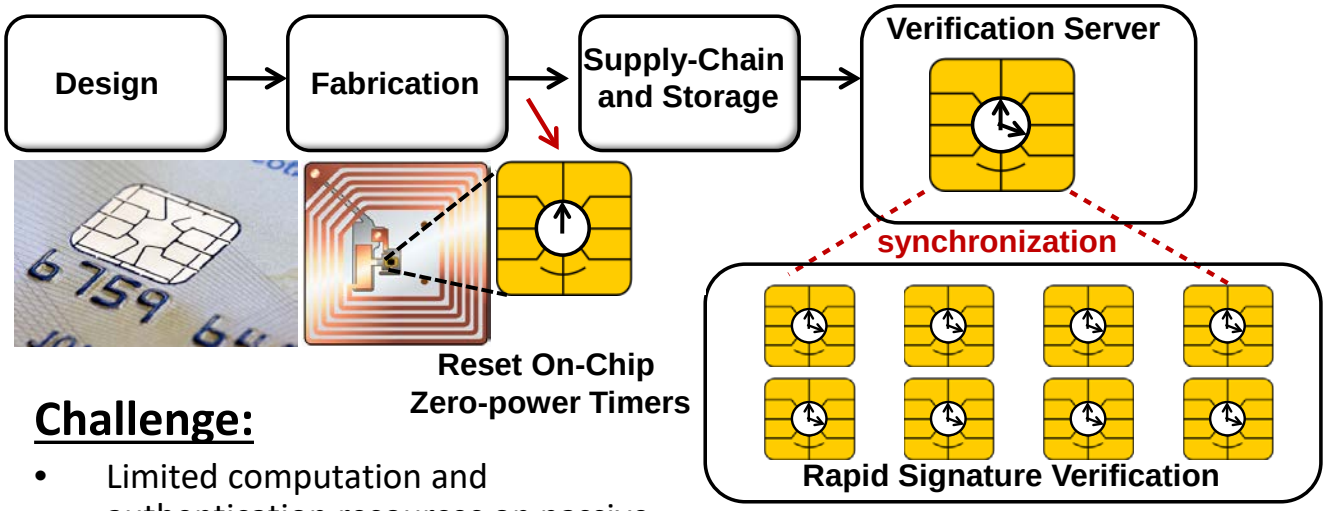
Zero-power Dynamic Signature for Trust Verification of Passive Sensors and Tags



Challenge:

- Limited computation and authentication resources on passive and remotely powered sensors, tags and cards (for e.g. radio-frequency identification tags or credit cards.
- Real-time authentication requirements
- Lack of a system clock obviates use of SecureID type authentication techniques involving random keys and tokens that need to be periodically generated and synchronized.

Solution:

- Zero-power timing and synchronization achieved due to the self-powering and self-compensating physics of Fowler-Nordheim (FN) quantum transport of electrons tunneling onto a floating-gate.
- A dynamic hardware-software authentication approach based on synchronization between zero-power timers.

Scientific Impact:

- Dynamic approach should provide enhanced security and make it more immune to counterfeiting and data theft.
- Enterprise-grade SecureID type authentication for passive and low-cost assets like RFIDs.
- Low-cost, low complexity, real-time implementation.

Broader Impact:

- Securing data in passive devices and sensors used in internet of things.
- Developing a cross-disciplinary forum between the electrical engineers and computer scientists with the focus on hardware-software trust verification.
- Joint collaboration with industry.

STARSS: 1525476, Washington University in St. Louis, Michigan State University.
Contact: Shantanu Chakrabartty
Email: shantanu@wustl.edu