

Encryption and Decryption IP Core

The KiviCrypt-AES-CTR IP core implements the Advanced Encryption Standard in Counter Mode as specified in NIST SP 800-38A. It provides high-speed encryption and decryption for continuous data streams and other applications requiring data confidentiality.

The IP core supports flexible initialization vectors of up to 128 bits. It can operate with either a pre-expanded key or its internal key expansion mechanism, which is used by default. Its fully synchronous architecture is optimized for high-speed operation and efficient implementation on LUT4-based FPGAs. The core requires no internal block RAM and can be delivered for FPGA and ASIC designs.

Variants	Description
KiviCrypt-AES-CTR-Fast	Optimized for high processing throughput, suitable for designs that require increased performance while maintaining efficient use of resources.

Key Features

- Compliant with NIST SP 800-38A
- AES encryption and decryption in Counter Mode
- Flexible IV length of up to 128 bits
- Pre-expanded key or internal key expansion
- Internal key expansion enabled by default
- AXI Stream data input and output
- Optional DMA engine
- Optional AMBA® AXI4-Lite control interface
- Fully synchronous design
- Optimized for high-speed operation
- Area- and speed-optimized for LUT4-based FPGAs
- No internal block RAM required
- Optional platform-independent C HAL and software driver
- Support for Linux, RTOS and bare-metal environments
- Suitable for FPGA and ASIC implementations

Applications

- High-speed data paths between FPGA, processor, memory and peripherals
- Confidential data transmission over custom communication protocols
- Encryption of data stored in external memory or flash
- Protection of video, sensor and other continuous data streams
- Storage and disk-encryption systems
- FPGA- and ASIC-based cryptographic accelerators
- Industrial, telecommunications, aerospace and embedded systems

Test And Verification

- NIST ACVP test vectors for AES-CTR block cipher mode
- Extended verification through simulation
- FPGA integration and implementation tests
- Unity tests for driver and whole IP Core

Support and Maintenance

- Maintenance and updates of IP core included
- Rapid bug fix cycles
- Documentation and integration examples included
- Web based support with response times of 8 hours (Mo to Fri)

Product License Deliverables

- System Verilog RTL Source Code or targeted FPGA netlist
- Testbenches
- Integration examples
- Simulation and synthesis scripts
- Optional software HAL & driver source code
- Optional software example for Linux and bare-metal
- Documentation

Evaluation License Deliverables

- Netlist format, time-bombed
- Testbenches
- Integration examples
- Software HAL & driver source code
- Software example source code
- Documentation

Evaluate KiviCrypt-AES-CTR

Register for the Evaluation Portal to access the evaluation package, technical documentation and integration resources.

[Get access](#)

FPGA Implementation Results

AMD (Xilinx)			
KiviCrypt-AES-CTR-Fast			
Device	LUTs	max. Frequency (MHz)	max. Throughput (Gbps)
Spartan 7	9212	199.3	25.5
Kintex 7	9263	325.6	41.6
Zynq US+ MPSoC	9236	453.3	58.0
Versal AI Cores Series	10447	527.1	67.5

Efinix			
KiviCrypt-AES-CTR-Fast			
Device	XLR	max. Frequency (MHz)	max. Throughput (Gbps)
Titanium	11839	379.7	48.6
Topaz	11839	238.5	30.6
Trion	12284	107.4	13.8

Microchip			
KiviCrypt-AES-CTR-Fast			
Device	LUT4	Frequency (MHz)	Max-throughput (Gbps)
PolarFire SoC	5256	201.1	25.8
PolarFire	5256	201.1	25.8
Igloo2	54269	119.3	15.3
RTG4	54423	96.5	12.4
SmartFusion 2	54269	119.3	15.3

Contact

KiviCore GmbH
Gostritzer Straße 61
01217 Dresden
Germany

+49 351 871 9801
info@kivicore.com