Physical Unclonable Functions (PUFs) for Securing the Internet of Things (IoT)

Sandia National Laboratories

Jason Hamlet[1], Ryan Helinski[1], Rachel Dondero[2], Todd Bauer[3], Calvin Chan[1]
[1] Systems Security Research, [2] Embedded Systems Analysis, [3] MESA Microfab
Sandia National Laboratories, Albuquerque, New Mexico, USA

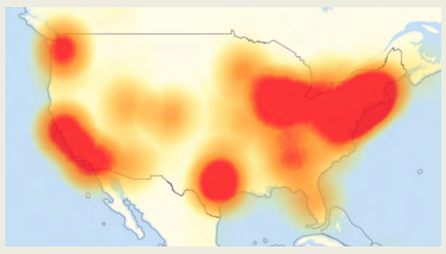
Internet-of-Things (IoT) Security

- Securing distributed networks like IoT requires verifying the authenticity of data and identities of devices.
- Authentication and attestation use cryptographic protocols that require unique, randomly generated, and closely guarded cryptographic keys for each device.

- Key generation and storage is problematic in IoT.
  1. Manufacturers can pre-program keys into memory
     - × Memory is space intensive and persistent
     - × Keys are often non-unique and reused
  2. Devices can computationally generate keys
     - × Insufficient behavioral entropy in devices to guarantee uniqueness of keys

Case Studies: Mirai Botnet & Linux TLS/SSH Keys

- Dictionary of 60+ commonly-used manufacturer default passwords (keys) and usernames (identities) to infect IoT devices (i.e., webcams, routers) with the *Mirai* malware. Botnet used to launch DDoS attack on DNS servers that "shutdown the internet".

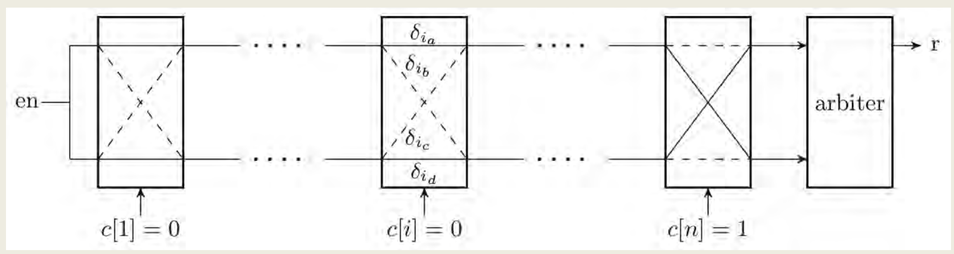


- Insufficient entropy during Linux boot-time RNG resulted in ~1% of TLS and SSH private keys being common.

Physical Unclonable Functions (PUFs)

- Semiconductor PUFs may facilitate IoT security by providing integrated, lightweight cryptographic primitives for authentication and attestation without significant changes to design or manufacturing.
- PUFs leverage inherent entropy in materials processing (e.g., dopant distribution, parasitic capacitance), which are observable as statistical variations in device behavior (e.g.,threshold voltage, switching speed).

Example: Arbiter PUFs



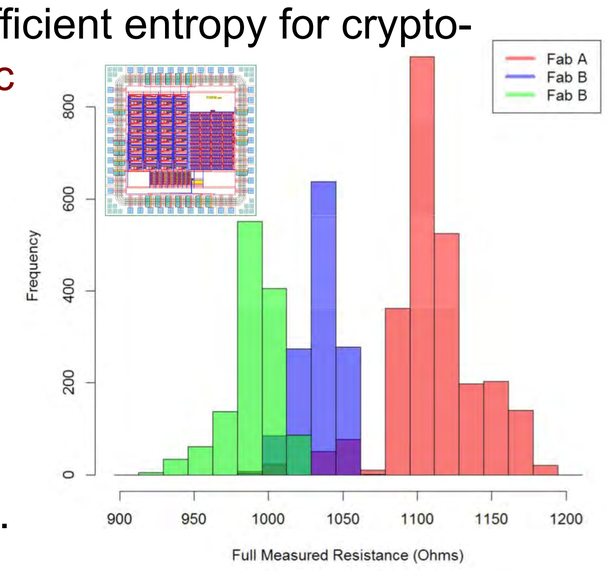
- Arbiter PUFs have multiple pairwise paths of nearly identical delays (δ_{ia} vs. δ_{id} or δ_{ib} vs. δ_{ic}). Differences in δ result from entropy in the materials. A "*strong PUF*" has an exponential number (2^n) of responses $\boldsymbol{r}$ for the challenge space $\boldsymbol{c}$.

PUFs in Practice

- PUFs can provide unique identities and keys for each physical object, which is desirable for systems like IoT, where many devices are manufactured and fielded.
- However, extreme care must be taken in designing PUFs so as to avoid pitfalls that may compromise security.
- Sandia has combined physics, materials science, electrical engineering, computer science, and cyber security to investigate the proper design of PUFs.

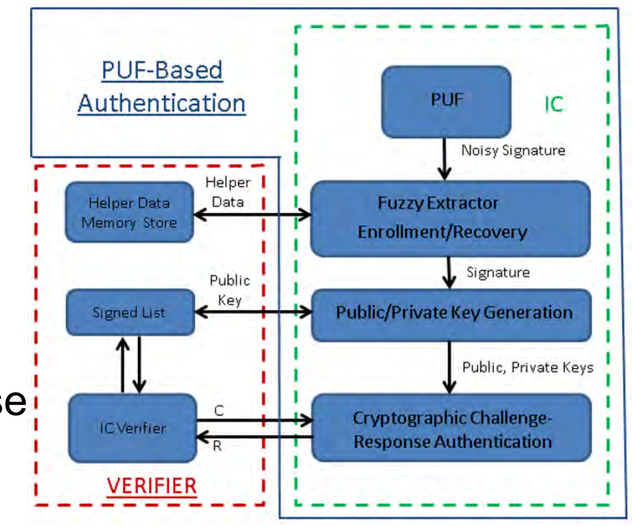
Study 1: Systematic vs. Random Variations

- PUFs must leverage random variations in materials and processes to guarantee sufficient entropy for crypto-graphic security. Systematic variations can lead to predictable biases.
- In 160 integrated circuits (3 lots, 2 foundries), systematic variations in resistance, capacitance, and ring oscillator frequencies were observed.



Study 2: Linear vs. Exponential Space

- "Strong PUFs" are desirable for their exponential challenge-response (*C*-*R*) space. However, strong PUFs may be vulnerable to modeling attacks if *R* is linearly dependent on *C*.
- Internal cryptographic components such as hashing or (a)symmetric crypto-functions can:
  1. Hide the raw *C*-*R* pairs
  2. Introduce non-linear functions to the response
  3. Further increase the *C*-*R* space



Summary

PUFs can provide unique identifiers and keys to help secure the massive number of devices found in IoT networks. Years of interdisciplinary study at Sandia has developed some general design principles to help keep PUFs secure.

U.S. DEPARTMENT OF ENERGY | National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.
This work was partially funded by Sandia National Laboratories' Laboratory Directed Research and Development program.
SAND No. SAND2017-4087 C