Embedded Crypto: SPECK

Lauren De Meyer, Candace Ross
Background on Speck

- **What is a block cipher?**

- **SPECK round function:**

  - Efficient:
    - Modular addition
    - Rotation
    - XOR
Folded Design

- Focus: small area!
- Folded:
  - 1 stage
  - 1 round function
- Key schedule in parallel
  - Better than storage
Design Exploration

We compared folded and unfolded designs
Results

- **Software Implementation (C)**
  - Throughput: 240 Mbps

- **Hardware Implementation**
  - Throughput: 400 Mbps

- **Clock frequency: 200MHz**
Setup of the DEMO