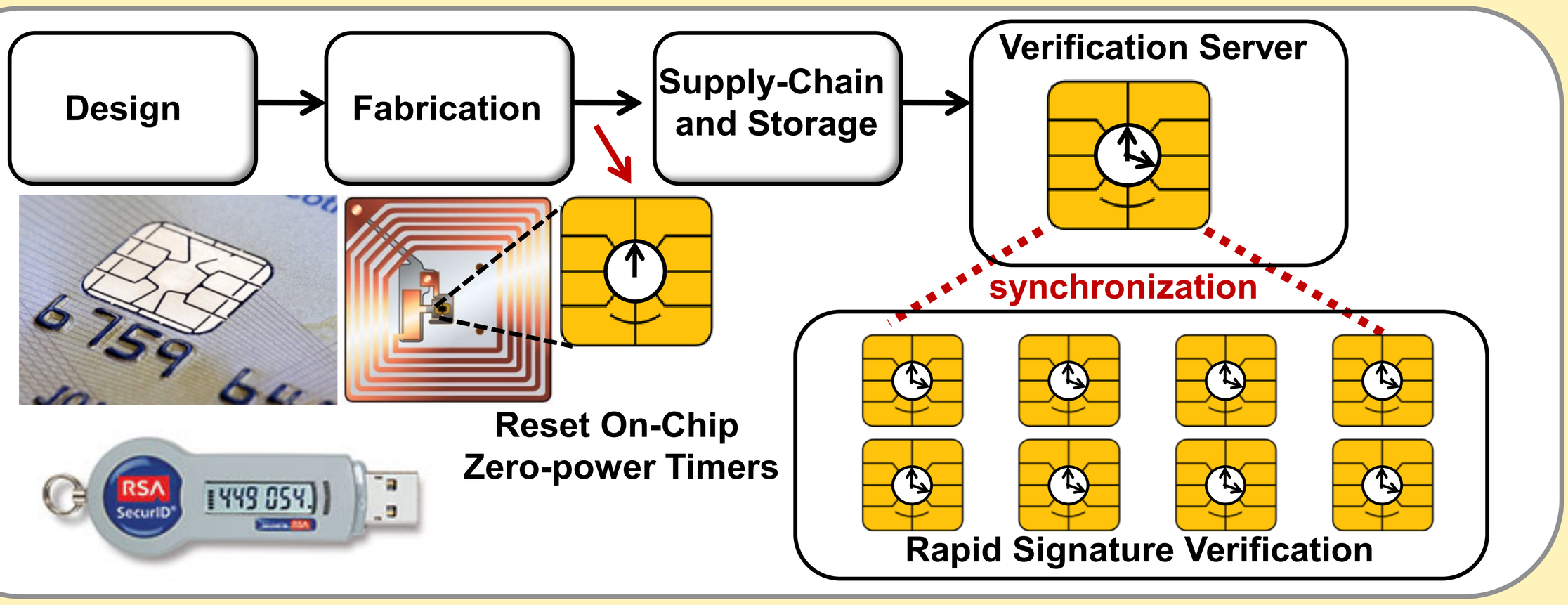
Zero-power Dynamic Signature for Trust Verification of Passive Sensors and Tags

PIs: Shantanu Chakrabartty (Washington University in St. Louis), Jian Ren (Michigan State University)

The objective of this research is to investigate dynamic hardware-software authentication techniques on passive assets (tags and IoT sensors) based on zero-power timing and synchronization circuits.

Passive assets have very limited computational capabilities which obviates the use of high-performance encryption techniques, use of strong hash functions and embedding of complex pseudo-random number generators. Also, the need for fast and real-time authentication obviates the use of multi-level authentication and challenge-response protocols in these assets.

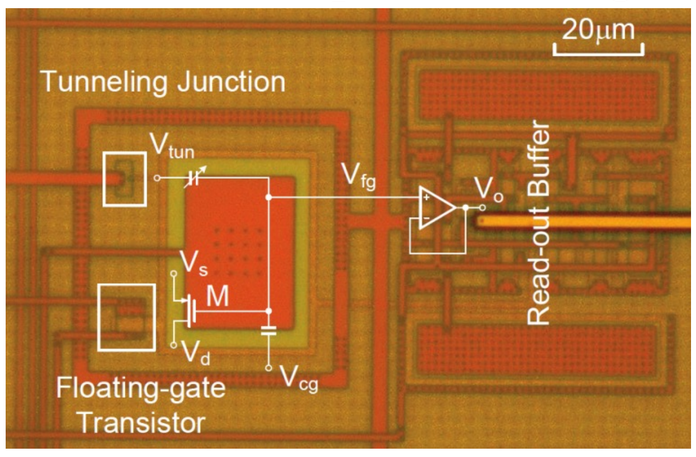


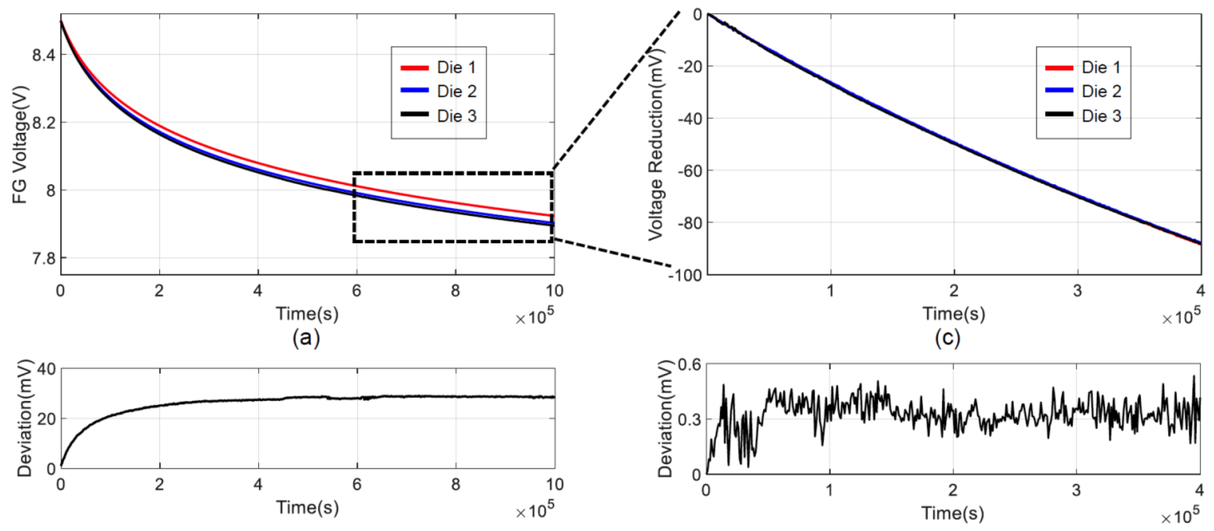
Approach

Enterprise-grade SecureID type authentication of passive devices based on a continuously running and a synchronized zero-power timer.

- Loss of synchronization between different clocks indication of counterfeiting, tampering or data theft.
- Verification tokens synchronously generated at the server and when the passive device is accessed.

Reliable Zero-power timing device





MSU Results here

Graphics/text as appropriate

Summary of Progress

- Zero power timers based on FN Tunneling – synchronization accuracy better than 60dB over 100 hours.
- Duration: greater than 3 years.
- One intellectual property, One Journal paper.
- Two graduate students.

Interested in meeting the PIs? Attach post-it note below!