# Proactive Threshold Cryptosystem for EPC Tags*

J. GARCIA-ALFARO[1], M. BARBEAU[2], E. KRANAKIS[2]

[1] *Institut TELECOM, TELECOM Bretagne, 35576 Cesson Sévigné, France*
[2] *Carleton University, School of Computer Science, Ottawa, K1S 5B6, Canada*

*E-mail:* joaquin.garcia-alfaro@acm.org,
{barbeau,kranakis}@scs.carleton.ca

We define three privacy-preserving solutions to the problem of distributing secrets between manufacturers and vendors of items labeled with Electronic Product Code (EPC) Gen2 tags. The solutions rely on the use of an anonymous threshold secret sharing scheme that allows the exchange of blinded information between readers and tags. Moreover, our secret sharing scheme allows self-renewal of shares with secret preservation between asynchronous shareholders. The first two solutions address the eavesdropping and rogue scanning threats. The third solution mitigates as well tracking threats.

*Key words:* Radio Frequency Identification (RFID), Electronic Product Code (EPC), Wireless Security, Threshold Cryptography, Privacy.

## 1 INTRODUCTION

The EPCglobal class-1 generation-2 (Gen2 for short) specification [2], approved as ISO18000-6C, has been reported vulnerable to privacy attacks in previous studies [3, 4]. Consumer privacy is indeed an important concern about Gen2 applications. For instance, the use of Gen2 tags for item-level passive tagging [5] of end-user goods, allows customers to enjoy the benefits of RFID technology, but anyone with a compatible Gen2 reader can access a

* An early version of this paper can be found in [1].

consumer's purchase data. The readability of tag identification in the Gen2 protocol clearly violates consumer privacy. The issue must be properly handled before releasing this technology for item-level tagging. A radical solution is the use of the *kill* feature that disables Gen2 tags at purchase time [2]. This solution is far from being effective because it requires spending more time at checkout stands and voids the benefits of the RFID technology offered to customers, such as processing of returns and automated recycling. Our goal is to provide non destructive lightweight alternatives that preserve consumer privacy. In this paper, we survey related works and present an original scheme for the construction of a lightweight threshold cryptosystem [6] that can be deployed on low-cost Gen2 systems. The scheme protects EPC Gen2 tag data against eavesdropping, rogue scanning, and tracking by malicious readers.

### 1.1 Tag Identification (TID) disclosure on the Gen2 Protocol

The memory of an EPC Gen2 tag is separated into four independent blocks: reserved memory, EPC data, Tag Identification (TID), and User memory. Gen2 tags communicate this information by accumulating power from reader interrogations [2]. Figure 1 shows the steps of the EPC Gen2 protocol for product inventory. In Step 1, a reader queries the tag and selects one of the following options: *select*, *inventory*, or *access* [2]. Figure 1 represents the execution of an *inventory* query. It assumes that a *select* operation has been previously completed in order to singulate a specific tag from the population of tags. When the tag receives the *inventory* query, it returns a 16-bit random string denoted as RN16. This random string is temporarily stored in the

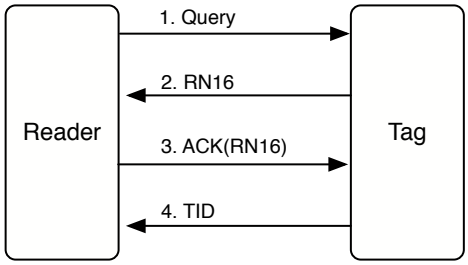



FIGURE 1
EPC Gen2 Inventory Protocol.

tag memory. As a response to the *inventory* query, the tag enters in the *ready* state, and backscatters in Step 2 the random string RN16. In Step 3, the reader replies to the tag a copy of the random string, as an acknowledgment. If the echoed string matches the copy of the RN16 squence stored in the tag memory, the tag enters in the *acknowledged* state and returns its corresponding *tag identification* (TID).

Security features on Gen2 tags are minimal. They protect message integrity via 16-bit Cyclic Redundancy Codes (CRC) and generate 16-bit pseudo random strings. Let us observe that any compatible Gen2 reader can access the TID. This is due to the lack of authentication between a Gen2 reader and a Gen2 tag. To overcome this problem, a number of solutions have been proposed in the literature. Two solutions proposed rely on the use of cryptographic primitives to encrypt TIDs and the use of pseudonyms for the TIDs. Both solutions require that the reader and tag share a common secret (either a key to decrypt a protected TID or a property to map a pseudonym to the true TID). Therefore, an effective mechanism for the distribution of secrets among the entities, readers and tags, of a supply chain must be introduced.

We present in this paper a threshold cryptosystem that provides both consumer privacy and distribution of secrets. Our solution addresses the following three threats: (1) Eavesdropping: an adversary listening passively to the RF (Radio Frequency) communications between a tag and reader aiming to intercept the TID; (2) Rogue Scanning: an adversary interacting actively with a tag to access the TID; (3) Tracking: an adversary correlating RF communications to either passively or actively identify an instance of a given tag. We present three different variants of our solution for the exchange of secrets between manufacturers and vendors of Gen2 labeled items. The two first variants handle the eavesdropping and rogue scanning threats. The proactiveness of the third variant addresses, in addition, the tracking threat.

The main properties of our approach are: (1) low-cost Gen2 tag renewal with secret preservation and without the need to synchronize to a reader performing an inventory process or any other tags holding shares of the same secret; (2) size of shares compact enough to fit into the inventory responses of low-cost EPC Gen2 tags (i.e., less than 528 bits, as suggested by EPCglobal in [2]); (3) secret sharing construction that guarantees strong security; (4) reconstruction of the secret does not require the identity of the shareholders, e.g., the TIDs. The remainder of the paper is organized as follows. Section 2 surveys privacy-preserving solutions for low-cost RFID systems. Section 3 presents the formalization of our proposal. Section 4 provides some simulation and experimental details. Section 5 concludes the paper.

## 2 RELATED WORK

The high constraints of EPC Gen2 tags makes challenging the use of standard cryptography-based solutions for the design of privacy preserving mechanisms. In this section, we survey solution and trends recently published in the literature.

### 2.1 Use of Standard Cryptography-based Solutions

MAC (Message Authentication Code) based security protocols are among the first solutions discussed in the literature for securing low-cost RFID applications. In [7], for example, Takaragi et al. present a solution based on CMOS technology that requires less than four thousand gates to generate MACs using 128 bit identifiers stored permanently in tags at manufacturing time. Each identifier relies on an initial authentication code concatenated with chip manufacturer data. The result of this concatenation is posteriorly hashed with a given secret to derive a final MAC. This MAC is communicated from manufacturers to clients and shared by readers and tags. The main benefit of this approach is that it increases the technical difficulties of performing eavesdropping and rogue scanning. However, the use of static identifiers embedded in tags at manufacturing time does not solve the tracking threat. Moreover, brute force attacks can eventually reveal the secrets shared between readers and tags. The discovery of secrets could lead to counterfeit tags.

An enhanced solution relies on the use of lock-based access control. In [8], Weis et al. propose a mechanism to prevent unauthorized readers from reading tag contents. A secret is communicated by authorized readers to tags on a secure channel. Every tag, using an internal function, performs a hash of this secret and stores the result in its internal memory. Then, the tag enters into a locked state in which it responds to any query with the stored hash value. Weis et al. also describe a mechanism for unlocking tags, if such an action is needed by authorized readers (i.e., to temporarily enable reading of private data). Regarding the tracking threat, Ohkubo et al. propose in [9] the use of hash chains achieving on-tag evolution of identifiers. Avoine and Oechslin discuss in [10] limitations of the aforementioned approach. They propose an enhanced hash-based RFID protocol to address eavesdropping, rogue scanning, and tracking by using timestamps. Similarly, Henrici and Müller discuss in [11] some weaknesses in the lock-based schemes presented in [8, 9] and present an improved mechanism. Several other improvements and lock-based protocols, most of them inspired by lightweight cryptography for devices such as smart cards, can be found in [12, 13, 14].

### 2.2 Hardware Limitations

Note that the approaches reviewed in Subsection 2.1 require the implementation of efficient one-way hash primitives within low-cost RFID tags. It is the main challenge of these proposals. Resource requirements of standard one-way hash functions, such as MD4, MD5, and SHA-128/SHA-256, exceed the constraints of low-cost Gen2 tags [2]. The implementation of these functions require from seven thousand to over ten thousand logic gates; and from six hundred to over one thousand two hundred clock cycles [14]. The complexity of these standard one-way hash functions is therefore an obstacle for their deployment on Gen2 tags.

The use of standard encryption engines for the construction of hash operations has also been discussed in the literature. For example, the use of Elliptic Curve Cryptosystem (ECC) [15] for the implementation of one-way hash primitives on RFID tags has been studied in [16]. Its use of small key sizes is seen as very promising for providing an adequate level of computational security at a relatively low cost [17]. An ECC implementation for low-cost RFID tags can be found in [18]. In [19], on the other hand, Feldhofer et al. present a 128-bit implementation of the Advanced Encryption Standard (AES) [20] on an IC of about three thousand five hundred gates with a power consumption of less than nine microampers at a frequency of 100 kHz. Although this implementation is considerably simpler than any previous implementation of the AES algorithm, its requirements are still seen as too high for low-cost RFID tags.

### 2.3 Towards Secret Sharing Strategies

The use of secret sharing schemes [6] is proposed by Langheinrich and Martin in [21, 22] as a key solution for addressing authentication in Gen2 scenarios (e.g., supply chain applications of the retail industry). The work presented in [21] simplifies the lookup process performed on back-end databases for identifying tags, while guaranteeing authentication. TIDs, seen in this work as the secrets that must be shared between readers and tags, are encoded as a set of shares, and stored in the internal memory of tags. The authors propose the use of a Perfect Secret Sharing (PSS) scheme, in which the size of the shares is equivalent to the size of the secret, based on the $(t,n)$-threshold secret sharing scheme introduced in [23]. The combination of shares at the reader side leads to the reconstruction of original TIDs. To prevent brute-force scanning from unauthorized readers — trying to obtain the complete set of shares —

the authors propose a time-limited access that controls the amount of data sent from tags to readers. At the same time, a cache based process ensures that authorized readers can quickly identify tags. In [21], the authors extend the previous proposal to spread the set of shares across multiple tags. Still based on Shamir's perfect secret sharing scheme, this new approach aims at encoding the identifier of an item tagged with multiple RFID devices by distributing it as multiple shares stored within tags. Authentication is achieved by requiring readers to obtain and combine the set of shares.

A different use of secret sharing schemes is presented by Juels, Pappu, and Parno in [24]. They propose the use of a dispersion of secrets strategy, rather than the aggregation strategy used by Langheinrich and Marti. In this approach, a secret used to encrypt Gen2 TIDs is split into multiple shares and distributed among multiple tagged items. Construction and recombination of shares is based on a Ramp Secret Sharing (RSS) scheme, in which the size of each share is considerably smaller than the size of the secret, at the price of leaking out secret information for unqualified sets of shares. To identify the tags, a reader must collect a number of shares above a threshold. At the manufacturer facility, large quantities of items of the same product, initially tagged together with shares of the same secret, guarantee that authorized readers can always reconstruct the secret and, therefore, decrypt the TID of the tagged items. At the consumer side, the items get isolated. Without the space proximity of other items holding the remainder shares of the secret, an unauthorized reader cannot obtain the sufficient number of shares to reconstruct the key that allows identifying the TID. Privacy is, therefore, achieved though the dispersion of secrets and encrypted identifiers. Moreover, the proposed scheme helps to improve the authentication process of tags. Assuming that $t$ shares are necessary for readers to obtain the EPC data assigned to a pallet, a situation where the number of shares obtained by readers is below $t$ leads to conclude that unauthorized tags are present in the pallet.

The main limitation of this approach is that a critical privacy threat to consumers, i.e., the tracking threat defined in Section 1.1, is not addressed. It is a requirement stated by most authors, such as Juels and Weis in [25]. Privacy-preserving solutions for RFID applications must guarantee both anonymity and untraceability. In the sequel, we show that it is possible to improve privacy-preserving using secret sharing strategies. We have developed a proof-of-concept threshold cryptosystem that provides, in addition to eavesdropping and rogue scanning, tracking protection.

## 3 ON THE CONSTRUCTION OF A PROACTIVE THRESHOLD SECRET SHARING SCHEME FOR EPC GEN2

The construction of our proactive (*t*,*n*)-threshold cryptosystem relies on the computation of the Moore-Penrose pseudoinverse of a homogeneous system of $n$ linear equations with $t$ unknowns (where $t < n$) over a finite field $\mathbb{Z}_p$,

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \quad \cdots \quad + a_{1t}x_t &= 0 \ (mod\ p), \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 + \quad \cdots \quad + a_{2t}x_t &= 0 \ (mod\ p), \\ \vdots & \\ a_{n1}x_1 + a_{n2}x_2 + a_{n3}x_3 + \quad \cdots \quad + a_{nt}x_t &= 0 \ (mod\ p), \end{aligned}$$

in which $t$ and $n$ are positive integers, and $p$ is a prime number. The vector columns of the coefficient matrix $A$ associated to the system of linear equations are linearly independent, i.e., matrix $A$ has rank $t$ and so the vector columns of $A$ span an inner-product subspace in $\mathbb{Z}_p^{n\times t}$ of dimension $t$.

The Moore-Penrose pseudoinverse (also called the generalized inverse) of a non-square matrix $A \in \mathbb{Z}_p^{n\times t}$, hereinafter denoted as $A^\dagger$, is the closest representation that $A$ can get to its inverse (since non-square matrices, i.e., $n \neq t$, do not have an inverse). Let us notice that if $rank(A) = t = n$, i.e., $A$ is a full rank square matrix, the Moore-Penrose pseudoinverse of $A$ is certainly equivalent to the inverse matrix $A^{-1}$, i.e.,

$$A^\dagger = A^{-1} \mid A \in \mathbb{Z}_p^{n\times t} \ \wedge \ rank(A) = t = n \tag{1}$$

Otherwise, the Moore-Penrose pseudoinverse of a rectangular matrix $A$ exists if and only if the subspaces *Ker A* (null space of matrix $A$) and *Im A* (range space of matrix $A$) have trivial intersection with their orthogonals. In the case that $A \in \mathbb{Z}_p^{n\times t}$ has *rank(A)*$= t$, it can be proved that $A^\dagger$ exists and it can be computed as follows:

$$A^\dagger = (A^\perp A)^{-1} A^\perp \in \mathbb{Z}_p^{t\times n} \mid A \in \mathbb{Z}_p^{n\times t} \ \wedge \ rank(A) = t \neq n, \tag{2}$$

in which $A^\perp$ denotes the transpose of matrix $A$. It can also be proved, cf. [26], that if $A \in \mathbb{Z}_p^{n\times t} \mid rank(A) = t$, $A^\dagger$ is the unique solution that satisfies all of the following four equations defined by Penrose in [27]:

$$\begin{aligned} (A\,A^\dagger)^\perp &= A\,A^\dagger, \\ A^\dagger\,A\,A^\dagger &= A^\dagger, \\ (A^\dagger\,A)^\perp &= A^\dagger\,A, \text{ and} \\ A\,A^\dagger\,A &= A \end{aligned} \tag{3}$$

For our specific construction, we are interested in showing that the resulting matrix $A^{\dagger}$ keeps the orthogonal projection property required in [27]. Indeed, we are interested in showing that the resulting matrix $P_A$ computed as

$$P_A = A\,A^{\dagger} \in \mathbb{Z}_p^{n\times n} \mid A \in \mathbb{Z}_p^{n\times t} \ \wedge \ rank(A) = t \neq n \tag{4}$$

is indeed an *orthogonal projector* that satisfies the idempotent property (meaning that $P_A^k = P_A$ for all $k \geq 2$. Certainly, if $P_A = A\,A^{\dagger}$, then $P_A^2 = (A\,A^{\dagger})\,(A\,A^{\dagger})$, i.e., $P_A^2 = (A\,A^{\dagger}\,A)\,A^{\dagger}$). From Equation (3), we obtain that $P_A^2 = A\,A^{\dagger}$, i.e., $P_A^2 = P_A$, and so $P_A^k = P_A$ for all $k \geq 2$. Therefore, if $A \in \mathbb{Z}_p^{n\times t}$ and rank($A$)$= t$, then $A\,A^{\dagger} \in \mathbb{Z}_p^{n\times n}$ is an orthogonal projector. Figure 2 shows how the orthogonal projector $P_A$ can be used to project a vector $v$ onto the column space of matrix $A$.

The Moore-Penrose pseudoinverse is a very useful technique used in many engineering fields such as error correction, identification, control design, and structural dynamics. For an over-determined system of linear equations without solution, the Moore-Penrose pseudoinverse finds the least squares solution (i.e., projection of the solution onto the range space of the coefficient matrix of the system). It is also helpful to find the infinite set of solutions in the range space of under-determined set of equations (i.e., fewer constraints than unknowns). The computation of the Moore-Penrose pseudoinverse of a homogenous system of $t$ linear equations with $n$ unknowns (e.g., the computation of the pseudoinverse of matrix $A^{\perp} \in \mathbb{Z}_p^{t\times n}$) is hence a valid alternative for the construction of our proactive threshold secret sharing.

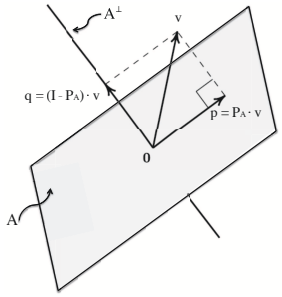



FIGURE 2
Orthogonal Projection of a Vector $v$ onto the Subspace Spanned by the Column Vectors of Matrix $A$.

### 3.1 Basic (*t*,*n*)-Threshold Secret Sharing Scheme Based on the Invariance Property of Orthogonal Projectors

Orthogonal projectors have already been used for the construction of threshold secret sharing schemes. In [28, 29], for example, the invariance property of orthogonal projectors is used for the redundant storage of computer images. Indeed, an asynchronous proactive (*t*,*n*)-threshold secret sharing scheme can be constructed based on the same observation — meaning that the invariance property of orthogonal projectors can be used to allow shareholders to renew their share without synchronization with other parties and without altering the secret. The key idea of the proposed approach is that the orthogonal projector $P_A$ computed from Equation (4) and a random matrix $A \in \mathbb{Z}_p^{n\times t}$ with rank $t$ is always equivalent to the projector $P_B$ obtained from the same equation and any $t$ independent random range images spanned from $A$.

Before going any further, let us start with a simple example that depicts the basic idea of our approach. It exemplifies the construction of a $(2,3)$-threshold, non-proactive yet, cryptosystem; and the reconstruction process by three independent reconstruction processes. Given two matrices $A \in \mathbb{Z}_{31}^{3\times 2}$, $X \in \mathbb{Z}_{31}^{2\times 3}$,

$$A = \begin{bmatrix} 7 & 13 \\ 6 & 29 \\ 13 & 28 \end{bmatrix} \quad X = \begin{bmatrix} 12 & 9 & 13 \\ 26 & 13 & 7 \end{bmatrix}$$

such that $A$ is a random matrix composed of two linearly independent column vectors $a_1, a_2 \in \mathbb{Z}_{31}^{3\times 1}$, i.e., rank($A$) is equal to 2; and $X$ is a random matrix composed of three linearly independent column vectors $x_1, x_2, x_3 \in \mathbb{Z}_{31}^{2\times 1}$, i.e., rank($X$) is equal to 3. Note that we simplify the notation, assuming $A = [a_1, a_2, \ldots, a_t]$, where each $a_i$ is the $i$-th column vector of matrix $A$; and $X = [x_1, x_2, \ldots, x_n]$ where each $x_i$ is the $i$-th column vector of matrix $X$. Let

$$A' \in \mathbb{Z}_{31}^{3\times 3} = \begin{bmatrix} 19 & 15 & 27 \\ 20 & 28 & 2 \\ 16 & 16 & 24 \end{bmatrix}$$

be the resulting matrix obtained by multiplying matrices $A$ and $X$. We assume hereafter that the column vectors $a'_1$, $a'_2$, and $a'_3$ in matrix $A'$ are indeed the shares of our cryptosystem; and that $P_A \in \mathbb{Z}_{31}^{3\times 3}$ is the secret of the cryptosystem, in which $P_A$ is the orthogonal projector obtained by applying Equation (4) to matrix $A$.

Let us now assume that a distribution process $\delta$ disseminates the shares $a'_1, a'_2, a'_3 \in A'$ to three independent shareholders $\alpha$, $\beta$, and $\gamma$. We define the following three column vectors:

$$V_\alpha = \begin{bmatrix} 19 \\ 20 \\ 16 \end{bmatrix}, \quad V_\beta = \begin{bmatrix} 15 \\ 28 \\ 16 \end{bmatrix}, \quad V_\gamma = \begin{bmatrix} 27 \\ 2 \\ 24 \end{bmatrix}$$

as the corresponding shares held respectively by $\alpha$, $\beta$, and $\gamma$. We also assume that a reconstruction process $\rho_1$ requests to shareholders $\alpha$ and $\beta$ their respective shares (notice that our example describes a $(2,3)$-threshold cryptosystem and so only two shares suffice to reconstruct the secret). A second reconstruction process $\rho_2$ requests to shareholders $\alpha$ and $\gamma$ their respective shares. Finally, a third reconstruction process $\rho_3$ requests to shareholders $\gamma$ and $\beta$ their shares. Processes $\rho_1$, $\rho_2$, and $\rho_3$ build, independently, three reconstruction matrices $B_1$, $B_2$, and $B_3$ (by simply joining the share vectors they collected from each shareholder):

$$B_1 = \begin{bmatrix} 19 & 15 \\ 20 & 28 \\ 16 & 16 \end{bmatrix}, \quad B_2 = \begin{bmatrix} 19 & 27 \\ 20 & 2 \\ 16 & 24 \end{bmatrix}, \quad B_3 = \begin{bmatrix} 27 & 15 \\ 2 & 28 \\ 24 & 16 \end{bmatrix}$$

We can now observe that the orthogonal projector obtained by applying Equation (4) to either $B_1$, $B_2$, or $B_3$ is equivalent to the orthogonal projector obtained by applying Equation (4) to matrix $A$:

$$P_A = \begin{bmatrix} 27 & 13 & 11 \\ 13 & 23 & 21 \\ 11 & 21 & 14 \end{bmatrix}, \; P_{B_1} = P_{B_2} = P_{B_3} = \begin{bmatrix} 27 & 13 & 11 \\ 13 & 23 & 21 \\ 11 & 21 & 14 \end{bmatrix}$$

Therefore, the three processes $\rho_1$, $\rho_2$, $\rho_3$ may successfully reconstruct the secret (i.e., $P_A$) by performing the same operation described by Equation (4). The following theorem establishes the corretness of the approach for the general case.

**Theorem 1** *Let $A \in \mathbb{Z}_p^{n \times t}$ be a random matrix of rank $t$. Let $A' \in \mathbb{Z}_p^{n \times n}$ be the result of multiplying matrix $A$ with a set of $n$ linearly independent column vectors $x_1, x_2, \ldots, x_n \in \mathbb{Z}_p^{t \times 1}$, i.e., $A' = Ax_i \pmod p \; \forall x_i \in [x_1, x_2, \ldots, x_n]$. Let*

*B be any submatrix from $A'$ with exactly t column vectors. Then, the orthogonal projectors $P_A$ and $P_B$ derived from Equation (4) are identical.*

**Proof** Note that $P_A = A\ A^{\dagger}$ and $P_B = B\ B^{\dagger}$ are the orthogonal projectors obtained by applying Equation (4) to both $A$ and $B$. Since $B$ is any submatrix derived from $A'$ with exactly $t$ column vectors, we can also denote $B$ as the resulting matrix obtained by multiplying $A \in \mathbb{Z}_p^{n\times t}$ times a given matrix $X \in \mathbb{Z}_p^{t\times t}$. Therefore, $P_B = B\ B^{\dagger}$ is equal to $P_B = (A\ X)(A\ X)^{\dagger}$ and so to $P_B = A\ X\ X^{\dagger}\ A^{\dagger}$. We know from Equation (1) that $X^{\dagger} = X^{-1}$ when $X$ is a square matrix. Therefore, $P_B = A\ X\ X^{-1}\ A^{\dagger}$. Since matrix $X$ gets cancelled, we obtain that $P_B = A\ A^{\dagger}$ and so identical to $P_A$. □

### 3.2 Efficiency

The efficiency of a secret sharing scheme can be evaluated in terms of the information entropy of its shares and secret of the cryptosystem [30]. A secret sharing scheme is said to be perfect if it holds that the entropy of the shares is greater that or equal to the entropy of the secret. As a consequence, the size of each share of a perfect secret sharing scheme must be equal or greater than the size of the secret. This is an inconvenient to the hardware limitations of the RFID model discussed in Section 2.2. RSS may considerably improve this efficiency, by allowing a trade-off between security and size of the shares [31]. This is the case of the approach presented in the previous section (cf. Section 3.1). Notice that the size of each share $a'_i \in A'$ of our construction is considerably smaller than the size of the secret $P_A$. More precisely, every share $a'_i$ is a column vector in $\mathbb{Z}_p^{n\times 1}$, while the size of the secret is a matrix in $\mathbb{Z}_p^{n\times n}$, i.e., the size of every share is $n$ times smaller than the secret.

To analyze the robustness of a RSS scheme, in terms of its security, it is necessary to quantify the amount of information about the secret that an intermediate set of shares, smaller than the threshold $t$, may leak out. This leakage of secret information represents the size of the ramp, in which a small ramp provides stronger security to the scheme than a larger ramp. Yakamoto proposed in [32] to quantify the exposure of secret information from each share by defining a second threshold $t'$, where $0 < t' \leq t$. By definition, a qualified coalition of $t$ shares may reconstruct the secret. An unqualified coalition of $t - t'$ shares cannot reconstruct the secret, but leaks out information about it. Less than $t'$ shares may not reconstruct the secret and does not reveal any information about the secret. The amount of information leaked out from the secret by an unqualified coalition of $t - t'$ shares can be quantified in terms

of information entropy. Yakamoto proved in [32] that the security of a ramp secret sharing scheme is strong enough when the following equivalence applies:

$$H(S|C) \quad = \quad \frac{t-t'}{t} H(S), \tag{5}$$

in which $H(S)$ is the information entropy of the secret, and $C$ is an unqualified coaliation of $t-t'$ shares. We prove in the sequel that the security of the threshold cryptosystem presented in Section 3.1 is, according to [32], strong enough.

**Theorem 2** *Let $A \in \mathbb{Z}_p^{n\times t}$ be a random matrix of rank $t$. Let $P_A \in \mathbb{Z}_p^{n\times t}$ be the orthogonal projector obtained by applying Equation (4) to matrix A. Let $A' \in \mathbb{Z}_p^{n\times n}$ be the result of multiplying matrix A with a set of n linearly independent column vectors $x_1, x_2, \ldots, x_n \in \mathbb{Z}_p^{t\times 1}$. Then, the basic $(t,t',n)$-threshold secret sharing scheme constructed from the invariance property of the orthogonal projector $P_A$, in which matrix $P_A$ is the secret of the cryptosystem, and the column vectors $a'_1, a'_2, \ldots, a'_n \in A'$ are the shares of the cryptosystem, is equivalent to Equation (5).*

**Proof** Since the information provided by matrix $A$ derives $P_A$ by simply applying Equation (4), we know that $H(P_A|A) = 0$. Using some information entropy algebra manipulation, we can use this result to decompose $H(P_A)$ as

$$\begin{aligned} H(P_A) &= H(P_A|A) + H(A) - H(A|P_A) \\ &= H(A) - H(A|P_A) \end{aligned} \tag{6}$$

Notice that matrix $A$ is any full rank matrix chosen uniformly at random from the sample space in $\mathbb{Z}_p^{n\times t}$. It is proved in [33] that there are exactly $\prod_{i=0}^{t-1}(p^n - p^i)$ random matrices of rank $t$ in $\mathbb{Z}_p^{n\times t}$. Therefore, we can compute $H(A)$ as follows:

$$H(A) = \log_2 \left( \prod_{i=0}^{t-1} (p^n - p^i) \right) \tag{7}$$

Knowing $A$ and $P_A$ easily leads to $H(A|P_A)$. From Equations (3) and (4), we have that $P_A$ times $A$ is equivalent to $A$, meaning that $A$ is an eigenvector matrix of $P_A$. Hence, the decomposition of $P_A$ into $t$ eigenvectors $[v_1, v_2, \ldots, v_t] = V \in \mathbb{Z}_p^{n\times t}$ provides information about $A$. More precisely,

matrix $A$ can be obtained from $V$ by using a transformation matrix $W \in \mathbb{Z}_p^{t\times t}$. Since the sample space from which matrix $W$ can be uniformly chosen is exactly of size $\prod_{i=0}^{t-1}(p^t - p^i)$, we have that $H(A|P_A)$ can be obtained as follows:

$$H(A|P_A) = \log_2\left(\prod_{i=0}^{t-1}(p^t - p^i)\right) \tag{8}$$

Using Equations (7) and (8) we can now compute $H(P_A) = H(A) - H(A|P_A)$:

$$H(P_A) = \log_2\left(\prod_{i=0}^{t-1}(p^n - p^i)\right) - \log_2\left(\prod_{i=0}^{t-1}(p^t - p^i)\right) \tag{9}$$

Let us now quantify, in terms of entropy, the information about $P_A$ provided by an unqualified coalition $A'$ of $t'$ shares, s.t., $A' = [a'_1, a'_2, \ldots, a'_{t'}]$, and where $0 < t' < t$. Since matrix $A'$ can be seen as a random matrix of rank $t'$ chosen uniformly from the sample space $\prod_{i=0}^{t'-1}(p^n - p^i)$, we have that $H(A')$ can be denoted as follows:

$$H(A') = \log_2\left(\prod_{i=0}^{t'-1}(p^n - p^i)\right) \tag{10}$$

Matrix $A'$ is also an eigenvector matrix of $P_A$. The decomposition of $P_A$ into $t$ eigenvectors $[v_1, v_2, \ldots, v_t] = V \in \mathbb{Z}_p^{n\times t}$ provides information about $A'$. Indeed, matrix $A'$ can be obtained from $V$ by using a transformation matrix $W' \in \mathbb{Z}_p^{t\times t'}$. Since the sample space from which matrix $W'$ can be uniformly chosen is exactly of size $\prod_{i=0}^{t'-1}(p^t - p^i)$, we have that $H(A'|P_A)$ can be obtained as follows:

$$H(A'|P_A) = \log_2\left(\prod_{i=0}^{t'-1}(p^t - p^i)\right) \tag{11}$$

We can quantify the amount of information about $P_A$ provided by $A'$, i.e., $H(P_A|A')$, using the results from Equations (9), (10), and (11):

$$\begin{aligned} H(P_A|A') &= H(P_A) - H(A') + H(A'|P_A) \\ &= \log_2\left(\prod_{i=0}^{t-1}(p^n - p^i)\right) - \log_2\left(\prod_{i=0}^{t-1}(p^t - p^i)\right) - \\ &\log_2\left(\prod_{i=0}^{t'-1}(p^n - p^i)\right) + \log_2\left(\prod_{i=0}^{t'-1}(p^t - p^i)\right) \end{aligned} \tag{12}$$

When $p$ is a large number, we can simplify the logarithmic expressions in Equations (9) and (12) to derive $H(P_A)$ and $H(P_A|A')$ as the following approximations:

$$\begin{aligned} H(P_A) &\approx t(n-t)\ \log_2\ p \\ H(P_A|A') &\approx (t-t')(n-t)\ \log_2\ p \end{aligned}$$

We observe that the information entropy of $P_A$, knowing $A'$, is approximatively $\frac{t-t'}{t}$ times the information entropy of $P_A$:

$$H(P_A|A') \approx \frac{t-t'}{t}\, H(P_A), \tag{13}$$

which, according to Equation (5) provided in [32], guarantees that the security of the ramp threshold secret sharing scheme is strong enough. □

Let us conclude this section by determining a value of $t$, in terms of $n$, that guarantees that $t-1$ shares cannot reconstruct the secret. Given that the secret is the orthogonal projection $P_A$ derived from the computation of Equation (4) and matrix $A$, and observing again that the projection of $A$ onto the subspace spanned by its range space remains in the same place, i.e., $P_A \cdot A = A$, it is therefore trivial to observe that the projection of any share onto the same subspace does not change either. This effect can be used by a malicious adversary in order to discover $P_A$ by solving $n$ consecutive equations of $(t-1)$ shares. Since, by definition, a $(t,n)$-threshold secret sharing scheme must prevent any coalition of less than $t$ shares from reconstructing the secret, the parameter $t$ of our construction shall be bounded in terms of $n$ as follows:

$$\begin{aligned} (t-1)n &< \frac{n(n+1)}{2} - 1, \\ t &< \frac{3+n}{2} \end{aligned} \tag{14}$$

From Theorems 1 and 2, we conclude that if $t < \frac{3+n}{2}$, the scheme presented in Section 3.1 is a strong ramp threshold secret sharing scheme in which exactly $t$ shares may reconstruct the secret, but $t-1$ or fewer shares cannot.

### 3.3 Pseudo-Proactive Threshold Secret Sharing Scheme Based on the Invariance Property of Orthogonal Projectors and Multiplicative Noise for the Renewal of Shares

We significantly improve in this section the results presented in Section 3.1 by showing that the introduction of multiplicative noise in the coefficients of

matrix $A'$ does not affect the reconstruction phase. By multiplicative noise we assume independent scalar multiplication of column vector shares $a'_i \in A'$ and scalar random numbers $r_1, \ldots, r_k$ for stretching these vectors. Indeed, we show that the introduction of multiplicative noise into the column vectors of any reconstruction matrix $B_i$ obtained from $t$ column vectors in $A'$ does not affect the results.

The following example shows the key idea of this new version. Assuming again a $(2,3)$-threshold secret sharing scheme based on the orthogonal projectors of matrices $A \in \mathbb{Z}_{31}^{3\times 2}$, $X \in \mathbb{Z}_{31}^{2\times 3}$, and $A' = AX \in \mathbb{Z}_{31}^{3\times 3}$:

$$A = \begin{bmatrix} 7 & 13 \\ 6 & 29 \\ 13 & 28 \end{bmatrix}, X = \begin{bmatrix} 12 & 9 & 13 \\ 26 & 13 & 7 \end{bmatrix}, A' = \begin{bmatrix} 19 & 15 & 27 \\ 20 & 28 & 2 \\ 16 & 16 & 24 \end{bmatrix}$$

If we now generate three matrices $B_1$, $B_2$, and $B_3$ as combinations of vector columns from $A' = [a'_1, a'_2, a'_3]$ and multiplicative noise, such as $B_1 \in \mathbb{Z}_{31}^{3\times 2} = [5 \cdot a'_1, 17 \cdot a'_2]$ $(mod\ 31)$, $B_2 \in \mathbb{Z}_{31}^{3\times 2} = [7 \cdot a'_1, 13 \cdot a'_3]$ $(mod\ 31)$, and $B_3 \in \mathbb{Z}_{31}^{3\times 2} = [9 \cdot a'_3, 22 \cdot a'_2]$ $(mod\ 31)$:

$$B_1 = \begin{bmatrix} 2 & 7 \\ 7 & 11 \\ 18 & 24 \end{bmatrix}, \quad B_2 = \begin{bmatrix} 9 & 10 \\ 16 & 26 \\ 19 & 2 \end{bmatrix}, \quad B_3 = \begin{bmatrix} 26 & 20 \\ 18 & 27 \\ 30 & 11 \end{bmatrix}$$

we can still observe that the orthogonal projectors obtained by applying Equation (4) to either $B_1$, $B_2$, or $B_3$ are certainly equivalent to the orthogonal projector obtained by applying Equation (4) to matrix $A$:

$$P_A = \begin{bmatrix} 27 & 13 & 11 \\ 13 & 23 & 21 \\ 11 & 21 & 14 \end{bmatrix}, P_{B_1} = P_{B_2} = P_{B_3} = \begin{bmatrix} 27 & 13 & 11 \\ 13 & 23 & 21 \\ 11 & 21 & 14 \end{bmatrix}$$

Theorem 1 also applies in the general case of this new approach. Notice that if $A \in \mathbb{Z}_p^{n\times t}$ is a random matrix of rank $t$, and $A' \in \mathbb{Z}_p^{n\times n}$ is the result of multiplying matrix $A$ with $n$ linearly independent column vectors $x_1, x_2, \ldots, x_n \in \mathbb{Z}_p^{t\times 1}$, i.e., $A' = Ax_i$ $(mod\ p)$ $\forall x_i \in [x_1, x_2, \ldots, x_n]$; then, any submatrix $B$ derived from exactly $t$ column vectors in $A'$, but streched by multiplicative noise, can still be factorized as $B = A\,X'$, where $X' \in \mathbb{Z}_p^{t\times t}$ is a square random matrix resulting from the set of $t$ linearly independent column vectors in $X$, but

stretched by a specific scaling random number $r$ modulo $p$. We know from Equation (1) that $(X')^{\dagger} = (X')^{-1}$ when $X'$ is square. Therefore, $X'$ gets cancelled during the reconstruction phase, i.e., $P_B = A\ X'\ (X')^{-1}\ A^{\dagger}$, and we obtain that $P_B = P_A = A\,A^{\dagger}$.

### 3.4 Proactive Threshold Secret Sharing Scheme Based on the Invariance Property of Orthogonal Projectors and Both Multiplicative and Additive Noise for the Renewal of Shares

We have seen in the previous section that every share in the set of shares derived from matrix $A'$ can be independently transformed by adding multiplicative noise, and so generating numerically different shares, but still guaranteeing the invariance property of orthogonal projectors to always reconstruct the initial secret (i.e., the orthogonal projector $P_A$ derived from matrix $A$). However, even if the new shares are numerically different, any malicious adversary can successfully observe that the shares are always linearly dependent, since the transformation process is simply stretching the initial share by some scaling random factor $r$.

We solve this problem by combining both multiplicative and additive noise in the transformation process. The only requirement is to provide to the process in charge of reconstructing the secret a reference used in the transformation process. We assume that this reference is the last column vector in matrix $A'$. We also assume that the generation process in charge of the construction of $A'$ guarantees that the last column vector is an un-ordered collection of distinct elements. Then, shareholders are given access to this reference to renew their shares with a linear combination of this reference column. Note that this reference column must be also known a priori by the reconstruction process, but not by any malicious adversary that has access to the renewed shares. Let us illustrate with an example the key idea of this version. Assuming a $(2,3)$-threshold secret sharing scheme based on matrices $A \in \mathbb{Z}_{31}^{3\times 2}$, $X \in \mathbb{Z}_{31}^{2\times 3}$, and $A' \in \mathbb{Z}_{31}^{3\times 3} = Ax_i\ (mod\ p)\ \forall x_i \in X$:

$$A = \begin{bmatrix} 7 & 13 \\ 6 & 29 \\ 13 & 28 \end{bmatrix},\ X = \begin{bmatrix} 12 & 9 & 13 \\ 26 & 13 & 7 \end{bmatrix},\ A' = \begin{bmatrix} 19 & 15 & \mathbf{27} \\ 20 & 28 & \mathbf{2} \\ 16 & 16 & \mathbf{24} \end{bmatrix}$$

Every shareholder is given column $a'_3$ and either column $a'_1$ or column $a'_2$. Let us assume two shareholders $\alpha$ and $\beta$ in the system, each holding one of

the following two share pairs $V_\alpha$ and $V_\beta$:

$$V_\alpha = \begin{bmatrix} 19 & \mathbf{27} \\ 20 & \mathbf{2} \\ 16 & \mathbf{24} \end{bmatrix}, \quad V_\beta = \begin{bmatrix} 15 & \mathbf{27} \\ 28 & \mathbf{2} \\ 16 & \mathbf{24} \end{bmatrix}$$

Let us assume that a reconstruction process $\rho_1$ requests to each shareholder their share combination. Both $\alpha$ and $\beta$ return to $\rho_1$ a linear transformation from the column vectors in their share pairs. Shareholder $\alpha$ generates a random value $r_\alpha = 15$, transforms $v_{\alpha 1}$ into $v_{\alpha 1} \cdot 15 \ (mod 31)$, and returns $b_\alpha \in \mathbb{Z}_{31}^{3\times 1} = v_{\alpha 1} + v_{\alpha 2}$. Similarly, $\beta$ generates a random value $r_\beta = 14$, transforms $v_{\beta 1}$ into $v_{\beta 1} \cdot 14 \ (mod 31)$ and returns $b_\beta \in \mathbb{Z}_{31}^{3\times 1} = v_{\beta 1} + v_{\beta 2}$. Two other reconstruction processes $\rho_2$ and $\rho_3$ request to each share holder their shares. Shareholders $\alpha$ and $\beta$ return to $\rho_2$ and $\rho_3$ two different linear combinations from the column vectors in their share pairs. Shareholder $\alpha$ returns $b'_\alpha \in \mathbb{Z}_{31}^{3\times 1} = 28 \cdot v_{\alpha 1} + v_{\alpha 2}$ to process $\rho_2$, and $b''_\alpha \in \mathbb{Z}_{31}^{3\times 1} = 5 \cdot v_{\alpha 1} + v_{\alpha 2}$ to process $\rho_3$. Shareholder $\beta$ returns $b'_\beta \in \mathbb{Z}_{31}^{3\times 1} = 19 \cdot v_{\beta 1} + v_{\beta 2}$ to process $\rho_2$, and $b''_\beta \in \mathbb{Z}_{31}^{3\times 1} = 21 \cdot V_{\beta 1} + V_{\beta 2}$ to process $\rho_3$. Finally, the process $\rho_1$ assembles with $b_\alpha, b_\beta$ the reconstruction matrix $B_1 \in \mathbb{Z}_{31}^{3\times 2}$; the process $\rho_2$ builds with $b'_\alpha, b'_\beta$ the reconstruction matrix $B_2 \in \mathbb{Z}_{31}^{3\times 2}$; and the process $\rho_3$ produces with $b''_\alpha, b''_\beta$ the reconstruction matrix $B_3 \in \mathbb{Z}_{31}^{3\times 2}$:

$$B_1 = \begin{bmatrix} 2 & 20 \\ 23 & 22 \\ 20 & 0 \end{bmatrix}, \quad B_2 = \begin{bmatrix} 9 & 18 \\ 1 & 10 \\ 17 & 2 \end{bmatrix}, \quad B_3 = \begin{bmatrix} 30 & 24 \\ 28 & 15 \\ 20 & 27 \end{bmatrix}$$

We observe that the orthogonal projectors obtained by applying Equation (4) to matrices $B_1$, $B_2$, and $B_3$ are identical to the orthogonal projector obtained by applying Equation (4) to matrix $A$:

$$P_A = \begin{bmatrix} 27 & 13 & 11 \\ 13 & 23 & 21 \\ 11 & 21 & 14 \end{bmatrix}, \ P_{B_1} = P_{B_2} = P_{B_3} = \begin{bmatrix} 27 & 13 & 11 \\ 13 & 23 & 21 \\ 11 & 21 & 14 \end{bmatrix}$$

Notice that each matrix $B_i = [b_{i1}, b_{i2}]$, s.t. $i \in \{1 \ldots 3\}$, can be decomposed as follows:

$$B_i \quad = \quad \left[ r_\alpha \cdot a'_1 + a'_3 \ , \ r_\beta \cdot a'_2 + a'_3 \right]$$

$$
\begin{aligned}
&= \left[r_\alpha \cdot Ax_1 + Ax_3 \ , \ r_\beta \cdot Ax_2 + Ax_3\right] \\
&= \left[A\ (r_\alpha \cdot x_1 + x_3) \ , \ A\ (r_\beta \cdot x_2 + x_3)\right] \\
&= \left[A\ x'_1 \ , \ A\ x'_2)\right] = A\ X'_i \qquad (15)
\end{aligned}
$$

in which $r_\alpha$ and $r_\beta$ are the random factors introduced by each shareholder on every interrogation as multiplicative noise; and $X'_i \in \mathbb{Z}_{31}^{2\times 2}$ is a random full rank square matrix derived from $A'$, and so from $A\ X$, plus the multiplicative and additive noise introduced by the shareholders on every interrogation. Since matrix $X'_i$ is a square matrix, the equivalence defined in Equation (1) applies, i.e., $X_i^{\dagger} = X_i^{-1}$. Therefore, the computation of any orthogonal projector $P_{Bi}$ based on Equation (4) cancels matrix $X'_i$ and so $P_{Bi}$ is always identical to matrix $P_A$. This establishes the general case of the new approach based on the proof of Theorem 1.

Let us also observe that if processes $\rho_1$, $\rho_2$, and $\rho_3$ are executed by a qualified entity $\Psi_1$ with knowledge of reference $a'_3$, the returned set of column vectors $b_\alpha$, $b'_\alpha$, $b''_\alpha$, and so forth, are clearly linked:

$$
b_\alpha = \begin{bmatrix} 2 \\ 23 \\ 20 \end{bmatrix}, b'_\alpha = \begin{bmatrix} 9 \\ 1 \\ 17 \end{bmatrix} = r_1 b_\alpha + \begin{bmatrix} 27 \\ 2 \\ 24 \end{bmatrix}, \ldots
$$

Conversely, if we assume that processes $\rho_1$, $\rho_2$, and $\rho_3$ were executed by a malicious adversary $\Psi_2$ who is trying to link the shares returned by either $\alpha$ or $\beta$, for tracking purposes, but not having access to the column vector reference $a'_3$, the returned set of column vectors $b_\alpha$, $b'_\alpha$, and $b''_\alpha$, as well as column vectors $b_\beta$, $b'_\beta$, and $b''_\beta$, are viewed as unlinked.

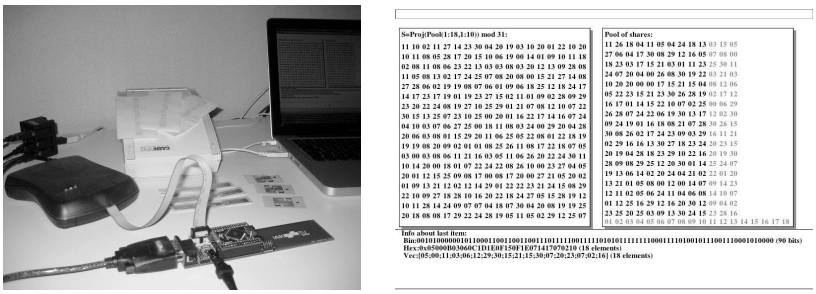
## 4 SIMULATION AND EXPERIMENTAL RESULTS

In Section 3, we have seen the formalization of our proposal for the reconstruction of a pre-distributed secret once a sufficient number of shares are collected. We present in this section the results obtained with an experimental setup that simulates EPC Gen2 adapted shares generation and reconstruction of secrets. Our prototype system allows to experiment the exchange of shares with a regular EPC Gen2 reader and simulated Gen2 tags. The objective of this setup is to demonstrate the practical viability of our proposal.

### 4.1 Experimental Setup

Figure 3 pictures our experimental setup. It is based on the execution of standard EPC Gen2 inventory queries, but enabled with TIDs that are enhanced by our proposed threshold cryptosystem, between a regular EPC Gen2 reader and several Gen2 tag instances simulated by the IAIK UHF demo tag [34]. The IAIK UHF demo tag is a programmable device intended for developing new extensions to the EPC Gen2 standard. The demo tag consists of an antenna, an RF front-end, a programmable microcontroller, and a firmware library. The antenna captures the energy emitted by the reader and powers up the RF front-end of the tag. The RF front-end demodulates the information encoded in the signal. The encoded data is processed by the programmable microcontroller to compute a response. To compute the response, the programmable microcontroller executes a software implementation of the EPC Gen2 protocol, implemented in the firmware library. The response is then modulated by the RF front-end and backscattered to the reader. More details can be obtained in [34, 35].

Our share renewal scheme has been implemented in ANSI C using the Crossworks IDE for AVR from Rowley Associates [36]. The theoretical construction detailed in Section 3 has been adapted to be executed over the Atmel AVR ATmega128 [37] microcontroller of the IAIK UHF demo tag. The ATmega128 is an 8-bit microcontroller based on the AVR architecture. It has




(a) (b)

FIGURE 3
Experimental Setup. In (a), we can see the CAEN A829EU Reader, the AVR JTAG MKII Programmer, the IAIK Graz UHF Demo Tag, and some regular EPC Gen2 tags. In (b), we can see the Java graphical front end that summarizes the process of collecting the secret shares and reconstruction of secrets.

32 registers of 8-bits that can act as the destinations of standard arithmetic operations. In addition, the ATmega128 microcontroller contains 128KB of flash memory and 4KB of data memory that can be addressed by three independent registers of 16-bits. Since the response of inventory queries is a mandatory operation specified in the EPC Gen2 protocol, an existing response function implemented for the ATmega128 microcontroller is already included in the original firmware stored on the IAIK UHF demo tag. By using the Crossworks IDE, we code and merge the new functionality with the general firmware library to adapt the existing inventory response process to the renewal scheme of shares. The AVR JTAG MKII programmer [37] is used to transfer and to debug the updated firmware merged with the adapted inventory routine. On the reader side, the short-range reader CAEN A829EU [38] emits the inventory queries. The reader is controlled by a back end computer over a USB serial port and a Java application. The Java application is in charge of generating the inventory queries and processing the reconstruction of secrets.

### 4.2 Collection of Shares and Reconstruction Rates

Four different populations of EPC Gen2 tags are simulated and tested. All four simulations are built according to the item-level inventory scenarios reported in [5, 24]. Our objective is to show how our construction can be used in order to maximize the item traceability rate at the upper levels of a supply chain, i.e., at the manufacturer, distributor and retailer sides, while minimizing the traceability rate at the lower levels of a supply chain, i.e., at the consumer side. The study presented in [5] shows that items that are initially assembled and tagged together within large collections at the manufacturer side, i.e., top level of the supply chain, get progressively dispersed into very small subsets when they reach the bottom level of the supply chain, i.e., the consumer side. Two appropriate item examples analyzed in [5] are personal hygiene tools and pharmaceuticals products. According to [5], personal hygiene tools like, for instance, razor blades, are initially assembled and tagged together at the manufacturer side of the supply chain in large populations of more than 6,000 tagged items. They are later dispersed in the supply chain until being picked up by consumers in groups of less that five items. Similarly, for pharmaceutical items assembled initially in large quantities of more than 7,000 tagged items at the manufacturer side, we should only expect that no more than six items from the initial population can end in possession of a single consumer at the same time. In accordance with these observations,

we simulate four different populations of EPC Gen2 tagged items. The tags of each population are initialized with four independent sets of secret sharing schemes constructed according to our proactive threshold secret sharing scheme in GF($2^5$–1). More precisely, we initialize the tags of the first population with a $(13, 24)$ scheme that produces tag inventory responses of 120 bits; the tags of the second population with a $(10, 18)$ scheme that produces tag inventory responses of 90 bits; the tags of the third population with a $(7, 12)$ scheme that produces tag inventory responses of 60 bits; and the tags of the fourth population with a $(5, 8)$ scheme that produces tag inventory responses of 40 bits.

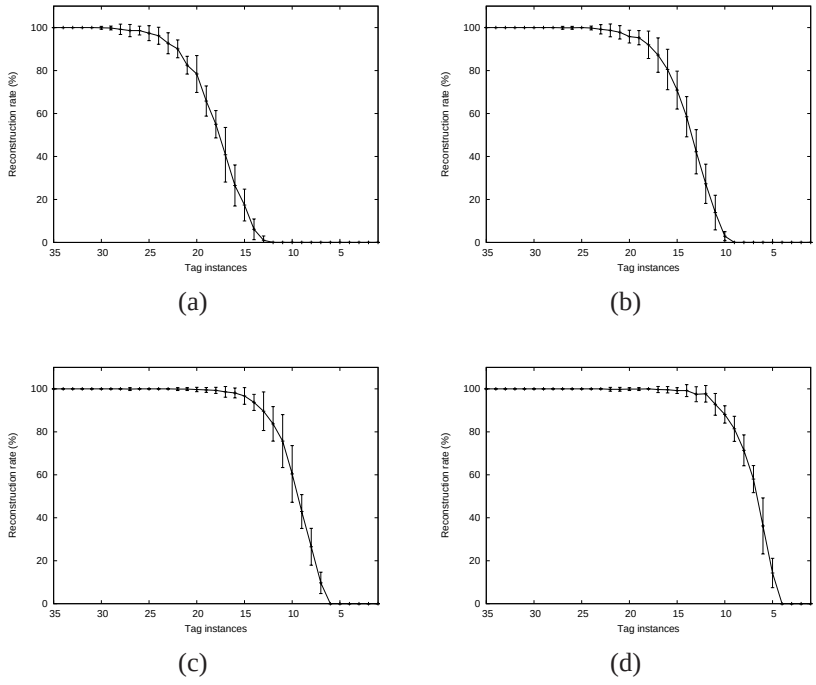



FIGURE 4
Simulation results. (a) First population results with a (13,24) proactive threshold secret sharing scheme of shares; (b) second population results with a (10,18) scheme; (c) third population results with a (7,12) scheme; (d) fourth population results with a (5,8) scheme.

Figure 4(a)—(d) pictures the average and the 95% confidence intervals of the reconstruction rates obtained with the collection of less than 35 shares from each simulated population. We recall that these simulations take into account the evaluation reported in [5]. We, therefore, consider the upper bounds of five to thirteen items as the sizes of groups of items picked up by consumers (i.e., lower level of a supply chain). Above these bounds, it is straighforward that authorized readers at the store, warehouse or manufacturer facilities will always reach the necessary threshold to reconstruct the secret and access the appropriate TIDs. For each experimental test of each population, the inventory query emitted by the EPC Gen2 reader is responded by exactly $m$ random tags, where $35 < m < 0$. We recall that the use of a ($t$,$n$) scheme means that of the $n$ available shares, we need to collect, at least, $t$ different shares to successfully reconstruct the distributed secret. Each population of tags is initialized by randomly allocating shares from each of threshold scheme. Each interrogation is executed 100 times with random series of simulated tags. The results we show are therefore the average and 95% confidence intervals computed after each series of interrogations.

The results confirm that while the reconstruction rate minimizes the traceability of tagged items as soon as these items get dispersed in small quantities on the consumer side (amount of tagged items below quantities of less than twenty tags), it guarantees the identification of these items at the upper levels of the supply chain (amount of tagged items above quantities of more than thirty tags). From these results, we may also conclude that the compact size of shares of all four schemes are appropriate enough to fit on the inventory responses suggested on the EPC standard. Note that the resulting inventory responses that are containing the shares (i.e., 120 bits for the first population; 90 bits for the second population; 60 bits for the third population; and 40 bits for the fourth population) do successfully fit within the maximum response size of 528 bits suggested by EPCglobal in [2].

## 5 CONCLUSIONS

We presented a proactive secret sharing procedure to provide consumer privacy and distribution of secrets. Our solution addresses the eavesdropping, rogue scanning, and tracking threats. The main properties of our approach are: (1) low-cost share renewal with secret preservation and without a need of synchronization; (2) compact size of shares; (3) secret sharing construction that guarantees strong security; (4) reconstruction of a secret does not require

the identity of the shareholders. We have also presented the implementation of a practical experiment with our proposed cryptosystem in a real EPC Gen2 scenario. By means of a compatible Gen2 reader, and a programmable Gen2 tag implementing our proactive share renewal process, we have shown that a standard EPC Gen2 reader can reconstruct an appropriate pre-disctributed secret dispersed over a set of Gen2 tags. The set of tags communicate the renewed shares to the reader by using a standard inventory response operation, enhanced by our proposed proactive share renewal.

**Acknowledgments —** This work has been supported by the Natural Sciences and Engineering Research Council of Canada (NSERC), the Mathematics of Information Technology and Complex Systems (MITACS), the Spanish Ministry of Science (grants TSI2007-65406-C03-03 E-AEGIS and CONSOLIDER-INGENIO 2010 CSD-2007-00004 ARES), and the Institut TELECOM (*Futur et Ruptures* program). We would also like to thank J. Melia-Segui and J. Herrera-Joancomarti for fruitful discussions on the experimental setup used in Section 4.

## REFERENCES

[1] J. Garcia-Alfaro, M. Barbeau, and E. Kranakis. (March 2009). A Proactive Threshold Secret Sharing Scheme Handling Gen2 Privacy Threats. Technical Report.

[2] EPCglobal. (2005). EPC Radio-frequency Identity Protocols Class-1 Generation-2 UHF. RFID Protocol for Communications at 860-960 MHz. http://epcglobalinc.org/standards/

[3] A. Juels. (2006). RFID Security and Privacy: A Research Survey. In: *IEEE Journal on Selected Areas in Communications*, 24(2):381–394. IEEE.

[4] J. Garcia-Alfaro, M. Barbeau, and E. Kranakis. (May 2008). Analysis of Threats to the Security of EPC Networks. In: *Proceedings of the 6th IEEE Annual Conference on Communication Networks and Services Research (CNSR'08)*, pages 67–74. IEEE.

[5] EPCglobal. (2007). EPC Item Level Tagging Joint Requirements Group.

[6] E. D. Karnin, J. W. Greene, and M. E. Hellman. (1983). On Secret Sharing Systems. IEEE Trans. Inform. Theory, 29(1):35–41. IEEE.

[7] K. Takaragi, M. Usami, R. Imura, R. Itsuki, and T. Satoh. (2001). An Ultra Small Individual Recognition Security Chip. *IEEE Micro*, 21(6):43–49. IEEE.

[8] S. Weis, S. Sarma, R. Rivest, and D. Engels. (March 2004). Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems. In *International Conference on Security in Pervasive Computing*, volume 2802 of *Lecture Notes in Computer Science*, pages 454–469. Springer.

[9] M. Ohkubo, K. Suzuki, and S. Kinoshita. (September 2004). Efficient Hash-chain Based RFID Privacy Protection Scheme. In *International Conference on Ubiquitous Computing – Ubicomp, Workshop Privacy: Current Status and Future Directions*, Nottingham, England.

[10] G. Avoine and P. Oechslin. (2005). A Scalable and Provably Secure Hash Based RFID Protocol. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2005*, pages 110–114.

[11] D. Henrici and P. Müller. (March 2004). Hash-based Enhancement of Location Privacy for Radio-frequency Identification Devices Using Varying Identifiers. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2004*, pages 149–153. IEEE.

[12] D. Molnar and D. Wagner. (October 2004). Privacy and Security in Library RFID: Issues, Practices, and Architectures. In *Conference on Computer and Communications Security – ACM CCS*, pages 210–219. ACM.

[13] T. Dimitriou. (September 2005). A Lightweight RFID Protocol to Protect Against Traceability and Cloning Attacks. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm*. IEEE.

[14] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda. (2007). An Efficient Authentication Protocol for RFID Systems Resistant to Active Attacks. In *Emerging Directions in Embedded and Ubiquitous Computing*, volume 4809 of *Lecture Notes in Computer Science*, pages 781–794. Springer.

[15] A. J. Menezes, P.C. Van Oorschot, and S. A. Vanstone. (1997). *Handbook of Applied Cryptography*. CRC Press.

[16] J. Wolkerstorfer. (July 2005). Is Elliptic-Curve Cryptography Suitable to Secure RFID Tags? In *Ecrypt Workshop on RFID and Lightweight Crypto*.

[17] P. Cole and D. Ranasinghe, editors. (2008). *Networked RFID Systems and Lightweight Cryptography — Raising Barriers to Product Counterfeiting*. Springer.

[18] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. (2006). An Elliptic Curve Processor Suitable for RFID-tags. In *Cryptology ePrint Archive, Report 2006/227*.

[19] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. (August 2004). Strong Authentication for RFID Systems Using the AES Algorithm. In *Workshop on Cryptographic Hardware and Embedded Systems – CHES 2004*, volume 3156 of *Lecture Notes in Computer Science*, pages 357–370. Springer.

[20] J. Daemen and V. Rijmen. (2002). *The Design of Rijndael: AES–the Advanced Encryption Standard*. Springer.

[21] M. Langheinrich and R. Marti. (2007). RFID Privacy Using Spatially Distributed Shared Secrets. In *4th International Symposium of Ubiquitous Computing Systems*, volume 4836 of *Lecture Notes in Computer Science*, pages 1–16. Springer.

[22] M. Langheinrich and R. Marti. (2007). Practical Minimalist Cryptography for RFID Privacy. *IEEE Systems Journal*, 1(2):115–128. IEEE.

[23] A. Shamir. (1979). How to Share a Secret. In Commun. of the ACM, 22(11):612–613.

[24] A. Juels, R. Pappu, and B. Parno. (2008). Unidirectional Key Distribution Across Time and Space with Applications to RFID Security. In *USENIX Security Symposium*. USENIX.

[25] A. Juels and S. Weis. (2007). Defining Strong Privacy for RFID. In *5th Annual IEEE International Conference on Pervasive Computing and Communications*, pages 342–347. IEEE.

[26] C. D. Meyer. (2000). Matrix Analysis and Applied Linear Algebra. SIAM, Society for Industrial and Applied Mathematics.

[27] R. Penrose. (1955). A Generalized Inverse for Matrices. In *Proceedings of the Cambridge Philosophical Society*, 51:406–413.

[28] L. Bai. (2006). A Reliable (k,n)-Image Secret Sharing Scheme. 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'06), pages 31–36. IEEE.

[29] L. Bai. (2006). A Strong Ramp Secret Sharing Scheme Using Matrix Projection. In *2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*, pages 652–656.

[30] M. Iwamoto and H. Yamamoto. (2006). Strongly Secure Ramp Secret Sharing Schemes For General Access Structures In *Information Processing Letters*, 97(2):52–57. Elsevier.

[31] G. Blakley and C. Meadows. (1985). Security of Ramp Schemes. In *Advances in Cryptology: Proceedings of CRYPTO'84*, volume 196 of *Lecture Notes in Computer Science*, pages 242–268. Springer.

[32] H. Yamamoto. (1985). On Secret Sharing Systems Using (k,l,n)-threshold Scheme. In *IECE Trans.* J68-A (9), pages 945–952 (in Japanese); English transl. (1986), Electron. Comm. Japan Part I 69 (9), pages 46–54.

[33] T. Migler, K. E. Morrison, and M. Ogle. (2004). Weight And Rank Of Matrices Over Finite Fields. Arxiv preprint math/0403314.

[34] SIC, Stiftung Secure Information and Communication Technologies. UHF RFID Demo Tag. [On-line] `http://jce.iaik.tugraz.at/sic/products/rfid_components`

[35] M. Aigner *et al.* BRIDGE — Building Radio frequency IDentification for the Global Environment. Report on first part of the security WP: Tag security (D4.2.1). July 2007. [On-line] `http://www.bridge-project.eu/`

[36] Rowley Crossworks IDE. Crossworks v1.4 and v2.0 for AVR. [On-line] `http://www.rowley.co.uk/`

[37] Atmel Corporation. [On-line] `http://www.atmel.com/`

[38] CAEN RFID. [On-line] `http://www.caen.it/rfid`