Journal of Mathematical Sciences: Advances and Applications
Volume 71, 2022, Pages 5-46
Available at http://scientificadvances.co.in
DOI: http://dx.doi.org/10.18642/jmsaa_7100122254

ON MODAL Θ-VALENT STEGANOGRAPHIC PROTOCOLS

JEAN ARMAND TSIMI, PEMHA BINYAM GABRIEL CEDRIC and ARMAND KEMADJOU KETCHANDJEU

Departement of Mathematics and Computer Sciences
Faculty of Sciences
University of Douala
PO Box: 24157, Douala
Cameroon
e-mail: tsimije@yahoo.fr
gpemha@yahoo.fr
karmand44@yahoo.com

Abstract

In this note, we plan to define a notion of modal Θ-valent steganographic protocols and then give some examples.

2020 Mathematics Subject Classification: 94D99, 03G25, 03B60.
Keywords and phrases: $m\Theta$ steganographic protocols, Hamming α-distance, $m\Theta$ embedding function, $m\Theta$ extraction function, $m\Theta$ covering radius, steganographic protocol $F_5^{2\mathbb{Z}}$.
Received July 11, 2022

1. Introduction

The $m\Theta$ (modal Θ-valent) chrysippian ring [2] is defined as an algebraic model of a non-classical logic named the $m\Theta$ chrysippian logic which is a modal Θ-valent chrysippian extension of the boolean logic. The modal Θ-valent chrysippian logic admits states of truth other than true and false. From the $m\Theta$ chrysippian rings, the notion of $m\Theta$ sets, of $m\Theta$ algebraic structures are defined and studied in [2]. The modal Θ-sets are a class of sets richer than the classical or boolean sets on the logical and overall levels. From finite $m\Theta$ sets and $m\Theta$ algebraic strutures, the notions of $m\Theta$ codes and $m\Theta$ linear codes are define in [3, 4, 5, 7, 8, 9, 10, 11]. With the $m\Theta$ codes one can mathematically stipulate that an error that occured during the transmission of an $m\Theta$ information is slow, medium or deep. Information plays a vital role in our daily life. Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. So many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Among those methods, Steganography or "covered writing" [13] is a technique of hiding information in digital media in such a way that no one apart from the intended recipient knows the existence of the information. Steganography is one such pro-security innovation in which secret data is embedded in a cover [14]. The notion of data hiding or steganography was first introduced with the example of prisoners' secret message by Simmons in 1983 [15]. There exist two types of materials in steganography: message and carrier. Message is the secret data that should be hidden and carrier is the material that takes the message in it [16]. A steganography system is a quintuple $\mathbb{P} = (C, M, K, D_K, E_K)$, where C is the set of all covers used in communication, M is the set of all secret messages that need to be transported using the covers, K the set of secret keys $E_K : C \times M \times K \to C$, and $D_K : C \times K \to M$ two

functions, the embedding and the extraction functions, respectively such that $D_K = (E_K(c, m, k), k) = m$. In this note, we intend to introduce the notion of modal Θ-valent steganography system as a quintuple $\mathbb{P}_\Theta = (C_\Theta, M_\Theta, K_\Theta, D_{K_\Theta}, E_{K_\Theta})$, where C_Θ, M_Θ, and K_Θ are modal Θ-sets, D_{K_Θ} and E_{K_Θ} are respectively, the modal Θ-valent embedding function and the modal Θ-valent extraction function, in the hope that this approach would logically and algebraically improves the classical view of steganography as presented in [1]. The rest of the paper is structured as follows: In Section 2, we recall the notions of $m\Theta$ set and $m\Theta$ algebraic structures. In Section 3, we define the notion of $m\Theta$ steganographic protocols with some examples. The $m\Theta$ codes and pseudo $m\Theta$ codes defined by $m\Theta$ steganographic protocols are defined in Section 4. In Section 5, we defined the $m\Theta$ linear steganographic protocols using $m\Theta$ codes.

2. The $m\Theta$ Algebraic Structures [2]

2.1. The $m\Theta$ sets

$m\Theta$ sets are considered to be non-classical sets which are compatible with a non-classical logic called the chrysippian $m\Theta$ logic.

Definition 2.1. Let E be a non-empty set, I be a chain whose first and last elements are 0 and 1, respectively, $(F_\alpha)_{\alpha \in I_*}$, where $I_* = I \setminus \{0\}$ be a family of applications from E to E. An $m\Theta s$ is the pair $(E, (F_\alpha)_{\alpha \in I_*})$ simply denoted by (E, F_α) satisfying the following four axioms:

- $\bigcap_\alpha F_\alpha(E) = \bigcap_{\alpha \in I_*} \{F_\alpha(x) : x \in E\} \neq \emptyset$;
- $\forall \alpha, \beta \in I_*$, if $\alpha \neq \beta$, then $F_\alpha \neq F_\beta$;

- $\forall \alpha, \beta \in I_*, F_\alpha \circ F_\beta = F_\beta$;

- $\forall x, y \in E$, if $\forall \alpha \in I_*, F_\alpha(x) = F_\alpha(y)$, then $x = y$.

Theorem 2.1 (The theorem of $m\Theta$ determination)**.** *Let* (E, F_α) *be an* $m\Theta s$.

$$\forall x, y \in E, x = y \text{ if and only if } \forall \alpha \in I_*, F_\alpha(x) = F_\alpha(y).$$

Proof. [2].

Definition 2.2. Let $C(E, F_\alpha) = \bigcap_{\alpha \in I_*} F_\alpha(E)$. We call $C(E, F_\alpha)$ the set of $m\Theta$ invariant elements of the $m\Theta s(E, F_\alpha)$.

Proposition 2.1. *Let* (E, F_α) *be an* $m\Theta s$. *The following properties are equivalent*:

(1) $x \in \bigcap_{\alpha \in I_*} F_\alpha(E)$;

(2) $\forall \alpha \in I_*, F_\alpha(x) = x$;

(3) $\forall \alpha, \beta \in I_*, F_\alpha(x) = F_\beta(x)$;

(4) $\exists \mu \in I_*, x = F_\mu(x)$.

Proof. [2].

Definition 2.3. Let (E, F_α) and (E', F'_α) be two $m\Theta s$. Let X be a non-empty set. We shall call

(1) $(E' F'_\alpha)$ a modal Θ-valent subset of (E, F_α) if the structure of $m\Theta s$ (E', F'_α) is the restriction to E' of the structure of the $m\Theta s$ (E, F_α), this means:

- $E' \subseteq E$;

- $\forall \alpha : \alpha \in I_*, F'_\alpha = F_{\alpha|_{E'}}$.

(2) X a modal Θ-valent subset of (E, F_α) if:

- $X \subseteq E$;
- $(X, F'_{\alpha|_X})$ is an $m\Theta s$ which is a modal Θ-valent subset of (E, F_α).

In all what follows we shall write $F_\alpha x$ for $F_\alpha(x)$, $F_\alpha E$ for $F_\alpha(E)$, etc.

Proposition 2.2. *Let* (E, F_α) *be an* $m\Theta s$ *and* E' *be a non-empty set such that* $E' \subseteq E$. *Let us suppose that* $\forall \alpha \in I_*, F'_\alpha = F_{\alpha|_{E'}}$ *and* $\mathcal{C}(E', F'_\alpha) = \bigcap_{\alpha \in I_*} F'_\alpha(E')$.

Then the following axioms are equivalent:

$\star$ $(E' F'_\alpha)$ *is an* $em\Theta$;

$\star\star$ $C(E', F'_\alpha) \neq \emptyset$,

$-$ $\forall \alpha \in I_*$, *if* $x \in E'$, *then* $F'_\alpha x \in E'$.

$-$ *If* $\alpha \neq \beta$, *then* $F'_\alpha \neq F'_\beta$.

Proof. [2].

Theorem 2.2 (Product of $m\Theta$ sets)**.** *Let* (E, F_α) *and* (E', F'_α) *be two* $m\Theta$ *sets. Let us set* $(E, F_\alpha) \times (E', F'_\alpha) = (E \times E', F_\alpha \times F'_\alpha)$ *such that* $F_\alpha \times F'_\alpha$ *is defined as follows*:

$$\forall \alpha \in I_*, F_\alpha \times F'_\alpha = (F_\alpha, F'_\alpha) : E \times E' \to E \times E'$$

$$(x, y) \mapsto F_\alpha \times F'_\alpha(x, y) = (F_\alpha x, F'_\alpha y)$$

$(E \times E', F_\alpha \times F'_\alpha)$ *is the structure of* $m\Theta s$ *on* $E \times E'$.

Proof. [2].

Definition 2.4. The product of (E, F_α) by (E', F'_α), is the $m\Theta s$ denoted $(E \times E', F_\alpha \times F'_\alpha)$ and defined as above.

2.1.1. Application or map between $m\Theta$ sets

Let (E, F_α) and (E, F'_α) be two $m\Theta$ sets having the same valence Θ. We call a modal $m\Theta$ morphism from (E, F_α) into (E', F'_α), every application $f : E \to E'$ such that for every $\alpha \in I_*$,

$f \circ F_\alpha = F'_\alpha \circ f$. If f is bijective, then f is called an $m\Theta$ isomorphism.

2.1.2. Some examples of $m\Theta$ sets

For $n \in \mathbb{N}^*$, we define the closed chain

$$I = \begin{cases} \{0, 1, 2\}, & n = 2, \\ \mathbb{N}_{n-1} = \{0, 1, \ldots, n-1\}, & \text{if } n \geq 3. \end{cases}$$

(1) The $m\Theta$ set $(\mathbb{Z}, n\mathbb{Z}, F_\alpha)$

We define $\forall \alpha \in I_* = I \backslash \{0\}$

$F_\alpha : \mathbb{Z} \to \mathbb{Z}$

$$x \mapsto \begin{cases} F_\alpha(x) = x, & \text{if } x \in n\mathbb{Z} \\ F_\alpha(x) = n(p + \alpha r), & \text{if } x \in \mathbb{Z} \backslash n\mathbb{Z} (x = pn + r \text{ for } 1 \leq r \leq n-1) \end{cases}$$

$(\mathbb{Z}, F_\alpha)$ is a $m\Theta s$ such that $C(\mathbb{Z}, F_\alpha) = n\mathbb{Z}$.

(2) The $m\Theta s$ $(\mathbb{Z}_{n\mathbb{Z}}, \mathbb{Z}, F'_\alpha)$

Let us set $x_{n\mathbb{Z}} = (p + \alpha r)_{\alpha \in I_*}$, where $x \in \mathbb{Z} \backslash n\mathbb{Z}\, (x = pn + r,\ p, r \in \mathbb{Z},\ 1 \leq r \leq n-1)$

$$x_{n\mathbb{Z}} \in \begin{cases} \mathbb{Z}^2, & \text{if } n = 2 \text{ or } n = 3, \\ \mathbb{Z}^{n-1}, & \text{if } n \geq 3. \end{cases}$$

Let us set $\mathbb{Z}_{n\mathbb{Z}} = \mathbb{Z} \cup \{x_{n\mathbb{Z}} : \neg (x \equiv 0 (\mathrm{mod}\ n))\}$.

We define for all $\alpha \in I_*$

$$F'_\alpha : \mathbb{Z}_{n\mathbb{Z}} \to \mathbb{Z}_{n\mathbb{Z}}$$

$$a \mapsto \begin{cases} F_\alpha a = a, & \text{if } a \in \mathbb{Z}, \\ F_\alpha a = b_1 + \alpha b_2, & \text{if } a = b_{n\mathbb{Z}},\ b \in \mathbb{Z}\backslash n\mathbb{Z}(b = b_1 n \\ & \qquad + b_2 : b_2 b_1 \in \mathbb{Z}, 1 \leq b_2 \leq n-1) \end{cases}$$

$(\mathbb{Z}_{n\mathbb{Z}}, F'_\alpha)$ is an $m\Theta s$ such that $C(\mathbb{Z}_{n\mathbb{Z}}, F'_\alpha) = \mathbb{Z}$.

- Consider $(\mathbb{Z}_{2\mathbb{Z}}, F_\alpha)$

$$\mathbb{Z}_{2\mathbb{Z}} = \mathbb{Z} \bigcup \{1_{2\mathbb{Z}}, 3_{2\mathbb{Z}}, 5_{2\mathbb{Z}}, 7_{2\mathbb{Z}}, \ldots\}$$

$$1_{2\mathbb{Z}} = (0 + \alpha.1)_{\alpha \in \{1,\ 2\}} = (1,\ 2) \in \mathbb{Z}^2$$

$$3_{2\mathbb{Z}} = (1 + \alpha.1)_{\alpha \in \{1,\ 2\}} = (2,\ 3) \in Z^2$$

$$5_{2\mathbb{Z}} = (2 + \alpha.1)_{\alpha \in \{1,\ 2\}} = (3,\ 4) \in \mathbb{Z}^2$$

$$7_{2\mathbb{Z}} = (3 + \alpha.1)_{\alpha \in \{1,\ 2\}} = (4,\ 5) \in \mathbb{Z}^2$$

$$\vdots$$

$$F_1\mathbb{Z} = F_2\mathbb{Z} = \mathbb{Z}$$

$$F_1 1_{2\mathbb{Z}} = 0 + 1.1 = 1;\ F_2 1_{2\mathbb{Z}} = 0 + 2.1 = 2$$

$$F_1 3_{2\mathbb{Z}} = 2;\ F_2 3_{2\mathbb{Z}} = 3.$$

Proposition 2.3. *Let* $(\mathbb{Z}, F_\alpha)$ *and* $(Z_{n\mathbb{Z}}, F'_\alpha)$ *be the* $m\Theta$ *sets defined as above.*

Let us define $spec_{n\mathbb{Z}}$ *as follows*:

$$spec_{n\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}_{n\mathbb{Z}}$$
$$x \mapsto \begin{cases} p, & \text{if } x = np, \\ x_{n\mathbb{Z}}, & \text{if } \neg(x \equiv 0 \,(\mathrm{mod}\, n)). \end{cases}$$

Thus, $spec_{n\mathbb{Z}}$ *is an* $m\Theta$ *bijective map from* $(\mathbb{Z}, F_\alpha)$ *into* $(\mathbb{Z}_{n\mathbb{Z}}, F'_\alpha)$.

Proof. [2].

(3) The $m\Theta s$ $(\mathbb{Z}_{n\mathbb{Z}}, \mathbb{N}, F'_\alpha)$

Let us set $x_{n\mathbb{Z}} = (p + \alpha r)_{\alpha \in I_*}$, where $x \in \mathbb{N}\backslash n\mathbb{Z} (x = pn + r,\ p,\ r \in \mathbb{Z},\ 1 \leq r \leq n-1)$

$$x_{n\mathbb{Z}} \in \begin{cases} \mathbb{N}^2, & \text{if } n = 2 \text{ or } n = 3, \\ \mathbb{N}^{n-1}, & \text{if } n \geq 3. \end{cases}$$

Let us set $\mathbb{N}_{n\mathbb{Z}} = \mathbb{N} \cup \{x_{n\mathbb{Z}} : \neg(x \equiv 0(\mathrm{mod}\, n))\}$.

We define for all $\alpha \in I_*$

$$F'_\alpha : \mathbb{N}_{n\mathbb{Z}} \to \mathbb{N}_{n\mathbb{Z}}$$

$$a \mapsto \begin{cases} F_\alpha a = a, & \text{if } a \in \mathbb{N}, \\ F_\alpha a = b_1 + \alpha b_2, & \text{if } a = b_{n\mathbb{Z}},\ b \in \mathbb{N}\backslash n\mathbb{Z} \\ & (b = b_1 n + b_2 : b_2 b_1 \in \mathbb{N},\ 1 \leq b_2 \leq n-1), \end{cases}$$

$(\mathbb{N}_{n\mathbb{Z}}, F'_\alpha)$ is an $m\Theta s$ such that $C(\mathbb{N}_{n\mathbb{Z}}, F'_\alpha) = \mathbb{N}$

• Consider $(\mathbb{N}_{2\mathbb{Z}}, F_\alpha)$

$$\mathbb{N}_{2\mathbb{Z}} = \mathbb{N} \bigcup \{1_{2\mathbb{Z}}, 3_{2\mathbb{Z}}, 5_{2\mathbb{Z}}, 7_{2\mathbb{Z}}, ...\}$$

$$1_{2\mathbb{Z}} = (0 + \alpha.1)_{\alpha\in\{1, 2\}} = (1, 2) \in \mathbb{N}^2$$

$$3_{2\mathbb{Z}} = (1 + \alpha.1)_{\alpha\in\{1, 2\}} = (2, 3) \in \mathbb{N}^2$$

$$5_{2\mathbb{Z}} = (2 + \alpha.1)_{\alpha\in\{1, 2\}} = (3, 4) \in \mathbb{N}^2$$

$$7_{2\mathbb{Z}} = (3 + \alpha.1)_{\alpha\in\{1, 2\}} = (4, 5) \in \mathbb{N}^2$$

$$\vdots$$

$$F_1\mathbb{N} = F_2\mathbb{N} = \mathbb{N}$$

$$F_1 1_{2\mathbb{Z}} = 0 + 1.1 = 1;\ F_2 1_{2\mathbb{Z}} = 0 + 2.1 = 2$$

$$F_1 3_{2\mathbb{Z}} = 2;\ F_2 3_{2\mathbb{Z}} = 3.$$

2.2. The $m\Theta$ algebraics structures [2]

2.2.1. Algebraic structure of $(\mathbb{Z}_{n\mathbb{Z}}, F'_\alpha)$

Let $n \in \mathbb{N}$ such that $n \geq 2$. Let us recall that if $a \in \mathbb{Z}_{n\mathbb{Z}}$. We define the $m\Theta$ support of a denoted $s(a)$ as follows:

$$s(a) = \begin{cases} a, & \text{if } a \in \mathbb{Z}, \\ x, & \text{if } a = x_{n\mathbb{Z}} \text{ with } (x \equiv 0(\text{mod } n)). \end{cases}$$

Thus $s(a) \in \mathbb{Z}$.

Let $\perp$ be a binary law on $\mathbb{Z}$, i.e., $\forall a, b \in \mathbb{Z}, a \perp b \in \mathbb{Z}$. Let $x, y \in \mathbb{Z}_{n\mathbb{Z}}$. We define a binary $\perp^*$ on $\mathbb{Z}_{n\mathbb{Z}}$ as follows:

$$x \perp^* y = \begin{cases} s(x) \perp^* s(y), & \text{if } \begin{cases} x, y \in \mathbb{Z}, \\ (s(x) \perp^* s(y)) \equiv 0 (\text{mod } n) \text{ otherwise.} \end{cases} \\ (s(x) \perp^* s(y))_{n\mathbb{Z}}, & \text{otherwise.} \end{cases}$$

$\perp^*$ as defined above on $\mathbb{Z}_{n\mathbb{Z}}$ will be called an $m\Theta$ law on $\mathbb{Z}_{n\mathbb{Z}}$ for $x, y \in \mathbb{Z}_{n\mathbb{Z}}$.

Thus we can define $x + y \in \mathbb{Z}_{n\mathbb{Z}}$ and $x \times y \in \mathbb{Z}_{n\mathbb{Z}}$ for every $x, y \in \mathbb{Z}_{n\mathbb{Z}}$, where $+$ and $\times$ are $m\Theta$ addition and $m\Theta$ multiplication, respectively.

Remark 2.1. In $\mathbb{Z}_{n\mathbb{Z}}$ although the $m\Theta$ addition and the $m\Theta$ multiplication are commutative, they are not associative. The $m\Theta$ multiplication is not distributive over the $m\Theta$ addition.

The $m\Theta$ law $\perp^*$ on $\mathbb{Z}_{n\mathbb{Z}}$ however, is $m\Theta$ associative, i.e., $\forall x_{n\mathbb{Z}}, y_{n\mathbb{Z}}, z_{n\mathbb{Z}} \in \mathbb{Z}_{n\mathbb{Z}}$ we have

$$(x_{n\mathbb{Z}} \perp^* y_{n\mathbb{Z}}) \perp^* z_{n\mathbb{Z}} = \begin{cases} (x \perp^* y) \perp^* z, & \text{if } ((x \perp^* y) \perp^* z) \equiv 0 (\text{mod } n), \\ ((x \perp^* y) \perp^* z)_{n\mathbb{Z}}, & \text{otherwise,} \end{cases}$$

$$x_{n\mathbb{Z}} \perp^* (y_{n\mathbb{Z}} \perp^* z_{n\mathbb{Z}}) = \begin{cases} x \perp^* (y \perp^* z), & \text{if } ((x \perp^* y) \perp^* z) \equiv 0 (\text{mod } n), \\ (x \perp \mathbb{Z}^* (y \perp^* z))_{n\mathbb{Z}}, & \text{otherwise.} \end{cases}$$

In the meaning of the $m\Theta$ law $\perp^*$ defined on $\mathbb{Z}_{n\mathbb{Z}}$, we have

$$(x_{n\mathbb{Z}} \perp^* y_{n\mathbb{Z}}) \perp^* z_{n\mathbb{Z}} = x_{n\mathbb{Z}} \perp^* (y_{n\mathbb{Z}} \perp^* z_{n\mathbb{Z}}).$$

We also define the $m\Theta$ distributivity of the $m\Theta$ multiplication over the $m\Theta$ addition $\forall x_{n\mathbb{Z}}, y_{n\mathbb{Z}}, z_{n\mathbb{Z}} \in \mathbb{Z}$

$$x_{n\mathbb{Z}} \times (y_{n\mathbb{Z}} + z_{n\mathbb{Z}}) = \begin{cases} x \times (y + z), & \text{if } (x \times (y + z)) \equiv 0 (\text{mod } n) \\ (x \times (y + z))_{n\mathbb{Z}} & \text{otherwise} \end{cases}$$

$$= \begin{cases} (x \times y) + (x \times z), & \text{if } ((x \times y) + (x \times z)) \equiv 0 (\text{mod } n) \\ ((x \times y) + (x \times z))_{n\mathbb{Z}} & \text{otherwise} \end{cases}$$

$$= x_{n\mathbb{Z}} \times y_{n\mathbb{Z}} + x_{n\mathbb{Z}} \times z_{n\mathbb{Z}}.$$

When we restrict $m\Theta$ laws on $\mathbb{Z} = C(\mathbb{Z}_{n\mathbb{Z}}, F'_\alpha)$ we have (classical) of $\mathbb{Z}$, respectively.

2.2.2. The $m\Theta$ congruences of $(\mathbb{Z}_{n\mathbb{Z}}, F'_\alpha)$

Let $p \in \mathbb{N}^*$ and let ρ_p be defined on $\mathbb{Z}_{n\mathbb{Z}}$ as follows:

$$\forall x, y \in \mathbb{Z}_{n\mathbb{Z}}, x \rho_p y \Leftrightarrow \forall \alpha \in I_*, F'_\alpha x = F'_\alpha y (\text{mod } p).$$

Proposition 2.4. *ρ_p defined on $\mathbb{Z}_{n\mathbb{Z}}$ as above is an equivalence relation on $\mathbb{Z}_{n\mathbb{Z}}$ which is compatible with the structure of $m\Theta$s $(\mathbb{Z}_{n\mathbb{Z}}, F'_\alpha)$.*

Proof. [2].

Notation 2.1. We shall denote $x \rho_p y$ by $x \equiv y (p\mathbb{Z}_{n\mathbb{Z}})$.

Definition 2.5. If $p \geq n$, we define the $m\Theta$ quotient of $(\mathbb{Z}_{n\mathbb{Z}}, F'_\alpha)$ modulo $(p\mathbb{Z}_{n\mathbb{Z}})$ as follows: $\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}} = \left\{ \frac{x}{p\mathbb{Z}_{n\mathbb{Z}}}; x \in \mathbb{Z}_{n\mathbb{Z}} \right\}$.

Proposition 2.5. $(\mathbb{Z}_{n\mathbb{Z}}, F'_\alpha)$ *is the* $m\Theta s$ *of* $m\Theta$ *relative integers.*

$$\forall \alpha \in I_*, \quad \begin{array}{l} \dfrac{F'_\alpha}{p\mathbb{Z}_{n\mathbb{Z}}} : \dfrac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}} \to \dfrac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}} \\ \dfrac{x}{p\mathbb{Z}_{n\mathbb{Z}}} \mapsto \dfrac{F'_\alpha}{p\mathbb{Z}_{n\mathbb{Z}}}\left(\dfrac{x}{p\mathbb{Z}_{n\mathbb{Z}}}\right) = \dfrac{F'_\alpha x}{p\mathbb{Z}}. \end{array}$$

Then $\left(\dfrac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}, \dfrac{F'_\alpha}{p\mathbb{Z}_{n\mathbb{Z}}}\right)$ *is an* $m\Theta s$ *if and only if* $p \geq n-1$.

Proof. [2].

Lemma 2.1. *According to the Proposition* 2.5 *above, the following axioms are equivalent*:

(1) $p \geq n-1$.

(2) $\forall \alpha, \beta \in I_*$, *if* $\alpha \neq \beta$ *then* $\dfrac{F'_\alpha}{p\mathbb{Z}_{n\mathbb{Z}}} \neq \dfrac{F'_\beta}{p\mathbb{Z}_{n\mathbb{Z}}}$.

Proof. [2].

Proposition 2.6. $\forall x, y \in \mathbb{Z}_{n\mathbb{Z}}$

(1) *If* $x \in \mathbb{Z}$ *and* $x \equiv y(p\mathbb{Z}_{n\mathbb{Z}})$, *then* $y \in \mathbb{Z}$.

(2) *If* $x \notin \mathbb{Z}$ *and* $x \equiv y(p\mathbb{Z}_{n\mathbb{Z}})$, *then* $y \notin \mathbb{Z}$.

Proof. [2].

Proposition 2.7. *If* $x, y \in \mathbb{Z}_{n\mathbb{Z}}$, *the following axioms are equivalent*:

(1) $x \equiv y(p\mathbb{Z}_{n\mathbb{Z}})$

(2) $\begin{cases} x \equiv y (\mathrm{mod}\ p) & \text{if } x \in \mathbb{Z} \text{ (therefore } y \in \mathbb{Z}), \\ s(x) \equiv s(y) (\mathrm{mod}\ np) & \text{if } x \notin \mathbb{Z} \text{ (therefore } y \notin \mathbb{Z}). \end{cases}$

Proof. [2].

Definition 2.6. We shall call:

(1) The $m\Theta$ congruence in $(\mathbb{Z}_{n\mathbb{Z}}, F'_\alpha)$, the $m\Theta$ equivalence relation denoted ρ_p, $p \in N^*$ and defined as above.

(2) An $m\Theta$ integer modulo p (a residual $m\Theta$ class modulo p), the class of equivalence modulo $p\mathbb{Z}_{n\mathbb{Z}}$ of every $x \in \mathbb{Z}_{n\mathbb{Z}}$ and denoted $\frac{x}{p\mathbb{Z}_{n\mathbb{Z}}}$.

(3) The set of $m\Theta$ integers modulo p, the $m\Theta s\left(\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}; \frac{F'_\alpha}{p\mathbb{Z}_{n\mathbb{Z}}}\right)$.

(4) The set of integers modulo p, the set: $C\left(\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}; \frac{F'_\alpha}{p\mathbb{Z}_{n\mathbb{Z}}}\right) = \frac{\mathbb{Z}}{p\mathbb{Z}}$.

(5) The α-modality of $\frac{x}{p\mathbb{Z}_{n\mathbb{Z}}}$, the integer modulo p defined as follows:

$$\forall \alpha \in I_*, \frac{F'_\alpha}{p\mathbb{Z}_{n\mathbb{Z}}}\left(\frac{x}{p\mathbb{Z}_{n\mathbb{Z}}}\right) = \frac{F'_\alpha x}{p\mathbb{Z}} \in \frac{\mathbb{Z}}{p\mathbb{Z}}.$$

In all what follows, we write F_α for $\frac{F'_\alpha}{p\mathbb{Z}_{n\mathbb{Z}}}$.

2.2.3. The Algebra of $\left(\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}, F_\alpha\right)$ [2]

Let us recall that $\forall x, y \in \mathbb{Z}$ and for any binary law $\perp^*$ on $(\mathbb{Z}_{n\mathbb{Z}}, F'_\alpha)$, we have $x \perp^* y \in \mathbb{Z}_{n\mathbb{Z}}$. The aim is to define a binary law on $\left(\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}, F_\alpha\right)$ denoted by $\perp^*$ such that $\frac{x}{p\mathbb{Z}_{n\mathbb{Z}}} \perp^* \frac{y}{p\mathbb{Z}_{p\mathbb{Z}}} \in \frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}$ as done in $\frac{\mathbb{Z}}{p\mathbb{Z}}$.

(1) The $m\Theta$ compatibility of $(\mathbb{Z}_{n\mathbb{Z}}, F'_{\alpha})$ with ρ_p

We require that $n, p \in \mathbb{Z} : 2 \leq n \leq p(\mathbb{Z}_{n\mathbb{Z}}, F'_{\alpha})$, is a structure of $m\Theta s$ of $m\Theta$ relative integers,

$$\forall x, y \in \mathbb{Z}_{n\mathbb{Z}}, x\rho_p y \Leftrightarrow \forall \alpha \in I_*, F_\alpha x \equiv F_\alpha y (\text{mod } p).$$

Let us recall that if $x_{n\mathbb{Z}}\rho_p y_{n\mathbb{Z}}$ we write $x_{n\mathbb{Z}} \equiv y_{n\mathbb{Z}}(p\mathbb{Z}_{n\mathbb{Z}})$.

Observation 2.1. If $x \in \mathbb{Z}, x = qn + r : 0 \leq r \leq n-1$, we have $\frac{x}{p\mathbb{Z}_{n\mathbb{Z}}} = \frac{x}{p\mathbb{Z}} = \frac{r}{p\mathbb{Z}}$, $r = 0 \times n + r = 0 \times n \times p + r$; therefore $r \equiv r(\text{mod } p)$ and $r \equiv r(\text{mod } np)$.

Hence, if $x = qn + r : 0 \leq r \leq m-1$, then $x \leq r(\text{mod } n)$.

However, $x \equiv r(\text{mod } np) \Leftrightarrow q \equiv 0(\text{mod } p)$; therefore the following definition:

According to the problem of the $m\Theta$ compatibility of $(\mathbb{Z}_{n\mathbb{Z}}, F'_{\alpha})$ with $p\mathbb{Z}_{n\mathbb{Z}}$, we call $m\Theta$ representative of $\frac{a}{p\mathbb{Z}_{n\mathbb{Z}}}, a \in \mathbb{Z}_{n\mathbb{Z}}$, every $b \in \mathbb{Z}_{n\mathbb{Z}}$ satisfying following conditions:

(1) If $a \in \mathbb{Z}$ (therefore $b \in \mathbb{Z}$) and $b \equiv a\,(\text{mod } np)$.

(2) Otherwise $a \notin \mathbb{Z}$, i.e., $a = x_{n\mathbb{Z}} : (x \equiv 0(\text{mod } n))$, and therefore $b = \mathbb{Z}_{n\mathbb{Z}} : (y \equiv 0(\text{mod } n))$ and $y \equiv x(\text{mod } np)$.

Notation 2.2. We denote the set of $m\Theta$ representatives of $\frac{a}{p\mathbb{Z}_{n\mathbb{Z}}}$ by $rm\frac{a}{p\mathbb{Z}_{n\mathbb{Z}}}$.

Example 2.1. In $\mathbb{Z}_{2\mathbb{Z}}$, we have:

$1\rho_3 4$ and $3_{2\mathbb{Z}}\rho_3 9_{2\mathbb{Z}}$ but $1 + 3_{2\mathbb{Z}} = 4 \in \mathbb{Z}$ and $4 + 9_{2\mathbb{Z}} = 13_{2\mathbb{Z}} \notin \mathbb{Z}$. Thus $((1 + 3_{2\mathbb{Z}})\rho_3(4 + 9_{2\mathbb{Z}}))$.

Similarly, $1 \times 3_{2\mathbb{Z}} = 3_{2\mathbb{Z}} \notin \mathbb{Z}$ and $4 \times 9_{2\mathbb{Z}} = 36 \in \mathbb{Z}$ and so $((1 \times 3_{2\mathbb{Z}})\rho_3(4 + 9_{2\mathbb{Z}}))$.

Remark 2.2. From example it can be seen that the $m\Theta$ addition and the $m\Theta$ multiplication of $(\mathbb{Z}_{n\mathbb{Z}}, F_\alpha)$ are not compatible with $p\mathbb{Z}_{n\mathbb{Z}}$.

As a result, we have no hope to get a passage to the quotient modulo ρ_p for the structure of the $m\Theta$ ring$(\mathbb{Z}_{n\mathbb{Z}}, F_\alpha, +, \times)$ as in the classical case.

However, when restricted to $m\Theta$ representatives, + and × are compatible with $p\mathbb{Z}_{n\mathbb{Z}}$ and so we can say that + and × are $m\Theta$ compatible with $p\mathbb{Z}_{n\mathbb{Z}}$.

Definition 2.7. $\forall a, b \in \mathbb{Z}_{n\mathbb{Z}}$, we define + and × in $\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}$ as follows:

$\frac{a}{p\mathbb{Z}_{n\mathbb{Z}}} + \frac{b}{p\mathbb{Z}_{n\mathbb{Z}}} = \frac{x + y}{p\mathbb{Z}_{n\mathbb{Z}}}$ and $\frac{a}{p\mathbb{Z}_{n\mathbb{Z}}} \times \frac{b}{p\mathbb{Z}_{n\mathbb{Z}}} = \frac{x \times y}{p\mathbb{Z}_{n\mathbb{Z}}}$, $\forall x \in rm\frac{a}{p\mathbb{Z}_{n\mathbb{Z}}}$, $\forall y \in rm\frac{b}{p\mathbb{Z}_{n\mathbb{Z}}}$. $x + y$ and $x \times y$ are elements of $\mathbb{Z}_{n\mathbb{Z}}$.

Theorem 2.3. $\left(\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}, F'_\alpha, +, \times\right)$ *is a* $m\Theta$ *ring of unity* $\frac{1}{p\mathbb{Z}}$ *and of* $m\Theta$ *unity* $\frac{1_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}$.

Proof. [2].

Definition 2.8. (1) We call the $m\Theta$ ring of $m\Theta$ residual classes modulo p the $m\Theta$ ring of Theorem 2.3 above.

(2) With conditions $2 \le n \le p : p \in \mathbb{N}$, $\frac{x}{p\mathbb{Z}_{n\mathbb{Z}}}$, $x \in \mathbb{Z}_{n\mathbb{Z}}$ is said to be $m\Theta$ inversible in $\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}$, if and only if $\exists y \in \mathbb{Z}_{n\mathbb{Z}}$ such that $\frac{x}{p\mathbb{Z}_{n\mathbb{Z}}} \times \frac{y}{p\mathbb{Z}_{n\mathbb{Z}}} = \frac{1_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}$.

Corollary 2.1. *If* $\left(\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}, F'_\alpha\right)$ *is an* $m\Theta$ *field, then p is prime.*

Proof. [2].

Definition 2.9. $\frac{x}{p\mathbb{Z}_{n\mathbb{Z}}}$ is a divisor of zero in $\left(\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}, F'_\alpha\right)$ if there exists a $y \in \mathbb{Z}_{n\mathbb{Z}}$ such that $\frac{x}{p\mathbb{Z}_{n\mathbb{Z}}} \times \frac{y}{p\mathbb{Z}_{n\mathbb{Z}}} = 0$.

(2) Some Examples of the $m\Theta$ ring $\left(\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}, F'_\alpha\right)$

(1) If $n = 2$ and $p = 1$, we have $\left(\frac{\mathbb{Z}_{2\mathbb{Z}}}{\mathbb{Z}_{2\mathbb{Z}}}, F_\alpha\right)' = \{0\}$.

(2) If $n = p = 2$, we have $\left(\frac{\mathbb{Z}_{2\mathbb{Z}}}{2\mathbb{Z}_{2\mathbb{Z}}}, F_\alpha\right)' = \left\{0, \frac{1}{2\mathbb{Z}_{2\mathbb{Z}}}, \frac{1_{2\mathbb{Z}}}{2\mathbb{Z}_{2\mathbb{Z}}}, \frac{3_{2\mathbb{Z}}}{2\mathbb{Z}_{2\mathbb{Z}}}\right\}$.

(i) The table of $m\Theta$ determination of the $\mathbb{F}_{2\mathbb{Z}} = \frac{(\mathbb{Z}_{2\mathbb{Z}}, F_\alpha)}{2\mathbb{Z}_{2\mathbb{Z}}} = \left(\frac{\mathbb{Z}_{2\mathbb{Z}}}{2\mathbb{Z}_{2\mathbb{Z}}}, F'_\alpha\right)$

$\mathbb{F}_{2Z}$	0	1	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
F_0	0	1	1	0
F_1	0	1	0	1

(ii) Tables laws of $\mathbb{F}_{2\mathbb{Z}} = \frac{(\mathbb{Z}_{2\mathbb{Z}}, F_\alpha)}{2\mathbb{Z}_{2\mathbb{Z}}} = \left(\frac{\mathbb{Z}_{2\mathbb{Z}}}{2\mathbb{Z}_{2\mathbb{Z}}}, F'_\alpha\right)$. We shall write $a \in \mathbb{Z}_{2\mathbb{Z}}$ to represent $\frac{a}{2\mathbb{Z}_{2\mathbb{Z}}}$ in all what follows. For example, we shall write $1_{2\mathbb{Z}}$ to represent $\frac{1_{2\mathbb{Z}}}{2\mathbb{Z}_{2\mathbb{Z}}}$ as done in the classical ring $\frac{\mathbb{Z}}{2\mathbb{Z}}$ where we represent $\frac{1}{2\mathbb{Z}}$ by 1.

+	0	1	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
0	0	1	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
1	1	0	0	0
$1_{2\mathbb{Z}}$	$1_{2\mathbb{Z}}$	0	0	0
$3_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$	0	0	0

×	0	1	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
0	0	0	0	0
1	0	1	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
$1_{2\mathbb{Z}}$	0	$1_{2\mathbb{Z}}$	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
$3_{2\mathbb{Z}}$	0	$3_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$	$1_{2\mathbb{Z}}$

.

Observation 2.2. $\mathbb{F}_{2\mathbb{Z}} = \left(\frac{\mathbb{Z}_{2\mathbb{Z}}}{2\mathbb{Z}_{2\mathbb{Z}}}, F'_\alpha\right)$ has no divisor of zero, is an m3 ring from four elements, that is not a field.

2.2.4. Algebraic study of $(\mathbb{F}^n_{p\mathbb{Z}}, F'^n_\alpha)$

In all what follows, $n = p$, a prime integer.

Given: $k, n, p \in \mathbb{N}^*$; $2 \leq p$, prime and $k \leq n$, we set $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$ and $\mathbb{F}_{p\mathbb{Z}} = \frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}$; $\mathbb{F}^n_p = \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^n$ and $\mathbb{F}^n_{p\mathbb{Z}} = \left(\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}\right)^n$.

Observation 2.3. (1) $\mathbb{F}_p \subseteq \mathbb{F}_{p\mathbb{Z}}$ and $\mathbb{F}_p^n \subseteq \mathbb{F}_{p\mathbb{Z}}^n$.

Doted with their respective structure of $m\Theta$ sets, $(\mathbb{F}_{p\mathbb{Z}}, F'_\alpha)$ and $(\mathbb{F}_{p\mathbb{Z}}^n, F''^n_\alpha)$ are $m\Theta$ sets having for subsets of $m\Theta$ invariants $\mathbb{F}_p$ and $\mathbb{F}_p^n$, respectively. That is, $\mathbb{F}_p = C(\mathbb{F}_{p\mathbb{Z}}, F'_\alpha)$ and $\mathbb{F}_p^n = C(\mathbb{F}_{p\mathbb{Z}}^n, F''^n_\alpha)$, respectively.

(2) $\mathbb{F}_p^n$ is a $\mathbb{F}_p$-vector space of dimension n.

(3) Let $a \in \mathbb{F}_{p\mathbb{Z}}^n$, $a = (a_1, \ldots, a_n)$:

$\forall i \in \{1, \ldots, n\}$, $a_i \in \mathbb{F}_{p\mathbb{Z}}$

$\forall \alpha \in I_*$, $F'_\alpha a_i \in \mathbb{F}_p$ and so $F''^n_\alpha a = (F'_\alpha a_1, \ldots, F'_\alpha a_n) \in \mathbb{F}_p^n$.

Definition 2.10. Let $(\mathbb{F}_{p\mathbb{Z}}, F'_\alpha)$ be the $m\Theta$ field of p^2 elements and of characteristic p. $(\mathbb{F}_{p\mathbb{Z}}^n, F''^n_\alpha)$ the $m\Theta s$ product of $(\mathbb{F}_{p\mathbb{Z}}, F'_\alpha)$. Let $x, y \in \mathbb{F}_{p\mathbb{Z}}^n$; $\lambda \in \mathbb{F}_{p\mathbb{Z}}$. If $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, then we define $x + y$ and λx as follows:

$$x + y = (x_1 + y_1, \ldots, x_n + y_n) : \forall i \in \{1, \ldots, n\}, x_i + y_i \in \mathbb{F}_{p\mathbb{Z}}.$$

$\lambda x = (\lambda x_1, \ldots, \lambda x_n) : \forall i \in \{1, \ldots, n\}, \lambda x_i \in \mathbb{F}_{p\mathbb{Z}}$. $x + y$ and λx are elements of $\mathbb{F}_{p\mathbb{Z}}^n$.

Definition 2.11. We call:

(1) A modal Θ-valent monoid, every $m\Theta s(A, F_\alpha)$ that is provided of a law of internal composition which is modal Θ-valent associative. The modal Θ-valent monoid is said modal Θ-valent unitary if it possesses a modal Θ-valent unity.

(2) A modal Θ-valent group $(m\Theta g)$ every modal Θ-valent monoid modal Θ-valent unitary in which every element admits at least a modal Θ-valent inverse.

(3) A modal Θ-valent ring $(m\Theta r)$ every $m\Theta s$ (A, F_α) which is additive and multiplicative modal Θ-valent monoid. The modal Θ-valent laws + and × are linked by the modal Θ-valent distributivity.

(4) A modal Θ-valent field $(m\Theta f)$ every $m\Theta r(A, F_\alpha)$ such that every element $a \neq 0$ of A admits at least a modal Θ-valent $(m\Theta)$ inverse for the $m\Theta$ multiplication.

Example 2.2. $(\mathbb{Z}_{n\mathbb{Z}}, F_\alpha, +, \times)$ is a $m\Theta r$, with as $m\Theta$ unity $1_{n\mathbb{Z}}$. Modal Θ-valent elements $1; 1_{n\mathbb{Z}}; -1_{n\mathbb{Z}}$, respectively admit as $m\Theta$ inverse $1_{n\mathbb{Z}}; 1_{n\mathbb{Z}}; -1_{n\mathbb{Z}}$.

$1_{n\mathbb{Z}}; -1_{n\mathbb{Z}}$, respectively admit as $m\Theta$ inverse $1_{n\mathbb{Z}}; 1_{n\mathbb{Z}}; -1_{n\mathbb{Z}}$.

2.2.5. The $m\Theta$ Hamming distance [3]

Let (A, F_α) be a finite $m\Theta$ set and (A^n, F_α^n) be the $m\Theta$ product set. Let d_H be the classical hamming distance. $A\alpha \in I_*$, we define d_{H_α} on $A^n \times A^n$ as follows:

$$d_{H_\alpha}(x, y) = d_H(F_\alpha^n x, F_\alpha^n y)$$

$$= Card\{i : F_\alpha x_i \neq F_\alpha y_i, \forall i \in \{1, 2, \ldots, n\}\}$$

d_{H_α} is not a distance on (A^n, F_α^n) but it is the Hamming α-distance on $C(A^n, F_\alpha^n)$.

Definition 2.12. The $m\Theta$ distance d_{H_Θ} on $A^n \times A^n$ is defined by

$$\forall x,\ y \in A^n,\ d_{H_\Theta}(x,\ y) = \begin{cases} d_H(x,\ y), & \text{if } x,\ y \in C(A^n,\ F_\alpha^n) \\ \sum\limits_{\alpha \in I_*} d_{H_\alpha}(x,\ y), & \text{otherwise.} \end{cases}$$

3. Modal Θ-Valent Steganographic Protocols

Definition 3.1. Let $n,\ k \in \mathbb{N}^*$ such that $k \leq n$. Let $(A,\ F_\alpha)$ be a finite $m\Theta$ sets. Let $(A^n,\ F_\alpha^n)$ and $(A^k,\ F_\alpha^k)$ be the $m\Theta$ sets product of the $m\Theta$ set $(A,\ F_\alpha)$. Let e_Θ and r_Θ be the $m\Theta$ maps defined as follows:

$$e_\Theta : (A^n,\ F_\alpha^n) \times (A^k,\ F_\alpha^k) \longrightarrow (A^n,\ F_\alpha^n)$$

$$r_\Theta : (A^n,\ F_\alpha^n) \longrightarrow (A^k,\ F_\alpha^k).$$

If for every $(x,\ s) \in A^n \times A^k$, $r_\Theta \circ e_\Theta(x,\ s) = s$, then e_Θ and r_Θ are, respectively called $m\Theta$ embedding and $m\Theta$ extraction functions.

Remark 3.1. Let x and s be elements of $(A^n,\ F_\alpha)^n$ and $(A^k,\ F_\alpha^k)$.

(1) If $x \in C(A^n,\ F_\alpha^n)$ and $s \in C(A^k,\ F_\alpha^k)$, then

$$d_{H_\Theta}(x,\ e_\Theta(x,\ s)) = d_H(x,\ e_\Theta(x,\ s))$$

$$\leq \max\{d_H(x,\ e_\Theta(x,\ s)),\ s \in A^k,\ x \in A^n)\}.$$

(2) If not, then

$$d_{H_\Theta}(x,\ e_\Theta(x,\ s)) = \sum_{\alpha \in I_*} d_{H_\alpha}(x,\ e_\Theta(x,\ s))$$

$$= \sum_{\alpha \in I_*} d_H(F_\alpha^n x,\ F_\alpha^k(e_\Theta(x,\ s)))$$

$$\leq card(I_*)\max\{d_H(F_\alpha^n x,\ F_\alpha^k(e_\Theta(x,\ s))),\ x \in A^n,\ s \in A^k\}.$$

Therefore

$$\rho_\Theta = \begin{cases} \max\{d_H(x, e(x, s))\} \text{ if } s \in C(A^k, F^k_{\alpha|_{A^k}}) \text{ and } x \in C(A^n, F^n_{\alpha|_{A^n}}) \\ card(I_*)\max\{d_{H_\Theta}(F^n_\alpha x, F^k_\alpha e_\Theta(x, s))\} \text{ if not.} \end{cases}$$

Definition 3.2. ρ_Θ defined as above is called the $m\Theta$ covering radius.

Definition 3.3. Let n, k, and ρ_Θ be three positive integers such that $k \leq n$. Let (A, F_α) be a finite $m\Theta$ set. We call an $m\Theta$ steganographic protocol denoted σ_Θ over a finite $m\Theta$ (A^n, F^n_α) set to hide $m\Theta$ message of length k (secret $m\Theta$ words) in $m\Theta$ words of length n (cover $m\Theta$ words) by modifying at most ρ_Θ α-coordinate ($m\Theta$ covering radius) is a pair of $m\Theta$ maps $\sum_\Theta = (e_\Theta, r_\Theta)$ satisfying:

$$e_\Theta : (A^n \times A^k, F^n_\alpha \times F^k_\alpha) \longrightarrow (A^n, F^n_\alpha),$$

$$r_\Theta : (A^n, F^n_\alpha) \longrightarrow (A^k, F^k_\alpha).$$

$$\forall (x, s) \in A^n \times A^k, r_\Theta(e_\Theta(x, s)) = s$$

$$\forall (x, s) \in A^n \times A^k, d_{H_\Theta}(x, e_\Theta(x, s)) \leq \rho_\Theta,$$

n, k, and ρ_Θ are the parameters of the $m\Theta$ steganographic protocol $\sum_\Theta$.

Example 3.1. Let s and x be the secret $m\Theta$ word to hide and the cover $m\Theta$ word, respectively. We may suppose that those two words are sequences of symbols of a finite $m\Theta$ alphabet (A, F_α). Let be $s = (s_1, \ldots, s_k)$ and $x = (x_1, \ldots, x_n)$, $s \in A^k$ and $x \in A^n$. Let us consider the two followings $m\Theta$ map:

$e_\Theta : (A^n \times A^k, F_\alpha^n \times F_\alpha^k) \to (A^n, F_\alpha^n)$ and $r_\Theta : (A^n, F_\alpha^n) \to (A^k, F_\alpha^k)$ defined by: $e_\Theta((x_1, x_2, \ldots, x_n), (s_1, \ldots, s_K)) = (x_1, \ldots, x_{n-k}, s_1, s_2, \ldots s_k)$ and $r_\Theta(x_1, \ldots, x_n) = (x_{n-k+1}, x_{n-k+2}, \ldots, x_n)$, e_Θ and r_Θ are $m\Theta$ maps.

Let $\alpha \in I_*$,

$$\begin{aligned} F_\alpha^n \circ e_\Theta((x_1, \ldots, x_n), (s_1, \ldots, s_k)) &= F_\alpha^n(x_1, x_2, \ldots, x_{n-k}, s_1, s_2, \ldots, s_k) \\ &= (F_\alpha x_1, F_\alpha x_2, \ldots, F_\alpha x_{n-k}, F_\alpha s_1, F_\alpha s_2, \ldots, F_\alpha s_k) \\ &= e_\Theta((F_\alpha x_1, \ldots, F_\alpha x_n), (F_\alpha s_1, F_\alpha s_2, \ldots, F_\alpha s_k)) \\ &= e_\Theta(F_\alpha^n(x_1, \ldots, x_n), F_\alpha^k(s_1, \ldots, s_k)) \\ &= e_\Theta \circ (F_\alpha^n, F_\alpha^k)((x_1, \ldots, x_n), (s_1, \ldots, s_k)). \end{aligned}$$

Thus, $\forall \alpha \in I_*$, $F_\alpha^n \circ e_\Theta = e_\Theta \circ (F_\alpha^n, F_\alpha^k)$.

Let $\alpha \in I_*$,

$$\begin{aligned} F_\alpha^n \circ r_\Theta(x_1, \ldots, x_n) &= F_\alpha^k(x_{n-k+1}, x_{n-k+2}, \ldots, x_n) \\ &= (F_\alpha x_{n-k+1}, F_\alpha x_{n-k+2}, \ldots, F_\alpha) \\ &= r_\Theta \circ F_\alpha^n(x_1, \ldots, x_n). \end{aligned}$$

Then (e_Θ, r_Θ) is a $(n, k, card(I_* \max\{d_{H_\alpha}(F_\alpha^n x, F_\alpha^n(e_\Theta(x, s)))\}))m\Theta$ steganographic over (A, F_α).

$$\forall (x, s) \in A^n \times A^k$$

$$r_\Theta(x_1, x_2, \ldots, x_{n-k}, s_1, s_2, \ldots s_k) = (s_1, s_2, \ldots s_k) = s$$

$$d_{H_\Theta}(x, e_\Theta(x, s)) \leq \rho_\Theta.$$

3.1. The $m\Theta$ steganographic protocol $F_5^{2\mathbb{Z}}$

The $m\Theta$ protocol $F_5^{2\mathbb{Z}}$ over the $m\Theta$ field $F_{2\mathbb{Z}}$ permits to $m\Theta$ hide messages of length k ($m\Theta$ secret words) in $m\Theta$ words ($m\Theta$ cover words) of length $n = 2^k - 1$ by changing more than one of them (i.e., $m\Theta$ protocol of type $(2^k - 1, k, 1)$). Let $\langle F_\alpha^k m \rangle_2$ be the binary expression of m with k $m\Theta$ bits (so can consider that $\langle m \rangle_2$ is in $\mathbb{F}_{2\mathbb{Z}}^k$). Conversely, for $z \in \mathbb{F}_{2\mathbb{Z}}^k$, $\forall \alpha \in I_*$, let $\langle F_\alpha^k z \rangle_{10}$ be the integer which has $\mathbb{F}_\alpha^k z$ as binary expression, then $1 \leq \langle F_\alpha^k(z) \rangle_{10} \leq 2^k - 1$. Finally, let e_i be the i-th $m\Theta$ vector of the $m\Theta$ canonical basis of $\mathbb{F}_{2\mathbb{Z}}^{2^k-1}$; $e_0 = 0 = (0, 0)$.

Proposition 3.1. *The maps* $\gamma_{2\mathbb{Z}}$, $e_{2\mathbb{Z}}$, *and* $r_{2\mathbb{Z}}$ *define as follows*:

(i) $\gamma_{2\mathbb{Z}} : \mathbb{F}_{2\mathbb{Z}}^{2^k-1} \times \mathbb{F}_{2\mathbb{Z}}^k \to (\mathbb{N}_{2\mathbb{Z}}, F'_\alpha)$

$$(x, s) \mapsto (\langle F_\alpha^k(s) + \sum_{i=1}^{2^k-1} F_\alpha(x_i)\langle i \rangle_2 \rangle_{10})_{\alpha \in I_*};$$

(ii) $e_{2\mathbb{Z}} : \mathbb{F}_{2\mathbb{Z}}^{2^k-1} \times \mathbb{F}_{2\mathbb{Z}}^k \to \mathbb{F}_{2\mathbb{Z}}^{2^k-1}$

$$(x, s) \mapsto (F_\alpha^{2^k-1}(x) + e_{F'_\alpha(\gamma_{2\mathbb{Z}}(x, s))})_{\alpha \in I_*};$$

(iii) $r_{2\mathbb{Z}} : \mathbb{F}_{2\mathbb{Z}}^{2^k-1} \to \mathbb{F}_{2\mathbb{Z}}^k$

$$x \mapsto (\sum_{i=1}^{2^k-1} F_\alpha(x_i)\langle i \rangle_2)_{\alpha \in I_*}$$

are $m\Theta$.

Proof. (i) Let $(x, s), (y, t) \in \mathbb{F}_{2\mathbb{Z}}^{2^k-1} \times \mathbb{F}_{2\mathbb{Z}}^{k}$ let us suppose that $(x, s) = (y, t)$ (i.e., $x = y$ and $s = t$) and let show that $\gamma_{2\mathbb{Z}}(x, s) = \gamma_{2\mathbb{Z}}(y, t)$.

$$(x, s) = (y, t) \Rightarrow \begin{cases} F_\alpha^{2^k-1}x = F_\alpha^{2^k-1}y & \forall \alpha \in I_*, \\ F_\alpha^{k}s = F_\alpha^{k}t & \forall \alpha \in I_*, \end{cases}$$

$\forall \alpha \in I_*$,

$$F_\alpha^k s + \sum_{i=1}^{2^k-1} F_\alpha x_i \langle i \rangle_2 = F_\alpha^k t + \sum_{i=1}^{2^k-1} F_\alpha y_i \langle i \rangle_2$$

$$\Rightarrow \langle F_\alpha^k s + \sum_{i=1}^{2^k-1} F_\alpha x_i \langle i \rangle_2 \rangle_{10} = \langle F_\alpha^k t + \sum_{i=1}^{2^k-1} F_\alpha y_i \langle i \rangle_2 \rangle_{10}$$

$$\Rightarrow (\langle F_\alpha^k s + \sum_{i=1}^{2^k-1} F_\alpha x_i \langle i \rangle_2 \rangle_{10})_{\alpha \in I_*} = (\langle F_\alpha^k t + \sum_{i=1}^{2^k-1} F_\alpha y_i \langle i \rangle_2 \rangle_{10})_{\alpha \in I_*}$$

$$\Rightarrow \gamma_{2\mathbb{Z}}(x, s) = \gamma_{2\mathbb{Z}}(y, t).$$

Therefore the map $\gamma_{2\mathbb{Z}}$ is define well.

– Let us verify $\gamma_{2\mathbb{Z}}$ is $m\Theta$ map.

Let $(x, s), (y, t) \in \mathbb{F}_{2\mathbb{Z}}^{2^k-1} \times \mathbb{F}_{2\mathbb{Z}}^{k}$,

$\forall \alpha \in I_*$,

$$\gamma_{2\mathbb{Z}} \circ (F_\alpha^{2^k-1}, F_\alpha^k)(x, s) = \gamma_{2\mathbb{Z}}(F_\alpha^{2^k-1}x, F_\alpha^k s)$$

$$= (< F_\alpha^k (F_\alpha^k s) + \sum_{i=1}^{2^k-1} F_\alpha ((F_\alpha^{2^k-1}x)_i) < i >_2 >_{10})_{\alpha \in I_*}$$

$$= (< F_\alpha^k s + \sum_{i=1}^{2^k-1} (F_\alpha^{2^k-1}x)_i \ < i >_2 >_{10})_{\alpha \in I_*}$$

$$= (< F_\alpha^k s + \sum_{i=1}^{2^k-1} F_\alpha x_i \ < i >_2 >_{10})_{\alpha \in I_*}$$

$$F'_\alpha \circ \gamma_{2\mathbb{Z}}(x, s) = F'_\alpha(\langle F^k_\alpha s + \sum\nolimits_{i=1}^{2^k-1} F_\alpha x_i \langle i \rangle_2 \rangle_{10})_{\alpha \in I_*}$$

$$= (\langle F^k_\alpha s + \sum\nolimits_{i=1}^{2^k-1} F_\alpha x_i \langle i \rangle_2 \rangle_{10})_{\alpha \in I_*}.$$

Therefore $\gamma_{2\mathbb{Z}}$ is an $m\Theta$ map.

(ii) $(x, s), (y, t) \in \mathbb{F}^{2^k-1}_{2\mathbb{Z}} \times \mathbb{F}^k_{2\mathbb{Z}}$ let us suppose that $(x, s) = (y, t)$ (i.e., $x = y$ and $s = t$) and let show that $e_{2\mathbb{Z}}(x, s) = e_{2\mathbb{Z}}(y, t)$.

$$(x, s) = (y, t) \Rightarrow \begin{cases} F^{2^k-1}_\alpha x = F^{2^k-1}_\alpha y & \forall \alpha \in I_* \\ F^k_\alpha s = F^k_\alpha t & \forall \alpha \in I_* \end{cases}$$

$$\begin{cases} F^{2^k-1}_\alpha x = F^{2^k-1}_\alpha y & \forall \alpha \in I_* \\ F^k_\alpha s = F^k_\alpha t & \forall \alpha \in I_* \end{cases} \Rightarrow \begin{cases} F^{2^k-1}_\alpha x = F^{2^k-1}_\alpha y & \forall \alpha \in I_* \\ \gamma_{2\mathbb{Z}}(x, s) = \gamma_{2\mathbb{Z}}(y, t) \end{cases}$$

$$\Rightarrow \begin{cases} F^{2^k-1}_\alpha x = F^{2^k-1}_\alpha y & \forall \alpha \in I_* \\ F'_\alpha \gamma_{2\mathbb{Z}}(x, s) = F'_\alpha \gamma_{2\mathbb{Z}}(y, t) \end{cases}$$

$$\Rightarrow \begin{cases} F^{2^k-1}_\alpha x = F^{2^k-1}_\alpha y & \forall \alpha \in I_* \\ e_{F'_\alpha \gamma_{2\mathbb{Z}}(x, s)} = e_{F'_\alpha \gamma_{2\mathbb{Z}}(y, t)} \end{cases}$$

$$\Rightarrow F^{2^k-1}_\alpha x + e_{F'_\alpha \gamma_{2\mathbb{Z}}(x, s)} = F^{2^k-1}_\alpha y + e_{F'_\alpha \gamma_{2\mathbb{Z}}(y, t)} \forall \alpha \in I_*$$

$$\Rightarrow (F^{2^k-1}_\alpha x + e_{F'_\alpha \gamma_{2\mathbb{Z}}(x, s)})_{\alpha \in I_*} = (F^{2^k-1}_\alpha y + e_{F'_\alpha \gamma_{2\mathbb{Z}}(y, t)})_{\alpha \in I_*}$$

$$\Rightarrow e_{2\mathbb{Z}}(x, s) = e_{2\mathbb{Z}}(y, t).$$

Therefore $e_{2\mathbb{Z}}$ is define well. Let us verify $e_{2\mathbb{Z}}$ is an $m\Theta$ map.

Let $(x, s) \in \mathbb{F}_{2\mathbb{Z}}^{2^k-1} \to \mathbb{F}_{2\mathbb{Z}}^{k}$

$$e_{2\mathbb{Z}} \circ (F_\alpha^{2^k-1}, F_\alpha^k)(x, s) = e_{2\mathbb{Z}}(F_\alpha^{2^k-1}x, F_\alpha^k s)$$

$$= (F_\alpha^{2^k-1}(F_\alpha^{2^k-1}x) + e_{F'_\alpha\gamma_{2\mathbb{Z}}(F_\alpha^{2^k-1}x,\, F_\alpha^k s)})_{\alpha\in I_*}$$

$$= (F_\alpha^{2^k-1}x + e_{F'_\alpha\gamma_{2\mathbb{Z}}(x,s)})_{\alpha\in I_*} \text{ because } \gamma_{2\mathbb{Z}} \text{ is } m\Theta \text{ map.}$$

$$F'_\alpha \circ e_{2\mathbb{Z}}(x, s) = F'_\alpha(F_\alpha^{2^k-1}x + e_{F'_\alpha(\gamma_{2\mathbb{Z}}(x,\, s))})_{\alpha\in I_*}$$

$$= (F_\alpha^{2^k-1}x + e_{F'_\alpha(\gamma_{2\mathbb{Z}}(x,\, s))})_{\alpha\in I_*}.$$

Therefore $e_{2\mathbb{Z}} \circ (F_\alpha^{2^k-1}, F_\alpha^k) = F'_\alpha \circ e_{2\mathbb{Z}}$.

(iii) Let show that $r_{2\mathbb{Z}}$ is define well.

Let us suppose that $x = y$ (i.e., $F_\alpha^{2^k-1}x = F_\alpha^{2^k-1}y$) and let show that $r_{2\mathbb{Z}}x = r_{2\mathbb{Z}}y$.

Let $\alpha \in I_*$

$$F_\alpha^{2^k-1}(x) = F_\alpha^{2^k-1}(y) \Rightarrow F_\alpha x_i = F_\alpha y_i$$

$$\Rightarrow F_\alpha x_{i<i>_2} = F_\alpha y_{i<i>_2}$$

$$\Rightarrow \sum_{i=1}^{2^k-1} F_\alpha x_{i<i>_2} = \sum_{i=1}^{2^k-1} F_\alpha y_{i<i>_2}$$

$$\Rightarrow (\sum_{i=1}^{2^k-1} F_\alpha x_{i<i>_2})_{\alpha\in I_*} = (\sum_{i=1}^{2^k-1} F_\alpha y_{i<i>_2})_{\alpha\in I_*}$$

$$\Rightarrow \gamma_{2\mathbb{Z}}(x) = \gamma_{2\mathbb{Z}}(y).$$

Therefore $r_{2\mathbb{Z}}$ is an $m\Theta$ map.

Let show that $r_{2\mathbb{Z}}$ is $m\Theta$ map.

$$r_{2\mathbb{Z}} \circ F_{\alpha}^{2^k-1}(x) = r_{2\mathbb{Z}}(F_{\alpha}^{2^k-1}x)$$

$$= (\sum_{i=1}^{2^k-1} F_{\alpha}((F_{\alpha}^{2^k-1}x)_i)<i>_2)_{\alpha\in I_*}$$

$$= (\sum_{i=1}^{2^k-1} F_{\alpha}(F_{\alpha}x_i)<i>_2)_{\alpha\in I_*}.$$

Let $x \in \mathbb{F}_{2\mathbb{Z}}^{2^k-1}$, let $\alpha \in I_*$.

$$= (\sum_{i=1}^{2^k-1} F_{\alpha}x_i <i>_2)_{\alpha\in I_*}$$

$$F'_{\alpha} \circ r_{2\mathbb{Z}}(x, s) = F'_{\alpha}((\sum_{i=1}^{2^k-1} F_{\alpha}x_i <i>_2)_{\alpha\in I_*})$$

$$= (\sum_{i=1}^{2^k-1} F_{\alpha}x_i <i>_2)_{\alpha\in I_*}.$$

Therefore $r_{2\mathbb{Z}}$ is an $m\Theta$ map.

□

Proposition 3.2. $(e_{2\mathbb{Z}}, r_{2\mathbb{Z}})$ *define in the Proposition* 3.1 *above is an* $m\Theta$ *steganographic protocols.*

Proof. Let show that $(e_{2\mathbb{Z}}, r_{2\mathbb{Z}})$ is an $m\Theta$ steganographic protocol, i.e., let show that $r_{2\mathbb{Z}}(e_{2\mathbb{Z}}(x, s)) = s$, for any $s \in \mathbb{F}_{2\mathbb{Z}}^k$ and for any $x \in \mathbb{F}_{2\mathbb{Z}}^{2^k-1}$, i.e., $\forall\alpha \in I_*$, $F_{\alpha}^k(r_{2\mathbb{Z}}(e_{2\mathbb{Z}}(x, s))) = F_{\alpha}^k s$.

(1)

$$F_\alpha^k(r_{2\mathbb{Z}}(e_{2\mathbb{Z}}(x,s))) = r_{2\mathbb{Z}}(F_\alpha^{2^k-1} \circ e_{2\mathbb{Z}}(x,s)) \text{ because } r_{2\mathbb{Z}} \text{ is an } m\Theta \text{ map}$$

$$= r_{2\mathbb{Z}}(e_{2\mathbb{Z}} \circ (F_\alpha^{2^k-1}, F_\alpha^k))(x,s) \text{ because } e_{2\mathbb{Z}} \text{ is an } m\Theta \text{ map}$$

$$= r_{2\mathbb{Z}}(e_{2\mathbb{Z}}(F_\alpha^{2^k-1}x, F_\alpha^k s))$$

$$= r_{2\mathbb{Z}}(F_\alpha^{2^k-1}x + e_{F'_\alpha(\gamma_{2\mathbb{Z}}(x,s))}),$$

we put

$$j = F'_\alpha(\gamma_{2\mathbb{Z}}(x,s)) = \gamma_{2\mathbb{Z}} \circ (F_\alpha^{2^k-1}, F_\alpha^k)(x,s)$$

$$= \gamma_{2\mathbb{Z}}(F_\alpha^{2^k-1}x, F_\alpha^k s)$$

$$= <F_\alpha^k(F_\alpha^k s) + \sum_{i=1}^{2^k-1} F_\alpha((F_\alpha^{2^k-1}x)_i)<i>_2>_{10}$$

$$= <F_\alpha^k s + \sum_{i=1}^{2^k-1} F_\alpha(F_\alpha x_i)<i>_2>_{10}$$

$$= <F_\alpha^k s + \sum_{i=1}^{2^k-1} F_\alpha(x_i)<i>_2>_{10}$$

$$<j>_2 = F_\alpha^k s + \sum_{i=1}^{2^k-1} F_\alpha(x)<i>_2. \quad (*)$$

(2)

$$r_{2\mathbb{Z}}(F_\alpha^{2^k-1}x + e_j) = r(F_\alpha x_1, F_\alpha x_2, \ldots, F_\alpha x_j + 1, \ldots, F_\alpha x_n)$$

$$= \sum_{i=1, i\neq j}^{2^k-1} F_\alpha(F_\alpha x_i)<i>_2 + (F_\alpha x_j + 1)<j>_2,$$

changing $<j>_2$ by

$$= \sum_{i=1, i\neq j}^{2^k-1} F_\alpha(x_i)<i>_2 + (F_\alpha x_j + 1)<j>_2$$

expression given in $(*)$ we obtain:

$$r_{2\mathbb{Z}}(F_\alpha^{2^k-1}x + e_j) = F_\alpha^k s \text{ so } \forall \alpha \in I_*,\ F_\alpha^k(r_{2\mathbb{Z}}(e_{2\mathbb{Z}}(x, s))) = F_\alpha^k s.$$

Therefore, $r_{2\mathbb{Z}}(e_{2\mathbb{Z}}(x, s)) = s$. Thus $F_5^{2\mathbb{Z}}$ is an $m\Theta$ steganographic protocol. □

Remark 3.2.

• Insert an $m\Theta$ messages by $F_5^{2\mathbb{Z}}$ in an $m\Theta$ covering consists to change the $m\Theta$ coordinate number $\gamma_{2\mathbb{Z}}(x, s)$.

• $m\Theta$ extraction consists to add all $m\Theta$ products of each $m\Theta$ component to the value of the $F_{2\mathbb{Z}}$ expression of the $m\Theta$ index, i.e., $r_{2\mathbb{Z}}(x) = \sum_{i=1}^{2^k-1} F_\alpha x_i <i>_2$.

Example 3.2. For $n = 7$, $k = 3$, how to insert $s = 01_{2\mathbb{Z}}1_{2\mathbb{Z}}$ in $x = 1_{2\mathbb{Z}}1_{2\mathbb{Z}}003_{2\mathbb{Z}}01_{2\mathbb{Z}}$.

$$F_1^3 s = 011,\ F_2^3 s = 000,\ F_1^3 x = 1100001,\ F_2^3 x = 0000100,$$

i.e., how to calculate $e_{2\mathbb{Z}}(01_{2\mathbb{Z}}1_{2\mathbb{Z}}, 1_{2\mathbb{Z}}1_{2\mathbb{Z}}003_{2\mathbb{Z}}01_{2\mathbb{Z}})$.

$$\gamma_{2\mathbb{Z}}(1_{2\mathbb{Z}}1_{2\mathbb{Z}}003_{2\mathbb{Z}}01_{2\mathbb{Z}}, 01_{2\mathbb{Z}}1_{2\mathbb{Z}}) = (<F_1^3(01_{2\mathbb{Z}}1_{2\mathbb{Z}}) + \sum_{i=1}^{7} F_1^7 x_i <i>_2 >_{10}, <F_2^3(01_{2\mathbb{Z}}1_{2\mathbb{Z}}) + \sum_{i=1}^{7} F_2^7 x_i <i>_2 >_{10}).$$

Or

$$<F_1^3(01_{2\mathbb{Z}}1_{2\mathbb{Z}}) + \sum_{i=1}^{7} F_1^7 x_i <i>_2 >_{10} = <011 + 1(001) + 1(010) + 1(111)>_{10} = 7,$$

and

$$< F_2^3(01_{2\mathbb{Z}}1_{2\mathbb{Z}}) + \sum_{i=1}^{7} F_2^7 x_i <i>_2 >_{10} = <000 + 1(101)>_{10} = 5$$

$$\gamma_{2\mathbb{Z}}(x, s) = (7; 5) = (F_1'(\gamma_{2\mathbb{Z}}(x, s)); F_2'(\gamma_{2\mathbb{Z}}(x, s)))$$

$$e_{2\mathbb{Z}}(x, s) = (F_1^7 x + e_{F_1'(\gamma_{2\mathbb{Z}}(x, s))}; F_2^7 x + e_{F_2'(\gamma_{2\mathbb{Z}}(x, s))})$$

$$F_1^7 x + e_{F_1'(\gamma_{2\mathbb{Z}}(x, s))} = 1100001 + e_7 = 1100001 + 0000001 = 1100000$$

$$F_2^7 x + e_{F_2'(\gamma_{2\mathbb{Z}}(x, s))} = 0000100 + e_5 = 0000100 + 0000100 = 0000000$$

$$e_{2\mathbb{Z}}(x, s) = (1100000, 0000000) = 1_{2\mathbb{Z}}1_{2\mathbb{Z}}00000 = v.$$

How to extract the $m\Theta$ message hidden s in the message $v = 1_{2\mathbb{Z}}1_{2\mathbb{Z}}00000$?, i.e., how to calculate $r_{2\mathbb{Z}}(1_{2\mathbb{Z}}1_{2\mathbb{Z}}00000)$?. By applying the second point of the previous remark we get that:

$$r_{2\mathbb{Z}}(v) = (\sum_{i=1}^{7} F_1 v_i <i>_2, \sum_{i=1}^{7} F_2 <i>_2)$$

$$r_{2\mathbb{Z}}(v) = (1(001) + 1(010); 1(000)) = (011; 000) = 01_{2\mathbb{Z}}1_{2\mathbb{Z}} = s.$$

4. $m\Theta$ Codes and Pseudo $m\Theta$ Codes Defined by an $m\Theta$ Steganographic Protocol; Construction of an $m\Theta$ Steganographic Protocol

Let $(\mathcal{C}, F_{\alpha|\mathcal{C}}^n)$ be an $m\Theta$ code of length n on an $m\Theta$ alphabet (A, F_α), $(\mathcal{C}, F_{\alpha|\mathcal{C}}^n)$ is an $m\Theta$ subset of (A^n, F_α^n). Recall that an $m\Theta$ correcting code of length n on an $m\Theta$ alphabet (A, F_α) is an $m\Theta$ subset of (A^n, F_α^n), and the $m\Theta$ covering radius ρ_Θ of an $m\Theta$ correcting code satisfies $\forall x = (x_1, \cdots, x_n) \in (A^n, F_\alpha^n)$:

$$d_{H_\Theta}(x, (\mathcal{C}, F^n_{\alpha|\mathcal{C}})) = \begin{cases} \min\limits_{c \in C(\mathcal{C}, F^n_{\alpha|\mathcal{C}})} d_H(x; c) & \text{if } x \in C(A^n, F^n_{\alpha|_{A^n}}) \\ \min\limits_{c \in \mathcal{C}} d_{H_\Theta}(x; c) & \text{if not} \end{cases}$$

$$= \begin{cases} \min\limits_{c=(c_1, \ldots, c_n) \in C(\mathcal{C}, F^n_{\alpha|\mathcal{C}})} |i : x_i \neq c_i| & \text{if } x = (x_1, \ldots, x_n) \in C(A^n, F^n_{\alpha|_{A^n}}) \\ \min\limits_{c \in \mathcal{C}} \sum\limits_{\alpha \in I_*} |\{i : F_\alpha x_i \neq F_\alpha c_i, \forall_i \in \{1, \ldots, n\}\}| & \text{if not} \end{cases}$$

$$\leq \rho_\Theta.$$

Definition 4.1. An $m\Theta$ steganographic protocol (e_Θ, r_Θ) of length n is said to be proper if the $m\Theta$ embedding functions e_Θ is such that: $e_\Theta(x, s)$ is the nearest element to x belonging to $r_\Theta^{-1}(s) = \{y \in (A^n, F^n_\alpha) \mid r_\Theta(y) = s\}$.

Proposition 4.1. *If an $m\Theta$ steganographic protocol (e_Θ, r_Θ) is proper then the $m\Theta$ covering radius ρ_Θ is given by*:

$$\rho_\Theta = \begin{cases} \max\{d_H(x, r_\Theta^{-1}(s))\} \text{ if } s \in C(A^k; F^k_{\alpha|_{A^k}}) \text{ and } x \in C(A^n, F^n_{\alpha|_{A^n}}) \\ card(I_*) \max\{d_H(F^n_\alpha x, r^{-1}(F^n_\alpha(s)))\} \text{ if } s \in A^k \backslash C(A^k, F^k_{\alpha|_{A^k}}) \\ \text{or } x \in A^n \backslash C(A^n, F^n_{\alpha|_{A^n}}). \end{cases}$$

Proof. Let $x \in A^n$ and $s \in A^k$

- If $x \in C(A^n, F^n_{\alpha|_{A^n}})$ and $s \in C(A^k, F^k_{\alpha|_{A^k}})$ then if $e_\Theta(x, s) = v$,

then $d_{H_\Theta}(x, v) = d_H(x, v) = \min\{d_H(x, y) / y \in r_\Theta^{-1}(s) = d(x, r_\Theta^{-1}(s))\}$. Since that

$$\rho_\Theta = \max\left\{d(x, e_\Theta(x, s)) / s \in C(A^k, F^k_{\alpha|_{A^k}}), x \in C(A^n, F^n_{\alpha|_{A^n}})\right\},$$

we have

$$\rho_\Theta = \max\left\{d(x, r_\Theta^{-1}(s))/s \in C(A^k, F_\alpha^k),\ x \in C(A^n, F_\alpha^n)\right\}.$$

- If not, then $x \in A^n \backslash C(A^n, F_\alpha^n)$ or $s \in A^k \backslash C(A^k, F_\alpha^k)$. If $e_\Theta(x, s) = v$, then $\forall \alpha \in I_*$, $F_\alpha^n(e_\Theta(x, s)) = F_\alpha^n(v)$

$$\Rightarrow \forall \alpha \in I_*,\ d_H(F_\alpha^n x, F_\alpha^n v) = \min\{d_H(F_\alpha^n x, F_\alpha^n y)/F_\alpha^n y \in r_\Theta^{-1}(F_\alpha^n(s))\}$$

$$= d(F_\alpha^n x, r^{-1}(F_\alpha^n(s)))$$

we have $\rho_\Theta = card(I_*)\max\{d_H(F_\alpha^n x, r^{-1}(F_\alpha^n(s))),\ s \in A^k \backslash C(A^k, F_\alpha^k)$, or $x \in A^n \backslash C(A^n, F_\alpha^n)\}$.

□

Let $\Upsilon_\Theta = (e_\Theta, r_\Theta)$ be an $m\Theta$ steganographic protocol. The $m\Theta$ protocol Υ_Θ define a collection F_{Υ_Θ} of $m\Theta$ correcting codes and pseudo $m\Theta$ codes defined by:

$$F_{\Upsilon_\Theta} = \{C_s = r_\Theta^{-1}(s)/s \in A^k\}.$$

Let x be an element of $(A^n, F_\alpha^n)_{\alpha \in I_*}$.

If $x \in C(A^n, F_\alpha^n)$, to decode x we proceed in this way: if ρ_Θ is the $m\Theta$ radius of γ_Θ, then there exists a word x' satisfying: $d_H(x, x') \le \rho_\Theta$ and $r_\Theta(x) = s$.

Then $r_\Theta(e_\Theta(x, s)) = s$ which means that $e_\Theta(x, s)$ is a word decoding x relative to the code $C(c_s, F^n_{\alpha\backslash_{c_s}})$. If $x \in A^n \backslash C(A^n, F_\alpha^n)$, to decode x we proceed in this way: if ρ_Θ is the $m\Theta$ radius of γ, then there exists an $m\Theta$ word x' satisfying $\forall \alpha \in I_*$, $d_H(F_\alpha^n(x), F_\alpha^n(x')) \le \rho_\Theta$ and $r_\Theta(F_\alpha^n(x')) = F_\alpha^n(s)$. Thus $d_{H_\Theta}(x, x') \le \rho_\Theta$ and $r_\Theta(x') = s$. Then $r_\Theta(e_\Theta(x, s)) = s$ which means that $e_\Theta(x, s)$ is an $m\Theta$ word decoding x relative to the $m\Theta$ code $(C_s, F^n_{\alpha\backslash_{C_s}})$.

To build an $m\Theta$ steganographic protocol of parameters (n, k, ρ_Θ) on an $m\Theta$ alphabet (A, F_α), one way is to start by building a surjective $r_\Theta : (A^n, F_\alpha^n) \to (A^k, F_\alpha^k)$ which $m\Theta$ map r_Θ define a family $F_{\gamma_\Theta} = \{C_s = r_\Theta^{-1}(s)/s \in A^k\}$ of $m\Theta$ codes and pseudo $m\Theta$ codes on (A, F_α) of length n.

Example 4.1. To build an $m\Theta$ steganographic protocol of parameters (3, 2, 4) on $\mathbb{F}_{2\mathbb{Z}} = \{0, 1, 1_{2\mathbb{Z}}, 3_{2\mathbb{Z}}\}$, start with given an $m\Theta$ surjective function $r_\Theta : \mathbb{F}_{2\mathbb{Z}}^3 \to \mathbb{F}_{2\mathbb{Z}}^2$, if $r_\Theta : \mathbb{F}_{2\mathbb{Z}}^3 \to \mathbb{F}_{2\mathbb{Z}}^2$, is such that: $\forall(x, y) \in \mathbb{F}_{2\mathbb{Z}}$, $r_\Theta^{-1}(x, y) = \{(x, y, z)\forall z \in \mathbb{F}_{2\mathbb{Z}}\}$.

$$r_\Theta^{-1}(00) = \{000, 001, 001_{2\mathbb{Z}}, 003_{2\mathbb{Z}}\},$$

$$r_\Theta^{-1}(01) = \{010, 011, 011_{2\mathbb{Z}}, 013_{2\mathbb{Z}}\},$$

$$r_\Theta^{-1}(10) = \{100, 101, 101_{2\mathbb{Z}}, 103_{2\mathbb{Z}}\},$$

$$r_\Theta^{-1}(11) = \{110, 111, 111_{2\mathbb{Z}}, 113_{2\mathbb{Z}}\},$$

are $m\Theta$ codes

$$r_\Theta^{-1}(01_{2\mathbb{Z}}) = \{01_{2\mathbb{Z}}0, 01_{2\mathbb{Z}}1, 01_{2\mathbb{Z}}1_{2\mathbb{Z}}, 01_{2\mathbb{Z}}3_{2\mathbb{Z}}\},$$

$$r_\Theta^{-1}(03_{2\mathbb{Z}}) = \{03_{2\mathbb{Z}}0, 03_{2\mathbb{Z}}1, 03_{2\mathbb{Z}}1_{2\mathbb{Z}}, 03_{2\mathbb{Z}}3_{2\mathbb{Z}}\},$$

$$r_\Theta^{-1}(11_{2\mathbb{Z}}) = \{11_{2\mathbb{Z}}0, 11_{2\mathbb{Z}}1, 11_{2\mathbb{Z}}1_{2\mathbb{Z}}, 11_{2\mathbb{Z}}3_{2\mathbb{Z}}\},$$

$$r_\Theta^{-1}(13_{2\mathbb{Z}}) = \{13_{2\mathbb{Z}}0, 13_{2\mathbb{Z}}1, 13_{2\mathbb{Z}}1_{2\mathbb{Z}}, 13_{2\mathbb{Z}}3_{2\mathbb{Z}}\},$$

$$r_\Theta^{-1}(1_{2\mathbb{Z}}0) = \{1_{2\mathbb{Z}}00, 1_{2\mathbb{Z}}01, 1_{2\mathbb{Z}}01_{2\mathbb{Z}}, 1_{2\mathbb{Z}}03_{2\mathbb{Z}}\},$$

$$r_\Theta^{-1}(3_{2\mathbb{Z}}0) = \{3_{2\mathbb{Z}}00, 3_{2\mathbb{Z}}01, 3_{2\mathbb{Z}}01_{2\mathbb{Z}}, 3_{2\mathbb{Z}}03_{2\mathbb{Z}}\},$$

$$r_\Theta^{-1}(1_{2\mathbb{Z}}1) = \{1_{2\mathbb{Z}}10, 1_{2\mathbb{Z}}11, 1_{2\mathbb{Z}}11_{2\mathbb{Z}}, 1_{2\mathbb{Z}}13_{2\mathbb{Z}}\},$$

$$r_\Theta^{-1}(3_{2\mathbb{Z}}1) = \{3_{2\mathbb{Z}}10,\ 3_{2\mathbb{Z}}11,\ 3_{2\mathbb{Z}}11_{2\mathbb{Z}},\ 3_{2\mathbb{Z}}13_{2\mathbb{Z}}\},$$

$$r_\Theta^{-1}(3_{2\mathbb{Z}}1_{2\mathbb{Z}}) = \{3_{2\mathbb{Z}}1_{2\mathbb{Z}}0,\ 3_{2\mathbb{Z}}1_{2\mathbb{Z}}1,\ 3_{2\mathbb{Z}}1_{2\mathbb{Z}}1_{2\mathbb{Z}},\ 3_{2\mathbb{Z}}1_{2\mathbb{Z}}3_{2\mathbb{Z}}\},$$

$$r_\Theta^{-1}(3_{2\mathbb{Z}}3_{2\mathbb{Z}}) = \{3_{2\mathbb{Z}}3_{2\mathbb{Z}}0,\ 3_{2\mathbb{Z}}3_{2\mathbb{Z}}1,\ 3_{2\mathbb{Z}}3_{2\mathbb{Z}}1_{2\mathbb{Z}},\ 3_{2\mathbb{Z}}3_{2\mathbb{Z}}3_{2\mathbb{Z}}\},$$

$$r_\Theta^{-1}(1_{2\mathbb{Z}}1_{2\mathbb{Z}}) = \{1_{2\mathbb{Z}}1_{2\mathbb{Z}}0,\ 1_{2\mathbb{Z}}1_{2\mathbb{Z}}1,\ 1_{2\mathbb{Z}}1_{2\mathbb{Z}}1_{2\mathbb{Z}},\ 1_{2\mathbb{Z}}1_{2\mathbb{Z}}3_{2\mathbb{Z}}\},$$

$$r_\Theta^{-1}(1_{2\mathbb{Z}}3_{2\mathbb{Z}}) = \{1_{2\mathbb{Z}}3_{2\mathbb{Z}}0,\ 1_{2\mathbb{Z}}3_{2\mathbb{Z}}1,\ 1_{2\mathbb{Z}}3_{2\mathbb{Z}}1_{2\mathbb{Z}},\ 1_{2\mathbb{Z}}3_{2\mathbb{Z}}3_{2\mathbb{Z}}\},$$

are pseudo $m\Theta$ codes.

Therefore $e_\Theta(000, -) : \mathbb{F}_{2\mathbb{Z}}^3 \to \mathbb{F}_{2\mathbb{Z}}^3$ satifies $e_\Theta(000, 00) = 000$ since $d_{H_\Theta}(000, x') = d_{H_\Theta}(000, c_{00}) = 0$. More generally,

$$\begin{aligned} e_\Theta : \mathbb{F}_{2\mathbb{Z}}^3 \times \mathbb{F}_{2\mathbb{Z}}^2 &\to \mathbb{F}_{2\mathbb{Z}}^3 \\ (x, s) &\mapsto e_\Theta(x, s) = d_{H_\Theta}(x, c_s). \end{aligned}$$

If $s = 10$ and $x = 111$, then we have:

$d_{H_\Theta}(111; C_{10}) = d_{H_\Theta}(111; \{100,\ 101, 101_{2\mathbb{Z}}, 103_{2\mathbb{Z}}\}) = 1$, x' is 101 because

$$d_{H_\Theta}(111; 101) = 1.$$

Thus $r_\Theta^{-1}(a\,b) = \{(a, b, c) | c \in \mathbb{F}_{2\mathbb{Z}}\} = \mathcal{C}_{a\,b}$.

Proposition 4.2. *An $m\Theta$ map $r_\Theta : (A^n, F_\alpha^n) \to (A^k, F_\alpha^k)$ is an $m\Theta$ extraction map of an $m\Theta$ $[n, k]$-steganographic protocol if and only if r_Θ is $m\Theta$ surjective.*

Proof. Indeed if $r_\Theta : (A^n, F_\alpha^n) \to (A^k, F_\alpha^k)$ is an $m\Theta$ extraction function of an $m\Theta$ $[n, k]$-steganographic protocol, then for all $x \in (A^n, F_\alpha^n)$ we have $r_\Theta \circ e_\Theta(x, \cdot) = I_{A^k}$, so r_Θ is $m\Theta$ surjective. If $r_\Theta : (A^n, F_\alpha^n)$

$\to (A^k, F_\alpha^k)$ is $m\Theta$ surjective then there exists an $m\Theta$ embedding map e_Θ such that (e_Θ, r_Θ) is an $m\Theta$ steganographic protocol of parameters (n, k, ρ_Θ).

For all $t \in \mathbb{R}$ and for all $x_0 \in (A^n, F_\alpha^n)$ put

$$B_\Theta(x_0, t) = \{y \in (A^n, F_\alpha^n) | d_{H_\Theta}(x_0, y) \le t\}.$$

□

Lemma 4.1. *For all (n, k, ρ_Θ)-steganographic protocol (e_Θ, r_Θ) over an $m\Theta$ alphabet (A, F_α) and for all $x_0 \in (A^n, F_\alpha^n)$ the $m\Theta$ map $r_{\Theta|B(x_0, \rho_\Theta)}$, the restriction of r_Θ to the ball $B(x_0, \rho_\Theta)$, is $m\Theta$ surjective or,*

$$r_{\Theta|B(x_0, \rho)} : B(x_0, \rho_\Theta) \to (A^k, F_\alpha^k)$$

$$y \to r_\Theta(y),$$

is an $m\Theta$ surjective map.

Proposition 4.3. *The $m\Theta$ map $r_{\Theta|B(x_0, \rho_\Theta)}$, is well defined. Let consider $s \in (A^k, F_\alpha^k)$, since e_Θ is the $m\Theta$ embedding map of the (n, k, ρ_Θ)-steganographic protocol (e_Θ, r_Θ), then $d_\Theta(x_0, e_\Theta(s, x_0)) \le \rho_\Theta$. Let $y = e_\Theta(s, x_0)$ then $d_\Theta(x_0, y) \le \rho_\Theta$ and $r_\Theta(y) = r_\Theta(e_\Theta(x_0, s)) = s$. That proves the existence of $y \in B(x_0, \rho_\Theta)$ such that $r_{\Theta|B(x_0, \rho_\Theta)}(y) = s$.*

5. Protocol Steganography Using $m\Theta$ Codes

Proposition 5.1. *Let* $\mathbb{F}_q$ *be a finite field such that* $\mathbb{F}_q = \mathbb{F}_p(\beta)$, *where* p *is a prime interger and* β *is a primitive element such that* $q = p^n$.

$$\mathbb{F}_q = \mathbb{F}_p(\beta) = \left\{ \sum_{i=0}^{n} a_i \beta^i,\ a_i \in \mathbb{F}_p \right\}.$$

Let $\left(\mathbb{F}_{p\mathbb{Z}}, F_\alpha\right)$ *be the finite* $m\Theta$ *field with* p^2 *elements such that* $C\left(\mathbb{F}_{p\mathbb{Z}}, F_\alpha\right) = \mathbb{F}_p$. *Let set* $\mathbb{K}_{p\mathbb{Z}} = \left\{ \sum_{i=0}^{n} a_i \beta^i,\ a_i \in \mathbb{F}_{p\mathbb{Z}} \right\}$. *Let for every* $\alpha \in I_*$, *define* $\mathcal{F}'_\alpha : \mathbb{K}_{p\mathbb{Z}} \to \mathbb{K}_{p\mathbb{Z}}$, $\sum_{i=0}^{n} a_i \beta^i \mapsto F'_\alpha\left(\sum_{i=0}^{n} a_i \beta^i\right) = \sum_{i=0}^{n} F_\alpha(a_i)\beta^i$, $\left(\mathbb{K}_{p\mathbb{Z}}, F'_\alpha\right)$ *is a finite* $m\Theta$ *field such that* $C\left(\mathbb{K}_{p\mathbb{Z}}, F'_\alpha\right) = \mathbb{F}_q$.

Proof. [2].

Proposition 9.13, p.304.

Proposition 5.2. *Let* $\mathcal{C}$ *be a linear code of length N, of dimension* k, *of alphabet* $\mathbb{F}_q$, *having* G *as generator matrix. Let* $f : \mathbb{F}_q^k \to \mathbb{F}_q^N$, $x \mapsto xG$ *the encoder of* $\mathcal{C}$. $f^\Theta : \mathbb{K}_{p\mathbb{Z}}^k \to \mathbb{K}_{p\mathbb{Z}}^N$, $x \mapsto xG$ *a map. If* f^Θ *is an* $m\Theta$ *map* (*i.e.*, $\forall x \in I_*,\ F'^N_\alpha \circ f^\Theta = f^\Theta \circ F'^k_\alpha$), *then*

(1) f^Θ *is a linear and injective map.*

(2) $\left(\mathrm{Im}(f^\Theta), F'^N_{\alpha_{|\mathrm{Im}(f^\Theta)}}\right)$ *is a linear* $m\Theta$ *code such that* $C\left(\mathrm{Im}(f^\Theta), F'^N_{\alpha_{|\mathrm{Im}(f^\Theta)}}\right) = \mathcal{C}$ *called the canonical* $m\Theta$ *extension of* $\mathcal{C}$.

(3) *If* f^{Θ} *is not an* $m\Theta$, *then let set* $E = \mathbb{K}_p^k \cup \{x \in \mathbb{K}_{p\mathbb{Z}}^k \backslash \mathbb{K}_p^k / (F_\alpha^k(x)G)_{\alpha \in I_*} \in \mathbb{K}_{p\mathbb{Z}}^N\}$ *and*

$$g^{\Theta} : E \to \mathbb{K}_{p\mathbb{Z}}^N$$

$$x \mapsto \begin{cases} xG \text{ if } x \in \mathbb{K}_p^k \\ (F_\alpha^k(x)G)_{\alpha \in I_*} \text{ if not} \end{cases}$$

(i) g^{Θ} *is a non linear map that is* $m\Theta$ *and injective.*

(ii) $(\mathrm{Im}(g^{\Theta}), F^N_{\alpha_{|\mathrm{Im}(g^{\Theta})}})$ *is non linear* $m\Theta$ *code such that* $C(\mathrm{Im}(g^{\Theta}), F^N_{\alpha_{|\mathrm{Im}(g^{\Theta})}}) = \mathcal{C}$, *called the canonical* $m\Theta$ *pseudo extension of the classical linear code* $\mathcal{C}$.

Proof. [10].

It comes from the proof of the propositions 0.18, 0.19, 0.20, 0.21.

Definition 5.1. Let denote $\mathrm{Im}(f^{\Theta}) = \mathcal{C}^{\Theta}$, $(\mathcal{C}^{\Theta}, F'^N_{\alpha_{|\mathcal{C}^{\Theta}}})$ is called the canonical $m\Theta$ extension of the classical linear code $\mathcal{C}$.

Proposition 5.3. *Let* $(\mathcal{C}, F^n_{\alpha_{|C}})$ *be a linear* $m\Theta$ *code of length* n, *of dimension* k *and of* $m\Theta$ *alphabet* $(\mathbb{K}_{p\mathbb{Z}}, F'_\alpha)$. *The subset of* $m\Theta$ *invariant elements* $C(\mathcal{C}, F^n_{\alpha_{|C}})$ *is a classical linear code of length* n, *of dimension* k *and of alphabet* $\mathbb{K}_p = \mathbb{F}_q = \mathbb{F}_p(\beta)$.

Proof. [3].

5.1. Connection with the $m\Theta$ coding theory

Let $\mathcal{C}$ be a linear classical code of length N, of dimension k, of alphabet $\mathbb{F}_q$ having parity check matrix H and covering raduis ρ. Let $(\mathcal{C}^{\Theta}, F_{\alpha}'^{N})$ be a canonical $m\Theta$ extension or a canonical $m\Theta$ pseudo extension of $\mathcal{C}$.

Let $a \in \mathbb{K}_{p\mathbb{Z}}^{N}$, we have $a = (F_{\alpha}'^{N}(a))_{\alpha \in I_*}$ and $\forall \alpha \in I_*$, $F_{\alpha}'^{N}(a) \in \mathbb{K}_{p}^{N}$.

Let sets $F = (\mathbb{K}_{p}^{N} \times \mathbb{K}_{p}^{N-k}) \cup \{(x, s) \in (\mathbb{K}_{p\mathbb{Z}}^{N} \setminus \mathbb{K}_{p}^{N}) \times (\mathbb{K}_{p\mathbb{Z}}^{N-k} \setminus \mathbb{K}_{p}^{N-k}) / (F_{\alpha}'^{N}(x) - F_{\alpha}'^{N}(e))_{\alpha \in I_*} \in \mathbb{K}_{p\mathbb{Z}}^{N}\}$ and

$$G = \mathbb{K}_{p}^{N} \cup \{y \in \mathbb{K}_{p\mathbb{Z}}^{N} \setminus \mathbb{K}_{p}^{N} / (HF_{\alpha}'^{N-k}(y))_{\alpha \in I_*} \in \mathbb{K}_{p\mathbb{Z}}^{N-k}\}.$$

Let $(x, s) \in F \setminus (\mathbb{K}_{p}^{N} \times \mathbb{K}_{p}^{N-k})$ $y \in G \setminus \mathbb{K}_{p}^{N}$. To insert s in x, the principle is to modify x in y such a way that $\forall \alpha \in I_*$, $HF_{\alpha}'^{N}(y) = F_{\alpha}'^{N-k}(s)$. We then check the vector $e \in \mathbb{K}_{p\mathbb{Z}}^{N}$ which modifies x in y, i.e., for every $\alpha \in I_*$, we check $F_{\alpha}'^{N}(e)$ which modifies $F_{\alpha}'^{N}(x)$ in $F_{\alpha}'^{N}(y)$

$$F_{\alpha}'^{N}(y) = F_{\alpha}'^{N}(x) - F_{\alpha}'^{N}(e)$$
$$\Rightarrow HF_{\alpha}'^{N}(e) = F_{\alpha}'^{N-k}(s) - HF_{\alpha}'^{N}(x).$$

The optimal α-vector is the α-chief of the α-coset $C(F_{\alpha}'^{N-k}(s) - HF_{\alpha}'^{N}(x)) = \{F_{\alpha}'^{N}(c) \in \mathbb{K}_{p}^{N} = \mathbb{F}_{q}^{N} / HF_{\alpha}'^{N}(c) = F_{\alpha}'^{N-k}(s) - HF_{\alpha}'^{N}(x)\}$.

Proposition 5.4. *Let Emb and Ext defined as follows*:

$$Emb : F \to G$$

$$(x, s) \mapsto \begin{cases} x - e = y \text{ if } (x, s) \in \mathbb{K}_p^N \times \mathbb{K}_p^{N-k} \\ (F_\alpha'^N(x) - F_\alpha'^N(e))_{\alpha \in I_*} \text{ if not} \end{cases}$$

$$Emb(x, s) = \begin{cases} x - e = y \text{ if } (x, s) \in \mathbb{K}_p^N \times \mathbb{K}_p^{N-k} \\ (F_\alpha'^N(x) - F_\alpha'^N(e))_{\alpha \in I_*} \text{ if not} \end{cases}$$

$$Ext : G \to \mathbb{K}_{p\mathbb{Z}}^{N-k}$$

$$y \mapsto \begin{cases} Hy \text{ if } y \in \mathbb{K}_p^N \\ (HF_\alpha'^{N-k}(y))_{\alpha \in I_*} \text{ if not} \end{cases}$$

Emb and Ext are mΘ map such that $Ext(Emb(x, s)) = s$.

□

Let $\lambda \in I_*$ and $(x, s) \in F$.

If $(x, s) \in \mathbb{K}_p^N \times \mathbb{K}_p^{N-k}$

$$\begin{aligned} F_\lambda'^N(Emb(x, s)) &= F_\alpha'^N(x - e) \\ &= x - e \\ &= y \\ &= Emb(F_\lambda'^N(x), F_\lambda'^{N-k}(s)) \\ &= Emb \circ (F_\lambda'^N \times F_\lambda'^{N-k})(x, s). \end{aligned}$$

If $(x, s) \in (\mathbb{K}_{p\mathbb{Z}}^{N} \backslash \mathbb{K}_{p}^{N}) \times (\mathbb{K}_{p\mathbb{Z}}^{N-k} \backslash \mathbb{K}_{p}^{N-k})$

$$\begin{aligned} F_{\lambda}'^{N}(Emb(x, s)) &= F_{\lambda}'^{N}((F_{\alpha}'^{N}(x) - F_{\alpha}'^{N}(e))_{\alpha \in I_*}) \\ &= F_{\lambda}'^{N}(x) - F_{\lambda}'^{N}(e) \\ &= Emb(F_{\lambda}'^{N}(x), F_{\lambda}'^{N-k}(s)) \\ &= Emb(F_{\lambda}'^{N} \times F_{\lambda}'^{N-k}(x, s)). \end{aligned}$$

Let $\alpha \in I_*$ and $y \in G$.

If $y \in \mathbb{K}_{p}^{N}$,

$$\begin{aligned} F_{\lambda}'^{N-k}(Ext(y)) &= F_{\lambda}'^{N-k}(Hy) \\ &= Hy \\ &= HF_{\lambda}'^{N}(y) \\ &= Ext(F_{\lambda}'^{N}(y)) \\ &= Ext(F_{\lambda}'^{N}(y)). \end{aligned}$$

If $y \in G \backslash \mathbb{K}_{p}^{N}$

$$\begin{aligned} F_{\lambda}'^{N-k}(Ext(y)) &= F_{\lambda}'^{N-k}((HF_{\alpha}'^{N-k}(y))_{\alpha \in I_*}) \\ &= HF_{\lambda}'^{N-k}(y) \\ &= Ext(F_{\lambda}'^{N-k}(y)). \end{aligned}$$

Thus Emb and Ext are $m\Theta$. $Ext(Emb(x, s)) = s$, $\forall (x, s) \in F$.

Remark 5.1. If $s \in \mathbb{K}_{p\mathbb{Z}}^N \backslash \mathbb{K}_p^N$, then $s = (F_\alpha'^N(s))_{\alpha \in I_*}$. So we observe that when hiding s in $x \in \mathbb{K}_{p\mathbb{Z}}^N \backslash \mathbb{K}_p^N$, this becomes to hide $card(I_*)$ classical messages in x. Indeed, for every $\alpha \in I_*$, we hide $F_\alpha^{N-k}(s)$ in $F_\alpha'^N(x)$, i.e., in other word we hide for every $\alpha \in I_*$, $F_\alpha^{N-k}(s)$ in x. According to what proceeds, we can hide classical messages in a cover $m\Theta$ object ($m\Theta$ codeword).

6. Conclusion

In the present work, we have been brougth from the $m\Theta$ algebraic structures to define $m\Theta$ steganographic protocols with some examples. We have also observe that one can hide classical messages in a cover $m\Theta$ objet ($m\Theta$ codeword).

References

[1] C. Munuera, Steganography and error-correcting codes, Signal Processing 87(6) (2007), 1528-1533.

DOI: https://doi.org/10.1016/j.sigpro.2006.12.008

[2] F. Ayissi Eteme, Logique et Algebre de Structures Mathematique Modales, Chrysipiennnes Edition Herman, Paris, 2009.

[3] F. Ayissi Eteme and J. A. Tsimi, A modal Θ-valent approach of the notion of code, Journal of Discrete Mathematical Science and Cryptography, 14(5) (2001), 445-473.

DOI: https://doi.org/10.1080/09720529.2011.10698348

[4] F. Ayissi Eteme and J. A. Tsimi, A $m\Theta$ approach of the Algebriac theory of linear codes, Journal of Discrete Mathematial Sciences and Cryptography 14(6) (2011), 559-581.

DOI: https://doi.org/10.1080/09720529.2011.10698356

[5] Fidèle Ayissi Eteme and J. A. Tsimi, $m\Theta$ cyclic codes on a $m\Theta$ field, International Journal of Mathematics, Game Theory, and Algebra 25(3) (2016), 313-344.

[6] F. A. Eteme, Chrysippian $m\Theta$ Valent Introducing Pure and Applied Mathematics, LAP Lambert Academic Pubblishing (2015), Deutschland, Germany.

[7] J. A. Tsimi, A. Kemadjou Kecthandjeu and L. Um, On a class of modal Θ-valent convolutional codes, Journal of Information and Optimization Sciences 42(5) (2021), 995-1026.

DOI: https://doi.org/10.1080/02522667.2020.1835036

[8] J. A. Tsimi, A. Kemadjou Ketchandjeu and L. Um, A $m\Theta$ analysis and a decoding α-viterbi algorithm of the $m\Theta$ convoulutional codes on $(\mathbb{F}_{2\mathbb{Z}}, F_\alpha)$, Journal of Information and Optimization Sciences 42(8) (2021), 1815-1840.

DOI: https://doi.org/10.1080/02522667.2021.1961976

[9] J. A. Tsimi and G. C. Pemha Binyam, On the generalized modal Θ-valent Reed-Muller codes, Journal of Information and Optimization Sciences 42(8) (2021), 1885-1906.

DOI: https://doi.org/10.1080/02522667.2021.1961977

[10] J. A. Tsimi and R. C. Youdom, The modal Θ-valent extensions of BCH codes, Journal of Information and Optimization Sciences, 42(8) (2021), 1723-1764.

DOI: https://doi.org/10.1080/02522667.2021.1914364

[11] J. A. Tsimi, R. C. Youdom and B. Boakye, Modal Θ-valent linear codes with complementary modal Θ-valent duals, Journal of Information and Optimization Sciences 42(5) (2021), 1027-1063.

DOI: https://doi.org/10.1080/02522667.2020.1843272

[12] M'hammed Boulagouaz and Mohamed Bouye, Correspondence between steganographic protocols and error correcting codes, Journal of Algebra Combinatorics Discrete Structures and Applications 4(2) (2017), 197-206.

DOI: https://doi.org/10.13069/jacodesmath.284966

[13] Khosravi Sara, Abbasi Dezfoli Mashallah and Yektaie Mohammad Hossein, A new steganography method based on HIOP (Higher Intensity of Pixel) algorithm and Strassen's matrix multiplication, Journal of Global Research in Computer Science 2(1) (2011), 6-12.

[14] S. Katzenbeisser and F. A. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.

[15] G. J. Simmons, The prisoners' problem and the subliminal channel, in Proc. Advances in Cryptology (CRYPTO '83), pp. 51-67. Berglund, J. F. and K.H. Hofmann, 1967. Compact semitopological semigroups and weakly almost periodic functions, Lecture Notes in Mathematics, No. 42, Springer-Verlag, Berlin-New York.

[16] Christian Cachin, Digital Steganography, Encyclopedia of Cryptography and Security, 2005.

DOI: https://doi.org/10.1007/0-387-23483-7_115

■