



# A Case for the use of PUFs in Indoor Localization Systems

Ana Isabel Gómez

Department of Computer Science  
Universidad Rey Juan Carlos  
Madrid (Spain)

# Outline

- 1 Introduction to Indoor Positioning
- 2 Practical security concerns
- 3 Proposed PKI infrastructure
- 4 Simulations
- 5 Conclusions and future work

# IPS- Indoor Positioning Systems

**Indoor Positioning systems:** Aimed at providing localization to any device in an efficient manner.

It is useful in

- Environments where GPS is not available (Warehouses, airports, supermarkets, big parking lots,..)
- Required precision is less than 5 – 10 meters.

Depending on the physical principle, the underlying technologies can be classified in inertial navigation, electromagnetic waves or mechanical waves.

# IPS- Technologies

Commercial IPS are usually beacon-based to provide good accuracy. Most solutions are based in [3]

- Ultrasound: Cheaper, prone to interferences and other non desired effects.
- Ultra wide Band (UWB signals): Expensive, good performance.

To share the same channel amongst several users, families of Time Hopping Sequences and Pulse Position Modulation are combined.

## IEEE 802.15.4 standard nodes

Mobiles users and beacons communicate in a wireless network.

- "Full-Function Devices" (FFD)
- "Reduced-Function Devices" (RFD): Resource constrained devices

**Roles:** Active and passive mobile users.

Different behavior in the network.

- Passive mobile users emit a blink to broadcast their location. Usually Active RFID (vests on humans)
- Active mobile users can interact with the network, send control commands and initiate a protocol to calculate the position of the nearest users. Usually FPGA (forklifts or heavy machinery)

# Network Architecture

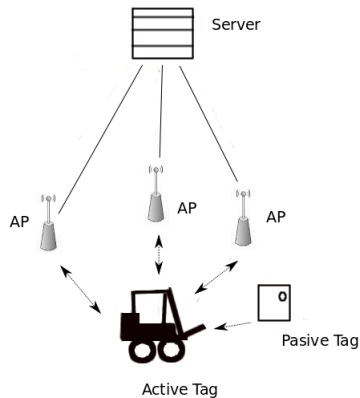


Figure: Communication links between the different actors of the system

# Different Security Scenarios

Most common security threats are active attacks:

- **Inject malicious constructed packages:** Deceive a receiver about the distance of a Mobile User.
- **Jamming attacks:** Disrupt the network.

Both cases require the knowledge of the Time Hopping sequences (THS).  
If not,

- Brute force attacks are costly.
- In an indoor location system, position information does not require confidentiality beyond a reasonable time.

# Different Security Scenarios

We consider two complementary approaches to security:

- Spread Spectrum techniques for physical layer security
- Authentication to access the medium.

We propose two authentication mechanism, depending on the mobile user

- Physical Unclonable function (PUF): Mobile user to anchor.
- Signature based: Active mobile users to passive mobile user.

Goal: Implement a public key infrastructure (PKI) where anchor and Mobile Users share a communication channel.



# Identity Based Encryption

IBE (Identity Based Encryption): Introduced by Adi Shamir [4] in 1984, is an alternative to public-key encryption.

- User's Public key can be an arbitrary identity string (v.g email address)
- Encrypted messages can be send using this identity without a full PKI.
- Requires a Trusted Authority to manage the private key of each user.
- No verification of the public key, it can be calculated from the security parameters provided by the authority.

IBE only guaranties confidentiality. It does not provide integrity, availability, authentication and non-repudiation.

# Identity Based Encryption

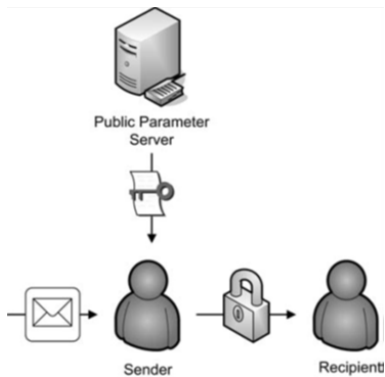


Figure: Encryption process in an IBE system

# IBE Scheme

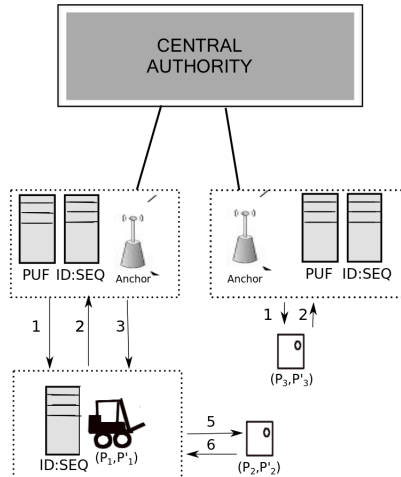
Consists in four algorithms:

- 1 Configure: Requires a security parameter  $k$  and returns the system parameters (public) and the master key ( $MPK$ ).
- 2 Extraction: Computes the IBE private key from input ( $MPK$  and an arbitrary  $ID \in \{0, 1\}^*$ ).
- 3 Encryption: Encryption with a public key that is calculated from system parameters (configuration step) and user's ID.
- 4 Decryption: Reverse process of encryption. It uses the already calculated private key to find the plaintext.

# Proposed Schema

- Integrating a physically unclonable function (PUF) to provide a ID for Mobile Users.
- Using Identity Based Encryption (IBE) for securing the communication for a passive node. This allows to change the THS to protect communications against an eavesdropper.
- Control of the active node communication, the node can listen and send control commands to the anchors and other MUs. This type of MUs have access to power sources like AC-batteries (forklifts, heavy machinery, etc) or DC-batteries (human vests).

# Scenarios



# Protocol

- **Mobile-to-Anchor authentication:**

(1) Anchor send a PUF challenge to Mobile User.

$$\text{Send}(\text{Encrypt}(\text{Challenge}(a, b)), r_A))$$

(2) Mobile User send an encrypted answer.

$$\text{Send}(\text{Encrypt}(\text{Response}(a, b)), r_{user}))$$

- **THS-change:**

(3) Anchor send new sequence using  $ID_{user}$

$$\text{Send}(\text{Encrypt}((p1, p2), ID_{user}))$$

(4) The user decrypt the message with its private key  $r_{user}$

- **Passive-to-Active authentication:**

(5) Active User send a random value  $C$  using  $ID_{user}$

(6) Pasive user sends  $C$  to the active user, after decrypting with  $r_{user}$

## IBE

We propose Cocks system [1] based in quadratic residue problem. The major disadvantage is in the cost of increased data to transmit due to two reasons:

- First, the sender cannot initially know whether the receiver has the private key  $r$  corresponding with the identifier  $a$  or  $-a$  due to the design of Cocks system (double sending)
- Each bit is encrypted with a number of bits as large as the key, this makes the ciphertext expand depending on the size of this key.

# Chosen PUF

The PUF architecture proposed in [2] provides an output with sufficient length (32 bits for this application).

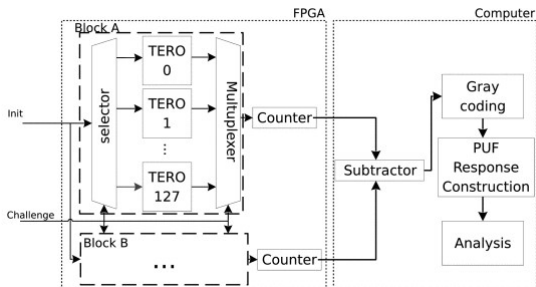


Figure: TERO-PUF. Source in [2]



# Parameters of the system

- **Key size:** For this prototype a key size of 1024 bits has been chosen (confidentiality  $<$  eight years).
- **Size of UWB messages.** Sequences of length 512 time slots. The capacity of the channel is 256kbit/s.
- **Key renewal policy:** Freely chosen by the system administrator depending on the security level.
- **Size of the identifiers:** Each node transmit using a pair of THS, occupying a total of 2 bytes each. Additionally, public ID is a 32-bit identifier.

# Time simulation

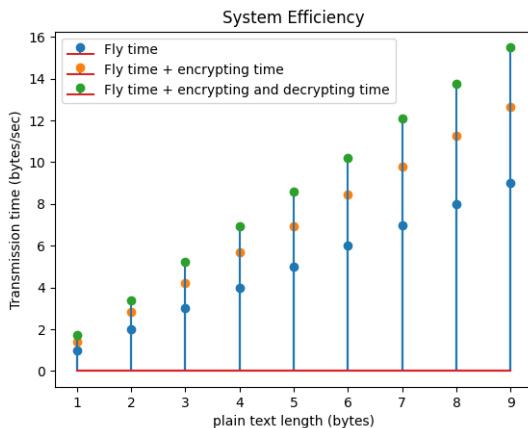






Figure: Simulation of transmission times in an UWB channel (256 kbit/s).

# Conclusions

- With 2-byte identifiers, authenticating a mobile user into the system would take less than 4 seconds.
- If THS needs to be changed, this would take twice as long (approximately 8 seconds).
- The PUF allows to avoid generating identifiers and the identification is made possible using challenges. Allows more sophisticated functions such as the delimitation of access zones for active and passive nodes, with application in access control or alarm management.
- Private key assignment stage is laborious as it has to be done on a secure channel.

# Future work & Questions

- Full network performance measurements
- Full integration of the PUF in the system as well as its performance in different hardware architectures.
- Explore the performance of the remaining IBE Schemes (elliptic curve pairings and hard problems on lattice).

-  Cocks, C. An identity based encryption scheme based on quadratic residues, In IMA international conference on cryptography and coding (pp. 360-363), 2001.
-  Marchand, C., Bossuet, L., Mureddu, U., Bochard N., Cherkaou, A. Implementation and characterization of a physical unclonable function for IOT: a case study with the Tero-puf *EEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 37(1):97–109, 2017..
-  Jiménez, A.R & Seco, F. Comparing ubisense, bespoon, and decawave uwb location systems: Indoor performance analysis. *IEEE Transactions on Instrumentation and Measurement*, pp:1–12, 04 2017.
-  Shamir, A. Identity-based cryptosystems and signature schemes. In *Workshop on the theory and application of cryptographic techniques* (pp. 47-53), 1984.