Application of the correcting codes to mutually trusted authority-free secret sharing schemes

Policarpo Abascal Fuentes [*] Juan Tena Ayuso [†]

Extended Abstract

Abstract

The problem of constructing secret sharing schemes has been treated from different branches of the Maths. In particular, Mc-Eliece & Sarwate [6] gave a generalization of the Shamir's construction [7] to solve the problem of sharing a secret in codes terms.

On the other hand, it has been also considered different variants of this problem. Among those ones is found the construction of secret sharing schemes in which is dispensed the intervention of a dealer for the distribution of the participations that permit the reconstruction of the secret to share, [4].

In this work, we consider the problem of constructing secret sharing schemes without the assistance of a dealer and show how to build a scheme based on error correcting codes to solve the mutually trusted authority-free problem.

1 Introduction

The problem of secret sharing has been treated by many authors in the last years, this is due to its applications in several fields, specially in data security.

Traditionally, it has been considered essential the existence of a dealer whose function is to choose the secret to share and to distribute the participations to the different persons that intervene in the problem. However, Ingemarsson & Simmons [4] have given a protocol to build a scheme that realizes an access structure without the intervention of a dealer. This has been designated a democratic scheme for secret sharing and, in this type of scheme, the set of participants transacts and distributes the participations.

[*]Dpto. de Matemáticas. U. de Oviedo. E–mail: abascal@etsiig.uniovi.es

[†]Dpto. de Algebra, Geometría y Topología. U. de Valladolid. E–mail: tena@agt.uva.es

In this work, we will build a democratic secret sharing scheme based on error correcting codes.

We will begin outlining the problem of secret sharing defining the different concepts associated with the problem and establishing the notation that we will find in this work, in order for the reader to become more familiar with it.

To solve the problem, Carpentieri described in [3] a construction based on the vectorial construction introduced by Brickell [2]. Supporting us in his construction, we will see how a democratic scheme can be built through the utilization of an error correcting code.

Also, we will see how we can modify our construction in order to improve efficiency measures outlined in [5].

2 Secret sharing

The problem that is stated is: given a secret, some information fragments are distributed among several participants, in such a way that the secret can be recovered by certain groups of these participants while other groups are not able to obtain any information about the secret.

To describe the problem, let's consider:

$\mathcal{P} = \{P_1, \ldots, P_l\}$ the set of l *participants* that want to share a secret,

$D \notin \mathcal{P}$ the *dealer* of the scheme,

$\mathcal{K}$ a set of *secrets* to share,

$\Gamma \subseteq 2^{\mathcal{P}}$ the set of subsets of $\mathcal{P}$ which are able to compute the secret. Γ is called *access structure* and its elements *authorized subsets*,

$\mathcal{S}$ the set of *participations* that are distributed, in particular, $\mathcal{S}_i \subset \mathcal{S}$ is the set of participations that P_i can receive.

When the dealer D wants to distribute a secret $K \in \mathcal{K}$, will give to every $P_i \in \mathcal{P}$ a participation $s_i \in \mathcal{S}_i$ according to some given *distribution rules*. Such rules configure a *scheme* that solves the stated problem. We will say, then, that the scheme *realizes* the access structure Γ.

2.1 Schemes based on correcting codes

We go to give the description of the construction of a scheme to share secret in codes terms. For this, we will consider $\mathcal{K} = I\!F_q^m$ the set of secrets, where $I\!F_q$ is a finite field with q elements, $m \in I\!N$ and $\mathcal{C}$ a linear $[n, k, d]$ code, $k \geq m$, with generator matrix $G \in \mathcal{M}_{k \times m}$.

This matrix is made public and its columns are assignated to the different participants in the scheme, included the dealer, according to certain sets of

indices. It could associate several columns with each participant and, even, a same column to different participants, but with the consideration of the fact that the columns assignated to the dealer should be dependent on the set of columns of each authorized subset but independent of the set of columns of every unauthorized subsets.

The sets of indices assignated to each participant P_i and to the dealer will be denoted by J_i and J_D, respectively. And, for each $A \in 2^{\mathcal{P}}$, will be denoted by $J_A = \bigcup_{P_i \in A} J_i$.

The description of the scheme is as follows:

- A secret $\overline{K}$ with m coordinates is considered and is widened until a vector $(\overline{K}, \overline{a})$ of length k is obtained.
- The vector $(\overline{K}, \overline{a})$ is codified in order to obtain a word

$$(\overline{K}, \overline{a})G = \overline{c} = (c_1, c_2, \ldots, c_n) \in \mathcal{C}$$

- The components of the vector $\overline{c}$ are distributed among the different participants, giving to each P_i the corresponding components to the sets of indices J_i and to the dealer those of J_D.
- To recover the secret, the authorized subsets have to decode the word built with the components with that they have been assigned considering as a gap type error the coordinates that they do not know. The subset should be able to determine the dealer's coordinates.

  Note that the code can correct $d - 1$ of such errors.

The described scheme is perfect and realizes the access structure Γ [1].

3 A construction of a democratic scheme

In [3], Carpentieri describes a democratic scheme for secret sharing based on the vectorial construction presented by Brickell [2]. In his construction is observed that: firstly, each participant P_i, $i = 1, \ldots, n$, chooses an element $a_i \in I\!F_q$ to build a secret $s = \sum_{i=1}^{n} a_i$, that will be distributed through a (n, n)-threshold scheme; secondly, each participant P_i acts as a dealer of a scheme that realizes the access structure Γ to share each a_i, giving a participation $a_{i,j}$ to each P_j, $j = 1, \ldots, n$; and finally, each P_j builds his own participation with the information fragments received $s_j = \sum_{i=1}^{n} a_{i,j}$.

It can be proved that an authorized set A will be able to recover all the a_i and the secret s as well. Furthermore, the information rate of such scheme is the same as a classic scheme with a dealer.

3.1 A construction based on error correcting codes

We are going to describe a construction of a democratic secret sharing scheme supporting us on the above construction.

Let be $\mathcal{P} = \{P_1, \ldots, P_n\}$ a set of participants, a virtual participant X, Γ an access structure defined on $\mathcal{P}$ and $\mathcal{S}$ a set of secrets.

It is considered a code $\mathcal{C}$, generated by a matrix G, that realizes the access structure Γ

- each participant P_i chooses at random a vector $\overline{v}_i$ and codifies it through the code $\mathcal{C}$ obtaining:

  $$\overline{v_i}G = (c_X^i, c_1^i, \ldots, c_n^i)$$

  and distributes to each participant P_j as participation c_j^i, $j = 1, \ldots, n$;
- each participant P_j builds his participation $c_j = \sum_{i=1}^n c_j^i$; and
- the secret is $s = \sum_{i=1}^n c_X^i$.

To recover the secret s, an authorized set $A = \{P_{i_1}, \ldots, P_{i_{r_A}}\} \in \Gamma$ will have to consider the subcode associated $\mathcal{C}_A$, generated by the matrix $G(J_A \cup J_X)$, and decode the codeword whose first component, the associated with the virtual participant X (the secret), is considered as a gap type error and the remainders components are the participations of each P_{i_j}, $j = 1, \ldots, r_A$.

4 Variants of the democratic schemes

In [5], the authors suggest that the authority that constructs the secret will not be the whole participants but a subset of them. This subset must be in the access structure.

On other hand, they propose three efficiency measures, based each one on a different assumption. The three assumptions are: that it is costly to initiate a communication using a secure channel; that it is costly to transmit information over a secure channel; and that it is costly to store information.

And, in order to optimize these rates, the authors outline different constructions and they also define some new access structures:

Definition 4.1 *Let $A \subset \mathcal{P}$. We define the contraction $\Gamma \cdot A$ of Γ at A to be the access structure on $\mathcal{P} - A$ such that, for $B \subset \mathcal{P} - A$*

$$B \in \Gamma \cdot A \Longleftrightarrow B \cup A \in \Gamma$$

We note that, in the scheme proposed by Carpentieri in [3], a participant P_i acts as a dealer of his information a_i and distributes the participations among

all the participants. In particular, he assigns to himself a participation $a_{i,i}$ to recover, together with other participants according to the access structure Γ, his own participation a_i. This provokes an information redundancy for P_i since he already knows a_i and therefore rebounds on the worsening of the rates defined in [5].

In order to settle this information duplication, in the construction exposed in the paragraph 3.1, we propose two solutions:

4.1 First solution

Maintaining the scheme defined by the code $\mathcal{C}$, generated by the matrix G, we can force to the fact that the participation that a participant P_i is granted to himself will be the same value that the information he builds, that is to say, $a_{i,i} = a_i$.

This solution is feasible since, supposing that the access structure is connected, the columns associated with the participant P_i form together with those which are associated with the dealer in the classic construction an independent set and then it can be chosen a vector $\overline{v_i}$ such that $\overline{v_i}G(J_X) = \overline{v_i}G(J_{\{P_i\}})$.

Theorem 4.1 *If $\mathcal{C}$ realizes the access structure Γ for a set of secrets $\mathcal{S}$, then $\mathcal{C}$ realizes the access structure $\Gamma_i = \Gamma \cdot P_i + P_i$ for the set of secrets $\mathcal{S}_i = \{s : \exists \overline{v}$ such that $s = \overline{v}G(J_X) = \overline{v}G(J_{\{P_i\}})\}$.*

Let be $A = \{P_{i_1}, \ldots, P_{i_{r_A}}\} \in \Gamma$ the set that builds the secret, we see how the members of A should act to realize the scheme.

- Each participant P_{i_j} with $j = 1, \ldots, r_A$ chooses a vector $\overline{v_{i_j}}$ so that $\overline{v_{i_j}}G(J_X) = \overline{v_{i_j}}G(J_{\{P_{i_j}\}})$ and codifies it obtaining:

  $$\overline{v_{i_j}}G = (a_{i_j}, a_{i_j,1}, \ldots, a_{i_j,i_j} = a_{i_j}, \ldots, a_{i_j,n})$$

  and distributes to each P_k as participation $a_{i_j,k}$, $k = 1, \ldots, n$.
- Each participant P_k builds his participation $c_k = \sum_{j=1}^{r_A} a_{i_j,k}$.
- The secret is $s = \sum_{j=1}^{r_A} a_{i_j}$.

For the construction of the secret and the participations the codification of the vector $\overline{v} = \sum_{j=1}^{r_A} \overline{v_{i_j}}$ is being accomplished.

If a set $B \in \Gamma$ intends to recover the secret s it will have to act as the form described in the paragraph 3.1.

4.2 Second solution

In the previous construction, though the participant P_i assigns his own participation a_i to himself, a sharing scheme goes on being accomplished among

all the participants, included P_i that accomplishes the dealer functions, when, actually it would suffice to build and to distribute participations between the $n-1$ remaining participants.

We can define subcodes $\mathcal{C}_i$ from the original $\mathcal{C}$ to accomplish such participations share among the $n-1$ remaining participants.

Theorem 4.2 *Let be $\mathcal{C}$ a code, generated by a matrix G, that realizes an access structure Γ, and $\mathcal{C}_i$ the code obtained by truncation as of $\mathcal{C}$, eliminating the corresponding coordinates to the participant P_i. Then $\mathcal{C}_i$ realizes an access structure $\Gamma_i' = \Gamma - \{B \in \Gamma / P_i \in B\}$ defined on $\mathcal{P}_i = \mathcal{P} - \{P_i\}$.*

Let's see the construction.
Let be $A = \{P_{i_1}, \ldots, P_{i_{r_A}}\} \in \Gamma$ the set that builds the secret.

- Each participant P_{i_j} with $j = 1, \ldots, r_A$ chooses randomly a vector $\overline{v_{i_j}}$ that codifies, using the code $\mathcal{C}_{i_j}$ of the proposition 4.2, obtaining:

  $$\overline{v_{i_j}} G_{i_j} = \overline{v_{i_j}} G(J_X \cup J_{\{P_i\}^c}) = (a_{i_j}, a_{i_j,1}, \ldots, a_{i_j,n})$$

  distributes to each P_k as participation $a_{i_j,k}$, $k = 1, \ldots, n$and keep as own participation a_{i_j}. Note that the coordinates of the participants P_{i_j} are eliminated.
- Each participant P_k with $k \neq i_1, \ldots i_{r_A}$ builds his participation $c_k = \sum_{j=1}^{r_A} a_{i_j,k}$.
- Each participant P_k with $k = i_1, \ldots i_{r_A}$ builds his participation $c_k = a_{i_j} + \sum_{\substack{j=1 \\ i_j \neq k}}^{r_A} a_{i_j,k}$
- The secret is $s = \sum_{j=1}^{r_A} a_{i_j}$

We observe that, according to this new construction, we can say the access structure for the recovery of a_i is $\Gamma_i = \Gamma_i' \cup \{P_i\}$, since the access structure Γ_i' recovers a_i and P_i already knows it because he is the dealer of a_i; furthermore it is improved the transmission cost.

To recover the secret, since the linearity has been lost, an authorized set must recover each information fragment a_{i_j} built by the participants of A and thereafter, they could obtain the secret.

In order not to lose the linearity we can do the same process as we accomplished in the construction of the paragraph 4.1, that is to say, each participant P_{i_j} chooses a vector that verifies certain conditions that we will see below.

When a participant P_{i_j} with $j = 1, \ldots, r_A$ chooses the vector $\overline{v_{i_j}}$ must make it so that $\overline{v_{i_j}} G(J_X) = \overline{v_{i_j}} G(J_{\{P_{i_j}\}})$, with this vector builds the participations $a_{i_j,k}$ with $k \in \{1, \ldots, n\} - \{i_j\}$.

In this way, the construction is similar to the solution described in the paragraph 4.1 since the linearity is not lost, as, actually, the vector $\overline{v} = \sum_{j=1}^{r_A} \overline{v_{i_j}}$

is being codified using the code $\mathcal{C}$ since if we observe the participations that the participants of A have built with this modification:

- each participant P_k with $k \neq i_1, \ldots, i_{r_A}$ continues with the participation $c_k = \sum_{j=1}^{r_A} a_{i_j,k}$; and
- each participant P_k with $k = i_1, \ldots i_{r_A}$ building his own participation obtains $c_k = a_{i_j} + \sum_{\substack{j=1 \\ i_j \neq k}}^{r_A} a_{i_j,k} = \sum_{j=1}^{r_A} a_{i_j,k}$ since $\overline{v_{i_j}} G(J_X) = \overline{v_{i_j}} G(J_{\{P_{i_j}\}}) = a_{i_j}$

Now, if a set $B \in \Gamma$ intends to recover the secret s it will have to act in the way described in the paragraph 3.1

5 Conclusions

We have revised the constructions of secret sharing schemes without the assistance of a dealer and we have provided a scheme based on error correcting codes to solve the problem.

Furthermore, we have optimized some of the constructions in the sense of the communications between the different participating as well as of the quantity of information that a participant must possess.

References

[1] Abascal, P. *Compartir secretos mediante esquemas basados en códigos correctores.* Ph. O. Dissertation. Universidad de Oviedo, (1999).

[2] Brickell, E.F. *Some ideal secret sharing schemes.* Journal of Combinatorial Mathematics and Combinatorial Computing **6** (1989), pp. 105-113.

[3] Carpentieri, M. *Some democratic secret sharing schemes* Discrete Applied Mathematics, **59**, 1995, pp. 293-298.

[4] Ingemarsson, I. & Simmons, G.J. *A protocol to set up shared secret schemes without the assistance of a mutually trusted party.* Advances in Cryptology, EUROCRYPT '90, I.B. Damgard, ed., Lecture Notes in Computer Science **473** 1991, pp. 266-282.

[5] Jackson, W.A., Martin, K. M. & O'Keefe,C. M. *Mutually trusted authority-free secret sharing schemes*, Journal of Cryptology **10** 1997, pp.261-289.

[6] Mc-Eliece, R.J. & Sarwate, D.V. *On Sharing Secrets and Reed-Solomon Codes.* Comm ACM. 1981, **24** pp. 583-584.

[7] Shamir, A. *How to share a secret.* Comm ACM. 1979, **22**(11) pp. 612-613.