Silicon IP of Algorithms

High-performance Silicon IPs of Crypto Cores

暗号アルゴリズムをハードウェア回路として実装したSilicon IPを提供します。

お客様のSoCやASIC、各種半導体デバイスへ容易に組み込むことができ、高性能・低消費電力なセキュリティ機能の実現を支援します。AESなどの暗号アルゴリズムSilicon IPを提供するとともに、NIST CAVP認証取得の実績に基づいた技術支援・コンサルティングサービスを提供。お客様の暗号機能実装から認証取得までをワンストップでサポートします。

Compliant and Customized Silicon IPs of Cryptographic Algorithms

Symmetric Cryptographic Algorithms

AES

- Selectable 128-bit, 192-bit, and 256-bit key sizes for AES encryption and decryption
- AES encryption/decryption modes: ECB, CBC, CFB (1-bit, 8-bit and 128-bit), OFB, CTR

Asymmetric Cryptographic Algorithms

ECC

- Elliptic Curve Diffie-Hellman (EC-DH) standard ANSI X9.63
- Elliptic Curve Digital Signature Algorithm (EC-DSA) standard ANSI X9.62
- Digital Signature Standard (DSS) FIPS-186
- Hardware Accelerators for ECC family

Hash Function

- SHA2-256 and SHA2-512
- FIPS 202: SHA-3 - Permutation-Based Hash and Extendable-Output Function
- FIPS 180-4: Secure Hash Functions (limited to SHA-3 use)

  All four fixed-length SHA-3 Hash Functions:
  - o SHA3-224
  - o SHA3-256
  - o SHA3-384
  - o SHA3-512

ワイセキュア株式会社｜WiSECURE Inc.
〒113-0033東京都文京区本郷7丁目2-5 6階　平清ビル
TEL: 03-6824-6088　https://wisecure-tech.jp