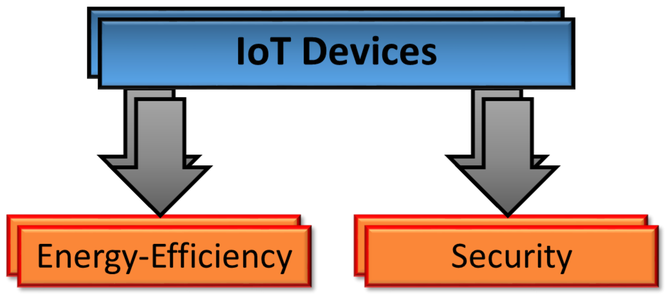
CAREER: Utilizing Principles of Energy Recovery Computing for Low-Energy and DPA-Resistant IoT Devices

Himanshu Thapliyal , University of Kentucky, Lexington, KY <hthapliyal@uky.edu>

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.

Scientific Impact

The investigation and development of energy recovery-based low-energy and DPA-resistant crypto circuits would pave the way for secure IoT devices which are working under energy constraints, and it will also have applications in smart devices, medical devices, various cyber-physical systems, etc.

Solution

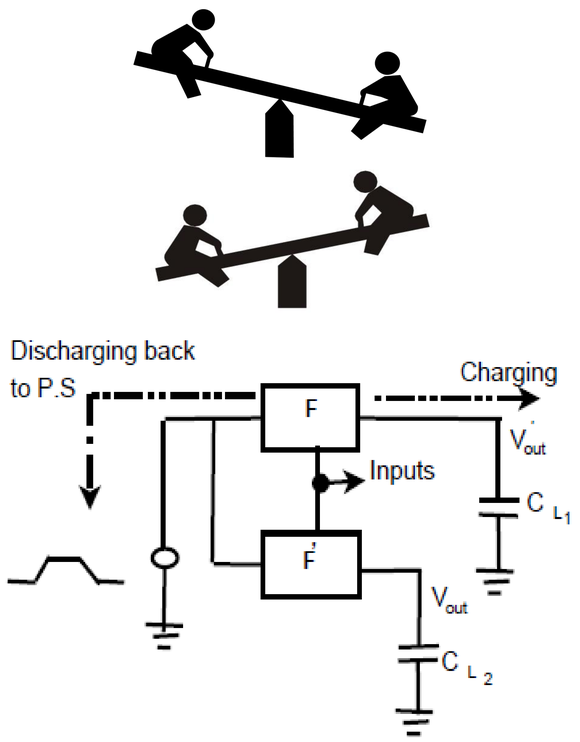


Fig. 1. Energy recovery principle.

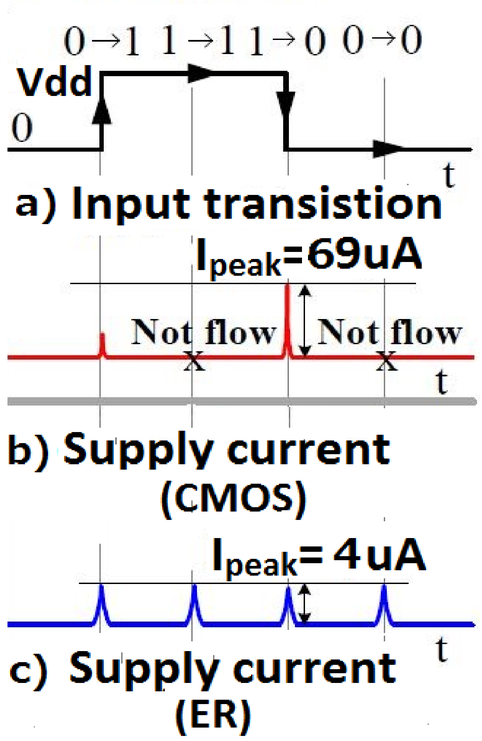


Fig. 2. Supply current traces.

Technical Approach

This project explores a set of energy recovery (ER) principles for low-energy and differential power analysis (DPA)-resistant IoT devices. The research objectives are: (i) to investigate information leakage in ER circuits and propose mitigation methodologies; (ii) to investigate and develop a low-energy and DPA-resistant ER standard cell library and semi-custom design flow for lightweight cryptographic circuits; and (iii) to investigate and develop power clock generation and distribution, and silicon prototyping to evaluate energy dissipation and the DPA-resistance of ER-based crypto circuits.

Broader Impact

Outcomes and results from this project would make a strong case for industry adoption of ER computing for the design of low-energy and secure IoT devices.

New courses and workshops in hardware security for undergraduate and graduate students. Internships to Appalachian high-school students and historically underrepresented minorities, and first-generation students.

Advance the hardware security and cybersecurity education from high school to graduate-level students at the University of Kentucky and the state of Kentucky.