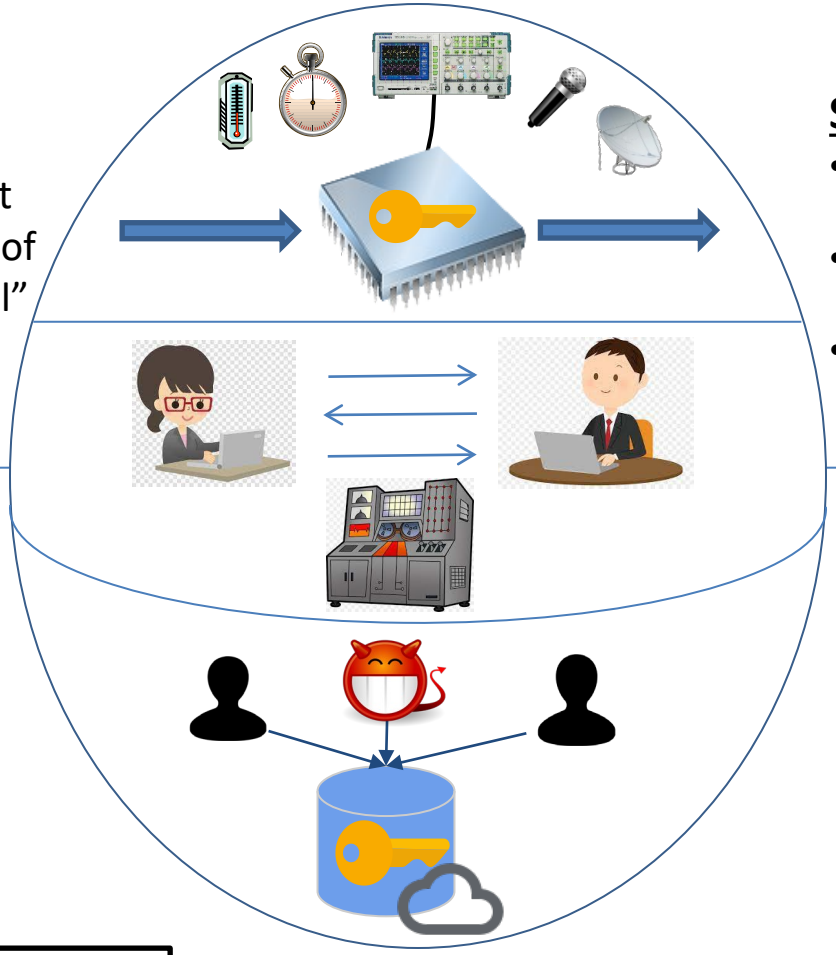
Making Crypto Too BIG To Break

Challenge:

- Making systems resilient to leakage / exfiltration of short amount of "critical" data (e.g., secret key).



Scientific Impact:

- Provably overwhelm the attacker with information
- Any poly-gap between honest users & attacker
- Novel settings for unconditional security

Solution:

- Big Key Cryptography
- Big Communication Cryptography
- Limited-Access Model (reusable + stateless)

Broader Impact and Broader Participation:

- Impact on technology
- Withstand powerful (state-run?) adversaries
- Significant mentoring & training opportunities

SaTC #2055578 (New York University)