Secure Hardware System Development

White Paper

WP100-1.1E, 12/06/2021

Disclaimer

GOWINSEMI assumes no liability and provides no warranty (either expressed or implied) and is not responsible for any damage incurred to your hardware, software, data, or property resulting from usage of the materials or intellectual property except as outlined in the GOWINSEMI Terms and Conditions of Sale. All information in this document should be treated as preliminary. GOWINSEMI may make changes to this document at any time without prior notice. Anyone relying on this documentation should contact GOWINSEMI for the current documentation and errata.

Abstract

IoT has introduced a large variety of devices that have their own unique system attributes. According to a 2018 Ericsson Mobility Report，1B cellular IoT connections were made in 2018, which is expected to grow to 3.5B connections by 2023. Most of these unique IoT hardware systems have brought a new generation of security threats. These threats now provide attackers access to more than just data – they provide localized control and monitoring of devices directly in the public environment which, if compromised, can jeopardize the safety of an individual or even the global.

Product security has vulnerability at all stages of production and procurement. At the component level, devices can be compromised in the factory during testing, handling or shipment. At the board level, modifications and vulnerabilities can be found during end product development, testing or manufacturing. After the connected product is manufactured, the device is susceptible to reverse engineering, hacking and cloning. All of these situations may lead to critical data being accessed, monitored or controlled.

In order to avoid these issues, one or more IC devices in the system need to establish a Root of Trust or RoT. These devices provide cryptographic capabilities to the system, which can be used for securely booting and authenticating firmware, generating or verifying keys, certificates and signatures, and encrypting or decrypting data.

The RoT device provides security capabilities to the rest of the system through a Chain of Trust. As a result, it is the most critical device in the system from a security perspective since the entire system is vulnerable if it is compromised. Evaluating the entire lifecycle of the RoT device from semiconductor manufacturing to product is important as a result.

Encryption functions use key pairs to identify and verify system functions. Semiconductor manufacturers that produce IOT need to be able to establish a root key that matches the private key inside the IOT device, and the private key is inaccessible and never can leave the device. If the private key is accessible in manufacturing, that device could be susceptible to cloning or hacking. Additionally, if the private key is stored

in the device’s flash or fuses, the key may be susceptible to retrieval in manufacturing or reverse in the design.

To solve these two problems, RoT devices should use a Physically Unclonable Function or SRAM PUF, which uses the intrinsic properties of an element in silicon as a truly random identifier. This identifier can then be used to generate key pairs when the device powers up rather than storing it in a particular area which could potentially be reversed. Additionally, to prevent cloning a certificate for the RoT, device should be issued on the manufacturing floor. This certificate should have a signature based on the root key pair within the encrypted engine of the device. With a signature from the manufacturer of the device as the certificate authority, the device can be validated as genuine to the system ensuring that the RoT device itself is not a clone.

Compliance to standards is also important to ensure that security elements in the RoT device are compatible with the rest of the system. As a result, in addition to complying with the standards set by the National Institute of Standards and Technology, SP 800-90 compliance for random number generation and SP 800 193 for Platform Firmware Resiliency or PFR are important factors for both security and compatibility.

Security and RoT Device Options

Historically, there have been two options for security devices in a given system: MCU and FPGA. Both of these systems have advantages and disadvantages. MCU has the advantage of ease of use, and it is much easier to license libraries and APIs that are more easily transplanted from one device to another. A good example of this would be something like FreeRTOS and MBED TLS, which has become widely used for embedded IoT systems to gain TCP/IP and TLS/SSL. One disadvantage to the MCU is IO available, which can cause limitations to the number of interfaces needed to provide security features over the entire system. Another disadvantage is the MCU's ability to check its own boot memory during runtime.

FPGA has a large number of IOs, low latency and the ability to check system components in parallel. A large number of IOs allows you to control and monitor more components in the system, low latency allows you to check system components faster, and parallel computing allows you to faster check the overall system. However, its main disadvantage is that it is not as easy to use as MCU. For example, enabling TCP/IP and SSL stacks in the FPGA without a processor and significant memory would be extremely challenging and likely not a priority for the OEM.

Ultimately, the ideal device would integrate security features into devices with both an MCU and FPGA fabric at a low cost and lower power. It would also have the right packaging needed for an array of applications from edge devices to the Server. This would provide the advantages of both historical options and optimize the system based what's required. Fast power up and parallel checking can be achieved by taking advantage of the FPGA fabric, while the MCU's ease of use and library integration can enable faster development time.

Gowin SecureFPGA™ – Secure µSoC FPGA for RoT in Edge, IoT and Server Systems

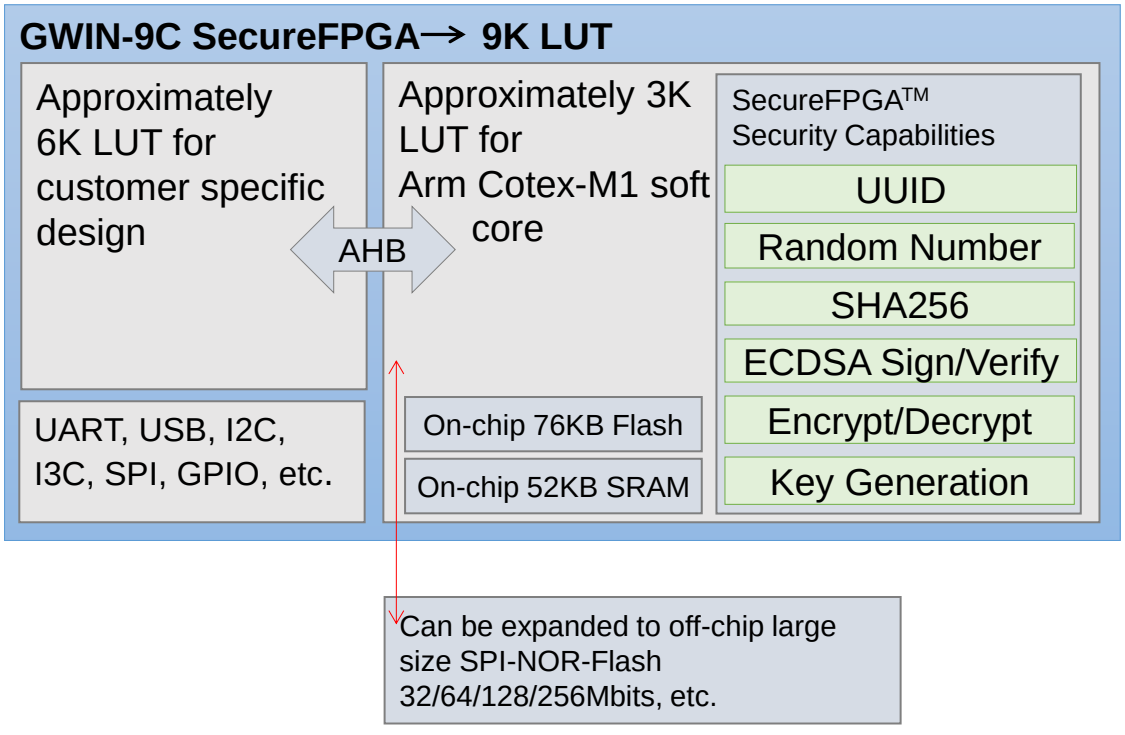
The latest innovation in RoT device security is Gowin SecureFPGA™, which combines the advantages of the MCU and FPGA with the security functions needed for edge, IoT and Server applications. SecureFPGA provides a security library based on SRAM PUF technology with Gowin genuine device authentication designed to eliminate attacks from the factory floor to the daily use of the end product.

The device has a wide range of packaging including BGA, QFN and TQFP to meet the needs of IoT and Server applications. There are different IoT packages. Server packaging is available such as QFN, BGA and TQFP depending on the application.

Full-Featured Security Library

Gowin SecureFPGA™ intends to solve and eliminate issues with current security devices by providing a full-featured security library along with a secure component based on SRAM PUF technology and Elliptic Curve Cryptography or ECC. Additionally, Gowin has cooperated with Intrinsic ID to offer the BroadKey-Pro security library. Developers can use encryption tools to create a RoT for applications in Gowin SecureFPGA devices, or use proven and mature security solutions to provide a RoT for multi-device systems

Figure 1 GW1N-9C SecureFPGA™ Device



Gowin SecureFPGA™ Security Capabilities

- Bitstream Lock - Removes the possibility of off-chip reading device bitstream
- Factory Provisioning - Activates code, UUID, CSR and Certificate
- Internal Dual Boot Flash - Online and remote upgradable with firmware signature checking
- SRAM PUF - Root devices keys generated at powerup; never stored in Flash
- UUID - Unique Device Identifier signed with the SRAM PUF root key pair
- Device Certificate - Validates device as a genuine Gowin device signed with SRAM PUF root key pair
- ECDH Encryption/decryption - AES128/192/256 Engine based on ECC Key Pair codes; SRAM PUF device unique or random.
- Asymmetric key pair generation - Based on SRAM PUF device, unique or random.
- ECDH Symmetric key generation - Based on SRAM PUF device, unique or random.
- ECDSA Signature - Generation and Verification
- Random Number Generator - Based on SRAM PUF and AES

Security Solution Maturity, Compliance, and Certificates

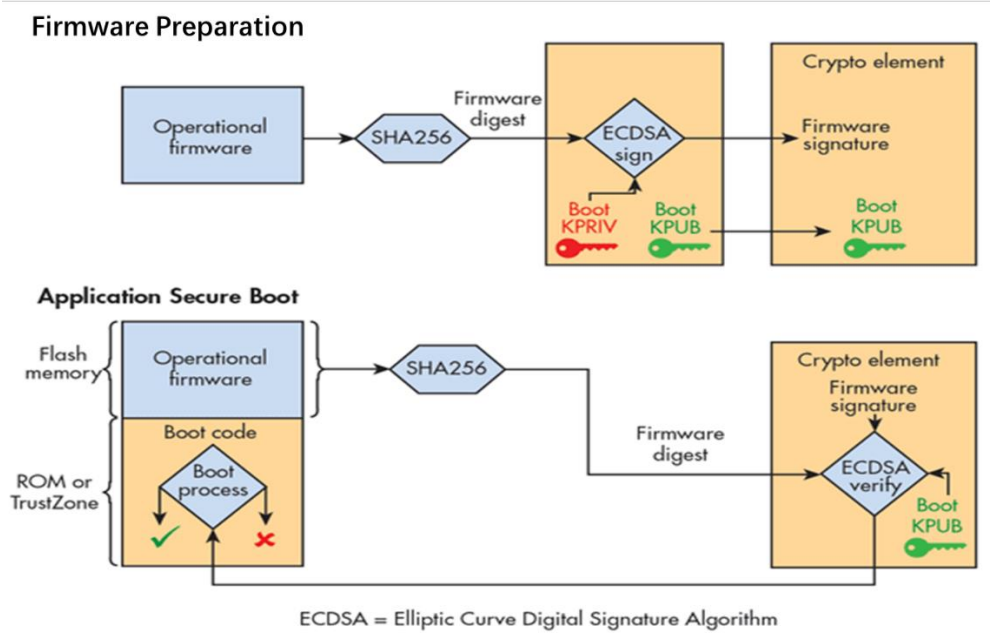
GOWINSEMI has cooperated with Intrinsic ID to offer the BroadKey-Pro security library within Gowin SecureFPGA devices. Intrinsic ID provides one of the most mature SRAM PUF technology solutions in the industry and has been adopted by many semiconductor device providers. It has been recognized in the industry for several years and recently was named IoT Security Product of the Year in the 2019 IoT Breakthrough Awards. It has been shipped into over 125 Million IoT devices, and meets the requirements of FIPS 140-2 Appendix B and China's OSCCA standards. Lastly, it has been deployed in everything from banks to banks, setting a high standard for security in RoT capable devices. The certificates include EMVCo, Visa, and CC EAL6+.

Typical Applications

Secure Boot and Secure Software Update

Secure boot is the process of hashing and generating a signature using a key and then verifying it versus a signature created at an earlier time, then the device can check whether the firmware has been tampered before executing it.

Figure 2 Secure Boot



For embedded applications, the secure boot starts by generating a signature over the firmware using the private key of a key pair. This signature is stored in the device for comparison at runtime. Once a signature is generated and stored, a small set of boot code can generate a signature using the public key and verify it versus the signature previously generated and stored in the device.

Figure 3 SecureFPGA™ - Secure Boot Preparation

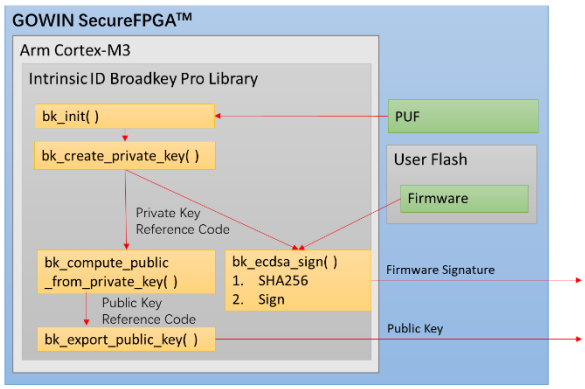
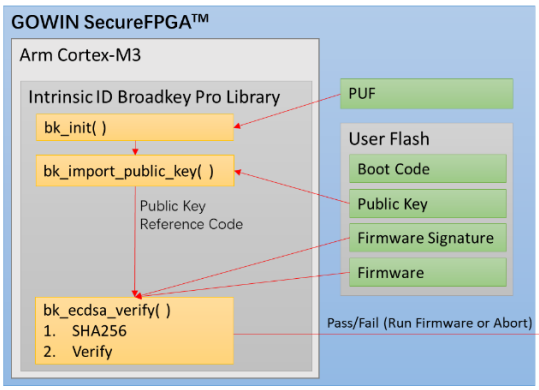
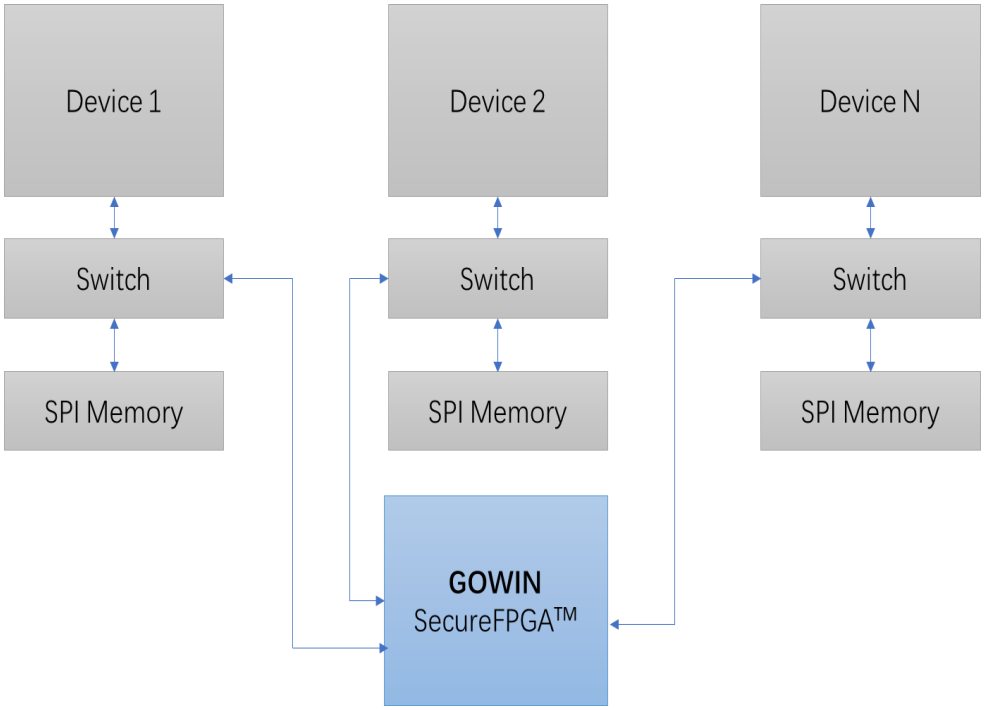


Figure 4 SecureFPGA™ - Secure Boot Verification



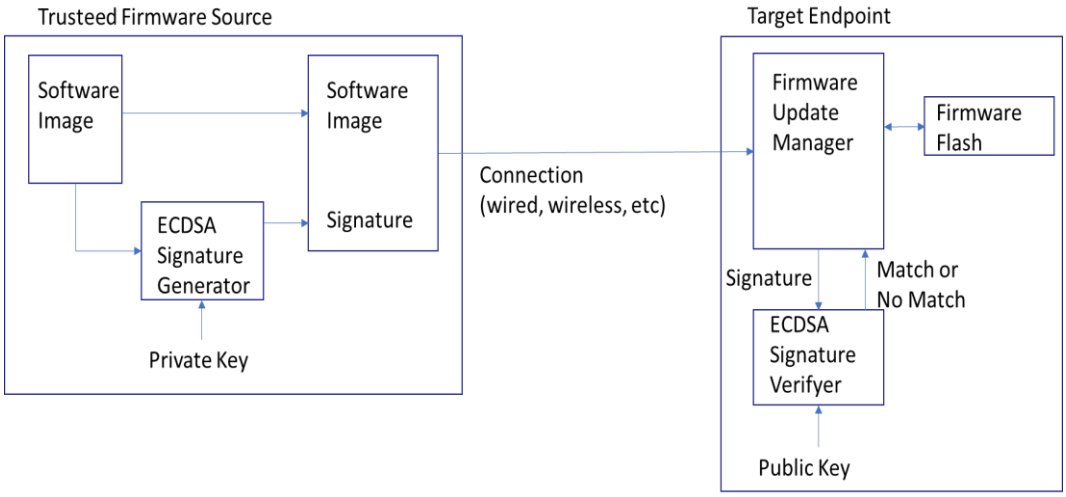
It also can be applied for verifying firmware for multiple devices on a server. Each firmware has a signature generated by the private key of the pair. Then at power up, Gowin SecureFPGA validates signatures of each firmware for each device.

Figure 5 Gowin SecureFPGA™ for Secure Boot in Server Applications



In addition to device secure boot and server secure boot applications, it also can be used for secure firmware updating. In this case, firmware is signed by the source and sent to a device over some medium such as the web or a cable. The device can then use the public key to verify the firmware before switching to it or retain the use of its base image.

Figure 6 Secure Firmware Update



Data Encryption

There are many applications that have a need for encrypting data. For example, a device can individually encrypt or decrypt data or firmware in its flash or ram so plaintext is never stored. Another scenario is that a device can exchange encrypted or decrypted data with another device with exchanged keys so that the data will not be leaked during transmission.

Figure 7 Gowin SecureFPGA™ Internal Device Encryption/Decryption Flow

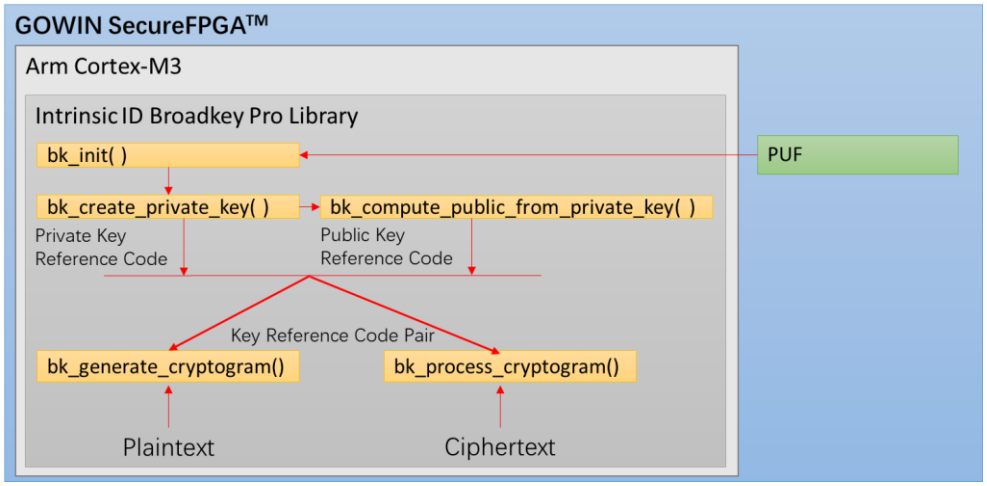
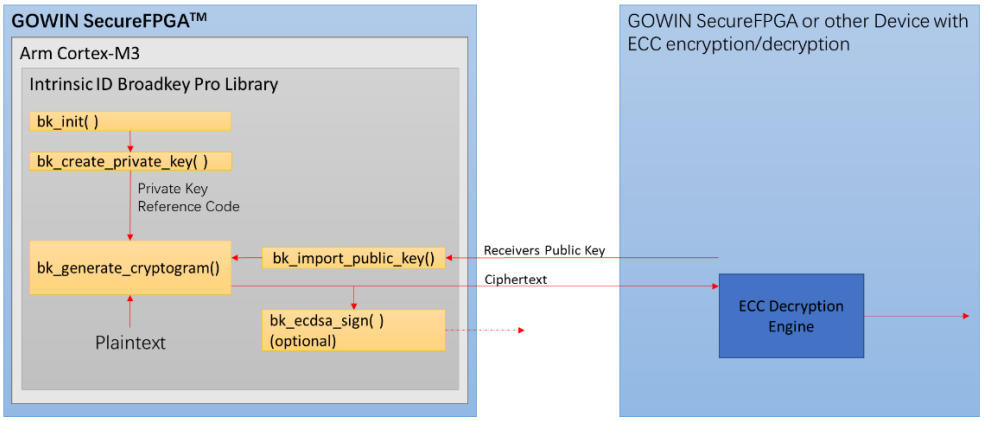


Figure 8 Gowin SecureFPGA™ Device to Device Encryption/Decryption Flow



Manufacturing

To ensure security over the entire manufacturing process, GOWINSEMI has special SecureFPGA equipment. SecureFPGAs are provided with an activation code during test time, which enables the device to always generate the same root key pair. The root private key that is generated with the SRAM PUF engine is never exposed to the user or outside the device. It is only available to security functions in the device and called by the user through key codes. During configuration, the root public key is exported from the device. A Certificate Signing Request or CSR and UUID for the device are formed, which can be used with a third party CA. Optionally, Gowin provides a Certificate Authority (CA) service to generate the certificate for each device in the factory. Gowin CA service provides the ability to confirm a device is genuine by validating the devices unique certificate or repudiating; if not genuine, please contact Gowin technical support. These features provide assurance that the device has a unique identity; it is genuine and does not contain content in flash that may be vulnerable to be attacked from factory floor to end of product life.

Conclusion

Gowin SecureFPGA products provide a Root of Trust based on SRAM PUF technology. These devices are virtually impossible to duplicate, clone or predict. This makes them very suitable for applications such as secure key generation and storage, device authentication, flexible key provisioning and chip asset management. Each device is provided with a unique key pair that is never exposed outside the device or during device development or manufacturing. The Intrinsic ID BroadKey-Pro security library is provided with Gowin SecureFPGA devices, allowing easy integration of common security features into user applications. Gowin SecureFPGA is used widely for a variety of applications such as consumer, industrial IoT, edge, and server management.

Related Material

1. Columbus, Louis. “2018 Roundup Of Internet Of Things Forecasts And Market Estimates.” Forbes, Forbes Magazine, 18 Dec. 2018, www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/#4b33a2747d83.
2. Lazich, Milan. “Intrinsic ID's BroadKey Named 'IoT Security Product of the Year' in 20.” PRWeb, 3 Jan. 2019, www.prweb.com/releases/intrinsic_ids_BroadKey_named_iot_security_product_of_the_year_in_2019_iot_breakthrough_awards/prweb16012275.htm.

Technical Support

Gowin Semiconductor provides customers with comprehensive technical support assistance. If you have any questions, comments, or suggestions, please feel free to contact us.

Website: www.gowinsemi.com

E-mail: support@gowinsemi.com


GOWIN
PROGRAMMING FOR THE FUTURE