Washington University in St. Louis
Office of Technology Management

SELF-POWERED, SOLID-STATE DEVICES FOR REMOTE SENSING, TIMING AND SECURITY OF INTERNET-OF-THINGS AND OTHER PASSIVE ASSETS

Chakrabartty, Shantanu, Zhou, Liang

Markiewicz, Gregory

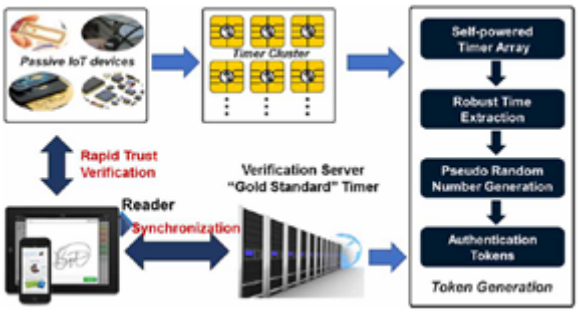
T-015908

Technology Description

Engineers in Prof. Shantanu Chakrabartty's laboratory have developed a self-powered, CMOS-based, nano-scale "smart sensor" and timer system that uses quantum-tunneling for reliable, long-lasting memory or authentication.

This technology is a floating gate device that continuously operates without external power by utilizing Fowler-Nordheim quantum tunneling and integration of electrons. The device was originally developed for continuously measuring and time stamping rare events in ultra-low power environments or remote locations over long periods of time **(WUSTL Technology T-015908)**. In these applications, the device detects and time stamps any deviation from normal storage or operating conditions. The floating gate acts as dynamic, non-volatile memory to store measurements that can be retrieved later for offline data analysis. Applications of the self-powered "smart sensor" include seismic and structural health monitoring, temperature sensing or detecting variations in medical devices.

Fowler-Nordheim tunneling in the floating gate architecture could also be leveraged as a timer module that could enable dynamic, rapid authentication of devices such as credit cards, security badges, RFID tags or other Internet-of-Things (IoT) devices. Specifically, this self-powered module **(WUSTL Technology T-016736)** would create a continuously running system clock that could be synchronized to a "gold standard" server for over three years. By using random keys or tokens that are periodically generated over time, this would allow trust verification in passive assets with limited computing and storage capability and no source of energy. This dynamic authentication system is more secure against theft, tampering or counterfeiting than static security like bar codes and product IDs.



Dynamic hardware-software authentication: combines zero-power timer technology and dynamic authentication software for an enhanced end-to-end security solution.

Stage of Research

Proof-of-concept - the inventors fabricated prototypes using standard 0.5um CMOS processing including:

- a modified non-volatile memory device which showed that less than 100fJ of sensing energy was required for event recording and time stamping
- a timer module device that would be operational for longer than 3 years (based on extrapolation study) and had a synchronization accuracy up to 0.5% even with device mismatch

Future work – planned studies include large-scale statistical testing and integrating the timer device on passive tags

Applications

- **Long-term/remote sensing** – basic device can be used for monitoring in applications with a using a "sense now, retrieve later" paradigm to track rare events, particularly where batteries and remote powering is impractical, such as:
  - seismic and structural health monitoring
  - medical devices – to detect misuse of an implant or deviation from normal operating conditions
- **IoT authentication:** continuous synchronization for "smart sensors" and other passive devices (e.g., RFID tags, credit cards, access cards or memory cards)
  - can implement dynamic, enterprise level Secure ID type authentication algorithms with periodically generated random keys and tokens
  - could be used as long-term clock to enable or disable features
  - trust verification of integrated circuits
- **Ultra secure root-of-trust security** for low resource IoT and IP protection

Key Advantages

- **Self-powered by omnipresent thermal and quantum fluctuations:**
  - activation energy for the device is well below 1-100 atto-watt range
  - zero external power needed for sensing, event detection, timing or authentication applications
- **Long life:**
  - continuously active with no downtime
  - timing keeping/authentication devices could last greater than 3 years
- **Robust and accurate –** different self-powered timers can be passively synchronized with respect to each other at an accuracy greater than 0.5%
- **Secure, dynamic authentication:**
  - no static identifiers (e.g., bar codes or product IDs) used for trust verification which should make timer-based authentication immune to theft, counterfeiting or tampering, practically zero side-channels
  - practically zero side-channels and immune to snooping
- **Solid-state:**
  - standard CMOS processing
  - 1/100,000,000 size of RSA Secure ID

Publications

- Zhou, L., Kondapalli, S. H., Aono, K., and Chakrabartty, S., Dynamic Signatures for Authenticating

IoT Devices Using Self-powered FN Tunneling Timers, *IEEE IoT Journal*, 2019.
- Zhou, L., Aono, K., and Chakrabartty, S., A CMOS timer-injector integrated circuit for self-powered sensing of time-of-occurrence, *IEEE Journal of Solid-State Circuits*, vol. 53, no. 5, pp. 1539–1549, 2018.
- Zhou, L., & Chakrabartty, S. (2016, May). Self-powered sensing and time-stamping of rare events using cmos fowler-nordheim tunneling timers. In 2016 IEEE International Symposium on Circuits and Systems (ISCAS) (pp. 2839-2842). IEEE.
- Zhou, L., & Chakrabartty, S. (2017). Self-powered timekeeping and synchronization using fowler–nordheim tunneling-based floating-gate integrators. *IEEE Transactions on Electron Devices*, 64(3), 1254-1260.THIS IS 160736

Patents

- Self-powered sensors for long-term monitoring (PCT Publication No. WO2017151628; WUSTL Technology T-015908)
- Self-powered timers and methods of use (U.S. Patent No. US10,446,234; WUSTL Technology T-016736)

Website

- Adaptive Integrated Microsystems (“AIM”) Laboratory