KEXP

Key Expander Core

AMD

The KEXP IP core performs AES key expansion, and is an option for the AES, AES-P, AES-CCM and AES-GCM cores. It processes 128-bit blocks, and is programmable for 128-, 192-, and 256-bit key lengths.

Two architectural versions are available to suit system requirements. The **Standard** version (KEXP32) is more compact and is used with AES cores using a 32-bit datapath. The **Fast** version (KEXP128) achieves higher throughput in conjunction with AES cores using a 128-bit datapath.

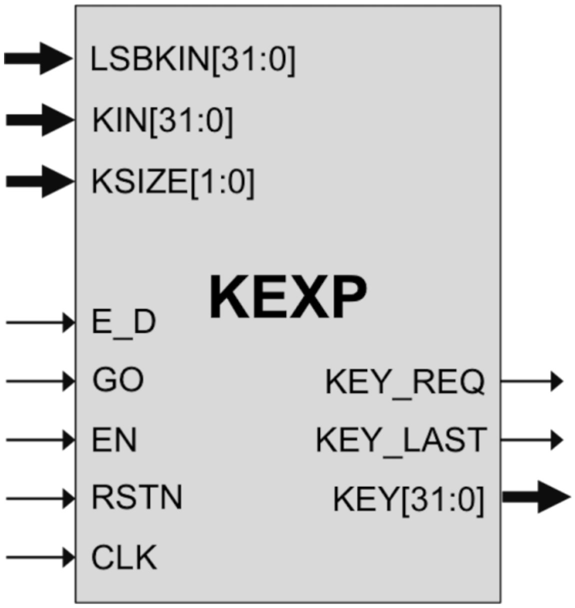
The KEXP core is a fully synchronous design and has been evaluated in a variety of technologies, and is available optimized for ASICs or FPGAs.

Applications

The KEXP can be utilized for a variety of encryption applications including:

- Protected network routers
- Electronic financial transactions
- Secure wireless communications
- Secure video surveillance systems
- Encrypted data storage

Symbol Diagram



FEATURES

- Satisfies Federal Information Processing Standard (FIPS) Publication 197 from the US National Institute of Standards and Technology (NIST)
- Employs user-programmable key size of 128, 192 or 256 bits
- Two architectural versions:
  - Standard is more compact: 32-bit data path size
  - Fast yields higher transmission rates: 128-bit data path
- Suitable for use with AES cores
- Forward and backward key expansion
- Simple, fully synchronous, reusable design
- Available as fully functional and synthesizable VHDL or Verilog, or as a netlist for popular programmable devices
- Complete deliverables include test benches, C model and test vector generator

Functional Description

The KEXP is a highly integrated implementation of the AES key expansion. The input key is expanded and it can be used during encryption on the fly, without the need to store the whole key in a buffer.

During decryption, the expanded key needs to be fed backwards. This core can perform backward expansion on the fly without the need for an additional buffer.

Rising the input on the GO port triggers the beginning of the expansion of the KEY input.

The key size selection can be selected by the KSIZE input. Valid values for KSIZE are “00”, ”01” and “10” selecting 128, 192 or 256 bits respectively. The KSIZE inputs must not be changed while the data is processed.

The core then raises the KEY_REQ signal requesting the key. It then starts to expand the key according to the AES algorithm.

During the expansion process, the expanded key data is available at the output KEY.

The expanded data is output in the correct order for use with AES cores during encryption.

At the end of the expansion operation, the signal KEY_LAST is raised. The core is immediately ready for another expansion operation and, in fact, the KEY_REQ signal is raised immediately after that.

Backward Key Expansion

During decryption, the expanded key must be fed to an AES core backwards. Backwards expansion works similarly to forward expansion and it is activated by raising the E_D input.

Implementation Results

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

KEXP Standard Version AMD Results

Family	LUTs	BRAMs	Freq. (MHz)
Kintex 7 (-3)	93	1	325
Virtex 7 (-3)	97	1	325
Kintex UltraScale (-3)	91	1	450
Kintex UltraScale+ (-3)	98	1	575
Versal (-2)	172	0	675

KEXP Fast Version AMD Results

Family	LUTs	BRAMs	Freq. (MHz)
Kintex 7 (-3)	581	1	250
Virtex 7 (-3)	579	1	250
Kintex UltraScale (-3)	580	1	325
Kintex UltraScale+ (-3)	580	1	425
Versal (-2)	603	1	300

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.

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.

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.

Verification

The core has been verified through extensive synthesis, place and route and simulation runs. It has also been embedded in several products, and is proven in FPGA technologies.

Deliverables

The core is available in ASIC (RTL) or FPGA (netlist) formats, and includes everything required for successful implementation. The AMD version includes

- Targeted FPGA netlist
- Sophisticated HDL Testbench (self-checking)
- C Model & test vector generator
- Simulation & synthesis scripts
- Vectors & expected results
- User documentation