Silicon IPs for Cryptographic Algorithms

Summary of features and specifications

- ***Morphing Machines*** provides a full portfolio of silicon IPs for cryptography algorithms – all variants, modes, and key strengths of the AES algorithm, reconfigurable finite field arithmetic with ECC support, SHA-2 and SHA-3 secure hash algorithms, and other custom IPs
- Optimized high-performance crypto IP cores compliant fully with NIST and FIPS specs and other relevant international standards
- Run-time reconfigurable support for the five standard AES encryption/decryption modes: ECB, CBC, CFB (1-bit, 8-bit and 128-bit), OFB, CTR)
- Dynamically selectable 128-bit, 192-bit, and 256-bit key sizes for AES encryption and decryption with 4 Gbps per core throughput
- Runtime reconfigurable software programmable engine for arithmetic over arbitrary size finite fields – specially optimized to support GF(2^{163}) used in Elliptic Curve Cryptography – supports up to 20,000 point multiplications per second over GF(2^{163}) using less than 50K gates and only 6 clock cycles per multiplication
- Compact high-performance SHA-3 IP with less than 35K gates supporting up to 53 Gbps throughput

General features

- Fully synchronous flow-through design with stallable easy-to-integrate interface
- Self-contained solutions – includes relevant key expansion logic and key schedule memory – as well as easy integration into ASIC or SoC
- Clock frequencies supported: 50MHz – 200 MHz on FPGA, 400 MHz and above on ASIC/SoC
- Available in multiple configurations with various combinations of clock frequency, area, power, latency, throughput, and external interface

Detailed datasheets

- For complete details of each crypto silicon IP, please see the corresponding datasheet of the relevant IP

Applications and use cases

- Bulk data encryption / decryption in *IPSec, SSL/TLS, TCP/IP, MACSec, ANSI A9.62, IEEE 802.16, and ad-hoc sensor networks*
- Data confidentiality in Kerberos and related applications
- Data authentication in IEEE 802.11 (Wi-Fi), 802.15 (ZigBee), 802.16 (WiMax) and related applications
- Data authentication in IPSec, IKE, IEEE 802.1, and related applications
- Data confidentiality and authentication in IEEE 802.1AE (MACSec), IEEE1619.1, SSH, SSL/TLS, etc.
- Data storage confidentiality in IEEE 1619.1 tape storage and related applications
- Digital signatures, RFID systems, Transport Layer Security (TLS), RSA computations
- Secure bulk transfer of electronic data, secure email systems, electronic fund transfer systems, secure data storage authentication, etc.

Deliverables

- Synthesizable Verilog RTL source code, or pre-synthesized FPGA netlist, or foundry-ready GDS-II format for specified process
- Self-checking testbench applying all relevant NIST or other standard specified test vectors
- Documentation including instructions for integration of the core into ASIC or SoC

Related IPs, solutions, and services

- ***REDEFINE*** ***Reconfigurable Massively Parallel Processor Fabric*** – flagship ***Morphing Machines*** SoC architecture platform provides an ideal infrastructure for building special-purpose extreme-performance application or domain specific silicon engines for any standard or custom crypto algorithms
- Customization and integration support services for incorporating ***MM*** crypto IPs or ***REDEFINE*** based accelerators into customer SoCs

Information on ***Morphing Machines*** and its technologies is overleaf. More information on ***Morphing Machines*** technology, IPs, products, solutions, and services is available at ***http://morphing.in***

Morphing Machines Pvt Ltd, *#17, 10A Main, 16 Cross, Malleshwaram, Bangalore 560 055, India*
Email: ***info@morphing.in*** *Phone/Fax: +91 80 4206 0618*

Morphing Machines

REDEFINE
Reconfigurable Silicon Cores

Crypto Silicon IPs

High-performance reconfigurable silicon IPs for standard and custom cryptography algorithms and modes

Reinventing cutting-edge silicon innovation in India ***morphing.in***

Silicon IPs for Cryptographic Algorithms

Crypto Silicon IP	Datasheet URL
MM Silicon IPs for Cryptographic Algorithms – Overview	*http://morphing.in/crypto/overview*
MM RAES–S5 (ECB, CBC, CFB, OFB, CTR)	*http://morphing.in/crypto/raes-standard*
MM RAES CBC–CS1	*http://morphing.in/crypto/raes-cbccs1*
MM RAES CCM	*http://morphing.in/crypto/raes-ccm*
MM RAES CMAC	*http://morphing.in/crypto/raes-cmac*
MM RAES GCM	*http://morphing.in/crypto/raes-gcm*
MM RAES XTS	*http://morphing.in/crypto/raes-xts*
MM RECC163 (Finite field arithmetic and ECC)	*http://morphing.in/crypto/recc*
MM SHARC3 (SHA-3 standard secure hash algorithm)	*http://morphing.in/crypto/sha*

Why use *Morphing Machines* crypto IPs

- Correct optimized design and realizations, easy integration, affordable prices, and caring direct support from developers
- Designed, implemented, and verified in India

About Morphing Machines

- ***Morphing Machines Pvt Ltd*** is a closely held fabless semiconductor company launched from the Technology Entrepreneurship Initiative of the ***Indian Institute of Science*** at Bangalore, India
- Emerging as one of India's most exciting cutting- edge IP focused technology start-up companies, ***Morphing Machines*** featured as one of the four global start-up semiconductor companies in the ***Cool Vendors 2011*** report of ***Gartner Research***
- Founded by a group of distinguished IIT and IISc alumni with decades of rich experience at world- leading semiconductor, computer, communication, and software technology corporations
- Working in close collaboration with research groups at th***e Indian Institute of Scien***ce at Bangalore, ***Morphing Machines*** has created an exciting portfolio of ***reconfigurable silicon cores***

Technologies and Key IPs

- ***REDEFINE*** – Platform for design and realization of runtime reconfigurable ***Massively Parallel Processor*** and ***Heterogeneous Multicore Processor*** hardware accelerators and SoCs supported by the parallelizing ***REDEFINE C Compiler***
- Breakthrough solutions in multi- protocol ***cryptography, numerical computation,*** and other domains
- ***REDEFINE XNOC*** – Scalable high-performance deadlock-free ***Network-on-Chip*** framework with reconfigurable topologies and multiple interfaces for rapid realization of complex SoCs
- ***MM RAES, MM RECC, MM SHARC*** – Optimized IPs for strong AES encryption / decryption, elliptic curve cryptography, and secure hash functions
- ***MM FPUX*** – High-performance floating-point unit IP supporting multiple precisions and special functions

Information on the ***MM Crypto IPs*** is overleaf. More information on the ***Morphing Machines*** technology, IPs, products, solutions, and services is available at ***http://morphing.in***

Morphing Machines Pvt Ltd, *#17, 10A Main, 16 Cross, Malleshwaram, Bangalore 560 055, India*
Email: ***info@morphing.in*** *Phone/Fax: +91 80 4206 0618*