Equiangular quantum key distribution in more than 2 dimensions

Radhakrishnan Balu*, Paul J. Koprowski[†], and Kasso Okoudjou[‡] *Radhakrishnan.Balu.civ@mail.mil, [†]pkoprows@math.umd.edu US Army Research Laboratory, Adelphi, MD [‡]kasso@math.umd.edu

Norbert Wiener Center, University of Maryland College Park, College Park, MD

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. The first being the eigenbasis of one observable and the second basis set being the eigenbasis of one of the two sets of complimentary observables. In [3], the BB84 protocol is extended 6 states: it employs both sets of complimentary measurements. The increase in the observables allows for better adversarial eavesdropper detection [2]. In [4], [5] and [6] the authors move to the more general framework of non-orthogonal positive operator valued measures (POVMs) for qubit qkd.

There is a well established correspondance between POVMs and the elegant field of tight frames. A tight frame is a set of vectors $\{f_j\}_{j\in J}$ in H (a real or complex valued Hilbert space) such that for all $x \in H$ we have that $\sum_{j\in J} |\langle x, f_j \rangle|^2 = A ||x||^2$ for some positive constant A. If $H = \mathbb{C}^d$ and $||f_j|| = 1$, then $|J| = N < \infty$ and $A = \frac{N}{d}$. We then have

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

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

Renes' four state protocol [6] employs a four element tight frame $\{f_j\}_{j=1}^4$ for \mathbb{C}^2 that has an additional equiangualar condition (also known as mutual unbiasedness): $|\langle f_j, f_k \rangle|^2 = \frac{1}{3} \ j \neq k$. 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 equiangular tight frame 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.

Both the three state and four state quantum key algorithms rely on a measurement ensemble, generated by a companion equiangular frame $\{g_j\}$ defined as follows: given an equiangular tight frame $F = \{f_j\}_{j=1}^N$, the equiangular tight frame $\{g_j\}_{j=1}^N$ is a companion equiangular frame for F if

$$\left|\langle g_j, f_k \rangle\right|^2 = \begin{cases} 0 & k = j \\ c & o.w. \end{cases}$$

Much like the existence of equiangular frames, the construction of such sets is a non-trivial problem.

We extend equiangular QKD algorithms to arbitrary finite dimensions assuming the existence of equiangular tight frames and their companions. We give an explicit example of the generalized QKD algorithm using Fourier equiangular frames in \mathbb{C}^4 , and we discuss the difficulties in finding companion equiangular frames, given an existing equiangular frame.

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_k , 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 $\{g_j\}_{j=1}^N$. Bob receives f_k from Alice and performs a measurement with outcome $l \in \{1, ..., N\}$. Now Bob knows with certainty, 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 that might have been sent. To determine this, Bob then communicate a random sampling S of N-2elements of $\{1, ..., N\} \setminus \{l\}$ without replacement. He sends the sample S to Alice through a classical channel. If $k \in S$, then then Alice signals failure and sends a new quantum state. If $k \notin S$ (which has a probability of $\frac{1}{n-1}$ 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_k or f_l . Alice and Bob generate a random classical bit based on an a priori agreed upon algorithm (say b = 1 if $(-1)^{l} = 1$ and b = 0 otherwise). Based on eavesdropping of the classical channel, an eavesdropper Eve has at best a 2^{-k} probability of guessing the correct k bit number 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 tasks of generating equiangular frames, and the associated companion set. In \mathbb{C}^2 , Renes and Pheonix et. al. exploited the geometric representation of the Bloch sphere in order to construct such sets. In higher dimensions, no such geometric representation allows for such visual solutions. We provide an example in \mathbb{C}^4 using a Fourier equiangular frame with 5 elements.

We construct an equiangular tight frame $\{f_j\}_{j=1}^4$ by sampling the 5 × 5 discrete Fourier transform matrix (DFT). Indeed, we have

$$DFT = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega \end{bmatrix},$$

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 $\frac{1}{2}P*DFT$. It is straightforward to show that $\{f_j\}_{j=1}^4$ is an equiangular tight frame for \mathbb{C}^4 . Define $g_j = Uf_j$ for j = 1, ..., 5 where

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \sigma_z \otimes \sigma_z.$$

Then we have $\langle g_j, f_j \rangle = 1 - 1 - 1 + 1 = 0$ 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 17 × 17 DFT matrix and employing U = diag[1, 1, -1, 1, -1, -1, 1, 1, 1, -1, -1, 1, 1, 1] generates an equiangular harmonic frame and a companion equiangular frame for \mathbb{C}^{16} .

In general, given any dimension d, sampling the last d rows of the $(d+1) \times (d+1)$ discrete Fourier transform matrix, and rescaling by $\frac{1}{\sqrt{d}}$ generates an equiangular tight frame of states for \mathbb{C}^d . When d = 2, 4 or 16 we can find a diagonal, traceless matrix U with eigenvalues of ± 1 the generates a companion equiangular frame. We conjecture that such a matrix exists when $d = 2^{2^3}$ and $d = 2^{2^4}$ as d + 1 is a (Fermat) prime in both cases. However, these are the only other known cases of Fermat primes, and it is conjectured that no more exist.

Using the aforementioned construction, and using a difference set sampling strategy, the class of harmonic equiangular tight frames may be constructed (cf. [7]). Let $F\{f_j\}_{j=1}^N$ be a harmonic equiangular frame. We conjecture that unitary matrices, other than the Fermat prime case presented here, exists such that

$$G\{g_j | g_j = Uf_j \ j = 1, ...N\}$$

is a companion equiangular frame for F.

REFERENCES

- C. H. Bennett. Quantum cryptography: Public key distribution and coin tossing. In *International Conference on Computer System and Signal Processing, IEEE, 1984*, pages 175–179, 1984.
- [2] K. Blow and S. J. Phoenix. On a fundamental theorem of quantum cryptography. *Journal of Modern Optics*, 40(1):33–36, 1993.
- [3] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81(14):3018, 1998.
- [4] S. J. Phoenix, S. M. Barnett, and A. Chefles. Three-state quantum cryptography. *Journal of modern optics*, 47(2-3):507–516, 2000.
- [5] J. M. Renes. Spherical-code key-distribution protocols for qubits. *Physical Review A*, 70(5):052314, 2004.
- [6] J. M. Renes. Equiangular spherical codes in quantum cryptography. *Quantum Information & Computation*, 5(1):81–92, 2005.
- [7] P. Xia, S. Zhou, and G. B. Giannakis. Achieving the welch bound with difference sets. *Information Theory, IEEE Transactions on*, 51(5):1900–1907, 2005.