

“A Scalable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags”

Andrea Soppera
David Molnar
David Wagner

British Telecom Research
University of California Berkeley
University of California Berkeley

Outline

- A brief introduction to RFID technology
- A scalable pseudonym protocol (Tree of Secrets)
- Transfer of ownership (Delegation Tree)

RFID Security and Privacy

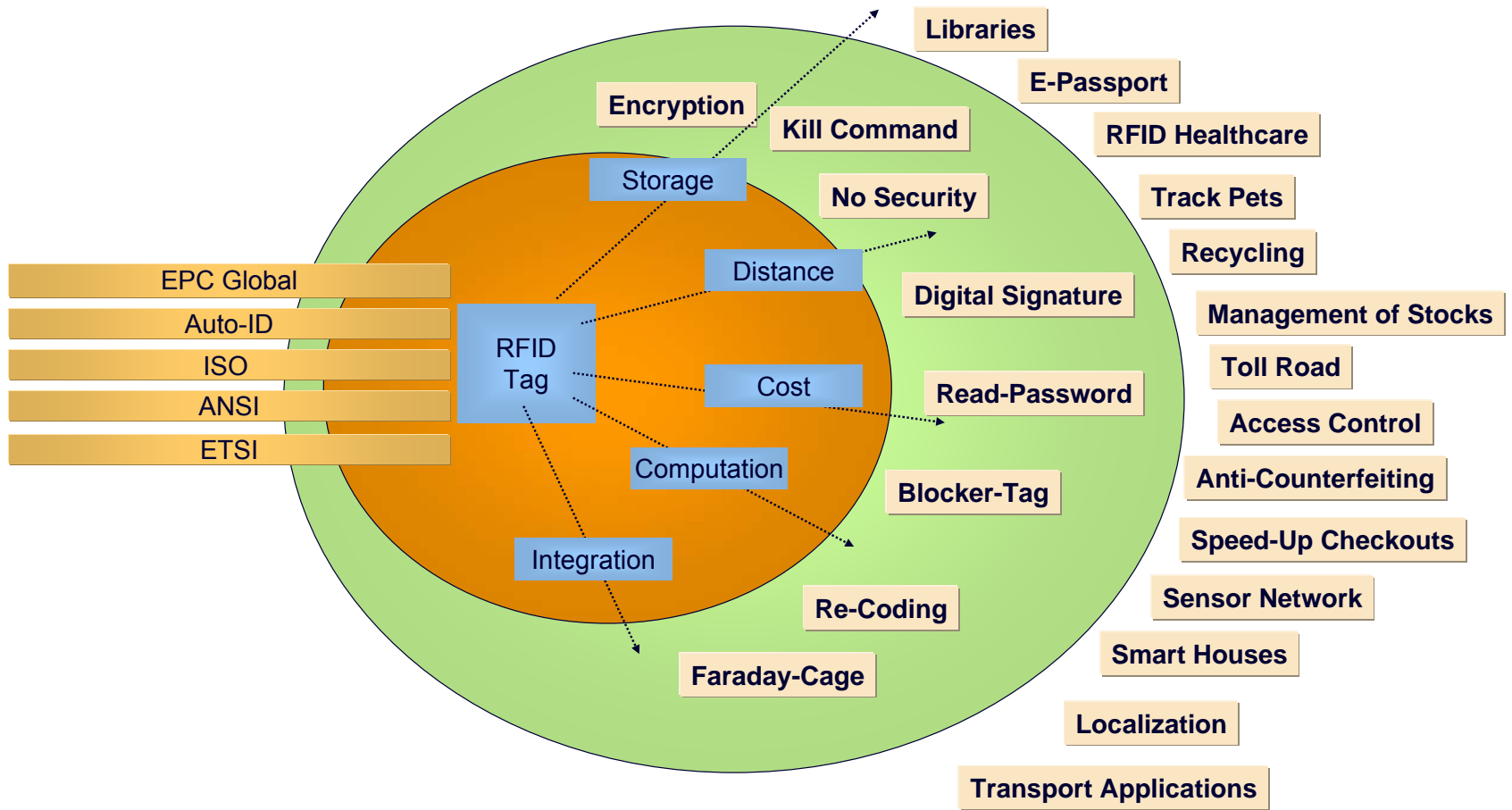
The release of a static identifier leads to privacy issues:

1. Leakage of personal or inventory information
2. Traceability of the tag

What level of security do you consider acceptable for the tag?

- Concealment of the identifier (unless an access password is provided) - as supported by EPC Gen 1
- Serialization or Encryption of the identifier
- Pseudonyms - Identifier changes at each read

RFID Multidimensional Problem



Example Application

RFID in Healthcare: Management of stock, Anti-counterfeiting, Speed up supply chain processes

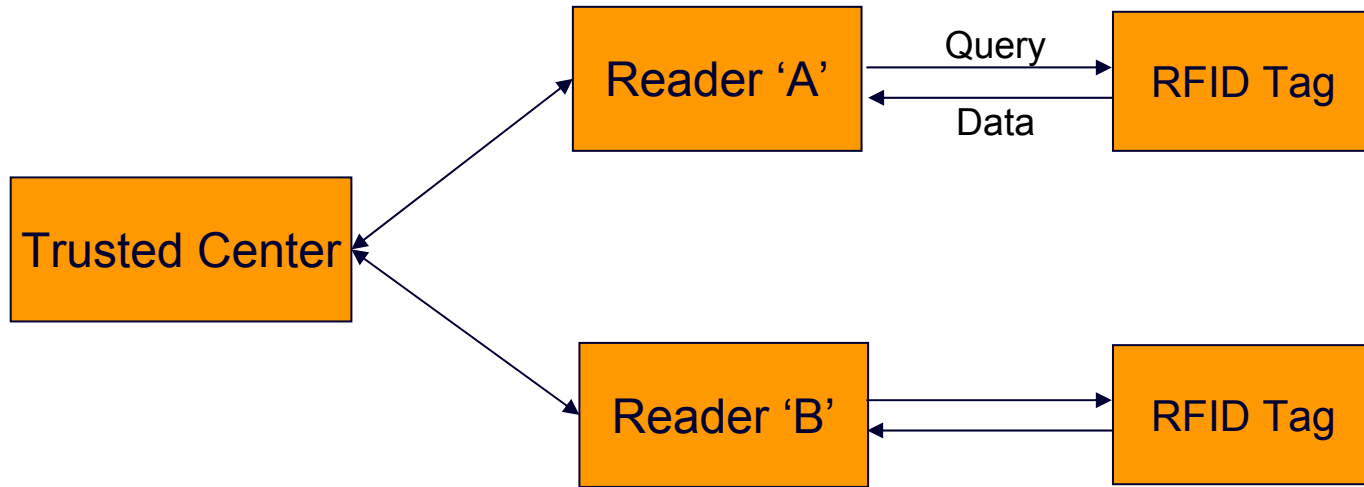
1. Ensuring patient privacy and security of the supply chain for controlled drugs by NOT identifying the product type.
2. Avoiding (as far as possible) correlations between identifiers for instances of the same product
3. Allowing for scalable (to several billions of units per year) lookup based on the identifier. The ability to pick and count products efficiently.
4. Sharing secure RFID drug data along the supply chain and control cloning of the identifier.

Secure RFID Protocol

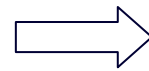
Goal: Only authorized readers should determine a tag's identifier. For all other readers, tag reads should be indistinguishable from each other.

1. **Pseudonym Based Solution-** We wish to stop linkability of RFID tag reads by unauthorised readers.
2. **Scalable Lookup-** With large number of tags the reading time should be small. Ability to pinpoint tag identity and pseudonym.
3. **Controlled Delegation-** Minimize trust in readers. Reader's ability to read a tag should be limited to a particular time period.
4. **Transfer of Ownership-** Control when tag changes hands. Ability to control access to the identifier without recoding the tag.

Protocol Sketch

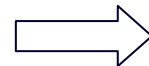


Security and Privacy



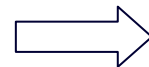
RFID Pseudonym Protocol

Scalability



Tree of Secrets

Controlled Delegation



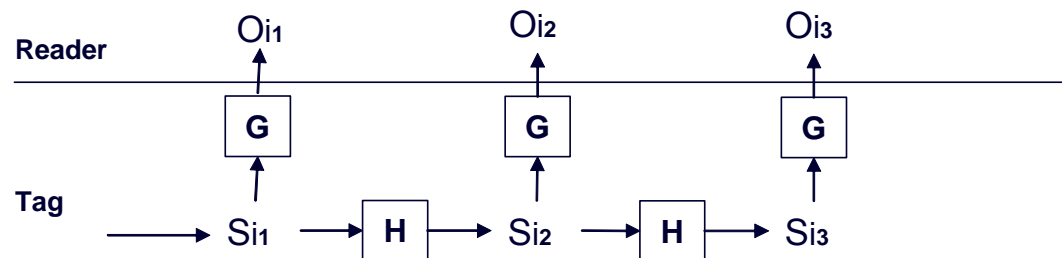
Delegation Tree

RFID Pseudonyms

The tag output changes at each reading operation and is un-linkable by unauthorized readers.

RFID tag replies with a pseudonym that changes each time the tag is queried.

- Tag stores in memory a random identifier S_i
- H and G are hash functions



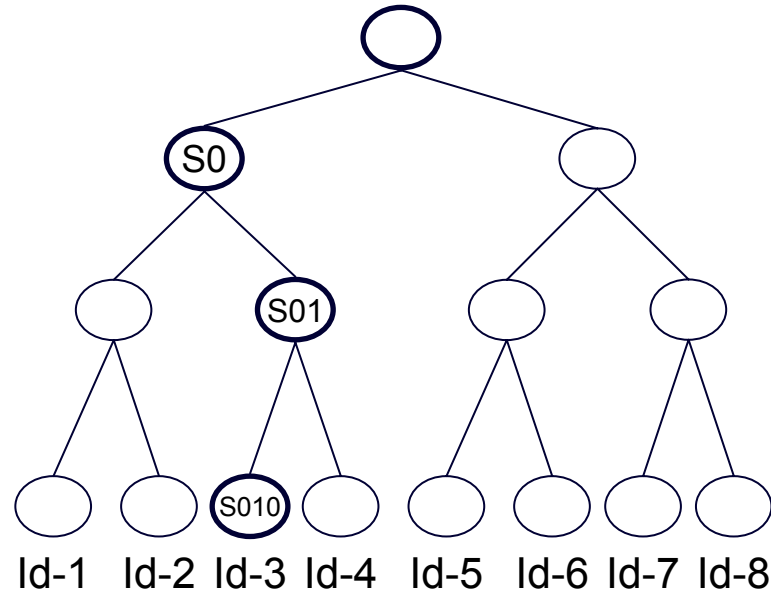
Ohkubo, Suzuki, and Kinoshita

Problems of scalability (searching of pseudonym space)
and resilience (loss of synchronisation)

Scalable Lookup

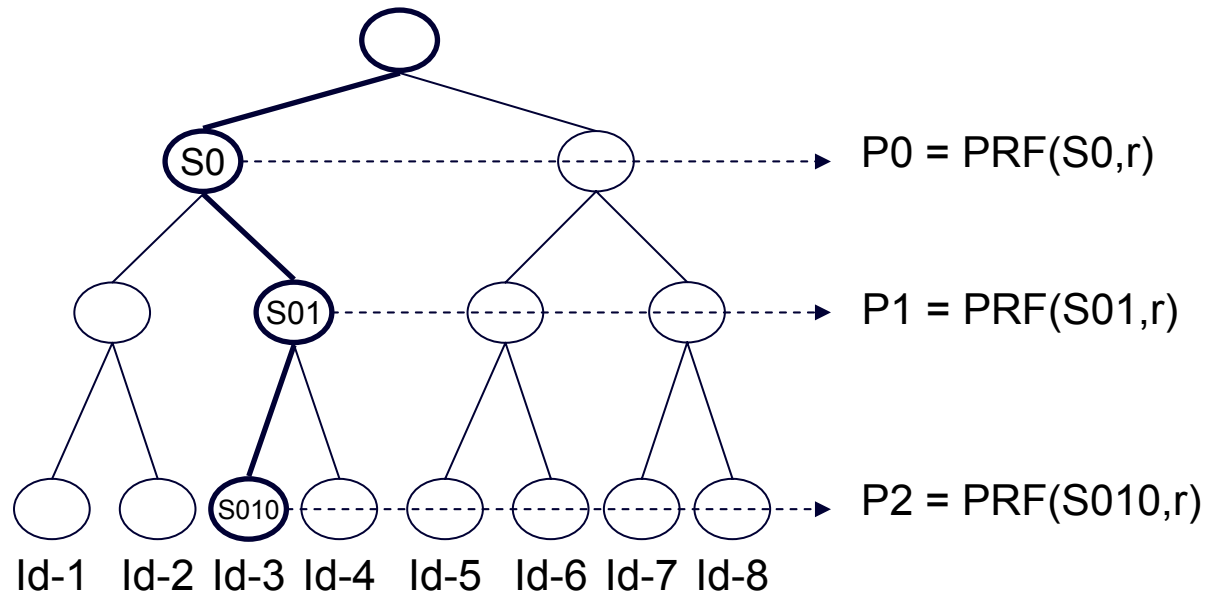
- Consider an RFID System with a database of N tags that receives a pseudonym to be decoded.
 - Naïve approach. Check for each of the N tags present in the database and verify if the pseudonym could have been generated by that tag.
Complexity: $O(N)$ check required each time a tag is read.
- The Idea is to store a Tree of Secrets on the “RFID tags”.
 - Each tag is identified with a leaf of the tree. A tag stores the secret from the root to the leaf of the tree.
Complexity: $O(\log N)$ check required to decode the pseudonym.

Tree of Secrets



1. Each S is a different, randomly chosen 128-bit secret key.
2. Associate each tag with a leaf of the tree
3. Tag knows secrets from root to its leaf.
4. Example: Tag ID-3 is associated with S0, S01, S010
5. Trusted Center knows all secrets.

Pseudonym Generation



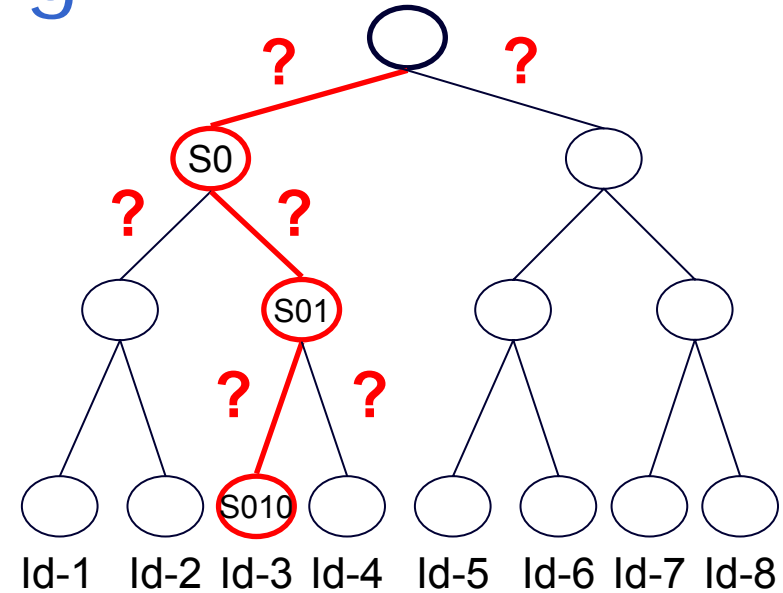
Generate a new Pseudonym every time a Tag is read.

1. Generate a random 128-bit number r .
2. Compute P_0 , P_1 and P_2
3. Output Pseudonym: $= (r, P) = (r, P_0, P_1, P_2)$

Pseudonym Decoding



Pseudonym: $= (r, P) = (r, P_0, P_1, P_2)$
 Trusted Center stores the tree of secrets.



The Trusted Center receives a Pseudonym: (r, p)

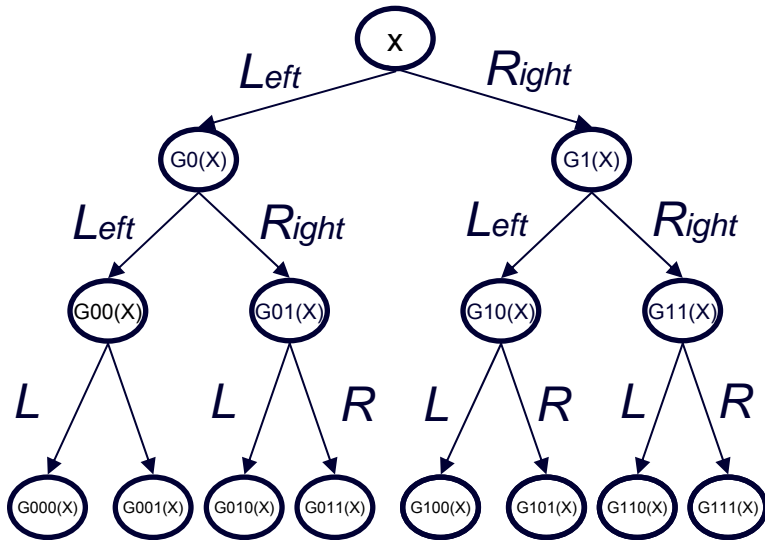
1. Does $\text{PRF}(S_0, r) == P_0$? Does $\text{PRF}(S_1, r) == P_0$?
2. Does $\text{PRF}(S_{00}, r) == P_1$? Does $\text{PRF}(S_{01}, r) == P_1$?
3. Does $\text{PRF}(S_{010}, r) == P_2$? Does $\text{PRF}(S_{011}, r) == P_2$?

Scalable Lookup: Tag Identified with a complexity $O(\log(N))$

Controlled Delegation

- Consider an RFID reader that receives a pseudonym to be decoded.
- Reader Online: The reader acts as a relay passing the pseudonym from the Tag to the Trusted Center (TC).
 - Weakness: Requires a costly interaction between the reader and the TC every time the tag is read.
- Reader Offline: The TC delegates a time-limited secret. The secret allows to recognize the next q -pseudonyms from the tag.
 - The reader can decode the tag for a limited amount of operations.

Delegation Tree



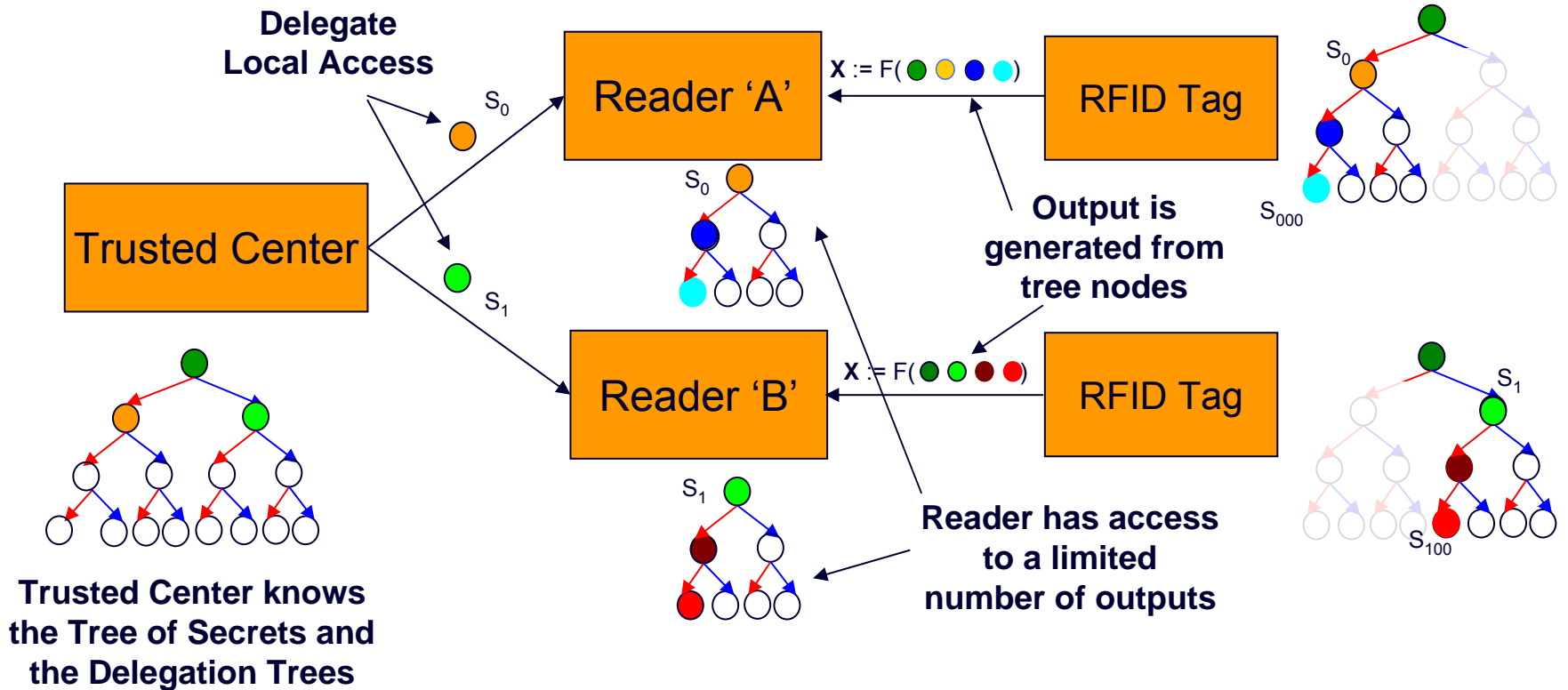
1. A leaf node in the Tree Secrets acts as the root of the delegation tree.
2. Let G be a Pseudo-Random-Generator (PRG).

$$G_0(X) \equiv \text{Left} \quad G_1(X) \equiv \text{Right}$$

Delegation trees are derived by the GGM construction of applying a pseudo-random generator to the parents.

The idea is to have a “delegation tree” for each tag. The TC delegates by giving access to a subtree to the reader. A sequence of pseudonyms is generated by intermediate nodes.

Delegation Process



Ownership Transfer

Recoding: when the tag changes hands the tag is recoded. The new ID is linked to the original ID of the tag in the database(s).

- Drawback: requires an online architecture and reader/tag that supports read/write operation.

With offline delegation, we introduce two techniques for ownership transfer:

1. **Soft Killing.** Suppose the previous user has been delegated K leaves. The new user needs to 'read' the tag $K+1$ times to ensure that privacy is maintained.
2. **Increasing the tag counter.** Perform mutual authentication between the tag and new reader.

Security Analysis

The protocol provides privacy for RFID Tags reading.
Without permission by the Trusted-Center a reader cannot determine the tag identity or track a tag.

Worst attacks:

1. Replay-only security against impersonation attacks.
2. Attacker compromises the tag.
 - Privacy affected. Two tags could share secret same path of the tree.
 - Solution pick the tree branching factor that optimize the trade-off between Privacy and Reader work

Practical Example – System Setup

RFID Tags & Trusted Center

- Tag needs to perform PRF and PRG
- Tag requires an EEPROM capable of storing a counter for the delegation tree.
- Tag memory stores $\log(N)$ secrets of the tree $S_1, \dots, S_{\log(N)}$. Where $S_{\log(N)}$ is the root of the GGM tree.
- Trusted Center initially contains the Tree of Secrets ($2N$ secrets) and the map with tag's identifiers.

RFID system

- Number of tags $N = 2^{20}$
- Assume a tag can be read $x = 2^{20}$
- Tree branching factor $k = 2^{10} = 1024$ (tree with 5 levels)
- Secret size = 64 bit

Practical Example – RFID System

RFID Tag

- Storage Cost = 3 Secret (S1, S2, S3) = 192-bit
- Computation Cost per read: 5 applications of PRF and 3 of PRG
- Communication cost (Output length) 112-bit -64-bit random value -32-bit truncation of the leaf -4-bit truncation for intermediary nodes.

Trusted Center

- Computation Cost to decode a pseudonym on average $10(2^{10})$ computation.
- Time to decode a pseudonym $\approx 0.000610s$

Reader Cost (N' = 100)

- Computation on average $100(2^{10})$

Conclusions

We have proposed a secure RFID pseudonym protocol that enables delegation and ownership transfer.

- Secure
 - Only authorized readers can decrypt tag pseudonym
 - Worst adversary can do is replay old pseudonyms
- Scalable
 - $O(\log N)$ work per tag
- Delegation
 - Minimizes trust on readers: delegate only as needed
- Transfer of ownership
 - Tag can change hands without need of re-coding