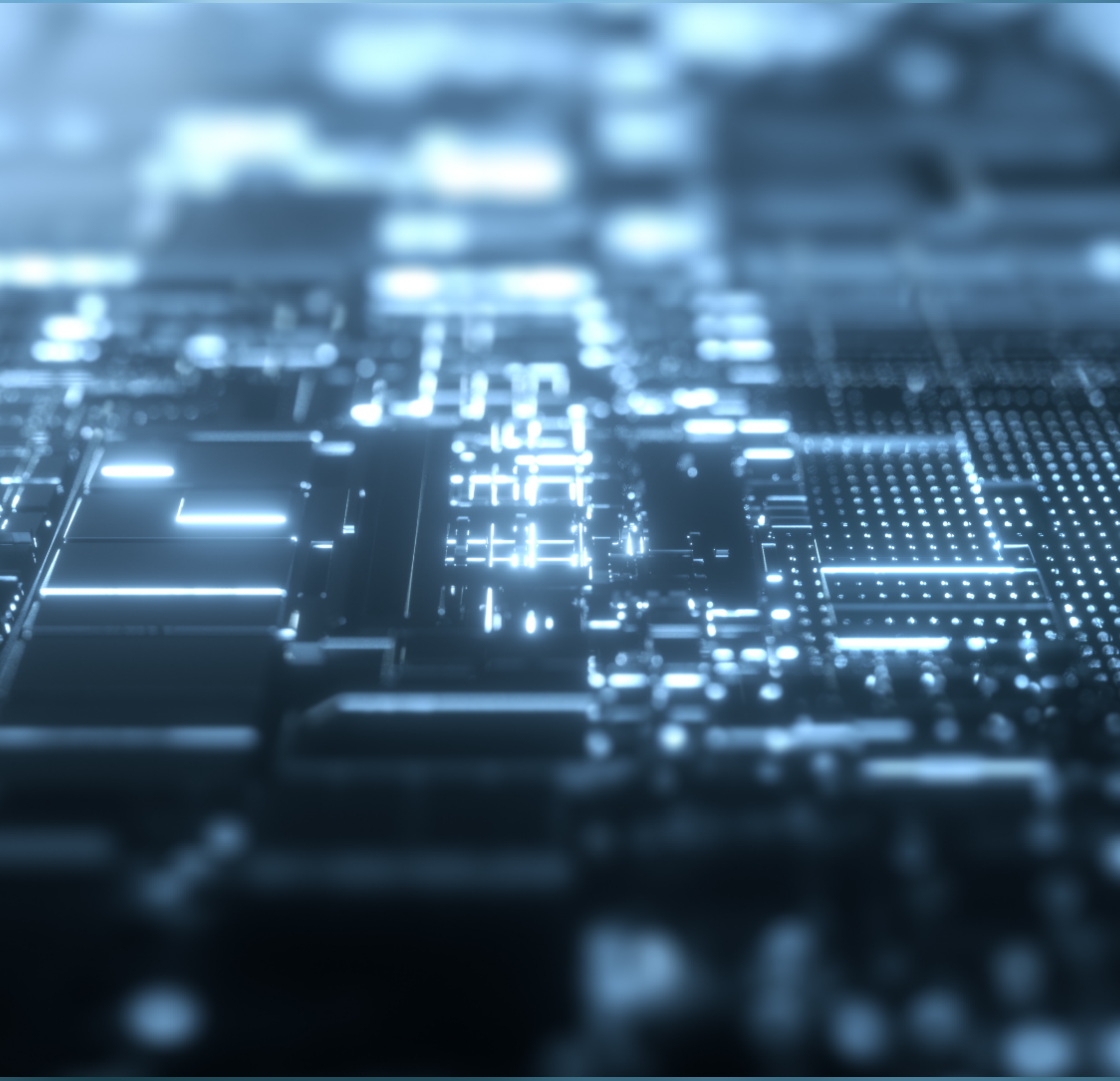


Silicon IP of Algorithms

High-performance Silicon IPs of Crypto Cores

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)

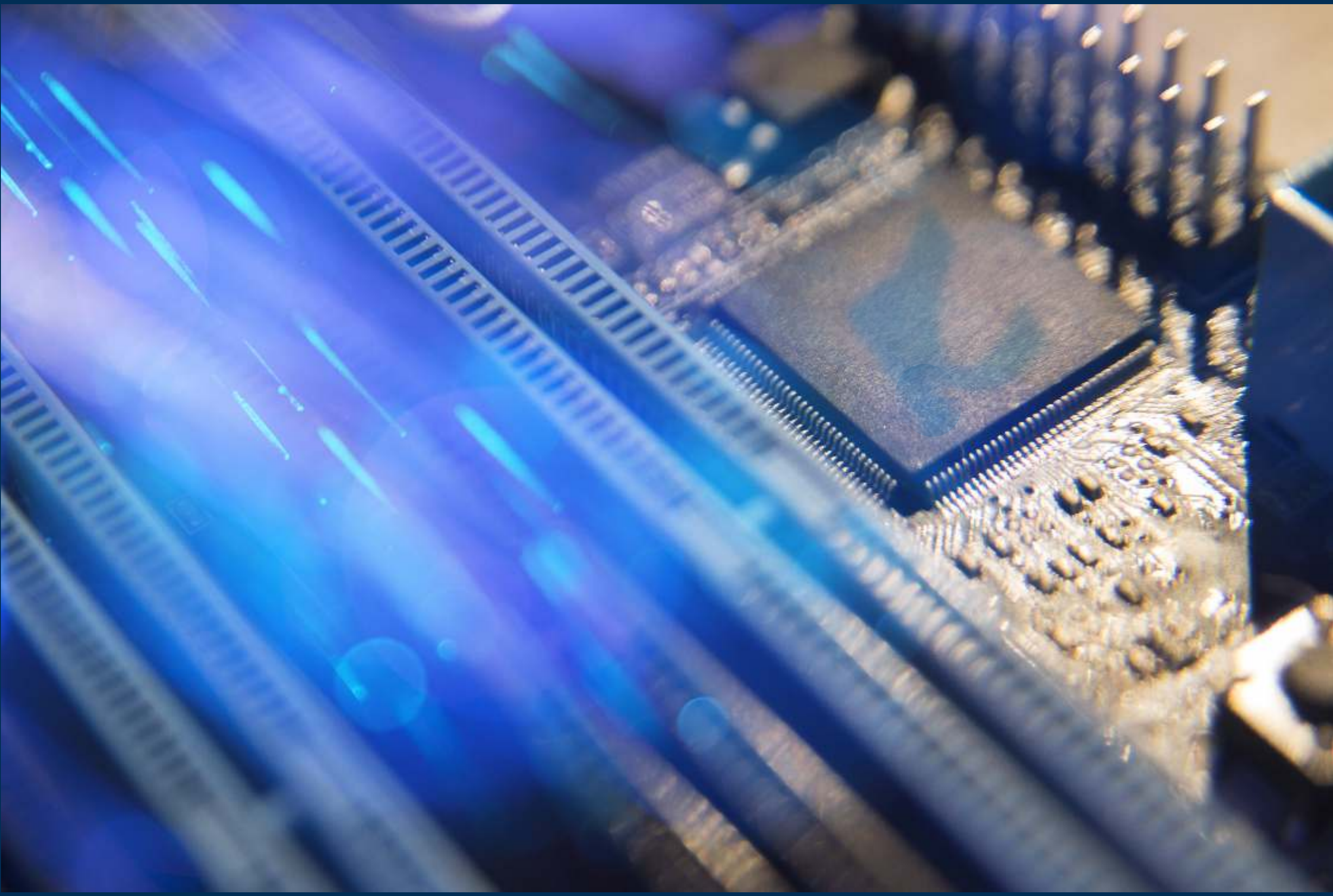
All four fixed-length SHA-3 Hash Functions:

o SHA3-224

o SHA3-256

o SHA3-384

o SHA3-512



Secure Vault at your fingertips

With IKV-Tech expertise, wide ranges of applications can attain security leveraging the silicon IP of cryptographic algorithms. We have boosted the performance of existing algorithms compliant with NIST and FIPS and enabled security, performance and usability to go hand in hand. All in all, our mission is to secure customers' operation seamlessly in space and time, especially in an era where attacks always keep abreast.

About InfoKeyVault Technology

InfoKeyVault Technology (IKV-Tech) is a service company in embedded security, also an independent design house for security solutions from global security chip vendors, such as Infineon and Microsemi. IKV-Tech specializes in cryptographic implementation, software, firmware and hardware protection, cryptographic key management and countermeasures against hardware attacks so as to secure customers' digital assets and intellectual property.

Contact Us

+886 2-2934-3166

info@email.ikv-tech.com

www.ikv-tech.com

www.facebook.com/InfoKeyVault