Hardware-Intrinsic Identity for IP Protection

John Ross Wallrabenstein

Sypris Research

Providing Trusted Solutions that
Secure our Customers' Interests Globally

SYPRIS®
TRUSTED SOLUTIONS

Sypris Electronics

TRUSTED SOURCE

Secure Site/ Personnel, Best Practices, Engineering Design & Technology Platforms

Dependable Execution, High Assurance, Mfct, & Secure Design Pedigree

TRUSTED "TACTICAL EDGE"

NSA Type 1 Communications, Key Distribution & Identity Management

40+ Year Leader in High Assurance Mobile Devices

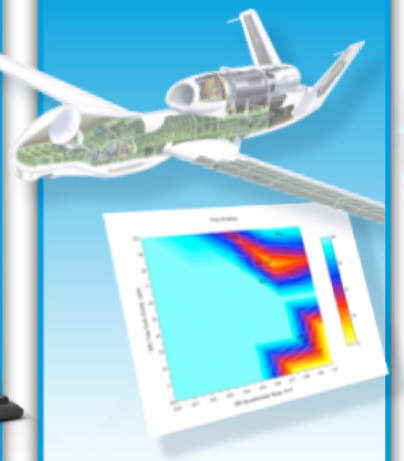
TRUSTED NETWORK & INFRASTRUCTURE

Agile Silicon Based Biometric Identity Management

Network/Enterprise Identity Authentication and Supply Chain Risk Management Architecture

TRUSTED PLATFORMS

High Assurance Control Systems



Integrates end point Identification, COMSEC design practices & pillars of "trusted" for critical Platforms/Applications

TRUSTED CYBER ANALYTICS

Tactical Cyber Range

Modeling, Simulation, Training & Test Bed Platform

PURDUE UNIVERSITY

Research Agenda for PLM Security

Critical requirements:

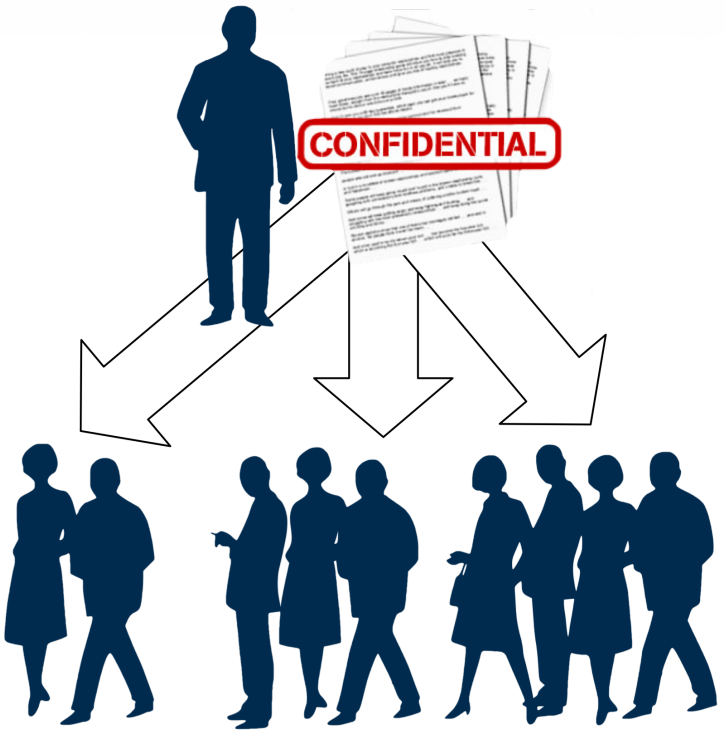
- Protection from Insider Threat
- Compliance with Export Regulations
- Secure Supply Chain
- Secure Remote 3D Printing
- Security for Industrial Control Systems
- Secure Collaboration Techniques
- Security Techniques for Networks-of-Things (NoT)

Research directions:

- Anomaly Detection Systems and Advanced Access Control Systems
- Security Techniques for Embedded Systems, and Firmware
- Security for Industrial Cyber-Physical Systems and Industrial Processes
- Secure Collaboration Platforms
- Tools for Compliance Support

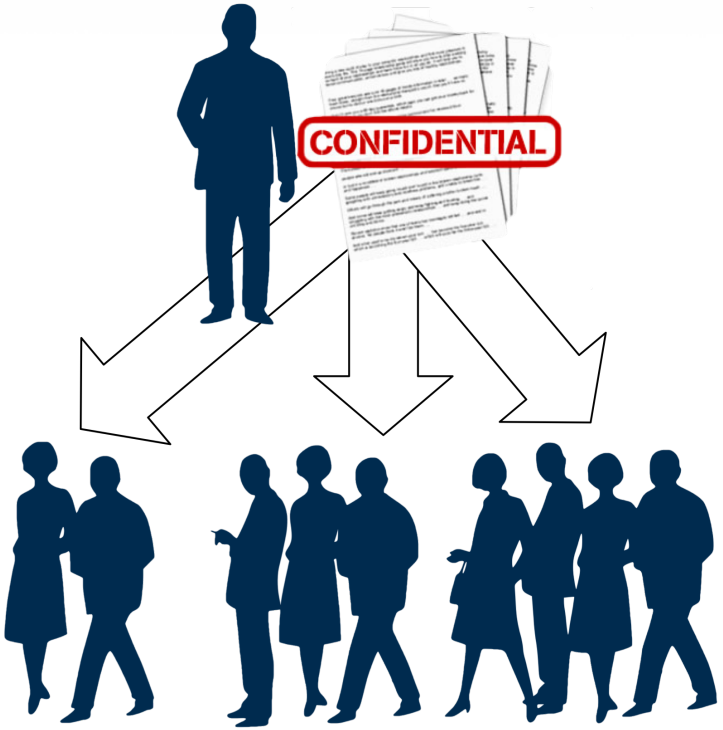
Digital Supply Chain Security

- How is digital information shared securely?



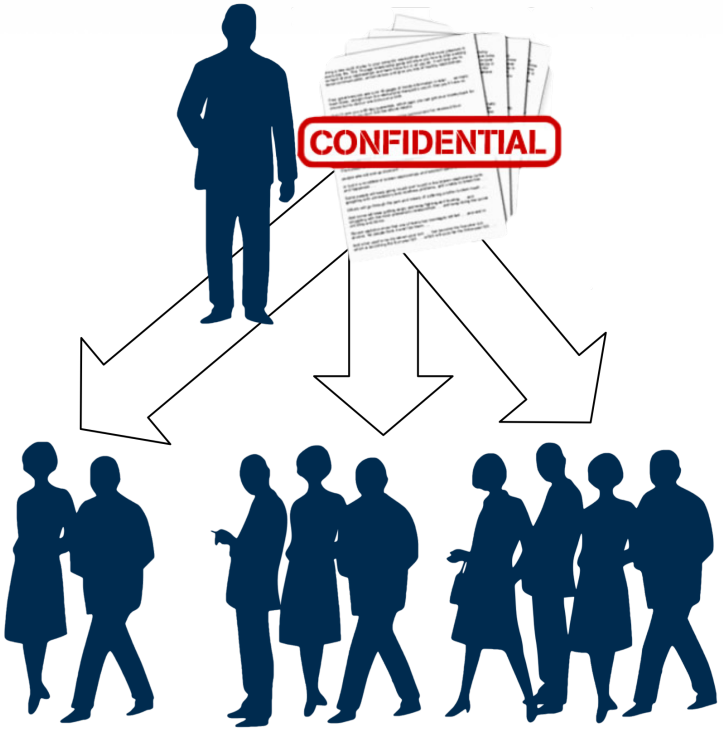
Digital Supply Chain Security

- How is digital information shared securely?
  - Cryptography



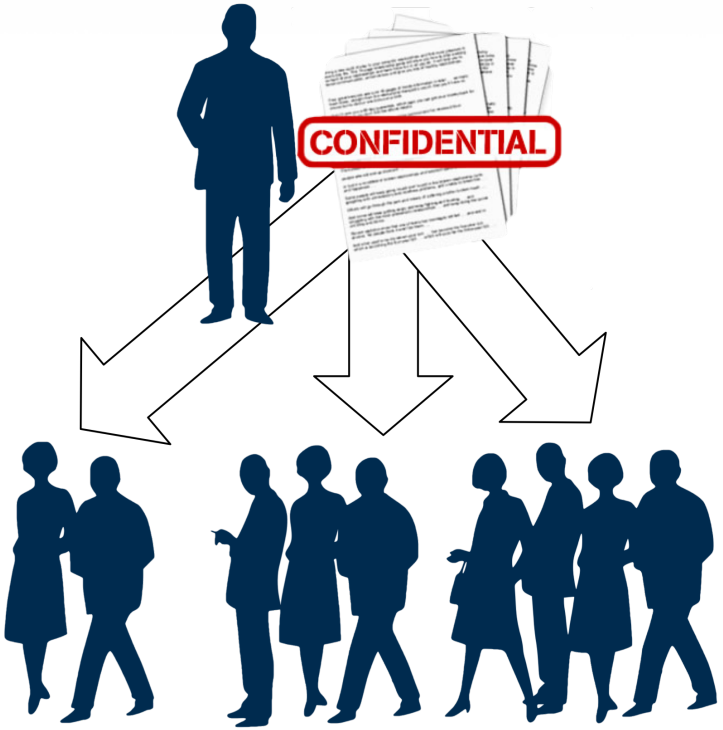
Digital Supply Chain Security

- How is digital information shared securely?
  - Cryptography
- What prevents an adversary from intercepting the information?



Digital Supply Chain Security

- How is digital information shared securely?
  - Cryptography
- What prevents an adversary from intercepting the information?
  - Assumption: Adversary cannot obtain private key of recipient



Identity: Traditional Cryptographic Systems

Symmetric Cryptography

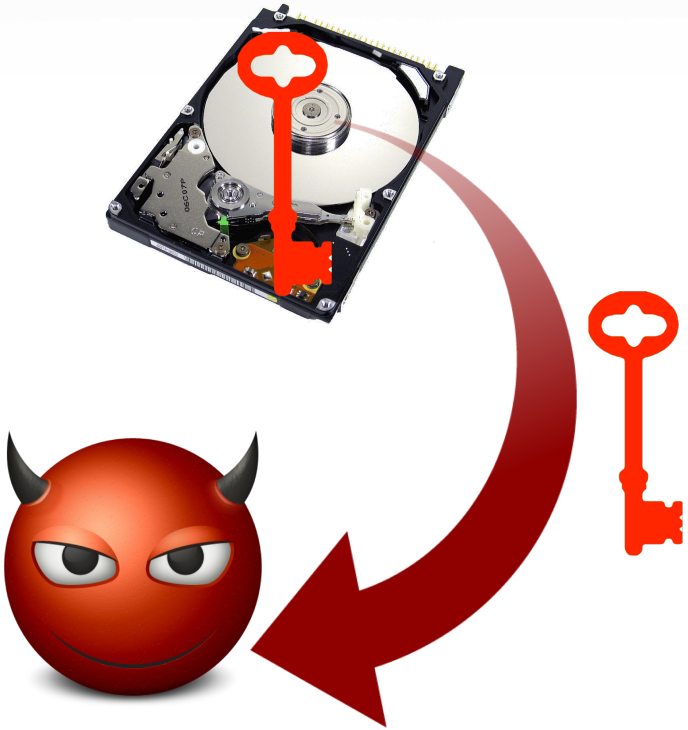
- Symmetric Private Key **Stored** on Drive

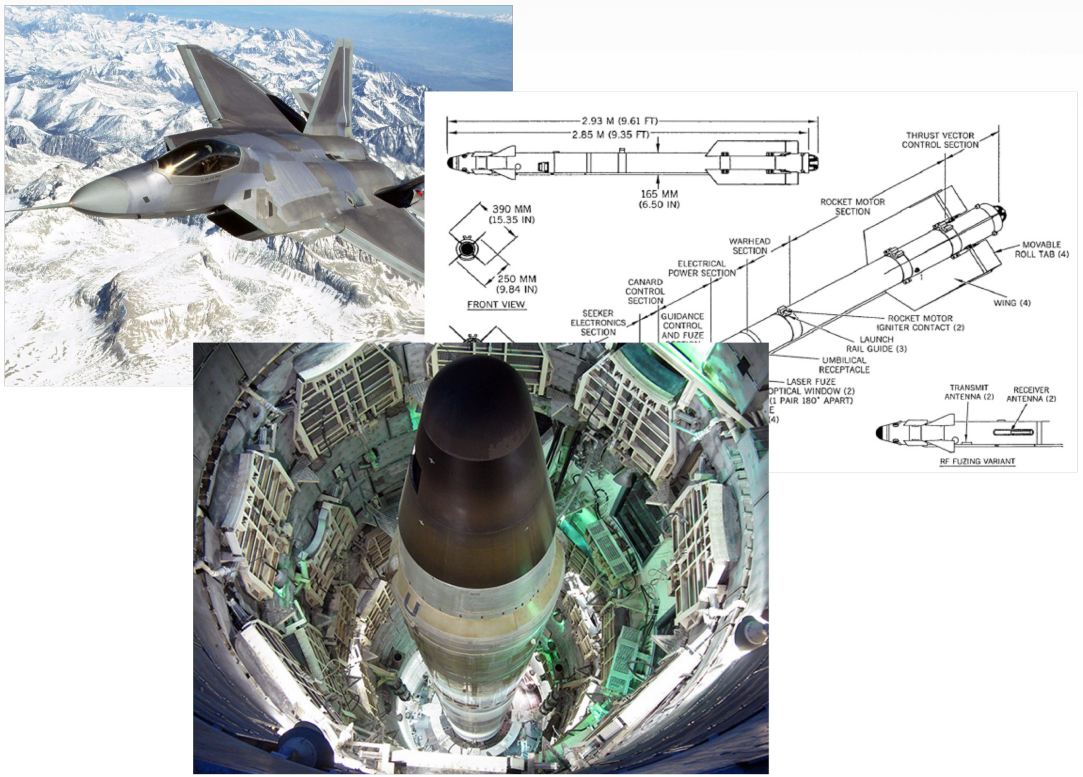
Identity: Traditional Cryptographic Systems

Symmetric Cryptography	Asymmetric Cryptography
	
	

- Asymmetric Private Key **Stored** on Drive

Powerful Adversaries





Identity: Traditional Approach Limitations

Symmetric Cryptography	Asymmetric Cryptography	Limitations
Generated Identity 		Transfer Identity Store Private Data Manage Private Keys No Tamper Protection Remote Compromise Device & Identity Independent
		

- Identity is **Stored**

Secure Hardware Solutions

- Secure Hardware
  - Rugged Enclosure
  - Tamper Resistance
  - Epoxy Coating
  - Battery Hold-Up
- Limitations
  - Size & Weight
  - $$$

PUF-Based Identity Management

Symmetric Cryptography	Asymmetric Cryptography	PUF-Based Technology
Generated Identity 		**Intrinsic** Identity 
		

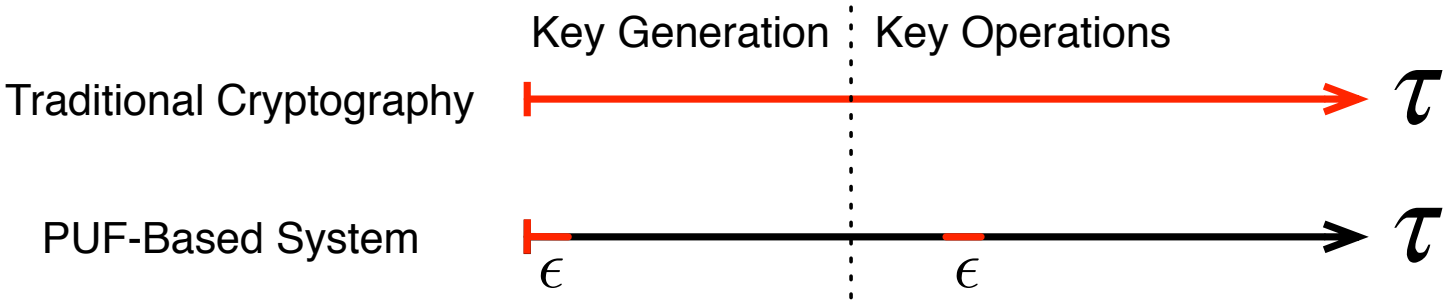
- Identity is **Dynamically Regenerated** As Needed

Physical Unclonable Functions

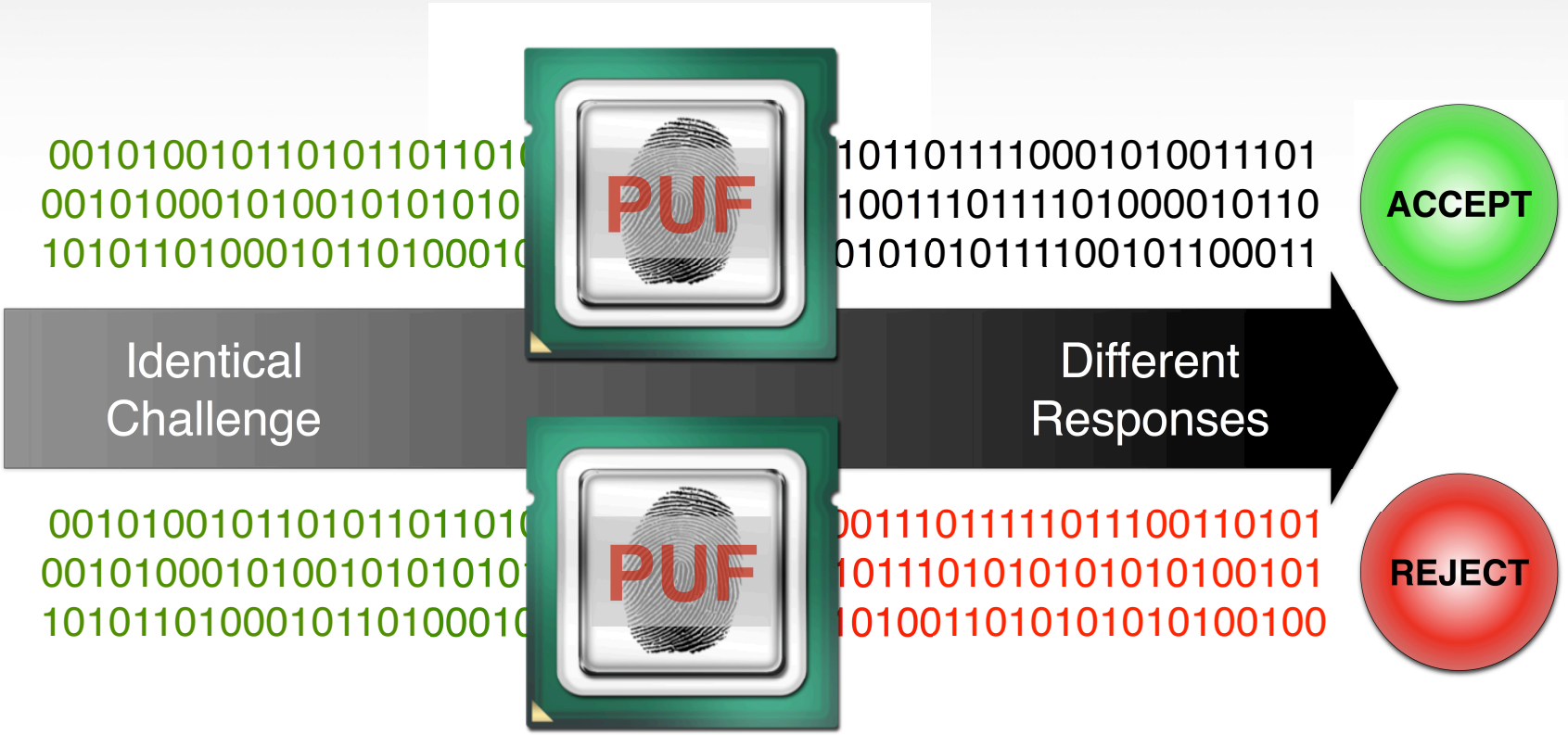
- A PUF is input a *challenge*, and outputs a *response*
- Mapping based on unique physical characteristics of device
- PUFs on different devices will return different responses for the same challenge

Core PUF Features

- **Identity Management:**
  Extract identity *intrinsically linked* to hardware
- **Tamper Detection:**
  Detect *hardware tampering* after trusted enrollment
- **Key Management:**
  Private key *regenerated* as needed, rather than stored

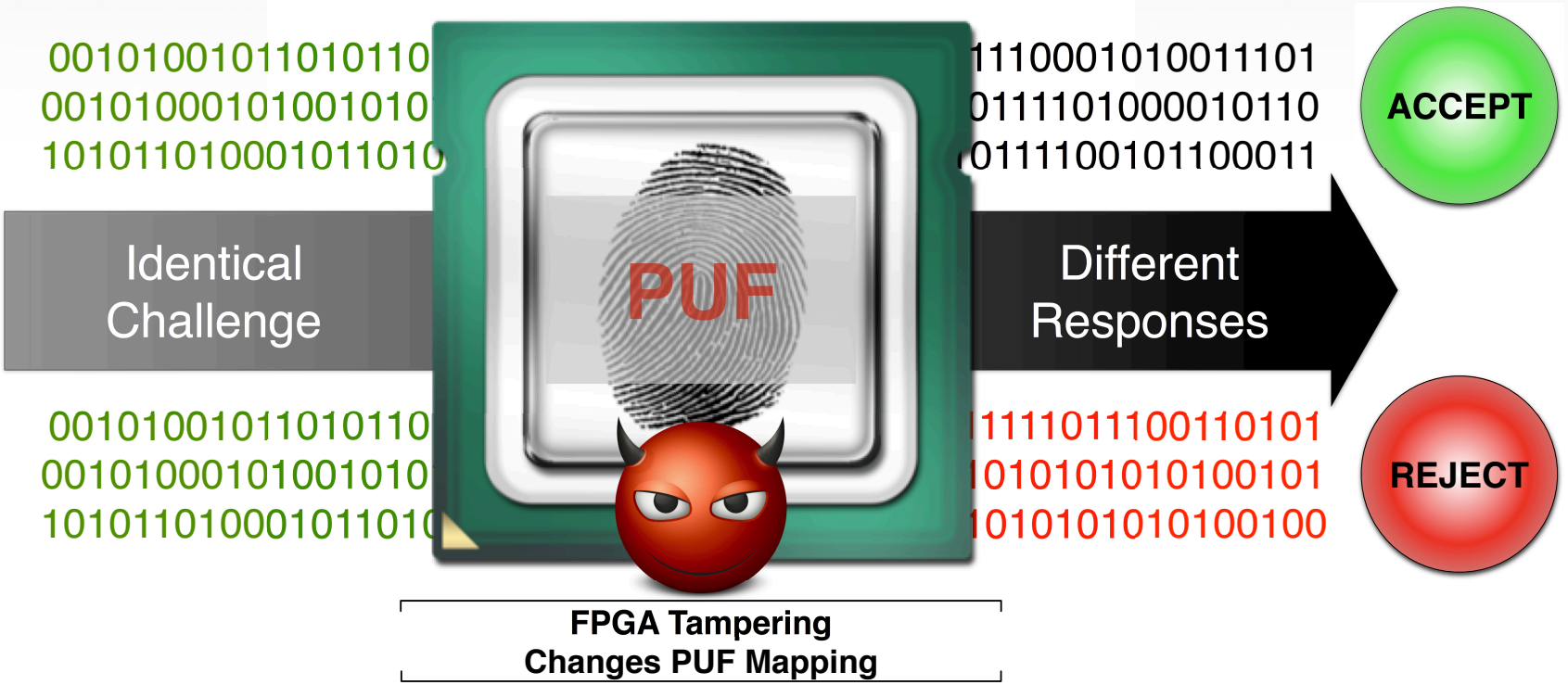


Identity



Core Concept: Identically manufactured devices have different hardware identities

Tamper Detection



Core Concept: Hardware tampering fundamentally changes hardware identity

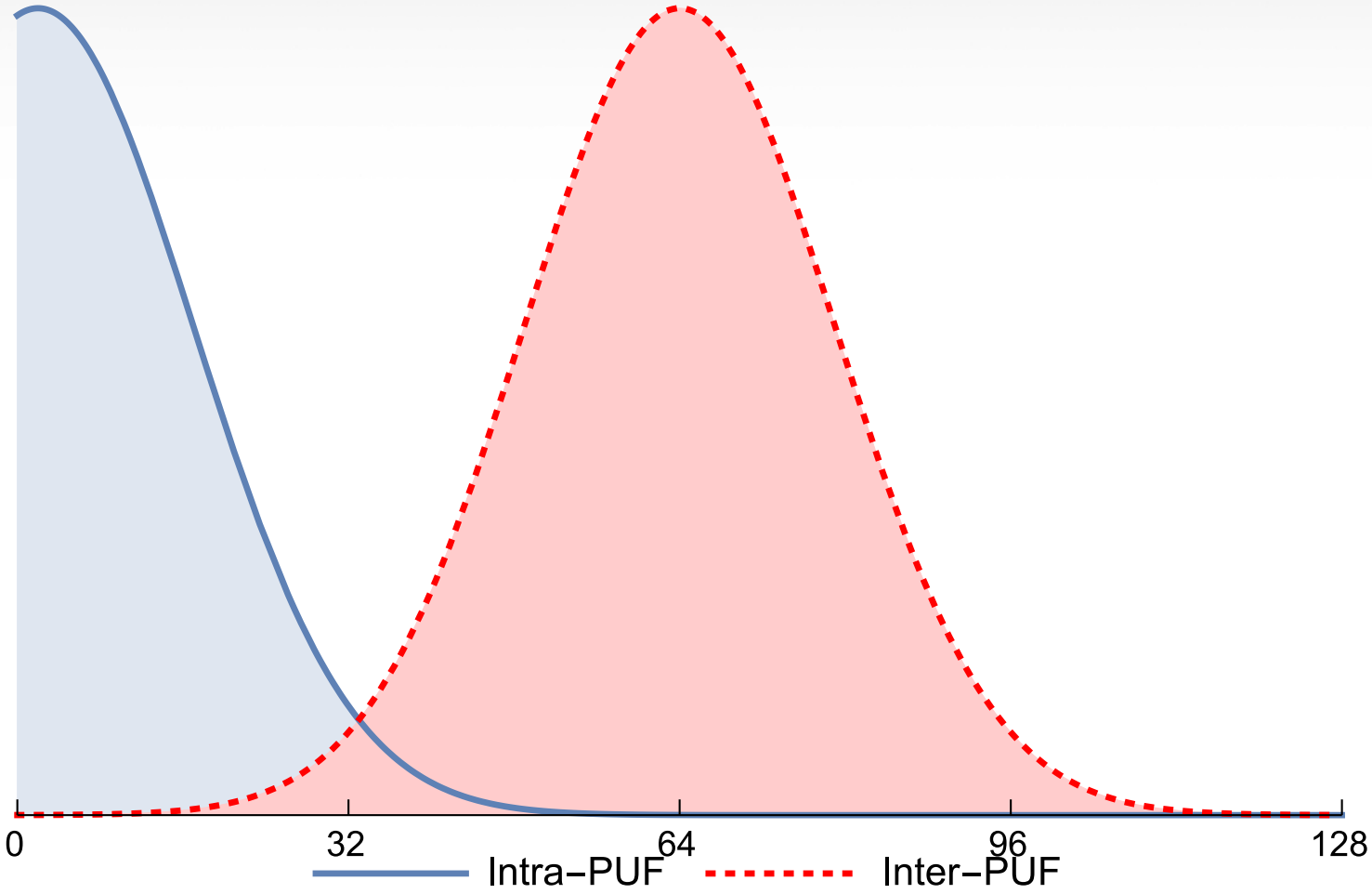
Key Properties

- **Resilience to Compromise:** *No* secret information is stored at *either* the device or server:
  - A device does not have any sensitive information stored in nonvolatile memory: the private key is dynamically regenerated as needed.
  - A server only stores the public keys of the devices.
- **Resilience to Tampering:**
  - Tampering (e.g., probing, modification) alters the unique characteristics of the hardware
  - Prevents the PUF from extracting the original identity of the device

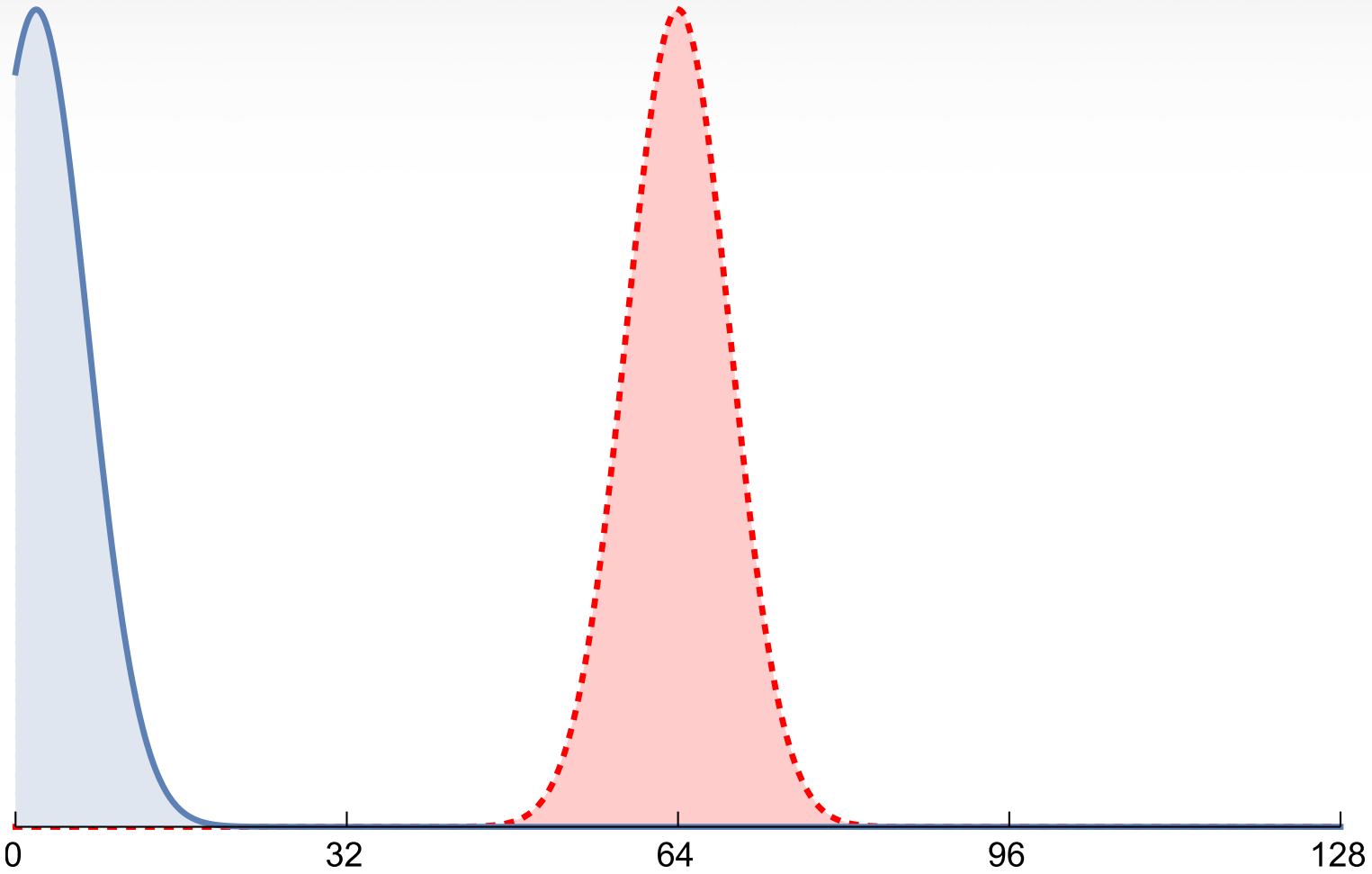
Deploying PUFs in Practice

- PUFs (like human biometrics) have noisy output
  - What if error correction "corrects" a different device's response?
  - What is the false positive and false negative rate?
- PUFs rely on slight manufacturing variations
  - How will fluctuations in temperature/voltage/etc. affect the response?

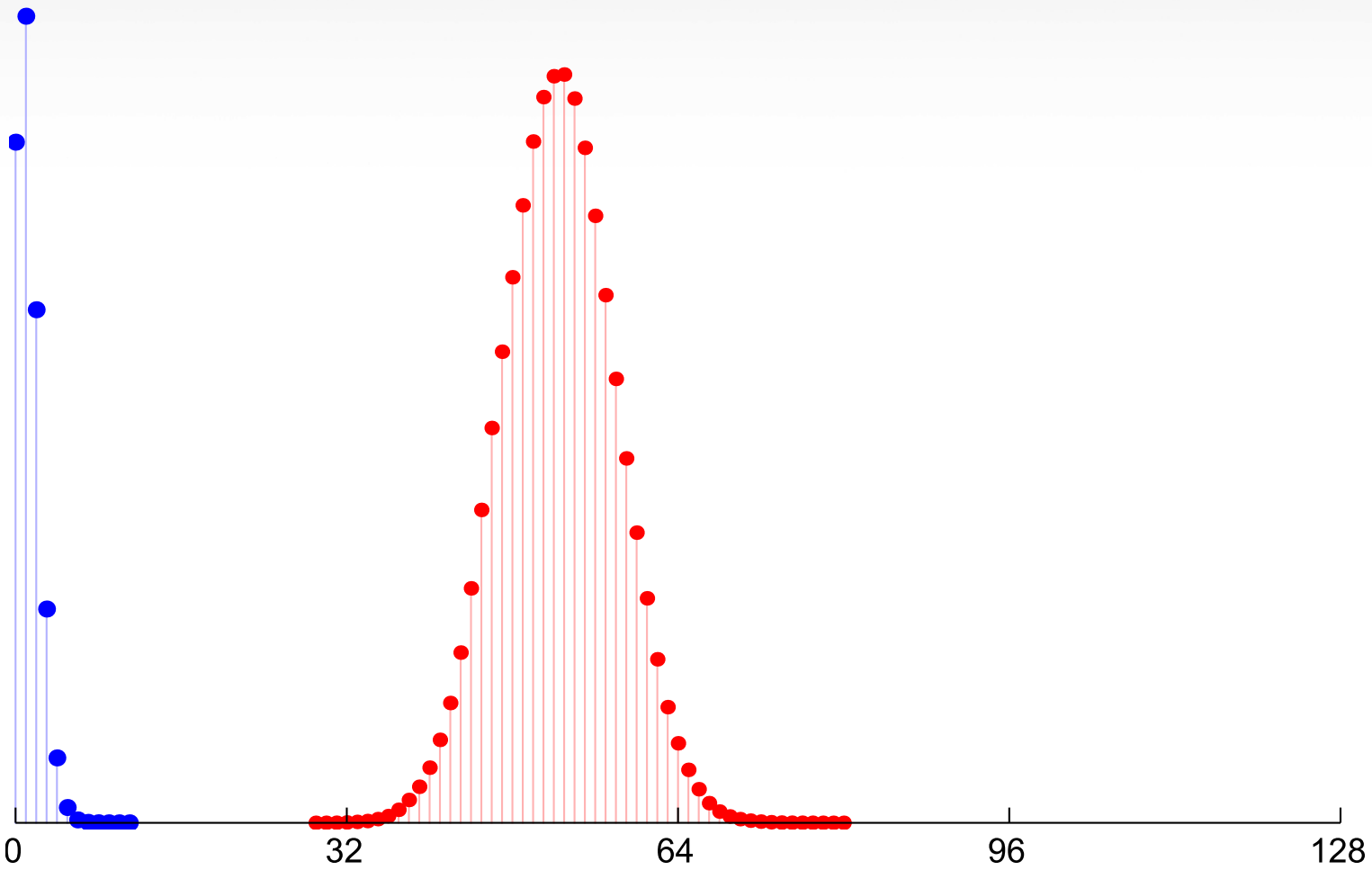
Overlapping Distributions



Separate Distributions



Experimentally Observed Distributions



Deploying PUFs in Practice

- PUFs have noisy output
  - What if error correction "corrects" a different device's response?
    - Experimental results suggest this occurs with only negligible probability
  - What is the false positive and false negative rate?
    - 0% in practice
    - Likely only under rapid and substantial variation
- PUFs rely on slight manufacturing variations
  - How will fluctuations in temperature/voltage/etc. affect the response?
    - Xilinx board placed in a temperature chamber
    - Varied from $0 - 60\,^{\circ}\mathrm{C}$
    - PUF output shift of $\approx 5 - 10$ bits

PUF-Based Benefits for PLM Solutions

- **Hardware-Intrinsic Identity:**
  Guarantee recipient has a specific piece of hardware
- **Tamper Detection:**
  Guarantee no adversarial tampering with recipient hardware
- **Key Management:**
  Guarantee an adversary cannot extract private key from recipient hardware

Discussion

Questions