**AES**

* Rambus AES CCM/GCM Engine
* Rambus - DPA Resistant AES Core
* Rambus - AES (ECB-CBC-CFB-CTR-GCM), 1 Billion Trace DPA Resistant Cryptographic Accelerator Cores
* Rambus - Rambus DPA & Fault Injection Resistant AES-AE Cryptographic Core
* Rambus - Rambus Full flexible multi-channel AES-GCM engine up to 2Tbps
* The FortifyIQ AES Core
* SphinX - AES-XTS encryption/decryption IP
* Xilinx – AES IP
* Alma Technologies – AES-P
* AES-IP-38 – Rambus
* AES-IP-61 – Rambus
* <https://www.synopsys.com/designware-ip/security-ip/cryptography-ip/symmetric-cryptographic-engines.html>

**AES Github**

<https://github.com/www-asics-ws/aes_128>

<https://github.com/secworks/aes>

<https://github.com/hadipourh/AES-VHDL>

<https://github.com/mmattioli/aes>

<https://github.com/ahegazy/aes>

<https://github.com/marph91/yaaes>

<https://opencores.org/projects/tiny_aes>

<https://opencores.org/projects/avs_aes>

<https://opencores.org/projects/aes_highthroughput_lowarea>

<https://github.com/tmeissner/cryptocores>

<https://github.com/hadipourh/CryptoHDL>

<https://opencores.org/projects?expanded=Crypto%20core>

https://www.librecores.org/search?query=aes

**HMAC**

<https://www.design-reuse.com/sip/?q=hmac>

* SecureIC - Tunable HMAC accelerator - compliant with all hash functions (SHA1, SHA2, SM3, SHA3) - optional SCA protection
* Rambus - HMAC-IP-59
* Rambus - DPA Resistant HMAC-SHA-2 Cryptographic Accelerator Core - HMAC-SHA-2 (224/256/384/512) 100 Million Trace DPA Resistant Cryptographic Accelerator Cores
* Xiphera - HKDF/HMAC/SHA-256/SHA-512, SHA-256 IP Core with Extended Functionalities

**Github**

<https://github.com/Goshik92/SHA256Hasher>

<https://github.com/secworks/sha256>

<https://github.com/lostpfg/SHA-256-HDL>

<https://github.com/dsaves/SHA-256>

<https://github.com/skordal/sha256>

<https://github.com/ahmad2smile/SHA256_Verilog>

<https://github.com/martinafogliato/Sha256_Hw_Accelerator>

<https://github.com/thinkski/hashpipe>

<https://github.com/fbv81bp/VHDL_SHA2-256>

**PRNG**

<https://www.design-reuse.com/sip/?q=prng>

* IP Cores - Cryptographically Secure Pseudo Random number Generator IP Core
* IP Cores - True Random and Pseudorandom Number Generator

**DSA Verify**

No IP found.