ReThink Secure Computing with CrossBar ReRAM PUF Technology

Physical Unclonable Function (PUF)

BACKGROUND

Attacks on electronic devices and systems such as IOT endpoints, computers, medical devices and infrastructure are on the rise. These attacks pose information security and safety hazards to companies and individuals. In addition, business must also deal with counterfeiting threats to brand name products. To resist such attacks, maintain secure computing and mitigate the threat of counterfeiting, new devices are implementing security features utilizing cryptographic "keys". These keys are used for identification, encryption/decryption and authentication. Cryptographic keys are commonly referred to as a "physical unclonable function", or PUF keys. These keys act as a secret "digital fingerprint" providing a set of random-unique identifying numbers for a specific device that cannot be easily observed, deciphered or copied thereby preventing an attacker from impersonating a valid device. PUF keys are often 256 bits in length and employed to secure and unlock the operation of devices by approved users. The foundation for the secure operation of computing systems is often referred to as "root of trust" which typically utilizes a challenge-response method of authentication. For higher levels of security, root of trust keys are typically implemented within integrated circuit semiconductor hardware.

While CrossBar's ReRAM technology has been traditionally utilized for non-volatile memory, the company has recently introduced its unique ReRAM cell technology for its novel use as cryptographic keys for the secure operation of electronic devices.

ADVANTAGES OF RERAM PUF

While numerous technologies are capable of operating as PUF keys, the most common hardware approach available today is to exploit the randomness characteristics of semiconductor Static Random Access Memory (SRAM). Unfortunately, SRAM PUF key technology has numerous drawbacks limiting its level of security and effectiveness as noted in its: 1) Lower levels of key randomness, 2) High bit error rates, 3) Limited tamper and side-channel resistance and 4) Longer sensing times.

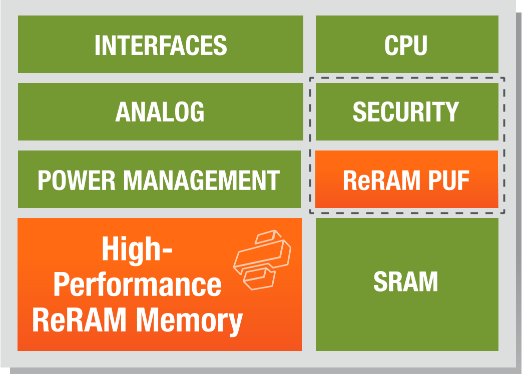
In contrast, CrossBar's latest ReRAM PUF cryptographic key technology is enabling a new class of secure devices and systems, addressing many of the shortfalls associated with SRAM PUF. CrossBar's ReRAM keys have a higher level of randomness, much lower bit error rate and is higher resistance to invasive attacks than SRAM. In addition, ReRAM has the capability of tolerating a wide range of operational extremes including temperature, supply voltages and electromagnetic fields due to the inherent physical characteristics of the technology.

ReRAM PUF KEY FACTS

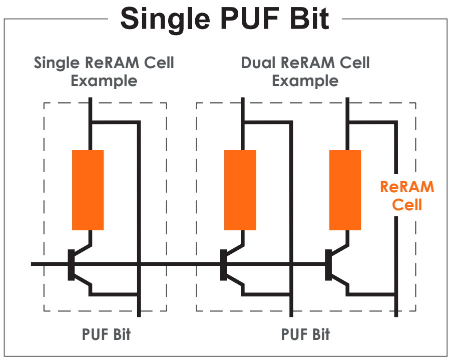
- New use of ReRAM technology for security applications
- ReRAM cell utilized for physical unclonable function (PUF) security keys
- More secure than SRAM based PUF keys
- Less exposure to invasive attacks
- Synergistic with CrossBar ReRAM non-volatile memory technology

TARGETED APPLICATIONS

- IOT end points
- Brand name supplies (example printer ink cartridges)
- Medical equipment & supplies
- Systems
- Infrastructure
- Automobiles
- Government applications


INTERFACES
CPU
ANALOG
SECURITY
POWER MANAGEMENT
ReRAM PUF
High-Performance ReRAM Memory
SRAM

MCU with Embedded ReRAM NVM & PUF



In addition, since the ReRAM PUF bit error rate is so low compared to SRAM PUF, ReRAM implementations do not require fuzzy extractors, helper data or heavy error correction code. ReRAM PUF is thus less complex to implement and operate, with higher performance and security than alternative solutions. Depending on its implementation, ReRAM PUF read/sense times can be less than 15ns, improving security system performance with reduced time to extract the key.

Randomness of the PUF cell itself is also a critical component for secure computing. CrossBar's ReRAM PUF has very high randomness characteristics and meets industry standards such as the NIST SP 800-22 and SP 800-90B randomness requirements. Compared to SRAM based PUF, CrossBar's ReRAM PUF has significantly higher spatial randomness as well.

Physically tampering with the ReRAM cell thru side-channel attacks to sense the secret PUF key is virtually impossible due to the inherent physical characteristics of CrossBar's ReRAM technology. The ReRAM PUF key is resistant to physical attacks such as simple/differential power analysis, photonic emission analysis, cold boot attack and probe based sensing.

CrossBar's new ReRAM PUF technology is an ideal candidate for applications requiring both high security (PUF cryptographic keys) and efficient non-volatile memory embedded in semiconductors, which is especially important at foundry nodes smaller than 28nm where embedded NVM memory (flash memory) is not typically available. In numerous situations, the same ReRAM NVM memory cell can be utilized as a ReRAM PUF cell.

HOW ReRAM PUF WORKS

Depending on the specific implementation, ReRAM PUF keys can be implemented using either a: 1.) Single ReRAM cell or 2.) Dual ReRAM cell, each representing a single PUF bit. When the ReRAM PUF bit is sensed, it's observed as randomly either a "1" or "0" for each PUF bit on each semiconductor. For example, if an IOT chip has fabricated 256 ReRAM PUF bits, each individual manufactured part will contain a 256 bit key, unique to that specific semiconductor chip.

Summary

CrossBar's Resistive RAM technology has numerous uses including both high-performance and high-density non-volatile memory. In addition, the company is now exploiting the benefits of its unique ReRAM PUF technology for secure computing, providing superior cryptographic security characteristics, simpler implementations, higher speed processing and synergy with embedded ReRAM NVM memories.