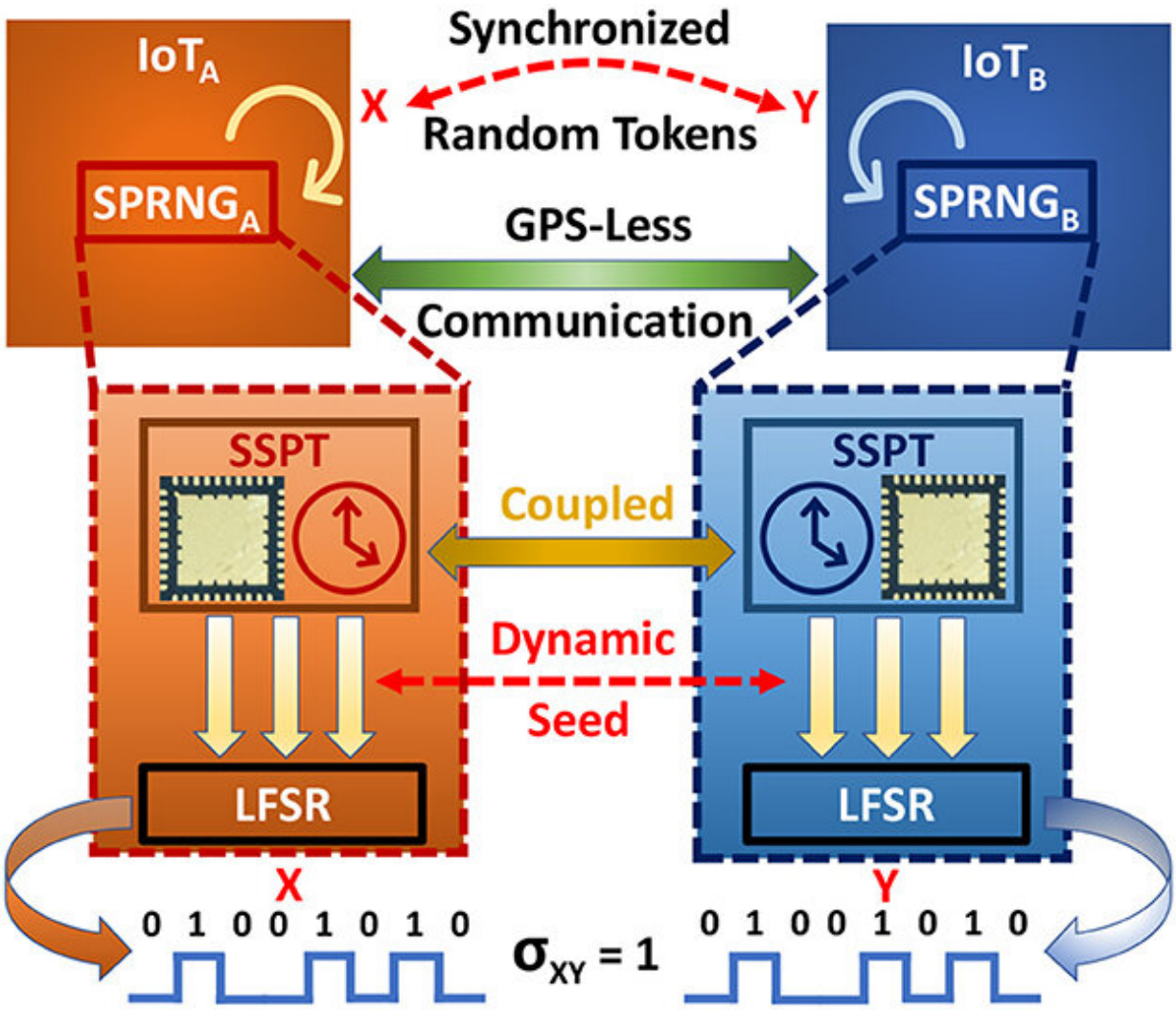
Making the Internet of Things more secure

March 30 2023, by Beth Miller



The concept of GPS-free secure Communication in spatially separated IoTs with SPRNGs: The IoTs generate random tokens using the SPRNG for use as cryptographic keys. The tokens are generated using a combination of a fast, low-complexity LFSR seeded by the Secure self-powered timers (SSPT). The synchronization of SSPT across both IoT_A and IoT_B ensures that the random

tokens X and Y exhibit a perfect cross-correlation, $\sigma_{XY} = 1$. Credit: *Frontiers in Computer Science* (2023). DOI: 10.3389/fcomp.2023.1157629

With wearable fitness trackers, car key fobs and smart home devices, the Internet of Things (IoT) has become ubiquitous in our lives. Unfortunately, much of this flow of information is vulnerable to malicious activity and attacks, as securing the IoT has not kept pace with new technological advances.

To address this, Shantanu Chakrabartty, the Clifford W. Murphy Professor in the Preston M. Green Department of Electrical & Systems Engineering at Washington University in St. Louis, and Mustafizur Rahman, a doctoral student in his lab, have developed a prototype method to better secure these communications using a synchronized pseudo-random-number generator (SPRNG). The method, which could be used to verify and authenticate secure transactions in IoTs, was published in *Frontiers in Computer Science* on March 20, 2023.

Securing wireless communications in IoT requires generation and synchronization of random numbers in real time—encrypting the data using a sequence of random numbers produced by a generator, then synchronizing them using a timing reference extracted from a global positioning system (GPS). For devices that operate on batteries or in energy-constrained resources, this is not practical, as many IoT devices do not have access to a GPS signal, said Chakrabartty, who also is vice dean for research and graduate education.

Chakrabartty and Rahman created a prototype synchronized self-powered timer array using quantum-mechanical tunneling of electrons that is secure against tampering, snooping and side-channel attacks. Specifically, they used Fowler-Nordheim (FN) quantum tunneling, in

which electrons jump through a triangular barrier, and in the process, change the shape of the barrier. FN tunneling provides a much simpler and more energy-efficient connection than existing methods that are too complex for computer modeling, and because it is self-powered, it is secure against attacks, Chakrabartty said.

"In this method, the proposed SPRNG could be used as a trusted platform module on Internet of Things and used to verify and authenticate secure transactions, such as software upgrades," he said. "Since this system does not require access to GPS for synchronization, it could be used in resource-constrained and adversarial environments, including health care and military IoTs."

Moving forward, Chakrabartty's team will investigate the effects of environmental variations, such as temperature drifts, on the synchronization of FN timers. They plan to develop a system-on-chip solution.

More information: Mustafizur Rahman et al, GPS-free synchronized pseudo-random number generators for internet-of-things, *Frontiers in Computer Science* (2023). DOI: 10.3389/fcomp.2023.1157629

Provided by Washington University in St. Louis