STARSS: Small: SecureDust -- The Physical Limits of Information Security

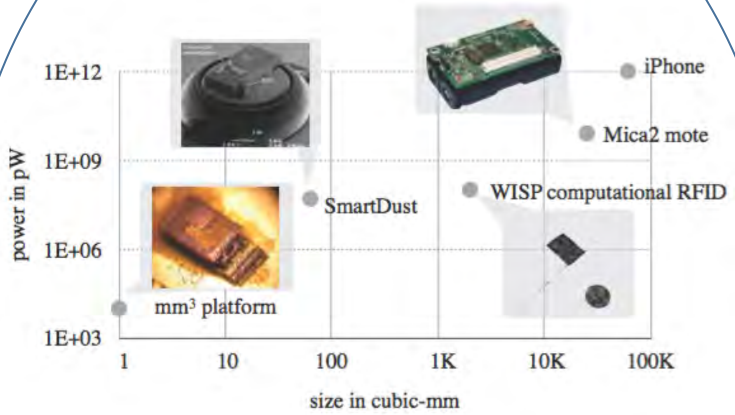
Challenge:

- Emerging chip-scale nodes bring new security challenges
- Lack of physical protection against fault injection
- Severe energy constraints limit countermeasures
- Target: resilient authenticated encryption at pJ/bit

Solution:

- Design to mitigate side channels leakages and fault injection attacks
- Efficient crypto implementations
- Securing sensors with PUFs
- Validate with future test chip

Award # 1619558
UMass Amherst
Dan Holcomb: holcomb@engin.umass.edu
Wayne Burleson: burleson@engin.umass.edu
Russell Tessier: tessier@engin.umass.edu



Emerging systems need new solutions: Ultra-lightweight devices accessible to attackers but extremely resource constrained

Scientific Impact:

- Understanding fundamental tradeoffs of security and power
- Understanding security implications of advanced VLSI process nodes

Broader Impact:

- Techniques for securing leading edge chip-scale nodes are applicable to variety of IoT and cyberphysical systems
- Improve understanding of VLSI statistics in advanced technologies
- Outreach to UMass SFS students and new security coursework