

Features

- FIPS 46-3/ANSI X9.52 compliant triple DES core
- Supports key sizes of 56 and 112-bits
- Performance >500 Mbps
- Higher performance available
- Portable to any technology library
- Easy integration into any SoC design
- Microprocessor bus interfaces available

Benefits

- Full-width data ports maximize performance, minimize latency
- Fast delivery for accelerated time to profit

Applications

- Encrypted data storage
- Secure communications
- Secure processing
- IPsec acceleration
- E-commerce
- VPN
- Financial Transactions



Triple Data Encryption Standard (3DES)

The Athena Group delivers the Triple Data Encryption Standard (3DES) as a semiconductor intellectual property (IP) core. Athena's 3DES-A100 3DES/DES core complements Athena's leading-edge TeraFire public key (PK) cryptography accelerators. This dedicated 3DES solution provides both performance and power savings.

The 3DES-A100 is compliant with FIPS 46-3 and ANSI X9.52 and supports user programmable key sizes of 56 and 112-bits. The 3DES-A100 can provide 3DES encryption/decryption performance greater than 500 Mbps and single DES performance greater than 3.2 Gbps.

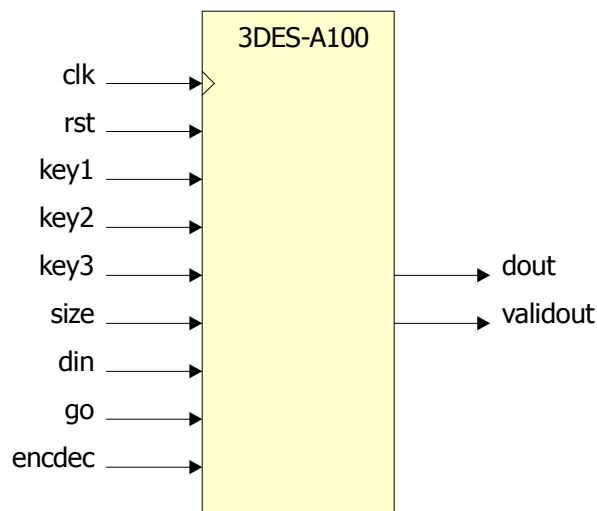


Figure 1: Block Diagram of 3DES-A100

Product Description

The 3DES-A100, shown in Figure 1, is a fully synchronous design and features dedicated, full-width data input, output, and key input ports for

Available Deliverables

- Simulation model (Verilog or VHDL)
- Synthesizable RTL (Verilog or VHDL) and scripts
- Targeted, timing closed netlist
- Verification suite
- Documentation
- Support



The Athena Group, Inc.
408 W. University Ave., Suite 306
Gainesville, FL 32601

Phone: (352) 371-2567
Toll-free: (800) 741-7440
Fax: (352) 373-5182
www.athena-group.com

Copyright The Athena Group, Inc., 2008. All rights reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner. The information presented in this document does not form part of any quotation or contract, is believed to be accurate and reliable, and may be changed without notice. No liability will be accepted by the publisher for any consequence of its use. Publication thereof does not convey nor imply any license under patent or other industrial or intellectual property rights.

maximum throughput and minimum latency. A data valid output is provided to simplify retrieval of output data. The 3DES-A100 area starts at 6K-gates in a typical 130 nm process, and can readily scale beyond 200 MHz. The 3DES-A100 may be delivered with an optional bus interface to simplify SoC integration.

TeraFire Cryptography Application Library (CAL)

The TeraFire CAL is a portable, ANSI C library of cryptographic software implementations and drivers for TeraFire hardware accelerators. The TeraFire CAL has been implemented and tested on multiple platforms, including leading SoC microprocessors from ARM. Athena's sophisticated configuration management system enables rapid configuration of the TeraFire CAL for your mix of hardware accelerator and software implementation requirements.

Designed for Easy Integration

Athena has over a decade of experience in delivering first-time physical design success. Athena has become a premier provider of semiconductor IP by always delivering quality. To ensure ease of integration, Athena goes the distance - by synthesizing *our* IP into *your* target library, in *your* process, with *your* constraints, and delivering a completed core, ready for place and route. Athena standard deliverables include everything you need to integrate our core into your design: netlists, simulation models, test vectors, support, and documentation.

About The Athena Group, Inc.

Based in Gainesville, Florida, Athena innovates breakthrough technologies that achieve the optimum balance of power, performance, and silicon area in a wide range of applications such as wireless, satellite, and secure communications. Athena provides patented semiconductor intellectual property (IP) solutions, with products ranging from the market-leading TeraFire® security cores, to Atomic DSP™ cores, and Atomic SDR™ software defined radio cores.

Athena was founded in 1986 and is privately held.