KVSoftKey

SRAM PUF for heightened security and flexible deployment

KVSoftKey
for Software-based Encryption

The need for efficiency and the will to overcome impediments caused by time and space have brought about technological breakthrough in AIoT, peripheral computing and virtual machine deployment, which contribute to IT network expansion around the globe.

As individuals are closely connected than ever, the growing number of endpoints require stronger foundations of trust, secure communication, identification, and authentication.

KVSoftKey features a hardware root of trust that is generated via SRAM PUF (Physically Unclonable Function) technology. It provides eclectic cryptographic services reducing customers' costs and efforts, allowing customers to deploy endpoints without tedious configuration.

From intellectual property protection, digital rights management, IoT, communication, payments, to automobile, KVSoftKey ushers in an era of revolutionary security mechanisms, meeting requirements for time-to-market and cost-efficient mass production.

Key Features of KVSoftKey

Innate uniqueness

An internally generated unique identity with no need for a costly security-dedicated silicon

Install anywhere anywhen

It can be installed later in the supply chain, and even remotely retrofitted on deployed devices

Invincible root of trust

The hardware root of trust effectively thwarts malicious attempts to extract cryptographic keys

Scalability and extensibility

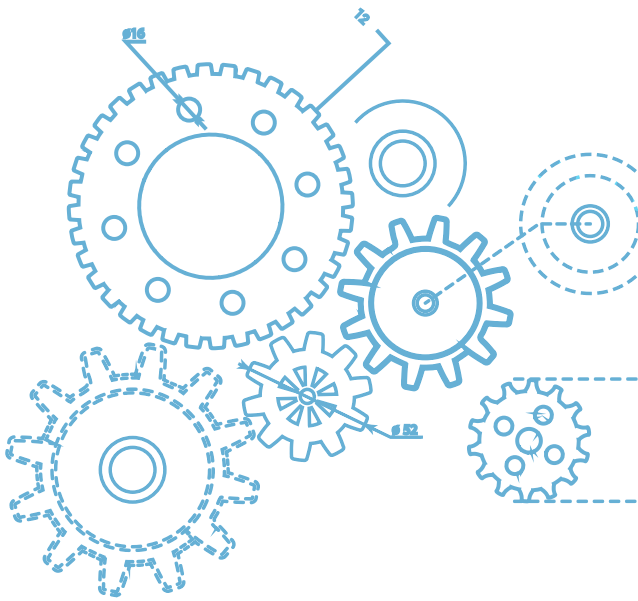
The software-based platform enables customers to scale their system to billions of devices

Leverage PUF and IKV Expertise

For systems or devices integrated with a secure element, KVSoftKey is "the last mile" to a holistic security solution building system-level defense.

KVSoftKey features Physically Unclonable Function (PUF), seamlessly incorporating every single component as a whole. PUF relies on the innate characteristics of the semiconductors to generate a root key that resembles a "fingerprint", which is unique and unpredictable.

Using the root key to establish a secure channel with the existent secure element for subsequent key derivation and wrapping is trustworthy as it vanishes without trace right after tasks are done. Compared with MCU TrustZone, in which a root key goes though the preload phase and gets stored in an isolated zone, PUF gets a head start with an innate root key dwelling by no means in memory, eradicating the threats of key extraction and data breaches.



Competence

I. Raising software-based security to hardware level

Whether it is data in transit or at rest, keys are by no means stored in memory, which allows the security of KVSoftKey mechanism to equal the one of a secure element, in which keys are protected by hardware.

II. Heightening hardware-based security with secure channels

KVSoftKey can create synergy and fulfill system-level protection with secure elements. To establish a secure channel between a microcontroller and a secure element, the root of trust used to access the secure element is generated via PUF. Once the task is done, the root of trust will be erased, which ensures sensitive key materials are securely handled and minimizes the possibility of exposure.

Fast, Flexible, Friendly

KVSoftKey is a platform providing holistic and customizable security for types of systems. From microcontrollers, memories to peripherals, it makes the most use of PUF to ensure data transmission among every component is well protected and that every phase in key lifecycle, from key derivation, distribution to destruction, is well-defined with FIPS 140-2 compliant measures and algorithms. With reliable roots of trust extracted on a need-basis only, never going off-chip and never stored, crypto functions during system operation greatly mitigates the risk of key leakage.

KVSoftKey helps customers enhance security and reduce cost because

- entropy from the silicon is random and offers uniqueness to the device
- keys are extracted on demand and do not need to be programmed in NVM,
- keys can be provisioned at any suitable stage in the production process,
- the flexible design make it suitable for most semiconductor platforms,
- the innate root key reduces hardware feature provisioning costs

IoT & Smart Factory

IoT devices are the target of DDoS attacks, and crack into connected equipment in smart factories may cause system-level breakdown. KVSoftKey can generate keys signifying unique identity for every single device. It enables device management, cloud-based authentication, encrypted end-to-end communication , and most importantly, system-level protection in case any data breach of a device may casue others to be compromised.

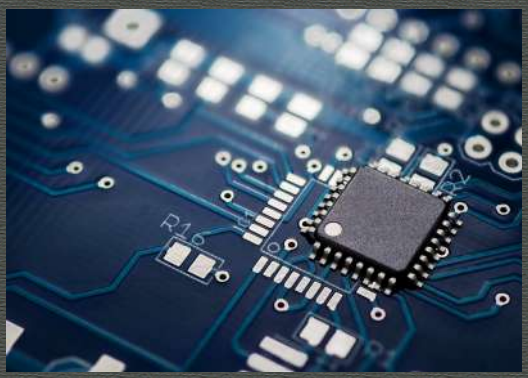
Automobile ECU & Sesnor

Hundreds of chips are embedded in a car for different purposes. Some of them are connected to engine, brakes, cruise control, gears, or other components. To avoid any carjack utilizing Internet of Things (IoT), secure connection inside and outside of the car should be established. KVSoftKey can endow every key component with the root of trust, which is used for encrypted data transmission, anti-counterfeiting, and other mechanisms for driving safety.

Secure Communication

Secure communication requires encrypted messages and user authentication, both of which rely on robust key management and tailor-made security design to mitigate the risk of encryption key leakage. KVSoftKey can provide the root of trust used to derive encryption keys. With IKV specializing in cryptographic algorithms, every message is encrypted with different keys. It ensures confidentiality of every single message in case any of them is cracked.

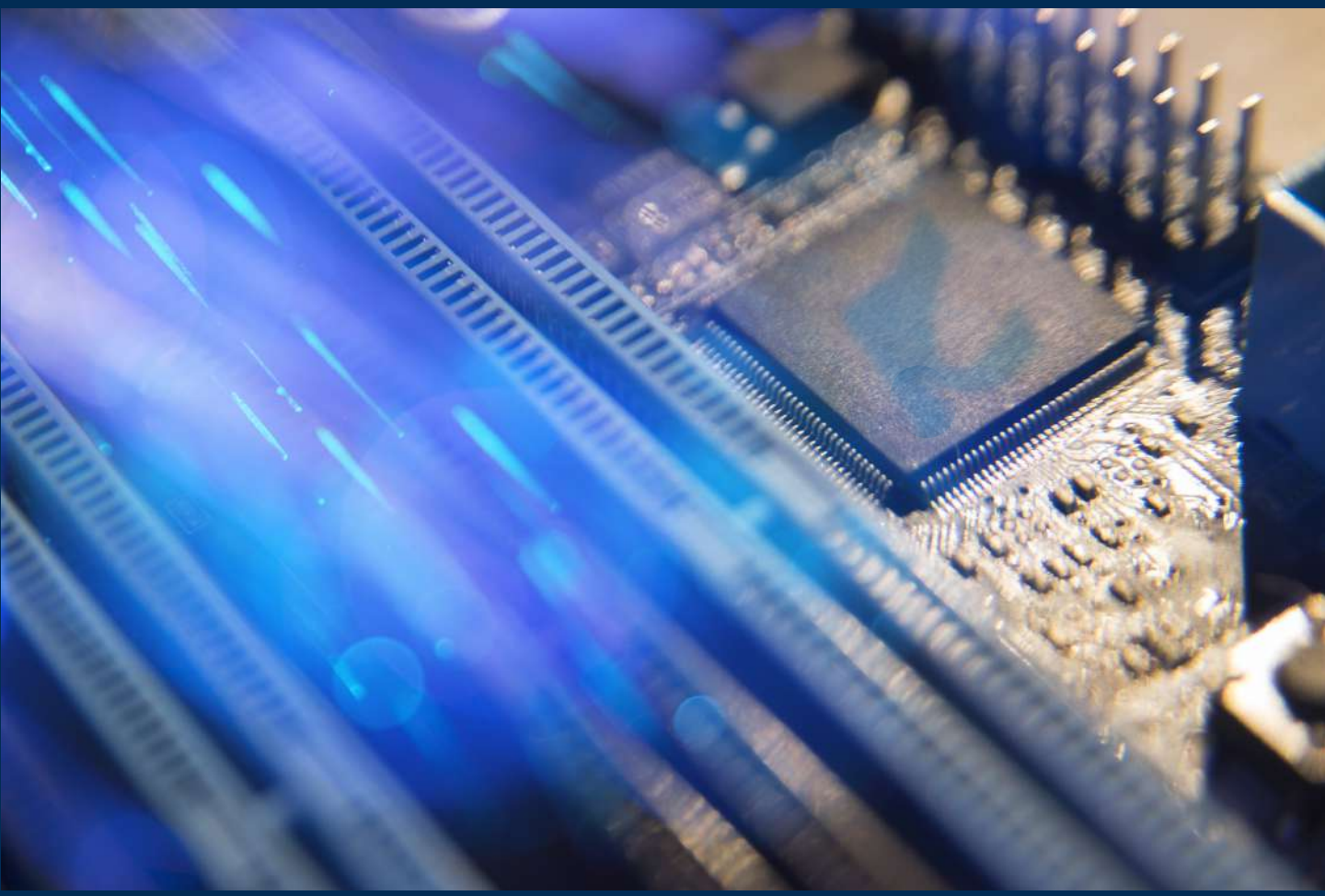
Hardware Security Module



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. KVSoftKey aims to enhance the security of systems already embedded with a security chip, serving as the access key to its primitives and key pairs. It adds another layer for system-level defense and effectively resist top-notch attacks.

Cryptocurrency Hardware Wallet

Typical hardware wallets use a security chip to store key pairs, authorizing and signing transaction. Losing the key pair equals losing all the digital assets in the hardware wallets since they are prone to being transferred to another digital wallet. KVSoftKey can protect the key pair inside the security chip, using PUF to generate the root of trust underlying the activation and legitmate use of key pairs and other crypto functions.



Secure Vault at your fingertips

With IKV-Tech expertise, a wide range of applications can attain tailor-made security leveraging KVSoftKey. We help customers optimize their existent security mechanism and fulfill scalability and time-to-market. 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