Wireless, Distance-Verifying Security System for ID Card/Document Enrollment Stations

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

Abstract

Modern ID Cards and passports have evolved into sophisticated, complex positive-ID instruments that embody a wide variety of anti-cloning and anti-forgery techniques, such as: digitized biometrics, micro-printing, encryption, RFID, embedded processing, holographic overlays, and UV/IR-visible features, among others. This poster describes a practical system for protecting against theft of the enrollment stations that produce these ID instruments, by providing a "lock" to a specific location. If a protected enrollment system is moved from that location, it will fail to function. This non-GPS location-locking technique is strongly protected against sniffing and spoofing, is immune to relay attacks, and cannot be copied – not even by its manufacturer.

System Overview

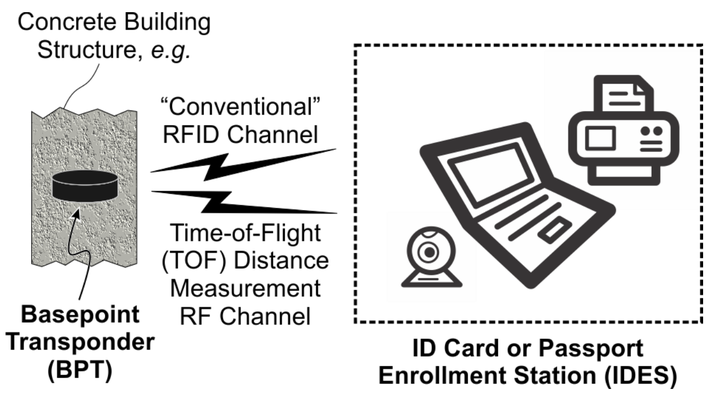


Figure 1. Basic System Structure

The security system employs a "Basepoint Transponder" that acts as a sort of "home base" for a client ID Enrollment Station (IDES). The BPT is a passively powered RFID transponder that would typically be embedded into a concrete pillar or other suitable building structure near the IDES.

The BPT/IDES communicate over a "conventional" RFID channel using asymmetric encryption, authenticated in both directions. The BPT and IDES determine a secret token from a secure hash of a Physical Unclonable Function (PUF) embedded in the BPT. This token is then used in a secure, hardware-based, distance bounding protocol over a dedicated distance measurement channel to determine if distance between the IDES and BPT has changed. If it has, the IDES shuts down.

Secure protocols prevent spoofing of the token or response. Any relay attack will fail the TOF distance test.

Physical Unclonable Functions (PUFs)

PUFs exploit molecular-level variations in chip structures to create a fingerprint function so unique to a chip that even identically manufactured chips will have different responses.

The figure below shows a serial PUF based on tiny wiring delay differences where a hashed *challenge* word selects a specific combination of wiring delays for comparison, producing a *response* word. PUFs are inherently "noisy" so ECC is typically used to "stabilize" the response.

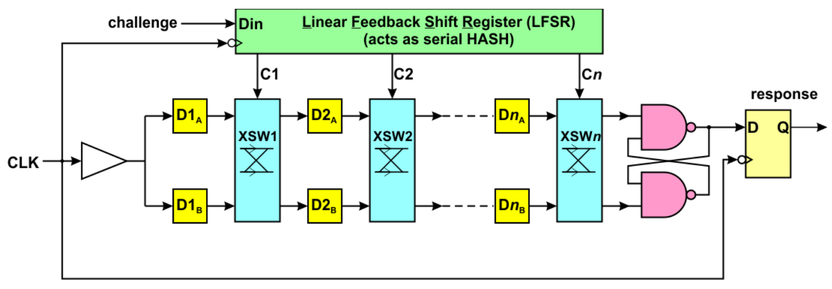


Figure 2. Serial Physical Unclonable Function (PUF)

BPT Architecture

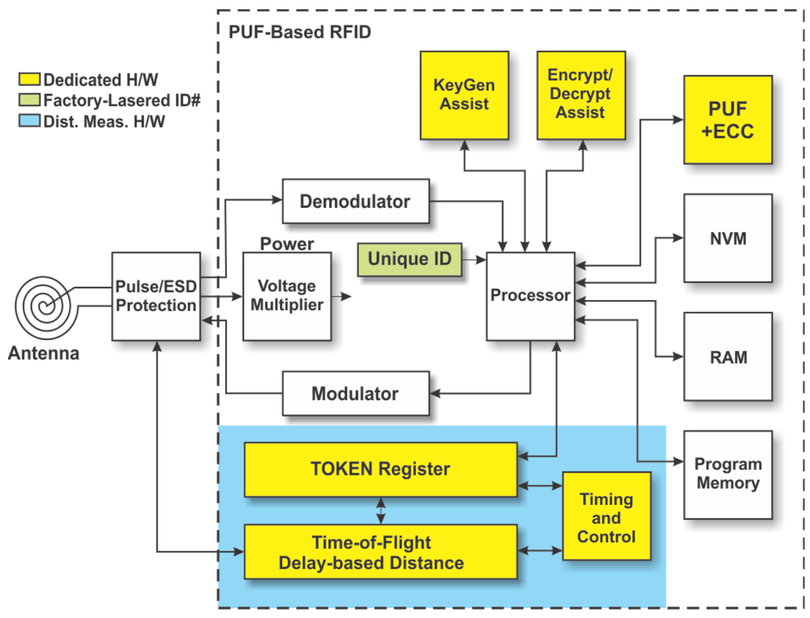


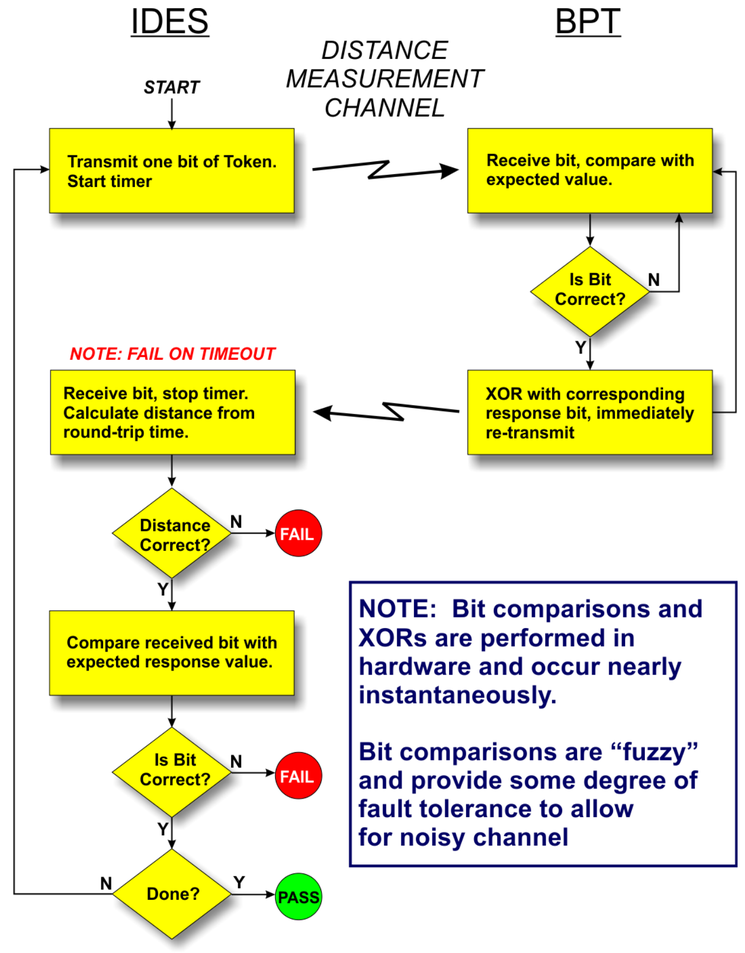
Figure 3. Block Diagram of Basepoint Transponder (BPT)

The BPT is passively-powered by the RFID signal and is not limited to the short burst communications typical of "on-the-fly" RFID because of the fixed installation. Longer carrier-on times provide sufficient power and time for the BPT to complete relatively long, compute-intensive operations.

To maximize speed and minimize software load, dedicated hardware-assist mechanisms are provided for key generation, encryption/hashing, PUF+ECC and TOF distance measurement. Functions not in use are powered down.

The BPT hides the PUF completely behind secure hash functions and encryption, using it only to generate encryption keys and TOF tokens. The PUF is *never* exposed directly, not even to the BPT manufacturer. A unique ID added to the PUF prevents any two BPTs from producing identical tokens or keys.

Time-of-Flight Distance Measurement



NOTE: Bit comparisons and XORs are performed in hardware and occur nearly instantaneously.

Bit comparisons are "fuzzy" and provide some degree of fault tolerance to allow for noisy channel

BPT Functions/Messages

- **Initialize** - Generate initial PUF-based public/private key values.
- **Verify Distance** – Coordinate TOF token and response values. Execute TOF distance sequence.
- **Transfer TA (Trusted Authority)** TA verifies BPT, transfers TA status to new TA. Initial TA is manufacturer.(Includes public key exchange)
- **Introduce Client** – TA introduces new client system (IDES) to BPT. (Includes public key exchange.) Establish initial distance
- **Invalidate Client** – TA instructs BPT to invalidate previously introduced client system.

CONCLUSION

This research provides a practical location-based security framework for ID card/passport enrollment systems that is highly resistant to sniffing/spoofing and is effectively immune to relay attacks. Ongoing research efforts are directed to refinement of the messaging protocols and development of a full hardware implementation.

Future related efforts will explore adaptation of this technique to secure automotive keyless-entry systems and similar wireless security systems against relay and sniffing attacks.