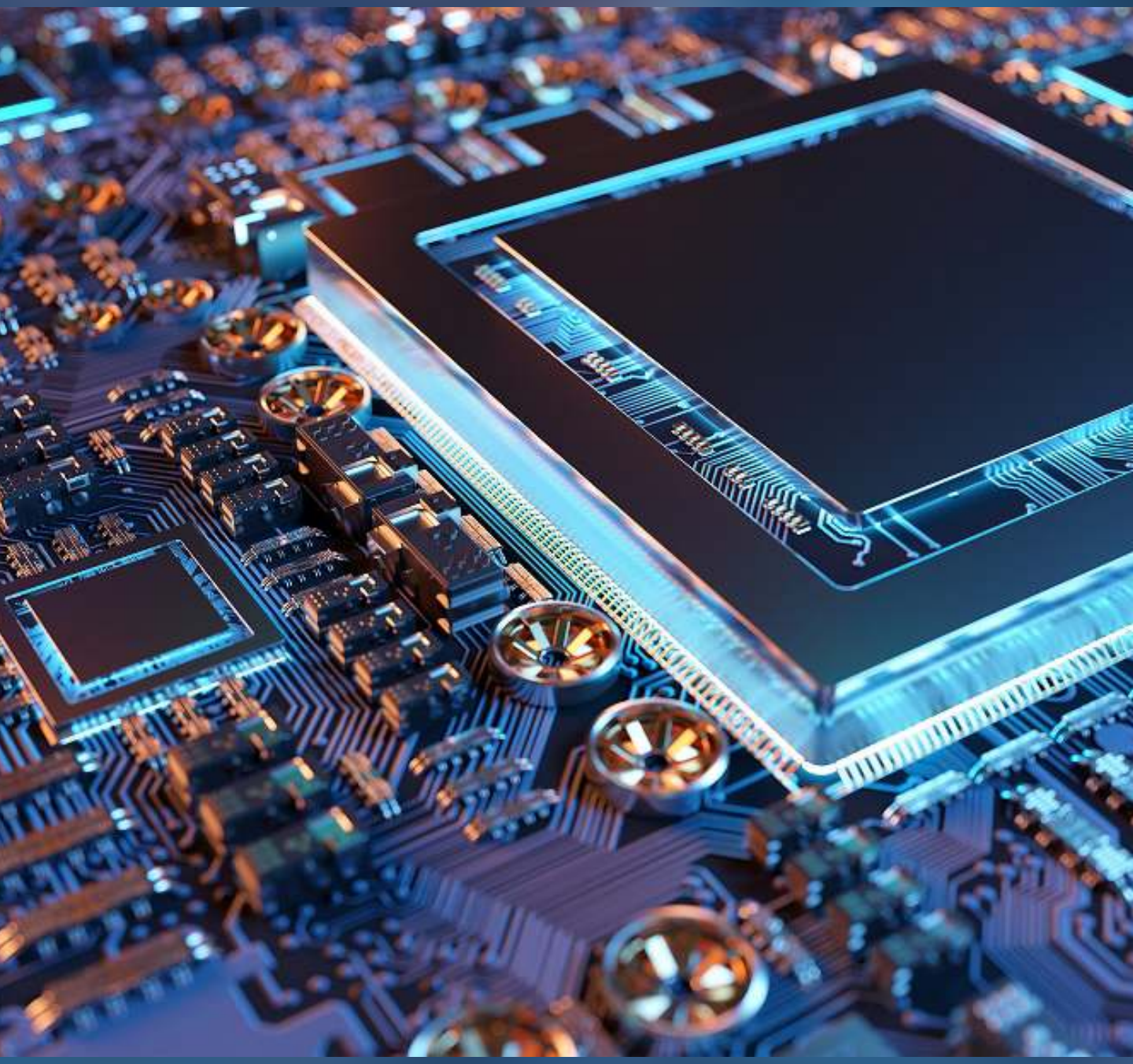
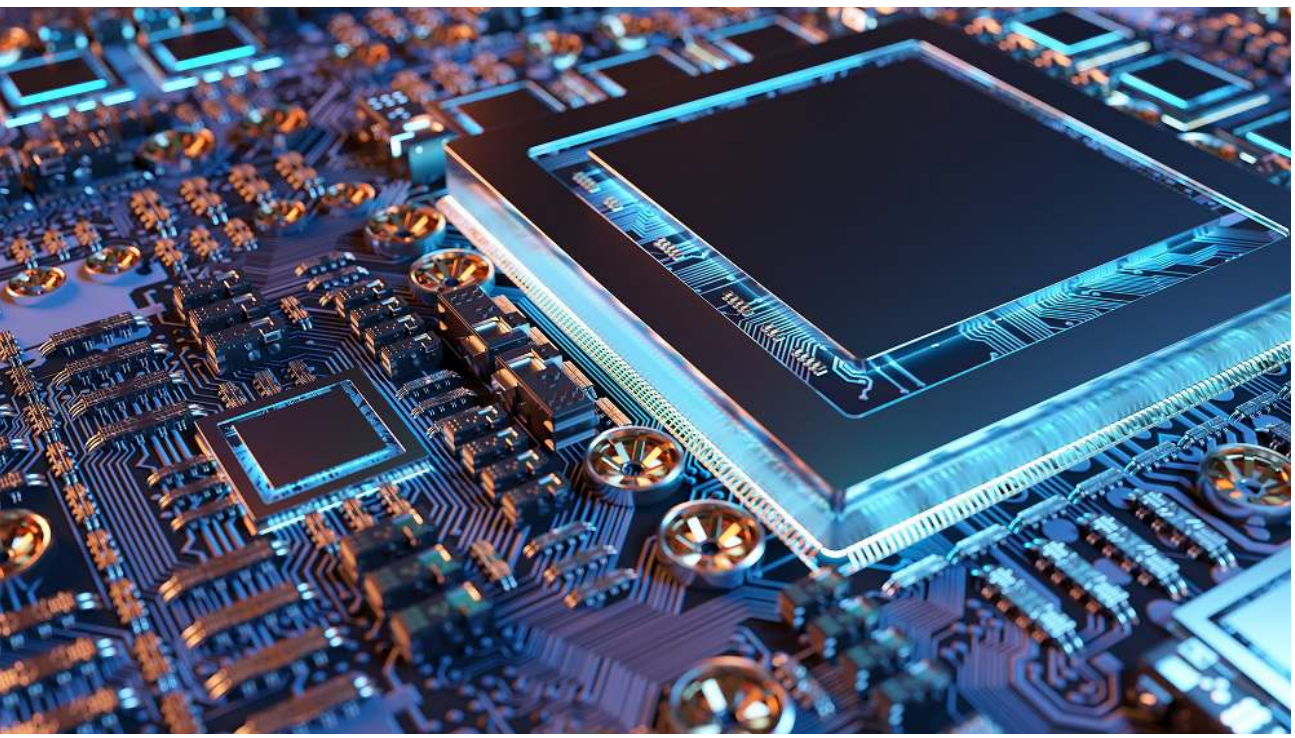


Fusion FPGA platform

Accelerate cryptographic computation with reconfigurable logic design

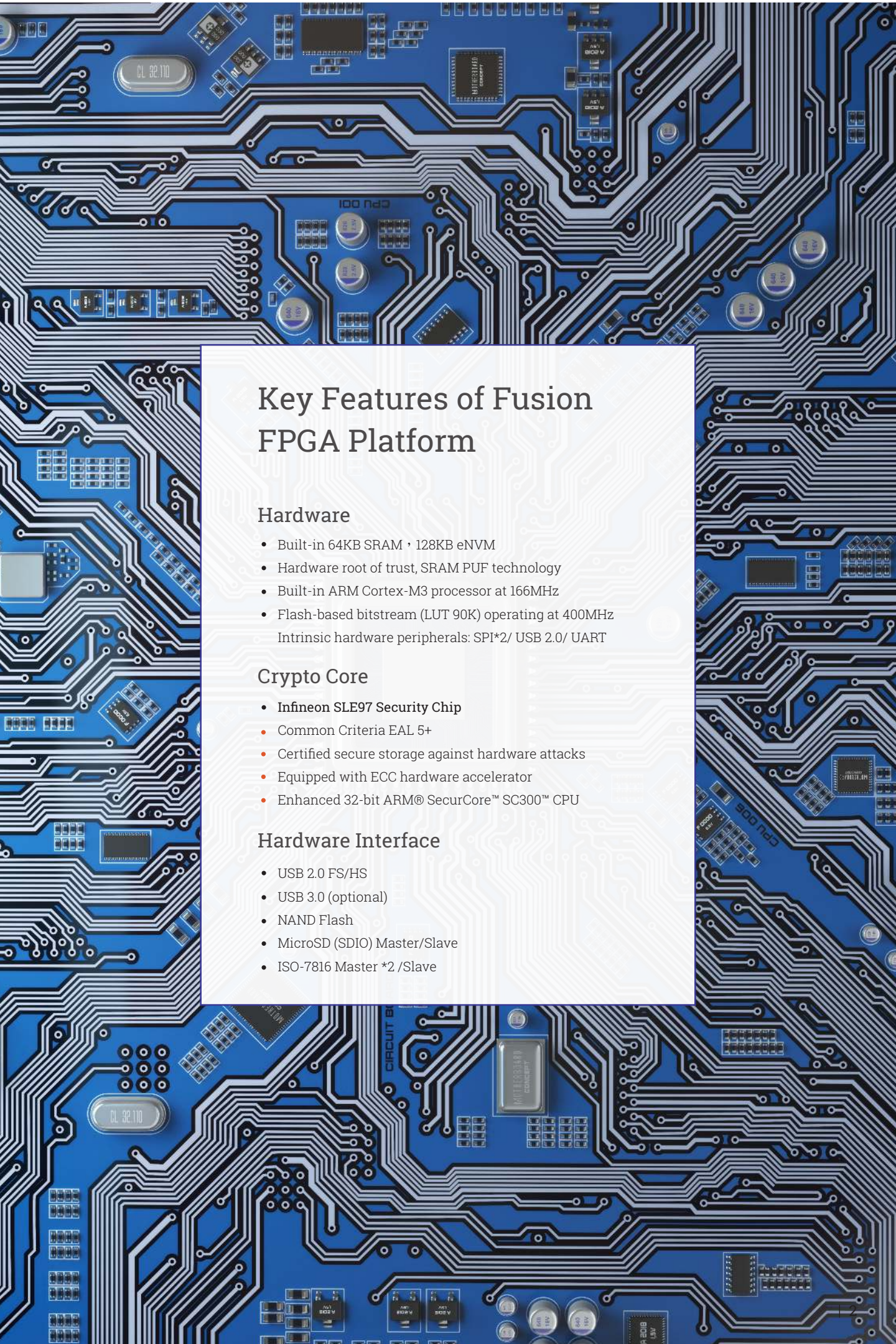
Fusion FPGA Platform with Reconfigurable Logic Design



As hardware attacks become increasingly tricky, large-scale businesses and governments struggle to keep up. Not like medium and small-scale ones, it takes longer and costs higher for them to compensate for losses. Moving to an era where digital assets are more valuable than materials, we all long for a painless, flexible and convenient way to protect digital assets and intellectual property.

In hardware security, compliance is a basic requirement, beyond which usability and flexibility determine how agile businesses are to cope with potential threats. To meet the requirement, security subsystem should allow for adaptive reconfiguration and customization.

Powered by IKV's specialization in cryptographic implementation, the Fusion FPGA platform enables customization of crypto algorithms to accelerate cryptographic computation or implement countermeasures against attacks. With the feature, customers have greater flexibility and adaptability in the fast changing threat landscape.



Key Features of Fusion FPGA Platform

Hardware

- Built-in 64KB SRAM，128KB eNVM
- Hardware root of trust, SRAM PUF technology
- Built-in ARM Cortex-M3 processor at 166MHz
- Flash-based bitstream (LUT 90K) operating at 400MHz
  Intrinsic hardware peripherals: SPI*2/ USB 2.0/ UART

Crypto Core

- **Infineon SLE97 Security Chip**
- Common Criteria EAL 5+
- Certified secure storage against hardware attacks
- Equipped with ECC hardware accelerator
- Enhanced 32-bit ARM® SecurCore™ SC300™ CPU

Hardware Interface

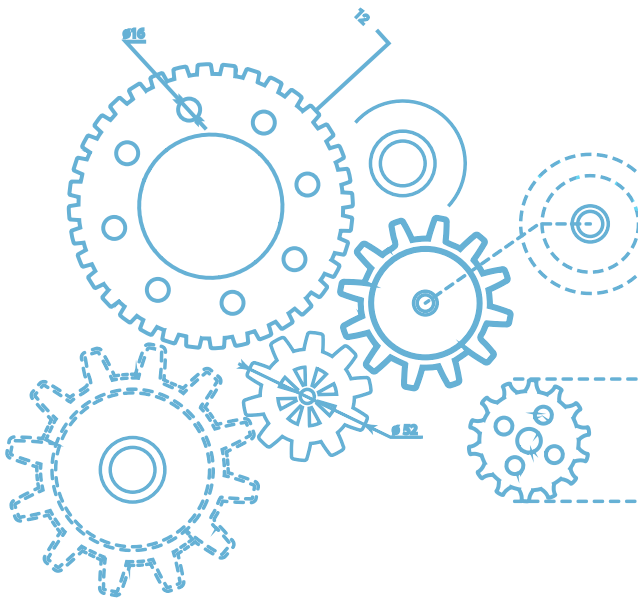
- USB 2.0 FS/HS
- USB 3.0 (optional)
- NAND Flash
- MicroSD (SDIO) Master/Slave
- ISO-7816 Master *2 /Slave

Leverage IKV Expertise

For systems processing transaction, confidential data and digital content, IKV aims to construct a pertinent subsystem, which can grant possessors complete control over the digital assets in transit and at rest.

Types of digital assets to be protected range from **confidential data**, which can be files that contain secret information, **digital assets**, which can be artificial intelligence (AI) codes and other kinds of intellectual properties, and **cryptographic keys** used for transaction.

Years of experience in embedded security enable IKV to embody robust security in any form factors to fit any system. On the given platform, IKV has exerted its ability to the greatest possible extent. From secure communication for national security to protection of digital content worth millions of US dollars, and cryptocurrency transaction used around the globe without any breaches, extensive exploration of its potential has not been marked with a period.



I. Security at the highest level

The Fusion FPGA platform possesses the hardware root of trust utilizing SRAM PUF (Static Random Access Memory Physical Unclonable Function) technology. It serves as the access key to the security chip, establishing secure channels protecting cryptographic keys and internal data transfer. Together with hardware-based built-in countermeasures and software-based intervention, the given platform facilitates product manufacture at the highest security level, resisting reverse engineering, responding to external intrusion, enabling standalone hardware protection and complying with external security management policies.

II. Flexible customization and reconfiguration

The never-ending pursuit of new vulnerabilities and attacks propels us to keep up with the top-notch countermeasure know-how. We effectively implement countermeasures against one of the notorious hardware attacks, side-channel attack (SCA), on both hardware and software, assuring customers the predominate position in the high-end market. We also specialize in the customization of cryptographic algorithms and reconfiguration of logic design, which are critical capabilities in the face of evolving attacks and unprecedented threat landscape.

Success Stories about Our Customers

Over the past years, public awareness of security has been raised, specifically for those who confronted imminent attacks or targeted markets that abounded with counterfeit products. Under the circumstance, security becomes a must rather than a choice. A great number of vendors consequently reached us and voiced their concerns. They covered a wide range of use case applications, in which the security mechanism was designed on the Fusion FPGA platform and is still taking effect now. In these cases, the given platform has proven a real-world impact on vendors' cost, trustworthiness and high-end market penetrability.

The Fusion FPGA platform fulfills the highest security level from a systematic and holistic view.

- The hardware root of trust based on SRAM PUF provides an unclonable identity for the system
- Cryptographic keys are stored in the military-grade security chip with CC EAL 5+ certification
- Secure channels built by SRAM PUF and the security chip protect internal data transfer
- FPGA customization and reconfiguration can reduce vulnerabilities of naive implementation
- High-performance crypto services powered by crypto accelerators mitigate risks of compromise

Edge Computing

The distributed nature of edge computing requires data to be encrypted from nodes to clouds. Diverse encryption mechanisms are to be adopted because data transit among different distributed nodes and systems. To ensure the whole system is well protected, the highly customizable Fusion FGPA can provide all-in-one solutions, which is able to streamline vendors' operation process, reduce development cost and enable the most desirable time-to-market.

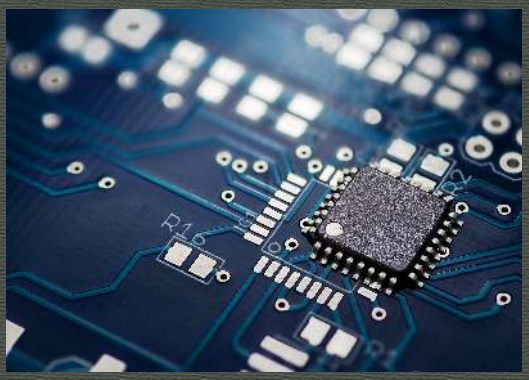
Secure Communication

The number of connected mobile devices has drastically risen in these years, which also indicates user privacy is in jeopardy. Thus, the market for private messaging is picking up. IKV has built a cryptographic infrastructure for an international unit to encrypt data, messages, and calls from the specialized communication devices. The infrastructure can also be integrated with secure messaging apps, such as Signal, Jitsi, and others.

Authentication Token

There are always great demands for the fine grained access control in governments and large-scale businesses. In this regard, token based authentication is required for access to storage clouds loaded with confidential data. With the Fusion FPGA platform, we've designed high-performance tokenization systems, in which tokens are used not only for key storage but for high-speed digital signature and encryption.

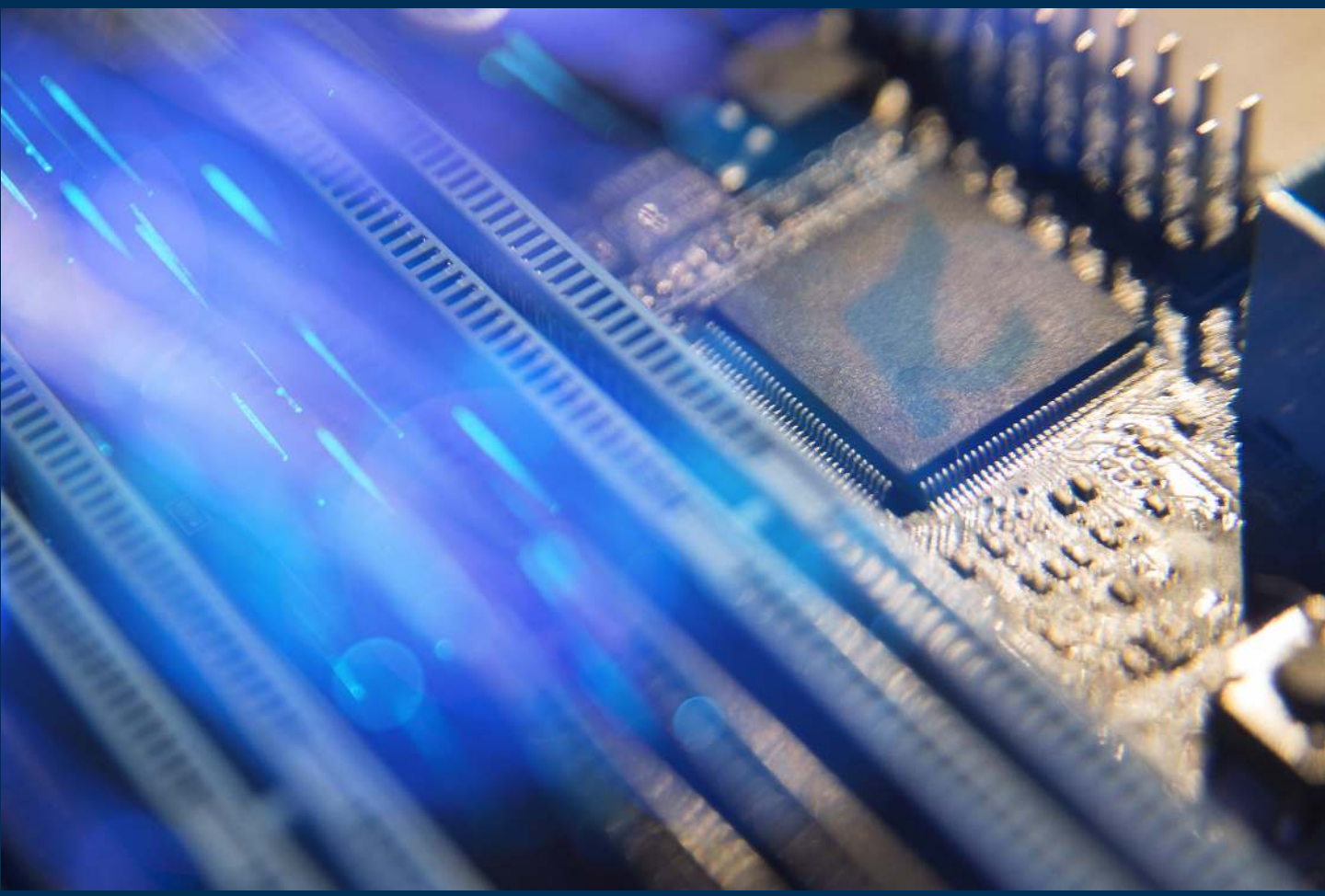
Hardware Security Module



Hardware security modules are embedded with security chips where cryptographic key pairs are pre-stored in secure memory. Providing key pairs in the security chips are cracked, all the data in the system are to be revealed. The platform offers a robust hardware-based root of trust and secure storage of cryptographic secret and other confidential data. Cryptographic algorithms can be customized; the logic design can be reconfigured; the services can be speeded.

Digital Right Management (DRM)

For customers requiring content protection of digital assets, such as game software, intellectual property, etc, IKV leveraged the Fusion FPGA platform to design systematic approaches, effectually restricting the way to copy content, preventing unauthorized distribution. Those who have adopted our DRM solution have successfully secured their digital asset worth billions of US dollars. Many attempts to comprise have also been proven failed.



Secure Vault at your fingertips

With IKV-Tech expertise, a wide range of applications can attain customizable and reconfigurable security leveraging the Fusion FPGA platform. We help customers optimize the existing security mechanism and enable security and usability to go hand in hand. All in all, our mission is to secure customers' business 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