A Linear Code and its Application into Secret Sharing

Juan Carlos Ku-Cauich[1] and Guillermo Morales-Luna[2⋆]

[1] Computer Science, CINVESTAV-IPN, Mexico City, Mexico, jckc35@hotmail.com
[2] Computer Science, CINVESTAV-IPN, Mexico City, Mexico,
gmorales@cs.cinvestav.mx

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 functions · vector linear codes

1 Introduction

Resilient maps were introduced in in the 90's [1, 4]. We build a linear code based on resilient maps, we produce a basis of the built code and we give lower and upper bounds for its minimal distance. A main feature of the linear code is that its non-zero words are minimal, hence it is suitable to be a platform to build vector space secret sharing schemes (VSSSS) [**?**]. In Section 2 we introduce the linear code based on resilient maps and we prove that all its non-zero codewords are minimal in the sense of [2].

In Section 3 we recall the constructions of Massey for secret sharing schemes (SSS) [2, 3] using an $[n, k]_q$-linear code and the characterisation of its access structure given in [2]. In this paper, an extension of Massey's method to vector secrets is introduced, the vector secrets have dimension $q^{k-1} + 1$, the Carlet *et al.* characterisation [2] is preserved and it is an ideal and perfect VSSSS [**?**]. For field characteristic greater than 2, in the produced VSSSS it may happen that several participants collude by modifying their shares in order to cheat other participants in the same access set. Within the scheme with scalar secrets, the cheating probability is at most q^{-1} and the information rate is 2^{-1}. By using vector secrets of dimension $q^{k-1} + 1$, the cheating probability is $q^{-(q^{k-1}+1)}$ and the information rate is also 2^{-1}.

Finally, we point out that the introduced code based on resilient maps can be used as platform to build robust VSSSS because all its non-zero codewords are minimal. Besides in the case of vector secrets, no vector share is zero, thus

⋆ Both authors acknowledge the support of Mexican Conacyt

all participants in a minimal access set are required to effectively participate in any process of recovering a secret and the cheating probability is even lowered.

2 A linear code based on resilient maps

Let q be a power of a prime number $p \geq 2$ and $m \in \mathbb{Z}^+$. Let $T_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ be the corresponding trace map. $\forall a \in \mathbb{F}_{q^m} - \{0\}$ the map $\mathbb{F}_{q^m} \to \mathbb{F}_q$, $x \mapsto T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(ax)$, is balanced.

For $n \in \mathbb{Z}^+$, let $\cdot : \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}$ be the inner product map. For each vector $b \in \mathbb{F}_{q^m}^n - \{0\}$, the map $\mathbb{F}_{q^m}^n \to \mathbb{F}_q$, $x \mapsto T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(b \cdot x)$, is balanced as well.

Let $f : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}$ be a map satisfying the following conditions:

- f is t-resilient, with $t \leq n$,
- the collection of points $x \in \mathbb{F}_{q^m}^n$ such that $f(x) \neq 0$, namely

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

  is such that $|N_f| = (q^m - 1)q^{m(n-1)}$, and
- $0 \notin N_f$, namely, $f(0) = 0$.

As a more general result than Corollary 2 at [4], we remark that whenever $(a, b) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}^n - \{(0, 0)\}$, the map

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

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

We identify $\mathbb{F}_{q^m}^t$ with the linear subspace $\mathbb{F}_{q^m}^t \oplus \{0^{n-t}\} \subset \mathbb{F}_{q^m}^n$, and we define

$$\mathcal{C}_f = \{\mathbf{c}_{abf} |\ a \in \mathbb{F}_{q^m} \ \& \ b \in \mathbb{F}_{q^m}^t\}. \tag{2}$$

$\mathcal{C}_f$ is a linear code of length $(q^m - 1)q^{m(n-1)}$.

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 $\alpha \in \mathbb{F}_{q^m}$ a primitive element. Then $\left(\alpha^k\right)_{k=0}^{m-1}$ forms a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Let $D = \left\{\alpha^k\ e_i |\ 0 \leq i \leq t-1\ ,\ 0 \leq k \leq m-1\right\} \subset \mathbb{F}_{q^m}^n$.

Proposition 1. *$\mathcal{D}_f = \left(\mathbf{c}_{\alpha^k 0 f}\right)_{k=0}^{m-1} \cup (\mathbf{c}_{0df})_{d \in D}$ is a basis of the linear code $\mathcal{C}_f$ defined by (2). Consequently, $\mathcal{C}_f$ is a linear $[(q^m - 1)q^{m(n-1)}, (1 + t)m]$-code.*

Proof. In a rather direct way, it can be seen that, for any element $a \in \mathbb{F}_{q^m}$ and any vector of the form $b = (b_0, \ldots, b_{t-1}, 0, \ldots, 0) \in \mathbb{F}_{q^m}^t \oplus \{0^{n-t}\})$, the vector $\mathbf{c}_{abf}$ is a linear combination of the elements in $\mathcal{D}_f$. Namely, since $b_i = \sum_{k=0}^{m-1} b_{ik}\alpha^k \in \mathbb{F}_{q^m}$ with $i = 0, \ldots, t-1$,

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

by writing $d_{ik} = \alpha^k\ e_i$. 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. □

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

$$\begin{aligned}
G^T = \big[&\mathbf{c}_{10f}\ \mathbf{c}_{\alpha 0 f}\ \cdots\ \mathbf{c}_{\alpha^{m-1}0f} \| \\
&\mathbf{c}_{0 d_{00} f}\ \cdots\ \mathbf{c}_{0 d_{0,m-1} f}\ | \\
&\quad\vdots \\
&\mathbf{c}_{0 d_{t-1,0} f}\ \cdots\ \mathbf{c}_{0 d_{t-1,m-1} f}\big]^T \in \mathbb{F}_p^{\left((q^m-1)q^{m(n-1)}\right)\times((1+t)m)}
\end{aligned} \tag{3}$$

(as a matter of notation: the above array should be read as a single row of length $(1+t)m$ in which each entry is a column vector of dimension $(q^m-1)q^{m(n-1)}$).

Proposition 2. *Let w_{min}, w_{max} be the minimum and maximum weights of $\mathcal{C}_f$. Then:*

$$\begin{aligned}
q^{m(n-1)}\left(q^{m-1}(q-1)-1\right)+1 &\le w_{min} \\
&\le w_{max} \\
&\le (q^m-1)q^{m(n-1)} - \left(q^{m-1}-1\right) q^{m(n-1)}.
\end{aligned} \tag{4}$$

Proof. We recall and point out the following remarks:

- The length of the linear code $\mathcal{C}_f$ is $(q^m-1)q^{m(n-1)}$.
- 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 $\left|\gamma_{abf}^{-1}(0)\right| = q^{mn-1}$.

Let $\mathbf{c}_{abf} = [\gamma_{abf}(x)]_{x \in N_f}$ be an arbitrary word in the code $\mathcal{C}_f$, with $a \in \mathbb{F}_{q^m}$ and $b \in \mathbb{F}_{q^m}^t$, the set N_f being defined as in (1). We claim:

$$|N_f| - \left(\left|\gamma_{abf}^{-1}(0)\right| - 1\right) \leq \left|N_f - \gamma_{abf}^{-1}(0)\right| \tag{5}$$

$$\leq |N_f| - \left(\left|\gamma_{abf}^{-1}(0)\right| - \left|f^{-1}(0)\right|\right) \tag{6}$$

On one side,

$$(N_f \cup \{0\}) \cap \gamma_{abf}^{-1}(0)^c = \left(N_f - \gamma_{abf}^{-1}(0)\right) \cup \left(\{0\} - \gamma_{abf}^{-1}(0)\right), \tag{7}$$

where $\gamma_{abf}^{-1}(0)^c = \mathbb{F}_{q^m}^n - \gamma_{abf}^{-1}(0)$.

If $0 \notin \gamma_{abf}^{-1}(0)$ then $\{0\} - \gamma_{abf}^{-1}(0) = \{0\}$, thus (7) entails (5).

If $0 \in \gamma_{abf}^{-1}(0)$ then $\{0\} - \gamma_{abf}^{-1}(0) = \emptyset$ but $N_f - \gamma_{abf}^{-1}(0) = N_f - (\gamma_{abf}^{-1}(0) - \{0\})$, (just because $0 \notin N_f$), thus also in this case (7) entails (5).

And on the other side,

$$\begin{aligned} \gamma_{abf}^{-1}(0)^c &= (N_f \cup f^{-1}(0)) \cap \gamma_{abf}^{-1}(0)^c \\ &= \left(N_f - \gamma_{abf}^{-1}(0)\right) \cup \left(f^{-1}(0) - \gamma_{abf}^{-1}(0)\right) \end{aligned} \tag{8}$$

The relation (8) entails as well (6).

Now, we observe that for any $a \in \mathbb{F}_{q^m}$ and $b \in \mathbb{F}_{q^m}^t$

$$q^{m(n-1)}\left(q^{m-1}(q-1)-1\right) + 1 \leq |N_f| - \left(\left|\gamma_{abf}^{-1}(0)\right| - 1\right) \qquad \text{and}$$

$$(q^m - 1)q^{m(n-1)} - \left(q^{m-1} - 1\right) q^{m(n-1)} \geq |N_f| - \left(\left|\gamma_{abf}^{-1}(0)\right| - \left|f^{-1}(0)\right|\right)$$

hence the proposition's claim (4) follows. □

Since the trace $T_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ is a balanced map, the following proposition results:

Proposition 3. *No column of the generator matrix G is zero. Or equivalently, no row of the matrix G^T, as displayed in (3), is zero.*

Proof. Assume that a row of G^T is zero. Without any loss of generality, assume that it is the first row, indexed by a vector $x_0 \in N_f$. Then

$$\forall k = 0, \ldots, m-1 : \ T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(\alpha^k\, f(x_0)\right) = 0,$$

thus

$$\forall (c_0, \ldots, c_{m-1}) \in \mathbb{F}_q^m : \; T_{\mathbb{F}_{q^m}/\mathbb{F}_q} \left(\sum_{k=0}^{m-1} c_k \, \alpha^k \, f(x_0) \right) = 0,$$

namely

$$\forall c \in \mathbb{F}_{q^m} : \; T_{\mathbb{F}_{q^m}/\mathbb{F}_q} (c \, f(x_0)) = 0,$$

which contradicts the balancedness of the trace map, since $f(x_0) \neq 0$. □

Remark 1. The dual code $\mathcal{C}_f^{\perp}$ has minimum weight greater than 1.

Let us recall an interesting definition and an important result:

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

Theorem 1 (Carlet *et al.* [2]). *Let $\mathcal{C}$ be a $[n,k]_q$-linear code and let w_{min}, w_{max} be its minimum and maximum weights. If*

$$\frac{w_{min}}{w_{max}} > \frac{q-1}{q} \tag{9}$$

then any non-zero codeword in $\mathcal{C}$ is minimal.

Proposition 4. *If*

$$\sum_{k=0}^{mn-m-1} \frac{1}{q^k} < q^{m-1} \tag{10}$$

then all non-zero codewords in the code $\mathcal{C}_f$ are minimal.

Proof. The bounds at (4) and the condition (10) entail the relation (9). Hence, the result follows from Theorem 1. □

3 Secret sharing

In this section we introduce a *secret sharing scheme* (SSS) using the code defined by the equation (2). We begin by recalling the SSS due to Massey.

3.1 Massey's SSS

This construction can be found in [2, 3]. As before, 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

$$s = u \cdot g_0 = u^T g_0 \tag{11}$$

and calculates

$$\forall j = 1, \ldots, n-1 : \quad v_j = u^T g_j. \tag{12}$$

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 $m = |J| \leq n-1$, $J = \{j_1, \ldots, j_m\}$, 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 G numbered by J, and $v_J = [v_j]_{j \in J}$. Clearly, $v_J^T = u^T G_J$.

Proposition 5. *The secret can be recovered by the participants at a subset $J \subset \{1, \ldots, n-1\}$ if and only if $g_0 \in \mathcal{L}\left((g_j)_{j \in J}\right)$.*

Proof. The recovering procedure is the following:

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

□

Within this context, the following holds:

Theorem 2 ([2, 3]). *A non-empty set $J \subset \{1, \ldots, n-1\}$ of cardinality $m \leq n-1$ 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*

$$[d_0 = 1] \ \& \ [\forall j \notin \{0\} \cup J : \ d_j = 0] \ \& \ [\exists j \in J : \ d_j \neq 0]. \tag{13}$$

Proof. The generator matrix G of D is a parity-check matrix of the dual code $D^\perp$. Let $d \in D^\perp \subset \mathbb{F}_q^n$ satisfying (13). Then $0 = Gd = g_0 + \sum_{j \in J} d_j g_j$, hence $g_0 \in \mathcal{L}\left((g_j)_{j \in J}\right)$. The result follows from Proposition 5. □

Corollary 1. *Let $E = \{(d_j)_{j=0}^{n-1} \in D^\perp | \ d_0 = 1\}$ 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.*

Proof. Let $J \subset \{1, \ldots, n-1\}$ be a minimal access set. Suppose $g_0 = \sum_{j \in J} c_j g_j$ and $s = \sum_{j \in J} c_j v_j$, with $c_j \in \mathbb{F}_p$, $j \in J$. In fact, being J minimal, necessarily $c_j \neq 0$, $\forall j \in J$. Then $d = (d_j)_{j=0}^{n-1}$ such that

$$\forall j = 0, 1, \ldots, n-1 : \quad d_j = \begin{cases} 1 \text{ if } j = 0 \\ 0 \text{ if } j \notin J \\ -c_j \text{ if } j \in J \end{cases}$$

is a minimal codeword in the set $E \subset D^{\perp}$.

Conversely, for a minimal codeword d in $E \subset D^{\perp}$, its support I is a minimal access set. □

Remark 2. 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 (11), let $[v_j]_{j=1}^{n-1}$ be the shares calculated according to (12). Then, from Proposition 5 $s = \sum_{j \in J} c_j v_j$.

Remark 3. For any minimal access set $J \subset \{1, \ldots, n-1\}$, the above remark obviously holds as well. However for a particular secret $s \in \mathbb{F}_q$ and a particular choice of the vector $u \in \mathbb{F}_q^k$ it may happen that some shares v_j, with $j \in J$, take the value 0. It implies that the corresponding participants do not take part in the recovering process! This seems to contradict the minimality of J, but it is not any contradiction. The notion of minimality is independent of the secrets, indeed.

Example Let us consider the $[7, 4, 3]$-Hamming linear binary code $\mathcal{H}$, whose parity check matrix and generator matrix are, respectively,

$$H = \begin{pmatrix} 1\,1\,0\,1\,1\,0\,0 \\ 1\,0\,1\,1\,0\,1\,0 \\ 0\,1\,1\,1\,0\,0\,1 \end{pmatrix} \quad , \quad (H^{\perp})^T = \begin{pmatrix} 1\,0\,0\,0\,1\,1\,0 \\ 0\,1\,0\,0\,1\,0\,1 \\ 0\,0\,1\,0\,0\,1\,1 \\ 0\,0\,0\,1\,1\,1\,1 \end{pmatrix}.$$

The code $\mathcal{H}$ has 2^4 elements as displayed in Table 1. All codewords with initial entry equal to 1 are minimal, in the sense of Definition 1, except $[1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1]^T$.

We consider the Massey's SSS over the dual code $\mathcal{H}^{\perp}$ with generator matrix $G = H$. Suppose the dealer has the secret $s = 1 \in \mathbb{F}_2$.

The dealer may select, for instance $u_0 = [1\ \ 0\ \ 1]^T$ because

$$u_0^T g_0 = [1\ \ 0\ \ 1][1\ \ 1\ \ 0]^T = 1 = s.$$

Let $v = [v_i]_{i=1}^6 = \left[u_0^T g_j\right]_{i=1}^6 = [0\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1]$ be the list of shares. It may seem that the participant indexed by 3 may be neglected because the corresponding share is $v_3 = 0$.

However, if the dealer selects instead $u_1 = [1\ \ 0\ \ 0]^T$ which also satisfies $s = u_1^T g_0$ then the list of shares is $[1\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0]$, and in this case $v_3 = 1$ and $v_6 = 0$.

$$\mathcal{H} = \left\{ \begin{bmatrix} 0\\0\\0\\0\\0\\0\\0 \end{bmatrix} \begin{bmatrix} 0\\0\\0\\1\\1\\1\\1 \end{bmatrix} \begin{bmatrix} 0\\0\\1\\0\\0\\1\\1 \end{bmatrix} \begin{bmatrix} 0\\0\\1\\1\\1\\0\\0 \end{bmatrix} \begin{bmatrix} 0\\1\\0\\0\\1\\0\\1 \end{bmatrix} \begin{bmatrix} 0\\1\\0\\1\\0\\1\\0 \end{bmatrix} \begin{bmatrix} 0\\1\\1\\0\\1\\1\\0 \end{bmatrix} \begin{bmatrix} 0\\1\\1\\1\\0\\0\\1 \end{bmatrix} \right\}$$
$$\left\{ \begin{bmatrix} 1\\0\\0\\1\\0\\0\\1 \end{bmatrix} \begin{bmatrix} 1\\0\\0\\0\\1\\1\\0 \end{bmatrix} \begin{bmatrix} 1\\0\\1\\0\\1\\0\\1 \end{bmatrix} \begin{bmatrix} 1\\0\\1\\1\\0\\1\\0 \end{bmatrix} \begin{bmatrix} 1\\1\\0\\0\\0\\1\\1 \end{bmatrix} \begin{bmatrix} 1\\1\\0\\1\\1\\0\\0 \end{bmatrix} \begin{bmatrix} 1\\1\\1\\0\\1\\0\\0 \end{bmatrix} \begin{bmatrix} 1\\1\\1\\1\\1\\1\\1 \end{bmatrix} \right\}$$

Table 1. Code $\mathcal{H}$.

Indeed, the minimal access sets are determined according to Remark 4 by the following relations (we use the enumeration of the minimal codewords in the second row of $\mathcal{H}$ as presented in Table 1):

$$\begin{aligned} s = 1 &= v_3 + v_6 \\ &= v_4 + v_5 \\ &= v_2 + v_4 + v_6 \\ &= v_2 + v_3 + v_5 \\ &= v_1 + v_5 + v_6 \\ &= v_1 + v_3 + v_4 \\ &= v_1 + v_2 \end{aligned}$$

□

Theorem 3 ([2]). *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, $1 \le j \le n-1$:*
   - *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 $d^\perp \ge 3$ and $1 \le m \le \min\{k-1, d^\perp - 2\}$, then any m-set of participants is included in $(q-1)^m q^{k-(m+1)}$ minimal access sets.*

3.2 Massey's SSS with vector secrets

An immediate extension of Massey's SSS consists in 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 $\{1,\dots,n-1\}$ and the dealer with the index 0. The vector space $\mathbb{F}_q^{q^{k-1}+1}$ is the set of secrets. Given a secret $s \in \mathbb{F}_q^{q^{k-1}+1}$, the dealer finds vectors $u_0,\dots,u_{q^{k-1}} \in \mathbb{F}_q^k$ such that

$$\forall \kappa = 0,\dots,q^{k-1}: \quad s_\kappa = u_\kappa^T g_0 \in \mathbb{F}_q, \tag{14}$$

and calculates the vectors

$$\forall j = 1,\dots,n-1: \quad v_j = \left[u_\kappa^T g_j\right]_{\kappa=0}^{q^{k-1}} \in \mathbb{F}_q^{q^{k-1}+1}. \tag{15}$$

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

The analogous to the Theorem 2 holds almost verbatim:

Theorem 4. *A non-empty set $J \subset \{1,\dots,n-1\}$ 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*

$$[d_0 = 1] \;\&\; [\forall j \notin \{0\}\cup J: \; d_j = 0] \;\&\; [\exists j \in J: \; d_j \neq 0]\,. \tag{16}$$

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. Thus for any index subset $J \subset \{1,\dots,n-1\}$ and any coefficients $c_j \in \mathbb{F}_q$, $j \in J$, the following two conditions are equivalent:

$$g_0 - \sum_{j\in J} c_j g_j = 0 \tag{17}$$

$$\exists u_0,\dots,u_{q^{k-1}} \in \mathbb{F}_q^k \text{ pairwise distinct,} \quad \forall \kappa = 0,\dots,q^{k-1}: \quad u_\kappa^T \left(g_0 - \sum_{j\in J} c_j g_j \right) = 0$$

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

Corollary 1 also holds within this context. Besides, similar to Remark 2:

Remark 4. Let $J \subset \{1,\dots,n-1\}$ be an access set of participants. Given a secret $s \in \mathbb{F}_q^{q^{k-1}+1}$ and vectors $u_0,\dots,u_{q^{k-1}} \in \mathbb{F}_q^k$ chosen by the dealer in order to satisfy (14), let $[v_j]_{j=1}^{n-1}$ be the shares calculated according to (15). Then, the eq. (17) entails $s = \sum_{j\in J} c_j v_j$.

Remark 5. In the vector secret case, no share can have the value 0.

Clearly, by identifying an alphabet of q symbols with $\mathbb{F}_q$, then the vector space $\mathbb{F}_q^{q^{k-1}+1}$ is identified with the set of words with length $(q^{k-1}+1)$ over that alphabet.

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

Massey's SSS with vector secrets is an ideal SSS [**?**], 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 (16) but, due to Theorem 4, 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) [**?**]. 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 (11) and builds the shares according to (12).

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

Robustness against cheaters in scalar secrets A malicious participant, a *cheater*, $m \in J$ may deceive other participants in an access set $J \in \Gamma$, where $m \in J$. Namely, when trying to recover a secret $s \in K$ each participant $j \in J_m = J - \{m\}$ provides his share v_j while m provides $v'_m = v + \varepsilon$. Then the recovering process gives

$$s' = \sum_{j \in J_m} c_j v_j + c_m v'_m = s + c_m \varepsilon.$$

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

Suppose that $J \in \Gamma$ is minimal. In order to avoid a deception from m, the participants at J_m would provide modified shares, say v'_j, instead of correct shares v_j, with $j \in J_m$. The probability to cheat m is

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

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 J_m do not know the secret, $A_m(v) \leq \varepsilon$.

A modified SSS with the aim to avoid cheaters is proposed in [**?**]. Suppose that the dealer and an auxiliary black-box are honest. For any secret $s \in \mathbb{F}_q$ the dealer selects two vectors $u_1, u_2 \in \mathbb{F}_q^r$ 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 black-box 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 black-box reveals t_1 as the secret, otherwise, the black-box warns the existence of a cheater among the participants in J. It is proved [**?**] that the modified SSS has information rate $\frac{1}{2}$ and that it is (Γ, q^{-1})-robust.

We consider the following slight generalisation of robustness.

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

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

and

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

Suppose that in the modified SSS, $\forall j \in J - I$, $(v'_{j1}, v'_{j2}) = (v_{j1}, v_{j2}) + (\varepsilon_{j1}, \varepsilon_{j2})$. 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, success occurs if

$$2s_1\varepsilon_1 + \varepsilon_1^2 = \varepsilon_2. \tag{18}$$

There are exactly q pairs $(\varepsilon_1, \varepsilon_2) \in \mathbb{F}_q^2$ satisfying (18). Thus, $A_{IJ}(v) \le q^{-1}$.

Robustness against cheaters in vector secrets Consider the setting in Section 3.2 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 $\mathbb{F}_q^{q^{k-1}+1}$ is the set of secrets and the shares are vectors in $\mathbb{F}_q^{q^{k-1}+1}$. Then the above construction provides a VSSSS whose information rate is also $\frac{1}{2}$ but it is $(\Gamma, q^{-(q^{k-1}+1)})$-robust. Let us check this last assertion.

Given a secret $s \in \mathbb{F}_q^{q^{k-1}+1}$, the dealer finds vectors

$$u_{01}, \ldots, u_{q^{k-1},1}, u_{02}, \ldots, u_{q^{k-1},2} \in \mathbb{F}_q^k$$

such that

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

and calculates the vectors

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

The dealer gives the vector pair (v_{j1}, v_{j2}) as the corresponding share to the j-th participant. Then, as before, if J is a minimal access set and $I \subset J$ is a proper non-empty set then $A_{IJ}(v) \leq q^{-q^{k-1}+1}$.

3.4 Using the code based on resilient functions

Let q be the power of a prime numbe 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 2. Let $\mathcal{C}_f$ be the linear code defined at relation (2). According to Proposition 1, $\mathcal{C}_f$ is a linear $[(q^m-1)q^{m(n-1)}, (1+t)m]$-code. Then the construction given at Section 3.3, using the code $\mathcal{C}_f$ as the code D, gives a VSSSS that is $(\Gamma, q^{-(q^{k-1}+1)})$-robust, with $k = (1+t)m$ and involving up to $(q^m-1)q^{m(n-1)}$ participants.

References

1. Camion, P., Canteaut, A.: Construction of t-resilient functions over a finite alphabet. In: Maurer, U.M. (ed.) EUROCRYPT. Lecture Notes in Computer Science, vol. 1070, pp. 283–293. Springer (1996)
2. 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)
3. Massey, J.: Minimal codewords and secret sharing. In: Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory. pp. 276–279 (1993)
4. Zhang, X.M., Zheng, Y.: Cryptographically resilient functions. IEEE Transactions on Information Theory 43(5), 1740–1747 (1997)