

Optimal Protocols and Tradeoffs in Quantum Key Distribution

Joseph M. Renes

*Department of Physics and Astronomy, University of New Mexico,
Albuquerque, New Mexico 87131–1156, USA*

Abstract. Quantum key distribution protocols based on equiangular spherical codes are introduced and a security comparison made to random and unbiased-bases schemes in two and three dimensions. Attention is limited to intercept/resend attacks for simplicity. In each case, a general tradeoff between eavesdropper resistance and key generation speed is observed, with the largest possible spherical code found to be the most robust, inviting the question of their optimality in general.

The possibility of secure key distribution using quantum states is by now a well established feature of quantum information theory. In the original 1984 proposal of Bennett and Brassard (BB84) [1], four states of a spin-1/2 system, the eigenstates of σ_z and of σ_x , are used as signals by the sender Alice. These states are naturally partitioned into two orthonormal bases from which the receiver Bob chooses one at random to measure the signal. Because the bases are *unbiased*—i.e., the overlap between vectors from distinct bases is always the same, equal to $1/2$ for qubits—Bob learns nothing when his measurement doesn't correspond to Alice's preparation, but everything when it does. The nonorthogonality of all the states allows Alice and Bob to detect eavesdropping by an adversary Eve, so the states form an unconditionally secure cryptographic protocol [2].

Here we introduce a new ensemble of signals, equiangular spherical codes, and make a comparison to three other protocols in terms of key generation speed and robustness to eavesdropping. These three additional protocols include the unbiased bases just discussed, as well as randomly-generated protocols, and those which are nearly spherical codes themselves, but have too many elements. The security analysis is based on the eavesdropper's use of the intercept/resend attack and, as such, doesn't provide firm proofs of security, but rather yields an insight into the general trend. We find that in this limited setting, the spherical code protocol with the most signals—equivalent to a symmetric informationally-complete POVM [8]—outperforms all others in robustness. This invites the question as to whether this specific protocol is most robust in general.

Recall the general setting of quantum key distribution. Two parties, Alice and Bob, wish to make use of an authenticated public classical broadcast channel and an insecure quantum channel controlled by an adversary Eve to establish a secret key for the purposes of encrypting and sharing other data. They start by using the classical channel to fix a signal ensemble and a measurement for the quantum channel. Alice sends states drawn from the signal ensemble through the quantum channel to Bob, who performs the chosen measurement (in the case of signaling states drawn from mutually unbiased bases, the several measurement bases Bob chooses from for his measurement are here amalgamated into a single generalized measurement). Eve is free to exploit knowledge of the protocol and her control of the quantum channel to mount an attack on their protocol; she can in principle subject the signal states to any physical interaction that she wishes. Effectively, this process produces a sequence of samples from a certain tripartite probability distribution shared between the three parties. Alice and Bob then proceed to “distill” the key by communicating information based on their individual sequences over the classical channel. Their goal is to exploit the quantum nature of the channel to make Eve's eavesdropping ineffective.

The relevant probability distribution is the joint probability $p(a_i, b_j, e_k)$ of Alice's signal, Bob's measurement result, and the result of whatever measurement Eve performs in the course of eavesdropping. Repeated use of the protocol yields a sequence of samples drawn from this distribution. Alice and Bob, however, must establish which distribution they are sampling from, as it depends on Eve's attack. We imagine Eve has some physical setup which can give rise to many different distributions as she changes the strength of her interference with the channel. Given an assumption of the type of attack, Alice and Bob determine the extent of Eve's interference by making public and comparing a

fraction of the Alice's signals and Bob's measurement results. In this way they estimate the error rate of the channel, and together with an assumption of the attack, determine the distribution p . From the remaining samples, which are supposed to be an asymptotically large number M , say, they can distill a key of length MR in accordance with the following bounds:

$$I_E \leq R \leq I(A:B|E), \quad (1)$$

where $I(X:Y) = H(X) + H(Y) - H(XY)$ is the mutual information of X and Y , $H(\cdot)$ being the Shannon entropy, and $I_E = I(A:B) - \min\{I(A:E), I(B:E)\}$. The lower bound is obtained when the key is distilled using one-way communication [3]; to progress beyond this requires a technique called *advantage distillation*, though this is of limited efficiency [4, 5].

These bounds provide a method of investigating the cryptographic usefulness of a protocol. Given a signal ensemble, Bob's measurement, and an assumption about the nature of Eve's attack, the probability distribution can be calculated, and the key rate bounds determined. In this way the security of the protocol against this attack is established. To say that a protocol is unconditionally secure is to demonstrate its security against all possible attacks.

The focus now turns to Alice's signal ensemble and Bob's measurement. An intuitively appealing ensemble is a *spherical code*, a complex-vector-space version of points on a sphere whose minimal pairwise distance is maximal. The complex version, called the *Grassmann packing problem*, asks for a set of unit vectors in \mathbb{C}^d whose *maximal* pairwise overlap is *minimal* [6]. When all these pairwise overlaps are equal, this *equiangular* spherical code (ESC) is called a *Grassmann frame*; i.e., a set $\mathcal{C} = \{|\phi_k\rangle \in \mathbb{C}^d\}_{k=1}^n$ for $n \geq d$ is a Grassmann frame if

$$|\langle \phi_j | \phi_k \rangle|^2 = \frac{n-d}{d(n-1)} \quad \forall j \neq k. \quad (2)$$

Grassmann frames also arise as the solution to the "minimum energy problem." For a set of unit vectors \mathcal{C} , call $V_t(\mathcal{C}) = \sum_{j,k} |\langle \phi_j | \phi_k \rangle|^{2t}$ the t -th order "potential energy" of the set of the vectors [7]. The minimum energy problem is to find \mathcal{C} having $n \geq d$ elements such that $V_1 = n^2/d$ and V_2 is minimized. Note that n^2/d is the global minimum of V_1 . This follows from considering the (at most) d nonzero (real) eigenvalues γ_j of the Gram matrix $G_{jk} = \langle \phi_j | \phi_k \rangle$. Clearly $\sum_k \gamma_k = n$ and $\sum_k \gamma_k^2 = V_1(\mathcal{C})$. These being the equations for a plane and a sphere, the minimum of V_1 occurs if and only if all the γ_k are equal to n/d , whence V_1 is bounded below by n^2/d . Thus what is sought is the set of vectors with the minimum V_2 energy, given minimum V_1 energy.

To find a lower bound for the minimum of V_2 , let $\lambda_{jk} = |\langle \phi_j | \phi_k \rangle|^2$, and employ the same method again. We have immediately that $\sum_{j \neq k} \lambda_{jk} = V_1 - n = n(n-d)/d$ and $\sum_{j \neq k} \lambda_{jk}^2 = V_2 - n$, whence the minimum of V_2 over all sets minimizing V_1 is bounded below by making all the λ_{jk} the same and given by Eq. (2). When this lower bound is achieved, i.e $V_2 = n^2(n-2d+d^2)/(n-1)$, the result is a Grassmann frame.

The existence of Grassmann frames isn't established for arbitrary n and d , though some general statements can be made [6, 8]. They always exist for $n = d+1$ (a regular simplex), but never when $n > d^2$. For $n \leq d^2$, when a Grassmann frame exists, it is a spherical code, but for $n > d^2$, spherical codes aren't equiangular.

Grassmann frames automatically form measurement POVMs, which can be used by Bob to detect Alice's signal. This is true because $S = \sum_k |\phi_k\rangle\langle\phi_k| = (n/d)I$, so that a POVM can be constructed from the subnormalized projectors $(d/n)|\phi_k\rangle\langle\phi_k|$. To see this, fix an orthonormal basis $\{|e_k\rangle\}$ and consider the matrix $T_{jk} = \langle e_j | \phi_k \rangle$. The Gram matrix can be written as $G_{jk} = (T^\dagger T)_{jk}$, while $S_{jk} = (TT^\dagger)_{jk}$, so both have the same eigenvalues. The d nonzero eigenvalues γ_k of G are equal to n/d by the minimization argument above.

By using the same ensemble as Alice, Bob's measurement confirms the signal she sent with probability d/n . Bob may also choose a measurement which attempts to repudiate some of Alice's signals, in a manner entirely similar to unambiguous state discrimination [9]. Because the number of states is larger than the dimension of the space on which they are supported, it is impossible to unambiguously determine the signal Alice sent with nonzero probability. However, for any ensemble, a *partial* determination may be made, a scheme which works as follows. First, partition the signal ensemble into the set of all subsets of size b . Then, for each subset, find the projector orthogonal to the span of the vectors in the subset. This procedure yields a measurement operator for each of the subsets. In order to find an orthogonal projector to the span, b must be restricted such that none of the subsets spans more than $d-1$ dimensions.

For general ensembles, the operators constructed by this procedure do not quite form a measurement; some additional "failure" outcome is required to make the entire set form a resolution of identity. Interestingly, this additional outcome appears not to be required when the signal ensemble is an equiangular spherical code. Numerical constructions starting with ESCs in modest dimensions always yields a proper POVM in which no "failure" outcome is necessary. Though both types of measurements deserve further study, we shall specialize to the case of confirmation protocols; repudiation protocols are developed for qubits in [10].

Confirmation protocols are appealing because the ESC ensembles are the sets that are “least classical” in the following sense [11]. Consider using these quantum states as signals on a *classical* channel as follows. Instead of sending the quantum state, Alice performs the associated measurement and communicates the result to Bob using a classical channel. Bob then prepares the associated quantum state at his end. The fidelity of Bob’s reconstruction with the input state, averaged over inputs and measurement results, measures how well the classical channel can be used to transmit quantum information. This fidelity is dV_2/n^2 , so among all ensembles which themselves form POVMs, Grassmann frames are hardest to transmit “cheaply” in this way. Eavesdropping on the communication between Alice and Bob makes the channel more classical—Eve is essentially trying to copy the signal—so one might expect that Grassmann frames are useful in foiling the eavesdropper.

Before making a comparison of the different signal sets, we remark on how Alice and Bob can concretely use the equiangular spherical codes to accomplish secure key distribution. Though a protocol satisfying the lower bound of equation 1 is guaranteed asymptotically, it may not be feasible in practice. Consider first the case of a noiseless quantum channel, i.e. no eavesdropping. In a length- N string of samples Alice and Bob will agree with probability d/n . When labelling the states 0 to $n - 1$, Bob’s string b is simply Alice’s string a plus a string δ having a fraction $(n-d)/n$ of non-zero elements. Alice can select a classical error-correcting code \mathcal{C} which can correct these errors, choose a codeword c randomly, and send $a + c$ to Bob. He then simply subtracts this from his string to obtain $c + \delta$, from which he uses the error-correcting property to determine the codeword c . From the Shannon noisy-channel coding theorem, there are roughly $NI(A:B)$ codewords, in accordance with the lower bound.

When Eve has no information about the quantum signals, the communicated string $a + c$ tells her nothing about c , since it’s effectively encrypted by a . Should Eve have some information about a , gleaned from her tampering with the quantum channel, Alice and Bob may proceed as before to establish c , and then use a privacy amplification procedure to shorten this string and remove any information Eve has about it.

Now we turn to comparison with three other kinds of protocols: those using unbiased bases, those using sets which minimize V_2 , but which are not equiangular spherical codes, and finally those formed from randomly-generated states. Now we restrict consideration to confirmation protocols, and in the random case, randomly-generated ensembles of states are converted into random rank-one measurements by using the “square root” or “pretty good” measurement [12]. These are then used both as signals by Alice and as Bob’s measurement, sidestepping questions about what Bob’s measurement should be when Alice uses an arbitrary ensemble. Finally, sifting of raw key strings is also not considered, purely to keep matters simple.

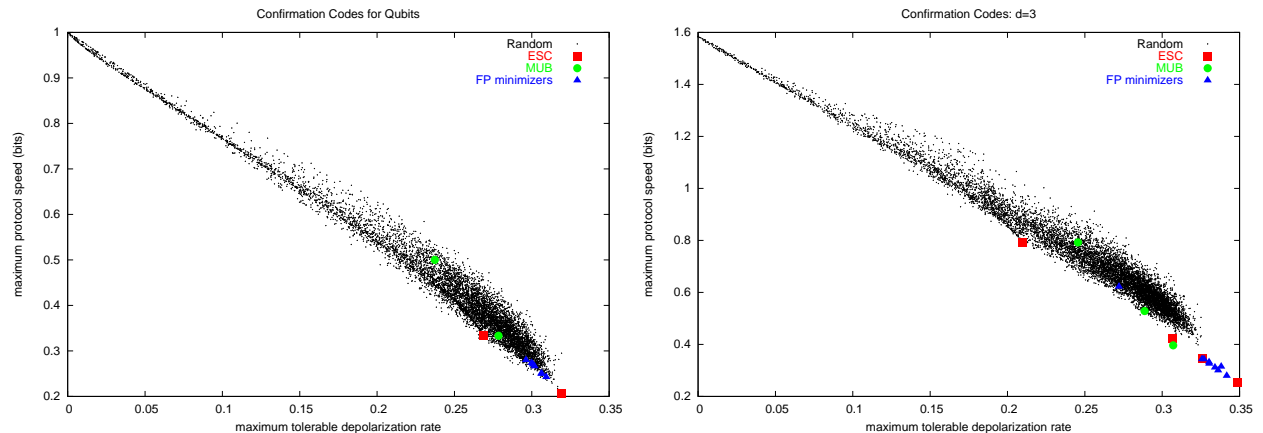


FIGURE 1. Comparison of different key distribution protocols based on maximum possible speed and maximum noise tolerance in two and three dimensions. Each protocol is a typical prepare & measure setup, the difference being in the signal set used. The key shows the four possibilities: random rank-one POVMs, equiangular spherical codes (ESC), mutually-unbiased bases (MUB), and finally second-order frame potential (FP) minimizers. The random protocols include signal sets with up to nine and 13 elements, respectively, while the frame potential minimizers include up to 12 and 16 signals, respectively. A tradeoff between speed and robustness is clear from the general trend of the random protocols, a trend which terminates with the largest ESC showing the greatest robustness and lowest speed.

To enable a proper comparison, the lower bound on the key generation rate is used to characterize the key generation abilities of each protocol; the maximum tolerable probability of eavesdropper interception is calculated from it. This intercept rate is then transformed into a channel noise rate that Alice and Bob would witness if the channel were a

depolarizing channel. From their point of view, the maximum secure noise rate is what really matters, since it is what they witness in practice. The details of this calculation may be found in [13].

However, robustness to eavesdropping is not the only desirable property of key distribution protocols; another is speed. It serves no purpose for a protocol to be very robust and at the same time operate at a snail's pace. Thus, the key generation rate in the noiseless case is calculated, and together with the robustness, these two quantities together are used to describe the abilities of each protocol.

Figure 1 shows a comparison of the four types of protocols in two and three dimensions based on these two quantities. A more or less linear tradeoff between speed and robustness is readily observed, and capping the trend in the lower right of each plot is the equiangular spherical code with d^2 elements. Moreover, already in three dimensions one may observe that the frame potential minimizers outperform random and unbiased basis protocols in robustness and are beginning to form a league of their own.

This raises the natural question of whether these protocols continue to fare so well in the setting where Eve is unconstrained, and in particular whether the symmetric informationally-complete POVM is the most robust possible within quantum cryptography. Questions of optimality are almost impossibly broad, but these results indicate a promising specific approach.

The author acknowledges helpful input from C. M. Caves, A. J. Scott, and K. K. Manne. This work was supported in part by Office of Naval Research Grant No. N00014-00-1-0578.

REFERENCES

1. C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175.
2. D. Mayers, *J. Assoc. Comput. Mach.* **48**, 351 (2001).
3. I. Csiszár and J. Körner, *IEEE Trans. Inf. Theory*, **IT-24**, 339 (1978).
4. U. M. Maurer, *IEEE Trans. Inf. Th.* **39**, 733 (1993).
5. N. Gisin and S. Wolf, *Phys. Rev. Lett.* **83**, 4200 (1999).
6. T. Strohmer and R. Heath, *Appl. Comp. Harm. Anal.* **14**, 257 (2003).
7. J. J. Benedetto and M. Fickus, *Adv. Comput. Math.* **18**, 357 (2003).
8. J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, *J. Math. Phys.* **45**, 2171 (2004).
9. A. Chefles, *Phys. Lett. A* **239**, 339 (1998).
10. J. M. Renes, quant-ph/0402135. Submitted to *Phys. Rev. A*.
11. C. A. Fuchs and M. Sasaki, *Quant. Info. Comp.* **3**, 377 (2003).
12. P. Hausladen and W. K. Wootters, *J. Mod. Opt.* **41**, 2385 (1994).
13. J. M. Renes, quant-ph/0409043. Submitted to *Quant. Info. Comp.*