A BEHAVIORAL AND PHYSICAL UNCLONABLE FUNCTION (BPUF) AND A MULTIMODAL CRYPTOGRAPHIC AUTHENTICATION METHOD USING THE SAME

University of Seville has developed a physically and behaviorally-defined set of digital fingerprints (BPUF) that serves as a set of identifying traits for a semiconductor device. The BPUF is tamper resistant, and tamper-evident to the physical attacks reported to currently known physically unclonable functions (PUFs) because those attacks change the behaviorally-defined fingerprints in the BPUFs. Physical clones of BPUFs are very much challenging to obtain since BPUFs consider behavioral and dynamic identifying traits. The multimodal cryptographic authentication method of the present invention is privacy-preserving because the identifying traits of the device are not disclosed. Besides, the authentication method can be very lightweight and a non-protected communication channel can be employed between the device containing the BPUF instance and the verifier.

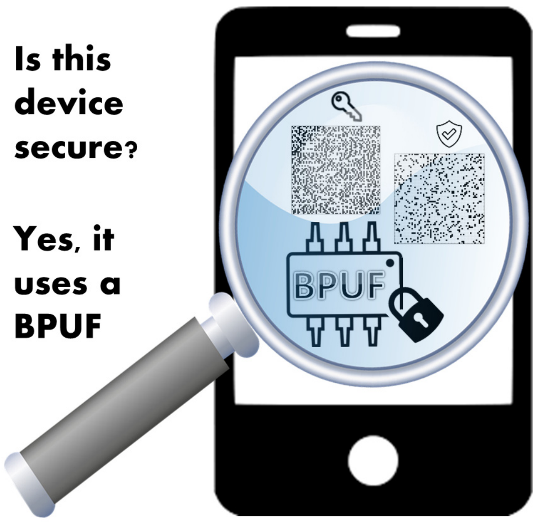
An offer for patent licensing

Technology summary

The protection of information is of crucial importance, especially when dealing with sensitive data. To achieve a high degree of protection, information security has to be conceived from the design of the cryptographic algorithms until its implementation into the software and hardware of devices (servers, routers, smartphones, etc.). Solutions are required to avoid and detect counterfeit devices as well as to avoid and detect tampering, which consists in permanently manipulating a device with the objective of carrying out unauthorized operations.

Since 2002, PUFs are being exploited to identify trusted devices uniquely (like a biometry for devices). A PUF is a physical construction (based, for example, on the Static Random-Access Memory, SRAM, in a device) that is able to measure the unique physical variations that affected during that SRAM fabrication, by generating unique responses to given challenges. However, several attacks have shown that PUFs made to date can be not only fully characterized and emulated but also cloned physically.

The BPUFs of the present invention improve the security of current PUFs because they generate not only unique physical but also behavioral distinctive responses to given challenges, allowing the use of stronger multi-factor authentication solutions.



A BPUF can be added to any electronic device, either by including a firmware that exploits intrinsic hardware of the device (SRAM, for example) or by including a dedicated hardware block in the device.
Hardware roots of trust and trusted platform modules are better with BPUFs than with PUFs.

Main applications and advantages

- The multi-factor cryptographic algorithm based on BPUFs satisfies diversity and revocability because different protected responses can be generated from the same BPUF. The solution also satisfies irreversibility and unlinkability because the stored data do not reveal anything about the specific device.
- As example to validate the proposed invention, BPUFs based on SRAMs, with one physical and one behavioral response to given challenges, were analyzed experimentally using integrated circuits of 90-nm CMOS technology. If an attacker succeeded in the reported attacks on SRAM PUFs, the highest probability to succeed in the proposed SRAM BPUFs was evaluated experimentally as 1.5e-34, considering changes in the operating conditions (power supply voltage, temperature, and aging).

Patent status

Request for grant of a European patent.

For further information please contact

Dra. Iluminada Baturone,
Instituto de Microelectrónica de Sevilla (IMSE-CNM), Universidad de Sevilla.
Tel.: + 34 95 446 66 66
E-mail: lumi@us.es