Designs, Codes and Cryptography (2022) 90:427–442
https://doi.org/10.1007/s10623-021-00988-z

A study of the separating property in Reed-Solomon codes by bounding the minimum distance

Marcel Fernandez[1] · **Jorge J. Urroz**[1]

Received: 22 December 2020 / Revised: 16 November 2021 / Accepted: 17 November 2021 /
Published online: 5 January 2022

Abstract
According to their strength, the tracing properties of a code can be categorized as frameproof, separating, IPP and TA. It is known that, if the minimum distance of the code is larger than a certain threshold then the TA property implies the rest. Silverberg et al. ask if there is some kind of tracing capability left when the minimum distance falls below the threshold. Under different assumptions, several papers have given a negative answer to the question. In this paper, further progress is made. We establish values of the minimum distance for which Reed-Solomon codes do not posses the separating property.

Keywords Reed-Solomon codes · IPP codes · Separating codes

Mathematics Subject Classification 94

1 Introduction

As a motivation for our work, consider the distribution of digital goods. In the trade of digital content, safe guarding ownership rights is certainly a critical issue. A way to protect copyright consists of making each copy of the content unique. This is done by embedding a different mark in each delivered item. These hidden marks are typically strings of symbols. However, since now all objects are different, traitor users can get together and by comparing their copies, they create a new copy that tries to disguise their identities. This is known as a collusion attack and the newly created copy is usually called a pirate copy.

Communicated by C. J. Colbourn.

This work has been supported by the Spanish Government Grant TCO-RISEBLOCK (PID2019-110224RB-I00) MINECO .

✉ Marcel Fernandez
marcel@entel.upc.edu

Jorge J. Urroz
jorge.urroz@upc.edu

[1] Universitat Politécnica de Catalunya, Barcelona, Spain

A way to deal with collusion attacks is by taking the embedded symbol strings to be the code words of a code with tracing properties. There is a large literature about codes possessing different degrees of robustness against collusion attacks. Let us give a brief overview. Formal definitions will be done in subsequent sections. In a c-frameproof code [3], a coalition of at most c users can not create a pirate copy that contains the code word of another user not in the coalition. In c-secure frameproof codes two disjoint coalitions of at most c users can not create the same pirate copy. It has been shown [15], that the secure frameproof property is the same as the separating property [16]. Loosely speaking, a code is called c-separating (c-SEP), if for any two disjoint sets of at most c code words each, there exists at least one position where the set of symbols of the first set is disjoint from the set of symbols of the second set (see Definition 2). Codes with the Identifiable Parent Property (IPP) were introduced in [11]. Informally, a code has the c-IPP property if all coalitions of at most c traitors that can generate the same pirate copy have a non-empty intersection, i.e. have a common user. The IPP has received considerable attention in the recent years, having been studied by several authors [1,2,4,10,19]. An even stronger property is the Traceability property (c-TA). In this case, it is guaranteed that the "closest" authorized copy to a given pirate copy belongs to one of the traitors. Sufficient conditions for a code to be a c-TA code are stated in [18].

The work in [17] discusses efficient algorithms for the identification of traitors in schemes that use c-TA codes. Let M denote the size of the code. For TA codes, tracing is an $O(M)$ process, whereas for IPP codes tracing is more expensive, since it is an $O(\binom{M}{c})$ process. Being the TA property stronger than the IPP, but being tracing more costly for the IPP, it seems reasonable to expect that by relaxing the TA requirements one is left with a code that, even though is no longer c-TA, still possesses c-IPP. In this regard, Silverberg et al. asked the following question:

Question 1 [17] Is it the case that all c-IPP Reed-Solomon codes are also c-TA?

Although intuition might lead us to give a negative answer, in that same paper the authors used truncated Reed-Solomon codes to credit the exact opposite, that is, if a Reed-Solomon code does not have the TA property then it neither has the IPP. Later, the work in [14] not only reinforced this conjecture, but proved a stronger implication, namely that a Reed-Solomon code that is not c-TA it is neither c-SEP. Therefore, they generalized the above question to the following one:

Question 2 [14] Is it the case that all c-SEP Reed-Solomon codes are also c-TA?

In this paper, we supplement more evidence to this last question. The results we present, will hopefully contribute to a complete understanding of the tracing properties in Reed-Solomon codes.

2 Definitions and previous results

Let q be a prime power and let $\mathbb{F}_q$ denote the finite field with q elements. $\mathbb{F}_q^n$ will denote the set of all n-tuples with elements from $\mathbb{F}_q$. We define a linear code of length n to be a vector subspace of $\mathbb{F}_q^n$. Then, $\mathbb{F}_q$ is called the *code alphabet*, and the n-vectors in the code are called *code words*. The dimension of the code is defined as the dimension of the vector subspace. Let $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$ be two words, then the *Hamming distance* $d(\mathbf{u}, \mathbf{v})$ between $\mathbf{u}$ and $\mathbf{v}$ is the number of positions where $\mathbf{u}$ and $\mathbf{v}$ differ. The *minimum distance* d, is defined as the smallest distance between two different code words. A linear code over $\mathbb{F}_q$, of length n, dimension k and minimum distance d is denoted as an $[n, k, d]_q$-code.

Reed-Solomon codes can be defined as follows. Let $\mathbb{F}_q[x]$ be the ring of polynomials over $\mathbb{F}_q$. Take all polynomials of degree less than k, $\mathbb{F}_q[x]_{k-1} \subset \mathbb{F}_q[x]$. Let α be a primitive element of $\mathbb{F}_q$, so we have $\{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\} = \mathbb{F}_q \setminus \{0\}$.

Definition 1 An extended Reed-Solomon, $RS[n,k]_q$, code is defined as the vector subspace of $\mathbb{F}_q^n$ determined by all vectors of the form

$$\mathbf{v} = (f(0), f(1), f(\alpha), \ldots, f(\alpha^{q-2}))$$

where $f \in \mathbb{F}_q[x]_{k-1}$. Note that $n = q$.

If vectors are of the form:

$$\mathbf{v} = (f(1), f(\alpha), \ldots, f(\alpha^{q-2})),$$

that is, the polynomials f are not evaluated in the field element 0, then we say the code is a non-extended Reed-Solomon code. In this case $n = q - 1$.

As in the previous definition, throughout the paper, and probably with a slight abuse of notation, we will denote polynomials with an italic lowercase letter.

Reed-Solomon codes are maximum distance separable (MDS) [13]. That means they attain the Singleton bound with equality $d = n - k + 1$.

2.1 Definitions about codes with tracing properties

Let C be an $[n,k,d]$ code over $\mathbb{F}_q$, let $T = \{\mathbf{t}^1, \ldots, \mathbf{t}^c\} \subseteq C$ with $\mathbf{t}^i = (t_1^i, \ldots, t_n^i)$ be a subset of size c. Also, let $T|_i = \{t_i^j | \mathbf{t}^j \in T\}$. The *descendant set* of T, is defined as

$$desc(T) = \left\{ \mathbf{z} = (z_1, \ldots, z_n) \in \mathbb{F}_q^n | z_i \in T|_i \}, 1 \leq i \leq n \right\}.$$

Definition 2 A code C, defined over $\mathbb{F}_q$, has the (c_1, c_2)-separating property (denoted (c_1, c_2)-SEP), $c_1 > 0, c_2 > 0$, if for any two disjoint subsets of C, $U = (\mathbf{u}^1, \ldots, \mathbf{u}^{c_1})$ and $V = (\mathbf{v}^1, \ldots, \mathbf{v}^{c_2})$, we have

$$U|_i \cap V|_i = \emptyset \text{ for some } 1 \leq i \leq n.$$

If $c_1 = c_2 = c$, then we say that the code is c-separating and denote it as c-SEP.

In the introduction we used the name secure frameproof for the separating property.

Definition 3 A code C, defined over $\mathbb{F}_q$, has the c-Identifiable Parent Property (denoted c-IPP), $c > 0$, if for all $\mathbf{z} \in \mathbb{F}_q^n$ and for all coalitions $T \subseteq C$ of at most c code words, we have

$$\mathbf{z} \notin \bigcup_{T, |T| \leq c} desc(T) \text{ or } \bigcap_{\mathbf{z} \in desc(T)} T \neq \emptyset.$$

Definition 4 A code C is a c-traceability code (denoted c-TA), for $c > 0$, if for all subsets (coalitions) $T \subseteq C$ of at most c code words, if $\mathbf{z} \in desc(T)$, then there exists a $\mathbf{t} \in T$ such that $d(\mathbf{z}, \mathbf{t}) < d(\mathbf{z}, \mathbf{w})$ for all $\mathbf{w} \in C - T$.

We will also have occasion to link our discussion to a weaker tracing property called c-frameproof (FP).

Definition 5 A code C, defined over $\mathbb{F}_q$, has the c-Frameproof Property (denoted c-FP), $c > 0$, if for any code word $\mathbf{u}$ and a subset of C of size at most c, $V = (\mathbf{v}^1, \ldots, \mathbf{v}^c)$, with $\mathbf{u} \notin V$, we have

$$\mathbf{u}|_i \notin V|_i \quad \text{for some} \quad 1 \leq i \leq n.$$

Note that from Definition 2, $(c, 1)$-SEP is equivalent to c-FP.

2.2 Bezout identity

Some results in this paper, make extensive use of the Bezout identity. Intuitively, the Bezout identity is the ability to do the euclidean algorithm backwards.

Definition 6 Let u and v be two polynomials in $\mathbb{F}_q[x]$, and let $d = (u, v)$ a greatest common divisor of u and v. Given any k multiple of d, the Bezout identity ensures the existence of some elements a and b in $\mathbb{F}_q[x]$ such that

$$au - bv = k.$$

Recall that the solutions of the Bezout identity are not unique, and if (a, b) is a solution to Bezout identity, then all the solutions are of the form

$$\hat{a} = a + t\frac{v}{d} \qquad \hat{b} = b + t\frac{u}{d} \tag{1}$$

for some $t \in \mathbb{F}_q[x]$.

2.3 The separating property for Reed-Solomon codes

Let us recall previous results that lead to the motivation of our work. In [8], a sufficient condition for the c-SEP property is given:

Proposition 1 ([8], Proposition 1) *A code of length n, with minimum distance d, is c-SEP if*

$$d \geq n - \frac{n}{c^2} + \frac{1}{c^2}.$$

On the other hand, in [5,6,18] the same sufficient condition is given for the c-TA property:

Theorem 1 ([18], Theorem 4.4) *Suppose that C is a code of length n, having minimum hamming distance*

$$d > n - \frac{n}{c^2}.$$

Then C is c-TA code.

The family of Reed-Solomon codes are MDS codes. In [12], it is shown that for MDS codes, the previous sufficient condition for the c-TA property is also necessary.

Theorem 2 ([12], Theorem 2.3) *Let C be a linear $[n, k, d]$ MDS code over a finite field $\mathbb{F}_q$ such that $n \leq q + 1$. Then, for $c \geq 2$, C is an c-TA code if and only if $d > n - \frac{n}{c^2}$.*

In [18, Lemma 1.6] the authors show that if $|C| > c \geq q$ then C is not a c-IPP code. In [18, Lemma 1.3] it is shown that the c-TA property implies the c-IPP property. Interestingly enough in [17, Theorem 8] the authors construct a family of truncated $(n < q - 1)$ $RS[n, k]_q$

codes that fail to be c-IPP if $c^2 \geq n/(n-d)$. Then in [17, Question 11], the authors ask if it is always true that for Reed-Solomon codes the c-IPP fails if $c^2 \geq n/(n-d)$. This is a very interesting question because a positive answer would mean that for Reed Solomon the c-IPP and c-TA properties are essentially the same. In view of Proposition 1, in [14] this question was changed to Question 2 stated as in Sect. 1. Question 2 has been addressed in [9,14], obtaining the following results.

Theorem 3 ([9], Theorem 6) *Let $RS[n,k]_q$ be a Reed-Solomon code over $\mathbb{F}_q$ such that $k-1$ divides $q-1$. Then, if $d \leq n - \frac{n}{c^2}$ the code is not c-SEP.*

Corollary 1 ([14], Corollary 2) *Let C be an $[n,k,d]$ Reed-Solomon code over $\mathbb{F}_q$. If $c \geq \sqrt{q-1}$ and $d \leq (1-1/c^2)n$, then the code is not c-SEP.*

Theorem 4 ([14],Theorem 2) *Let $RS[n,k,d]_q$ be a Reed-Solomon code over $\mathbb{F}_q$ and c a divisor of q. Then, if $d \leq n - \frac{n}{c^2}$ the code is not c-SEP.*

Remark 1 It is worth noting, that the proofs of Theorem 3, Corollary 1 and Theorem 4, are constructive in the sense that, given a Reed-Solomon code C, explicit disjoint sets of code words F, G, with $|F| = r \leq c$, $|G| = s \leq c$, such that

$$F \cap G = \emptyset \text{ and } desc(F) \cap desc(G) \neq \emptyset \tag{2}$$

are found. In this paper our proofs are also constructive. Most of the results we obtain are based on the following observation, which in a sense, is a way to express the c-SEP property for Reed-Solomon in an algebraic manner. Suppose that $f_1, \ldots, f_r$, and $g_1, \ldots, g_s$ are the polynomials that generate the code words of F, G in (2) respectively. Then, it is clear that for extended Reed-Solomon codes, (2) is equivalent to

$$(x^q - x) \left| \prod_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}} (f_i - g_j). \right. \tag{3}$$

The code words in F, G belong to a Reed-Solomon code of minimum distance $d = q - m$ if the polynomials f_i, g_j are of degree at most m. See also Lemma 1 below. Further, note that if a Reed-Solomon code of minimum distance d over $\mathbb{F}_q$ is not c-SEP, then trivially codes of smaller minimum distance are not c-SEP, so we prove our results for the maximum possible minimum distance.

2.4 Our contribution

In this paper, progress in the understanding of the tracing properties in Reed-Solomon codes is made. Since the case $c \geq q$ is trivially true, by taking one coalition that includes all the constant polynomials, in the rest of the paper we assume $c < q$. In the style of Theorem 3 and Theorem 4, we use the structure of the finite field $\mathbb{F}_q$, over which the code is defined. In our particular case, we take advantage of the divisors of $q-1$. With that, we are able to give a complete answer to Question 2 by proving, in a constructive way, that in Reed-Solomon codes c-SEP and c-TA properties are essentially the same when $q \equiv 1 \pmod{c^2}$. More precisely, we set the minimum distance to $d = \lceil n - \frac{n}{c^2} \rceil$, which is the maximum allowed so the code is not c-TA, and then find two disjoint sets of code words that are not separated. In the rest of the paper, although the proofs are also constructive, the approach is somehow

different. We relax the distance condition and study whether an $[n, k, d]$ Reed-Solomon code over $\mathbb{F}_q$ with minimum distance $d < (n - r)$ is c-SEP for some $r > n/c^2$. We prove that Reed-Solomon codes are not c-SEP for $r = n/c$. Then, we proceed to strengthen this result. For the case $c = 2$, we answer the question for $r = \left[\frac{q}{3}\right]$ and for $c = 3$ we do so for $r = 2\left[\frac{q}{8}\right]$. For any $c \geq 2$, the question is answered for $r = \left[\frac{q}{2c-1}\right]$. We round up the paper using an elegant result of Cilleruelo [7], to give an alternate and more concise proof of known results.

3 A connection with the frameproof property

We start our discussion by studying Reed-Solomon codes over $\mathbb{F}_q$ with minimum distance $d \leq q - \frac{q}{c}$.

Theorem 5 *For any q a power of prime, $c \geq 2$ and $d \leq q - \dfrac{q}{c}$, extended Reed-Solomon $[n, k, d]$ codes over $\mathbb{F}_q$ are not c-SEP.*

Proof Let $\mathbb{F}_q = \{\alpha_1, \alpha_2 \ldots, \alpha_q\}$, with $\alpha_q = 0$, and $c \geq 2$ an integer. Also, write $q = cl + r$ where $0 \leq r < c$ and $l \in \mathbb{N}$. Since the case $c|q$ is taken care of in Theorem 4, we consider $c \nmid q$ and then $r > 0$. Since we are assuming $d \leq q - \dfrac{q}{c}$, we take the maximum allowed minimum distance $d = \lfloor q - \frac{q}{c} \rfloor$, and so $k = q - d + 1$.

Consider any set of c distinct polynomials $\{f_1, \ldots, f_c\} \subset \mathbb{F}_q[x]_{l-1}$. Observe that $c < q$, so we could take c distinct constant polynomials. Also note that we have the inequalities $1 \leq l = \frac{q}{c} - \frac{r}{c} < q - d$ and since l is an integer it implies $l + 1 \leq q - d = k - 1$. In this case $c(k - 1) \geq q$. Now, for $1 \leq i \leq r$ we take

$$g_i = f_i + \alpha_i \prod_{m=1}^{l+1} (x - \alpha_{(l+1)(i-1)+m}),$$

while for $r + 1 \leq i \leq c$ take

$$g_i = f_i + \alpha_i \prod_{m=1}^{l} (x - \alpha_{(i-1)l+m+r}).$$

Observe that $g_i \in \mathbb{F}_q[x]_{k-1}$ for all $1 \leq i \leq c$. Then, by construction, for every $1 \leq j \leq q$ the polynomials f_t and g_t, with $t = \lceil \frac{j}{l+1} \rceil$ when $j \leq r(l + 1)$ and $t = \lceil \frac{j-r}{l} \rceil$ when $r(l + 1) < j \leq q$, are such that $f_t(\alpha_j) = g_t(\alpha_j)$. Note that indeed $t \leq c$. Hence we have that $\{f_1(\alpha), \ldots, f_c(\alpha)\} \cap \{g_1(\alpha), \ldots, g_c(\alpha)\} \neq \emptyset$ for any $\alpha \in \mathbb{F}_q$ and so the two sets of code words given by $(f_i(\alpha_1), \ldots, f_i(\alpha_n))$ and $(g_i(\alpha_1), \ldots, g_i(\alpha_n))$ for $1 \leq i \leq c$ are not separated.

We now show that the constructed polynomials are all different. First note that $f_i \neq g_i$, for all $1 \leq i \leq c$. Now, suppose $g_i = f_j$ for some $1 \leq i \neq j \leq c$. Then, by definition of g_i, we have

$$f_j - f_i = g_i - f_i = \alpha_i \prod_{\alpha \in A} (x - \alpha),$$

for some set $A \subset \mathbb{F}_q$ of size $|A| \geq l$, which is not possible since f_i, f_j are two distinct polynomials of degree at most $l - 1$.

In the same way if $g_i = g_j$ for some $i \neq j$, then

$$f_j - f_i = \alpha_i \prod_{\alpha \in A} (x - \alpha) - \alpha_j \prod_{\beta \in B} (x - \beta),$$

for some sets $A, B \subset \mathbb{F}_q$ of size $|A|, |B| \geq l$ which, again, is not possible since $\deg(f_j - f_i) \leq l - 1$ and on the right we have a polynomial of degree at least l, for $\alpha_i \neq \alpha_j$. □

In the previous proof, we have shown that all polynomials involved in the construction are different. In fact, this is more than we need, and proving that $f_i \neq g_j$ is enough by the following lemma. Given any multiset C, we will use the notation C' to denote the set of distinct elements of C.

Lemma 1 *Let c be a positive integer and F and G two multisets of not necessarily distinct polynomials with $F \cap G = \emptyset$ and $|F| = c$, $|G| = c$ such that*

$$(x^q - x) \left| \prod_{f_i \in F, g_j \in G} (f_i - g_j) \right. .$$

Then, there exist two sets of distinct polynomials, say $\hat{F}, \hat{G}$, so that $\hat{F} \supseteq F'$ and $\hat{G} \supseteq G'$ with $\hat{F} \cap \hat{G} = \emptyset$ and $|\hat{F}| = |\hat{G}| = c$ such that

$$(x^q - x) \left| \prod_{\hat{f}_i \in \hat{F} i, \hat{g}_j \in \hat{G}} (\hat{f}_i - \hat{g}_j) \right. .$$

Proof We start by noting that all the roots of $x^q - x$ are simple so, for any $p(x)|x^q - x$, we have that if $p(x)|R(x)^k$ for some $R(x)$ and any integer $k \geq 2$, then $p(x)|R(x)$. Then, by hypothesis

$$(x^q - x) \left| \prod_{f_i \in F, g_j \in G} (f_i - g_j) = \prod_{f_i \in F'} \left(\prod_{g_j \in G} (f_i - g_j) \right)^{e_i} \right. ,$$

for some $e_i \geq 1$. So, by the previous observation

$$(x^q - x) \left| \prod_{f_i \in F'} \left(\prod_{g_j \in G} (f_i - g_j) \right) = \prod_{g_j \in G} \prod_{f_i \in F'} (f_i - g_j) = \prod_{g_j \in G'} \prod_{f_i \in F'} (f_i - g_j)^{b_j} \right.$$

for some $b_j \geq 1$, and again we deduce

$$(x^q - x) \left| \prod_{f_i \in F', g_j \in G'} (f_i - g_j) \right| \prod_{\hat{f}_i \in \hat{F}, \hat{g}_j \in \hat{G}} (\hat{f}_i - \hat{g}_j) \; .$$

□

In Sect. 2.1 we defined c-frameproof codes, and stated that according to Definition 2, c-FP is in fact $(c, 1)$-SEP. It is a known result, see the proof of Lemma III.2 in [3], that if the minimum distance of a code of length n satisfies, $d > n - \frac{n}{c}$, then the code is c-FP. The proof of Theorem 5 can be easily adapted to show that a Reed-Solomon code with minimum distance $d \leq n - \frac{n}{c}$, is not $(c, 1)$-SEP, and therefore not c-FP.

4 Increasing the minimum distance

In the previous section we saw that Reed Solomon codes with small distance are not separated. This is consistent with intuition. Since the code has a larger dimension as a vector space, then chances there exist more sets of code words that are not "separated". In this section, we discuss strategies to increase the minimum distance of the code and still keep non-separation.

4.1 The case $c = 2$

To show our approach we first deal with a particular case.

Lemma 2 *The* [11, 4, 8] *extended Reed-Solomon code over* F_{11} *is not* 2*-separating.*

Proof We will find polynomials f_1, f_2 and g_1, g_2, such that the corresponding pairs of code-words $\{\mathbf{f}_1, \mathbf{f}_2\}$ and $\{\mathbf{g}_1, \mathbf{g}_2\}$ are not separated.

Consider the polynomial $f_1 = 0$, and take $g_1 = \gamma_1 \prod_{i=1}^{3}(x - \alpha_i)$, for some $\{\gamma_1, \alpha_1, \alpha_2, \alpha_3\} \subset \mathbb{F}_{11}$. Now, let

$$f_2 = \sum_{i=1}^{3} g_1(\alpha_{3+i}) \frac{\prod_{j\in\{1,2,3\}, j\neq i}(x - \alpha_{3+j})}{\prod_{j\in\{1,2,3\}, j\neq i}(\alpha_{3+i} - \alpha_{3+j})} + \phi_2 \prod_{i=1}^{3}(x - \alpha_{3+i}),$$

for some $\{\phi_2, \alpha_4, \alpha_5, \alpha_6\} \subset \mathbb{F}_{11}$. Finally, consider

$$g_2 = \gamma_2 \prod_{i=1}^{3}(x - \alpha_{6+i}),$$

for some $\{\gamma_2, \alpha_7, \alpha_8, \alpha_9\} \subset \mathbb{F}_{11}$.

By construction $\{f_1(\alpha_i),\ f_2(\alpha_i)\} \cap \{g_1(\alpha_i),\ g_2(\alpha_i)\} \neq \emptyset$ for $i = 1, \ldots, 9$. Now, selecting ϕ_2, γ_2 such that

$$\sum_{i=1}^{3} g_1(\alpha_{3+i}) \frac{\prod_{j\in\{1,2,3\}, j\neq i}(\alpha_{10} - \alpha_{3+j})}{\prod_{j\in\{1,2,3\}, j\neq i}(\alpha_{3+i} - \alpha_{3+j})} \tag{4}$$

$$= \gamma_2 \prod_{i=1}^{3}(\alpha_{10} - \alpha_{6+i}) - \phi_2 \prod_{i=1}^{3}(\alpha_{10} - \alpha_{3+i}) \tag{5}$$

$$\sum_{i=1}^{3} g_1(\alpha_{3+i}) \frac{\prod_{j\in\{1,2,3\}, j\neq i}(\alpha_{11} - \alpha_{3+j})}{\prod_{j\in\{1,2,3\}, j\neq i}(\alpha_{3+i} - \alpha_{3+j})} \tag{6}$$

$$= \gamma_2 \prod_{i=1}^{3}(\alpha_{11} - \alpha_{6+i}) - \phi_2 \prod_{i=1}^{3}(\alpha_{11} - \alpha_{3+i}), \tag{7}$$

which is possible whenever

$$\prod_{i=1}^{3}(\alpha_{10} - \alpha_{6+i})(\alpha_{11} - \alpha_{3+i}) \neq \prod_{i=1}^{3}(\alpha_{11} - \alpha_{6+i})(\alpha_{10} - \alpha_{3+i}),$$

we get

$$f_2(\alpha_{10}) = g_2(\alpha_{10})$$
$$f_2(\alpha_{11}) = g_2(\alpha_{11})$$

and hence the pairs $\{\mathbf{f}_1, \mathbf{f}_2\}$ and $\{\mathbf{g}_1, \mathbf{g}_2\}$ are not separated. □

As an example take $\alpha_i = i$. Then

$$\prod_{i=1}^{3}(\alpha_{10} - \alpha_{6+i})(\alpha_{11} - \alpha_{3+i}) = \prod_{i=1}^{3}(4-i)(8-i) = 7!/4,$$

while

$$\prod_{i=1}^{3}(\alpha_{11} - \alpha_{6+i})(\alpha_{10} - \alpha_{3+i}) = \prod_{i=1}^{3}(5-i)(7-i) = 4 \cdot 6!.$$

In this case

$$\begin{aligned} g_1 &= x^3 - 6x^2 + 11x - 6 \\ f_2 &= 5x^3 + 10x + 9 \\ g_2 &= 10x^3 + x^2 + x + 9 \end{aligned}$$

and we have that

$$\begin{aligned} \mathbf{f}_1 &= (0,0,0,0,0,0,0,0,0,0,0) \\ \mathbf{f}_2 &= (2,3,9,6,2,5,1,9,4,5,9) \end{aligned}$$

$$\begin{aligned} \mathbf{g}_1 &= (0,0,0,6,2,5,10,1,6,9,5) \\ \mathbf{g}_2 &= (6,1,10,5,2,6,0,0,0,5,9) \end{aligned}$$

are not separated. It is clear that the solution is not unique, Taking $\alpha_i = i + 1$, we get

$$\begin{aligned} g_1 &= x^3 - 9x^2 + 26x - 24 \\ f_2 &= -\frac{13}{4}x^3 + \frac{135}{2}x^2 - \frac{1715}{4}x + \frac{1737}{2} \\ g_2 &= -x^3 + 27x^2 - 242x + 720, \end{aligned}$$

which give the pairs

$$\begin{aligned} \mathbf{f}_1 &= (0,0,0,0,0,0,0,0,0,0,0) \\ \mathbf{f}_2 &= (9,2,3,9,6,2,5,1,9,4,5) \end{aligned}$$

$$\begin{aligned} \mathbf{g}_1 &= (5,0,0,0,6,2,5,10,1,6,9) \\ \mathbf{g}_2 &= (9,6,1,10,5,2,6,0,0,0,5) \end{aligned}$$

that are also not separated.

Note that the previous lemma answers Question 2, for $q = 11$ and $c = 2$ and for these particular values improves Theorem 5. However, this approach does not fully generalize. Fortunately, for general q we can give a fully explicit answer, by decreasing a bit the distance of the code.

Theorem 6 *The extended Reed Solomon code over $\mathbb{F}_q$ with distance given by $d = q - \left[\frac{q}{3}\right]$ is not 2-SEP.*

Proof Let $q = 3l + r$ where $0 \leq r \leq 2$, and consider for any $1 \leq i, j \leq 2$, $A_{i,j} \subset \mathbb{F}_q$ disjoint sets such that $A_{2,2} = \emptyset$, and $|A_{i,j}| = l + 1$ for r of them and $|A_{i,j}| = l$ for the remaining $3 - r$ sets. Now let $p_{i,j} = \prod_{\alpha \in A_{i,j}} (x - \alpha)$. Observe that $\cup_{i,j} A_{i,j} = \mathbb{F}_q$. The following polynomials, of degree at most $l + 1$ define a code that is not 2-SEP.

$$\begin{aligned} f_1 &= 0, \\ f_2 &= p_{2,1} - p_{1,1}, \\ g_1 &= -p_{1,1}, \\ g_2 &= -p_{1,2}. \end{aligned}$$

Indeed, for any $\alpha \in A_{1,1}$ we have $f_1 = g_1$, for those $\alpha \in A_{1,2}$, $f_1 = g_2$, and for those $\alpha \in A_{2,1}$, $f_2 = g_1$, completing all the roots in $\mathbb{F}_q$. □

4.2 The case $c = 3$

Let us move to a larger value of c and deal with the case $c = 3$.

The representation of the Bezout identity in Definition 6 is not unique. For univariate polynomials we have the following lemma.

Lemma 3 *Let $u, v \in \mathbb{F}_q[x]$ be two non constant polynomials relatively prime and $z \in \mathbb{F}_q[x]$. Then there exist non zero polynomials $a, b \in \mathbb{F}_q[x]$ such that*

$$z = au - bv,$$

with $\max\{\deg(au), \deg(bv)\} \leq \max\{\deg(z), \deg(uv) - 1\}$*, if z is not a multiple of neither u nor v, or* $\max\{\deg(au), \deg(bv)\} \leq \max\{\deg(z), \deg(uv)\}$ *if $u|z$ or $v|z$.*

Proof If $u|z$ then all the solutions are of the form $a = z/u + kv$, $b = ku$ and the result follows taking $k \in \mathbb{F}_q^*$. So, we assume $u \nmid z$ and $v \nmid z$. By the Bezout identity we have that, for some $\hat{a}, \hat{b} \in F_q[x]$,

$$\hat{a}u - \hat{b}v = z \tag{8}$$

Suppose $\deg(z) < \deg(uv)$. If $\deg(\hat{a}) < \deg(v)$ then the theorem follows because

$$\deg(\hat{b}v) = \deg(\hat{a}u - z) \leq \max\{\deg(\hat{a}u), \deg(z)\} < \deg(uv) \tag{9}$$

Assume $\deg(\hat{a}) \geq \deg(v)$. As stated in (1), the pair $a = \hat{a} + tv$, $b = \hat{b} + tu$ also satisfies Bezout's identity for any $t \in \mathbb{F}_q[x]$. Dividing $\hat{a}$ by v, we get $\hat{a} = q_a v + r_a$ with $\deg(r_a) < \deg(v)$ and taking $t = -q_a$, we have that $a = r_a$, $b = \hat{b} - q_a u$ and the result follows using the same reasoning as in (9), since a and b also satisfy Bezout's identity.

Now, suppose $\deg(uv) \leq \deg(z)$. Dividing z by u we get $z = q_z u + r$ with $r \neq 0$, and $\deg(r) < \deg(u)$. We solve

$$\hat{a}u - \hat{b}v = r$$

with $\deg(\hat{a}) < \deg(v)$, which is possible by using the previous case, since $\deg(r) < \deg(u) < \deg(uv)$. Then, taking $a = \hat{a} + q_z$, $b = \hat{b}$ we have

$$au - bv = z, \tag{10}$$

with $\deg(a) = \deg(\hat{a} + q_z) = \deg(q_z) = \deg(z) - \deg(u)$, since by the assumption done in this case,

$$\deg(\hat{a}) < \deg(v) \leq \deg(z) - \deg(u) = \deg(q_z).$$

Hence $\deg(au) = \deg(z)$ and then, by identity (10), $\deg(bv) \leq \deg(z)$. Indeed, if $\deg(bv) > \deg(z)$, then

$$\deg(z) = \deg(au - bv) = \deg(bv) > \deg(z),$$

which is impossible. □

We have the following theorem.

Theorem 7 *Let q be a power of a prime, $c = 3$ and $d < q - 2\left[\frac{q}{8}\right]$. A Reed Solomon code of length q over $\mathbb{F}_q$ with distance d is not 3-SEP.*

Proof In order to get the result, we need to define 6 distinct polynomials $f_1, f_2, f_3, g_1, g_2, g_3$, that satisfy (3) for $c = r = s = 3$, that is,

$$(x^q - x) \Bigg| \prod_{1 \leq i,j \leq 3} (f_i - g_j). \tag{11}$$

Let $q = 8l + r$, where $0 \leq r < 8$. We make a partition of $\mathbb{F}_q$ in nine disjoint sets $U_{i,j} \subset \mathbb{F}_q$, $1 \leq i, j \leq 3$, as follows: $U_{1,1} = \emptyset$, r sets of size $l + 1$ and the other remaining $8 - r$ sets of size l. Since $r < 8$, we will always take $|U_{2,1}| = l$. Observe that $\sum_{i,j} |U_{i,j}| = q$ and let $u_{1,1} = -1$, $u_{i,j} = \prod_{\alpha \in U_{i,j}} (x - \alpha)$ for $(i, j) \neq (1, 1)$. Note that (11) is verified if

$$f_i - g_j = u_{i,j} v_{i,j}$$

for some $v_{i,j} \in \mathbb{F}_q[x]$ and $1 \leq i, j \leq 3$. This condition is equivalent to

$$f_i = g_i + u_{i,i} v_{i,i}. \tag{12}$$

and

$$g_3 - g_j = u_{i,j} v_{i,j} - u_{i,3} v_{i,3}. \tag{13}$$

for $1 \leq j \leq 3$, $1 \leq i \leq 3$. Indeed, one direction is immediate, while for the other we have

$$\begin{aligned} f_i - g_j &= f_i - f_3 + f_3 - g_j \\ &= g_i - g_3 + u_{i,i} v_{i,i} - u_{3,3} v_{3,3} + u_{3,3} v_{3,3} + g_3 - g_j \\ &= u_{i,3} v_{i,3} - u_{i,i} v_{i,i} + u_{i,i} v_{i,i} + u_{i,j} v_{i,j} - u_{i,3} v_{i,3} \\ &= u_{i,j} v_{i,j} \end{aligned}$$

Observe that, to verify (13) we need to define $v_{i,j}$ so that the right hand side is independent of the value of i. So, for example let us start by taking $v_{i,j}$ for $j \neq 1$, solutions of the Bezout equations

$$v_{i,2} u_{i,2} - v_{i,3} u_{i,3} = 1, \tag{14}$$

for $i = 1, 2, 3$. Note that according to Lemma 3, we can take the solutions such that $\deg(v_{i,j} u_{i,j}) \leq 2l + 1$, for $j \neq 1$.

Then, we proceed similarly to define $v_{2,1}$, $v_{3,1}$ to be solutions of the Bezout equation

$$v_{3,3} u_{3,3} - v_{2,3} u_{2,3} = v_{3,1} u_{3,1} - v_{2,1} u_{2,1}. \tag{15}$$

Again, since $\deg(u_{2,1}) = l$, by Lemma 3 we can take the degree of $v_{2,1} u_{2,1}$, $v_{3,1} u_{3,1}$ at most $2l + 1$. Finally, let us take the last entry $v_{1,1} = v_{3,3} u_{3,3} - v_{3,1} u_{3,1} - v_{1,3} u_{1,3}$. If $v_{1,1} = 0$, then according to (1) we consider the solution to (15) given by $\hat{v}_{3,1} = v_{3,1} + c u_{2,1}$, $\hat{v}_{2,1} = v_{2,1} + c u_{3,1}$ for some constant $c \neq 0$ so that $\hat{v}_{3,1} \neq 0$ and $\hat{v}_{2,1} \neq 0$, and the corresponding $\hat{v}_{1,1} = v_{3,3} u_{3,3} - \hat{v}_{3,1} u_{3,1} - v_{1,3} u_{1,3} = -c u_{2,1} u_{3,1} \neq 0$.

Observe that

$$\deg(\hat{v}_{3,1}u_{3,1}) = \deg(v_{3,1}u_{3,1} + cu_{2,1}u_{3,1}) \leq 2l+1$$

by our selection of $u_{2,1}$, and then $\deg(\hat{v}_{2,1}u_{2,1}) \leq 2l+1$, so we can always take $v_{1,1} \neq 0$. Now we define

$$\begin{aligned} g_1 &= -v_{3,1}u_{3,1}, \quad & f_1 &= g_1 + v_{1,1}u_{1,1}, \\ g_2 &= -v_{3,2}u_{3,2}, \quad & f_2 &= g_2 + v_{2,2}u_{2,2}, \\ g_3 &= -v_{3,3}u_{3,3}, \quad & f_3 &= g_3 + v_{3,3}u_{3,3}. \end{aligned} \tag{16}$$

Note that $f_3 = 0$. Now we need to prove (13). Observe that by definition,

$$g_3 - g_j = v_{3,j}u_{3,j} - v_{3,3}u_{3,3}.$$

It remains to prove (13) for $i = 1, 2$, $j = 1, 2$. For $j = 2$, the right hand of (13) is independent of i as a consequence of (14). Now, for $j = 1$ on the one hand,

$$u_{2,1}v_{2,1} - u_{2,3}v_{2,3} = u_{3,1}v_{3,1} - u_{3,3}v_{3,3} = g_3 - g_1$$

by (15). On the oher hand, by the definitions of $u_{1,1}$ and $v_{1,1}$

$$u_{1,1}v_{1,1} - u_{1,3}v_{1,3} = u_{3,1}v_{3,1} - u_{3,3}v_{3,3} = g_3 - g_1$$

as we wanted. Observed that, by construction $\deg(f_i) \leq 2l+1$, $\deg(g_i) \leq 2l+1$ and $f_i \neq g_j$ for $1 \leq i, j \leq 3$, and hence the result follows by Lemma 1. Also, since $2l+1 \leq k-1$, for extended Reed-Solomon codes $n - d = q - d = k - 1$, the claim about the distance follows by Remark 1, since we are taking $q = 8l + r$. □

5 The general case

In order to obtain stronger results, we have to deal with larger values of both c and the minimum distance. The following theorem generalizes Theorem 6 for $c \geq 2$.

Theorem 8 *Let q be a power of a prime, $c \geq 2$ and $d < q - \left\lceil \frac{q}{2c-1} \right\rceil$. Extended Reed Solomon codes over $\mathbb{F}_q$ with distance d are not c-SEP.*

Proof Let $q = (2c-1)l + r$ where $0 \leq r < 2c-1$, and consider for any $1 \leq i \leq 2c-1$, $A_i \subset \mathbb{F}_q$ disjoint sets such that: r of the sets are of size $|A_i| = l+1$ and the remaining $2c - r - 1$ are of size $|A_i| = l$. Now let $p_i = \prod_{\alpha \in A_i}(x - \alpha)$. Observe that $\cup_i A_i = \mathbb{F}_q$. The following polynomials, of degree at most $l+1$ evaluate to code words of a code that is not c-SEP.

$$\begin{aligned} f_1 &= 0, \\ f_{i+1} &= p_{c+i} - p_i, \quad \text{for } 1 \leq i \leq c-1 \\ g_i &= -p_i, \quad \text{for } 1 \leq i \leq c. \end{aligned}$$

Indeed, observe that $f_1(\alpha) = g_i(\alpha)$ for any $\alpha \in A_i$, $1 \leq i \leq c$, while $f_{i+1}(\alpha) = g_i(\alpha)$ for any $\alpha \in A_{c+i}$ for any $1 \leq i \leq c-1$.

The claim about the distance follows by Remark 1, using the same reasoning as in the proof of Theorem 7. □

To cope with a larger minimum distance, we would like to extend Theorem 7. Unfortunately, the generalization is not immediate because when c grows, the degree of the

polynomials $v_{i,j}$ blows up, so we try to take advantage of the structure of the field over which the code is defined. In this case we are able to state a result for a minimum distance matching the conjectured one.

Theorem 9 *Let c be any integer and $q \equiv 1 \pmod{c^2}$. The non extended Reed Solomon code over F_q with distance $d = q - \frac{q-1}{c^2} - 1$ is not c-SEP.*

Proof Let α be a primitive root of the multiplicative group $\mathbb{F}_q^*$. Since $c^2 | q-1$, we can consider $g_i = \alpha^{i\frac{(q-1)}{c^2}}$, and $f_i = \alpha^{\frac{-i(q-1)}{c}} x^{\frac{q-1}{c^2}}$, $i = 0, \ldots, c-1$. Now, every element of $\mathbb{F}_q^*$ can be written as $\alpha_{r,s} = \alpha^{lc^2+rc+s}$ for some $0 \leq s, r < c$, and certain integer l. Then

$$f_r(\alpha_{r,s}) = \alpha^{\frac{-r(q-1)}{c}} (\alpha^{lc^2+rc+s})^{\frac{q-1}{c^2}} = \alpha^{\frac{s(q-1)}{c^2}} = g_s,$$

proving the result. □

Corollary 2 *For any p and c there exist infinitely many integers e so that for $q = p^e$ the non extended Reed-Solomon code over $\mathbb{F}_q$ of distance $d = q - \left[\frac{q}{c^2}\right] - 1$ is not c-SEP.*

Proof Simply note that by Euler's theorem $p^{\varphi(c^2)} \equiv 1 \pmod{c^2}$, so the result follows for any $e = k\varphi(c^2)$, $k \in \mathbb{N}$, applying the previous theorem. □

6 The "linear" case $d = q - 1$

The case presented in this section is already dealt with, in Corollary 1. We include it here, because the proofs might provide new ways to approach a complete solution to the problem.

The first result we prove is a straight forward application of the following theorem of J. Cilleruelo in [7].

Theorem 10 ([7], J. Cilleruelo) *Let α be a generator of $\mathbb{F}_q^*$. Then*

$$\{\alpha^i - \alpha^j \ : \ 0 \leq i, j \leq 2q^{3/4}\} = \mathbb{F}_q.$$

Now, we have

Theorem 11 *Let $c \geq 2q^{3/4}$. Then, the $[n, k, d]$ extended Reed Solomon codes over F_q and distance $d = q - 1$ are not c-SEP.*

Proof Let us first note that, since $c \geq 2q^{3/4}$, then $c^2 > q$ and then $q - [q/c^2] - 1 = q - 1$. So we take $d = q - 1$ as distance of the code. This means that we need to find two sets of polynomials of size c each, with all polynomials of degree at most 1, such that

$$\{f_1(\alpha), \ldots, f_c(\alpha)\} \cap \{g_1(\alpha), \ldots, g_c(\alpha)\} \neq \emptyset$$

for any $\alpha \in \mathbb{F}_q$. As already mentioned, this is the same as (3), with $r = s = c$. Now, let α be a generator of $\mathbb{F}_q^*$, and consider $f_i = x - \alpha^i$, $g_i = -\alpha^i$, for $i = 1, \ldots, c$. It follows that,

$$\prod_{1 \leq i,j \leq c} (f_i - g_j) = \prod_{1 \leq i,j \leq c} (x - (\alpha^i - \alpha^j))$$

and by the previous theorem we trivially have

$$(x^q - x) \left| \prod_{1 \le i,j \le c} (f_i - g_j). \right.$$

Observe that in this case $\deg(f_i) = 1$ while $\deg(g_i) = 0$ so they can not be equal. □

But we can make it better.

Theorem 12 *Suppose that $q-1 = rs$ such that $(r, s) = 1$ and suppose $c > \max\{r, s\}$. Then, $[n, k, d]$ extended Reed Solomon codes with distance $d = q - 1$ over F_q are not c-SEP.*

Proof Let $q - 1 = rs$ such that $(r, s) = 1$, α a generator of $\mathbb{F}_q^*$ and consider the sets $A = \{1, \alpha^r, \ldots, \alpha^{r(s-1)}\}$ and $B = \{1, \alpha^s, \ldots, \alpha^{s(r-1)}\}$. Then, all the quotients a/b with $a \in A$ and $b \in B$ are distinct. Indeed, suppose $\alpha^{ri}/\alpha^{sj} = \alpha^{rI}/\alpha^{sJ}$. Then $\alpha^{r(i-I)-s(j-J)} = 1$ but, since α is a generator, this is only possible either if $r(i - I) - s(J - j) = 0$ or else if $(q - 1)|r(i - I) - s(J - j)$. In any of the two cases, since $r|q - 1$, we have $r|s(J - j)$ and since $(r, s) = 1$, then $r|(J - j)$ but this is impossible, since $|J - j| < r$, unless $J = j$, and then $i = I$.

Now, consider polynomials $f_i = \alpha^{ri}x$, $g_j = \alpha^{sj}$ with $0 \le i \le s - 1$ and $0 \le j \le r - 1$. We can do that since $\max\{r, s\} < c$. By the previous argument, the roots of $f_i - g_j$ are all distinct and we have $rs = q - 1$ distinct roots. Since $r < c$ we can just add the root missing by adding a polynomial $g_r = 0$, and again the proof follows by (3).

Observe that, since $c > s$, then $c^2 > rs = q - 1$, and we can suppose $c^2 > q$ since the case $c^2 = q$ is already proved, (see Theorem 2 in [14]). So $[q/c^2] = 0$ and the correct distance is $d = q - 1$, so we in fact have to consider linear polynomials. □

Note that, any q a power of a prime except $q = 9$, verifies the condition $q - 1 = rs$ with $(r, s) = 1$. Indeed, if not r and s would be powers of the same prime l, but then $q - 1 = p^r - 1 = l^e$. By the proof of Catalan 's conjecture, we know that $q^x - p^y = 1$ only in the case $3^2 - 2^3$.

The previous theorem improves Theorem 11 when q is an even power of a prime. Indeed, in the case in which $q = p^{2t}$, then either $(p^t-1)/2$ is odd or $(p^t+1)/2$ is odd. Without loss of generality, assume $(p^t-1)/2$ is odd. Then, we can take $r = (p^t-1)/2$ and $s = 2(p^t+1)$ and so $s \le 4r+4$. Therefore, $q-1 = rs \le 4r^2+4r$ or $q \le 4r^2+4r+1 = (2r+1)^2$ which gives $r \ge (\sqrt{q}-1)/2$. Then, $q-1 = rs \ge ((\sqrt{q}-1)/2)s$ which gives $s \le \frac{q-1}{(\sqrt{q}-1)/2} = 2(\sqrt{q}+1)$. Hence, since Theorem 12 assumes $c > s$ then for any $c > 2(\sqrt{q} + 1)$ we have that Reed Solomon code with distance $d = q - 1$ over F_q are not c-SEP, improving Theorem 11.

In general, the theorem provides a general bound on c, depending on the factorization of the exponent. However, in the case of a sophie germain prime, $q - 1 = 2p$ where q and p are primes, then Theorem 12 only gives $c \ge q/2$.

7 Conclusion

The aim of the paper, is to find out whether or not there exist values of the minimum distance for which a Reed-Solomon is c-SEP but not c-TA. We start the presentation by considering a sufficiently small value of the minimum distance. For this much convenient value, we prove that codes do not posses the separating property. For cases $c = 2$ and $c = 3$, we improve

this almost naive result by introducing to our discourse both polynomial interpolation and Bezout's identity.

The approach for case $c = 3$ does not generalize to larger values of c. In order to deal with the general case, we resort to the structure of $\mathbb{F}_q$, the finite field over which the code is defined. This allows us to prove an assertion for all c, whenever $q \equiv 1 \pmod{c^2}$. Along the same line of reasoning, we provide an alternative proof of existing results by applying an elegant theorem concerning the generator of the multiplicative group of $\mathbb{F}_q$.

Our presentation shows that for the general case, a constructive proof is by no means trivial. This is because, when using the structure of the field defining the code one can not encircle all cases and cases without "structure" do not seem to follow any common pattern. So, although the problem is algebraic in nature, it seems that an existence proof could be considered.

Finally, to put our contribution into perspective, we present a list of families of $[n, k, d]_q$ Reed-Solomon codes, both from existing literature and this paper, for which Question 2 is answered.

- **Previous works**
  - *Maximum minimum distance*, $d \leq n - \frac{n}{c^2}$.
    - If $c^2 \geq q - 1$. Corollary 2 in [14].
    - If $c|q$. Theorem 2 in [14].
    - If $k - 1|q - 1$. Theorem 6 in [9].
- **This paper**
  - *Maximum minimum distance*.
    - If $d = q - \frac{q-1}{c^2} - 1$ and $q \equiv 1 \pmod{c^2}$. Theorem 9.
    - If $d = q - \frac{q-1}{c^2} - 1$, for any p and c, there exist infinitely many integers e for which we can take $q = p^e$. Corollary 2.
    - If $d = q - 1$ and $c \geq 2q^{3/4}$. Theorem 11.
    - If $d = q - 1$ and $q - 1 = rs$ with $(r, s) = 1$ and $c > \max\{r, s\}$. Theorem 12.
  - *Conditions on the minimum distance*.
    - If $d \leq q - \frac{q}{c}$ and $c \geq 2$. Theorem 5.
    - If $d = q - \left[\frac{q}{3}\right]$ and $c = 2$. Theorem 6.
    - If $d < q - 2\left[\frac{q}{8}\right]$ and $c = 3$. Theorem 7.
    - If $d < q - \left[\frac{q}{2c-1}\right]$ and $c \geq 2$. Theorem 8.

Acknowledgements We would like to express our gratitude to the referees for their detailed reviews and their valuable comments.

References

1. Barg A., Cohen G.D., Encheva S.B., Kabatiansky G., Zemor G.: A hypergraph approach to the identifying parent property: the case of multiple parents. Electron. Notes Discret. Math. **6**, 1–3 (2001).
2. Barg A., Kabatiansky G.A.: A class of i.p.p. codes with efficient identification. J. Complexity **20**(2–3), 137–147 (2004).
3. Boneh D., Shaw J.: Collusion-secure fingerprinting for digital data. IEEE Trans. Inf. Theory **44**(5), 1897–1905 (1998).
4. Cohen M., Fu H.-L., Jing J., Yuan-Hsun L., Ying M.: Codes with the identifiable parent property for multimedia fingerprinting. Des. Codes Cryptogr. **83**, 11 (2014).
5. Chor B., Fiat A., Naor M.: Tracing traitors. Adv. Cryptol. Crypto'94. LNCS **839**, 480–491 (1994).
6. Chor B., Fiat A., Naor M., Pinkas B.: Tracing traitors. IEEE Trans. Inform. Theory **46**, 893–910 (2000).
7. Cilleruelo J.: Combinatorial problems in finite fields and Sidon sets. Combinatorica **32**(5), 497–511 (2012).
8. Cohen G.D., Schaathun H.G.: Separating codes: constructions and bounds. In: LATIN 2004: Theoretical Informatics: 6th Latin American Symposium, Buenos Aires, Argentina, April 5–8, 2004. Proceedings, volume **2976**, pp. 322–328, April (2004).
9. Fernandez M., Cotrina J., Soriano M., Domingo N.: A note about the identifier parent property in Reed-Solomon codes. Comput. Secur. **29**(5), 628–635 (2010).
10. Gu Y., Minquan C., Grigory K., Ying M.: Probabilistic existence results for parent-identifying schemes. IEEE Trans. Inf. Theory **65**(10), 6160–6170 (2019).
11. Hollmann H.D.L., van Lint J.H., Linnartz J.-P., Tolhuizen L.M.G.M.: On codes with the identifiable parent property. J. Comb. Theory **82**(2), 121–133 (1998).
12. Hongxia J., Mario B.: Combinatorial properties for traceability codes using error correcting codes. IEEE Trans. Inf. Theory **53**(2), 804–808 (2007).
13. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. North Holland, Amsterdam (1977).
14. Moreira K., Fernández M., Soriano M.: On the relationship between the traceability properties of Reed-Solomon codes. Adv. Math. Commun. **6**(4), 467–478 (2012).
15. Moreira K., Fernández M., Kabatiansky G.: Almost separating and almost secure frameproof codes over q-ary alphabets. Des. Codes Cryptogr. **80**(1), 11–28 (2016).
16. Sagalovich Y.L.: Separating systems. Problems Inf. Transm. **30**(2), 105–123 (1994).
17. Silverberg A., Staddon J., Walker J.L.: Applications of list decoding to tracing traitors. IEEE Trans. Inf. Theory **49**(5), 1312–1318 (2003).
18. Staddon J.N., Stinson D.R., Wei R.: Combinatorial properties of frameproof and traceability codes. IEEE Trans. Inf. Theory **47**(3), 1042–1049 (2001).
19. van Trung T., Sosina M.: New constructions for ipp codes. Des. Codes Cryptogr. **35**(2), 227–239 (2005).