mathematics

MDPI

Article

Twisted Hermitian Codes

Austin Allen [1], Keller Blackwell [2], Olivia Fiol [3], Rutuja Kshirsagar [4], Bethany Matsick [5], Gretchen L. Matthews [4,*] and Zoe Nelson [6]

[1] Department of Mathematical Sciences, Carnegie Mellon University, Pittsburgh, PA 15213, USA; apallen@andrew.cmu.edu
[2] Department of Computer Science, Stanford University, Stanford, CA 94305, USA; kellerb@stanford.edu
[3] Department of Mathematics and Statistics, Vassar College, Poughkeepsie, NY 12604, USA; ofiol@vassar.edu
[4] Department of Mathematics, Virginia Polytechnic Institute & State University (Virginia Tech), Blacksburg, VA 24061, USA; rutujak@vt.edu
[5] Department of Mathematics, Liberty University, Lynchburg, VA 24515, USA; blmatsick@liberty.edu
[6] Department of Mathematics, Oglethorpe University, Atlanta, GA 30319, USA; znelson@oglethorpe.edu
* Correspondence: gmatthews@vt.edu

Abstract: We define a family of codes called twisted Hermitian codes, which are based on Hermitian codes and inspired by the twisted Reed–Solomon codes described by Beelen, Puchinger, and Nielsen. We demonstrate that these new codes can have high-dimensional Schur squares, and we identify a subfamily of twisted Hermitian codes that achieves a Schur square dimension close to that of a random linear code. Twisted Hermitian codes allow one to work over smaller alphabets than those based on Reed–Solomon codes of similar lengths.

Keywords: algebraic geometry code; code-based cryptography; Hermitian code; Hermitian curve; McEliece cryptosystem

JEL Classification: 94B27; 11T71

Citation: Allen, A.; Blackwell, K.; Fiol, O.; Rutuja Kshirsagar; Matsick, B.; Matthews, G.L.; Nelson, Z. Twisted Hermitian Codes. *Mathematics* **2021**, *9*, 40. https://dx.doi.org/10.3390/math9010040

Received: 9 November 2020
Accepted: 22 December 2020
Published: 26 December 2020

1. Introduction

Reed–Solomon and Hermitian codes are algebraic geometry codes based on the projective line and the Hermitian curve, respectively. To define an algebraic geometry code, let X be a smooth, projective, absolutely irreducible curve over a finite field $\mathbb{F}$. Let G and $D := P_1 + \cdots + P_n$ be divisors on X such that $P_1, \ldots, P_n$ are distinct $\mathbb{F}$-rational points and the support of G does not contain any of the P_i. An algebraic geometric code is of the form

$$C(D, G) = \{(f(P_1), f(P_2), \ldots, f(P_n)) : f \in \mathcal{L}(G)\} \subseteq \mathbb{F}^n$$

where $\mathcal{L}(G) = \{f : (f) \geq -G\} \cup \{0\}$ and (f) denotes the divisor of the rational function f on X. In this paper, we will modify this construction for Hermitian codes to yield a new family of codes, called twisted Hermitian codes, with the goal of producing codes which have large Schur squares. Given a finite field $\mathbb{F}$ and a positive integer n, the Schur product of vectors $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}^n$ is

$$\mathbf{x} * \mathbf{y} := (x_1 y_1, \ldots, x_n y_n) \in \mathbb{F}^n.$$

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

$$\mathcal{C}_1 * \mathcal{C}_2 := \langle \mathbf{c_1} * \mathbf{c_2} \mid \mathbf{c_1} \in \mathcal{C}_1, \mathbf{c_2} \in \mathcal{C}_2 \rangle,$$

meaning $\mathcal{C}_1 * \mathcal{C}_2$ is the set of all linear combinations of vectors of the form $\mathbf{c_1} * \mathbf{c_2}$ with coefficients in $\mathbb{F}$ and $\mathbf{c_1} \in \mathcal{C}_1, \mathbf{c_2} \in \mathcal{C}_2$. The Schur square of a linear code $\mathcal{C}$ is $\mathcal{C}^2 := \mathcal{C} * \mathcal{C}$. Schur products were originally used to define error-locating pairs [1] and now

arise in several applications, such as secret sharing [2] and code-based cryptography [3]. A challenge in coding theory is to specify explicit codes with high-dimensional Schur squares.

When either a Reed–Solomon code or a Hermitian code is squared, the result is typically a code of the same type which limits its dimension. To obtain a code of the same dimension whose square is much larger, twisted Reed–Solomon codes were defined by Beelen, Puchinger, and Nielsen [4], drawing upon ideas from the twisted Gabidulin codes of Sheekey [5]. These same ideas serve as inspiration for the recent work [6]. In this paper, we introduce twisted Hermitian codes which have an advantage over twisted Reed–Solomon codes in that codes of similar lengths can be obtained over smaller alphabets. Utilizing smaller alphabets can reduce the computational complexity of the finite field arithmetic. For instance, to obtain a (twisted) Reed–Solomon code of length 4096, one must use an alphabet of size 4096 whereas a (twisted) Hermitian code of the same length only requires an alphabet size of 256; hence, one can work over the field with 256 elements rather than the field of cardinality 4096. Twisted Hermitian codes can have a large Schur square, as demonstrated herein, by making use of field extensions.

The motivation is to explicitly construct codes whose behavior, loosely speaking, mimics that of random codes. While this is interesting in its own right, it is also prompted by the McEliece cryptosystem, which is a code-based cryptosystem introduced by McEliece in 1978 [7]. The public key in the McEliece cryptosystem is an obfuscation of the underlying linear code (chosen by McEliece to be a binary Goppa code), disguised to appear as a random code, meaning one lacking any recognizable structure. The security of the McEliece cryptosystem is derived from the NP-hardness of decoding a random linear code, proven by Berlekamp, McEliece, and Tilborg in 1978 [8]. Though the McEliece cryptosystem remains unbroken to this day (even with quantum algorithms), its reliance on binary Goppa codes results in large key sizes that hinder practical implementation. As a result, many variants of the McEliece cryptosystem have been introduced, with other linear codes (including the algebraic geometry codes [9]) substituted within. Additional structure can lead to a reduction in key size but often at the cost of introducing vulnerabilities that allow an attacker to extract identifying characteristics of the underlying code from the public-key matrix; see, for instance, the recent work by Couvreur, Márquez-Corbella, and Pellikaan on algebraic geometry codes [10] as well as that of Márquez-Corbella, Martínez-Moro and Pellikaan [3]. Once the attacker can identify the underlying code, the fundamental assumption that secures the McEliece cryptosystem is no longer valid. The twisted construction presents a challenge to the attacker in that its square is not readily identifiable due to its large dimension. However, Lavauzelle and Renner recently demonstrated that for many parameter choices, twisted Reed–Solomon codes have a subfield subcode which is vulnerable to attack [11]. We discuss the possibility of such an attack for twisted Hermitian codes, pointing out a few key differences.

This paper is organized as follows. This section concludes with a brief guide to notation. Necessary background is covered in Section 2. In Section 3, we define the twisted Hermitian codes and explore their properties. In Section 4, we consider the McEliece cryptosytem employing certain families of twisted Hermitian codes. Section 4 considers a potential attack by casting the ideas of Lavauzelle and Renner in the Hermitian setting. A conclusion may be found in Section 5.

Notation. Given a vector space V over a field $\mathbb{F}$ and $B := \{v_1, \ldots, v_t\} \subseteq V$, we write $\langle v_1, \ldots, v_t \rangle_{\mathbb{F}} := \left\{ \sum_{i=1}^{t} a_i v_i : a_i \in \mathbb{F} \right\}$ to denote the span of the set B; at times, we write $\langle B \rangle$ and when it is clear from the context, we omit the subscript $\mathbb{F}$ and simply write $\langle v_1, \ldots, v_t \rangle$. The set of all $m \times n$ matrices with entries from a field $\mathbb{F}$ is written as $\mathbb{F}^{m \times n}$, and $I_m \in \mathbb{F}^{m \times m}$ denotes the $m \times m$ identity matrix over $\mathbb{F}$.

The finite field with q elements is denoted by $\mathbb{F}_q$, where q is a power of a prime; $\mathbb{N}$ denotes the set of nonnegative integers; and $\mathbb{Z}^+$ denotes the set of positive integers. An $[n, k, d]$ code $\mathcal{C}$ over $\mathbb{F}_q$ is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$ with $k := \dim_{\mathbb{F}_q} \mathcal{C}$ and minimum distance $d := \min\{wt(c) : c \in \mathcal{C} \setminus \{0\}\}$. Here, $wt(w) = |\{i : w_i \neq 0\}|$ denotes the Hamming

weight of a word $w \in \mathbb{F}_q^n$. Elements of $\mathcal{C}$ are called codewords. An $[n,k,d]$ code is MDS, or maximum distance separable, if and only if $d = n-k+1$. We say that a code is an $[n,k]$ code if its length is n and its dimension is k. A generator matrix for an $[n,k]$ code $\mathcal{C}$ over a field $\mathbb{F}_q$ is any matrix $M \in \mathbb{F}_q^{k\times n}$ whose rows form a basis for $\mathcal{C}$. A generator matrix $M = [I_k \mid A]$ is said to be in systematic form.

2. Preliminaries

We begin this section with a review of algebraic geometry codes and the necessary details on Hermitian codes followed by a discussion of the Schur product. There are a number of excellent references such as [12–15] which provide more comprehensive surveys.

Recall that an algebraic geometry code is of the form $C(D,G)$ as described in Section 1. If $\deg G < n$, then $C(D,G)$ is a $[n, \dim \mathcal{L}(G), \geq n - \deg G]$ code. At times, it will be useful to consider nested codes. If $G \leq G'$, where G' is another divisor on X whose support does not contain any of the P_i, then $C(D,G) \subseteq C(D,G')$. See [16] for more on nested Hermitian codes. In this paper, we restrict our attention to the case where $G = \alpha P$ with $\alpha \in \mathbb{Z}^+$, P is an $\mathbb{F}$-rational point on X, and D is the sum of the remaining $\mathbb{F}$-rational points; such codes are referred to as one-point codes in the literature and will be denoted here by $C(G)$.

Reed–Solomon codes are obtained from the construction above by taking $X = \mathbb{P}^1(\mathbb{F}_q)$, the projective line; $k < n \leq q$; $G = kP$ where P denotes the unique point at infinity on X; and D to be the sum of all other rational points on X. It is well known that $C(kP)$ is an $[n,k,n-k+1]$ code; that is, $C(kP)$ is MDS. Notice that the alphabet size, meaning the cardinality of the field $\mathbb{F}_q$, is at least the length of the Reed–Solomon code; thus, to define a Reed–Solomon code of length n requires that $\mid \mathbb{F}_q \mid \geq n$.

Beyond Reed–Solomon codes, the best understood algebraic geometry codes are Hermitian codes. For a prime power q, let $\mathcal{X}_q$ denote the smooth, projective curve given by $y^q + y = x^{q+1}$ over the finite field $\mathbb{F}_{q^2}$; $\mathcal{X}_q$ is known as the Hermitian curve. The genus of $\mathcal{X}_q$ is $g = \frac{q(q-1)}{2}$, and there are q^3 affine $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}_q$ in the projective plane, meaning points the form $(a:b:1) \in \mathbb{P}^2\left(\mathbb{F}_{q^2}\right)$ with $b^q + b = a^{q+1}$, and a unique point at infinity $P_\infty = (0:1:0)$. Let $n := q^3$ and $P_1, \ldots, P_n$ denote the affine rational points of $\mathcal{X}_q$. Given a vector space V of functions on $\mathcal{X}_q$ which do not have poles at any of the P_i, $1 \leq i \leq n$, a code can be defined by taking the image of the evaluation map

$$\begin{array}{rccc} ev: & V & \to & \mathbb{F}_{q^2}^n \\ & f & \mapsto & (f(P_1), \ldots, f(P_n)). \end{array}$$

For $\alpha \in \mathbb{N}$ with $2g < \alpha < n$, we consider the space of functions

$$\mathcal{L}(\alpha P_\infty) = \langle x^i y^j : i,j \in \mathbb{N}, j \leq q-1, \delta(x^i y^j) \leq \alpha \rangle$$

where $\delta(x^i y^j) := iq + j(q+1)$ is the pole order of $x^i y^j$ at P_∞. The one-point Hermitian code determined by α is the algebraic geometry code $C(\alpha P_\infty) = ev(\mathcal{L}(\alpha P_\infty))$. Henceforth, we use the term Hermitian code to mean one-point Hermitian curve. Notice that $C(\alpha P_\infty)$ is a code of length q^3, dimension at least $\alpha + 1 - g$, with equality achieved when $\alpha \geq 2g+1$, and minimum distance as given in [17].

Schur squares of algebraic geometry codes have been studied in [10,18]. Given a Hermitian code $C(\alpha P_\infty)$,

$$C(\alpha P_\infty)^2 \subseteq C(2\alpha P_\infty),$$

and equality is achieved when $\alpha \geq 2g+1$. In this case, $C(\alpha P_\infty)$ has dimension $\alpha + 1 - g$ and

$$\dim C(\alpha P_\infty)^2 = \dim C(2\alpha P_\infty) = 2\alpha + 1 - g << \binom{(\alpha+1-g)+1}{2}; \quad (1)$$

see also [19] for details. These ideas may be applied to more general algebraic geometry codes, meaning those constructed via evaluation maps analagous to *ev* using curves other than $\mathcal{X}_q$ ([20] (Prop. 2)).

We seek a family of codes whose behavior under the Schur operation is indistinguishable from that of random codes. A guiding principle is the following result obtained by Cascudo, Cramer, Mirandola, and Zémor.

Proposition 1 ([2] (Theorem 2.3))**.** *Let $n : \mathbb{N} \to \mathbb{N}$ be such that $n(k) \geq \binom{k+1}{2}$. Then for some positive real number δ and k large enough,*

$$\Pr\left[\dim \mathcal{C}^2 = \binom{k+1}{2}\right] \geq 1 - 2^{-\delta\left(n(k)-\binom{k+1}{2}\right)} \tag{2}$$

where $\mathcal{C}$ is chosen uniformly at random from the family of all $[n(k), k]$ codes over $\mathbb{F}_q$ whose generator matrices are in systematic form.

In keeping with Proposition 1, given a code $\mathcal{C}$ of dimension k, it is desirable for $\mathcal{C}^2$ to have dimension close to $\binom{k+1}{2}$ or quadratic in k. This is in contrast to that seen in (1) where the dimension is linear in k. This serves as motivation to consider twisted Hermitian codes which are defined in the next section.

3. Twisted Hermitian Codes

In [4], Beelen, Puchinger, and Rosenkilde introduce a new code construction based on generalized Reed–Solomon codes; the resulting codes can have Schur squares with larger dimensions than the Schur squares of the generalized Reed–Solomon codes themselves. The study of these new codes is carried on in [21] by Beelen, Bossert, Puchinger, and Rosenkilde. In this section, we adapt the construction to Hermitian codes, determine their basic properties, and apply new tools to address subtleties that arise in considering their squares. Decoding is also discussed.

3.1. Properties of Twisted Hermitian Codes

We begin by defining the twisted Hermitian codes. To do so, let

$$B(\alpha P_\infty) := \left\{x^i y^j : i, j \in \mathbb{N}, j \leq q-1, \delta(x^i y^j) \leq \alpha\right\},$$

which is a basis of $\mathcal{L}(\alpha P_\infty)$ on the Hermitian curve $\mathcal{X}_q : y^q + y = x^{q+1}$.

Definition 1. *Consider $\alpha = uq + v(q+1) \geq q^2 - q - 1$ where $u, v \in \mathbb{N}$. Let $\ell \in \mathbb{Z}^+$,*

$$\mathbf{t} = ((r_1, s_1), \ldots, (r_\ell, s_\ell)) \in \left((\mathbb{Z} \setminus \{0\})^2\right)^\ell$$

be a vector whose coordinates are ℓ pairwise distinct ordered pairs of nonzero integers, and

$$\mathbf{h} = ((a_1, b_1), \ldots, (a_\ell, b_\ell)) \in \left(\mathbb{Z}^2\right)^\ell$$

be a vector whose coordinates are ℓ pairwise distinct ordered pairs of integers satisfying

$$a_k q + b_k(q+1) \leq uq + v(q+1) < (u + r_k)q + (v + s_k)(q+1) < q^3$$

for $k = 1, \ldots, \ell$. Let $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_\ell) \in \left(\mathbb{F}_{q^2} \setminus \{0\}\right)^\ell$. The set of $(\mathbf{t}, \mathbf{h}, \boldsymbol{\eta})$-twisted bivariate polynomials is

$$B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = \left(B(\alpha P_\infty) \setminus \bigcup_{k=1}^{\ell} \left\{x^{a_k} y^{b_k}\right\}\right) \cup \bigcup_{k=1}^{\ell} \left\{x^{a_k} y^{b_k} + \eta_k x^{u+r_k} y^{v+s_k}\right\}.$$

Let $\mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = \langle B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)\rangle$. *The twisted Hermitian code* $C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ *is*

$$C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) := ev\big(\mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}\big) \subseteq \mathbb{F}_{q^2}^n.$$

Remark 1. *It is immediate from the construction that* $C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ *has the same length as the code* $C(\alpha P_\infty)$. *Furthermore,*

$$\dim C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = \dim \mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = |B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)| = |B(\alpha P_\infty)| = \dim C(\alpha P_\infty).$$

In addition, a generator matrix for the twisted Hermitian code is

$$\mathcal{G}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = \begin{bmatrix} ev(f_1) \\ ev(f_2) \\ \vdots \\ ev(f_k) \end{bmatrix}$$

where $B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = \langle f_1, f_2, \ldots, f_k\rangle$.

We sometimes write $C^{n,k}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ to emphasize the length and dimension of a twisted Hermitian code.

Example 1. *Let* $q = 2$ *and* $\alpha = 1(q) + 1(q+1) = 5$. *The Hermitian curve* $\mathcal{X}_2$ *is given by* $y^2 + y = x^3$, *and we consider* $\mathcal{X}_2$ *over a finite field of order* $q^2 = 4$, *which may be described as* $\mathbb{F}_4 = \{0, 1, a, a+1\} \cong \mathbb{Z}_2[x]/\langle x^2+x+1\rangle$. *Note that*

$$B(5P_\infty) = \{1, x, y, x^2, xy\}.$$

The $q^3 + 1 = 8$ *rational points on* X_2 *other than* P_∞ *are enumerated below:*

$$\begin{array}{rcl} P_1 & = & (0:0:1) \\ P_2 & = & (0:1:1) \\ P_3 & = & (1:a:1) \\ P_4 & = & (1:a+1:1) \\ P_5 & = & (a:a:1) \\ P_6 & = & (a:a+1:1) \\ P_7 & = & (a+1:a:1) \\ P_8 & = & (a+1:a+1:1). \end{array}$$

Choose $\ell = 2$ *and the following vectors:*

$$\begin{aligned} \mathbf{t} &= ((1,0),(2,0)), \\ \mathbf{h} &= ((2,0),(1,1)), \\ \boldsymbol{\eta} &= (1,a). \end{aligned}$$

Then

$$\bigcup_{k=1}^{2} \{x^{a_k} y^{b_k}\} = \{x^2, xy\},$$

and

$$\bigcup_{k=1}^{2} \{x^{a_k} y^{b_k} + \eta_k x^{u+r_k} y^{v+s_k}\} = \{x^2 + x^2 y, xy + a x^3 y\}$$

so that

$$B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(5P_\infty) = \{1, x, y, x^2 + x^2 y, xy + a x^3 y\}.$$

The resulting space of functions is

$$\mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(5P_\infty) = \langle B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(5P_\infty)\rangle,$$

and the twisted Hermitian code is

$$C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(5P_\infty) = ev\big(\mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(5P_\infty)\big).$$

A generator matrix $\mathcal{G}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(5P_\infty)$ for the twisted Hermitian code may be obtained by evaluating each element of $B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(5P_\infty)$ at each of the P_i, $1 \le i \le 8$, to obtain

$$\mathcal{G}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(5P_\infty) = \begin{array}{c} \\ 1 \\ x \\ y \\ x^2{+}x^2y \\ xy{+}ax^3y \end{array} \begin{array}{c} \begin{array}{cccccccc} P_1 & P_2 & P_3 & P_4 & P_5 & P_6 & P_7 & P_8 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & a & a & a+1 & a+1 \\ 0 & 1 & a & a+1 & a & a+1 & a & a+1 \\ 0 & 0 & a+1 & a & a & 1 & 1 & a+1 \\ 0 & 0 & 1 & a & 0 & 0 & a & a+1 \end{bmatrix} \end{array}.$$

Because twisted Hermitian codes share some similarities with one-point Hermitian codes (such as length and dimension per Remark 1), it is reasonable to ask how the codes themselves compare and more pointedly if they are essentially the same codes. With this in mind, we next demonstrate that the twisted Hermitian codes are not one-point Hermitian codes.

To reveal the distinction between twisted Hermitian codes and one-point Hermitian codes, we determine the largest subcode of $C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ which is a one-point Hermitian code as well as its smallest supercode which is a one-point Hermitian code. Recall that $\mathbf{t} = ((r_1, s_1), \ldots, (r_\ell, s_\ell)) \in \left((\mathbb{Z}\setminus\{0\})^2\right)^\ell$ and $\mathbf{h} = ((a_1, b_1), \ldots, (a_\ell, b_\ell)) \in \left(\mathbb{Z}^2\right)^\ell$. Let

$$\alpha' = \min\{a_i q + b_i(q+1) : i = 1, \ldots, \ell\} - 1$$

and

$$\alpha'' = \alpha + \max\{r_i q + s_i(q+1) : i = 1, \ldots, \ell\}.$$

Then

$$\mathcal{L}(\alpha' P_\infty) \subseteq \mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) \subseteq \mathcal{L}(\alpha'' P_\infty)$$

follows from the definition of the twisted code by considering basis elements of the space of functions that are used to define the codewords. Therefore,

$$C(\alpha' P_\infty) \subseteq C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) \subseteq C(\alpha'' P_\infty).$$

Notice that

$$\dim C(\alpha' P_\infty) = \left| \left\{ x^i y^j \in B(\alpha P_\infty) \mid \delta(x^i y^j) < \min\{a_i q + b_i(q+1) : i = 1, \ldots, \ell\} \right\} \right| < k,$$

$a_k q + b_k(q+1) \le uq + v(q+1)$ for all $1 \le k \le l$, and the (a_k, b_k) are distinct. In addition,

$$\dim C(\alpha'' P_\infty) = (\alpha + \max\{r_k q + s_k(q+1) \mid k = 1, \ldots, \ell\}) + 1 - g \ge k + q.$$

Hence, we conclude that twisted Hermitian codes are not one-point Hermitian codes. These observations are recorded in the next result, followed by their impact on bounding the minimum distance of the twisted Hermitian code.

Proposition 2. *Consider a twisted Hermitian code $C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ constructed as in Definition 1 with*

$\mathbf{t} = ((r_1, s_1), \ldots, (r_\ell, s_\ell)) \in \left((\mathbb{Z} \setminus \{0\})^2\right)^\ell$ *and* $\mathbf{h} = ((a_1, b_1), \ldots, (a_\ell, b_\ell)) \in \left(\mathbb{Z}^2\right)^\ell$. *Then*

$$C(\alpha' P_\infty) \subsetneqq C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) \subsetneqq C(\alpha'' P_\infty)$$

where

$$\alpha' = \min\{a_i q + b_i(q+1) : i = 1, \ldots, \ell\} - 1$$

and

$$\alpha'' = \alpha + \max\{r_i q + s_i(q+1) : i = 1, \ldots, \ell\}.$$

According to Proposition 2, the minimum distance d of $C^{n,k}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ satisfies

$$n - \alpha'' \leq d\big(C(\alpha'' P_\infty)\big) \leq d \leq d\big(C(\alpha' P_\infty)\big).$$

Both $d(C(\alpha'' P_\infty))$ and $d(C(\alpha' P_\infty))$ are known [17], being minimum distances of Hermitian codes. In the case that $2g - 2 < \alpha'$ and $\alpha'' < n$, we have that

$$n - \alpha'' \leq d\big(C(\alpha'' P_\infty)\big) \leq n - \alpha'.$$

Thus, the twisted code $C^{n,k}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ is capable of correcting at least $t = \left\lfloor \frac{n-\alpha''-1}{2} \right\rfloor$ errors. We can use such a value of t for implementation within the McEliece cryptosystem (as detailed in Section 4), even though the code may be capable of correcting more errors.

Determining tighter bounds on the minimum distance of twisted Hermitian codes is an interesting but nontrivial problem. For instance, in the (perhaps simpler) Reed–Solomon situation, determining weights of codewords of twisted codes can amount to considering roots of sparse polynomials, which is a problem of current interest; see, for instance [22,23]. Another interesting question to consider is if the minimum distance of a twisted Hermitian code can attain that of a Hermitian code, especially given that there exist twisted Reed–Solomon codes which are MDS [4,24].

Example 2. *Consider the twisted Hermitian code* $C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(12P_\infty)$ *with* $q = 3$, $\alpha = 12$,

$$\begin{array}{rcl} \mathbf{t} & = & ((1,0),(0,1)), \\ \mathbf{h} & = & ((1,2),(0,3)), \end{array}$$

and $\boldsymbol{\eta} = (\eta_1, \eta_2)$, *where* $\eta_1, \eta_2 \in \mathbb{F}_9$ *satisfy the conditions of Definition 1. By Proposition 2,*

$$\alpha'' = 12 + \max\{r_i q + s_i(q+1) : i = 1, 2\} = 16$$

and

$$\alpha' = \min\{a_i q + b_i(q+1) : i = 1, 2\} - 1 = 10$$

from which it follows that

$$C(10P_\infty) \subsetneqq C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(12P_\infty) \subsetneqq C(16P_\infty).$$

According to ([13] (Theorem 5)), $d(C(10P_\infty)) = 17$ *and* $d(C(16P_\infty)) = 11$ *so that*

$$11 \leq d\big(C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(12P_\infty)\big) \leq 17.$$

3.2. Squares of Twisted Hermitian Codes

Recall from (1) that a Hermitian code $C(\alpha P_\infty)$ has a Schur square with relatively small dimension: $\dim C(\alpha P_\infty)^2 \leq 2\alpha + 1 - g$. In this section, we show that the twisted Hermitian code $C^{n,k}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ may have a Schur square with much larger dimension in comparison to the square of the code itself.

Because the codes of interest are obtained by evaluating sets of functions, it is useful to consider the Schur product of sets. Given $B, B' \subseteq \mathbb{F}_q[x,y]$, let

$$B \underline{*} B' := \left\{ \mathbf{b} \cdot \mathbf{b}' \mid \mathbf{b} \in B, \mathbf{b}' \in B' \right\},$$

and

$$B^{\underline{2}} := B \underline{*} B.$$

Lemma 1. *Let $\mathscr{M}$ denote the set of bivariate monomials*

$$\mathscr{M} := \left\{ x^i y^j : i,j \in \mathbb{N}, 0 \leq i \leq q^2 - 1, 0 \leq j \leq q-1 \right\} \subseteq \mathbb{F}_{q^2}[x,y].$$

Then the evaluation map $ev : \langle \mathscr{M} \rangle \to \mathbb{F}_{q^2}^n$ is an injective mapping.

Proof. Let the domain of ev be restricted to $\langle \mathscr{M} \rangle$ as described above. It suffices to show that $\ker(ev) = \{0\}$. Assume to the contrary that $0 \neq p(x,y) \in \langle \mathscr{M} \rangle$ such that $ev(p(x,y)) = \mathbf{0} \in \mathbb{F}_{q^2}^n$. Then every rational affine point $(x : y : 1)$ of the Hermitian curve $\mathcal{X}_q$ also satisfies $p(x,y) = 0$. Fix $a \in \mathbb{F}_{q^2}$. Then there are then q distinct $b_i \in \mathbb{F}_{q^2}$ such that $(a : b_i : 1)$ is a rational point on the Hermitian curve $\mathcal{X}_q$. Then the univariate polynomial $p(a,y)$ has q distinct zeros in $\mathbb{F}_{q^2}$, despite the fact that $\deg(p(a,y)) \leq q-1$. Hence $p(a,y) \equiv 0$ for all $a \in \mathbb{F}_{q^2}$. On the other hand,

$$p(x,y) = \sum_{j=0}^{q-1} \left(\sum_{i=0}^{q^2-1} a_{ij} x^i \right) y^j = \sum_{j=0}^{q-1} q_j(x) y^j$$

where $q_j(x) = \sum_{i=0}^{q^2-1} a_{ij} x^i$ and $q_j(a) = 0$ for all $a \in \mathbb{F}_{q^2}$. This implies the univariate polynomial $q_j(x)$ has q^2 zeros in $\mathbb{F}_{q^2}^n$, despite the fact that $\deg(q_j) \leq q^2 - 1$. As a result, $p(x,y) \equiv 0$, which is a contradiction. □

We can use properties of the finite field to define a reduction scheme for bivariate polynomials.

Definition 2. *Suppose $i, j \in \mathbb{N}$ are such that $0 \leq i \leq 2(q^2-1)$ and $0 \leq j \leq q-1$. We define*

$$\overline{x^i y^j} := \begin{cases} x^i y^j & \text{if } 0 \leq i \leq q^2 - 1 \\ x^{i-(q^2-1)} y^j & \text{otherwise.} \end{cases}$$

For $f(x,y) = \sum c_k x^{i_k} y^{j_k} \in \mathbb{F}_{q^2}[x,y]$, we define

$$\overline{f} := \sum c_k \overline{x^{i_k} y^{j_k}}. \tag{3}$$

It follows immediately that for $f = \sum c_k x^{i_k} y^{j_k}, g = \sum d_h x^{i_h} y^{j_h} \in \mathcal{L}(\alpha P_\infty)$,

$$ev(f \cdot g) = ev(\overline{f \cdot g}).$$

Given $f(x,y) = \sum_{k=1}^n c_k x^{i_k} y^{j_k} \in \mathbb{F}_{q^2}[x,y]$,

$$\delta(f) := \max\{i_k q + j_k (q+1) : k = 1, \ldots, n\}. \tag{4}$$

If $B = \{f_1, \ldots, f_m\} \subseteq \mathbb{F}_{q^2}[x,y]$, then

$$\delta(B) := \{\delta(f_k) : k = 1, \ldots, m\}. \tag{5}$$

We can now establish a lower bound on $\dim C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)^2$.

Lemma 2. *Let $C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ be a twisted Hermitian code. Then*

$$\dim C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)^2 \geq \mid \overline{D} \mid$$

where $\overline{D} := \{\delta(\overline{f \cdot g}) \mid f, g \in \mathcal{L}(\alpha P_\infty)\}$.

Lemma 2 suggests that $\dim C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)^2$ can be made large by choosing $\mathbf{t}, \mathbf{h}, \boldsymbol{\eta}$ to maximize the size of $\overline{D}$. Before applying it, we first establish a few relevant tools.

Given $\mathscr{M}$ as in Lemma 1, set

$$\mathscr{M}_2 := \left\{ x^i y^j \in \mathscr{M} : \delta(x^i y^j) \leq \left\lceil \frac{\max \delta(\mathscr{M})}{2} \right\rceil \right\}.$$

Observe that for any prime power q,

$$\left\lceil \frac{\max \delta(\mathscr{M})}{2} \right\rceil = \left\lceil \frac{(q^2-1)q + (q-1)(q+1)}{2} \right\rceil \geq 2g+1.$$

It follows that

$$\mathscr{M} \subseteq \mathscr{M}_2^{\underline{2}}.$$

We make use of this observation in the following lemma.

Lemma 3. *Let $A \subseteq \mathbb{F}[x,y]$ be a set of elements with distinct pole orders such that $\delta(A) \subseteq \delta(\mathscr{M}_2)$. Then $\mid \delta\left(A^{\underline{2}}\right) \setminus \delta(\mathscr{M}) \mid \leq g$.*

Proof. Since $\mathscr{M} \subseteq \mathscr{M}_2^{\underline{2}}$, $\delta(\mathscr{M}) \subseteq \delta(\mathscr{M}^{\underline{2}})$. Observe that

$$\mid \delta(\mathscr{M}_2^{\underline{2}}) \setminus \delta(\mathscr{M}) \mid = \mid \delta\left(\mathscr{M}_2^{\underline{2}}\right) \mid - \mid \delta(\mathscr{M}) \mid = \left[(q^3+q^2-q-1)+1-g\right] - q^3 = g.$$

Since $\delta(A^{\underline{2}}) \subseteq \delta(\mathscr{M}_2^{\underline{2}})$, it follows that $\mid \left(\delta\left(A^{\underline{2}}\right) \setminus \delta(\mathscr{M})\right) \mid \leq g$. □

Next, we employ a few basic results from additive number theory; specifically, we make use of the notion of a Sidon set.

Definition 3. *A set $A \subseteq \mathbb{N}$ is a finite Sidon set provided it is finite and $\forall a, b, c, d \in A$, $a + b = c + d$ if and only if $(a, b) = (c, d)$ or $(a, b) = (d, c)$.*

Erdös and Turan show in [25] that every subset of a Sidon set is itself a Sidon set and that every nonempty subset of $\mathbb{N}$ contains a Sidon set. For finite and nonempty $A \subseteq \mathbb{N}$, let $S[A]$ denote the largest subset of A that is a Sidon set. Gowers shows in [26] that $\mid S[A] \mid \leq 2\sqrt{\mid A \mid}$.

We now introduce a family of twisted Hermitian codes with a large Schur square dimension. It will be useful to consider the map

$$\begin{array}{rccc} \phi_q : & \mathbb{N} & \to & \mathbb{Z}^2 \\ & w & \mapsto & ((q+1)\lfloor \frac{w}{q} \rfloor - w, w - q\lfloor \frac{w}{q} \rfloor). \end{array}$$

Theorem 1. *For a given prime power q_0, let $\alpha \in \delta(\mathscr{M})$ be such that $\alpha \leq \frac{q^3+2\sqrt{q^3+1}+1}{4}$ and*

$$\begin{aligned} \mathcal{P} &:= \left\{ \delta(x^i y^j) : x^i y^j \in \mathscr{M}, \delta(x^i y^j) \leq \alpha \right\} \\ \mathcal{T} &:= \left\{ \delta(x^i y^j) : x^i y^j \in \mathscr{M}, \delta(x^i y^j) > \alpha \right\} = \{t_1, \ldots, t_\ell\} \\ \mathcal{H} &:= \mathcal{P} \setminus S[\mathcal{P}] = \{h_1, \ldots, h_\ell\} \end{aligned}$$

satisfying $\ell := \mid \mathcal{H} \mid \leq \mid \mathcal{T} \mid$. *Let*

$$\mathbf{h} = (\phi(h_1), \ldots, \phi(h_\ell));$$
$$\mathbf{t} = (\phi(t_1) - (u, v), \ldots, \phi(t_\ell) - (u, v));$$

$s_1, \ldots, s_\ell$ *be prime powers such that*

$$\mathbb{F}_{q_0^2} = \mathbb{F}_{s_0} \subsetneqq \mathbb{F}_{s_1} \subsetneqq \cdots \subsetneqq \mathbb{F}_{s_\ell} = \mathbb{F}_{q^2}; \tag{6}$$

and $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_\ell)$ *be such that* $\eta_i \in \mathbb{F}_{s_i} \setminus \mathbb{F}_{s_{i-1}}$ *for* $i = 1, \ldots, \ell$. *Then*

$$\dim C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)^2 \geq \binom{k+1}{2} - g$$

where $k := \dim C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$.

Proof. Let $B = \left\{x^i y^j : \delta(x^i y^j) \in S[\mathcal{P}]\right\}$ and $B_t = \left\{x^{a_m} y^{b_m} + \eta_m x^{u+r_m} y^{v+s_m} : m = 1, \ldots, \ell\right\}$. Then $C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = ev\langle B \cup B_t \rangle$ and $C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)^2 = ev\langle (B \cup B_t)^{\underline{2}} \rangle$. Note that $B \cup B_t$ is a set of functions with distinct pole orders. We claim that $(B \cup B_t)^{\underline{2}}$ is a linearly independent set. Consider $f_m := x^{i_m} y^{j_m} \in B$ and $f'_m := x^{a_m} y^{b_m} + \eta_m x^{u+r_m} y^{v+s_m} \in B_t$. Then $(B \cup B_t)^{\underline{2}}$ can be written as $(B \cup B_t)^{\underline{2}} = A \cup C \cup D$ where $A := \{f_m f_{m'} : \delta(f_m), \delta(f_{m'}) \in S[\mathcal{P}]\}$, $C := \left\{f_m f'_{m'} : \delta(f_m) \in S[\mathcal{P}], m' = 1, \ldots, \ell\right\}$, and $D := \left\{f'_m f'_{m'} : m, m' = 1, \ldots, \ell\right\}$. Notice that if $\delta(x^{i+i'} y^{j+j'}) = \delta(x^{i''+i'''} y^{j''+j'''})$ for $x^{i+i'} y^{j+j'}, x^{i''+i'''} y^{j''+j'''} \in A$, then $\delta(x^i y^j) = \delta(x^{i''} y^{j''})$ (in which case $\delta(x^{i'} y^{j'}) = \delta(x^{i'''} y^{j'''})$) or $\delta(x^i y^j) = \delta(x^{i'''} y^{j'''})$ (in which case $\delta(x^{i'} y^{j'}) = \delta(x^{i''} y^{j''})$) follows from the properties of the Sidon set. In the first case, this implies that $i = i''$ and $j = j''$. In the second, $i = i'''$ and $j = j'''$. As a result, all elements of A have distinct pole orders. Furthermore, no pole order of an element of A is that of an element of C or D as $\delta(f_m f_{m'}) \leq \alpha \leq \delta(f)$ for all $f_m f_{m'} \in A$ and $f \in C \cup D$. Continuing in this way, we see that

$$\begin{aligned} \mid (B \cup B_t)^{\underline{2}} \mid &= \binom{\mid B \mid + \mid B_t \mid + 1}{2} \\ &= \binom{k+1}{2}. \end{aligned}$$

and applying Lemma 3 gives

$$\mid \delta((B \cup B_t))^{\underline{2}} \setminus \delta(\mathscr{M}) \mid \leq g$$

which implies that at most g elements of $\delta(B \cup B_t)^{\underline{2}}$ are not in $\mathscr{M}$. Then at least $\binom{k+1}{2} - g$ elements of $\delta\left((B \cup B_t)^{\underline{2}}\right)$ lie in $\mathscr{M}$; i.e., $\dim ev\langle (B \cup B_t)^{\underline{2}} \rangle \geq \binom{k+1}{2} - g$. Thus, $\dim C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)^2 \geq \binom{k+1}{2} - g$. □

This particular subfamily achieves a large Schur square dimension by first maximizing the size of $\overline{D}$ as seen in Theorem 2 and then forcing linear independence by choosing coefficients according to the nested field structure shown in (6).

3.3. Decoding Twisted Hermitian Codes

Tailored decoding algorithms for twisted Hermitian codes can be designed by borrowing ideas from those for twisted Reed–Solomon codes given in [4]. For a twisted Hermitian code $C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ with $\mathbf{t} \in \left(\mathbb{Z}^2\right)^\ell$ and received message $m \in \mathbb{F}_{q^2}^n$, ℓ coefficients $\gamma_1, \ldots, \gamma_\ell \in \mathbb{F}_{q^2}$ may be guessed (or selected at random). A decoding algorithm for a Hermitian code may then be applied to $m - ev\left(\sum_{i=1}^{\ell} \eta_i \gamma_{a_i,b_i} x^{u+r_i} y^{v+s_i}\right)$ as if it was a received word. This allows

application of any Hermitian decoder. These rounds of guessing will only be successful if $\gamma_i = a_{a_i,b_i}$, for $i = 1, ..., \ell$. Because the alphabet size is q^2, this may require up to q^{2^ℓ} rounds of Hermitian decoding. As with twisted Reed–Solomon codes, these rounds might produce twisted Hermitian polynomials where $\gamma_i \neq a_{a_i,b_i}$. The polynomials that are produced with these characteristics will be discarded as they do not yield valid codewords.

The efficiency of decoding twisted Hermitian codes may be considered by taking the cost of the Hermitian decoder used and multiplying it by the number of guessing rounds. Two methods of decoding Hermitian codes that might be utilized are those that have sub-quadratic efficiency, which is the best complexity known for decoding Hermitian codes. The Guruswami-Sudan Algorithm [27] has a Hermitian decoding efficiency of $O(n^{2+\omega/3}s^\omega m)$, where m and s are the multiplicity and list size parameters respectively and $\omega \leq 3$ is the exponent of matrix multiplication. This means that decoding twisted Hermitian codes using the Guruswami-Sudan Algorithm would have efficiency $O(q^{2^\ell} n^{2+\omega/3}s^\omega m)$. Power decoding also has a similar decoding efficiency for Hermitian codes, which is $O(n^{2+\omega/3}p^\omega)$, where p is the powering parameter and ω is as defined before [28]. This means that the efficiency of decoding twisted Hermitian codes using power decoding is $O(q^{2^\ell} n^{2+\omega/3}p^\omega)$. Determining more efficient and specialized decoding methods for twisted algebraic geometry codes remains a topic of study.

4. Applications of Twisted Hermitian Codes to the McEliece Cryptosystem

In this section, we consider the potential use of twisted Hermitian codes in a code-based cryptosystem. First, we abstract the key elements of the McEliece cryptosystem for use with an arbitrary linear code (in place of the Goppa code in [7]). Then we consider the role of squares in attacking the resulting system, noting how the twisted codes avoid direct distinguisher attack. This section concludes with considerations prompted by the recent attack of Lavauzelle and Renner [11] on a twisted Reed–Solomon code-based cryptosystem.

Let G be a $k \times n$ generator matrix for an $[n, k, d]$ linear code $\mathcal{C}$ over a finite field $\mathbb{F}$ capable of correcting at least t errors. The public key is $(G^{\text{PUB}}, t) := SGP$, where $S \in \mathbb{F}^{k\times k}$ is nonsingular and $P \in \mathbb{F}^{n\times n}$ is a permutation matrix. The private key is $(S, P, D_\mathcal{C})$, where $D_\mathcal{C}$ is an efficient decoding algorithm of $\mathcal{C}$. To transmit a message to a receiver Alice, Bob encodes the message $m \in \mathbb{F}^k$ as $mG^{\text{PUB}} + e$, where $e \in \mathbb{F}^{1\times n}$ has weight $wt(e) \leq t$. Alice receives a transmission in the form $x := mSGP + e$ and initiates deciphering by left-multiplying x by P^{-1} to yield $mSG + eP^{-1}$. Alice then applies the decoding algorithm $D_\mathcal{C}$ to retrieve mS and left-multiplies by S^{-1} to recover m. To maintain security, the underlying code $\mathcal{C}$ must not be revealed.

Role of Squares in the McEliece Cryptosystem

The Schur square distinguisher is an attack applied to the McEliece cryptosystem implemented with Reed–Solomon codes in [18]. Though the attacker does not know the linear code $\mathcal{C}$ underlying G^{PUB}, the distinguisher may allow the attacker to know $\dim \mathcal{C}^2$. The low-dimensional squares of Reed–Solomon and Hermitian codes imply that $\dim \mathcal{C}^2$ can be used to distinguish $\mathcal{C}$ from a random linear code. This is demonstrated in [18] where generalized Reed–Solomon codes are considered; Schur products are used to identify $\mathcal{C}^2$ within the family from which it is drawn; and the Sidelnikov and Shestakov algorithm may then be used to identify $\mathcal{C}$. See also [29] for other approaches involving generalized Reed–Solomon codes. Since $\dim \mathcal{C}^2$ can be an identifying characteristic of the family of codes from which $\mathcal{C}$ is drawn, the attacker may then use a family-specific structural attack on intercepted messages. Both twisted Reed–Solomon and twisted Hermitian codes may avoid a direct application of this attack if constructed to have large dimensional squares.

Based on the attacks described above, it is desirable to implement this code-based cryptosystem with a family of codes whose Schur squares are indistinguishable from those of random codes. With this in mind twisted Reed–Solomon codes were introduced in [4] and can be defined as follows.

Definition 4. *Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ be pairwise distinct field elements, and fix $1 \leq k \leq n$, $\ell \geq 1$. Let $\mathbf{h} \in \{0, \cdots, k-1\}^\ell, \mathbf{t} \in \{1, \ldots, n-k\}^\ell$ such that $\boldsymbol{\eta} \in (\mathbb{F}_q \backslash \{0\})^\ell$. A twisted Reed–Solomon code of length n and dimension k is given by:*

$$C_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}(k) = \left\{ (f(\alpha_1), \cdots, f(\alpha_n)) : f \in \left\{ \sum_{i=0}^{k-1} a_i x^i + \sum_{j=1}^{\ell} \eta_j a_{h_j} x^{k-1+t_j} : a_i \in \mathbb{F}_q \right\} \right\}.$$

Consider the evaluation map

$$\begin{array}{rccc} ev_\alpha : & \mathbb{F}_q[x] & \to & \mathbb{F}_q^n \\ & f & \mapsto & (f(\alpha_1), \cdots, f(\alpha_n)). \end{array}$$

Let q_0 be a prime, and $q = q_\ell = q_0^{2^\ell}$. Lavazuelle and Renner showed in [11] that the subfield subcode $C_{sub} = C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(k) \cap \mathbb{F}_{q_0}^n$ of $C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(k)$ is given by

$$C_{sub} = \left\langle ev_\alpha(x^i) : i \in \{0, 1, \cdots, k-1\} \backslash \{h_1, h_2, \cdots, h_\ell\} \right\rangle_{\mathbb{F}_{q_0}}.$$

Given that C_{sub} is not a Reed–Solomon code, the Sidelnikov-Shestakov attack cannot be directly applied. However, for $\ell \leq \frac{1}{2}(\sqrt{n} - 3)$ the Schur square C_{sub}^2 is a Reed–Solomon code of length n and dimension $2k - 1$. This idea forms the basis for an efficient key-recovery attack on the code-based cryptosystem employing twisted Reed Solomon codes.

The similarity in construction of twisted Hermitian codes and twisted Reed–Solomon codes suggests a possible attack on the cryptosystem based on the twisted Hermitian codes. In the remaining part of this section, we consider the possible components of such an attack. Recall the code $C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ over $\mathbb{F}_{q^2}$ constructed in Theorem 1 where

$$\mathbb{F}_{q_0^2} = \mathbb{F}_{s_0} \subsetneqq \mathbb{F}_{s_1} \subsetneqq \cdots \subsetneqq \mathbb{F}_{s_\ell} = \mathbb{F}_{q^2},$$

and consider the subfield subcode

$$C_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) \cap \left(\mathbb{F}_{q_0}^2\right)^n$$

where $\mathbf{h} = ((a_1, b_1), \ldots, (a_\ell, b_\ell)) \in \left(\mathbb{Z}^2\right)^\ell$.

Lemma 4. *Let $f \in \langle \mathscr{M} \rangle_{\mathbb{F}_{q^2}} \subseteq \mathbb{F}_{q^2}[x, y]$ and $P_1, \ldots, P_n \in \mathcal{X}_{q_0^2}(\mathbb{F}_{q_0^2})$. Then $ev(f) \in \mathbb{F}_{q_0^2}^n$ if and only if $f \in \langle \mathscr{M}_0 \rangle_{\mathbb{F}_{q_0^2}}$ where $\mathscr{M}_0 := \left\{ x^i y^j : i, j \in \mathbb{N}, 0 \leq i \leq q_0^2 - 1, 0 \leq j \leq q_0 - 1 \right\}$.*

Proof. Suppose $f \in \langle \mathscr{M}_0 \rangle_{\mathbb{F}_{q_0^2}}$ and $P_1, \ldots, P_n \in \mathcal{X}_{q_0^2}(\mathbb{F}_{q_0^2})$. Then it is clear that $ev(f) \in \mathbb{F}_{q_0^2}^n$. Conversely, consider $c := ev(f) \in \mathbb{F}_{q_0^2}^n$ where $f \in \langle \mathscr{M} \rangle_{\mathbb{F}_{q^2}} \subseteq \mathbb{F}_{q^2}[x, y]$. According to ([28] (Lemma 6)), there exists $p = \sum_{\alpha \in \mathbb{F}_{q_0^2}} \prod_{\alpha' \in \mathbb{F}_{q_0^2} \backslash \{\alpha\}} \frac{x - \alpha'}{\alpha - \alpha'} \left(\sum_{\beta \in B_\alpha} \gamma_{\alpha,\beta} \prod_{\beta' \in B_\alpha \backslash \{\beta\}} \frac{y - \beta'}{\beta - \beta'} \right)$ such that $ev(p) = c$. Notice that $p \in \langle \mathscr{M}_0 \rangle_{\mathbb{F}_{q_0^2}} \subseteq \langle \mathscr{M} \rangle_{\mathbb{F}_{q^2}}$. Since $ev : \langle \mathscr{M} \rangle_{\mathbb{F}_{q^2}} \to \mathbb{F}_{q^2}^n$ is an injective map (as shown in Lemma 1) and $c = ev(p) = ev(f)$, it follows that $f = p \in \langle \mathscr{M}_0 \rangle_{\mathbb{F}_{q_0^2}}$. □

Proposition 3. *Given a twisted Hermitian code $\mathcal{C} = C_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}(\alpha P_\infty)$ and $P_1, \ldots, P_n \in \mathcal{X}_{q_0^2}(\mathbb{F}_{q_0^2})$,*

$$\mathcal{C} \cap \mathbb{F}_{q_0^2}^n = \left\{ ev(f) : f \in \left\langle B(\alpha P_\infty) \setminus \bigcup_{k=1}^{\ell} \left\{ x^{a_k} y^{b_k} \right\} \right\rangle_{\mathbb{F}_{q_0^2}} \right\}.$$

Proof. Consider $ev(f)$ where $f \in \left\langle B(\alpha P_\infty) \setminus \bigcup_{k=1}^{\ell} \left\{ x^{a_k} y^{b_k} \right\} \right\rangle_{\mathbb{F}_{q_0^2}}$. Then $ev(f) \in \mathcal{C} \cap \mathbb{F}_{q_0^2}^n$ as each $P_i \in \mathcal{X}_{q_0}(\mathbb{F}_{q_0^2})$. On the other hand, suppose that $ev(f) \in \mathcal{C} \cap \mathbb{F}_{q_0^2}^n$. Then Lemma 4 applies so that $f \in \left\langle B(\alpha P_\infty) \setminus \bigcup_{k=1}^{\ell} \left\{ x^{a_k} y^{b_k} \right\} \right\rangle_{\mathbb{F}_{q_0^2}}$. □

This result prompts the conjecture that the Schur square of the subfield subcode of a twisted Hermitian code in Proposition 3 is a Hermitian code. This is related to ([10] (Conjecture 19)). Positive resolution of these conjectures would lay the groundwork for an attack on a twisted Hermitian code-based cryptosystem.

5. Conclusions

In this paper, we present a new family of codes, called twisted Hermitian codes, whose construction is based on Hermitian codes. The length and dimension of the new codes is the same as the Hermitian codes, but these codes are not Hermitian codes. These new codes can have Schur squares larger than those of Hermitian codes. In particular, we identify a subfamily of the new codes that have Schur squares of dimension close to that expected of a random linear code. Codes of this subfamily are resistant to Schur square distinguishing when applied directly. However, the associated code-based cryptosystems may exhibit potential vulnerabilities related to square distinguisher attacks on particular subfield subcodes. This work leaves open several avenues that are worth investigation. Obtaining an improved lower bound on the twisted Hermitian codes, either in general or for the particular subfamily identified in this work, remains a challenge. Addressing it would allow one to consider if it is possible to obtain twisted Hermitian codes with parameters rivaling those of one-point Hermitian codes. It would also allow for the introduction of more noise in the associated code-based cryptosystem. We have not considered in this work the potential to construct twisted Hermitian codes C which are linearly complementary dual (LCD), meaning the intersection of C and its dual is trivial. In addition, the interested reader may find that it is possible to design tailored decoding algorithms for the twisted Hermitian codes beyond what is addressed in this work.

Author Contributions: Investigation, writing and revision: A.A., K.B., O.F., R.K., B.M., G.L.M. and Z.N. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by NSF DMS-1547399.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: The work of the sixth author is supported in part by NSF DMS-2037833, NSF DMS-1802345, and the Commonwealth Cyber Initiative.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Pellikaan, R. On decoding by error location and dependent sets of error positions. *Discret. Math.* **1992**, *106–107*, 369–381. [CrossRef]
2. Cascudo, I.; Cramer, R.; Mirandola, D.; Zémor, G. Squares of random linear codes. *IEEE Trans. Inf. Theory* **2015**, *61*, 1159–1173. [CrossRef]
3. Márquez-Corbella, I.; Martínez-Moro, E.; Pellikaan, R. The non-gap sequence of a subcode of a generalized Reed-Solomon code. *Des. Codes Cryptogr.* **2013**, *66*, 317–333. [CrossRef]
4. Beelen, P.; Puchinger, S.; Rosenkilde né Nielsen, J. Twisted Reed-Solomon codes. In Proceedings of the 2017 IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, 25–30 June 2017; pp. 336–340.
5. Sheekey, J. A new family of linear maximum rank distance codes. *Adv. Math. Commun.* **2016**, *10*, 475–488. [CrossRef]
6. Lv, J.; Li, R.; Wang, J. Constructions of quasi-twisted quantum codes. *Quantum Inf. Process.* **2020**, *19*, 1–25. [CrossRef]
7. McEliece, R.J. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *Deep. Space Netw. Prog. Rep.* **1978**, *44*, 114–116.
8. Berlekamp, E.; McEliece, R.; Van Tilborg, H. On the inherent interactability of certain coding problems. *IEEE Trans. Inf. Theory* **1978**, *IT-24*, 384–386. [CrossRef]

9. Janwa, H.; Moreno, O. McEliece public key cryptosystems using algebraic-geometric codes. *Des. Codes Cryptogr.* **1996**, *8*, 293–307. [CrossRef]
10. Couvreur, A.; Márquez-Corbella, I.; Pellikaan, R. Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes. *IEEE Trans. Inf. Theory* **2017**, *63*, 5404–5418. [CrossRef]
11. Lavauzelle, J.; Renner, J. Cryptanalysis of a system based on twisted Reed-Solomon codes. *Des. Codes Cryptogr.* **2020**, *88*, 1285–1300. [CrossRef]
12. Høholdt, T.; Lint, J.; Pellikaan, R. Algebraic geometry codes. In *Handbook of Coding Theory*; Elsevier: Amsterdam, The Netherlands, 1998; Volume 1, pp. 871–961.
13. Stichtenoth, H. A note on Hermitian codes over GF(q^2). *IEEE Trans. Inform. Theory* **1988**, *34*, 1345–1348. [CrossRef]
14. Stichtenoth, H. *Algebraic Function Fields and Codes*, 2nd ed.; Springer: Berlin, Germany, 2008.
15. Vladut, S.; Nogin, D.; Tsfasman, M. *Algebraic Geometric Codes: Basic Notions*; American Mathematical Society: Providence, RI, USA, 2007.
16. Christensen, R.B.; Geil, O. On nested code pairs from the Hermitian curve. *Finite Fields Their Appl.* **2020**, *68*, 101742. [CrossRef]
17. Yang, K.; Kumar, P.V. On the true minimum distance of Hermitian codes. In *Coding Theory and Algebraic Geometry (Luminy, 1991)*; Volume 1518 of Lecture Notes in Mathematics; Springer: Berlin, Germany, 1992; pp. 99–107
18. Couvreur, A.; Gaborit, P.; Gauthier-Umana, V.; Otmani, A.; Tillich, J.-P. Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes. *Des. Codes Cryptogr.* **2014**, *73*, 641–666. [CrossRef]
19. Bolkema, J.; Gluesing-Luerssen, H.; Kelley, C.A.; Lauter, K.E.; Malmskog, B.; Rosenthal, J. Variations of the McEliece cryptosystem. In *Algebraic Geometry for Coding Theory and Cryptography*; Volume 9 of Association for Women in Mathematics Series; Springer: Cham, Switzerland, 2017; pp. 129–150.
20. Pellikaan, R.; Márquez-Corbella, I. Error-correcting pairs for a public-key cryptosystem. *J. Phys. Conf. Ser.* **2017**, *855*, 012032. [CrossRef]
21. Beelen, P.; Bossert, M.; Puchinger, S.; Rosenkilde, J. Structural properties of twisted Reed-Solomon codes with applications to cryptography. In Proceedings of the 2018 IEEE International Symposium on Information Theory (ISIT), Vail, CO, USA, 17–22 June 2018; pp. 946–950.
22. Cheng, Q.; Gao, S.; Rojas, J.M.; Wan, D. Sparse univariate polynomials with many roots over finite fields. *Finite Fields Their Appl.* **2017**, *46*, 235–246. [CrossRef]
23. Kelley, Z. Roots of sparse polynomials over a finite field. *LMS J. Comput. Math.* **2016**, *19*, 196–204. [CrossRef]
24. Liu, H.; Liu, S. New constructions of MDS twisted Reed-Solomon codes and LCD MDS codes. *arXiv*, **2020**, arXiv:2008.03708.
25. Erdos, P.; Turan, P. On a problem of Sidon in additive number theory, and on some related problems. *J. London Math. Soc.* **1941**, *16*, 212–215. [CrossRef]
26. Gowers, T. What are Dense Sidon Subsets of {1,2,...,n} Like? Available online: https://gowers.wordpress.com/2012/07/13/what-are-dense-sidon-subsets-of-12-n-like/ (accessed on 16 July 2018).
27. Guruswami, V.; Sudan, M. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Trans. Inf. Theory* **1999**, *45*, 1757–1767. [CrossRef]
28. Nielsen, J.S.R.; Beelen, P. Sub-quadratic decoding of one-point Hermitian codes. *IEEE Trans. Inf. Theory* **2015**, *61*, 3225–3240. [CrossRef]
29. Wieschebrink, C. Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes. In *Post-Quantum Cryptography*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 61–72.