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

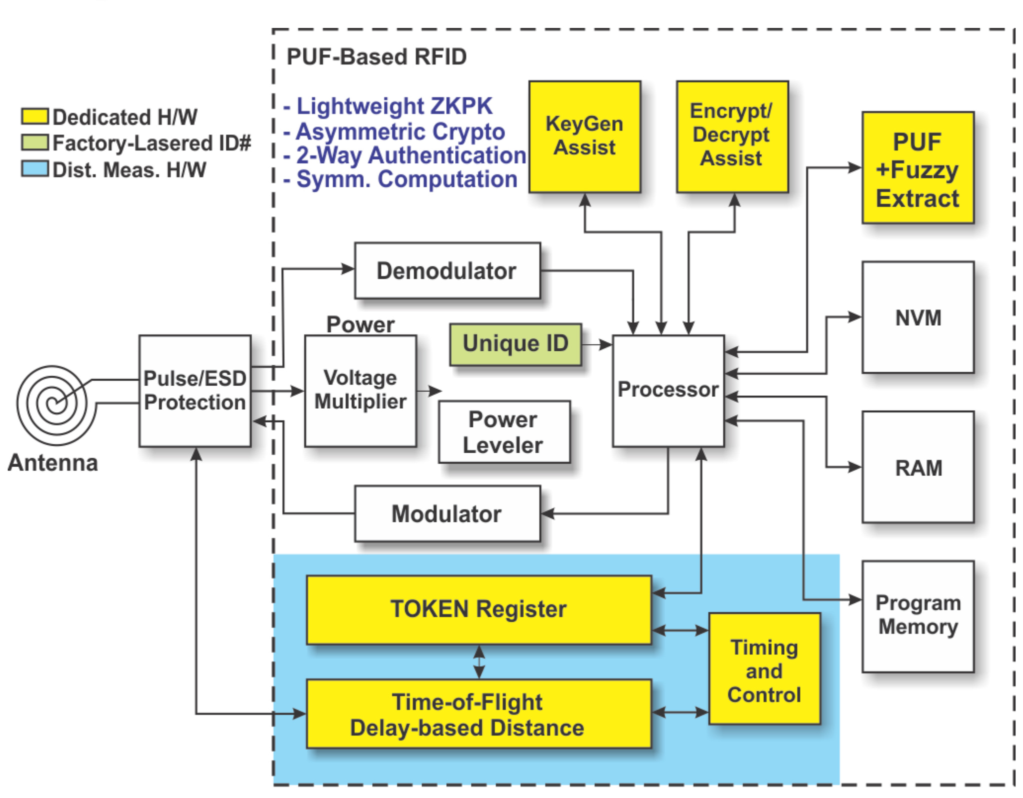
Eugene P. Gerety, Khaled Elleithy
Department of Computer Science and Engineering
University of Bridgeport, Bridgeport, CT

Abstract

Wireless near-field (NFC) and short-range RFID "security" devices are ubiquitous, commonly found in vehicle security (keyless-entry, remote-start), access control (employee key cards), travel cards, point-of-sale (PoS) transactions via NFC-enabled mobile phone or credit card, among others. Whenever assets of high-value are at stake, adversaries will stop at nothing to gain access to those assets, so it should be assumed that security systems will be subjected to many forms of attack. There have already been several highly publicized successful breaches of keyless entry systems, including relay and key-cloning attacks.

This poster describes a a highly-secure, distance-bounding, clone-proof RFID mechanism for protecting high-value assets. The system employs a unique combination of technologies to make it highly-resistant to relay attacks, probing, modeling, cloning and snooping.

System Overview



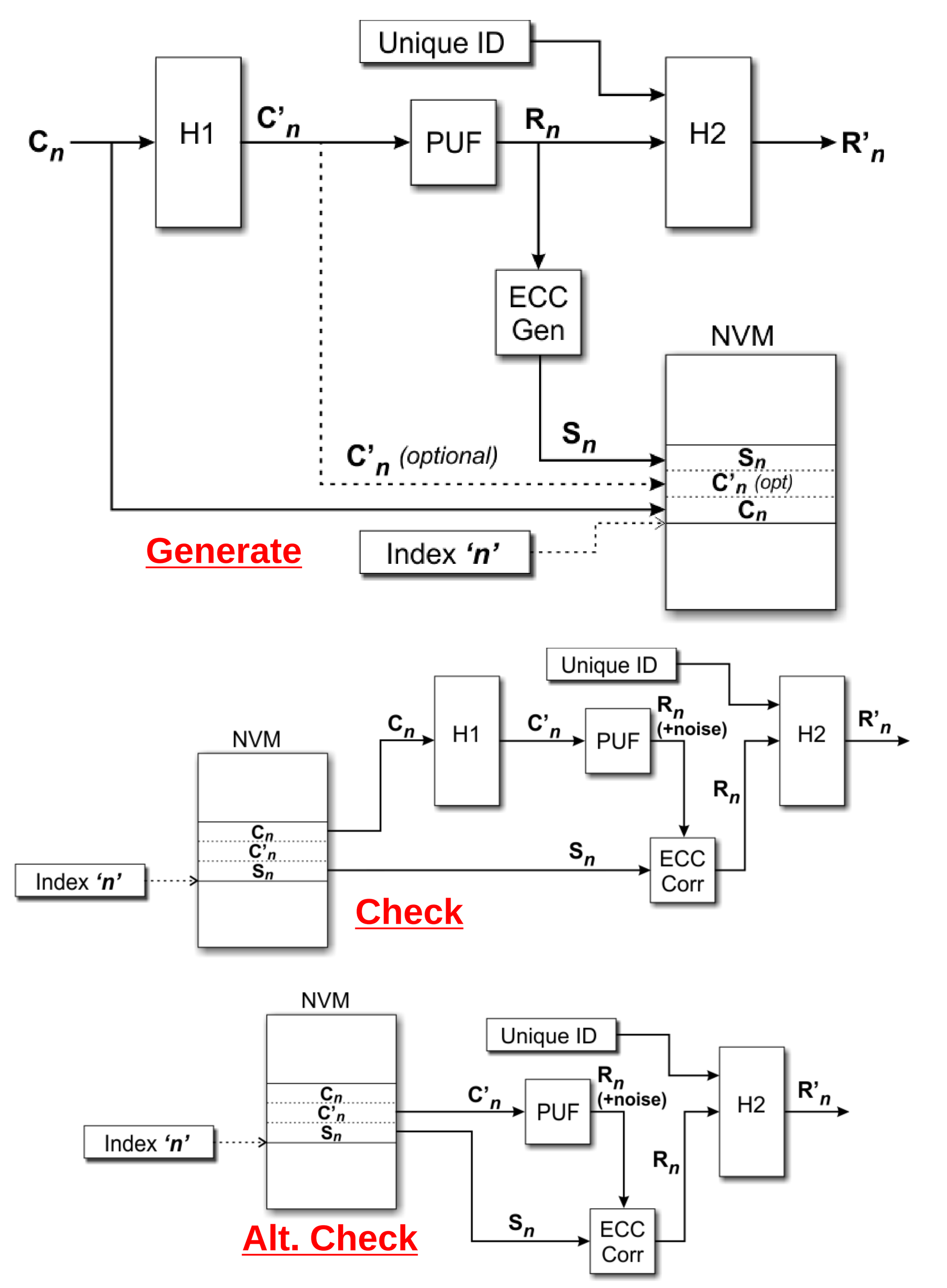
Major Hardware/Firmware Features:

- **PUF+Fuzzy Extractor**. Stabilizes "noisy" PUF response
- **Lightweight ZKPK** (Zero Knowledge Proof of Knowledge) protocol limits information "leakage"
- **Secure TOF Distance Bounding**. Time-of-Flight distance measurement using secure ZKPK protocol. Token derived from PUF.
- **Asymmetric Encryption**. Eliminates "shared secret" vulnerabilities
- **Power-leveling** mitigates any data-dependent power-consumption
- **Symmetric design** to minimize any data dependent timing or switching "signatures"

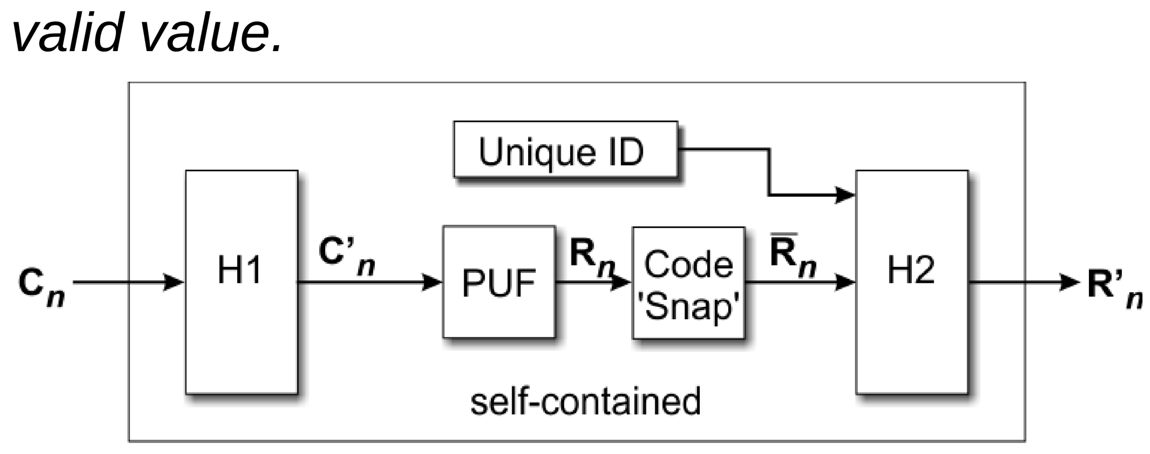
Physical Unclonable Function

PUF hidden behind secure hash functions and ZKPK protocol to minimize data leakage.

"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):*



Standalone version requiring no auxiliary data, using code-distance "snap" to nearest valid value.

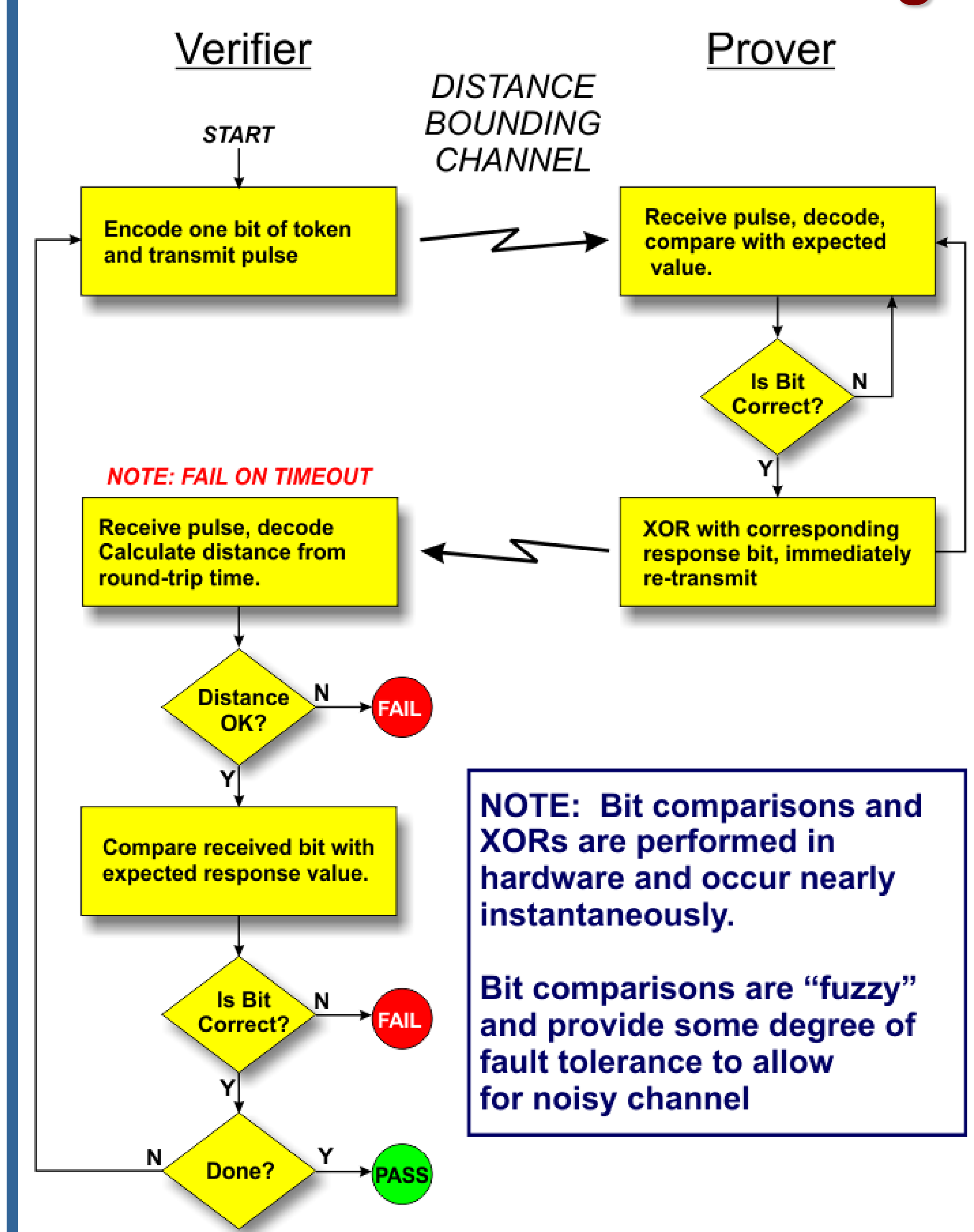


Resistance to Attacks

This system is highly immune to the following types of attacks:

- **Relay**: Distance limits (using TOF distance bounding) cause relay attack to fail distance tes**t**
- **Probing/Cloning**: If PUF is even microscopically altered, its responses change, effectively destroying it.
- **Modeling**: PUF hiding behind ZKPK and secure hashes prevent this
- **Snooping**: Low-information ZKPK techniques and encryption severely restrict information available to snoopers.

Secure 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) to permit verification of exact location (min. 4 units required to fix position in 3-space)

Conclusions

The RFID system described here provides a highly secure platform for protecting high-value assets. 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 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).

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