TARDIS

Time and Remanence Decay in SRAM

Amir Rahmati, Mastooreh Salajegheh, Daniel Holcomb,
Jacob Sorber, Wayne Burleson, **Kevin Fu**

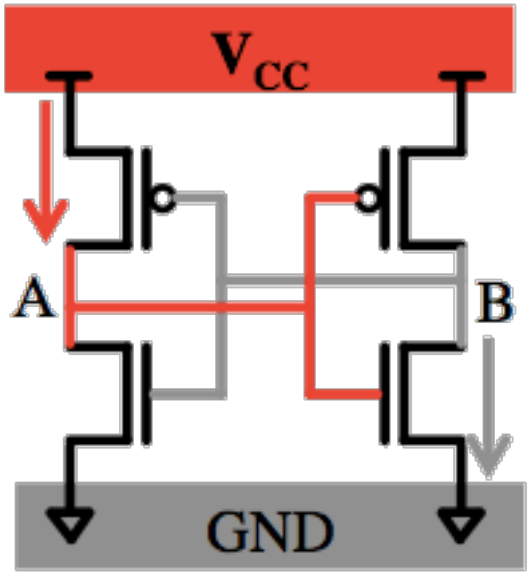
To appear at USENIX Security, August 2012

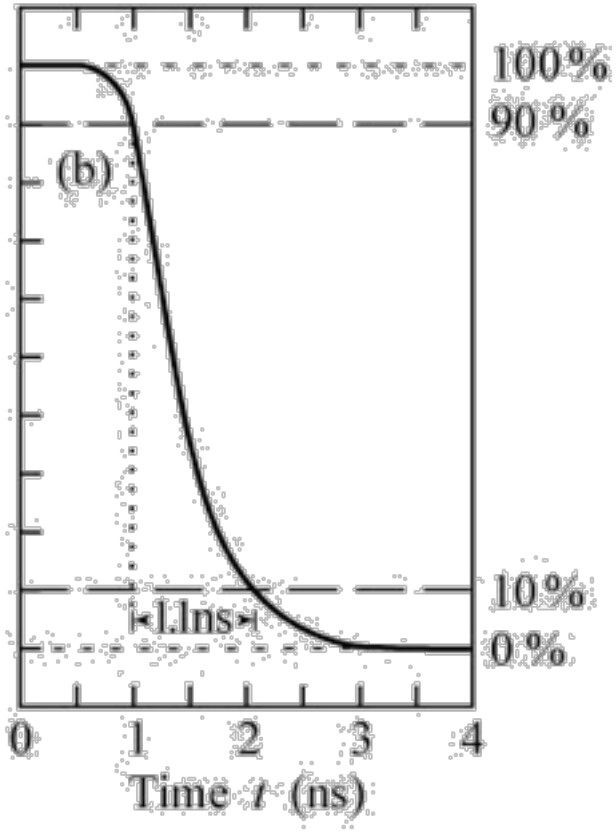
What is TARDIS?

A mechanism to estimate power loss duration based on decay in SRAM memory

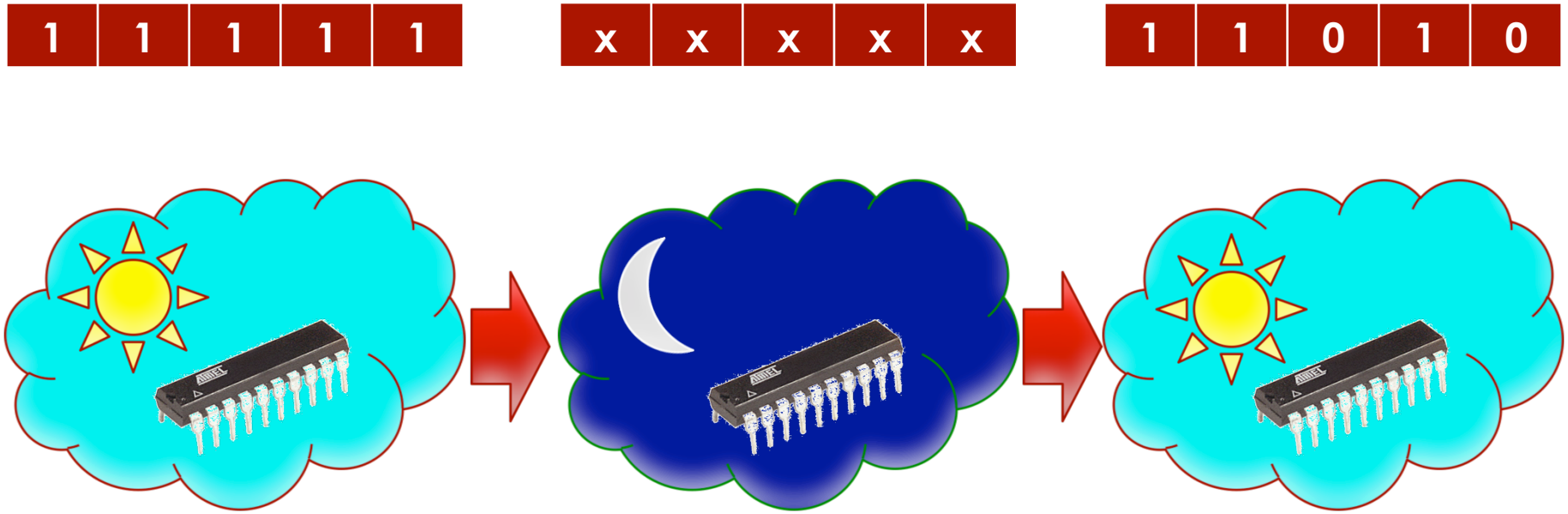
SRAM

- Volatile Memory
- Decay



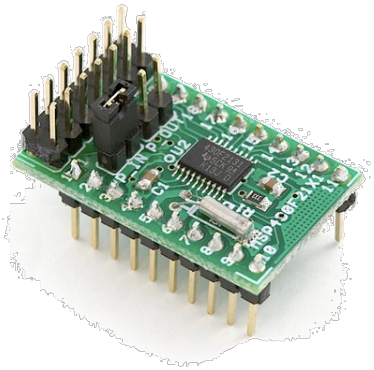


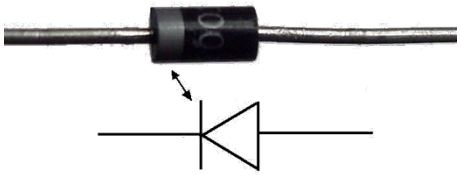
How TARDIS works



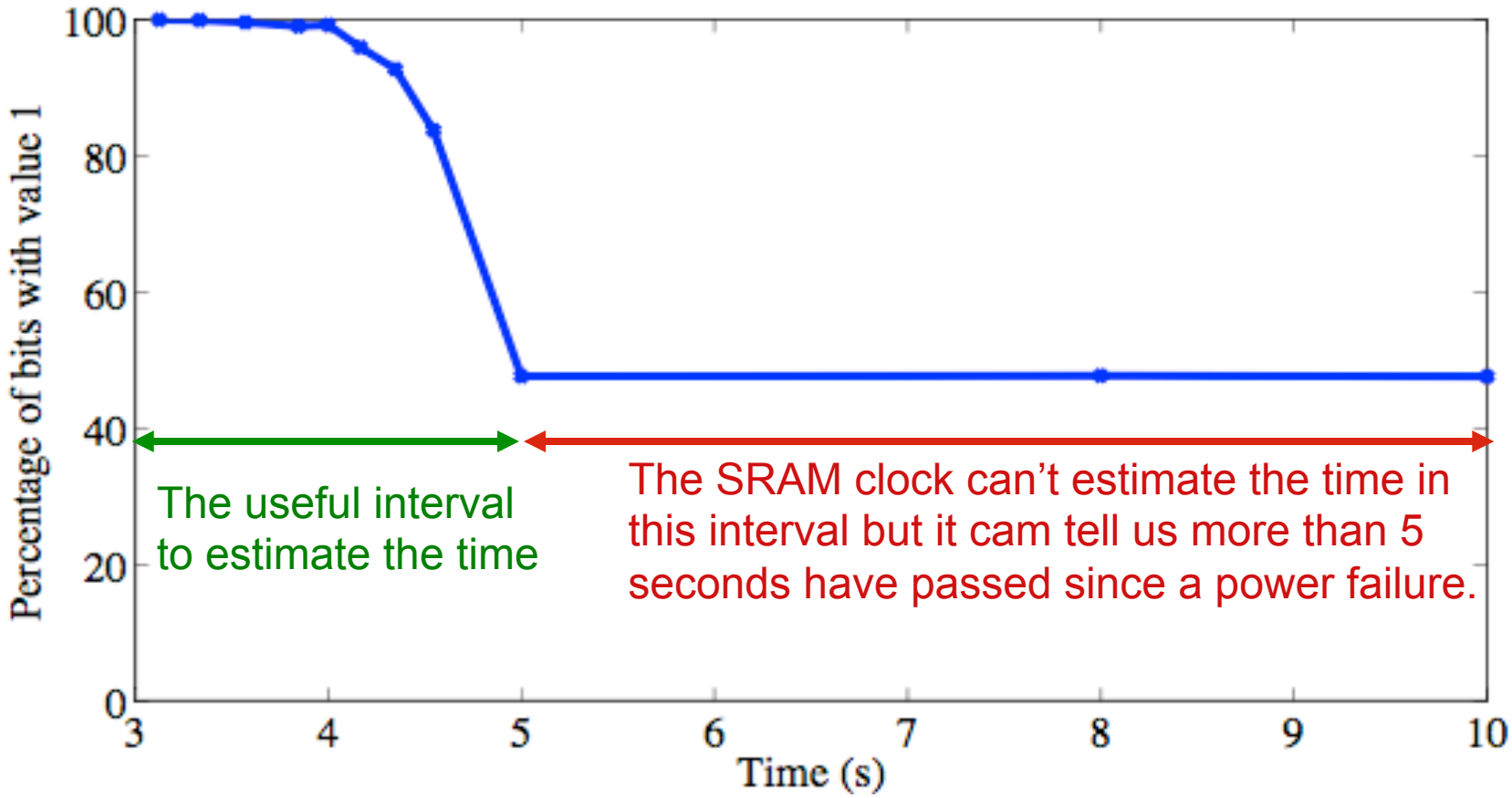
Experimental Setup

- TI MSP430F2131 – 256 Byte RAM
- Agilent DAQ
- Diode for graceful degradation





Experimental Results

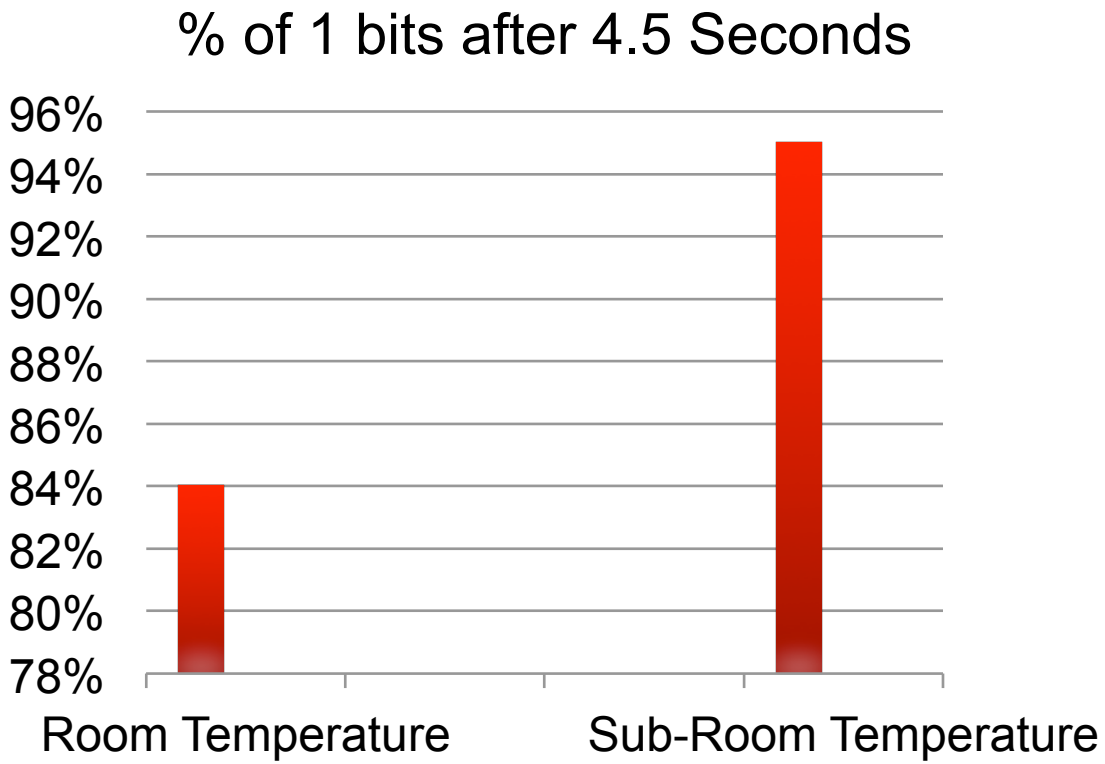


Limitations

- Sensitivity to Temperature
- Time Duration
- Precision

Temperature

- Decreasing temperature causes remanence time to increase



Time Duration

- Hardware Modification
  - Capacitor
  - Wider CMOS
  - Custom Hardware

Applications

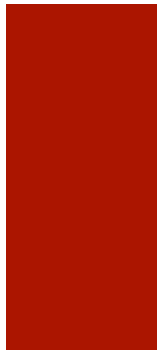
- Preventing Double Reads
- Preventing Some Types of Replay Attacks
- etokens: Refuse to provide service if not enough time has elapsed
- Time Lock
- Prevent Brute-Force Attacks
  - collision detection security hole on ISO18000-3 Standard
- TARDIS + MEMENTOS

Alternative Approaches

- Independently Powered Clock
  - Circuit Area Overhead
  - Needs Hardware Modifications
  - Needs Power Source
  - Can't be Implemented on Currently In-Use Devices

Future Work

- Use other Microcontrollers
- Add Capacitors
- Test under different temperatures
- Analyzing overhead(Time, Power, Space)
- Design custom TARDIS hardware



http://SPQR.cs.umass.edu/tardis/

Pros & Cons

Pros

+ No Hardware Modification for battrieless devices
+ Can be implemented on current in use devices

Cons

– Small duration