Equiangular quantum key distribution in more than two dimensions

Radhakrishnan Balu\textsuperscript{1,2,6}, Paul J Koprowski\textsuperscript{3}, Kasso A Okoudjou\textsuperscript{3}, Justin S Park\textsuperscript{4} and George Siopsis\textsuperscript{5}

\textsuperscript{1} Computer and Information Sciences Directorate, Army Research Laboratory, Adelphi, MD 21005-5069, United States of America
\textsuperscript{2} Computer Science and Electrical Engineering, University of Maryland Baltimore County, 1000 Hilltop Circle, Baltimore, MD 21250, United States of America
\textsuperscript{3} Department of Mathematics \& Norbert Wiener Center for Harmonic Analysis and Applications, University of Maryland, College Park, MD 20742, United States of America
\textsuperscript{4} Massachusetts Institute of Technology, Cambridge, MA 02139, United States of America
\textsuperscript{5} Department of Physics and Astronomy, University of Tennessee, Knoxville, TN 37996-1200, United States of America

E-mail: radhakrishnan.balu.civ@mail.mil, pkoprowsk@math.umd.edu, kasso@math.umd.edu, jpark00@mit.edu, siopsis@tennessee.edu and radbalu1@umbc.edu

Received 14 October 2018, revised 21 November 2018
Accepted for publication 11 December 2018
Published 22 January 2019

Abstract

We extend the spherical code-based key distribution protocols to qudits with dimensions 4 and 16 by constructing equiangular frames and their companions. We provide methods for equiangular frames in arbitrary dimensions for Alice to use and the companion frames, that have one antipode to eliminate one of the possibilities, made up of qudits with $N = 4, 16$ as part of Bob’s code. Non-orthogonal bases that form positive operator-valued measures can be constructed using the tools of frames (overcomplete bases of a Hilbert space), and here we apply them to key distribution that is robust due to the large size of the bases, making it hard to eavesdrop. We demonstrate a method to construct a companion frame for an equiangular tight frame for $\mathbb{C}^{p-1}$ generated from the discrete Fourier transform, where $p$ is any odd prime. The security analysis is based on the assumption of restricting possible attacks to an intercept/resend scenario, highlighting the advantages of qudit-based over qubit-based protocols.

Keywords: QKD, spherical codes, equiangular frames, tight frames, qudits

\textsuperscript{6} Author to whom any correspondence should be addressed.
1. Introduction

Quantum key distribution (QKD) uses the laws of quantum mechanics to allow two users to effectively and securely generate a one-time pad in order to protect sensitive information from adversaries. The first such protocol, the so-called BB84 algorithm [1], employs two sets of mutually unbiased orthonormal bases of $\mathbb{C}^2$. In this protocol, the first basis set is the eigenbasis of one observable (e.g. $\sigma_x$) and the second basis set is the eigenbasis of one of the two sets of complementary observables ($\sigma_y$ and $\sigma_z$). In [2], the BB84 protocol is extended to six states, employing both sets of complementary measurements. The increase in the observables allows for better detection of adversarial eavesdroppers [3]. Another way to set up quantum communication protocols that minimize error probabilities while maximizing mutual information involve non-orthogonal positive-operator-valued measures (POVMs) such as the three-state quantum cryptography protocol introduced by Chefles et al [4]. This class of protocols is interesting due to the existence of powerful results on POVMs that can be used to design rejected-data protocols that reveal the presence of an eavesdropper using the bits that would be discarded. In [4, 5] and [6] the authors move to the more general framework of non-orthogonal POVMs for qubit QKD based on equiangular spherical codes. The simplicity of spherical codes is due to the avoidance of sacrificing potential key letters in order to determine the amount of information that an attacker has learned about the key sequence because the success rate provides this information. The protocols further provide a wide range of security and rate of key generation for a given dimension of the system. When the number of signal states is fixed, spherical codes offer a higher noise threshold for security than mutually unbiased bases with a trade-off in terms of lower key generation rates. Specific examples of this family of protocols include two-qubit-based spherical codes— the trine that improves upon BB84 and the tetrahedron which performs better than six-state (it has improved resistance to eavesdropping and provides the key error rate in terms of sift rate, thus offering a simplified framework). QKD protocols in higher dimensions up to 16 [7] and those based on qudits [8, 9] that are error-resilient inspired us to look for spherical codes in similar dimensions as they would combine the advantages of both classes of protocol. With the experimental realization of qudits, the d-levels may be encoded on spatial [10, 11] or time-energy [12, 13] modes or the orbital angular momentum [14] of photons, and our class of protocols is interesting from the point of view of efficiency and robustness. In this work we are concerned with developing more general spherical codes in higher dimensions using Hilbertian frames and carry out the security analysis in the context of intercept/resend attacks. The basic ingredients of our protocol for QKD, namely generation, transmission, measurement of qubits and classical handshake, are the same as in existing implementations such as the BB84 family of protocols. Our contribution is mainly in systematically choosing the non-orthogonal bases in higher dimensions, increasing complexity due to scaling and special requirements of the spherical codes that require rigorous treatments, to encode information. In the physical realization of QKD protocols one often uses weak coherent sources of photons because that is more practical. One may use the same sources in our case and modulate them accordingly in order to engineer the higher-dimensional states used in our protocols (e.g. with time-binning [15]). The security analysis presented here will have to be modified to take into account realistic sources. As in the BB84 case, one way to avoid photon-number-splitting attacks is through the implementation of decoy states [16]. We hope to report on a security proof taking into account a realistic setup in the near future.

There is a well-established correspondence between POVMs and the class of tight frames. Let $d \geq 2$. A tight frame for $\mathbb{C}^d$ is a set of vectors $\{f_j\}_{j=1}^N \subset \mathbb{C}^d$ such that for all $x \in \mathbb{C}^d$ we
have that $\sum_{j=1}^{N} |\langle x, f_j \rangle|^2 = A \| x \|^2$ for some positive constant $A$. If, in addition, $\| f \| = 1$, for each $j = 1, \ldots, N$, then $(f_j)_{j=1}^{N}$ is called a finite unit norm tight frame (FUNTF), and it is easy to see that $A = Nd$. A FUNTF $F = (f_j)_{j=1}^{N}$ for which there exists a constant $c > 0$ with $|\langle f_j, f_k \rangle| = c$ for $j \neq k$ is called an equiangular tight frame (ETF) (also known as mutual unbiasedness). We refer to [17–19] for more on finite frame theory and some of its applications. Observe that if $(f_j)_{j=1}^{N}$ is a FUNTF for $\mathbb{C}^d$, then we can write

$$\sum_{j=1}^{N} \frac{d}{N} f_j \otimes f_j^\dagger = I_{d \times d},$$

which is to say, $\{ I_j = \frac{d}{N} f_j \otimes f_j^\dagger \}$ forms a POVM. Similarly, one may construct a unit norm tight frame from any POVM [20].

Renes’ four-state protocol [6] employs a four-element ETF $(f_j)_{j=1}^{4}$ for $\mathbb{C}^2$ with $|\langle f_j, f_k \rangle|^2 = \frac{1}{4}$, $j \neq k$. The corresponding POVM is known as a symmetric, informationally complete POVM (SIC-POVM). In general, if $N = d^2$ and $(f_j)_{j=1}^{d^2}$ forms an ETF for $\mathbb{C}^d$, then the corresponding POVM is a SIC-POVM. The existence of such ensembles in all dimensions is an open problem in harmonic analysis and quantum information theory, respectively. Nonetheless, for every dimension $d \geq 2$ there exists an ETF of $d + 1$ vectors in $\mathbb{C}^d$ obtained by taking any $d$ rows of the $(d + 1) \times (d + 1)$ discrete Fourier transform (DFT) matrix and renormalizing the resulting column vectors. In the sequel, we shall consider the ETF obtained by taking the last $d$ rows of the $(d + 1) \times (d + 1)$ DFT matrix. We call this ETF the $(d + 1, d)$ Fourier ETF, or simply the Fourier ETF when the context is clear. More generally, using a difference set sampling strategy, the class of harmonic equiangular tight frames may be constructed (see [21]).

Both the three-state and four-state quantum key algorithms rely on a measurement ensemble generated by a companion ETF $(g_j)_{j=1}^{4}$ defined as follows: given an ETF $F = (f_j)_{j=1}^{N}$, the ETF $G = (g_j)_{j=1}^{N}$ is a companion ETF for $F$ if

$$|\langle g_j, f_l \rangle|^2 = \begin{cases} 0 & k = j \\ \frac{N}{N} & \text{otherwise} \end{cases}.$$  \hspace{1cm} (1)

Much like the existence of equiangular frames, the construction of such sets is a non-trivial problem. In this paper we offer constructions of companion equiangular tight frames to the $(d + 1, d)$ Fourier ETF for a family of values of $d$. We then extend the equiangular QKD algorithms to these dimensions, and illustrate our algorithms with some examples.

For completeness, we recall the setup of the equiangular QKD protocol. Assume that Alice and Bob wish to communicate securely and have access to a quantum channel as well as a classical one. Alice and Bob predetermine an equiangular frame set of states $(f_j)_{j=1}^{N}$ from which Alice uniformly samples from the $N$ states and picks out $f_l$, which she sends to Bob.

Bob has a measurement device corresponding to the POVM $\{ G_j = \frac{d}{N} g_j \otimes g_j^\dagger \}_{j=1}^{N}$, where $(g_j)_{j=1}^{N}$ is a companion equiangular frame for $(f_j)_{j=1}^{N}$. Bob receives $f_l$ from Alice and performs a measurement with outcome $l \in \{ 1, \ldots, N \}$. Now Bob knows with certainty that Alice did not send $f_l$, as the probability of measuring $l$ given $f_l$ is $|\langle g_l, f_l \rangle|^2 = 0$. However, Bob knows nothing about which of the other $N - 2$ possible states might have been sent. To determine this, Bob then communicates a random sampling $S$ of $N - 2$ elements of $\{ 1, \ldots, N \} \setminus \{ l \}$ without replacement. He sends the sample $S$ to Alice through a classical channel. If $k \in S$, then Alice
signals failure and sends a new quantum state. If \( k \not\in S \) (which has a probability \( \frac{1}{N-1} \) of happening) then Alice and Bob both know that Alice sent state \( k \), while anyone viewing the classical communication only knows that Alice sent either \( f_0 \) or \( f_1 \). Alice and Bob generate a random classical bit based on an \textit{a priori} algorithm that has been agreed upon (say \( b = 1 \) if \( -1)^j = 1 \) and \( b = 0 \) otherwise). Based on eavesdropping of the classical channel, an eavesdropper Eve has at best a \( 2^{-t} \) probability of guessing the correct bit number \( k \) based on complete knowledge of the classical communications, which would presumably have some sort of classical encryption. Similarly, an intercept and resend attack on the quantum channel would quickly be detected, as Alice and Bob’s keys would not match with arbitrarily high probability.

Before the difficulty of experimental implementation, there is the non-trivial task of generating equiangular frames and the associated companion set. In \( \mathbb{C}^2 \), the geometric representation of the Bloch sphere was used in order to construct such sets \([4, 5]\). However, this type of geometric construction seems absent in higher dimensions. Nonetheless we shall construct a family of companion ETFs starting from some \((d + 1, d)\) Fourier ETFs.

We demonstrate later that when \( d + 1 \) is any odd prime, a \((d + 1, d)\) Fourier ETF \( F = \{f_j\}_{j=1}^{d+1} \) for \( \mathbb{C}^d \) and a \( d \times d \) diagonal unitary and traceless matrix \( U \) exist such that

\[
G = \{g_j | g_j = Uf_j, j = 1, ..., d + 1\}
\]

is a companion equiangular frame for \( F \).

This is easily accomplished in two dimensions using the Bloch sphere representation, doing a three-dimensional rotation within that representation and mapping back to \( \mathbb{C}^2 \). For example, let \( f_j = \frac{1}{\sqrt{2}} \left[1 \ e^{i\pi/3}\right]^* \) for \( j = 0, 1, 2 \). Then the transformation

\[
R = \begin{bmatrix}
1 & 0 \\
0 & e^{i\pi}
\end{bmatrix},
\]

which amounts to a 180 degree rotation in the \( xy \) plane in the Bloch sphere, accomplishes the desired result:

\[
|\langle Rf_j, f_k \rangle|^2 = \begin{cases}
0 & j = k \\
\frac{1}{4} & j \neq k
\end{cases}. \tag{2}
\]

If \( F = \{f_j\}_{j=1}^N \) is an ETF for \( \mathbb{C}^d \) and if there exists a companion ETF \( G = \{g_j = Uf_j\}_{j=1}^N \) for some unitary \( d \times d \) matrix \( U \), then we may proceed in generalizing Renes’ protocol. In particular, the common inner product of \( F \) (hence of \( G \)) is

\[
\alpha = \frac{d}{dN - 1}.
\]

The frame operators of \( F \) and \( G \) are also identical, and equal \( N/d \times d \). Hence we may define a POVM associated with each frame as \( G_j = \frac{d}{\parallel g_j \parallel^2} g_j g_j^* \) and \( F_j = \frac{d}{\parallel f_j \parallel^2} f_j f_j^* \).

Suppose Alice prepares a state \( f_k \) and sends it to Bob. If Bob then measures using the \( G_j \)s then the probability of measuring outcome \( j \) in an experiment is given by

\[
Pr(j | f_k) = \text{tr}(G_j f_k f_k^*) = \text{tr}(f_k^* G_j f_k) = \frac{d}{N} \langle g_j, f_k \rangle \langle f_k, g_j \rangle = \frac{d}{N} |\langle g_j, f_k \rangle|^2. \tag{3}
\]

Now, using the fact that the \( f_j \)s form an \( N/d \) tight frame, that \( g_j \) has a unit norm and that the sets satisfy equation (1), we have for \( j \neq k \)

\[
|\langle g_j, f_k \rangle|^2 = \frac{1}{N-1} \sum_{k \neq j=1}^N |\langle g_j, f_k \rangle|^2 = \frac{N}{d(N-1)} ||g_j||^2 = \frac{N}{d(N-1)}.
\]

Combining this with equation (3) yields
pr(j|fi) = \begin{cases} 0 & j = k \\ \frac{1}{\sqrt{N}} & j \neq k \end{cases}

Hence, for a fixed measurement outcome j, there is an equal probability that the state being measured was fi for k ≠ j and no probability that the state was fj.

In some cases there might not exist a unitary matrix U that would produce a companion ETF G = {U fj}N j=1 from an ETF F = {fj}N j=1 for Cd. Indeed, Renes also has a four-element equiangular frame given by

\[
F = \begin{bmatrix}
\alpha & \alpha & \beta & \beta \\
\beta & -i\beta & \alpha & \alpha
\end{bmatrix}
\]

where \(\alpha = \sqrt{\frac{1}{5}(3 + \sqrt{3})}\) and \(\beta = \sqrt{\frac{1}{5}(3 - \sqrt{3})}\). Let

\[
U = \begin{bmatrix}
a & b \\
c & d
\end{bmatrix}
\]

be unitary. Then solving \(\text{diag}(F^*UF) = [0, 0, 0, 0]\) non-trivially is actually impossible as it requires b = c which implies a = d = 0 which implies b = -c or a similar contradiction. Therefore, no unitary U exists such that a \(g_j = Uf_j\) exists that satisfies (1). However, if we set a = d = 0 and b = c = 1 then \(g_j = Uf_j\) for \(j = 1, 2\) and \(g_3 = Uf_4\) and \(g_4 = Uf_3\) then \(g_j\) and \(f_j\) satisfy (1). One can ask whether such a unitary transformation (up to re-indexing) exists for higher dimensions. If it does, then we can generalize the two-dimensional results from Renes to arbitrary higher finite dimensions. Namely, if such an R works in dimension d, we would have \(g_j = Rf_j\) in (1) and our measurement operators would be scaled versions of \(g_jg_j^*\). Therefore, a companion ETF can be constructed if one can find a unitary transformation U and a permutation matrix P such that \(G = UFP\) where F is the matrix synthesis operator of the initial frame and \(G = [g_1, g_2, ..., g_N]\) is the synthesis operator for the desired new frame. Hence, (1) may be reformulated as

\[
|\langle G^*PFU\rangle_{ij}|^2 = |\langle P^*FU^*G\rangle_{ij}|^2 = \begin{cases} 0 & i = j \\ \frac{1}{c} & \text{o.w.} \end{cases}
\]

The main goal of this paper is to construct companion ETF from the \(d + 1\) Fourier ETF when \(d + 1\) is prime. This is achieved by constructing a \(d \times d\) traceless diagonal matrix of \(\pm 1\). Let \(\tilde{u} \in C^d\) be the vector of \(\pm 1\) consisting of the diagonal entries of U, and \(u = \begin{bmatrix} 0 \\ u \end{bmatrix} \in C^{d+1}\). Then u is an eigenvector of W, the \((d + 1) \times (d + 1)\) DFT matrix. We conjecture that every unitary diagonal traceless matrix U yielding a companion ETF to the \((d + 1, d)\) Fourier ETF necessarily generates either an eigenvector of the DFT matrix, as described above, or a vector u such that \(Wu = \lambda u^*\) for some unimodular number \(\lambda\). We have not been able to prove this conjecture, but through exhaustive search we observed that there indeed exists such a vector for all prime numbers up to 59. Furthermore, our numerical search shows that no such eigenvector exists for composite numbers in this range.

2. Companion ETF in prime dimensions

As mentioned in the introduction, starting from the ETF \(\{f_k\}_{k=0}^2 \subset C^2\), it is known that the family \(\{Rf_k\}_{k=0}^2\) is a companion ETF where \(R = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\). Note that R is unitary and...
traceless. One is naturally led to ask if, given a FUNTF \( \{ f_k \}_{k=1}^N \subset \mathbb{C}^d \), can one find a unitary traceless \( d \times d \) matrix \( U \) such that \( \{ f_k \}_{k=1}^N \) and \( \{ U f_k \}_{k=1}^N \) are companion ETFs.

Before we answer this question in some special cases, we note that if \( \{ f_k \}_{k=1}^N \) is an equiangular FUNTF for \( \mathbb{C}^d \), the set of \( N^2 d \times d \) matrices defined by \( \{ f_j \otimes f_k \}_{j,k=1}^N \) forms a two-distance tight frame for \( \mathbb{C}^{d \times d} \) under the Hilbert–Schmidt inner product, \([22]\).

**Proposition 1.** Suppose that \( \{ f_j \}_{j=1}^N \) is an equiangular FUNTF for \( \mathbb{C}^d \). Then

\[
\{ f_j \otimes f_k \}_{j,k=1}^N = \{ f_k^* f_j \}_{j,k=1}^N
\]

is a two-distance FUNTF for \( \mathbb{C}^{d \times d} \) under the Hilbert–Schmidt inner product.

**Proof.** We have from the properties of the tensor product that

\[
\langle f_m \otimes f_n, f_j \otimes f_l \rangle_{\text{HS}} = \langle f_m, f_j \rangle \langle f_n, f_l \rangle.
\]

Since \( \langle f_j, f_k \rangle^2 = \alpha = \frac{N-1}{d(N-1)} \) for all \( j \neq k \), we have that

\[
\big| \langle f_m \otimes f_n, f_j \otimes f_l \rangle_{\text{HS}} \big|^2 = \begin{cases} 
1 & m = j, l = n \\
\alpha & m = j, l \neq n \\
\alpha & m \neq j, l = n \\
\alpha^2 & m \neq j, l \neq n
\end{cases}
\]

So we have a unit normed two-distance (in absolute value) set (distances \( \alpha \) and \( \alpha^2 \)) with \( \alpha \) occurring \( 2(N^2)(N-1) \) times and \( \alpha^2 \) occurring \( N^2(N-1)^2 \) times. To show tightness, let \( M \in \mathbb{C}^{d \times d} \) be arbitrary. We have

\[
\sum_j \sum_k |\langle M, f_j^* M_k \rangle_{\text{HS}}|^2 = \sum_j \sum_k |\text{tr}(f_j^* M_k)|^2 = \sum_j \sum_k |\langle M f_j, f_k \rangle|^2 = \frac{N}{d} \sum_k \|M_k\|^2.
\]

We also have for \( M^* = [M_1, \ldots, M_d] \) that \( \|M_k\|^2 = \sum_j |\langle f_k, M_j \rangle|^2 \) and therefore

\[
\sum_k \|M_k\|^2 = \sum_j \sum_k |\langle f_j, M_k \rangle|^2 = \sum_j \frac{N}{d} \|M_j\|^2
\]

\[
= \frac{N}{d} \sum_j \|M_j\|^2 = N \|M\|_{\text{HS}}^2.
\]

Plugging into (4) shows that \( \{ f_j \otimes f_k \}_{j,k \in \{1, \ldots, N\}} \) is a \( N^2/d^2 \) tight frame for \( \mathbb{C}^{d \times d} \). \( \square \)

Proposition 1 can be used as follows. If \( F = \{ f_j \}_{j=1}^N \) is an ETF for \( \mathbb{C}^d \), then to find a unitary \( d \times d \) matrix \( U \) such that \( G = \{ g_j = U f_j \}_{j=1}^N \) is a companion ETF to \( F \) reduces to finding the coefficients \( (\langle U f_j \otimes f_l \rangle_{\text{HS}})^N_{j,l=1} \). However,

\[
\langle U f_j \otimes f_l \rangle_{\text{HS}} = \text{tr}(U f^*_j f_l) = \text{tr}(f_j^* U f_l) = \langle U f_j, f_l \rangle = \langle g_j, f_l \rangle = \sqrt{\alpha} e^{2 \pi i \theta_{lj}}
\]

where \( \alpha = \frac{N-1}{d(N-1)} \) and \( \theta_{lj} \in [0, 1) \) is an unknown phase factor. Thus, determining \( U \) is equivalent to finding these unknown phases. This is an example of the non-trivial phase retrieval problem (see [23] and the references therein for more details). From a complexity point of view, \( U \) belongs to the \( d^2 \) dimensional space \( \mathbb{C}^{d \times d} \) for which \( \{ f_j \otimes f_k \}_{j,k=1}^N = \{ f_k^* f_j \}_{j,k=1}^N \) is a
two-distance FUNTF of $N^2$ vectors. The right regime to recover $U$ from only the magnitudes of its frame coefficients is $N^2 > d^4$, i.e. $N > d^2$. But as we shall see, the results we obtain are for $N = d + 1$. Consequently, our results are not covered by the phaseless reconstruction theory.

Because of the complexity of the problem, we seek a unitary, diagonal and traceless $d \times d$ matrix that would produce a companion ETF from an ETF $F$. In particular, we shall only consider the case where $F$ is the $(d + 1, d)$ Fourier ETF, and show that finding such diagonal unitary matrix reduces to finding a specific eigenvector of the DFT matrix.

2.1. Construction of companion FUNTFs in prime dimensions

Let $d \geq 2$ be fixed and set $\omega = e^{-\frac{2\pi i}{d}}$. Suppose that $F = \{f_k\}_{k=1}^{d+1}$ is a $(d + 1, d)$ Fourier ETF for $\mathbb{C}^d$ generated by taking the columns of the $(d + 1)$-dimensional DFT matrix, removing the top row and scaling by $\frac{1}{\sqrt{d}}$. Let $v[k]$ denote the $k$th entry in the vector $v$, starting with 0 (so $v[0]$ is the leading entry). Assume there exists a traceless, diagonal, unitary $d \times d$ matrix $U$ such that $\langle (Uf_k, f_j) \rangle = \begin{cases} 0 & k = j \\ c & \text{o.w.} \end{cases}$. We recall that $c = \frac{\sqrt{d} \pi}{d}$, and we have for $k \neq j$ that

$$|\langle Uf_k, f_j \rangle| = \left| \sum_{n=1}^{d} (Uf_k)[n] - 1 [f_j[n] - 1] \right| = \frac{1}{d} \left| \sum_{n=1}^{d} U_{n,0} \omega^{nk} \right| = \frac{1}{d} \sqrt{d+1},$$

where $\ell = k - j \neq 0$. Hence, if we denote the diagonal $D$ of $U$ as $D = \begin{pmatrix} U_{1,1} \\ \vdots \\ U_{d,d} \end{pmatrix}$ and embed $D$ in $\mathbb{C}^{d+1}$ via the mapping

$$D \mapsto \begin{bmatrix} 0 \\ D \end{bmatrix} = f,$$

then (5) implies that for $\ell \neq 0$

$$|\hat{f}[\ell]| = \frac{1}{\sqrt{d+1}} \sum_{n=0}^{d} \omega^{n\ell} f[n] = \frac{1}{\sqrt{d+1}} \left| \sum_{n=1}^{d} U_{n,0} \omega^{n\ell} \right| = 1,$$

where $\hat{f}$ is the $(d + 1)$ DFT of $f$. Since $U$ is unitary, we have that $|f[j]| = 1$ for $j \neq 0$. Furthermore, the traceless condition on $U$ implies that $\hat{f}[0] = f[0] = 0$. Thus the vector $f$ and its DFT $\hat{f}$ have unimodular entries except for their first entry which is 0. Because the eigenvalues of the $(d + 1 \times d + 1)$ DFT matrix are $\pm 1$, $\pm i$, it is clear that the corresponding eigenvectors $u$ have the property that $|u[k]| = |u[k]|$ for $k = 0, \ldots, d$. Therefore, if we find a function of the form of $f$ that is an eigenfunction of the ($(d + 1) \times (d + 1)$) DFT, then the lower $d$ unit modulus entries of $f$ define a traceless, diagonal, unitary transformation that generates a companion ETF for $\{f_k\}_{k=1}^{d+1}$. The following construction of such an eigenvector is given in [24], when $d + 1 = p$ is a prime odd number. In the sequel we denote the $p \times p$ DFT matrix by $W$. We refer to [24] for a proof.
Proposition 2. Define $f \in \mathbb{C}^p$ by
\[ f = \left[ 0, \left( \frac{1}{p} \right)_2, \left( \frac{2}{p} \right)_2, \ldots, \left( \frac{k}{p} \right)_2, \ldots, \left( \frac{p-1}{p} \right)_2 \right]^* \]
where $\left( \frac{n}{p} \right)_2$ is the Legendre symbol, defined by
\[ \left( \frac{n}{p} \right)_2 = \begin{cases} 1 & \text{if } n \text{ is a quadratic residue modulo } p \\ -1 & \text{if } n \text{ is not a quadratic residue modulo } p \end{cases} \]
for $1 \leq n \leq p - 1$. Then $f$ is an eigenvector of $W$. Furthermore, when $p \equiv 1 \pmod{4}$, the eigenvalue for this vector is 1, and when $p \equiv 3 \pmod{4}$, the eigenvalue is $-i$.

In fact, our main result shows that this is the only eigenvector of the form $[0, \pm 1, \pm 1, \ldots, \pm 1]^*$ for $W$. More specifically,

Theorem 3. If $u_1, u_2$ are eigenvectors of $W$ of the form $[0, 1, \pm 1, \ldots, \pm 1]^*$, then $u_1 = u_2$.

The proof of this result is based on the following lemmas, which we first prove. For simplicity, and without loss of generality, the following proofs standardize the vectors by assuming that the first non-zero entry is $+1$.

Lemma 4. If $u_1, u_2$ are distinct vectors of the form $[0, 1, \pm 1, \ldots, \pm 1]^*$ such that $Wu_1 = \lambda_1 u_1$ and $Wu_2 = \lambda_2 u_2$, then $\lambda_1 \neq \pm \lambda_2$.

Proof. Assume for the sake of contradiction that $\lambda_1 = \lambda_2$. (The $\lambda_1 = -\lambda_2$ case is shown similarly.)

From the first row of $W$,
\[ u_1[1] + u_1[2] + u_1[3] + \cdots + u_1[p-1] = 0 \]
and
\[ u_2[1] + u_2[2] + u_2[3] + \cdots + u_2[p-1] = 0. \]
Define $v[k] = (u_1[k] - u_2[k])/2$ for $1 \leq k \leq p - 1$. Then by subtracting the second equation from the first and dividing by 2,
\[ v[1] + v[2] + v[3] + \cdots + v[p-1] = 0. \] (7)

From the second row of $W$,
\[ u_1[1] + u_1[2] + u_1[3] + \cdots + u_1[p-1] + u_1[p-1] = \lambda_1 \]
and
\[ u_2[1] + u_2[2] + u_2[3] + \cdots + u_2[p-1] = \lambda_2. \]
By subtracting the second equation from the first and dividing by 2,
\[ v[1] + v[2] + v[3] + \cdots + v[p-1] = 0. \] (8)
Let \( A = \{ k : v[k] = 1, 1 \leq k \leq p - 1 \}, \quad B = \{ k : v[k] = -1, 1 \leq k \leq p - 1 \}, \) and \( C = \{ 0, 1, 2, \cdots, p - 1 \} \setminus B \). By a basic property of roots of unity,
\[
\sum_{k \in B} \omega^k + \sum_{k \in C} \omega^k = 0.
\]
Equation (8) can be written as
\[
\sum_{k \in A} \omega^k - \sum_{k \in B} \omega^k = 0.
\]
Combining the two equations above,
\[
\sum_{k \in A} \omega^k + \sum_{k \in C} \omega^k = 0. \tag{9}
\]
Equation (7) implies that \(|A| = |B|\). Then \(|A| + |C| = |A| + p - |B| = |A| + p - |A| = p\). Note that \(A\) and \(B\) are disjoint, so \(A\) and \(C\) are not. Thus, (9) is a vanishing asymmetric sum of \(p\) \(p\)th roots of unity. However, this is not possible by [25, theorem 3.3], raising a contradiction. Therefore, \(\lambda_1 \neq \lambda_2\).

**Lemma 5.** If \(u_1, u_2\) are distinct vectors of the form \([0, 1, \pm 1, \cdots, \pm 1]^t\) such that \(Wu_1 = \lambda_1 u_1\) and \(Wu_2 = \lambda_2 u_2\), then \(\lambda_1 \neq \pm i \lambda_2\).

**Proof.** Assume for the sake of contradiction that \(\lambda_1 = i \lambda_2\). (The \(\lambda_1 = -i \lambda_2\) case is shown similarly.)

From the second row of \(W\),
\[
u_1[1] \omega + u_1[2] \omega^2 + u_1[3] \omega^3 + \cdots + u_1[p - 1] \omega^{p - 1} = u_1[1] \lambda_1 = \lambda_1
\]
and
\[
u_2[1] \omega + u_2[2] \omega^2 + u_2[3] \omega^3 + \cdots + u_2[p - 1] \omega^{p - 1} = u_2[1] \lambda_2 = \lambda_2 = -i \lambda_1.
\]
Let \(A_1 = \{ k : v[k] = 1, 1 \leq k \leq p - 1 \}, \quad B_1 = \{ k : v[k] = -1, 1 \leq k \leq p - 1 \}, \) and \(C_1 = \{ 0, 1, 2, \cdots, p - 1 \} \setminus B\). Then \(|A_1| + |C_1| = p\), and by following the process in lemma 4,
\[
\sum_{k \in A_1} \omega^k + \sum_{k \in C_1} \omega^k = \lambda_1.
\]
Similarly, by letting
\(A_2 = \{ k : u_2[k] = 1, 1 \leq k \leq p - 1 \}, \quad B_2 = \{ k : u_2[k] = -1, 1 \leq k \leq p - 1 \}, \) and \(C_2 = \{ 0, 1, 2, \cdots, p - 1 \} \setminus B\), it follows that \(|A_2| + |C_2| = p\) and
\[
\sum_{k \in A_2} \omega^k + \sum_{k \in C_2} \omega^k = -i \lambda_1.
\]
Let \(\omega_0 = e^{\frac{2 \pi i}{p}}\), so \(\omega_0^p = 1\). Then the previous two equations are equivalent to
\[
\sum_{k \in A_1} \omega_0^{dk} + \sum_{k \in C_1} \omega_0^{dk} = \lambda_1 \tag{10}
\]
and
\[ \sum_{k \in A_2} \omega_0^{4k} + \sum_{k \in C_2} \omega_0^{4k} = -i \lambda_1, \]
respectively. Multiplying the second equation by \( -i = e^{-\frac{\pi i}{2}} = \omega_0^p \),
\[ \sum_{k \in A_2} \omega_0^{4k+p} + \sum_{k \in C_2} \omega_0^{4k+p} = -\lambda_1. \] (11)

Adding (10) and (11),
\[ \sum_{k \in A_1} \omega_0^{4k} + \sum_{k \in C_1} \omega_0^{4k} + \sum_{k \in A_2} \omega_0^{4k+p} + \sum_{k \in C_2} \omega_0^{4k+p} = 0. \] (12)

This is a sum of \( 2p \) 4th roots of unity. Since \( p \) is an odd prime, it follows from [25, theorem 3.3] that such a sum must be one of:

- \( p \) symmetric sums of two 4th roots of unity, or
- two symmetric sums of \( p \) 4th roots of unity.

We now show that both of these are impossible.

Choose any \( k \) in \( A_1 \cup C_1 \). Since \( p \) is odd, \( k + \frac{p}{2} \) cannot be in \( A_1 \cup C_1 \) and \( k + \frac{p}{4} \) cannot be in \( A_2 \cup C_2 \), so \( \omega^{4k} \) is in the sum but \( -\omega^{4k} = \omega^{4k+2p} \) is not. Thus, the sum cannot consist of \( p \) symmetric sums of two 4th roots of unity.

Since \( |A_1| + |C_1| = p \) and \( A_1 \) and \( C_1 \) are not disjoint, the sum in equation (10) is not a symmetric sum of \( p \) roots of unity. However, every term in this sum is a \( p \)th root of unity, while no term in (11) is a \( p \)th root of unity. Thus, the sum in (12) cannot consist of two symmetric sums of \( p \) 4th roots of unity.

The sum in (12) is neither \( p \) symmetric sums of two 4th roots of unity nor two symmetric sums of \( p \) 4th roots of unity, which gives the desired contradiction. Therefore, \( \lambda_1 \neq i \lambda_2 \). □

We are now ready to prove theorem 3.

**Proof of theorem 3.** Let \( W_{u_1} = \lambda_1 u_1 \) and \( W_{u_2} = \lambda_2 u_2 \). Since the only eigenvalues of the DFT are \( 1, -1, i, \) and \( -i \), either \( \lambda_1 = \pm \lambda_2 \) or \( \lambda_1 = \pm i \lambda_2 \). If \( u_1 \neq u_2 \), then these are both impossible according to lemmas 4 and 5. Therefore, \( u_1 = u_2 \). □

Using this construction, an ETF \( F = \{f_j\}_{j=1}^N \) for \( C^{N-1} \) along with a companion frame \( G \) can be constructed for any prime \( N = p + 1 \). In particular, the companion frame satisfies
\[ G = \{ g_j | g_j = U f_j, j = 1, ..., N \} \]
where \( U \) is the \( (N-1) \times (N-1) \) matrix whose diagonal entries are the lower \( N-1 \) entries in \( f \).

By an exhaustive computational search, the existence and uniqueness of the eigenvector in the above construction was verified for all primes up to 59. Interestingly, the search yielded no eigenvectors of the form \([0, \pm 1, \pm 1, \cdots, \pm 1]^*\) for composite \( N \) up to this same value, and we conjecture that no such eigenvector exists for any composite \( N \). While this fact is evident if \( N \) is even (one need simply consider the first row of the DFT), a full proof of this fact is not forthcoming.
Example 6. We provide a few examples of the construction above. We construct an ETF \( \{f_j\}_{j=1}^4 \) in \( \mathbb{C}^4 \) by sampling the \( 5 \times 5 \) DFT matrix. Indeed, we have

\[
\text{DFT} = \frac{1}{\sqrt{5}} \begin{bmatrix}
1 & 1 & 1 & 1 & 1 \\
1 & \omega & \omega^2 & \omega^3 & \omega^4 \\
1 & \omega^2 & \omega^4 & \omega & \omega^3 \\
1 & \omega^3 & \omega^4 & \omega^2 & \omega \\
1 & \omega^4 & \omega^3 & \omega^2 & \omega
\end{bmatrix},
\]

and

\[
P = \begin{bmatrix}
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1
\end{bmatrix},
\]

and we set \( f_j \) equal to the \( j \)th column of \( \frac{1}{\sqrt{5}} P \ast \text{DFT} \). Define \( g_j = U f_j \) for \( j = 1, \ldots, 5 \) where

\[
U = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 \\
0 & 0 & -1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}.
\]

Then we have \( \langle g_j, f_l \rangle = 1 - 1 - 1 + 1 = 0 \) and \(|\langle g_k, f_l \rangle|^2 = \frac{5}{16} \) for \( k \neq l \). Hence, \( \{g_j\}_{j=1}^4 \) is a companion equiangular frame for \( \{f_j\}_{j=1}^4 \).

Similarly, sampling the \( 7 \times 7 \) DFT matrix and employing \( U = \text{diag}[1, 1, -1, 1, -1, -1] \) generates an equiangular harmonic frame and a companion equiangular frame for \( \mathbb{C}^6 \), where \( \langle g_l, f_l \rangle = 1 + 1 - 1 - 1 - 1 = 0 \) and \(|\langle g_k, f_l \rangle|^2 = \frac{7}{36} \) for \( k \neq l \).

Remark 7. When \( p \equiv 1 \text{ mod } 4 \) is prime, \([24]\) provides a second construction which satisfies the criteria for \( f \). The vector is

\[
f = \left[ 0, \left( \frac{1}{p} \right)_4, \left( \frac{2}{p} \right)_4, \ldots, \left( \frac{k}{p} \right)_4, \ldots, \left( \frac{p-1}{p} \right)_4 \right]^*\]

where \( \left( \frac{n}{p} \right)_4 \) is defined by

\[
\left( \frac{n}{p} \right)_4 = \begin{cases}
1 & \text{if } n^{(p-1)/4} \equiv 1 \text{ mod } p \\
i & \text{if } n^{(p-1)/4} \equiv c \text{ mod } p \\
-1 & \text{if } n^{(p-1)/4} \equiv c^2 \equiv -1 \text{ mod } p \\
-i & \text{if } n^{(p-1)/4} \equiv c^3 \equiv -c \text{ mod } p
\end{cases}.
\]

Here, \( c \) is defined as a primitive fourth root of unity in the multiplicative group of integers mod \( p \), i.e. an integer \( c \) such that \( c^2 \equiv -1 \text{ mod } p \).

While this \( f \) is not an eigenvector of the DFT, it still satisfies the property that each entry except for the first has magnitude 1 and that the magnitude of each entry remains fixed under the DFT. In particular, there exists a complex constant \( z \) of magnitude 1 such that \( Wf = z f \).

Thus, as in the previous construction, this vector \( f \) can be used to construct a diagonal matrix \( U \) which generates a companion frame.
As an example of this construction, sampling the \(5 \times 5\) DFT matrix and employing \(U = \text{diag}[1, i, -i, -1]\) generates an equiangular harmonic frame and a companion equiangular frame for \(C^4\), where \(|\langle g_i,f_i \rangle| = 1 + i - i - 1 = 0\) and \(|\langle g_k,f_i \rangle|^2 = \frac{2}{16}\) for \(k \neq l\).

In fact, as a generalization of the above constructions, if \(p\) is a prime number congruent to \(1 \mod m\), then we define the vector

\[
f = \left[0, \frac{1}{p}, \frac{2}{p}, \ldots, \frac{k}{p}, \ldots, \frac{p-1}{p}\right]^*
\]

where \(\left(\frac{n}{p}\right)_m\) is defined by

\[
\left(\frac{n}{p}\right)_m = \begin{cases} 
1 & \text{if } n^{(p-1)/m} \equiv 1 \mod p \\
\zeta & \text{if } n^{(p-1)/m} \equiv c \mod p \\
\zeta^2 & \text{if } n^{(p-1)/m} \equiv c^2 \mod p \\
\zeta^3 & \text{if } n^{(p-1)/m} \equiv c^3 \mod p \\
& \vdots \\
\zeta^{m-1} & \text{if } n^{(p-1)/m} \equiv c^{m-1} \mod p
\end{cases}
\]

Here, \(\zeta\) is a primitive \(m\)th root of unity in \(C\), and \(c\) is defined as a primitive \(m\)th root of unity in the multiplicative group of integers \(\mod p\), i.e., an integer \(c\) such that \(c^m \equiv 1 \mod p\) and \(c^k \neq 1 \mod p\) for all positive integers \(k < m\).

While this \(f\) is not an eigenvector of the DFT, it still satisfies the property that each entry except for the first has magnitude 1 and that the magnitude of each entry remains fixed under the DFT. In particular, there exists a complex constant \(z\) of magnitude 1 such that \(Wf = zf\).

As an example of this construction, let \(w\) and \(w^*\) be such that \(w^2 = i\) and \((w^*)^2 = -i\). Sampling the \(17 \times 17\) DFT matrix and employing \(U = \text{diag}[1, i, -w^*, -1,w^*, w, -w, -i,-i, -w, w^*, -1, -w^*, i, 1]\) generates an equiangular harmonic frame and a companion equiangular frame for \(C^{16}\), where \(|\langle g_i,f_i \rangle| = 0\) and \(|\langle g_k,f_i \rangle|^2 = \frac{17}{256}\) for \(k \neq l\).

### 2.2. Security analysis

Here, we assume that the attacks Eve can carry out against the key distribution are of the type intercept/resend, that is, she measures a fraction of signals sent by Alice and forwards a different state to Bob. In the asymptotic limit of sample size of the qubits transmitted, the length \(R\) of the key string that can be distilled by Alice and Bob with Eve having zero information is:

\[
R = I(A : B) - \min\{I(A : E), I(B, E)\},
\]

(13)

where the quantity \(I\) refers to the mutual information between two parties that quantifies how much knowledge of one party’s outcome implies the result of the second party. The best strategy for Eve is to use Alice and Bob’s basis 50% of the time as the expression is symmetric with respect to both of them. Eve can choose only one of the bases that will increase the length of the key by breaking the symmetry. She can use a combination of the strategies to restore the symmetry and at the same time maximize the mutual information with either of the parties. It is desirable to quantify the mutual information in terms of the quantity \(q\), the fraction of the signal that Eve intercepts.

Let \(\{f_j\}_{j=1}^N\) be an equiangular FUNTF for \(C^d\), where \(N > d\), of square angle \(\alpha = |\langle f_j, f_k \rangle|^2 = \frac{k-d}{d(N-1)}, \forall j \neq k\). Suppose \(d = 2^n\). Then the space \(C^d\) can be described by \(n\)
qubits. In it, the FUNTF as defined in the introduction. Let \( \{g_j\}_{j=1}^N \) be a companion equiangular frame for \( \{f_j\}_{j=1}^N \), so \( \langle g_j, f_k \rangle^2 = \frac{\delta_{jk}}{N(N-1)} \).

Alice generates one of the states \( f_j \) with equal probability, \( \frac{1}{N} \), and sends it to Bob. He, in turn, performs a measurement obtaining an outcome \( g_k \) (\( k \neq j \)) with probability \( \frac{1}{N-1} \). He publicly announces a set of \( N-2 \) numbers \( l \neq k \). If the set does not contain \( j \), then Alice declares success, otherwise the protocol fails. Evidently, it succeeds with probability

\[
R_0 = \frac{1}{N-1}.
\] (14)

When it succeeds, Alice and Bob share the information \( (j,k) \) which is an ordered pair. By listening to Bob’s announcement, Eve knows the set \( \{j,k\} \) but she does not know the order. Therefore, Alice and Bob have generated one shared secret classical bit which is the order of \( j,k \) in the pair \( (j,k) \), say

\[
epsilon_{jk} = \begin{cases} 0, & j > k \\ 1, & j < k \end{cases}.
\] (15)

To gain advantage, Eve intercepts Alice’s signal and performs a measurement. Her outcome agrees with Alice’s signal with probability \( \frac{d}{N} \). The rest of time, she obtains one of the other \( N-1 \) states, each with probability \( \frac{N-d}{N(N-1)} \).

When Eve and Alice agree, the protocol fails with probability \( \frac{N-2}{N(N-1)} \), as in the case of no interference by Eve. When Eve disagrees with Alice, then either one of the two numbers Bob leaves out of his public announcement can match Alice’s, so the probability of failure is now \( \left(\frac{N-2}{N-1}\right)^2 \). Then the probability of Alice announcing success is

\[
R = 1 - \frac{N-2}{N-1} - \frac{N-2}{N-1}^2 \left( 1 - \frac{d}{N} \right)
= \frac{2N^2 - (d+3)N + 2d}{N(N-1)^2}
\] (16)

to be compared with the probability of success (14) without Eve’s interference. The error is

\[
\epsilon_E = \frac{R}{R_0} - 1 = \frac{(N-d)(N-2)}{N(N-1)}
\] (17)

which approaches 100% as \( N \) becomes large. This is only possible in higher-dimensional spaces \( (d \gg 1) \).

When Eve and Alice disagree, Alice can announce success even though she disagrees with Bob’s bit (a fact she is unaware of). This occurs once every \( N-1 \) times, resulting in an error. Therefore,

\[
QBER = \frac{1}{R} \left( 1 - \frac{d}{N} \right) \frac{1}{N-1}
= \frac{(N-1)(N-2)}{2N^2 - (d+3)N + 2d}.
\] (18)

Notice that QBER approaches 50% as \( N \) becomes large in higher-dimensional spaces.
Acknowledgments

GS acknowledges support from the US Office of Naval Research under award number N00014-15-1-2646.

KAO was partially supported by a grant from the Simons Foundation number 319197, and the US Army Research Office grant W911NF1610008.

ORCID iDs

Radhakrishnan Balu @ https://orcid.org/0000-0003-1494-5681
Kasso A Okoudjou @ https://orcid.org/0000-0003-4679-5534
George Siopsis @ https://orcid.org/0000-0002-1466-2772

References

[1] Bennett C H 1984 IEEE Int. Conf. on Computer System and Signal Processing pp 175–9
[2] Bruß D 1998 Phys. Rev. Lett. 81 3018
[3] Blow K and Phoenix S J 1993 J. Mod. Opt. 40 33
[4] Phoenix S J, Barnett S M and Chefles A 2000 J. Mod. Opt. 47 507
[5] Renes J M 2004 Phys. Rev. A 70 052314
[6] Renes J M 2005 Quantum Inf. Comput. 5 81
[7] Tselniker I, Nazarathy M and Orenstein M 2009 IEEE J. Sel. Top. Quantum Electron. 15 1713
[8] Chau H 2015 Phys. Rev. A 92 062324
[9] Cerf N J, Bourennane M, Karlsson A and Gisin N 2002 Phys. Rev. Lett. 88 127902
[10] Groblacher S, Jennewein T, Vaziri A, Wehner G and Zeilinger A 2006 New J. Phys. 8 17783
[11] Leach J, Bolduc E, Gauthier D and Boyd R 2012 Phys. Rev. A 85 060304
[12] Brougham T, Barnett S, McCusker K, Kwiat P and Gauthier D 2013 J. Phys. B: At. Mol. Opt. Phys. 46 104010
[13] Mower J, Zhang Z, Desjardins P, Lee C, Shapiro J and Englund D 2013 Phys. Rev. A 87 062322
[14] Mair A, Vaziri A, Wehner G and Zeilinger A 2001 Nature 412 313
[15] Brougham T and Stephen M B 2010 Phys. Rev. Lett. 104 30003
[16] Lo H K, Ma X and Chen K 2005 Phys. Rev. Lett. 89 230504
[17] Benedetto J J and Fickus M 2003 Adv. Comput. Math. 18 357
[18] Casazza P and Kutyniok G 2012 Finite Frames: Theory and Applications (Applied and Numerical Harmonic Analysis) (Boston, MA: Birkhäuser)
[19] Okoudjou K A 2016 Finite Frame Theory: a Complete Introduction to Overcompleteness (Proc. Symp. in Applied Mathematics, AMS Short Course Lecture Notes vol 73) (Providence, RI: American Mathematical Society)
[20] Benedetto J J and Kebo A 2008 J. Fourier Anal. Appl. 14 443
[21] Xia P, Zhou S and Giannakis G B 2005 IEEE Trans. Inf. Theory 51 1900
[22] Barg A, Glazyrin A, Okoudjou K A and Yu W H 2015 Linear Algebr. Appl. 475 163
[23] Balan R 2016 Finite Frame Theory: a Complete Introduction to Overcompleteness (Proc. Symp. in Applied Mathematics, AMS Short Course Lecture Notes vol 73) (Providence, RI: American Mathematical Society) pp 175–99
[24] Horn B K P 2010 Trans. R. Soc. S. Afr. 65 100
[25] Lam T Y and Leung K H 2000 J. Algebra 224 91