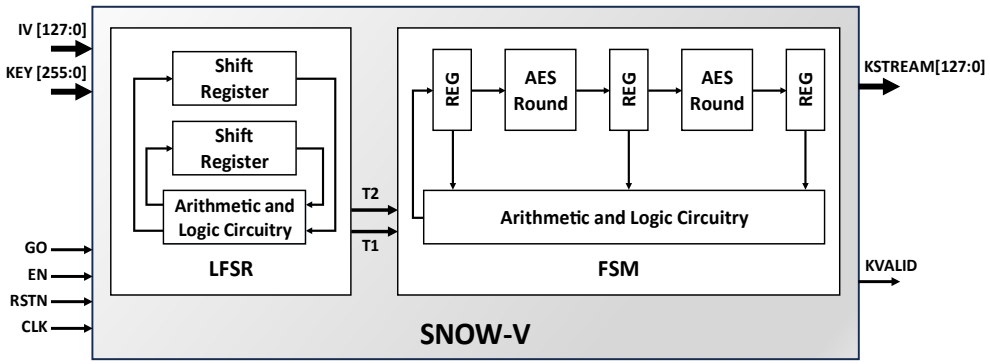
The SNOW-V IP core implements the SNOW-V stream cipher mechanism, aiming to meet the security demands of modern high-speed communication systems. It conforms to the official SNOW-V mechanism, published in 2019 by the IACR Transactions on Symmetric Cryptology, as an extensive revision of SNOW 3G stream cipher.

Receiving a 256-bit Key and a 128-bit Initialization Vector (IV), the core processes 128 bits of information in one cycle and it produces a stream of 128-bit keys. It employs two main building blocks, a Linear Feedback Shift Register (LFSR) and a Finite State Machine (FSM) that applies an Advanced Encryption Standard (AES) round function.

The core can be easily incorporated in a Galois/Counter mode (GCM) topology and by interoperating with a Galois Message Authentication Code (GMAC) realize an Authenticated Encryption with Associated Data (AEAD) mechanism. What is more, the core is a drop-in replacement for SNOW 3G in EPS Encryption/Integrity Algorithm (EEA/EIA) architectures and New Radio Encryption/Integrity Algorithm (NEA/NIA) architectures for 4G and 5G communications, while also targeting future mobile network generations (e.g. 6G).

The SNOW-V IP core is a microcode-free and fully synchronous design developed for reuse in ASIC and FPGA implementations, aiming at throughput-demanding environments. The efficient and compact hardware design enables high throughput, achieving over 50 Gbps in high-performance AMD FPGAs. Moreover, being a scan-ready, LINT-clean, and single-clock design with a simple handshake interface, facilitates straightforward integration.

Block Diagram



Applications

The SNOW-V IP core can help provide fast and secure communication in high-speed 4G, 5G, and future 6G networks. Furthermore, it can safeguard device interactions and prevent cyber threats in IoT ecosystems, while for multimedia streaming, it will enable real-time encryption to protect content from unauthorized access. Additionally, the SNOW-V IP core may be used for data storage encryption and high-quality pseudo-random number generation.

Implementation Results

The SNOW-V core can be mapped to any AMD ® FPGA device (pro-vided sufficient silicon resources are available). 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)	1,242 LUTs	16 RAMB18	300 MHz	38.4 Gbps
Virtex 7 (-3)	1,246 LUTs	16 RAMB18	250 MHz	32 Gbps
Kintex US (-3)	1,236 LUTs	16 RAMB18	400 MHz	51.2 Gbps
Kintex US+ (-3)	1,253 LUTs	16 RAMB18	540 MHz	69 Gbps
Versal AI (-2)	1,253 LUTs	16 RAMB18	350 MHz	44.8 Gbps
Versal Prem (-2)	1,253 LUTs	16 RAMB18	450 MHz	57.6 Gbps
Zynq US+ (-1)	1,232 LUTs	16 RAMB18	400 MHz	51.2 Gbps

FEATURES

Security Mechanism Support

- SNOW-V stream cipher
  - IACR 2019 publication
- AEAD-mode ready
  - Easy adoption to a GCM core
  - Seamless interoperation with a GMAC block
- Drop-in replacement of SNOW 3G in 4G/5G security architectures

High-throughput and Compact Design

- Processing 128 bits/cycle
- Over 50 Gbps and less than 1,300 LUTs in high-performance AMD FPGAs

Easy Integration and Technology Mapping

- Simple handshake interface
- 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
- Complete testbenches
- C model and test-vector generator
- Simulation and synthesis scripts
- Documentation

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

Related Products

A set of AES engines, including AES-GCM Authenticated Encrypt/Decrypt, are also available from CAST as stand-alone cores.

Support

The core as delivered is warranted against defects for ninety days from purchase. Thirty days of phone and email technical support are included, starting with the first interaction. Additional maintenance and support options are available.

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.

Deliverables

The core is available in RTL (VHDL or Verilog) source code, or as a targeted FPGA netlist. Its deliverable package includes the following:

- Self-checking HDL testbench
- C Model & test vector generator
- Sample simulation & synthesis scripts
- User documentation