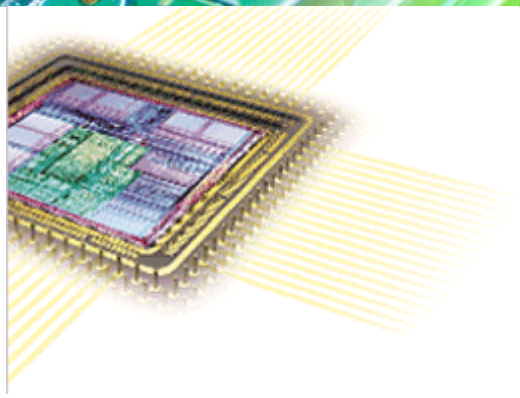
ntSHA256

SHA 256-bit hash generator



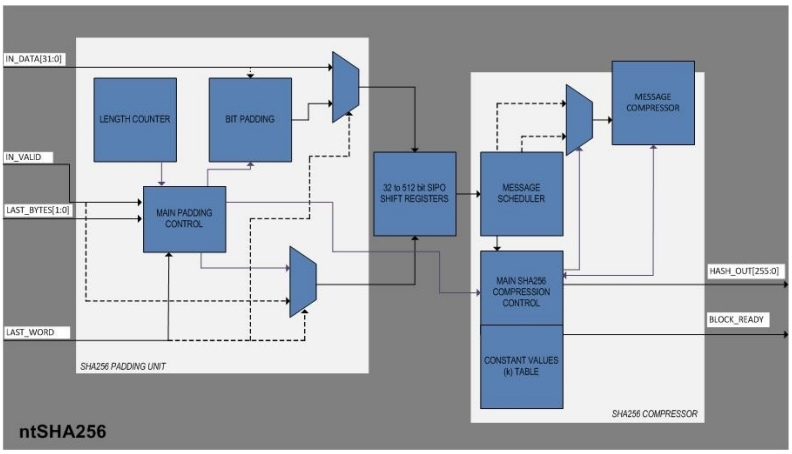
An n-bit hash is a map from arbitrary length messages to n-bit hash values. An n-bit cryptographic hash is an n-bit hash which is one-way and collision-resistant. Such functions are important cryptographic primitives used for such things as digital signatures and password protection. Current popular hashes produce hash values of length n = 128 (MD4 and MD5) and n = 160 (SHA-1), and therefore can provide no more than 64 or 80 bits of security, respectively, against collision attacks. Since the goal of the new Advanced Encryption Standard (AES) is to offer, at its three cryptovariable sizes, 128, 192, and 256 bits of security, there is a need for companion hash algorithms which provide similar levels of enhanced security. ntSHA256 IP Core implements SHA-256, or Secure Hash Algorithm-256 which is one of the latest hash functions standardized by the U.S. Federal Government. It is a 256-bit hash and is meant to provide 128 bits of security against collision attacks. The implementation is very low on latency, high speed with a simple interface for easy integration in SoC applications.

Applications

The ntSHA256 core can be used in a variety of applications, including:

- Security applications and protocols (TLS, PGP, SSH, S/MIME, IPsec)
- Authentication of Debian GNU/Linux software packages
- DKIM message signing standard.
- Transaction verification and proof-of-work calculation for several crypto-currencies (Bitcoin).
- Password protection
- Digital signatures
- Message authentication
- Data integrity check

Block Diagram



Features

- Compliant to FIPS 180-2 specification of SHA-256.
- Internally implemented bit padding unit.
- Supports input message length multiple of 8-bit.
- Parametric hash values (h) of Chaining Variables.
- Parametric SHA256 constant values table (k).
- 66 processing cycles per 512-bit message block.
- Simple interface.
- Fully synchronous design.
- Silicon proven in ASIC and FPGA technologies for a variety of applications.

Implementation results

The core has been targeted to both ASIC and FPGA technologies for various applications. Noesis Technologies can also deliver netlist versions of the core optimized to specific area resources and performance requirements.

Silicon Vendor	Device	Resources	Fmax (MHz)
Xilinx	Spartan 3A	1577 CLB Slices / 1 Block RAM	50

Block size	Throughput rate [1]
512 bits	312 Mbps

1. Throughput rates are for Xilinx Spartan-3A technology.

Deliverables

Noesis has engaged an "open" licensing philosophy in order to allow maximum technology transfer to our client's engineering teams and to facilitate the integration of our IP cores into our client's product. Various licensing models are available. The ntSHA256 core is available as a soft core (synthesizable HDL) or as a firm core (netlist for FPGA technologies). The following deliverables are included:

- Fully commented synthesizable VHDL or Verilog source code or FPGA netlist.
- VHDL or Verilog test benches and example configuration files.
- Comprehensive technical documentation.
- Technical support.

Support

Technical support by phone or email is included. First year of maintenance is also included. Additional support and annual maintenance options are available.

Ordering information

To purchase or make any further inquiries about our ntSHA256 core, or any other Noesis Technologies products or services, contact us at info@noesis-tech.com. Noesis Technologies products are purchased under a License Agreement, copies of which are available on request.

Noesis Technologies P.C.
Patras Science Park
Stadiou Rd, Platani Rion
GR-26504 - Patras
GREECE
Phone: +30 2610 911531
Email: info@noesis-tech.com

NOESIS TECHNOLOGIES

www.noesis-tech.com