INTRINSIC ID

GOWIN
PROGRAMMING FOR THE FUTURE

Gowin SecureFPGA

Securing the IoT, One FPGA at a Time

The Internet of Things (IoT) offers great opportunities, but it is also a scary place. Not in the least for IoT device makers, or OEMs. Between anonymous online hacks and cutthroat competition, there are plenty of threats OEMs need to consider. Whether worrying about attacks on devices in the field or protecting their supply chain, it can be overwhelming for an OEM to consider all risks. Especially given that most OEMs are not security experts. How do I protect the data my device creates? And what about securing communications? How do I make sure no one creates counterfeits that will damage my revenue and/or reputation? Do I need to move to a costlier supply chain to deal with all of this?

To help OEMs address these serious concerns, without raising production and BOM costs, GOWIN Semiconductor launched its latest innovation: SecureFPGA. It combines the advantages of an MCU and FPGA with the security functions needed for edge, IoT and server applications. Using Intrinsic ID's security library BK™, SecureFPGA provides a robust hardware-based Root of Trust (RoT) for protecting devices in the field as well as for keeping the supply chain flexible, without an increased risk of attackers making counterfeit devices. In this case study we will focus on how this benefits IoT OEMs.

Challenge

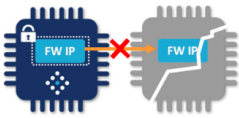
- OEMs need to protect the created data and communications of their IoT devices
- These devices also need to be protected from overproduction and counterfeiting
- None of this should adversely affect costs and supply chain flexibility for OEMs

Results

- Every device gets an unclonable, immutable, invisible, unique identity for authentication
- This identity is the basis for protecting data and communications, as well as supply chain
- Burden of security is lifted from OEMs, without affecting their OpEx or BOM

Solution

- GOWIN's SecureFPGA's Root of Trust delivers an anchor of trust for security use cases
- Using Intrinsic ID's BK, SecureFPGA offers turnkey security solutions for OEMs



"BK Software allows our customers to protect their assets from being stolen or cloned during manufacturing, and provide authentication and encryption functions for edge-to-cloud applications"

Jason Zhu, CEO at GOWIN Semiconductor

Use Cases

Deployed IoT devices create valuable data, which is the currency of the IoT. This data needs to be protected at all times to keep its value. This requires a Root of Trust in the device that protects data by encryption (at rest and in transit) and authenticates the device and data to establish it as trustworthy. This is of vital importance to the customers of OEMs.

Besides offering this RoT to customers for data protection and authentication, OEMs are also concerned about how to protect their devices against counterfeiting and overproduction. If others can replicate these devices for gain, this will hurt the OEM's revenue, and most likely reputation, due to inferior quality counterfeits. OEMs need to bind their valuable IP to the hardware of devices (anti-counterfeiting) and and limit the number of devices enabled during production (anti-overproduction). Again, a strong hardware-based RoT is the solution.

GOWIN's SecureFPGA

So, how can OEMs add this functionality to their IoT devices, to protect their customers and themselves? The answer is GOWIN's SecureFPGA, an FPGA with an integrated MCU, which includes the hardware-based Root of Trust needed to solve these use cases. SecureFPGA has an unclonable device identity to authenticate IoT devices. It also provides encryption to protect sensitive data and valuable IP and set up secure communication to the cloud or other devices. Finally, SecureFPGA allows OEMs to automate the deployment of the RoT in a less-than-trustworthy supply chain. Besides the described IoT market, SecureFPGA is also very suitable for protecting devices in edge computing and server markets.

BK-Pro

Now, what is under the hood of SecureFPGA to create this strong hardware-based RoT, while keeping the flexibility in the supply chain? This is Intrinsic ID's product BK-Pro.

BK-Pro is a software library that uses tiny variations in the silicon of every individual chip to extract a "silicon fingerprint," creating an unclonable identity from within. This unclonable identity consists of a secret key, a public key and a certificate. The secret key is derived from inherent randomness in the start-up pattern of SRAM inside SecureFPGA. The secret key is never stored, but dynamically generated when needed, which makes the RoT highly secure.

Besides the secret key generation and secure storage, BK-Pro offers a complete asymmetric crypto library. This allows for key pair generation, creating and verifying signatures, and key agreement functionality.

Bottom Line Benefits

SecureFPGA offers a combination of FPGA with MCU that has a strong Root of Trust to help OEMs and their customers solve the most urgent security issues in IoT, while lowering costs and increasing supply chain flexibility.

GOWIN Semiconductor

Founded in 2014, GOWIN Semiconductor Corp., headquartered with major R&D in China, has the vision to accelerate customer innovation worldwide with its programmable solutions. GOWIN focuses on removing barriers for customers using programmable logic devices. Offerings include programmable logic devices, design software, intellectual property (IP) cores, reference designs, and development kits. Visit www.gowinsemi.com