A Proactive Threshold Secret Sharing Scheme Handling Gen2 Privacy Threats

Joaquin Garcia-Alfaro, Michel Barbeau, and Evangelos Kranakis
Carleton University, School of Computer Science, 5302 Herzberg Building,
1125 Colonel By Drive, Ottawa, Ontario, K1S 5B6, Canada

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

Abstract

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.

1 Introduction

The EPCglobal class-1 generation-2 (Gen2 for short) specification [1], approved as ISO18000-6C in [2], 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 consumer's purchase data. The readability of tag identification in the Gen2 protocol clearly violates consumer privacy. It 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 [1]. 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 lightweight alternatives that preserve consumer privacy while avoiding killing the tags. In this paper, we survey related works and present an original scheme for the construction of a threshold cryptosystem lightweight enough to be deployed on low-cost Gen2 systems. The scheme protects EPC tag data against access by malicious readers for eavesdropping, rogue scanning, and tracking purposes.

Tag Identification (TID) disclosure on the Gen2 Protocol

Security features on Gen2 tags are minimal [4]. They may basically protect message integrity via 16-bit Cyclic Redundancy Codes (CRC), and generate 16-bit pseudo random strings. Their memory, very limited, 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 [1]. Figure 1 shows the steps of the EPC Gen2 protocol for product inventory. In Step 1, reader queries the tag and selects one of the following options: *select*, *inventory*, or *access* [1]. 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 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. The reader replies to the tag in Step 3 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).

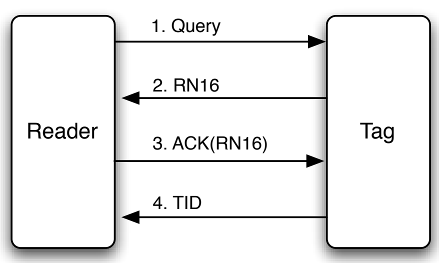

Figure 1. EPC Gen2 Inventory Protocol.

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 whole bunch of solutions have been proposed in the literature. Two solutions proposed in the literature rely on the use of cryptographic primitives to encrypt TID and the use of pseudonyms for the TID. Both solutions require that reader and tag share a common secret (either a key to decrypt the 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: adversary listening passively through the RF (Radio Frequency) communication between a tag and reader to access the Tag Identification (TID); (2) Rogue Scanning: adversary interacting actively with a tag to access the TID; (3) Tracking: adversary correlating RF communication to either passively or actively identify the same 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 for the same secret; (2) size of shares compact enough to fit into the memory of low-cost EPC Gen2 tags (e.g., 96 bits); (3) secret sharing construction that guarantees strong security; (4) reconstruction of the secret does not require the identity of the shareholders, e.g., the Gen2 tag identifiers. 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 closes the paper.

2 Related Work

The design and implementation of privacy-preserving mechanisms on Gen2 tags is gaining great attention in both industry and academia. The hardware and power constraints of Gen2 tags makes challenging the use of solutions based on traditional cryptography. The adoption of low-overhead procedures becomes the main approach to problems where traditional cryptography cannot be accomodated. We survey solutions and trends recently published in the literature.

2.1 Use of Traditional Cryptosystems

MAC (Message Authentication Code) based security protocols are among the first solutions discussed in the literature for securing low-cost RFID applications. In [6], 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 manufacturing chip 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 for 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 [7], 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 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 [8] the use of hash chains to allow on-tag evolution of identifiers. Avoine and Oechslin discuss in [9] 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 [10] some weaknesses in the lock-based schemes presented in [7, 8] and present an improved mechanism intended to enhance them. Several other improvements and lock-based protocols, most of them inspired on lightweight cryptography for devices such as smart cards, can be found in [11, 12, 13].

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, might exceed the constraints of low-cost Gen2 tags [1]. The implementation of these functions may require from seven thousand to over ten thousand logic gates; and from six hundred to over one thousand two hundred clock cycles [13]. 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) [14] for the implementation of one-way hash primitives on RFID tags has been studied in [15]. Its use of small key sizes is seen as very promising for providing an adequate level of computational security at a relatively low cost [16]. An ECC implementation for low-cost RFID tags can be found in [17]. In [18], on the other hand, Feldhofer et al. present a 128-bit implementation of the Advanced Encryption Standard (AES) [19] 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 is proposed by Langheinrich and Martin in [20, 21] as a key solution for addressing authentication in Gen2 scenarios (e.g., supply chain applications of the retail industry). The work presented in [20] simplifies the lookup process performed on back-end databases for identifying tags, while guaranteeing authentication. Tag identifiers, 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 [22].

The combination of shares at the reader side leads to the reconstruction of original tag identifiers. To prevent brute-force scanning from unauthorized reader — 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 [20], 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 [23]. They propose the use of a dispersion of secrets strategy, rather than the aggregation strategy used by Langheinrich and Marti. In this new approach, a secret used to encrypt Gen2 Tag Identifiers (TID) is split into multiple shares and distributed among multiple labelled objects. Their proposed construction and recombination of shares is based on a Ramp Secret Sharing scheme (RSS), 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. Privacy is achieved though the dispersion of secrets and encrypted identifiers. On the one hand, their dispersion helps to improve the authentication process between readers and tags, as tags move through a supply chain. Assuming that a given number of shares is necessary for readers to obtain the EPC data assigned to a pallet, for example, a situation where the number of shares obtained by readers is not sufficient to reach the threshold leads to conclude that unauthorized tags are present in the pallet. This dispersion increases the security of tags against unauthorized readers as well as they are dispersed outside the supply chain. Without the space proximity of other tags, an unauthorized reader cannot obtain the sufficient number of shares to identify the original tag identifier.

The main limitation that we see on this approach is that a critical privacy threat to consumers, such as the tracking threat defined in Section 1, is not addressed. This is indeed a requirement stated by most authors in the literature, such as Juels and Weis in [24], claiming that privacy-preserving solutions for RFID applications must guarantee both anonymity and untraceability. We show in the sequel that it is possible to improve these state-of-the-art privacy-preserving approaches based on secret sharing strategies by providing 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 Gen2

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

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

in which the vector columns of the coefficient matrix A associated to the system of linear equations are linearly independent, i.e., the coefficient 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.,

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

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:

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

in which $A^{\perp}$ denotes the transpose of matrix A. It can also be proved, cf. [25], 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 [26]:

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

For our specific construction, we are interested in showing that the resulting matrix $A^{\dagger}$ keeps the orthogonal projection property required in [26]. Indeed, we are interested in showing that the resulting matrix P_A computed as

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

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.

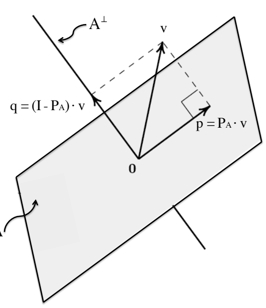

Figure 2. Orthogonal Projection of a Vector v onto the Subspace Spanned by the Column Vectors of Matrix A.

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.

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

Orthogonal projectors have already been used in the literature for the construction of threshold secret sharing schemes. In [27, 28], 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 shares 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($A$)= 2; and X is a random matrix composed of three linearly independent column vectors $x_1, x_2, x_3 \in \mathbb{Z}_{31}^{2 \times 1}$. 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 δ disseminates shares $a'_1, a'_2, a'_3 \in A'$ to three independent shareholders α, β, and γ. 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 α, β, and γ.

Let us now assume that a reconstruction process ρ_1 requests to shareholders α and β 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 ρ_2 requests to shareholders α and γ their respective shares. Finally, a third reconstruction process ρ_3 requests to shareholders γ and β their shares. Processes ρ_1, ρ_2, and ρ_3 build independently three reconstruction matrices B_1, B_2, and B_3:

$$B_1 = \begin{bmatrix} 22 & 25 \\ 13 & 4 \\ 20 & 1 \end{bmatrix}, \quad B_2 = \begin{bmatrix} 15 & 29 \\ 28 & 26 \\ 16 & 5 \end{bmatrix}, \quad B_3 = \begin{bmatrix} 8 & 15 \\ 4 & 25 \\ 13 & 28 \end{bmatrix}$$

We can finally 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 ρ_1, ρ_2, ρ_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., $A' = Ax_i \ (mod\ p)\ \forall x_i \in [x_1, x_2, \ldots, x_n]$. 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 equivalent.*

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 equivalent 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 equivalent to P_A. $\square$

3.2 Efficiency

The efficiency of a secret sharing scheme can be evaluated in terms of the information entropy of its shares and the secret of the cryptosystem [29]. A secret sharing scheme is said to be perfect if it holds that the entropy of the shares is greater or equal than the entropy of the secret. As a consequence, the size of each share on 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. Ramp secret sharing schemes may considerably improve this efficiency, by allowing a trade-off between security and size of the shares. 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 ramp secret sharing 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 [30] 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 [30] 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 [30], 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 Given that 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 by Yakamoto in [30], 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:

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

Hence, 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 or elongating 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 or elongated 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 or elongated 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 or elongating 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 procees 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 new 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 α and β in the system, each holding one of the following two share pairs V_α and V_β:

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

Let us assume that a reconstruction process ρ_1 requests to each shareholder their share combination. Both α and β return to ρ_1 a linear transformation from the column vectors in their share pairs. Shareholder α 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, β 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 ρ_2 and ρ_3 request to each share holder their shares. Shareholders α and β return to ρ_2 and ρ_3 two different linear combinations from the column vectors in their share pairs. Shareholder α returns $b'_\alpha \in \mathbb{Z}_{31}^{3\times 1} = 28 \cdot v_{\alpha 1} + v_{\alpha 2}$ to process ρ_2, and $b''_\alpha \in \mathbb{Z}_{31}^{3\times 1} = 5 \cdot v_{\alpha 1} + v_{\alpha 2}$ to process ρ_3. Shareholder β returns $b'_\beta \in \mathbb{Z}_{31}^{3\times 1} = 19 \cdot v_{\beta 1} + v_{\beta 2}$ to process ρ_2, and $b''_\beta \in \mathbb{Z}_{31}^{3\times 1} = 21 \cdot V_{\beta 1} + V_{\beta 2}$ to process ρ_3. Finally, the process ρ_1 assembles with b_α, b_β the reconstruction matrix $B_1 \in \mathbb{Z}_{31}^{3\times 2}$; the process ρ_2 builds with b'_α, b'_β the reconstruction matrix $B_2 \in \mathbb{Z}_{31}^{3\times 2}$; and the process ρ_3 produces with b''_α, b''_β 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 equivalent to the orthogonal projector obtained by applying Equation (4) to matrix A:

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

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

$$\begin{aligned} B_i &= \left[r_\alpha \cdot a'_1 + a'_3\ ,\ r_\beta \cdot a'_2 + a'_3\right] \\ &= \left[r_\alpha \cdot Ax_1 + Ax_3\ ,\ r_\beta \cdot Ax_2 + Ax_3\right] \\ &= \left[A\ (r_\alpha \cdot x_1 + x_3)\ ,\ A\ (r_\beta \cdot x_2 + x_3)\right] \\ &= \left[A\ x'_1\ ,\ A\ x'_2)\right] = A\ X'_i \end{aligned} \tag{15}$$

in which r_α and r_β 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 equivalent 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 ρ_1, ρ_2, and ρ_3 are executed by a qualified entity Ψ_1 with knowledge of reference a'_3, the returned set of column vectors b_α, b'_α, b''_α, 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 ρ_1, ρ_2, and ρ_3 were executed by a malicious adversary Ψ_2 who is trying to link the shares returned by either α or β, for tracking purposes, but not having access to the column vector reference a'_3, the returned set of column vectors b_α, b'_α, and b''_α, as well as column vectors b_β, b'_β, and b''_β, are viewed as unlinked.

4 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 need of synchronization; (2) compact size of shares; (3) secret sharing construction that guarantees strong security; (4) reconstruction of the secret does not require the identity of the shareholders.

Acknowledgments — The authors graciously acknowledge the financial support received from the following organizations: Natural Sciences and Engineering Research Council of Canada (NSERC), Mathematics of Information Technology and Complex Systems (MITACS), and *La Caixa* (Canada awards).

References

[1] EPCglobal. EPC Radio-frequency Identity Protocols Class-1 Generation-2 UHF. RFID Protocol for Communications at 860-960 MHz. Tech.Rep., 2005. [On-line] http://www.epcglobalinc.org/standards/

[2] ISO/IEC 18000-6. [On-line] http://wwwiso.org/, 2006.

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

[4] J. Garcia-Alfaro, M. Barbeau, and E. Kranakis. 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, Canada, May 2008.

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

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

[7] S. Weis, S. Sarma, R. Rivest, and D. Engels. 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, Germany, March 2004. Springer.

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

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

[10] D. Henrici and P. Müller. 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, Orlando, Florida, USA, March 2004. IEEE, IEEE Computer Society.

[11] D. Molnar and D. Wagner. Privacy and Security in Library RFID: Issues, Practices, and Architectures. In *Conference on Computer and Communications Security – ACM CCS*, pages 210–219, Washington, DC, USA, October 2004. ACM Press.

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

[13] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda. 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, 2007.

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

[15] J. Wolkerstorfer. Is Elliptic-Curve Cryptography Suitable to Secure RFID Tags? Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.

[16] P. Cole and D. Ranasinghe, editors. *Networked RFID Systems and Lightweight Cryptography — Raising Barriers to Product Counterfeiting*. Springer, 1rst edition, 2008.

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

[18] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. 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, Boston, Massachusetts, USA, August 2004. IACR, Springer.

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

[20] M. Langheinrich and R. Marti. RFID Privacy Using Spatially Distributed Shared Secrets. In *4th International Symposium of Ubiquitous Computing Systems*, LNCS, 4836, pages 1–16, 2007. Springer.

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

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

[23] A. Juels, R. Pappu, and B. Parno. Unidirectional Key Distribution Across Time and Space with Applications to RFID Security. In *USENIX Security Symposium*, San Jose, CA, July-August 2008. USENIX.

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

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

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

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

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

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

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

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

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

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