Structural Properties of Twisted Reed–Solomon Codes with Applications to Cryptography

Peter Beelen[1], Martin Bossert[2], Sven Puchinger[2], and Johan Rosenkilde[1]

[1]Department of Applied Mathematics & Computer Science, Technical University of Denmark, Lyngby, Denmark
[2]Institute of Communications Engineering, Ulm University, Ulm, Germany
Email: *pabe@dtu.dk, martin.bossert@uni-ulm.de, sven.puchinger@uni-ulm.de, jsrn@jsrn.dk*

Abstract—We present a generalisation of Twisted Reed–Solomon codes containing a new large class of MDS codes. We prove that the code class contains a large subfamily that is closed under duality. Furthermore, we study the Schur squares of the new codes and show that their dimension is often large. Using these structural properties, we single out a subfamily of the new codes which could be considered for code-based cryptography: we show that these codes resist existing structural attacks for Reed–Solomon-like codes, i.e. methods for retrieving the code parameters from an obfuscated generator matrix.

Index Terms—MDS Codes, Reed–Solomon Codes, McEliece Cryptosystem, Structural Attacks

I. INTRODUCTION

Twisted Reed–Solomon codes [1] are maximum distance separable (MDS) codes[1] that can be efficiently decoded. Their construction is based on Reed–Solomon (RS) codes, by adding an extra monomial ("twist") to the low-degree evaluation polynomials and choosing the evaluation points in a suitable way.

We present a generalisation of twisted RS codes, where instead of one additional monomial, we add ℓ monomials ("twists") to the evaluation polynomials, similar to the recent extension of twisted Gabidulin codes [2]. We describe a large family of these which are MDS codes. We study the Schur square of twisted RS code and show that, unlike for RS codes, the dimension of the Schur square is not small. Moreover, we prove that the dual of a large class of twisted RS codes is equivalent to a twisted RS code. Finally, we show that decoding is feasible for codes with few twists.

As a potential application, we consider the use of twisted RS codes in the McEliece cryptosystem [3], which is a public-key cryptosystem and one of the candidates for post-quantum cryptography: a structured code $\mathcal{C}$ with an efficient decoding algorithm is the "secret key", while an obfuscated generator matrix $\tilde{\boldsymbol{G}}$ of $\mathcal{C}$ is made public, together with the decoding algorithm's decoding radius τ. Encryption consists of encoding a secret message with $\tilde{\boldsymbol{G}}$ and adding τ errors at random. A "structural attack" on the system is to recover an efficiently decodable code that is sufficiently close to $\mathcal{C}$ so that decoding the encrypted message is feasible. Such an attack is mostly interesting if it is faster than a generic decoding algorithm, e.g. information-set decoding see e.g. [3]–[5]. The original proposal [3], which remains unbroken, uses binary Goppa codes. For most other proposed codes, efficient structural attacks have been found (cf. [6]). Attacks on RS-like codes were presented in [7]–[10].

We single out a family of twisted RS codes for which all but one of these attacks will provably not work, provided we

add sufficiently many twists. The last attack – Wieschebrink's attack on the dual code – does not apply in any obvious way, but could conceivably apply in a surprising manner. The number of twists in our codes is $\ell = \lfloor \frac{1}{R} \rfloor$ for long enough codes, where R is the code rate.

The new codes are over large fields with field size $q \approx n^{2^\ell}$. This increases the size of storing the public key at a given length and dimension, i.e. the generator matrix, but since the complexities of generic attacks strongly depend on the field size, quite short lengths are sufficient for a target security level. We give example parameters for security levels 2^{100} and 2^{128} whose public key sizes are reduced by factors 2.7 and 7.4 compared to suggested parameters when using binary Goppa codes [11], [12] for the same security levels.

Notationally, matrices and vectors are generally bold-face, e.g. $\boldsymbol{A}$ and $\boldsymbol{v}$. If $\boldsymbol{v}$ is a vector, then v_i denotes its i'th element. When adding a constant to a vector, e.g. $\boldsymbol{v}+1$, we really mean $\boldsymbol{v} + (1, \ldots, 1)$. The diagonal matrix with diagonal entries $\boldsymbol{v}$ is denoted $\mathrm{diag}(\boldsymbol{v})$. We say that two codes are "equivalent" if one can be obtained from the other by permuting positions and element-wise scaling with non-zero field elements.

II. MULTI-TWISTED REED–SOLOMON CODES

A. Definition

Let $\mathcal{V} \subset \mathbb{F}_q[X]$ be a $\mathbb{F}_q$-linear subspace of polynomials. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ be distinct and write $\boldsymbol{\alpha} = [\alpha_1, \ldots, \alpha_n]$. We call $\alpha_1, \ldots, \alpha_n$ the *evaluation points*. Then we define the *evaluation map* of $\boldsymbol{\alpha}$ on $\mathcal{V}$ by

$$\mathrm{ev}_{\boldsymbol{\alpha}}(\cdot) : \mathcal{V} \to \mathbb{F}_q^n, \quad f \mapsto [f(\alpha_1), \ldots, f(\alpha_n)].$$

In this notation, an $[n, k]$ Reed–Solomon (RS) code with evaluation points $\boldsymbol{\alpha}$ is just the image of $\mathrm{ev}_{\boldsymbol{\alpha}}(\mathbb{F}_q[X]_{<k})$, where $\mathbb{F}_q[X]_{<k}$ denotes the set of polynomials in $\mathbb{F}_q[X]$ of degree at most $k-1$. A generalised Reed–Solomon code (GRS) is a code which is equivalent to an RS code.

Definition 1: Given a finite field $\mathbb{F}_q$ and code parameters $[n, k]$, let $\ell \in \mathbb{Z}_{>0}$ and $\boldsymbol{t}, \boldsymbol{h} \in \mathbb{Z}_{>0}^\ell$ such that

- The t_i are all distinct and $1 \le t_i \le n - k$.
- The h_i are all distinct and $0 \le h_i < k$.

Furthermore, let $\boldsymbol{\eta} \in (\mathbb{F}_q \setminus \{0\})^\ell$. The set of $(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$-*twisted polynomials* is given as:

$$\mathcal{P}_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}^{n,k} = \left\{ \sum_{i=0}^{k-1} f_i X^i + \sum_{j=1}^{\ell} \eta_j f_{h_j} X^{k-1+t_j} \; \Big| \; f_i \in \mathbb{F}_q \right\}.$$

$\mathcal{P}_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}^{n,k}$ is a k-dimensional $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q[X]$. We say that the space of polynomials has ℓ twists, each with twist t_i, hook h_i and coefficient η_i.

[1]Their length n, dimension k, and minimum distance d fulfil $d = n - k + 1$.

A $(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$-*twisted Reed–Solomon code* is given by $\boldsymbol{\alpha} \in \mathbb{F}_q^n$ with distinct entries and twisted polynomials $\mathcal{P}_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}^{n,k}$ as:

$$\mathcal{C}^{n,k}(\boldsymbol{\alpha},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}) = \mathrm{ev}_{\boldsymbol{\alpha}}(\mathcal{P}_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}^{n,k}) \subseteq \mathbb{F}_q^n .$$

For brevity, we will use the phrase *twisted RS codes*. Note that $\mathcal{C}^{n,k}(\boldsymbol{\alpha},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})$ indeed has dimension k since the evaluation map is injective: any polynomial $f \in \mathcal{P}_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}^{n,k}$ satisfies $\deg f \le k - 1 + \max_i\{t_i\} < n$.

The twisted RS codes of [1] are the special case of the above definition when $\ell = 1$; these will be referred to as "single-twisted RS codes". Specifically, the $(*)$-twisted codes introduced in [1] are the codes $\mathcal{C}^{n,k}(\boldsymbol{\alpha},1,0,\eta)$, where the set of coordinates $\boldsymbol{\alpha}$ is a subset of $\{0\} \cup G$ for a proper subgroup G of $\mathbb{F}_q^*$ and $(-1)^k\eta^{-1} \in \mathbb{F}_q^* \setminus G$. The $(+)$-twisted codes from [1] were defined as $\mathcal{C}^{n,k}(\boldsymbol{\alpha},1,k-1,\eta)$, where the set of coordinates $\boldsymbol{\alpha}$ is a subset of $\{\infty\} \cup V$ for a proper subspace V of $\mathbb{F}_q$ and $\eta^{-1} \in \mathbb{F}_q \setminus V$. Note that in [1] we defined evaluation at ∞, but that in the current paper we for simplicity refrain from using ∞ as an evaluation point.

B. A Constructive Class of MDS Twisted RS Codes

Not all twisted RS codes as defined in the previous section are MDS. We will now describe a simple way to choose the parameters which lead to a large family of MDS codes. This generalises a construction in [1] and is also inspired by a recently proposed family of twisted Gabidulin codes [2] which are MRD, i.e., MDS with respect to the rank metric.

Consider some $[n, k]$ ℓ-twisted RS code $\mathcal{C}^{n,k}(\boldsymbol{\alpha},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})$ and write $H = \{h_i \mid i = 1,\ldots,\ell\}$. A generator matrix $\boldsymbol{G} \in \mathbb{F}_q[\boldsymbol{\eta}]^{k \times n}$ for $\mathcal{C}^{n,k}(\boldsymbol{\alpha},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})$ can be obtained as the image of $\mathrm{ev}_{\boldsymbol{\alpha}}$ on the monomial-like basis of $\mathcal{P}_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}^{n,k}$; that is, row j of $\boldsymbol{G}$ equals $\mathrm{ev}_{\boldsymbol{\alpha}}(x^j)$ if $j \notin H$, while row h_i equals $\mathrm{ev}_{\boldsymbol{\alpha}}(x^{h_i} + \eta_i x^{k-1+t_i})$. Recall that $\mathcal{C}^{n,k}(\boldsymbol{\alpha},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})$ is MDS if and only if any k columns of $\boldsymbol{G}$ are linearly independent.

Theorem 1: Let $s_0,\ldots,s_\ell \in \mathbb{Z}_{\ge 0}$ such that $\mathbb{F}_{s_0} \subsetneq \mathbb{F}_{s_1} \subsetneq \cdots \subsetneq \mathbb{F}_{s_\ell} = \mathbb{F}_q$ is a chain of subfields. Let $k < n \le s_0$ and $\alpha_1,\ldots,\alpha_n \in \mathbb{F}_{s_0}$ be distinct, and let $\boldsymbol{t}$, $\boldsymbol{h}$, and $\boldsymbol{\eta}$ be chosen as in Section II-A and such that $\eta_i \in \mathbb{F}_{s_i} \setminus \mathbb{F}_{s_{i-1}}$ for $i = 1,\ldots,\ell$. Then $\mathcal{C}^{n,k}(\boldsymbol{\alpha},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})$ is MDS.

Proof: We will prove that any $k \times k$ sub-matrix of $\boldsymbol{G}$ is invertible, where $\boldsymbol{G}$ is the generator matrix defined above. Consider an arbitrary such sub-matrix $\hat{\boldsymbol{G}}$. Note that $\det \hat{\boldsymbol{G}}$ will equal a sum of terms of the form $\prod_{i \notin H} \alpha_{\sigma(i)}^i \prod_{j=1}^\ell (\alpha_{\sigma(h_j)}^{h_j} + \eta_j \alpha_{\sigma(h_j)}^{k-1+t_j})$ ranging over all k-permutations σ. In particular, we can write $\det \hat{\boldsymbol{G}} = \eta_\ell u_\ell + v_\ell$ where $u_\ell, v_\ell \in \mathbb{F}_{s_0}[\eta_1,\ldots,\eta_{\ell-1}] \subseteq \mathbb{F}_{s_{\ell-1}}$ and both of total degree at most 1 in the $\eta_1,\ldots,\eta_{\ell-1}$. Since $\eta_\ell \notin \mathbb{F}_{s_{\ell-1}}$ then $\det \hat{\boldsymbol{G}} = 0$ only if $u_\ell = v_\ell = 0$. We can continue similarly and write both u_ℓ and v_ℓ as linear expressions in $\eta_{\ell-1}$ over $\mathbb{F}_{s_0}[\eta_1,\ldots,\eta_{\ell-2}]$ and conclude that their coefficients all needs to be identically zero for $u_\ell = v_\ell = 0$. Continuing with the remaining η_i, we finally conclude that $\det \hat{\boldsymbol{G}} = 0$ is only possible if a set of linear expressions of the form $\eta_1 u_1 + v_1$ with $u_1, v_1 \in \mathbb{F}_{s_0}$ are all identically 0 – which none of them can be. Thus $\hat{\boldsymbol{G}}$ is invertible, and since $\hat{\boldsymbol{G}}$ was chosen arbitrarily, this finishes the proof. ∎

Note that this construction produces quite short codes: if we use ℓ twists, then the field size q has $q \ge n^{2^\ell}$, where n is the length.

C. Decoding by brute-forcing the twists

A simple decoding strategy for $\mathcal{C} = \mathcal{C}^{n,k}(\boldsymbol{\alpha},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})$ with ℓ twists is to guess ℓ coefficients $g_1,\ldots,g_\ell \in \mathbb{F}_q$ and then

decode $\boldsymbol{r} - \mathrm{ev}_{\boldsymbol{\alpha}}(\sum_{i=1}^\ell g_i \eta_i X^{t_i+k-1})$ as if it is a codeword in the $[n, k]$ RS code with evaluation points $\boldsymbol{\alpha}$. This will succeed when $g_i = f_{h_i}$ for $i = 1,\ldots,\ell$, where $\mathrm{ev}_{\boldsymbol{\alpha}}(f)$ is the sent codeword and $f \in \mathcal{P}_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}^{n,k}$. This requires $q^\ell \ge n^{\ell 2^\ell}$ rounds of RS decoding to succeed. Some of these rounds might output purported message polynomials $\hat{f}_0 + \ldots + \hat{f}_{k-1} x^{k-1}$ for which $g_i \ne \hat{f}_{h_i}$: these will not correspond to close codewords in the twisted RS code and should be sifted away.

This will be a τ-error correcting decoder for $\mathcal{C}$ when using a τ-error correcting RS decoder – even if the minimum distance of the twisted RS code is much lower than $n - k + 1$. Of course, in spite of the many decoding attempts, the usual bounds apply to the number of successful decoded words (after sifting away spurious RS decoding successes): if $\mathcal{C}$ is MDS and $\tau = \lfloor \frac{n-k}{2} \rfloor$, then there can be at most 1 successful decoding. Similarly, if we use an RS list-decoder, e.g. the Guruswami–Sudan algorithm [13], then the total output list size will be bounded by the Johnson bound [14] or the stronger Cassuto–Bruck bound [15].

The complexity will be q^ℓ times the cost of the RS decoder. The current best complexity for half-the-minimum distance RS decoding is $O(n \log^2 n \log\log n)$ operations in $\mathbb{F}_q$ [16], while list-decoding up to the Johnson radius using the Guruswami–Sudan algorithm has a Las Vegas randomized algorithm in $O(m^4 n (\log^2(mn) + \log(q)) \log\log(mn))$ operations in $\mathbb{F}_q$ [17], [18], where m is the "list size" parameter of the decoder. In either case, the twisted RS decoder then has a complexity of $\tilde{O}(n^{\ell 2^\ell+1} 4^\ell)$ bit operations, ignoring $\ell \log(n)$-factors, considering m a constant, and assuming $q \in O(n^{2^\ell})$. m can be considered a constant if one takes $\tau = (1-\epsilon)J_{n,k}$ for some constant $\epsilon < 1$, where $J_{n,k} = n - \sqrt{n(k-1)}$ is the Johnson radius.

Hence, decoding is feasible only for a very small number of twists, e.g., $\ell = 1, 2$, and finding more efficient algorithms is an open problem.

III. Structural Properties

A. Duals

Twisted RS codes as defined in Definition 1 do not generally seem to be closed under duality; however, if we choose evaluation points which form a multiplicative group, then they are:

Theorem 2: Let $\alpha_1,\ldots,\alpha_n$ be a multiplicative subgroup of $\mathbb{F}_q^*$ and let $\mathcal{C}^{n,k}(\boldsymbol{\alpha},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})$ be some twisted RS code with $\boldsymbol{\alpha} = [\alpha_1,\ldots,\alpha_n]$. Then $\mathcal{C}^{n,k}(\boldsymbol{\alpha},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})^\perp$ equals $\mathcal{C}^{n,n-k}(\boldsymbol{\alpha}, k - \boldsymbol{h}, n - k - \boldsymbol{t}, -\boldsymbol{\eta})$ up to column multipliers.

Proof: Let $\boldsymbol{J}$ be the matrix with 1's on the anti-diagonal and zeroes elsewhere of suitable size. Left-multiplying by $\boldsymbol{J}$ reverses rows while right-multiplying reverses columns. We denote by $\boldsymbol{V}$ the $n \times n$ Vandermonde matrix over $\boldsymbol{\alpha}$, i.e.

$$\boldsymbol{V} := [\alpha_i^{j-1}]_{\substack{i=1,\ldots,n \\ j=1,\ldots,k}} .$$

Since the entries of $\boldsymbol{\alpha}$ form a multiplicative group, we have $\alpha_i^n = 1$ for all i and by [19], we obtain

$$(\boldsymbol{V}^{\mathrm{T}})^{-1} = \boldsymbol{J} \cdot \boldsymbol{V} \cdot \mathrm{diag}(\boldsymbol{\alpha}/n)$$

Similar to Section II-A, a generator matrix of $\mathcal{C}^{n,k}(\boldsymbol{\alpha},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})$ is given by $\boldsymbol{G} = [\boldsymbol{I} \mid \boldsymbol{L}] \cdot \boldsymbol{V}$, where

$$\boldsymbol{L}_{ij} = \begin{cases} \eta_\mu, & \text{if } (i,j) = (h_\mu + 1, t_\mu) \\ 0, & \text{else.} \end{cases}$$

We claim that a parity check matrix for $\mathcal{C}^{n,k}(\boldsymbol{\alpha}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$ is:

$$\boldsymbol{H} = [\boldsymbol{I} \mid -\boldsymbol{J}\boldsymbol{L}^{\mathrm{T}}\boldsymbol{J}] \cdot \boldsymbol{V} \cdot \mathrm{diag}(\boldsymbol{\alpha}/n) \ .$$

$\boldsymbol{H}$ has rank $n-k$ so left is to show $\boldsymbol{G} \cdot \boldsymbol{H}^{\mathrm{T}} = \boldsymbol{0}$. Note that

$$\boldsymbol{H} = \boldsymbol{J}[-\boldsymbol{L}^{\mathrm{T}} \mid \boldsymbol{I}]\boldsymbol{J}\boldsymbol{V}\,\mathrm{diag}(\boldsymbol{\alpha}/n) = \boldsymbol{J}[-\boldsymbol{L}^{\mathrm{T}} \mid \boldsymbol{I}](\boldsymbol{V}^{-1})^{\mathrm{T}} \ .$$

Therefore, $\boldsymbol{G} \cdot \boldsymbol{H}^{\mathrm{T}} = [\boldsymbol{I} \mid \boldsymbol{L}] \begin{bmatrix} -\boldsymbol{L} \\ \boldsymbol{I} \end{bmatrix} \boldsymbol{J}^{\mathrm{T}} = \boldsymbol{0}$ and the entries of $-\boldsymbol{J}\boldsymbol{L}^{\mathrm{T}}\boldsymbol{J}$ are of the form

$$(-\boldsymbol{J}\boldsymbol{L}^{\mathrm{T}}\boldsymbol{J})[i,j] = \begin{cases} -\eta_\mu, & (i,j) = (n-k-t_\mu+1, k-h_\mu) \\ 0, & \text{else.} \end{cases}$$

In other words, a twist $x^{h_\mu} + \eta_\mu x^{k-1+t_\mu}$ becomes the twist $x^{n-k-t_\mu} + (-\eta_\mu)x^{(n-k-1)+(k-h_\mu)}$ in the dual code. This proves the claim. ∎
Note that Theorem 2 implies that the dual of a $(*)$-twisted code from [1] is equivalent to a $(*)$-twisted code as long as 0 is not a coordinate of $\boldsymbol{\alpha}$.

B. Schur Squares

There has been a rising interest in the *Schur product* of codes both as an independent object of study, but also due to its occurrence in applications of codes, see e.g. [20], [21] and references therein. In particular, it is key in the structural attacks on the McEliece cryptosystem using certain Goppa codes or other RS-like codes [10].

Definition 2: The *Schur product*, or *component-wise* product, of two vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$ is

$$\boldsymbol{x} \star \boldsymbol{y} := [x_1 \cdot y_1, \ldots, x_n \cdot y_n] \ .$$

The Schur product of two linear codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^n$ is the set

$$\mathcal{C}_1 \star \mathcal{C}_2 := \langle \boldsymbol{c}_1 \star \boldsymbol{c}_2 \mid \boldsymbol{c}_1 \in \mathcal{C}_1, \boldsymbol{c}_2 \in \mathcal{C}_2 \rangle_{\mathbb{F}_q} \ .$$

We write $\mathcal{C}^2 := \mathcal{C} \star \mathcal{C}$ for the Schur square code.

It is easy to see that for an $[n,k]$ code $\mathcal{C}$, then $\dim \mathcal{C}^2 \leq \min\{n, \frac{1}{2}k(k-1)\}$. Furthermore, if $\mathcal{C}$ is MDS then $\dim \mathcal{C}^2 \geq \min\{2k-1, n\}$ [21, p.31]. GRS codes attain this lower bound with equality.

Since twisted RS codes are obtained by evaluating specific polynomials, we show below how to obtain a lower bound for the dimension of its Schur square. For a given evaluation vector $\boldsymbol{\alpha}$, we denote for a polynomial $f \in \mathbb{F}_q[X]$ by $\overline{f}$ the polynomial remainder of f modulo $\prod_{i=1}^n (X - \alpha_i)$. Then we obtain the following:

Theorem 3: Let $\overline{D} = \{\deg(\overline{f \cdot g}) \mid f, g \in \mathcal{P}_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}^{n,k}\}$. Then $\dim \mathcal{C}^{n,k}(\boldsymbol{\alpha}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})^2 \geq \#\overline{D}$.

Proof: First of all note that $\mathrm{ev}_{\boldsymbol{\alpha}}(f) = \mathrm{ev}_{\boldsymbol{\alpha}}(\overline{f})$, since the evaluation map $\mathrm{ev}_{\boldsymbol{\alpha}}(\cdot)$ vanishes on any multiple of $\prod_{i=1}^n (X - \alpha_i)$. Further, the evaluation map $\mathrm{ev}_{\boldsymbol{\alpha}}(\cdot)$ is an injective homomorphism on $\mathbb{F}_q[X]_{<n}$, the space of polynomials of degree at most $n-1$. This implies that

$$\dim \mathcal{C}^{n,k}(\boldsymbol{\alpha}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})^2 = \dim\langle \overline{f \cdot g} \mid f, g \in \mathcal{P}_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}^{n,k} \rangle \geq \#\overline{D}.$$

∎

Especially if the evaluation vector consists of elements of a multiplicative subgroup of $\mathbb{F}_q^*$, the bound in the theorem is easy to compute, since in that case $\prod_{i=1}^n (X - \alpha_i) = X^n - 1$.

Alternatively, the bound implies the following simpler formulation for which no remainders need be computed:

Corollary 4: Let $D = \{\deg(f \cdot g) \mid f, g \in \mathcal{P}_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}^{n,k}\}$. Then,

$$\dim \mathcal{C}^{n,k}(\boldsymbol{\alpha}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})^2 \geq \#\{d \in D \mid d < n\}.$$

Proof: This follows from $\{d \in D \mid d < n\} \subset \overline{D}$. ∎
This corollary is usually easy to apply: let S be the degrees occurring in the usual monomial-like basis of $\mathcal{P}_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}^{n,k}$, i.e.:

$$S = (\{0, \ldots, k-1\} \setminus \{h_i\}_{i=1,\ldots,\ell}) \cup \{t_i + k - 1\}_{i=1,\ldots,\ell}.$$

Then $D = \{d_1 + d_2 \mid d_1, d_2 \in S\} \cap \{0, \ldots, n-1\}$.

C. Separation from GRS codes

Consider a twisted RS code $\mathcal{C}$. Since twisted RS codes are close kin to GRS codes, one can consider the question of finding GRS codes $\mathcal{D}_{\mathrm{INN}}, \mathcal{D}_{\mathrm{OUT}}$ such that

$$\mathcal{D}_{\mathrm{INN}} \subset \mathcal{C} \subset \mathcal{D}_{\mathrm{OUT}} \ ,$$

while maximising $\dim \mathcal{D}_{\mathrm{INN}}$ and minimising $\dim \mathcal{D}_{\mathrm{OUT}}$, i.e. the "separation" of $\mathcal{C}$ from GRS codes. Note that $\mathcal{C} \subset \mathcal{D}_{\mathrm{OUT}} \iff (\mathcal{D}_{\mathrm{OUT}})^\perp \subset \mathcal{C}^\perp$ and that $(\mathcal{D}_{\mathrm{OUT}})^\perp$ is a GRS code itself where we now try to maximise $\dim(\mathcal{D}_{\mathrm{OUT}})^\perp$. When applying the codes to cryptography, we will motivate further why we consider these questions.

The following three statements separate any code $\mathcal{C}$ from GRS codes from above and below based entirely on the dimension of $\mathcal{C}^2$. Since we saw in the preceding section that many twisted RS codes have large Schur square, this provides separation from GRS codes.

Lemma 5: Let $\mathcal{C}^{n,k}(\boldsymbol{\alpha}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$ be a twisted RS code. Then $\mathcal{C}^{n,k}(\boldsymbol{\alpha}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$ contains an RS code of dimension $\min_i\{h_i\}$ and is contained in an RS code of dimension $k + \max_i t_i$.

Proof: This follows from the observations that

$$\{x^j \mid 0 \leq j \leq \min_i\{h_i\} - 1\} \subset \mathcal{P}_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}^{n,k} \subset$$
$$\{x^j \mid 0 \leq j \leq k - 1 + \max_i\{t_i\}\} \ .$$

∎

The description in the preceding section on the Schur square $\dim \mathcal{C}^2$ of a twisted RS code $\mathcal{C}$ gives a way to prove $\mathcal{C}$ is non-GRS: if $\dim \mathcal{C}^2 > 2k-1$, or if $\dim(\mathcal{C}^\perp)^2 > 2(n-k)-1$, then it must be non-GRS. This can be strengthened to bound the dimension of the smallest GRS code which contains $\mathcal{C}$ or $\mathcal{C}^\perp$ supplementing the observation from Lemma 5.

Proposition 6: Let $\mathcal{C}$ be an $[n,k]$ code with $k < n/2$ and such that $\dim \mathcal{C}^2 = 2k - 1 + \delta$ for $\delta > 0$. Then if $\mathcal{D}_{\mathrm{OUT}}$ is a GRS code with $\mathcal{C} \subseteq \mathcal{D}_{\mathrm{OUT}}$, then $\dim \mathcal{D}_{\mathrm{OUT}} \geq k + \delta/2$.

Proof: Since $\mathcal{C}^2 \subseteq \mathcal{D}_{\mathrm{OUT}}^2$ then $\dim(\mathcal{D}_{\mathrm{OUT}}^2) \geq 2k - 1 + \delta$ i.e. $\dim(\mathcal{D}_{\mathrm{OUT}}) \geq k + \delta/2$. ∎

Proposition 7: Let $\mathcal{C}$ be an $[n,k]$ code with $k < n/2$ and such that $\dim \mathcal{C}^2 = 2k - 1 + \delta$ for $\delta > 0$. If $\mathcal{D}_{\mathrm{INN}}$ is a GRS code with $\mathcal{D}_{\mathrm{INN}} \subseteq \mathcal{C}$, then

$$\dim \mathcal{D}_{\mathrm{INN}} \leq \sqrt{\left(k - \tfrac{5}{2}\right)^2 - 2\delta} + \tfrac{5}{2} \ .$$

Proof: Let $K = \dim \mathcal{D}_{\mathrm{INN}}$. Pick a basis $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_K$ of $\mathcal{D}_{\mathrm{INN}}$ and extend this basis with $k - K$ vectors $\boldsymbol{c}_{K+1}, \ldots, \boldsymbol{c}_k$ to form a basis for $\mathcal{C}$. Then $\mathcal{C}^2$ must be spanned by a basis of $\mathcal{D}_{\mathrm{INN}}^2$ together with all Schur products $\boldsymbol{c}_i \star \boldsymbol{c}_j$ with $1 \leq i \leq K < j \leq k$, together with all Schur products $\boldsymbol{c}_i \star \boldsymbol{c}_j$ with $K < i, j \leq k$. In total

$$\dim \mathcal{C}^2 \leq (2K - 1) + K(k - K) + \tfrac{1}{2}(k - K)(k - K - 1) \ .$$

This implies $\left(K - \tfrac{5}{2}\right)^2 \leq \left(k - \tfrac{5}{2}\right)^2 - 2\delta$. ∎

Remark 8: A simpler question than separation from GRS codes is simply inequivalence to GRS codes. We considered this question for single-twisted RS codes in [1], using different tools; unfortunately the proof of [1, Theorem 18] contains a

mistake and its statement is not true in general. However, the Schur square arguments above show that still most twisted RS codes are not GRS codes.

IV. APPLIED TO THE MCELIECE CRYPTOSYSTEM

In this section, we present a subfamily of twisted RS codes which provably resist the known structural attacks on RS-like codes by Sidelnikov–Shestakov [7] and Couvreur et al. [10]. Wieschebrink's attack [8], [9] is inefficient when applied to the code itself, and not obviously efficient on the dual code.

Definition 3: Choose positive integers $k < n \leq q_0$ with q_0 a prime power and $2\sqrt{n} + 4 < k \leq \frac{n}{2}$. Furthermore, choose $\ell \in \mathbb{Z}_{\geq 0}$ such that $\frac{n+1}{k-\sqrt{n}} - 2 < \ell < \min\{k+1; \frac{2n}{k} - 2; \sqrt{n} - 2\}$. Let $r := \lceil \frac{n+1}{\ell+2} \rceil$, let $q = q_0^{2^\ell}$, and for $i = 1, \ldots, \ell$, let

$$t_i = (i+1)r - k \quad \text{and} \quad h_i = r - 1 + i.$$

Then the family of codes $\mathcal{F}_\ell^{n,k}$ is the set of all codes $\mathcal{C}^{n,k}(\boldsymbol{\alpha}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$, where $\boldsymbol{\alpha} \in \mathbb{F}_{q_0}^n$ with distinct elements, and where $\eta_i \in \mathbb{F}_{q_0^{2^i}} \setminus \mathbb{F}_{q_0^{2^{i-1}}}$. Further, we let $\tilde{\mathcal{F}}_\ell^{n,k} \subset \mathcal{F}_\ell^{n,k}$ be those codes which furthermore satisfy that $\boldsymbol{\alpha}$ form a multiplicative subgroup of $\mathbb{F}_{q_0}$.

Note that if $n = q_0 - 1$ then $\tilde{\mathcal{F}}_\ell^{n,k} = \mathcal{F}_\ell^{n,k}$, while if $n \nmid (q_0 - 1)$ then $\tilde{\mathcal{F}}_\ell^{n,k} = \emptyset$.

It is technical but easy to show that for any $n > 67$ and any k satisfying the restrictions, then there is always a valid choice for ℓ. For triples (n, k, ℓ) satisfying the restrictions, however, it is not immediate that $\mathcal{F}_\ell^{n,k}$ is well-defined, i.e. $0 < h_i < k$ and $0 < t_i \leq n - k$ for all i. Clearly $h_1 = r > 0$. Then $t_1 = 2r - k > 0$ since $\ell < \frac{2n}{k} - 2 < \frac{2(n+1)}{k} - 2$ i.e. $k < 2\left(\frac{n+1}{\ell+2}\right)$. Then, since $n+1 < (\ell+2)(k-\sqrt{n}) \leq (\ell+2)(k-(\ell+1))$ then $k > \frac{n+1}{\ell+2} + \ell + 1 > r + \ell = h_\ell$. Lastly, $t_\ell \leq n - k$ simplifies to $r \leq \frac{n}{\ell+1}$, but this is true since $\frac{n}{\ell+1} - \frac{n+1}{\ell+2} = \frac{n-(\ell+1)}{(\ell+1)(\ell+2)}$ which is greater than 1 since $n > (\ell+2)^2$.

By Theorem 1 all codes in $\mathcal{F}_\ell^{n,k}$ are MDS. It is clear that for a fixed rate $R = k/n$, the lower bound for ℓ in Theorem 10 converges to $\frac{1}{R} - 1$ for $n \to \infty$, so for large enough n, it suffices to choose $\ell = \lfloor \frac{1}{R} \rfloor$.

Remark 9: If one desires a code rate greater than $\frac{1}{2}$, one can use the dual of a code in $\tilde{\mathcal{F}}_\ell^{n,k}$, for values of n for which $\tilde{\mathcal{F}}_\ell^{n,k}$ is not empty. These will be twisted RS codes with ℓ twists, by Theorem 2, and will resist the attacks since the primal codes do.

A. Resistance to Schur Square Distinguishing

Couvreur et. al [10] built a structural attack on McEliece with RS codes using the fact that the square code of a k-dimensional RS code $\mathcal{D}$ has abnormally low dimension when $k < n/2$: $\dim(\mathcal{D}^2) = \min\{2k-1, n\}$. By comparison, a random linear code achieves $\dim(\mathcal{C}^2) = \min\{\frac{1}{2}k(k+1), n\}$ with high probability [22]. In this section we show that the codes of $\mathcal{F}_\ell^{n,k}$ are impervious to this attack.

Theorem 10: Let n, k, ℓ be as in Definition 3, and let $\mathcal{C} \in \mathcal{F}_\ell^{n,k}$. Then $\dim \mathcal{C}^2 = n$ and $\dim((\mathcal{C}^\perp)^2) = n$.

Proof: Let $r, \boldsymbol{t}, \boldsymbol{h}$ be as in Definition 3. We will use Corollary 4, so let $D = \{\deg(f \cdot g) \mid f, g \in \mathcal{P}_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}^{n,k}\}$. Since $x^0, \ldots, x^{r-1} \in \mathcal{P}_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}^{n,k}$ then $0, \ldots, 2r-2 \in D$. For each i, there is a polynomial of degree $t_i + k - 1$ in $\mathcal{P}_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}^{n,k}$, so also $(i+1)r - 1, (i+1)r, \ldots, (i+1)r + r - 2 \in D$. Summing up we have all $0, 1, \ldots, (\ell+2)r - 2 \in D$. By definition of r, we have $(\ell+2)r - 2 \geq n - 1$, so Corollary 4 implies the claim for $\mathcal{C}$. The dual code has Schur square dimension n since it is MDS and has dimension $> n/2$ [21, p.31]. ∎

Remark 11: It is not hard to come up with more twisted RS codes of Schur square dimension n. The crucial ingredient of the proof of Theorem 10 is that $x^0, \ldots, x^{r-1} \in \mathcal{P}_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}^{n,k}$. As long as all hooks h_i are at least r, then the argument will work. The reason for setting h_1 as small as possible is discussed in the following section, but the remaining h_i could be chosen as any subset of $\{r+1, \ldots, k-1\}$. Further, whenever $(\ell+2)r$ is much bigger than $n-1$, the choice of t_i can be perturbed in many ways; this will e.g. always be the case if ℓ is chosen above the minimal possible value. Lastly, we can allow independent permutations of the t_i and the η_i.

B. Resistance to Sidelnikov–Shestakov & Wieschebrink attack

The Sidelnikov–Shestakov (SiS) attack [7] completely breaks McEliece with GRS codes; we use the description from [9]. Let $[\boldsymbol{I} \mid \boldsymbol{A}]$ be the systematic generator matrix of a GRS code with evaluation points $\boldsymbol{\alpha} \in \mathbb{F}_q^n$ and column multipliers $\boldsymbol{v} \in (\mathbb{F}_q^\star)^n$. Using the automorphisms of a GRS code, the attacker can assume $\alpha_1 = 0$ and $\alpha_1 = 1$. Row i of the matrix is the evaluation of the polynomial

$$f_i = c_i \prod_{\mu=1, \mu\neq i}^k (x - \alpha_\mu),$$

where c_i is a suitably chosen constant in $\mathbb{F}_q$. It is well known [23], [24] that the matrix $\boldsymbol{A}$ is a Cauchy matrix exactly when the code is GRS. This means that for $d_j = \prod_{\nu=1}^k (\alpha_j - \alpha_\nu)$ for $j = k+1, \ldots, n$, we have the simple expression

$$A_{ij} = \frac{c_i \cdot d_j}{\alpha_j - \alpha_i}. \tag{1}$$

Due to this compact formula, after guessing the values $c_1, c_2 \in \mathbb{F}_q$, the remaining secret values $\alpha_3, \ldots, \alpha_n$ and $v_1, \ldots, v_n$ can be computed by solving simple linear equations.

Since Theorem 10 shows that the codes of $\mathcal{F}_\ell^{n,k}$ have large Schur square, then none of these codes can be GRS. Therefore, a systematic generator matrix for these codes will have $[\boldsymbol{I} \mid \boldsymbol{A}]$ where $\boldsymbol{A}$ will *not* be Cauchy. Since the SiS attack rested on the simple Cauchy structure, it will not work for these codes.

Wieschebrink [8] generalised the SiS to apply for subcodes of RS codes of small codimension. Assume that we have given a $k \times n$ generator matrix $[\boldsymbol{I} \mid \boldsymbol{A}]$ of a subcode of an $(n, k + \delta)$ RS code. Then, the i-th row of the matrix $\boldsymbol{A}$ is obtained from a polynomial

$$f_i = c_i(x) \prod_{\mu=1, \mu\neq i}^k (x - \alpha_\mu),$$

where $c_i(x) \in \mathbb{F}_q[X]$ is a polynomial of degree $\deg c_i(x) \leq \delta$. One now needs to guess the polynomials $c_1(x)$ and $c_2(x)$ instead of only scalars, which will succeed after at most $\approx q^{2\delta}$ iterations. For large enough values of δ, this becomes infeasible.

For $\mathcal{C} \in \mathcal{F}_\ell^{n,k}$, since $\dim \mathcal{C}^2 = n$, then Proposition 6 implies that any GRS code $\mathcal{D}_{\text{OUT}}$ with $\mathcal{C} \subset \mathcal{D}_{\text{OUT}}$ must have $\dim \mathcal{D}_{\text{OUT}} \geq k + (n - 2k + 1)/2$. This very quickly makes Wieschebrink's attack infeasible for $\mathcal{C}$.

Wieschebrink's attack can also be carried out on the dual code, so that one seeks a GRS code $\mathcal{D}_{\text{INN}}^\perp$ such that $\mathcal{C}^\perp \subset \mathcal{D}_{\text{INN}}^\perp$, i.e. $\mathcal{D}_{\text{INN}} \subset \mathcal{C}$. If $\dim \mathcal{D}_{\text{INN}}$ is close to $\dim \mathcal{C}$, this is a bad sign: it may reveal structural information on $\mathcal{C}$ or may drastically reduce the cost of brute-force decoding the encrypted message. We are at this point unable to categorically refute this attack. Proposition 7 provides only a small separation between $\mathcal{D}_{\text{INN}}$ and $\mathcal{C}$, and it is not hard to realise that this separation can never be greater than the

number of twists ℓ, which we wish to keep fairly small for decoding purposes. As per Lemma 5, the obvious GRS code contained in $\mathcal{C}$ is the one with the same evaluation points $\boldsymbol{\alpha}$ and dimension $\min\{h_1\} = r$. If $\mathcal{C}$ contains a larger GRS code, it seems it would have to be a surprising, or spurious, code with other evaluation points and column multipliers.

If we choose n such that $\tilde{\mathcal{F}}_\ell^{n,k}$ is non-empty and $\mathcal{C} \in \tilde{\mathcal{F}}_\ell^{n,k}$, then $\mathcal{C}^\perp$ is itself a twisted RS code by Section II-C. Now the obvious GRS code $\mathcal{D}_{\text{INN}}$ such that $\mathcal{C}^\perp \subset \mathcal{D}_{\text{INN}}^\perp$ is the one having the same evaluation points and dimension $\max\{\tilde{t}_i + n - k\} = n - r$, where $\tilde{\boldsymbol{t}} = k - \boldsymbol{h}$ is the twist vector of $\mathcal{C}^\perp$. Perhaps this strengthens the belief that it is not likely that $\mathcal{C}$ contains another, surprisingly large GRS code.

Summarising, assuming that $\mathcal{C} \in \mathcal{F}_\ell^{n,k}$ contains no surprisingly large GRS code, then Wieschebrink's attack on $\mathcal{C}$ or $\mathcal{C}^\perp$ will have work factor roughly $q^{2\delta}$ if

$$k \in [r + \delta, \tfrac{n+1}{2} - \delta] \approx [\tfrac{n}{\ell+1} - \delta, \tfrac{n}{2} - \delta] .$$

C. Example Code Parameters

We consider the following example parameters: Let $(n,k) = (255, 117)$, $\ell = 1$, $q_0 = 2^8$ and pick a code over $\mathbb{F}_q, q = 2^{16}$, with these parameters as in Definition 3. The number of such codes is upper-bounded by the number of permutations on an n-dimensional set (here, $n! > 2^{2038}$) times the number of choices for η_1 ($= q - \sqrt{q} \approx 2^{16}$). The actual number of inequivalent codes is presumably much smaller, but seems to suffice for avoiding exhaustive search attack. Twisted RS codes also seem to have much smaller automorphism groups than RS codes, though this is still to be investigated further. Under the assumptions of the previous subsection, the work factor of Wieschebrink's attack is 2^{336}.

As for generic decoding attacks, we consider classical information set decoding [3], [4][2] with work factor $W_{\text{I}} = \binom{n}{k}/\binom{n-\tau}{k}k^3 \log_2(q)^2$, where τ is the number of errors inserted by the sender. Since the example codes can correct up to $\tau_{\text{unique}} = 69$ errors uniquely and $\tau_{\text{list}} = 83$ using a list decoder, we obtain the following work factors for unique and list decoding, respectively:

$$W_{\text{I,unique}} \geq 2^{105}, \quad W_{\text{I,list}} \geq 2^{126}.$$

In both cases, the key size is

$$K_{\text{sys}} = k(n-k)\log_2(q)/8192 = 31.5\,\text{KB},$$

using a systematic generator matrix for the public key.[3]

The security level of the two variants above is $\geq 2^{100}$ respectively $\approx 2^{128}$. We compare the key size to the originally proposed parameters based on binary Goppa codes of similar security level (both using systematic key):

Security level 2^{100} [11]: $(n,k) = (2048, 1608)$, $\tau = 40$,

$$K = 86.4\,\text{KB}$$

Security level 2^{128} [12]: $(n,k) = (3262, 2482)$, $\tau = 66$,

$$K = 236.3\,\text{KB}$$

In this example, using twisted RS codes reduce the key size by a factor 2.7 and 7.4 at security levels $\approx 2^{100}$ respectively $\approx 2^{128}$.

---

[2]The improvements for non-binary information-set decoding considered in [5] seem to be not more efficient since, unlike the original algorithm [3], the cost of an iteration strongly depends on the field size, which is large for our codes: $q = 2^{16}$. However, this should be more carefully studied by e.g. by estimating the number of iterations using a Markov chain simulation as in [5].

[3]Systematic generator matrices might decrease semantic security if they are not carefully used, cf. [6, Section 5.1].

V. CONCLUSION

We have presented a natural generalisation of twisted RS codes, pointed out a large subfamily of MDS codes, and presented a decoder that is feasible for $\ell = 1, 2$ twists. Those codes whose evaluation points form a multiplicative group are closed under duality with explicit duals. We also showed that the Schur square of a twisted RS code is usually large, which shows that they are in a sense "far" from GRS codes, cf. Lemma 5. Furthermore, we identified a subfamily of twisted RS codes that resist the relevant known structural attacks on the McEliece cryptosystem: Sidenlikov–Shestakov [7], Wieschebrink [9] and Schur square-distinguishing [10]. For Wieschebrink's attack on the dual code we could say only that the attack does not apply in an obvious way. We gave example parameters that achieve lower key sizes than the original McEliece cryptosystem for the same security level.

REFERENCES

[1] P. Beelen, S. Puchinger, and J. Rosenkilde né Nielsen, "Twisted Reed-Solomon Codes," in *IEEE ISIT*, 2017.

[2] S. Puchinger, J. Rosenkilde né Nielsen, and J. Sheekey, "Further Generalisations of Twisted Gabidulin Codes," in *WCC*, 2017.

[3] R. J. McEliece, "A Public-Key Cryptosystem Based On Algebraic Coding Theory," *DSN Progress Report*, vol. 42, no. 44, pp. 114–116, 1978.

[4] E. Prange, "The Use of Information Sets in Decoding Cyclic Codes," *IRE Trans. Inf. Theory*, vol. 8, no. 5, pp. 5–9, 1962.

[5] C. Peters, "Information-Set Decoding for Linear Codes over Fq." *PQCrypto*, vol. 2010, pp. 81–94, 2010.

[6] R. Overbeck and N. Sendrier, "Code-Based Cryptography," in *Post-Quantum Cryptography*. Springer, 2009, pp. 95–145.

[7] V. M. Sidelnikov and S. O. Shestakov, "On Insecurity of Cryptosystems Based on Generalized Reed–Solomon Codes," *Discrete Math. Appl.*, vol. 2, no. 4, pp. 439–444, 1992.

[8] C. Wieschebrink, "An Attack on a Modified Niederreiter Encryption Scheme," in *PKC*, vol. 3958. Springer, 2006, pp. 14–26.

[9] ——, "Cryptanalysis of the Niederreiter Public Key Scheme Based on GRS Subcodes," in *PQCrypto*. Springer, 2010, pp. 61–72.

[10] A. Couvreur, P. Gaborit, V. Gauthier-Umaña, A. Otmani, and J.-P. Tillich, "Distinguisher-based Attacks on Public-key Cryptosystems Using Reed–Solomon Codes," *Des. Codes Cryptogr.*, vol. 73, no. 2, pp. 641–666, 2014.

[11] A. Canteaut and N. Sendrier, "Cryptanalysis of the Original McEliece Cryptosystem," in *Asiacrypt*, vol. 1514. Springer, 1998, pp. 187–199.

[12] M. Barbier and P. S. L. M. Barreto, "Key Reduction of McEliece's Cryptosystem Using List Decoding," in *IEEE ISIT*, July 2011.

[13] V. Guruswami and M. Sudan, "Improved Decoding of Reed–Solomon Codes and Algebraic-Geometric Codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1757–1767, 1999.

[14] S. M. Johnson, "A New Upper Bound for Error-Correcting Codes," *IEEE Trans. Inf. Theory*, vol. 46, pp. 203–207, 1962.

[15] Y. Cassuto and J. Bruck, "A Combinatorial Bound on the List Size," California Institute of Technology, Tech. Rep., 2004.

[16] J. Justesen, "On the complexity of decoding Reed-Solomon codes (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 22, no. 2, pp. 237–238, Mar. 1976.

[17] M. Chowdhury, C.-P. Jeannerod, V. Neiger, E. Schost, and G. Villard, "Faster Algorithms for Multivariate Interpolation With Multiplicities and Simultaneous Polynomial Approximations," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2370–2387, May 2015.

[18] V. Neiger, J. Rosenkilde, and E. Schost, "Fast Computation of the Roots of Polynomials Over the Ring of Power Series," in *ISSAC*, 2017.

[19] H. Althaus and R. Leake, "Inverse of a Finite-Field Vandermonde Matrix (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 15, no. 1, pp. 173–173, 1969.

[20] R. Cramer, I. B. Damgård, and J. B. Nielsen, *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press, 2015.

[21] H. Randriambololona, "On Products and Powers of Linear Codes Under Componentwise Multiplication," in *AGCT*, 2015.

[22] I. Cascudo, R. Cramer, D. Mirandola, and G. Zémor, "Squares of Random Linear Codes," *IEEE Transactions on Information Theory*, vol. 61, no. 3, pp. 1159–1173, Mar. 2015.

[23] R. M. Roth and G. Seroussi, "On Generator Matrices of MDS Codes (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 31, no. 6, pp. 826–830, 1985.

[24] R. M. Roth and A. Lempel, "On MDS Codes via Cauchy Matrices," *IEEE Trans. Inf. Theory*, vol. 35, no. 6, pp. 1314–1319, 1989.