Mitsubishi Electric, Ritsumeikan University and JST Develop Security Solution for IoT Devices

2/5/2015

Protects the safety and security of embedded devices by using individual differences of LSIs

Mitsubishi Electric Corporation (TOKYO:6503), Ritsumeikan University and Japan Science and Technology Agency (JST) today announced that they have developed a security technology that uses the individual differences of large scale integrations (LSIs) arising during their fabrication to ensure confidentiality and authentication for interconnected devices in the Internet of things (IoT). The new technology helps to reduce security risks for networked devices by protecting embedded programs and preventing spoofing. Mitsubishi Electric will begin applying the technology in its products from April 2016.

LSIs make calculations based on internal circuits that dictate output, so LSIs with the same circuits yield the same results when processing the same input. Intermediate routes to the computation result, however, are different in each LSI, serving as something like a fingerprint, which the new technology uses to generate unique IDs for LSIs with the same circuits. The unique ID cannot be analyzed even by opening the LSI package and examining its insides because the ID appears only while the circuit is running. The embedded program is encrypted so that it can be decrypted and used only in the device that has the LSI with a specified ID. It is also possible to configure devices to connect only with devices that have specified IDs.

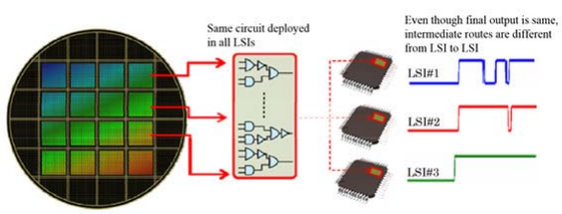

Fig. 1 Slight differences in computation processes of circuit gates in different LSIs

The unique ID is generated as follows:
Step1. Count the number of glitches (peaks) that arise on signal input. If the number is even, assign 0 as an output bit, and if odd, 1. **Step2.**Repeatedly change the signal input and compute the corresponding output bit, thus generating a unique ID.

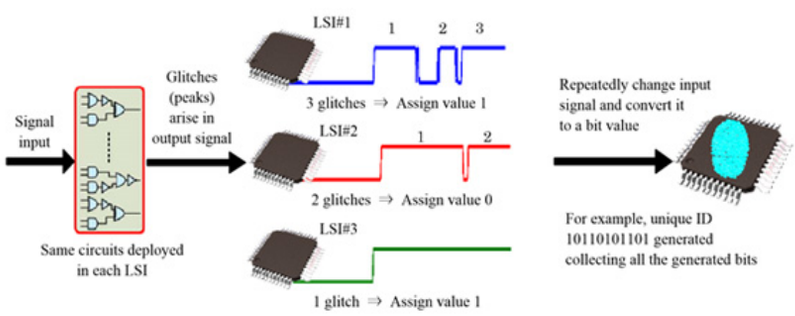

Fig. 2 Unique ID generation

Three functions—generation of unique ID, encryption and authentication—can be implemented in a small circuit area by letting them share some of their components. The required area is one third of that in the case where each function is separately implemented. In addition, prototype LSIs developed jointly with Ritsumeikan University using multiple manufacturing processes have been confirmed to generate unique IDs stably, so the technology can be modularized and thereby easily applied in a general LSI design flow.

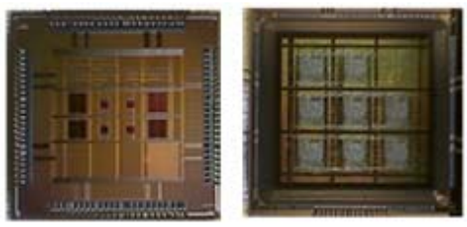

Fig. 3 Prototype LSIs that generate unique IDs via signal transition (Left: 65 nm, 2.1 square mm; Right: 180 nm, 2.5 square mm)

As the use of networked embedded devices increases, countermeasures to prevent program analysis, falsification, data theft and device spoofing are becoming more important. Especially in the case of embedded devices with high safety demands, complete measures for program and data protection are required. Generally, ID information for cryptographic use is stored in memory embedded in a device, and this information remains in memory even after powering off, so analysis of the ID is possible by opening the LSI package and examining its insides.