CAREER: Utilizing Principles of Energy Recovery Computing for Low-Energy and DPA-Resistant IoT Devices

Challenge:

- **Low-energy, lightweight, and secure devices, which are also resistant against malicious attacks that use power consumption traces to extract private or sensitive information.**
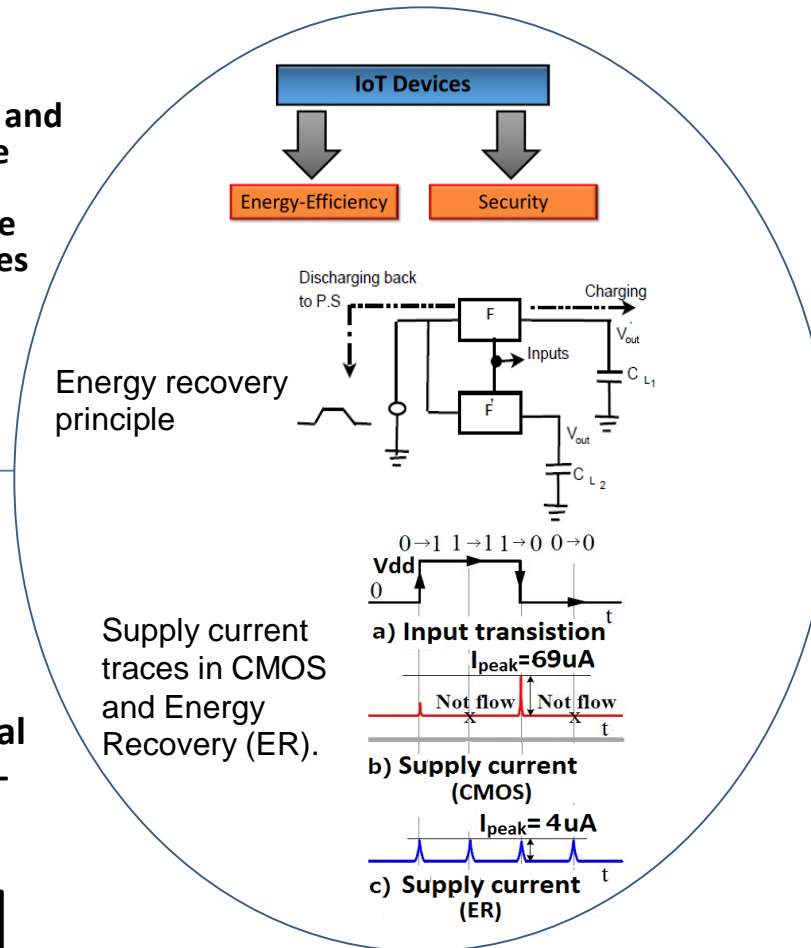
Solution:

- **Explores a set of energy recovery (ER) principles for low-energy and differential power analysis (DPA)-resistant IoT devices.**

Energy recovery principle

Supply current traces in CMOS and Energy Recovery (ER).

Scientific Impact:

- **Low-energy and DPA-resistant crypto circuits would pave the way for secure IoT devices which are working under energy constraints.**
- **Applications in smart devices, medical devices, various cyber-physical systems, etc.**

Broader Impact:

- **Industry adoption of ER computing based low-energy and secure IoT devices.**
- **Internships to Appalachian high-school students and underrepresented minorities, and first-generation students.**
- **Advance the hardware security and cybersecurity education.**