High-Security, Clone-proof RFID with Secure Distance Bounding

Eugene P. Gerety, Advisor: Prof. Khaled M. Elleithy
Department of Computer Science and Engineering, University of Bridgeport, CT.

Abstract

This poster describes a system that provides a highly-secure RFID-based mechanism for controlling access to high-value assets. The system employs a unique combination and coordination of technologies, preferably on a single chip, to render it immune to relay attacks, probing, modeling, cloning and snooping.

Introduction

Wireless access-control devices have become ubiquitous. Examples are:

- **Vehicle Security Systems** (keyless entry/remote-start key fob)
- **Physical Access Control** (*e.g.*, employee ID cards for building access)
- **Travel and Public Safety** (RFID travel cards, passports, driver's licenses)
- PoS (Point-of-Sale) transactions (payment via NFC-enabled mobile phone or card)

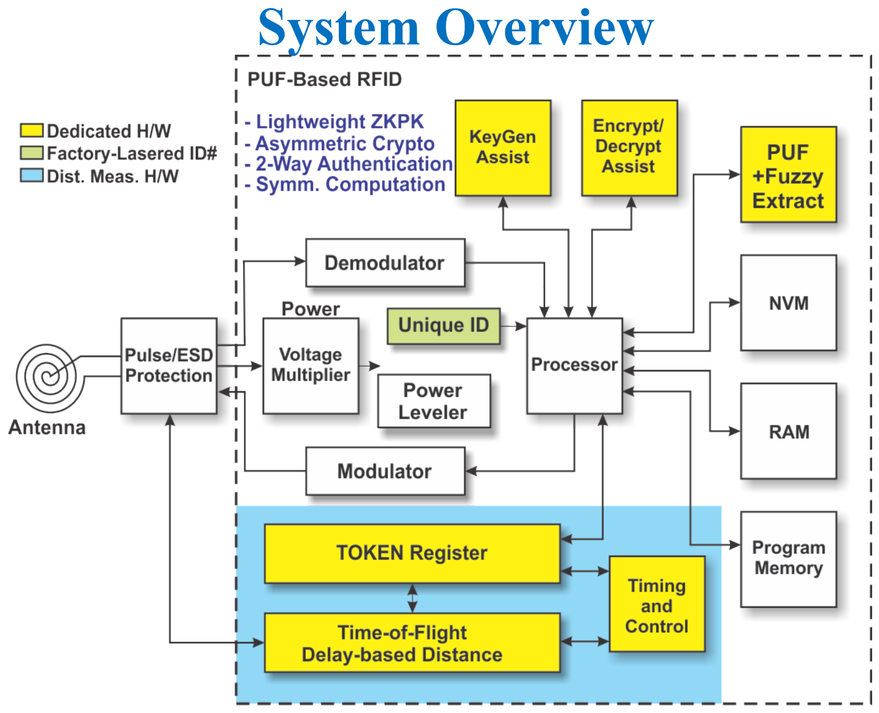
Of particular interest are **applications** concerning the **protection and control of**:

- **Assets of high financial value** (theft of: vehicles, jewelry, currency)
- **Assets of high strategic value** (business documents & plans, gov't. & military access control, access to critical computer systems)
- Assets of **great historical value** (artifacts, art, rare documents)
- **Public and Personal Safety** (access to: buildings, personal vehicles, planes, trains, buses; police and corrections, border control)

The Threat:

- **High value assets →highly motivated attackers** and **sophisticated attacks**
- **Highly publicized RFID security breaches:**
  - ✓ University researchers crack popular KeeLoq® vehicle security system
  - ✓ Simple relay attack successfully demonstrated against popular passive keyless entry system used by multiple automobile manufacturers

System Overview

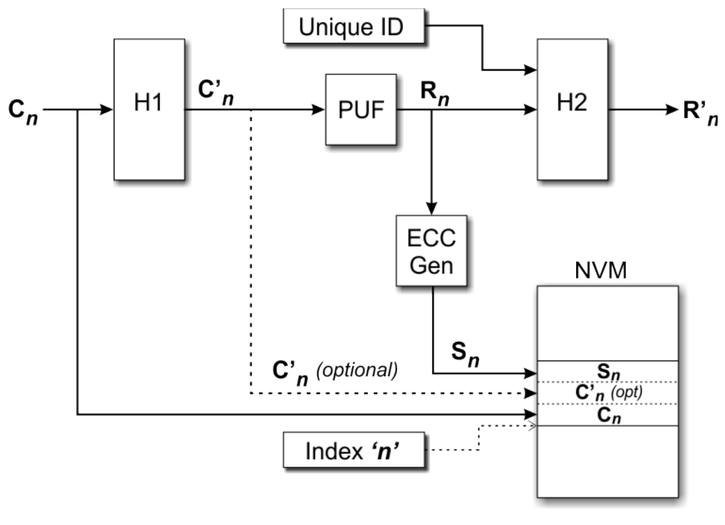


In addition to "basic" digital RF communication capability, some of the major features and functions of the system are:

- **PUF** (Physical Unclonable Function). Exploits molecular-level differences between "identical" integrated circuits to create an "uncopyable" function unique to a single IC chip. Even the manufacturer cannot produce a "duplicate"
- **"Fuzzy" Extractor.** PUFs are inherently noisy. Fault-tolerant "fuzzy" extractors "stabilize" the PUF responses
- **Hardware "Obfuscation" Layer.** On-chip hardware "shield" features protect PUF and other critical circuits from most forms of scanning and probing. Any attempt to probe or penetrate the shield destroys the PUF by altering its responses
- **Zero-Knowledge-Proof-of-Knowledge** (ZKPK) protocol strategy hides PUF and other critical information behind secure hashes and encryption, ensuring low information "leakage" using low-complexity hardware/algorithm
- **Time-of-flight (TOF) distance bounding.** Impulse radio scheme determines distance via a secure distance bounding protocol using a series of encoded rapid-fire, single-pulse 'ping-pong' exchanges
- **Asymmetric Encryption.** Eliminates "shared secret" vulnerabilities
- **Power-leveling.** Constant current mechanism "flattens out" the power profile to prevent Differential Power Analysis (DPA – a form of 'side-channel' attack)
- **Symmetric hardware/firmware mechanisms.** Careful system design to minimize data-dependent timing, power consumption and RF emission "signatures" variations. Frustrates many forms of side-channel attack

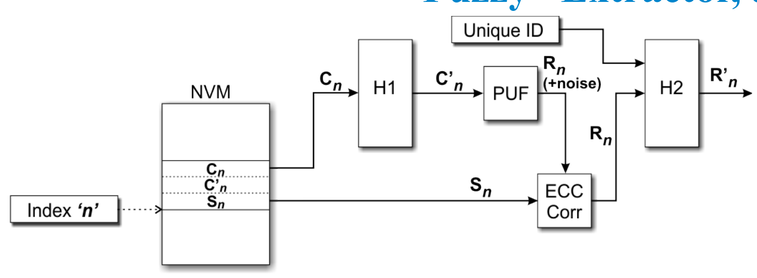
"Fuzzy" Extractor

"Fuzzy extractor" stabilizes PUF by providing stable output from "noisy" PUF responses. Any PUF response "close" to the 'correct' response (in the Hamming distance sense) will provide the correct response value. *(Examples using ECC auxiliary data (e.g., Reed-Solomon or BCH):*

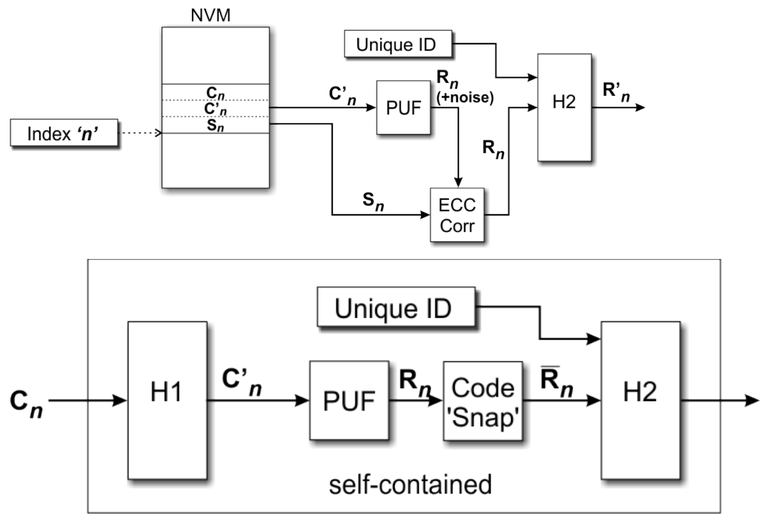


Response Generator

"Fuzzy" Extractor, *cont'd.*



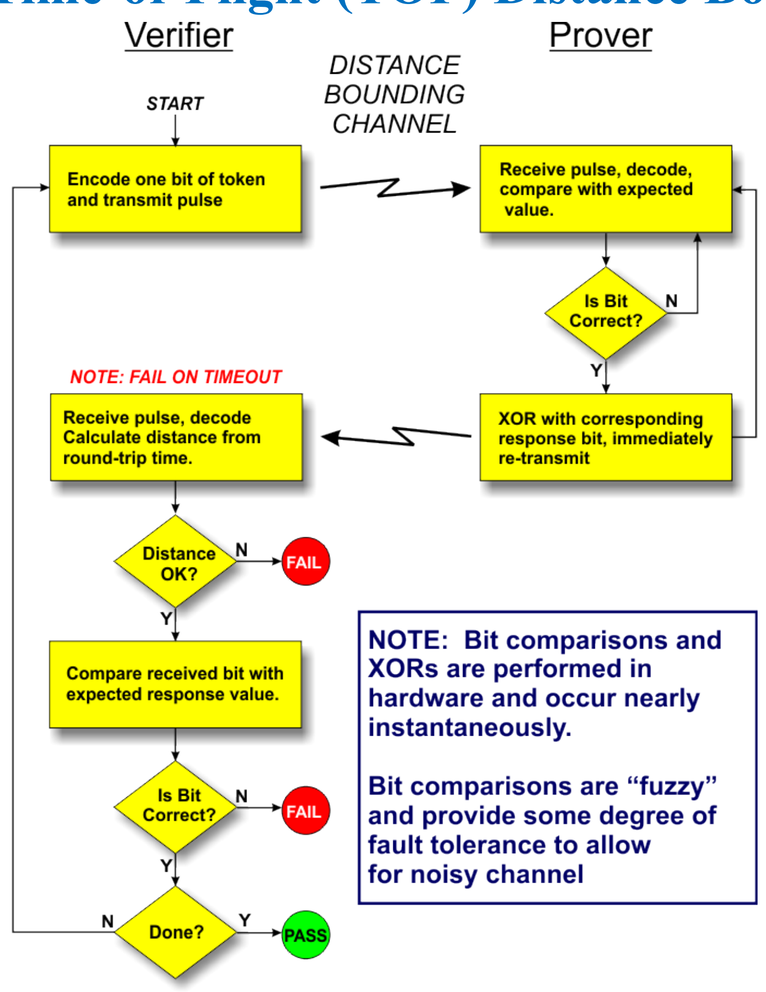
Response Checker



Alt. Response Checker

Standalone Version using Code "Snap"

Secure Time-of-Flight (TOF) Distance Bounding



TOF Channel Characteristics:

- ✓ Narrow pulse transmissions (e.g., impulse radio)
- ✓ Message transmitted as a series of quick single-bit transactions
- ✓ Short-highly predictable processing time
- ✓ Unpredictable messages
- ✓ Non-repeating protocol
- ✓ Bidirectional, end-to-end security

Multiple units can be embedded in fixed positions (i.e., buried in a building's structure) and used in coordination to permit verification of exact location (min. 4 units required to fix position in 3-space)

Resistance to Attacks

This system is highly immune to the following forms of attack:

- ✓ **Relay**: Distance limits (using TOF distance bounding) cause relay attack to fail distance test
- ✓ **Probing/Cloning**: If PUF is even microscopically altered, its responses change, effectively destroying it. Hardware obfuscation further enhances protection
- ✓ **Scanning:** Hardware obfuscation greatly complicates attempts at scanning.
- ✓ **Modeling**: PUF hiding behind ZKPK and secure hashes prevent this
- ✓ **Snooping**: Low-information-leakage ZKPK techniques and encryption severely restrict information available to snoopers.

Conclusions

The **High-Security RFID** system described above provides a highly secure platform for protecting high-value assets, and has numerous potential areas of application. The system can be used to secure a physical system against removal from its intended point of operation by confirming its location via the distance bounding mechanism. The same mechanism can be used to improve vehicle keyless entry security by ensuring that the key is within a predetermined distance of the vehicle before allowing it to be opened or driven (eliminates relay attacks).

Future Work

Further research efforts will be directed towards the development of lightweight implementations of the hardware mechanisms and refinement of the messaging protocols.