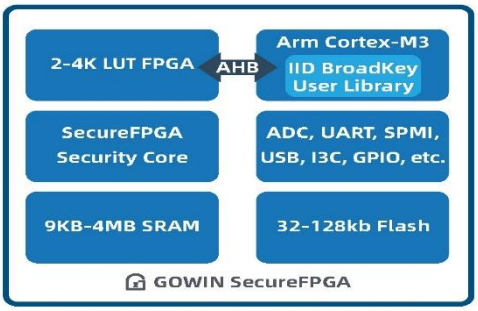
SecureFPGA

The latest innovation in RoT device security is GOWIN's SecureFPGA™, which combines the advantages of an 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.

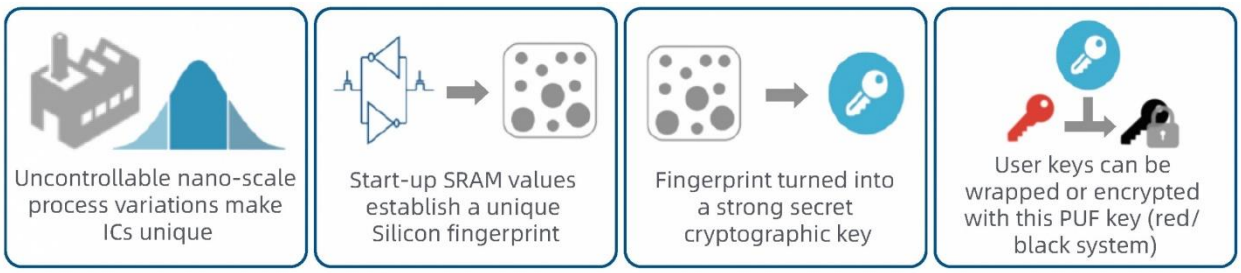
The included security library also provides commonly used security functions making it easy to add protection to any current MCU or FPGA project

- **SRAM Based PUF**
  - No private key storage
  - Device keys recovered on power-up
- **Factory Provisioning**
  - Activation, UUID, Certificate
- **Low Cost, Small Form Factor Packaging**
  - As small as 2.5 x 2.5 mm²



Features

SecureFPGA products provide a hardware Root of Trust based on PUF (Physically Unclonable Function) technology. PUFs use the behavior of SRAM to differentiate chips from each other. They 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 factory provisioned with a unique key pair that is never exposed outside of the device.



The Intrinsic ID BroadKey-Pro Security library is provided with GOWIN SecureFPGA devices allowing easy integration of common security features into user applications. These features allow users to create unique device identifiers, generate/verify signatures for secure boot and encrypt/decrypt data.

INTRINSIC ID

BroadKey-Pro Features

- Device-unique key derivation
- Random number generation
- Elliptic curve private key generation and storage
- Importing and exporting of public keys
- Signature generation and verification
- Key agreement functionality
- Public key encryption and decryption