Noname manuscript No.
(will be inserted by the editor)

Secret Sharing Schemes Based on Resilient Boolean Maps

Juan Carlos Ku-Cauich · Guillermo Morales-Luna

Received: date / Accepted: date

Abstract We introduce a linear code based on resilient maps on vector spaces over finite fields, we give a basis of this code and upper and lower bounds for its minimal distance. Then the use of the introduced code for building vector space secret sharing schemes is explained and an estimation of the robustness of the schemes against cheaters is provided.

Keywords Secret sharing schemes · Cheater detection · Resilient maps · Vector linear codes

Mathematics Subject Classification (2000) 94A62 · 51E22 · 06E30

1 Introduction

Secret sharing schemes (SSS) were proposed in 1979, independently by Shamir [20] and Blakley [3]. Several variants appeared later, e.g. in [14] it was discussed the relation between SSS and Reed-Solomon codes and in [7, 10, 18, 16] error correcting codes built within finite fields were constructed. Through the Massey's SSS [13], a general relation between linear codes and SSS is obtained. However, within this approach characterising or predetermining the access structure may not be an easy task. The most common approach is to calculate the minimal words at the dual code. In [1] a sufficient condition, based on the ratio of the maximal and minimal weights in codewords, is provided in order to have that all non-null codewords be minimal and in [10] the corresponding access structure is determined.

J. C. Ku-Cauich
Computer Science, CINVESTAV-IPN, Mexico City, Mexico
Tel.: +52-555-7473759
Fax: +52-555-7473758
E-mail: jckc35@hotmail.com

G. Morales-Luna
Computer Science, CINVESTAV-IPN, Mexico City, Mexico

In a SSS some participants may cheat their shares in order to gain some illicit benefit. We use vector space secret sharing schemes (VSSSS) [4], and the modifications in [17], to diminish the risk of cheaters. VSSSS has been used in several constructions, e.g. in [8], high information rate ramp schemes are built whose secrets are vector of field elements, producing non-perfect SSS. Cheater detection has been analysed in the context of threshold SSS in [15, 21].

We propose a SSS in the current paper fitting the first non-threshold scheme in [17] having an information rate of 2^{-1}, which is almost optimal and is asymptotically optimal (see Proposition 3 in [17]). The cheating probability is at most q^{-1}, where q is the order of the finite field. Thereafter we generalise this contruction in order to have a k-dimensional VSSSS, with information rate 2^{-1} and cheating probability q^{-r}, where r is the dimension of the vector space of secrets, namely, the probability of uniform random selection in the space of secrets. This VSSSS is perfect in the sense introduced in [17].

On the other hand, resilient maps were introduced in [9] and in [2] they reappeared in the context of key distribution protocols for quantum cryptography. Among several application in Cryptography [5, 24], resilient maps have been used for random number generation for stream ciphering [19] as well as for authentication schemes [12].

In the current paper a linear code is introduced whose dual code allows the construction of a SSS with a well characterised access structure. Using resilient maps over finite fields and the trace map we build a code whose non-zero words are all minimal, the minimal distance of its dual is greater or equal than 2 hence the access structure of the corresponding Massey SSS can be determined [7] and it is a perfect and ideal scheme [17].

In Section 2 we present our modification of the non-threshold VSSSS. In Section 3 we introduce the linear code based on resilient maps and we prove that all its non-zero codewords are minimal in the sense of [7]. Besides, this code is such that for any coordinate there is a codeword with a non-zero value at that entry, and its dual code has also this property. This property is useful in the context of Massey's secret sharing schemes, because using this code there is a guarantee that no participant would receive a zero sharing when a secret is splitted. Finally at Section 3.2 we discuss the generalised VSSSS using the linear code built in Section 3.

2 Secret sharing

In this section we introduce a *secret sharing scheme* (SSS) from a general linear code, satisfying *ad-hoc* conditions. Later, we will restrict the construction using the code defined by the equation (17). We begin by recalling the SSS due to Massey.

2.1 Massey's SSS

This construction can be found in [7,13]. As usual, let us assume that 0 denotes a dealer and the set of integers $\{1,\ldots,n-1\}$ is naming $n-1$ participants. Let D be an $[n,k,d]_q$-linear code over the field $\mathbb{F}_q$, with generator matrix

$$G = [g_0\ g_1\ \cdots\ g_{n-1}] = \begin{bmatrix} h_0^T \\ \vdots \\ h_{k-1}^T \end{bmatrix} \in \mathbb{F}_q^{k\times n},$$

where all g_j are non-zero vectors in $\mathbb{F}_q^k$ and all h_i are non-zero vectors in $\mathbb{F}_q^n$ (here we are assuming that all vectors are indeed column vectors).

The field $\mathbb{F}_q$ is the set of secrets. Given a secret $s \in \mathbb{F}_q$, the dealer selects randomly a vector $u \in \mathbb{F}_q^k$ such that

$$s = u \cdot g_0 = u^T g_0 \tag{1}$$

and calculates

$$\forall j = 1,\ldots,n-1: \quad v_j = u^T g_j. \tag{2}$$

For each $j = 1,\ldots,n-1$, the dealer gives the j-th value $v_j \in \mathbb{F}_q$ to the j-th participant as the j-th share.

For any subset $J \subseteq \{1,\ldots,n-1\}$ of cardinality $m = |J| \le n-1$, $J = \{j_1,\ldots,j_m\}$, let

$$G_J = [g_{j_1} \quad \cdots \quad g_{j_m}] \in \mathbb{F}_q^{k\times m}$$

be the matrix whose columns are the columns of the generator matrix G numbered by J, and $v_J = [v_j]_{j\in J}$. Clearly, $v_J^T = u^T G_J$.

For the set J, the recovering procedure of the secret should be the following:

1. Express g_0 as a linear combination of $(g_j)_{j\in J}$, say $g_0 = \sum_{j\in J} c_j g_j$;
2. in case of success, recover the secret as $s = \sum_{j\in J} c_j v_j$.

We recall that a set of participants $J \subset \{1,\ldots,n-1\}$ is an *access set* if, by joining all their shares, the participants in J can recover the secret, and an access set J is *minimal* if no proper subset of J is an access set.

The following three results are common knowledge on Massey's SSS:

Proposition 1 *$J \subset \{1,\ldots,n-1\}$ is an access set on Massey's SSS if and only if the first column in the generator matrix is in the linear space spanned by the columns indexed by J, in symbols, $g_0 \in \mathcal{L}\left((g_j)_{j\in J}\right)$.*

Proposition 2 ([7,13]) *A non-empty set $J \subset \{1,\ldots,n-1\}$ of cardinality $m \le n-1$ is an access set in the Massey's SSS if and only if there is a codeword $d = (d_j)_{j=0}^{n-1}$ in the dual code $D^\perp$ such that*

$$[d_0 = 1]\ \&\ [\forall j \notin \{0\}\cup J:\ d_j = 0]\ \&\ [\exists j \in J:\ d_j \neq 0]\,. \tag{3}$$

Definition 1 For any $x \in \mathbb{F}_q^n$, let $\mathrm{Spt}(x) = \{i |\ x_i \neq 0\}$. A vector $x \in \mathbb{F}_q^n$ *covers* another vector $y \in \mathbb{F}_q^n$ if $\mathrm{Spt}(y) \subseteq \mathrm{Spt}(x)$. The vector $x \in \mathbb{F}_q^n$ is *minimal* if it covers just its non-zero multiples.

Corollary 1 *Let $E = \{(e_j)_{j=0}^{n-1} \in D^\perp |\ e_0 = 1\}$ be the collection of codewords in the dual code whose first entry is 1. In the SSS based on the linear code D, there is a one-to-one and onto correspondence between the collection of minimal access sets and the collection of minimal words in E.*

Remark 1 Let $J \subset \{1, \ldots, n-1\}$ be an access set of participants. Given a secret $s \in \mathbb{F}_q$ and a vector $u \in \mathbb{F}_q^k$ chosen by the dealer in order to satisfy (1), let $[v_j]_{j=1}^{n-1}$ be the shares calculated according to (2). Then, from Proposition 1, $s = \sum_{j \in J} c_j v_j$.

Remark 2 For any minimal access set $J \subset \{1, \ldots, n-1\}$, the above remark obviously holds as well, and condition (3) holds in a stronger form:

$$[d_0 = 1] \ \&\ [\forall j \notin \{0\} \cup J :\ d_j = 0] \ \&\ [\forall j \in J :\ d_j \neq 0] .$$

Now we recall the following result concerning secret sharing schemes over the dual code and their minimal access sets:

Theorem 1 ([7,23]) *Let D be an $[n,k,d]_q$-linear code over $\mathbb{F}_q$, with generator matrix $G = [g_0\ g_1\ \cdots\ g_{n-1}] \in \mathbb{F}_q^{k \times n}$. If any non-zero word at D is minimal, then on the Massey's SSS based on $D^\perp$ we have:*

1. *There are q^{k-1} minimal access sets.*
2. *If the minimal distance $d^\perp$ of the code $D^\perp$ is 2 then for any j, $1 \leq j \leq n-1$:*
   - *If g_j is a multiple of g_0, then the j-th participant is in every minimal access set.*
   - *If g_j is not a multiple of g_0, then the j-th participant is in exactly $(q-1)q^{k-2}$ minimal access sets.*
3. *If $d^\perp \geq 3$ and $1 \leq m \leq \min\{k-1, d^\perp - 2\}$, then any m-set of participants is included in $(q-1)^m q^{k-(m+1)}$ minimal access sets.*

We may point here another relevant property of codes in secret sharing schemes. If D is an $[n,k,d]_q$-linear code over the field $\mathbb{F}_q$ we will say that D *has a zero constant coordinate* if for some index $i \in \{0, \ldots, n-1\}$ and any codeword $\pi \in D$ we have $\pi_i = 0$, where π_i is the i-th coordinate of π.

If D has a zero constant coordinate, then the generator matrix G of that code would have a zero column, thus his partcipation does not contribute to the secret recovering process and it will be publicly known.

On the other side, if the dual code $D^\perp$ has a zero constant coordinate, then the share corresponding to that participant in the Massey's SSS will be always zero and it will be publicly known as well.

2.2 Massey's SSS with vector secrets

An immediate extension of Massey's SSS consists of vector secrets.

Let D be an $[n,k,d]_q$-linear code over $\mathbb{F}_q$ with generator matrix

$$G = [g_0 \;\; g_1 \;\; \cdots \;\; g_{n-1}] \in \mathbb{F}_q^{k\times n}.$$

The set of $n-1$ participants is identified with the set of indexes $\{1,\ldots,n-1\}$ and the dealer with the index 0.

Observe that for any non-zero vector $g \in \mathbb{F}_q^k$, the map $\mathbb{F}_q^k \to \mathbb{F}_q$, $u \mapsto u\cdot g$, is a balanced function. Thus, the following implication holds:

$$\forall g \in \mathbb{F}_q^k : \;\; \left[\left|\{u \in \mathbb{F}_q^k |\; u\cdot g = 0\}\right| > q^{k-1} \implies g = 0\right]. \tag{4}$$

Let $r \in \mathbb{Z}^+$be an arbitrary positive integer. The r-dimensional vector space $\mathbb{F}_q^r$ is taken as the set of secrets. Given a secret $s \in \mathbb{F}_q^r$, the dealer chooses randomly vectors $u_0,\ldots,u_{r-1} \in \mathbb{F}_q^k$ such that

$$\forall \rho = 0,\ldots,r-1 : \quad s_\rho = u_\rho^T g_0 \in \mathbb{F}_q, \tag{5}$$

and calculates the vectors

$$\forall j = 1,\ldots,n-1 : \quad v_j = \left[u_\rho^T g_j\right]_{\rho=0}^{r-1} \in \mathbb{F}_q^r. \tag{6}$$

The dealer gives the vector v_j as the corresponding share to the j-th participant.

The analogous to the Proposition 2 holds almost verbatim:

Proposition 3 *A non-empty set $J \subset \{1,\ldots,n-1\}$ of cardinality $m \le n-1$ is an access set in the Massey's SSS with vector secrets if and only if there is a codeword $d = (d_j)_{j=0}^{n-1}$ in the dual code $D^\perp$ such that*

$$[d_0 = 1] \;\&\; [\forall j \notin \{0\}\cup J : \; d_j = 0] \;\&\; [\exists j \in J : \; d_j \neq 0]. \tag{7}$$

Proof First let us recall that for any $g \in \mathbb{F}_q^k - \{0\}$, the map $\mathbb{F}_q^k \to \mathbb{F}_q$, $u \mapsto u^T g$, is balanced. Due to implication (4), for any index subset $J \subset \{1,\ldots,n-1\}$ and any coefficients $c_j \in \mathbb{F}_q$, $j \in J$, the following two conditions are equivalent:

$$\text{(I)} \;\; g_0 - \sum_{j\in J} c_j g_j = 0 \tag{8}$$

$$\text{(II)} \;\; \exists u_0,\ldots,u_{r-1} \in \mathbb{F}_q^k \; \forall \rho = 0,\ldots,r-1 : \quad u_\rho^T \left(g_0 - \sum_{j\in J} c_j g_j\right) = 0$$

Then, the proof of the current theorem is similar to the proof of Proposition 2.

Proposition 3 characterises the access structure for vector secrets in the same way as Proposition 2 for scalar secrets.

Corollary 1 also holds within this context. Besides, similar to Remark 1:

Remark 3 Let $J \subset \{1,\ldots,n-1\}$ be an access set of participants. Given a secret $s \in \mathbb{F}_q^r$ and vectors $u_0,\ldots,u_{r-1} \in \mathbb{F}_q^k$ chosen by the dealer in order to satisfy (5), let $[v_j]_{j=1}^{n-1}$ be the shares calculated according to (6). Then, eq. (8) entails $s = \sum_{j\in J} c_j v_j$, and this representation of the secret, as a linear combination of the shares $(v_j)_{j\in J}$, is unique.

Clearly, by identifying an alphabet of q symbols with $\mathbb{F}_q$, then the vector space $\mathbb{F}_q^r$ is identified with the set of words with length r over that alphabet.

2.3 Massey's SSS variations as vector space SSS's

In this section we will discuss the robustness of the introduced Massey's SSS variations against cheating. Let us firstly recall basic notions.

Massey's SSS with vector secrets is an ideal SSS [17], namely its information rate equals 1, i.e. the length in bits of a secret equals the maximum length of the distributed shares.

Besides, it is perfect because a set of participants may recover any secret if and only if there is a word in the dual code satisfying (7) but, due to Proposition 3, it means that the set is indeed an access set. Thus, no non-access set may recover any secret.

We recall the notion of *vector space SSS* (VSSSS) [17]. Let us identify a set of n *participants* with the set of indexes $\{0,1,\ldots,n-1\}$, being 0 the index of the *dealer*. For a vector space V over a field K let us assume a set $(g_j)_{j=0}^{n-1}$ of vectors in V. An access structure $\Gamma \subset \mathcal{P}(\{1,\ldots,n-1\})$ is a *vector space access structure* if:

$$\forall J \subset \{1,\ldots,n-1\}: \ \left[J \in \Gamma \iff g_0 \in \mathcal{L}\left((g_j)_{j\in J}\right)\right]$$

($\mathcal{L}(U)$ denotes the K-linear span of a set $U \subset V$). Within such a structure, Massey's SSS can be implemented. For any secret $s \in K$ the dealer selects a vector $u \in K$ satisfying (1) and builds the shares according to (2).

In the remaining of this section we will assume that the characteristic of the field K is a prime greater than 2.

Let $J \in \Gamma$ be an access set and let $I \subset J$ be a proper non-empty set consisting of *cheaters*. The participants in I *succeed in deceiving* the participants in $J - I$ if, during a secret recovering process, each participant $i \in I$ provides a fake share v_i' (instead of his correct share v_i), each participant $i \in J - I$ provides his correct share v_i, the recovery process produces a secret s' and $s' \neq s$, where s is the resulting secret if all participants in J would provide their correct shares. There may be two kind of cheaters: Either the cheaters know somehow in advance the correct secret s and make believe the other participants that it is s', or the cheaters do not know in advance s but they are able to recover s from s' (and their own correct shares). We will assume the second type of cheaters.

2.3.1 Robustness against cheaters in VSSSS with scalar secrets

In a VSSSS with scalar secrets, as in Section 2.1, let $J \subset \{1, \ldots, n-1\}$ be an access set.

Suppose first that there is just one cheater $i \in J$ in a minimal access set J. The cheater i may deceive other participants in $J_i = J - \{i\}$: When trying to recover a secret $s \in K$ each participant $j \in J_i = J - \{i\}$ provides his share v_j while i provides $v_i' = v_i + \varepsilon$. Then the recovering process gives

$$s' = \sum_{j \in J_i} c_j v_j + c_i v_i' = s + c_i \varepsilon.$$

The cheater recovers the secret as $s = s' - c_i\varepsilon$, while the others get the erroneous secret $s' = s + c_i\varepsilon$.

Now, suppose again that $J \in \Gamma$ is minimal and the set of cheaters is $I = J - \{m\}$, where $m \in J$. The participants at I would provide modified shares, say v_i', instead of the correct shares v_i, with $i \in I$. The probability to cheat m is

$$a_m(v', v) = \Pr\left(m \text{ is cheated by } v' \,|\, I\text{-shares are } v\right).$$

The cheating success probability is

$$A_m(v) = \max_{v'} a_m(v', v).$$

A VSSSS is (Γ, ε)-*robust* if, under the assumption that the participants at I do not know the secret, $A_m(v) \leq \varepsilon$.

A modified SSS with the aim to avoid cheaters is proposed in [17].

Suppose that the dealer and an auxiliary *combiner* (or *black-box*) are honest. For any secret $s \in \mathbb{F}_q$ the dealer selects two vectors $u_1, u_2 \in \mathbb{F}_q^k$ such that $s = u_1^T g_0$ and $s^2 = u_2^T g_0$, calculates $(v_{j1}, v_{j2}) = (u_1^T g_j, u_2^T g_j) \in \mathbb{F}_q^2$ and deals the shares (v_{j1}, v_{j2}). In the recovering process, for any access set J, the combiner receives the shares $\{(v_{j1}, v_{j2})\}_{j \in J}$ and calculates $t_1 = \sum_{j \in J} c_j v_{j1}$ and $t_2 = \sum_{j \in J} c_j v_{j2}$. If $t_1^2 = t_2$ then the combiner reveals t_1 as the secret, otherwise, the combiner warns the existence of a cheater among the participants in J.

It is proved [17] that the modified SSS has information rate $\frac{1}{2}$ and that it is (Γ, q^{-1})-robust.

Namely, let $J \subset \{1, \ldots, n-1\}$ be a minimal access set and let $I \subset J$ be a proper non-empty set of supposed cheaters. The participants in I collude in order to cheat the participants in $J - I$. Let

$$a_{IJ}(v', v) = \Pr\left((J-I)\text{-participants are cheated by } v' \,|\, I\text{-shares are } v\right)$$

and

$$A_{IJ}(v) = \max_{v'} a_{IJ}(v', v).$$

Suppose that in the modified SSS, $\forall j \in I$, $(v'_{j1}, v'_{j2}) = (v_{j1}, v_{j2}) + (\varepsilon_{j1}, \varepsilon_{j2})$. Their cheating attempt will be successful if $(t'_1)^2 = t'_2$, where

$$t'_1 = \sum_{j\in J} c_j v_{j1} + \sum_{j\in J-I} c_j v_{j1}\varepsilon_{j1} = s_1 + \varepsilon_1,$$
$$t'_2 = \sum_{j\in J} c_j v_{j2} + \sum_{j\in J-I} c_j v_{j2}\varepsilon_{j2} = s_2 + \varepsilon_2.$$

Thus, cheating success occurs if

$$2s_1\varepsilon_1 + \varepsilon_1^2 = \varepsilon_2. \tag{9}$$

There are exactly q pairs $(\varepsilon_1, \varepsilon_2) \in \mathbb{F}_q^2$ satisfying (9). Thus, $A_{IJ}(v) \leq q^{-1}$.

2.3.2 Robustness against cheaters in VSSSS with vector secrets

Consider the setting in Section 2.2 with vector secrets.

Let D be an $[n, k, d]_q$-linear code over $\mathbb{F}_q$, with q a power of a prime greater than 2, with generator matrix $G = [g_0 \;\; g_1 \;\; \cdots \;\; g_{n-1}] \in \mathbb{F}_q^{k\times n}$.

The vector space $\mathbb{F}_q^r$ is the set of both secrets and shares.

Then the above construction provides a VSSSS whose information rate is also $\frac{1}{2}$ but it is (Γ, q^{-r})-robust.

Let us check this last assertion.

Given a secret $s \in \mathbb{F}_q^r$, the dealer finds r vector pairs

$$(u_{01}, u_{02}), \ldots, (u_{r-1,1}, u_{r-1,2}) \in \mathbb{F}_q^k \times \mathbb{F}_q^k$$

such that

$$\forall \rho = 0, \ldots, r-1: \quad s_\rho = u_{\rho,1}^T g_0 \;\; \& \;\; s_\rho^2 = u_{\rho,2}^T g_0$$

and calculates the vectors

$$\forall j = 1, \ldots, n-1: \quad v_{j1} = \left[u_{\rho,1}^T g_j\right]_{\rho=0}^{r-1}, v_{j2} = \left[u_{\rho,2}^T g_j\right]_{\rho=0}^{r-1} \in \mathbb{F}_q^r.$$

The dealer gives the vector pair (v_{j1}, v_{j2}) as the corresponding share to the j-th participant.

For a minimal access set $J \subset \{1, \ldots, n-1\}$, a proper non-empty set of supposed cheaters $I \subset J$ is in collusion to cheat the participants in $J - I$. They alter their shares as $(v'_{\rho 1}, v'_{\rho 2}) = (v_{\rho 1}, v_{\rho 2}) + (\varepsilon_{\rho 1}, \varepsilon_{\rho 2})$. The cheating success condition is similar to (9):

$$\forall \rho = 0, \ldots, r-1: \quad 2s_1\varepsilon_{\rho 1} + \varepsilon_{\rho 1}^2 = \varepsilon_{\rho 2}.$$

Then, the cheating success probability satisfies $A_{IJ}(v) \leq q^{-r}$.

3 A linear code based on resilient maps

3.1 Construction of the linear code

For any $n \in \mathbb{Z}^+$, let $\mathbb{F}_2^n$ be the n-dimensional vector space over the prime field $\mathbb{F}_2$ of characteristic 2.

Let $n, m \in \mathbb{Z}^+$ be such that $1 \leq m \leq n$. For any index t-subset $J \subset \{0, \ldots, n-1\}$, say $J = \{j_0, \ldots, j_{t-1}\}$, and any $a = (a_0, \ldots, a_{t-1}) \in \mathbb{F}_2^t$, the *affine J-variety determined by a* is

$$V_{J,a,n} = \{x \in \mathbb{F}_2^n |\ \forall k \in \{0, \ldots, t-1\} :\ x_{j_k} = a_k\}.$$

A map $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is *J-resilient* if $\forall a = (a_0, \ldots, a_{t-1}) \in \mathbb{F}_2^t$, the map $f|_{V_{J,a,n}}$ is balanced, namely, $\forall y \in \mathbb{F}_2^m$, $\left|V_{J,a,n} \cap f^{-1}(y)\right| = 2^{n-t-m}$.

A map $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is *t-resilient* if it is J-resilient for any set J such that $|J| = t$.

Let q be a power of a prime number $p \geq 2$ and $m, n \in \mathbb{Z}^+$. The above characterisation of resilient maps, assumed as definition, is suitable to be stated on maps $\mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}$ defined on vector spaces over finite fields [6].

As a sort of example, let $s = m \log_p(q)$ and

$$\phi : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}^n \quad , \quad \left(\sum_{i=0}^{s-1} a_{i0} p^i, \ldots, \sum_{i=0}^{s-1} a_{i,n-1} p^i\right) \mapsto (a_{00}, \ldots, a_{0,n-1}) \tag{10}$$

Let $g : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}$ be an arbitrary map. Then the map

$$f : \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m} \quad , \quad (x, y) \mapsto f(x, y) = x \cdot \phi(y) + g(y),$$

where "$\cdot$" is the inner product, is t-resilient, with $t = n - 1$. □

As usual, $T_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ denotes the trace map $z \mapsto \sum_{j=0}^{m-1} z^{q^j}$. Then,

- for each non-zero scalar $a \in \mathbb{F}_{q^m} - \{0\}$, the map $\mathbb{F}_{q^m} \to \mathbb{F}_q$, $z \mapsto T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(az)$, is balanced, and
- for each non-zero vector $b \in \mathbb{F}_{q^m}^n - \{0\}$, the map $\mathbb{F}_{q^m}^n \to \mathbb{F}_q$ defined over the vector space $\mathbb{F}_{q^m}^n$, $x \mapsto T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(b \cdot x)$, is balanced as well.

Let $f : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}$ be a t-resilient map with $t < n$. Then, for any non-zero scalar $a \in \mathbb{F}_{q^m} - \{0\}$, the map $x \mapsto a\, f(x)$ is t-resilient, hence balanced. Thus, the collection of points $x \in \mathbb{F}_{q^m}^n$ such that $f(x) \neq 0$, namely

$$N_f = f^{-1}(\mathbb{F}_{q^m} - \{0\}) \subset \mathbb{F}_{q^m}^n, \tag{11}$$

is such that $|N_f| = q^{m(n-1)}(q^m - 1)$. Let us fix an enumeration

$$\nu : \{0, \ldots, q^{m(n-1)}(q^m - 1) - 1\} \to N_f = \mathbb{F}_{q^m}^n - f^{-1}(0), \tag{12}$$

say $N_f = (\nu(\iota))_{\iota=0}^{q^{m(n-1)}(q^m-1)-1}$. Under these conditions, by Corollary 1 at [24], we may state a more general result than Corollary 2 at [24]:

Whenever $(a,b) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}^n - \{(0,0)\}$ *is such that* $w_H(b) \leq t$, *where* w_H *denotes the Hamming weight, the map*

$$\gamma_{abf} : \mathbb{F}_{q^m}^n \to \mathbb{F}_q \ , \ x \mapsto \gamma_{abf}(x) = T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a\, f(x) + b \cdot x), \tag{13}$$

is balanced.

On one side, fixed $(a,b) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}^n - \{(0,0)\}$, we have

$$N_f = \left(N_f \cap \gamma_{abf}^{-1}(0)\right) \cup \left(N_f \cap (\mathbb{F}_{q^m}^n - \gamma_{abf}^{-1}(0))\right),$$

then necessarily

$$\left|N_f \cap (\mathbb{F}_{q^m}^n - \gamma_{abf}^{-1}(0))\right| > 2. \tag{14}$$

On the other side, $\left[\gamma_{abf}(x) = 0 \ \Leftrightarrow \ a\, f(x) + b \cdot x \in \ker\left(T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\right)\right]$. Suppose that $x \in N_f$, i.e. $f(x) \neq 0$, then the map $a \mapsto a\, f(x)$ is a permutation within $\mathbb{F}_{q^m}$, hence necessarily there exists an element $a \in \mathbb{F}_{q^m} - \{0\}$ such that $a\, f(x) \notin \ker\left(T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\right)$. Thus

$$\forall x \in N_f \ \exists (a,b) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}^t - \{(0,0)\} : \ \gamma_{abf}(x) \neq 0. \tag{15}$$

Define

$$\mathbf{c}_{abf} = [\gamma_{abf}(x)]_{x \in N_f} \in \mathbb{F}_q^{q^{m(n-1)}(q^m-1)} \tag{16}$$

where each $\mathbf{c}_{abf}$ is regarded as a column vector, namely, as a matrix of order $(q^{m(n-1)}(q^m-1)) \times 1$. By identifying $\mathbb{F}_{q^m}^t$ with $\mathbb{F}_{q^m}^t \oplus \{0^{n-t}\} \subset \mathbb{F}_{q^m}^n$, we may define

$$\mathcal{C}_f = \{\mathbf{c}_{abf} |\ a \in \mathbb{F}_{q^m} \ \& \ b \in \mathbb{F}_{q^m}^t\}. \tag{17}$$

Proposition 4 *Let* $e_i = (\delta_{ij})_{j=0}^{n-1}$ *be the i-th vector in the canonical basis of* $\mathbb{F}_{q^m}^n$, *where* δ_{ij} *is the Kronecker delta, and* $\alpha \in \mathbb{F}_{q^m}$ *be a primitive element, i.e.* $\left(\alpha^k\right)_{k=0}^{m-1}$ *is a basis of* $\mathbb{F}_{q^m}$ *over* $\mathbb{F}_q$.

Let $D = \left\{\alpha^k \ e_i |\ 0 \leq i \leq t-1 \ , \ 0 \leq k \leq m-1\right\} \subset \mathbb{F}_{q^m}^n$. *Then*

$$\mathcal{D}_f = \left(\mathbf{c}_{\alpha^k 0 f}\right)_{k=0}^{m-1} \cup \left(\mathbf{c}_{0df}\right)_{d \in D}$$

is a basis of the linear code $\mathcal{C}_f$ *defined by (17).*

Proof Fix $a \in \mathbb{F}_{q^m}$ and a vector of the form $b = (b_0, \ldots, b_{t-1}, 0, \ldots, 0) \in \mathbb{F}_{q^m}^t \oplus \{0^{n-t}\}$. By writing, for each $i = 0, \ldots, t-1$, $b_i = \sum_{k=0}^{m-1} b_{ik}\alpha^k \in \mathbb{F}_{q^m}$, we have

$$b = \sum_{i=0}^{t-1} b_i e_i = \sum_{i=0}^{t-1}\sum_{k=0}^{m-1} b_{ik}\alpha^k e_i = \sum_{i=0}^{t-1}\sum_{k=0}^{m-1} b_{ik} d_{ik},$$

where $d_{ik} = \alpha^k \ e_i$, $k \in \{0, \ldots, m-1\}$.

We claim that the vector $\mathbf{c}_{abf}$ is a linear combination of the elements in $\mathcal{D}_f$.

For each $x \in \mathbb{F}_{q^m}^n$:

$$\begin{aligned}
\gamma_{abf}(x) &= T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a\, f(x) + b \cdot x) \\
&= T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(\left(\sum_{k=0}^{m-1} a_k \alpha^k\right) f(x) + \left(\sum_{i=0}^{t-1}\sum_{k=0}^{m-1} b_{ik} d_{ik}\right) \cdot x\right) \\
&= T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(\sum_{k=0}^{m-1} a_k \left(\alpha^k f(x)\right) + \sum_{i=0}^{t-1}\sum_{k=0}^{m-1} b_{ik} \left(d_{ik} \cdot x\right)\right) \\
&= \sum_{k=0}^{m-1} a_k T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(\alpha^k f(x)\right) + \sum_{i=0}^{t-1}\sum_{k=0}^{m-1} b_{ik} T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(d_{ik} \cdot x\right),
\end{aligned}$$

hence $\mathbf{c}_{abf} \in \mathcal{L}_{\mathbb{F}_p}(\mathcal{C}_f)$.

Now, let us check that $\mathcal{D}_f$ is linearly independent. Suppose that

$$\sum_{k=0}^{m-1} a_k T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(\alpha^k f(x)\right) + \sum_{i=0}^{t-1}\sum_{k=0}^{m-1} b_{ik} T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(d_{ik} \cdot x\right) = 0.$$

Thus, for $a = \sum_{k=0}^{m-1} a_k \alpha^k$ and $b = \sum_{i=0}^{t-1}\sum_{k=0}^{m-1} b_{ik} d_{ik}$ we have that for all $x \in \mathbb{F}_{q^m}^n$, $\gamma_{abf}(x) = 0$. Then, for these special a and b, γ_{abf} is not a balanced map. This entails $a = 0$ and $b = 0$ and all coefficients a_k and b_{ik} are zero. The proof of the proposition is thus complete.

Corollary 2 *The code $\mathcal{C}_f$ is a linear $[q^{m(n-1)}(q^m-1), (1+t)m]$-code.*

From the above discussion, the generator matrix for the code $\mathcal{C}_f$ is $G \in \mathbb{F}_q^{((1+t)m)\times\left(q^{m(n-1)}(q^m-1)\right)}$ whose transpose is

$$\begin{aligned}
G^T = \big[&\mathbf{c}_{10f}\ \mathbf{c}_{\alpha 0 f}\ \cdots\ \mathbf{c}_{\alpha^{m-1}0f} \| \\
&\mathbf{c}_{0d_{00}f}\ \cdots\ \mathbf{c}_{0d_{0,m-1}f}\ | \\
&\quad\vdots \\
&\mathbf{c}_{0d_{t-1,0}f}\ \cdots\ \mathbf{c}_{0d_{t-1,m-1}f}\big]^T \in \mathbb{F}_q^{\left(q^{m(n-1)}(q^m-1)\right)\times((1+t)m)}
\end{aligned} \tag{18}$$

where the column vectors $\mathbf{c}_{abf}$ are those defined at eq. (16) (as a matter of notation: the array at (18) should be read as a single row of length $(1+t)m$ in which each entry is a column vector of dimension $q^{m(n-1)}(q^m-1)$). Hence, the rows of the generator matrix are of the form $\mathbf{c}_{abf}^T$ for some $a \in \mathbb{F}_{q^m}$ and $b \in \mathbb{F}_{q^m}^n$.

Due to relations (13) and (16), $\mathcal{C}_f$ is certainly a $\mathbb{F}_q$-linear space, by (14) it has minimum weight greater than 2, and by (15), $\mathcal{C}_f$ has no zero constant coordinate.

Proposition 5 *No column of the generator matrix G is zero. (Or equivalently, no row of the matrix G^T, as displayed in (18), is zero.)*

In the sequel, we will enumerate the rows of G as follows:

For any $k \in \{0, \ldots, (1+t)m-1\}$ let $k_0 = k \bmod m$ and $k_1 = \frac{k-k_0}{m}$. Then $k = k_1 m + k_0$. Let

$$\mu(k) = \begin{cases} (\alpha^{k_0}, 0) & \text{if } k_1 = 0 \\ (0, d_{k_1-1,k_0}) = (0, \alpha^{k_0} e_{k_1-1}) & \text{if } k_1 > 0 \end{cases} \tag{19}$$

Then, according with (18), $G = \left[\mathbf{c}^T_{\mu(k)f}\right]_{k=0}^{(1+t)m-1}$.

Proposition 6 *The dual code $\mathcal{C}_f^\perp$ has minimum weight greater than 1, and besides, for each entry i there is a codeword $\pi \in \mathcal{C}_f^\perp$ such that $\pi(i) \neq 0$.*

Proof The first assertion follows from Proposition 5. For the second assertion, we observe:

$$\forall x \in \mathbb{F}_q^{q^{m(n-1)}(q^m-1)} : \quad \left[x \in \mathcal{C}_f^\perp \iff Gx = 0 \in \mathbb{F}_q^{(1+t)m}\right].$$

Let $H \in \mathbb{F}_q^{((1+t)m)\times\left(q^{m(n-1)}(q^m-1)\right)}$ be the row-equivalent row-reduced echelon matrix of G. The matrix H is obtained from G through row-elementary operations [11], hence it has the same rank as G, it spans as well the code $\mathcal{C}_f$, and being the rows of H codewords in $\mathcal{C}_f$ they have minimum weight greater than 2. The linear equations system $Hx = 0$ can be expressed as

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 0 = Hx = H_I x_I + H_J x_J = [H_I \;\; H_J] \begin{bmatrix} x_I \\ x_J \end{bmatrix}$$

where H_I is a non-singular matrix of order $(1+t)m \times (1+t)m$ consisting of $(1+t)m$ columns of H indexed by I and J is the complement set of I. Thus, $x_I = -H_I^{-1} H_J x_J$, namely, $(1+t)m$ "dependent" variables are put in terms of $q^{m(n-1)}(q^m-1) - (1+t)m$ "independent" variables. By assigning proper values to the independent variables the assertion at the proposition is obtained.

Proposition 7 *Let w_{min}, w_{max} be the minimum and maximum weights of $\mathcal{C}_f$. Then:*

$$\ell_f \leq w_{min} \leq w_{max} \leq u_f \tag{20}$$

where

$$\ell_f = q^{m(n-1)}\left(q^{m-1}(q-1)-1\right) + \begin{cases} 1 \text{ if } f(0) = 0 \\ 0 \text{ if } f(0) \neq 0 \end{cases} \qquad \text{and}$$

$$u_f = q^{mn-1}(q-1).$$

Proof We recall and point out the following remarks:

- The length of the linear code $\mathcal{C}_f$ is $q^{m(n-1)}(q^m-1)$.
- Since $f : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}$ is t-resilient, it is balanced, hence $\left|f^{-1}(0)\right| = q^{m(n-1)}$.

– For any $(a,b) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}^n - \{(0,0)\}$, the map

$$\gamma_{abf} : \mathbb{F}_{q^m}^n \to \mathbb{F}_q \ , \ \gamma_{abf} : x \mapsto T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a\, f(x) + b \cdot x)$$

is balanced, hence $\left|\gamma_{abf}^{-1}(0)\right| = q^{mn-1}$.

Besides, he following implication holds trivially: $[f(0) = 0 \ \Rightarrow \ \gamma_{abf}(0) = 0]$.

Let $\mathbf{c}_{abf} = [\gamma_{abf}(x)]_{x \in N_f}$ be an arbitrary word in the code $\mathcal{C}_f$, with $a \in \mathbb{F}_{q^m}$, $b \in \mathbb{F}_{q^m}^t$ and the set N_f defined in (11). We have $f^{-1}(0) = \mathbb{F}_{q^m}^n - N_f$. The vector space $\mathbb{F}_{q^m}^n$ can be partitioned by the following sets:

– $S_{00} = f^{-1}(0) \cap \gamma_{abf}^{-1}(0)$,
– $S_{01} = f^{-1}(0) \cap (\mathbb{F}_{q^m}^n - \gamma_{abf}^{-1}(0))$,
– $S_{10} = N_f \cap \gamma_{abf}^{-1}(0)$,
– $S_{11} = N_f \cap (\mathbb{F}_{q^m}^n - \gamma_{abf}^{-1}(0))$.

Thus, writing $s_{ij} = |S_{ij}|$, the following relations are immediate:

$$\begin{array}{ll} s_{00} + s_{01} = q^{m(n-1)} & s_{00} + s_{10} = q^{mn-1} \\ s_{10} + s_{11} = q^{m(n-1)}(q^m - 1) & s_{01} + s_{11} = q^{mn-1}(q-1) \end{array} \tag{21}$$

where $w(\mathbf{c}_{abf}) = s_{11}$ is the weight of the codeword $\mathbf{c}_{abf}$. From (21) we obtain,

$$s_{00} = w(\mathbf{c}_{abf}) - q^{m(n-1)} \left(q^{m-1}(q-1) - 1\right), \tag{22}$$
$$s_{01} = q^{mn-1}(q-1) - w(\mathbf{c}_{abf}), \tag{23}$$
$$s_{10} = q^{m(n-1)}(q^m - 1) - w(\mathbf{c}_{abf}).$$

Clearly $q^{m(n-1)}(q^m - 1) \geq q^{mn-1}(q-1)$, thus (22) and (23) establish lower and upper bounds for the weight of the codeword, just because s_{00}, s_{01} are non-negative integers.

On one extreme, for $w(\mathbf{c}_{abf}) = q^{m(n-1)} \left(q^{m-1}(q-1) - 1\right)$ we have

$$s_{00} = 0 \ \ , \ \ s_{01} = q^{m(n-1)} \ \ , \ \ s_{10} = q^{mn-1},$$

while on the other extreme, for $w(\mathbf{c}_{abf}) = q^{mn-1}(q-1)$,

$$s_{00} = q^{m(n-1)} \ \ , \ \ s_{01} = 0 \ \ , \ \ s_{10} = q^{m(n-1)}(q^{m-1} - 1).$$

If $f(0) = 0$ then $0 \in S_{00}$, hence $w(\mathbf{c}_{abf}) \geq q^{m(n-1)} \left(q^{m-1}(q-1) - 1\right) + 1$. The proposition's claim (20) follows.

Let us recall an important result:

Theorem 2 (Carlet *et al.* [7]) *Let $\mathcal{C}$ be a $[n,k]_q$-linear code and let w_{min}, w_{max} be its minimum and maximum weights. If*

$$\frac{w_{min}}{w_{max}} > \frac{q-1}{q} \tag{24}$$

then any non-zero codeword in $\mathcal{C}$ is minimal (in the sense of definition (1)).

Proposition 8 *Whenever $q \geq 2$, all non-zero codewords in the code $\mathcal{C}_f$ are minimal.*

Proof The polynomial $P_{mn}(X) = X^{mn-1} - X^{mn-2} - X^{mn-m} + 1$ is such that the following implication holds:

$$q \geq 2 \implies P_{mn}(q) > 0.$$

But the following relations are equivalent:

$$\begin{aligned} P_{mn}(q) > 0 &\iff \left(q - \frac{1}{q^{m(n-1)-1}}\right) < q^{m-1}(q-1) \\ &\iff \frac{1}{q-1}\left(q - \frac{1}{q^{m(n-1)-1}}\right) < q^{m-1} \\ &\iff \sum_{k=0}^{mn-m-1} \frac{1}{q^k} < q^{m-1}. \end{aligned} \tag{25}$$

Now, (20) and the relation (25) entail the relation (24). Hence, the result follows from Theorem 2.

3.2 Using the introduced code for VSSSS

Let q be the power of a prime number p, and $m, n \in \mathbb{Z}^+$. Let $f : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}$ be a resilient map as introduced in Section 3. Let $\mathcal{C}_f$ be the linear code defined at relation (17). $\mathcal{C}_f$ is a linear $[q^{m(n-1)}(q^m-1), (1+t)m]$-code, according to Proposition 4.

The general results quoted in Section 2.1 are applied directly to the linear code $\mathcal{C}_f$ defined in eq. (17). In particular from Theorem 1 and the comments thereafter, we have that for Massey's SSS over the dual code $\mathcal{C}_f^\perp$, the codewords in $\mathcal{C}_f$ are minimal.

According to Proposition 5, the introduced generator matrix G of $\mathcal{C}_f$ has no zero constant coordinate. Thus, all participants contribute effectively in the secret recovery processes. Since also the generator matrix of $\mathcal{C}_f^\perp$ has no zero constant coordinate then no participant will receive a zero share.

The construction given at Section 2.3.2, using the code $\mathcal{C}_f$ as the code D, gives a VSSSS that is (Γ, q^{-r})-robust, with $k = (1+t)m$ and involving up to $q^{m(n-1)}(q^m-1)$ participants, including the dealer.

Thus within this paper, we have introduced a VSSSS whose information rate is $\frac{1}{2}$ and it is (Γ, q^{-r})-robust; in the introduced VSSSS no null shares appear; when applied the shown construction to the linear code based on reslient maps of Section 3, then the VSSSS has parameters that can entirely be calculated, the cheating probabilities can be exponentially be decreased in terms of k, and finally, the VSSSS is an application of the balanced functions (13) obtained by resilient maps.

References

1. Ashikhmin, A.E., Barg, A., Cohen, G.D., i Rotger, L.H.: Variations on minimal codewords in linear codes. In: G.D. Cohen, M. Giusti, T. Mora (eds.) Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 11th International Symposium, AAECC-11, Paris, France, July 17-22, 1995, Proceedings, *Lecture Notes in Computer Science*, vol. 948, pp. 96–105. Springer (1995). DOI 10.1007/3-540-60114-7_7. URL http://dx.doi.org/10.1007/3-540-60114-7_7
2. Bennett, C.H., Brassard, G., Robert, J.M.: Privacy amplification by public discussion. SIAM Journal on Computing **17**(2), 210–229 (1988). DOI 10.1137/0217014. URL http://dx.doi.org/10.1137/0217014
3. Blakley, G.: Safeguarding cryptographic keys. In: Proceedings of the 1979 AFIPS National Computer Conference, pp. 313–317. AFIPS Press, Monval, NJ, USA (1979)
4. Brickell, E.F.: Some ideal secret sharing schemes. In: J.J. Quisquater, J. Vandewalle (eds.) EUROCRYPT, *Lecture Notes in Computer Science*, vol. 434, pp. 468–475. Springer (1989). URL http://dblp.uni-trier.de/db/conf/eurocrypt/eurocrypt89.html#Brickell89
5. Camion, P., Canteaut, A.: Construction of t-resilient functions over a finite alphabet. In: U.M. Maurer (ed.) EUROCRYPT, *Lecture Notes in Computer Science*, vol. 1070, pp. 283–293. Springer (1996)
6. Carlet, C.: More correlation-immune and resilient functions over galois fields and galois rings. In: W. Fumy (ed.) Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding, *Lecture Notes in Computer Science*, vol. 1233, pp. 422–433. Springer (1997). DOI 10.1007/3-540-69053-0_29. URL http://dx.doi.org/10.1007/3-540-69053-0_29
7. Carlet, C., Ding, C., Yuan, J.: Linear codes from perfect nonlinear mappings and their secret sharing schemes. IEEE Transactions on Information Theory **51**(6), 2089–2102 (2005)
8. Chen, H., Cramer, R., Goldwasser, S., de Haan, R., Vaikuntanathan, V.: Secure computation from random error correcting codes. In: M. Naor (ed.) Advances in Cryptology - EUROCRYPT 2007, 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, Spain, May 20-24, 2007, Proceedings, *Lecture Notes in Computer Science*, vol. 4515, pp. 291–310. Springer (2007). DOI 10.1007/978-3-540-72540-4_17. URL http://dx.doi.org/10.1007/978-3-540-72540-4_17
9. Chor, B., Goldreich, O., Hasted, J., Freidmann, J., Rudich, S., Smolensky, R.: The bit extraction problem or t-resilient functions. In: Foundations of Computer Science, 1985., 26th Annual Symposium on, pp. 396–407 (1985). DOI 10.1109/SFCS.1985.55
10. Ding, C., Yuan, J.: Covering and secret sharing with linear codes. In: C. Calude, M.J. Dinneen, V. Vajnovszki (eds.) Discrete Mathematics and Theoretical Computer Science, 4th International Conference, DMTCS 2003, Dijon, France, July 7-12, 2003. Proceedings, *Lecture Notes in Computer Science*, vol. 2731, pp. 11–25. Springer (2003). DOI 10.1007/3-540-45066-1_2. URL http://dx.doi.org/10.1007/3-540-45066-1_2
11. Hoffman, K., Kunze, R.: Linear Algebra 2Nd Ed. Prentice-Hall Of India Pvt. Limited (1971). URL https://books.google.com.mx/books?id=SeBIPgAACAAJ
12. Ku-Cauich, J.C., Morales-Luna, G.: Authentication codes based on resilient boolean maps. Designs, Codes and Cryptography pp. 1–15 (2015). DOI 10.1007/s10623-015-0121-3. URL http://dx.doi.org/10.1007/s10623-015-0121-3
13. Massey, J.: Minimal codewords and secret sharing. In: Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory, pp. 276–279 (1993)
14. McEliece, R.J., Sarwate, D.V.: On sharing secrets and reed-solomon codes. Commun. ACM **24**(9), 583–584 (1981). DOI 10.1145/358746.358762. URL http://doi.acm.org/10.1145/358746.358762
15. Obana, S., Tsuchida, K.: Cheating detectable secret sharing schemes supporting an arbitrary finite field. In: Yoshida and Mouri [22], pp. 88–97. DOI 10.1007/978-3-319-09843-2_7. URL http://dx.doi.org/10.1007/978-3-319-09843-2_7
16. Özadam, H., Özbudak, F., Saygi, Z.: Secret sharing schemes and linear codes. In: Proceedings of The International Conference on Information Security and Cryptology (ISCTURKEY 2007), pp. 101–106 (Ankara, 2007)

17. Padró, C., Sáez, G., Villar, J.: Detection of cheaters in vector space secret sharing schemes. Designs, Codes and Cryptography **16**(1), 75–85 (1999). DOI 10.1023/A:1008378426278
18. Pieprzyk, J., Zhang, X.: Ideal threshold schemes from MDS codes. In: P.J. Lee, C.H. Lim (eds.) Information Security and Cryptology - ICISC 2002, 5th International Conference Seoul, Korea, November 28-29, 2002, Revised Papers, *Lecture Notes in Computer Science*, vol. 2587, pp. 253–263. Springer (2002). DOI 10.1007/3-540-36552-4_18. URL http://dx.doi.org/10.1007/3-540-36552-4_18
19. Rueppel, R.A.: Analysis and Design of Stream Ciphers. Springer-Verlag New York, Inc., New York, NY, USA (1986)
20. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979). DOI 10.1145/359168.359176. URL http://doi.acm.org/10.1145/359168.359176
21. Xu, R., Morozov, K., Takagi, T.: Cheater identifiable secret sharing schemes via multi-receiver authentication. In: Yoshida and Mouri [22], pp. 72–87. DOI 10.1007/978-3-319-09843-2_6. URL http://dx.doi.org/10.1007/978-3-319-09843-2_6
22. Yoshida, M., Mouri, K. (eds.): Advances in Information and Computer Security - 9th International Workshop on Security, IWSEC 2014, Hirosaki, Japan, August 27-29, 2014. Proceedings, *Lecture Notes in Computer Science*, vol. 8639. Springer (2014). DOI 10.1007/978-3-319-09843-2. URL http://dx.doi.org/10.1007/978-3-319-09843-2
23. Yuan, J., Ding, C.: Secret sharing schemes from three classes of linear codes. IEEE Transactions on Information Theory **52**(1), 206–212 (2006). DOI 10.1109/TIT.2005.860412. URL http://dx.doi.org/10.1109/TIT.2005.860412
24. Zhang, X.M., Zheng, Y.: Cryptographically resilient functions. IEEE Transactions on Information Theory **43**(5), 1740–1747 (1997). URL http://dblp.uni-trier.de/db/journals/tit/tit43.html#ZhangZ97