Reliability of Calderbank–Shor–Steane codes and security of quantum key distribution

2004 J. Phys. A: Math. Gen. 37 8303

(http://iopscience.iop.org/0305-4470/37/34/009)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **37** (2004) 8303–8328 PII: S0305-4470(04)78124-X

Reliability of Calderbank–Shor–Steane codes and security of quantum key distribution

Mitsuru Hamada

Quantum Computation and Information Project, ERATO Program, Japan Science and Technology Agency, 5-28-3, Hongo, Bunkyo-ku, Tokyo 113-0033, Japan

E-mail: mitsuru@ieee.org

Received 22 March 2004, in final form 12 July 2004
Published 11 August 2004
Online at stacks.iop.org/JPhysA/37/8303
doi:10.1088/0305-4470/37/34/009

Abstract

After Mayers (1996 *Advances in Cryptography: Proc. Crypto'96* pp 343–57; 2001 *J. Assoc. Comput. Mach.* **48** 351–406) gave a proof of the security of the Bennett–Brassard (1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India)* pp 175–9) (BB84) quantum key distribution protocol, Shor and Preskill (2000 *Phys. Rev. Lett.* **85** 441–4) made a remarkable observation that a Calderbank–Shor–Steane (CSS) code had been implicitly used in the BB84 protocol, and suggested its security could be proved by bounding the fidelity, say F_n, of the incorporated CSS code of length n in the form $1 - F_n \leqslant \exp[-nE + o(n)]$ for some positive number E. This work presents such a number $E = E(R)$ as a function of the rate of codes R, and a threshold R_0 such that $E(R) > 0$ whenever $R < R_0$, which is larger than the achievable rate based on the Gilbert–Varshamov bound that is essentially given by Shor and Preskill. The codes in the present work are robust against fluctuations of channel parameters, which fact is needed to establish the security rigorously and was not proved for rates above the Gilbert–Varshamov rate before in the literature. As a byproduct, the security of a modified BB84 protocol against any joint (coherent) attacks is proved quantitatively.

PACS number: 03.67.Dd

1. Introduction

The security of quantum key distribution (QKD), the aim of which is to share a random secret string of digits between two parties, has been said to rest on the principle of quantum mechanics since the time of its proposal [1]. However, proofs of the security against a reasonably wide class of attacks were obtained only recently on the first QKD protocol, which uses Wiesner's idea of conjugate coding [2] and is called the Bennett–Brassard 1984 (BB84)

protocol [1]. Since a preliminary report on such a proof of the security of the scheme was given by Mayers [3], there have been considerable efforts to refine, strengthen or support this result in the literature (e.g., [4–9]). Especially, Shor and Preskill [6] (see also [7, section III]) made a remarkable observation that a Calderbank–Shor–Steane (CSS) quantum code had been implicitly used in the BB84 protocol, and suggested if the fidelity, F_n, of the incorporated Calderbank–Shor–Steane code [10, 11] goes to unity exponentially as the code length n increases, namely, $1 - F_n \leqslant \exp[-nE + o(n)]$ for some positive number E, then the security of the BB84 protocol will be ensured in the sense that the mutual information between the shared key and the data obtained by the eavesdropper is less than $\exp[-nE + o(n)]$. However, no one seems to have given such an exponent E for CSS codes explicitly in the literature. Thus, this paper is concerned with the problem of finding such an exponent $E(R)$ as an explicit function of the rate R of CSS codes.

The proviso for the security proof in this paper is as follows: in the main text, we assume that the possible eavesdropper tries to obtain data by performing an identical measurement on each 'particle' (what is really meant is the d-level quantum system carrying a digit from $\{0, \ldots, d-1\}$, which is typically assumed to be the polarization of a photon, a two-level system); the two legitimate participants of the protocol can communicate with each other by means of a classical noiseless 'public channel' that may be susceptible to passive eavesdropping but is free from tampering; we adopt the formalism developed by Kraus and others to describe measurements (e.g., [12–16]). We assume the so-called individual-attack assumption as mentioned above in order to discuss trade-offs between the level of attacks (including noises) and the allowed rates of transmission of the key; without such an assumption, the level of attacks (often called error rates) could not be properly defined for this purpose. After this tractable case is worked out, the security of a modified BB84 protocol against any joint (coherent) attacks is proved quantitatively in appendix C.

Among others, this paper shows that a code of 'balanced weight spectrum', i.e., a code whose weight distribution is almost proportional to the binomial coefficients (when $d = 2$), attains the desired fidelity bound. This would show the direction to designers of codes for QKD. The code is robust against fluctuations of channel parameters, which is essential to complete the proof of the security rigorously for rates beyond the Gilbert–Varshamov one even in the case of individual attacks. The channel parameters have to be estimated by the participants of the BB84 for assessing the level of eavesdropping, and the robustness is necessary because the estimated channel parameters are not exactly equal to the true ones in general. The robustness issue will be resolved by utilizing the idea of universal codes [17, 18] in information theory. A universal code means one whose structure does not depend on the channel characteristics.

The CSS codes form a class of symplectic (stabilizer or additive) codes [19–21], and there exists a simple class of CSS codes, in which a CSS code is specified by a classical code, say C', satisfying some condition on orthogonality. If we are content with correcting the errors of Hamming weight up to $\delta n/2$, where δn is the minimum distance of C', exponential convergence of fidelity immediately follows from the Gilbert–Varshamov bound for CSS codes [10] and Sanov's theorem (section 7), which is central in large deviation theory [22, 23]. Nevertheless, this argument only ensures the security of the BB48 protocol of code rate up to $1 - 2h(\delta_X + \delta_Z)$, where h is the base-two binary entropy function, δ_Z is the raw bit error rate in transmitting a bit encoded into an eigenvector $|0\rangle$ or $|1\rangle$ of a Pauli operator, say Z, and δ_X is that with a bit encoded into $|0\rangle \pm |1\rangle$. Note that the argument of Shor and Preskill [6] can easily be modified to establish the rate $1 - 2h(\delta_X + \delta_Z)$ for individual attacks (section 7). The aim of this paper includes obtaining, in a rigorous manner, the better achievable rate $1 - 2h((\delta_X + \delta_Z)/2)$. This rate seems essentially the same as the one previously mentioned

in the literature [6], [7, equation (38)], though these papers focused on other issues and gave no details on their codes achieving this higher rate.

We remark that in comparing this paper's bound with the previously claimed ones, we should give due importance to the meaning of 'error rates'. Strictly speaking, we should distinguish the error rates in this paper from the 'error rates' in security proofs for joint attacks. Specifically, our δ_X and δ_Z are parameters of the channel that represent the eavesdropper's attack on each digit whereas it is natural to define the 'error rates' for joint attacks as some fictional random variables which are associated with the much larger channel that represents a general joint attack. In appendix C, the 'error rates' for joint attacks will appear as $P_{\xi'}(1)$ and $P_{\zeta'}(1)$, where $P_{\xi'}$ [$P_{\zeta'}$] is the *type*, i.e., the empirical distribution of the 'sifted' part, or an even smaller part, $\boldsymbol{\xi}'$ [$\boldsymbol{\zeta}'$], of the sequence of random variables $\boldsymbol{\xi}$ [$\boldsymbol{\zeta}$].

Results on exponential convergence of the fidelity of quantum codes (quantum error-correcting codes) have already been obtained by the present author with random coding—which is a proof technique of Shannon's—over general symplectic codes [24–26]. These previous results, however, ensure only the existence of reliable symplectic codes, and use of symplectic codes other than CSS codes in QKD seems to require a quantum computer to implement [6]. Thus, this paper will provide a rigorous but elementary proof that the fidelity F_n of some CSS codes of rate R satisfies $1 - F_n \leqslant \exp[-nE(R) + o(n)]$ for some function $E(R)$ such that $E(R) > 0$ whenever $R < 1 - 2h((\delta_X + \delta_Z)/2)$.

Using this bound and Schumacher's argument [28], which related channel codes to quantum cryptography, we prove the security of the BB84 protocol. The proof to be presented below is basically a refinement of Shor and Preskill's. Whereas use of two-level systems is often assumed when symplectic codes or the BB84 protocol are discussed in the literature, most notions and results easily extend to d-level systems with an arbitrary prime d. Moreover, maybe contrary to one's expectation, our analysis in the case where $d \geqslant 3$ will turn out to be more tractable than in the case where $d = 2$ except for the part treating channel estimation, so that we will begin with the easier case where $d \geqslant 3$.

We neither touch on more practical issues such as the one on the difficulty in preparing a single photon or how to implement d-level systems, nor treat more elaborate models allowing basis-dependent attacks and so on [8].

We remark that there has already been a proposal to use *two-way* entanglement distillation protocols for QKD in order to increase the maximum tolerable error rate [29], whereas the security of the BB84 protocol to be treated in this paper relies on simpler quantum error-correcting (CSS) codes, which can be viewed as *one-way* entanglement distillation protocols. The former class is still based on CSS codes, and would deserve further investigation. However, we will stay around the simple class of protocols in this paper in order to resolve the issues mentioned above.

Attainable fidelity of codes given in this paper may also be interesting from a viewpoint of quantum computing since CSS codes are well-suited for fault-tolerant quantum computing [30, 31]. Incidentally, the technique (permutation argument) in the existence proof of CSS codes in this paper can be incorporated into those of [24–26] to show that the fidelity bounds of [24–26] can be attained by robust symplectic codes.

The paper is organized as follows. In section 2, the needed notation on CSS codes is fixed and a brief review on this class of codes is given. In section 3, we establish the exponential convergence of the fidelity of CSS codes. In section 4, we apply Schumacher's argument to CSS codes to interpret a quantum code as a QKD protocol, and describe how this reduces to the BB84 protocol. Section 5 reviews the method for channel parameter estimation in the BB84 protocol. In section 6, the security proof is completed. Sections 7 and 8 contain discussions and the conclusion, respectively. Proofs of subsidiary results are given in appendix A. In

appendix B, an even better achievable rate, $1 - h(\delta_X) - h(\delta_Z)$, in the BB84 protocol is given. A proof of security of a simple BB84-type protocol for joint attacks is given in appendix C. The case of general joint attacks is treated in appendix C. Nomenclature can be found in appendix D.

2. Calderbank–Shor–Steane codes

The complex linear space of operators on a Hilbert space H is denoted by $\mathsf{L}(\mathsf{H})$. A quantum code usually means a pair $(\mathcal{Q}, \mathcal{R})$ consisting of a subspace $\mathcal{Q}$ of $\mathsf{H}^{\otimes n}$ and a trace-preserving completely positive (TPCP) linear map $\mathcal{R}$ on $\mathsf{L}(\mathsf{H}^{\otimes n})$, called a recovery operator; the subspace $\mathcal{Q}$ alone is also called a (quantum) code. Symplectic codes have more structure: they are simultaneous eigenspaces of commuting operators on $\mathsf{H}^{\otimes n}$. Once a set of commuting operators is specified, we have a collection of eigenspaces of them. A symplectic code refers to either such an eigenspace or a collection of eigenspaces, each possibly accompanied by a suitable recovery operator. Hereafter, we assume H is a Hilbert space with an orthonormal basis $\{|i\rangle\}_{i=0}^{i=d-1}$, and d is a prime. Throughout, $\mathbb{F}_d$ denotes $\mathbb{Z}/d\mathbb{Z}$, a finite field. We use the dot product defined by

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = \sum_{i=1}^{n} x_i y_i \tag{1}$$

where the arithmetic is performed in $\mathbb{F}_d$ (i.e., modulo d), and let $C^\perp$ denote $\left\{ y \in \mathbb{F}_d^n \,\middle|\, \forall x \in C, x \cdot y = 0 \right\}$ for a subset C of $\mathbb{F}_d^n$.

In constructing symplectic codes, the following basis of $\mathsf{L}(\mathsf{H}^{\otimes n})$ is used. Let unitary operators X, Z on H be defined by

$$X|j\rangle = |j-1\rangle, \qquad Z|j\rangle = \omega^j |j\rangle \qquad j \in \mathbb{F}_d \tag{2}$$

with ω being a primitive dth root of unity (e.g., $\mathrm{e}^{\mathrm{i}2\pi/d}$). For $u = (u_1, \ldots, u_n) \in \mathbb{F}_d^n$, let X^u and Z^u denote $X^{u_1} \otimes \cdots \otimes X^{u_n}$ and $Z^{u_1} \otimes \cdots \otimes Z^{u_n}$, respectively. The operators $X^u Z^w$, $u, w \in \mathbb{F}_d^n$, form a basis of $\mathsf{L}(\mathsf{H}^{\otimes n})$, which we call the Weyl (unitary) basis [32]. Observe the commutation relation

$$(X^u Z^w)(X^{u'} Z^{w'}) = \omega^{u \cdot w' - w \cdot u'} (X^{u'} Z^{w'})(X^u Z^w), \qquad u, w, u', w' \in \mathbb{F}_d^n, \tag{3}$$

which follows from $XZ = \omega ZX$. It is sometimes useful to rearrange the components of (u, w) appearing in the operators $X^u Z^w$ in the Weyl basis as follows: for $u = (u_1, \ldots, u_n)$ and $w = (w_1, \ldots, w_n) \in \mathbb{F}_d^n$, we denote the rearranged one $((u_1, w_1), \ldots, (u_n, w_n)) \in \mathcal{X}^n$, where $\mathcal{X} = \mathbb{F}_d \times \mathbb{F}_d$, by $[u, w]$. We occasionally use another symbol N for the Weyl basis: $N_{[u,w]} = X^u Z^w$ and $N_J = \{N_x \mid x \in J\}$ for $J \in \mathcal{X}^n$.

A CSS code is specified by a pair of classical linear codes (i.e., subspaces of $\mathbb{F}_d^n$) such that one contains the other. The quantum codes to be proved to have the desired performance in the following are CSS codes of a special type, for which the pair is a classical code C and its dual $C^\perp$ with the property

$$C \subseteq C^\perp.$$

This condition is equivalent to $\forall x, y \in C, x \cdot y = 0$, and a code C satisfying it is said to be *self-orthogonal* (with respect to the dot product).

Coset structures are exploited in construction of CSS codes. We fix some transversal (set of coset representatives in which each coset has exactly one representative) of the quotient group $\mathbb{F}_d^n / C^\perp$. Identifying $\mathbb{F}_d^n / C^\perp$ and $C^\perp / C$ with their fixed transversals, respectively, we sometimes write, say, $x \in \mathbb{F}_d^n / C^\perp$ and $v \in C^\perp / C$ for coset representatives x and v.

Put $\kappa = \dim C$, and assume $g_1, \ldots, g_\kappa$ form a basis of C. The operators

$$Z^{g_1}, \ldots, Z^{g_\kappa}, X^{g_1}, \ldots, X^{g_\kappa}, \tag{4}$$

commute with each other by (3) and $C \subseteq C^\perp$, so that we have a collection of simultaneous eigenspaces of these operators, which is called a CSS code. Specifically, put

$$|\phi_{xzv}\rangle = \frac{1}{\sqrt{|C|}} \sum_{w \in C} \omega^{z \cdot w} |w + v + x\rangle \tag{5}$$

for coset representatives $x, z \in \mathbb{F}_d^n / C^\perp$ and $v \in C^\perp / C$. Then, we have

$$Z^{g_j} |\phi_{xzv}\rangle = \omega^{x \cdot g_j} |\phi_{xzv}\rangle \qquad \text{and} \qquad X^{g_j} |\phi_{xzv}\rangle = \omega^{z \cdot g_j} |\phi_{xzv}\rangle, \quad j = 1, \ldots, \kappa. \tag{6}$$

It is easy to check that $|\phi_{xzv}\rangle$, $x, z \in \mathbb{F}_d^n / C^\perp$, $v \in C^\perp / C$, form an orthonormal basis of $\mathsf{H}^{\otimes n}$. In words, we have $d^{n-2\kappa}$-dimensional subspaces $\mathcal{Q}_{xz}$ such that $\bigoplus_{x,z} \mathcal{Q}_{xz} = \mathsf{H}^{\otimes n}$, and $\mathcal{Q}_{xz}$ is spanned by orthonormal vectors $|\phi_{xzv}\rangle$, $v \in C^\perp / C$, for each pair $(x, z) \in \left(\mathbb{F}_d^n / C^\perp\right)^2$. The subspaces $\mathcal{Q}_{xz}$, $(x, z) \in \left(\mathbb{F}_d^n / C^\perp\right)^2$, are the simultaneous eigenspaces of the operators in (4), and form a CSS code.

We will consistently use κ and k to denote $\kappa = \dim_{\mathbb{F}_d} C$ and

$$k = n - 2\kappa = \log_d \dim_{\mathbb{C}} \mathcal{Q}_{xz}. \tag{7}$$

Decoding or recovery operation for this type of CSS quantum code is simple. If we choose a transversal Γ of $\mathbb{F}_d^n / C^\perp$, we can construct a recovery operator $\mathcal{R}$ for $\mathcal{Q}_{xz}$ so that the code $(\mathcal{Q}_{xz}, \mathcal{R})$ is $N_{J(\Gamma)}$-correcting in the sense of [33], where

$$J(\Gamma) = \{[x, z] \mid x \in \Gamma \text{ and } z \in \Gamma\}. \tag{8}$$

This directly follows from the general theory of symplectic codes [19–21, 26] on noting that the operators in the Weyl basis that commute with all of those in (4) are $X^u Z^w$, $u \in C^\perp$, $w \in C^\perp$, due to (3). The $N_{J(\Gamma)}$-correcting CSS code specified by C and Γ as above will be denoted by $\mathsf{CSS}(C, \Gamma)$.

3. Exponential convergence of fidelity of codes to unity

First, we treat the simple problem of establishing an attainable fidelity of CSS codes. We write $P^n((x_1, \ldots, x_n))$ for $P(x_1) \cdots P(x_n)$ and $P^n(J)$ for $\sum_{x \in J} P^n(x)$, where P is a probability distribution on $\mathcal{X}$ and $J \subseteq \mathcal{X}^n$. More generally, PQ denotes the usual product of two probability distributions P and Q, which is specified by $[PQ](s, t) = P(s)Q(t)$. For a probability distribution Q on $\mathcal{Y} \times \mathcal{Y}$, we denote the two marginal distributions by $\overline{Q}$ and $\overline{\overline{Q}}$:

$$\overline{Q}(s) = \sum_{t \in \mathcal{Y}} Q(s, t), \qquad \overline{\overline{Q}}(s) = \sum_{t \in \mathcal{Y}} Q(t, s), \qquad s \in \mathcal{Y}.$$

3.1. The case where $d \geqslant 3$

The fidelity of the $N_{J(\Gamma)}$-correcting quantum code $\mathsf{CSS}(C, \Gamma)$ is not smaller than $P^n(J(\Gamma))$ when it is used on the quantum channel that maps $\rho \in \mathsf{L}(\mathsf{H}^{\otimes n})$ to $\sum_{x \in \mathcal{X}^n} P^n(x) N_x \rho N_x^\dagger$. This is true whether entanglement fidelity [28] or minimum fidelity [33] is employed. This bound applies to general channels as well (section 5). Then, noting

$$P^n(J(\Gamma)^c) \leqslant \overline{P}^n(\Gamma^c) + \overline{\overline{P}}^n(\Gamma^c), \tag{9}$$

where J^c denotes the complement of J, which holds by the definition (8) of $J(\Gamma)$, we will prove the following theorem.

Theorem 1. *Assume $d \geqslant 3$. Let a number $0 \leqslant R \leqslant 1$ be given. There exists a sequence of pairs $\{(C_n, \Gamma_n)\}$, each consisting of a self-orthogonal code $C_n \subseteq \mathbb{F}_d^n$ with $n - 2\dim_{\mathbb{F}_d} C_n \geqslant nR$ and a set Γ_n of coset representatives of $\mathbb{F}_d^n / C_n^\perp$, such that for any probability distribution P on $\mathcal{X} = \mathbb{F}_d \times \mathbb{F}_d$,*

$$P^n(J(\Gamma_n)^c) \leqslant \overline{P}^n\left(\Gamma_n^c\right) + \overline{\overline{P}}^n\left(\Gamma_n^c\right) \leqslant d^{-nE(R,\overline{P},\overline{\overline{P}})+o(n)}$$

where

$$E(R, \overline{P}, \overline{\overline{P}}) = \min\{E^*(R, \overline{P}), E^*(R, \overline{\overline{P}})\},$$

$$E^*(R, p) = \min_Q [D(Q\|p) + 2^{-1}|1 - 2H(Q) - R|^+],$$

$|t|^+ = \max\{t, 0\}$, H and D denote the entropy and the Kullback–Leibler information with logarithms of base d, respectively, and the minimization with respect to Q is taken over all probability distributions on $\mathbb{F}_d$.

Remark 1. The function $E(R, \overline{P}, \overline{\overline{P}})$ is strictly positive for $R < 1 - 2\max\{H(\overline{P}), H(\overline{\overline{P}})\}$. The code $\mathsf{CSS}(C_n, \Gamma_n)$ has the rate $1 - 2\dim_{\mathbb{F}_d} C_n/n \geqslant R$. The code $C_n^\perp$, as a classical channel code of rate not less than $R' = (R + 1)/2$, attains the error exponent $E^*(2R' - 1, p)$ known as the random coding error exponent [17] of the memoryless additive channel that changes an input $a \in \mathbb{F}_d$ into $a - b$ with probability $p(b)$.

Remark 2. Whereas $P^n(J(\Gamma_n))$ is a measure of the performance of quantum code $\mathsf{CSS}(C_n, \Gamma_n)$, the probability $\overline{P}^n\left(\Gamma_n^c\right)$ has its own meaning. It is an upper bound on the probability of decoding error for the key transmission, which is proved in appendix A. In fact, the error probability is $\overline{P}^n\left(\Gamma_n'^c\right)$ where $\Gamma_n' = \Gamma_n + C_n$, not $\overline{P}^n\left(\Gamma_n^c\right)$ because adding a word e in C_n to the key $v + C_n$ does not change it.

Remark 3. That Γ_n' is the effective correctable error in QKD (remark 2) may be interpreted as a manifestation of an inherent property, which is sometimes called 'degeneracy', of CSS codes (more generally, of symplectic codes): put $\Gamma' = \Gamma + C$; then, a CSS code $\mathsf{CSS}(C, \Gamma)$, as a quantum code, can correct the 'errors' N_y, $y \in J(\Gamma')$ [19, 20] (or e.g., [26, 27]).

Remark 4. The function $o(n)$ is explicitly given as $3(d - 1)\log_d(n + 1) + \log_d 2 + d$ by (18).

We prove the theorem by a random coding argument, which is analogous to that in [24], where the idea of universal decoding, i.e., minimum entropy (maximum mutual information) decoding of Goppa (e.g., [17, 18]) was already used. For the present purposes, we want the codes C_n also to be robust or universal in the sense that their structures do not depend on the distribution P which characterizes the channel. To show this, we begin with the next lemma, which is a variant of Calderbank and Shor's [10, section V] and says that the ensemble of all self-orthogonal codes is 'balanced'.

Lemma 1. *Assume $d \geqslant 3$, and let*

$$\mathsf{A} = \mathsf{A}^{(n,\kappa)} = \left\{C \subseteq \mathbb{F}_d^n \,\middle|\, C \text{ linear}, C \subseteq C^\perp, \dim C = \kappa\right\}$$

and

$$\mathsf{A}_x = \{C \in \mathsf{A} \mid x \in C^\perp\}.$$

Then, for any $u \in \mathbb{F}_d$, there exists a constant T_u such that $|\mathsf{A}_x| = T_u$ for any nonzero word $x \in \mathbb{F}_d^n$ with $x \cdot x = u$.

Remark. The proof below is the same as that of lemma 6 in [25] except that the dot product is used here in place of the standard symplectic form. This is possible because $\mathbb{F}_d^n$ equipped with the dot product is an orthogonal space if d is a prime other than 2. The case of $d = 2$ is exceptional, and will be treated later. Lemma 1 and the corollary below are true if the dot product is replaced by any orthogonal, symplectic or unitary form more generally.

Proof. To prove $|\mathsf{A}_x| = |\mathsf{A}_y|$ for nonzero vectors x and y with $x \cdot x = y \cdot y = u$, it is enough to show the existence of an isometry α (an invertible linear map α that preserves the 'product', i.e., that satisfies $\alpha(x) \cdot \alpha(y) = x \cdot y$ for all x and y) on $\mathbb{F}_d^n$ with $y = \alpha(x)$, but this directly follows from the well-known Witt lemma [34–37], which states that any isometry that is defined on a subspace of an orthogonal space V can be extended to an isometry on the whole space V. □

Corollary 1. *For $x \in \mathbb{F}_d^n$, $d \geqslant 3$,*

$$\frac{|\mathsf{A}_x|}{|\mathsf{A}|} \leqslant \begin{cases} d^{-\kappa+d-1} & \text{if} \quad x \neq 0^n \\ 1 & \text{if} \quad x = 0^n. \end{cases}$$

Proof. The case of $x = 0^n$ is trivial. Let $S_u = \left|\left\{x \in \mathbb{F}_d^n \,\middle|\, x \cdot x = u, x \neq 0^n\right\}\right|$ for $u \in \mathbb{F}_d$. Counting the pairs (x, C) such that $x \in C^\perp, x \cdot x = u, x \neq 0^n$ and $C \in \mathsf{A}$ in two ways, we have $S_u T_u \leqslant |\mathsf{A}|(d^{n-\kappa} - 1)$. But $S_u \geqslant d^{n-d+1} - 1$ (since $x \in S_u$ can take arbitrary values in the first $n - d + 1$ positions except $(0, 0, \ldots, 0)$), and hence we have $(d^{n-d+1} - 1)T_u \leqslant |\mathsf{A}|(d^{n-\kappa} - 1)$, from which the desired estimate follows. □

In the proof of theorem 1, we will use the method of types, a standard tool in information theory. Here we collect the needed notions and basic inequalities regarding the method of types. With a finite set $\mathcal{Y}$ fixed, the set of all probability distributions on $\mathcal{Y}$ is denoted by $\mathcal{P}(\mathcal{Y})$. The *type* of a sequence $y = (y_1, \ldots, y_n) \in \mathcal{Y}^n$, denoted by P_y, represents the relative frequencies of appearances of symbols $s \in \mathcal{Y}$ in y:

$$\mathsf{P}_y(s) = \frac{|\{i \mid 1 \leqslant i \leqslant n, y_i = s\}|}{n}, \qquad s \in \mathcal{Y}. \tag{10}$$

The set of all possible types of sequences in $\mathcal{Y}^n$ is denoted by $\mathcal{P}_n(\mathcal{Y})$, and for $Q \in \mathcal{P}_n(\mathcal{Y})$, the set of sequences of type Q and length n is denoted by $\mathcal{T}_Q^n$ or $\mathcal{T}_Q^n(\mathcal{Y})$. In what follows, we use

$$|\mathcal{P}_n(\mathcal{Y})| \leqslant (n+1)^{d-1} \qquad \text{and} \qquad \forall Q \in \mathcal{P}_n(\mathcal{Y}), \qquad \left|\mathcal{T}_Q^n\right| \leqslant d^{nH(Q)}, \tag{11}$$

where $d = |\mathcal{Y}|$. Note that if $x \in \mathcal{Y}^n$ has type Q, then $p^n(x) = \prod_{s\in\mathcal{Y}} p(s)^{nQ(s)} = d^{-n[H(Q)+D(Q\|p)]}$ for any $p \in \mathcal{P}(\mathcal{Y})$, so that the probability that words of a fixed type $Q \in \mathcal{P}_n(\mathcal{Y})$ occur has the bound

$$\sum_{y\in\mathcal{Y}^n:\mathsf{P}_y=Q} p^n(x) \leqslant d^{-nD(Q\|p)}. \tag{12}$$

Now we are ready to prove the existence of a 'balanced' code, which will turn out to be universal. Given a set $C' \subseteq \mathbb{F}_d^n$, put

$$\begin{aligned} M_Q(C') &= |\{x \in C' \mid \mathsf{P}_x = Q\}| \\ &= \sum_{x\in\mathbb{F}_d^n} \mathbf{1}[x \in C' \text{ and } \mathsf{P}_x = Q], \qquad Q \in \mathcal{P}_n(\mathbb{F}_d), \end{aligned}$$

where $\mathbf{1}[T]$ equals 1 if the statement T is true and equals 0 otherwise, and put

$$\overline{M}_Q = \frac{1}{|\mathsf{A}|} \sum_{C\in\mathsf{A}} M_Q(C^\perp).$$

Then, we obtain the next lemma following the method in [38] (cf [39]).

Lemma 2. *For any $n \geqslant 2$ and $\kappa \leqslant n/2$, there exists a code C in $\mathsf{A} = \mathsf{A}^{(n,\kappa)}$ such that*

$$\forall Q \in \mathcal{P}_n(\mathbb{F}_d), \qquad M_Q(C^\perp) \leqslant |\mathcal{P}_n(\mathbb{F}_d)|\overline{M}_Q.$$

Remark. The list of numbers $(M_Q(C'))_{Q\in\mathcal{P}_n(\mathbb{F}_d)}$, type spectrum, so to speak, is a natural generalization of the weight spectrum (distribution) in coding theory. In fact, they are the same when $d = 2$.

Proof. Regarding C as a random variable uniformly distributed over A and using Markov's inequality (e.g., [23]), which states that $\Pr\{\mathsf{X} \geqslant a\mu\} \leqslant 1/a$ for a positive constant a, and a random variable X that takes non-negative values and has a positive mean μ, we have

$$\begin{aligned}\Pr\{\exists Q \in \mathcal{P}_n(\mathbb{F}_d), M_Q(C^\perp) \geqslant |\mathcal{P}_n(\mathbb{F}_d)|^{1+\varepsilon}\overline{M}_Q \quad \text{and} \quad \overline{M}_Q > 0\} \\ \leqslant \sum_{Q\in\mathcal{P}_n(\mathbb{F}_d):\overline{M}_Q>0} \Pr\{M_Q(C^\perp) \geqslant |\mathcal{P}_n(\mathbb{F}_d)|^{1+\varepsilon}\overline{M}_Q\} \leqslant 1/|\mathcal{P}_n(\mathbb{F}_d)|^\varepsilon\end{aligned}$$

for any $\varepsilon > 0$. Hence, $\Pr\{\forall Q \in \mathcal{P}_n(\mathbb{F}_d), M_Q(C^\perp) < |\mathcal{P}_n(\mathbb{F}_d)|^{1+\varepsilon}\overline{M}_Q \text{ or } \overline{M}_Q = 0\} \geqslant 1 - 1/|\mathcal{P}_n(\mathbb{F}_d)|^\varepsilon > 0$. Since $\varepsilon > 0$ is arbitrary, this implies the lemma. □

Corollary 2. *There exists a code C in $\mathsf{A} = \mathsf{A}^{(n,\kappa)}$ such that for any $Q \in \mathcal{P}_n(\mathbb{F}_d)$, $Q \neq \mathsf{P}_{0^n}$,*

$$\frac{M_Q(C^\perp)}{|\mathcal{T}_Q^n|} \leqslant |\mathcal{P}_n(\mathbb{F}_d)|d^{-\kappa+d-1}.$$

Proof. We have

$$\begin{aligned}\overline{M}_Q &= \frac{1}{|\mathsf{A}|}\sum_{C\in\mathsf{A}}\sum_{x\in\mathbb{F}_d^n} \mathbf{1}[x \in C^\perp \text{ and } \mathsf{P}_x = Q] \\ &= \sum_{x\in\mathbb{F}_d^n:\mathsf{P}_x=Q} \frac{1}{|\mathsf{A}|}\sum_{C\in\mathsf{A}} \mathbf{1}[x \in C^\perp] \\ &\leqslant \sum_{x\in\mathbb{F}_d^n:\mathsf{P}_x=Q} d^{-\kappa+d-1} \\ &= |\mathcal{T}_Q^n|d^{-\kappa+d-1}, \qquad Q \neq \mathsf{P}_{0^n}, \end{aligned} \tag{13}$$

where the inequality is due to corollary 1, and hence the desired estimate. □

Corollary 2 says that there exists a code $C \in \mathsf{A}$ such that $(M_Q(C^\perp))_{Q\in\mathcal{P}_n(\mathbb{F}_d)}$ is almost proportional to $\big(M_Q(\mathbb{F}_d^n)\big)_{Q\in\mathcal{P}_n(\mathbb{F}_d)} = \big(|\mathcal{T}_Q^n|\big)_{Q\in\mathcal{P}_n(\mathbb{F}_d)}$. (Clearly, the code $C^\perp$ in this corollary satisfies the Gilbert–Varshamov bound asymptotically.) We will see that the code in lemma 2 or corollary 2 has the universality mentioned above.

The decoding should also possess such universality. Note that for CSS codes, in theory, the design of a decoder is accomplished by choosing a transversal of $\mathbb{F}_d^n/C^\perp$. Based on the idea of minimum entropy decoding, *from each of the d^κ cosets of $C^\perp$ in $\mathbb{F}_d^n$, we choose a vector that minimizes $H(\mathsf{P}_x)$ in the coset*. To break ties, we use an arbitrarily fixed order, say a lexicographic order in $\mathbb{F}_d^n$.

Proof of theorem 1. In the proof, $\mathcal{P}_n(\mathbb{F}_d)$ is abbreviated as $\mathcal{P}_n$. Fix a code C of the property in corollary 2 and a transversal Γ chosen as above. We will show C is the desired code. Let $\mathcal{S}_n$ be the group composed of all permutations on $\{1, \ldots, n\}$ and assume $\pi \in \mathcal{S}_n$, when applied to C or Γ, permutes all words in C or Γ as $\pi([x_1, \ldots, x_n]) = [x_{\pi(1)}, \ldots, x_{\pi(n)}]$. Clearly,

$p^n(\pi(\Gamma)) = p^n(\Gamma)$ for any $\pi \in \mathcal{S}_n$ and any probability distribution p on $\mathbb{F}_d$. For a technical reason, we will evaluate the ensemble average of $p^n(\pi(\Gamma))$ over $\mathcal{S}_n$, which equals $p^n(\Gamma)$, the original quantity in question. Specifically, put

$$B(p) = \frac{1}{|\mathcal{S}_n|} \sum_{\pi \in \mathcal{S}_n} p^n(\pi(\Gamma)^{\mathrm{c}}) \tag{14}$$

for $p = \overline{P}, \overline{\overline{P}}$. We will show, for some polynomial $f(n)$, that $B(p)$ is bounded above by $f(n)d^{-nE^*(R,p)}$, which implies $B(\overline{P}) + B(\overline{\overline{P}}) \leqslant 2f(n)d^{-n\min\{E^*(R,\overline{P}),E^*(R,\overline{\overline{P}})\}}$. This, together with (9), establishes the theorem.

It was shown that an exponential fidelity bound holds for a 'balanced' ensemble of additive codes [24, 25]. To take the same approach as in [24, 25], we show that the ensemble $\pi(C)^\perp, \pi \in \mathcal{S}_n$, is almost 'balanced'. Imagine we list all words in $\pi(C)^\perp$ for all $\pi \in \mathcal{S}_n$. Clearly, for any $Q \in \mathcal{P}_n$, there exists a constant, say L_Q, such that $|\{\pi \in \mathcal{S}_n \mid x \in \pi(C)^\perp\}| = L_Q$ for any word x with $\mathsf{P}_x = Q$. Then, counting the number of words of a fixed type Q in the list in two ways, we have $\left|\mathcal{T}_Q^n\right| L_Q = |\mathcal{S}_n| M_Q(C^\perp)$. Hence, for any type $Q \neq \mathsf{P}_{0^n}$,

$$\frac{L_Q}{|\mathcal{S}_n|} = \frac{M_Q(C^\perp)}{\left|\mathcal{T}_Q^n\right|} \leqslant |\mathcal{P}_n| d^{-\kappa+d-1}, \tag{15}$$

where we have used corollary 2. We have proved the next lemma. □

Lemma 3. *Put*

$$\mathsf{A}_y(C) = \{\pi \in \mathcal{S}_n \mid y \in \pi(C)^\perp\}.$$

For $y \in \mathbb{F}_d^n$, $y \neq 0^n$, we have

$$\frac{|\mathsf{A}_y(C)|}{|\mathcal{S}_n|} \leqslant |\mathcal{P}_n| d^{-\kappa+d-1}.$$

From (14), we have

$$\begin{aligned} B(p) &= \frac{1}{|\mathcal{S}_n|} \sum_{\pi \in \mathcal{S}_n} \sum_{x \notin \pi(\Gamma)} p^n(x) \\ &= \sum_{x \in \mathbb{F}_d^n} p^n(x) \frac{|\{\pi \in \mathcal{S}_n \mid x \notin \pi(\Gamma)\}|}{|\mathcal{S}_n|}. \end{aligned} \tag{16}$$

Since $x \notin \pi(\Gamma)$ occurs only if there exists a word $u \in \mathbb{F}_d^n$ such that $H(\mathsf{P}_u) \leqslant H(\mathsf{P}_x)$ and $u - x \in \pi(C)^\perp \backslash \{0^n\}$ from the design of Γ specified above (minimum entropy decoding), it follows:

$$\begin{aligned} &|\{\pi \in \mathcal{S}_n \mid x \notin \pi(\Gamma)\}|/|\mathcal{S}_n| \\ &\quad\leqslant \sum_{u \in \mathbb{F}_d^n : H(\mathsf{P}_u) \leqslant H(\mathsf{P}_x), u \neq x} |\mathsf{A}_{u-x}(C)|/|\mathcal{S}_n| \\ &\quad\leqslant \sum_{u \in \mathbb{F}_d^n : H(\mathsf{P}_u) \leqslant H(\mathsf{P}_x)} |\mathcal{P}_n| d^{-(\kappa-d+1)}, \\ &\quad= \sum_{Q' \in \mathcal{P}_n : H(Q') \leqslant H(\mathsf{P}_x)} |\mathcal{P}_n| \left|\mathcal{T}_{Q'}^n\right| d^{-(\kappa-d+1)} \\ &\quad\leqslant \sum_{Q' \in \mathcal{P}_n : H(Q') \leqslant H(\mathsf{P}_x)} |\mathcal{P}_n| d^{nH(Q')-(\kappa-d+1)} \end{aligned} \tag{17}$$

where we have used lemma 3 for the second inequality, and (11) for the last inequality. Then, recalling (7) and (12), and choosing the smallest integer k such that $k \geqslant nR$ and $\kappa = (n-k)/2$ is an integer, which implies $nR \leqslant k < nR+2$, with repeated use of the inequality $\min\{s+t,1\} \leqslant \min\{s,1\} + \min\{t,1\}$ for $s, t \geqslant 0$, we can proceed from (16) as follows:

$$\begin{aligned}
B(p) &\leqslant \sum_{x\in\mathbb{F}_d^n} p^n(x) \min\left\{ \sum_{Q'\in\mathcal{P}_n : H(Q') \leqslant H(\mathsf{P}_x)} |\mathcal{P}_n| d^{nH(Q')-(\kappa-d+1)}, 1 \right\} \\
&\leqslant |\mathcal{P}_n| \sum_{Q\in\mathcal{P}_n} d^{-nD(Q\|p)+d} \min\left\{ \sum_{Q'\in\mathcal{P}_n : H(Q') \leqslant H(Q)} d^{nH(Q')-\frac{n-k}{2}-1}, 1 \right\} \\
&\leqslant |\mathcal{P}_n| \sum_{Q\in\mathcal{P}_n} d^{-nD(Q\|p)+d} \sum_{Q'\in\mathcal{P}_n : H(Q') \leqslant H(Q)} \min\{d^{-n[1-R-2H(Q')]/2}, 1\} \\
&\leqslant |\mathcal{P}_n|^2 \sum_{Q\in\mathcal{P}_n} d^{-nD(Q\|p)+d} \max_{Q'\in\mathcal{P}(\mathbb{F}_d) : H(Q') \leqslant H(Q)} d^{-n|1-R-2H(Q')|^+/2} \\
&= |\mathcal{P}_n|^2 \sum_{Q\in\mathcal{P}_n} d^{-nD(Q\|p)+d} d^{-n|1-R-2H(Q)|^+/2} \\
&\leqslant d^d |\mathcal{P}_n|^3 \max_Q d^{-n[D(Q\|p)+|1-R-2H(Q)|^+/2]} = d^d |\mathcal{P}_n|^3 d^{-nE^*(R,p)}.
\end{aligned}$$

Hence, we have

$$\begin{aligned}
B(\overline{P}) + B(\overline{\overline{P}}) &= \frac{1}{|\mathcal{S}_n|} \sum_{\pi\in\mathcal{S}_n} [\overline{P}^n(\pi(\Gamma)^{\mathrm{c}}) + \overline{\overline{P}}^n(\pi(\Gamma)^{\mathrm{c}})] \\
&\leqslant 2d^d |\mathcal{P}_n|^3 d^{-n \min\{E^*(R,\overline{P}), E^*(R,\overline{\overline{P}})\}}. \qquad (18)
\end{aligned}$$

Since $|\mathcal{P}_n| \leqslant (n+1)^{d-1}$, we obtain the desired bound.

3.2. The case where $d = 2$

Calderbank and Shor [10] proved the following lemma on the basis of a result in coding theory.

Lemma 4. *Assume $d = 2$, $n \geqslant 2$ is an even integer, and $0 < \kappa \leqslant n/2$ is an integer. Let*

$$\mathsf{A} = \left\{ C \subseteq \mathbb{F}_d^n \,\middle|\, C \text{ linear}, \{1^n\} \subseteq C \subseteq C^\perp, \dim C = \kappa \right\},$$

and

$$\mathsf{A}_x = \{C \in \mathsf{A} \mid x \in C^\perp\}.$$

Then, there exists a constant T_0 satisfying $|\mathsf{A}_x| = T_0$ for any $x \in \mathbb{F}_d^n$ with $x \cdot x = 0$, $x \neq 0^n$ and $x \neq 1^n$.

Corollary 3. *For $x \in \mathbb{F}_2^n$,*

$$\frac{|\mathsf{A}_x|}{|\mathsf{A}|} \leqslant \begin{cases} d^{-\kappa+d-1} & \text{if} \quad x \neq 0^n \quad \text{and} \quad x \neq 1^n \\ 1 & \text{if} \quad x = 0^n \quad \text{or} \quad x = 1^n. \end{cases}$$

Remark. Trivially, $|\mathsf{A}_x| = 0$ for all x with $x \cdot x = 1$ since $x \cdot x = x \cdot 1^n$. We can also prove this lemma noting a hidden structure of a symplectic space. Namely, letting $\mathsf{F}_{\mathrm{even}}$ be the set of of all words x with $x \cdot x = 0$ in $\mathbb{F}_2^n$, and noting that the additive quotient group $\mathsf{F}_{\mathrm{even}}/\mathsf{span}\, 1^n$, where $\mathsf{span}\, 1^n = \{0^n, 1^n\}$, is a symplectic space equipped with the natural form $(x + \mathsf{span}\, 1^n) \cdot (y + \mathsf{span}\, 1^n) = x \cdot y$, we can argue as in the proof of lemma 1.

In theorem 1, due to remark 3 thereof, we could have used Γ' or a subset $\widetilde{\Gamma}$ of Γ' in place of Γ for the purposes of evaluating the fidelity (and the probability of disagreement between Alice's key and Bob's due to remark 2 to theorem 1). Namely, we obtain theorem 1 with '$d \geqslant 3$' and '$P^n(J(\Gamma_n)^{\mathrm{c}}) \leqslant \overline{P}^n\left(\Gamma_n^{\mathrm{c}}\right) + \overline{\overline{P}}^n\left(\Gamma_n^{\mathrm{c}}\right)$' replaced by '$d = 2$ and n is even' and '$P^n(J(\widetilde{\Gamma}_n)^{\mathrm{c}}) \leqslant \overline{P}^n\left(\widetilde{\Gamma}_n^{\mathrm{c}}\right) + \overline{\overline{P}}^n\left(\widetilde{\Gamma}_n^{\mathrm{c}}\right)$', respectively, where $\widetilde{\Gamma}_n = \Gamma_n + 1^n$, using corollary 3 instead of corollary 1 in the above proof of theorem 1. In fact, with Γ replaced by $\widetilde{\Gamma}$, the proof of theorem 1 can read verbatim except the first inequality in (17), which should be replaced by

$$|\{\pi \in \mathcal{S}_n \mid x \notin \pi(\widetilde{\Gamma})\}| \leqslant \sum_{u \in \mathbb{F}_d^n : H(\mathsf{P}_u) \leqslant H(\mathsf{P}_x),\, u-x \neq 0^n, 1^n} |\mathsf{A}_{u-x}(C)|,$$

and the other few expressions. Thus, the statement of theorem 1 is true for $d = 2$ with Γ replaced by $\widetilde{\Gamma}$ and with the restriction of n being even, where the code C_n always contains 1^n. (For $d = 2$ and n odd, a geometric argument based on isometries as before shows that the rate $1 - 2h((\delta_X + \delta_Z)/2)$ is achievable for $(\delta_X + \delta_Z)/2 \leqslant 1/2$, whereas the restriction $(\delta_X + \delta_Z)/2 \leqslant 1/2$ is not needed for n even. In this case, we use isometries on $\mathbb{F}_d^n$ that fix 1^n, with respect to the dot product, noting that $\mathbb{F}_d^n = \mathsf{F}_{\mathrm{even}} + \mathsf{span}\, 1^n$ and 1^n is orthogonal to $\mathsf{F}_{\mathrm{even}}$ in order to prove the existence of balanced codes; we use the minimum Hamming distance decoding in place of the minimum entropy decoding.)

4. Bennett–Brassard 1984 quantum key distribution protocol

In the proof of the security of the BB84 protocol, Shor and Preskill used the observation of Lo and Chau [40], who upper-bounded the amount of information that the eavesdropper, Eve, could obtain on the key by the Holevo bound [41]. However, a similar observation using the Holevo bound had already been made by Schumacher [28, section V-C], who directly related Eve's information with quantum channel codes. In this section, we will apply Schumacher's argument to CSS codes to avoid a detour to entanglement distillation.

4.1. Quantum codes and quantum cryptography

Suppose we send a k-digit key $\mathsf{V} + C \in C^{\perp}/C$ encoded into $|\phi_{\mathsf{XZV}}\rangle \in \mathcal{Q}_{\mathsf{XZ}}$, where we regard $\mathsf{X}, \mathsf{Z}, \mathsf{V}$ as random variables, and $(\mathsf{X}, \mathsf{Z}, \mathsf{V})$ are randomly chosen according to the uniform distribution. Once Eve has done an eavesdropping, namely, a series of measurements, Eve's measurement results form another random variable, say E. We use the standard symbol I to denote the mutual information (appendix D).

According to [28, section V-C],

$$I(\mathsf{V}; \mathsf{E}|\mathsf{X} = x, \mathsf{Z} = z) \leqslant S_{xz} \tag{19}$$

where S_{xz} is the entropy exchange after the system suffers a channel noise $\mathcal{N}$, Eve's attack $\mathcal{E}$, another channel noise $\mathcal{N}'$, and the recovery operation $\mathcal{R} = \mathcal{R}_{xz}$ for $\mathcal{Q}_{xz}$ at the receiver's end. Let us denote by F_{xz} the fidelity of the code $(\mathcal{Q}_{xz}, \mathcal{R})$ employing the entanglement fidelity F_{e} [28]. Specifically,

$$F_{xz} = F_{\mathrm{e}}\left(\pi_{\mathcal{Q}_{xz}}, \mathcal{R}\mathcal{N}'\mathcal{E}\mathcal{N}\right)$$

where $\pi_{\mathcal{Q}}$ denotes the normalized projection operator onto $\mathcal{Q}$, and $\mathcal{B}\mathcal{A}(\rho) = \mathcal{B}(\mathcal{A}(\rho))$ for two CP maps $\mathcal{A}$ and $\mathcal{B}$, etc. Then, by the quantum Fano inequality [28, section VI], we have

$$S_{xz} \leqslant h(F_{xz}) + (1 - F_{xz})2nR \tag{20}$$

where $R = n^{-1}\log_d \dim \mathcal{Q}_{xz}$. Combining (19) and (20) and taking the averages of the end sides, we obtain

$$\begin{aligned} I(\mathsf{V};\mathsf{E}|\mathsf{XZ}) &\leqslant \mathbb{E}h(F_{\mathsf{XZ}}) + (1-\mathbb{E}F_{\mathsf{XZ}})2nR \\ &\leqslant h(\mathbb{E}F_{\mathsf{XZ}}) + (1-\mathbb{E}F_{\mathsf{XZ}})2nR, \end{aligned} \tag{21}$$

where $\mathbb{E}$ denotes the expectation operator with respect to (X,Z). Hence, if $1-\mathbb{E}F_{\mathsf{XZ}}$ goes to zero faster than $1/n$, then $I(\mathsf{V};\mathsf{E}|\mathsf{XZ}) \to 0$ as $n \to \infty$. We have seen that the convergence is, in fact, exponential for some good CSS codes, namely, $1-\mathbb{E}F_{\mathsf{XZ}} \leqslant d^{-nE+o(n)}$ with some $E > 0$. This, together with (21), implies

$$I(\mathsf{V};\mathsf{E}|\mathsf{XZ}) \leqslant 2d^{-nE+o(n)}[n(E+R)-o(n)], \tag{22}$$

where we used the upper bound $-2t\log t$ for $h(t)$, $0 \leqslant t \leqslant 1/2$, which can easily be shown by differentiating $t\log t$ (or by lemma 2.7 of [17]). Thus, we could safely send a key $v + C$ provided we could send the entangled state $|\phi_{xzv}\rangle$ in (5) and the noise level of the quantum channel including Eve's action were tolerable by the quantum code.

4.2. Reduction to the Bennett–Brassard 1984 protocol

To reduce the above protocol to a more practical one, namely the BB84 protocol, we use Shor and Preskill's observation that the probabilistic mixture of $|\phi_{xzv}\rangle$ with x, v fixed and z chosen uniformly randomly over $\mathbb{F}_d^n/C^\perp$ is given as

$$\frac{1}{|C|}\sum_z |\phi_{xzv}\rangle\langle\phi_{xzv}| = \frac{1}{|C|}\sum_{w\in C} |w+v+x\rangle\langle w+v+x|, \tag{23}$$

which can be prepared as the mixture of states $|w+v+x\rangle$ with no entanglement. Then, it is seen that sending the key v encoded into the state in (23) with x chosen randomly is exactly what is done in the following protocol of Bennett and Brassard, which is essentially the same as that in [6] except that a CSS code of a higher rate is chosen in step (vii).

In the protocol, three more sequences of independent and identically distributed binary random variables $\mathsf{a},\mathsf{b},\mathsf{c}$ are introduced, where $\mathsf{a} = (\mathsf{a}_1,\ldots,\mathsf{a}_m)$ and so on. The probability of occurrence of 1 for the bits of $\mathsf{a},\mathsf{b},\mathsf{c}$ will be denoted by p_{a}, p_{b}, p_{c}, respectively, where $p_{\mathrm{a}}, p_{\mathrm{b}}, p_{\mathrm{c}} \in (0,1)$. We put

$$r = \frac{p_{\mathrm{a}}p_{\mathrm{b}}}{p_{\mathrm{a}}p_{\mathrm{b}} + (1-p_{\mathrm{a}})(1-p_{\mathrm{b}})}, \tag{24}$$

which is the expected ratio of the number of i with $a_i = b_i = 1$ to that of i with $a_i = b_i$. In what follows, the Z-basis denotes the collection $|j\rangle$, $j \in \mathbb{F}_d$, the Z-basis measurement denotes the simple (projective) measurement $\{|j\rangle\langle j|\}_j$. We also say 'measure Z' in place of 'perform the Z-basis measurement'. The X-basis, X-basis measurement and 'measure X' are to be similarly understood with the d orthogonal eigenstates of X. Specifically, the X-basis consists of

$$|j\rangle' = \sum_{l\in\mathbb{F}_d} \omega^{jl}|l\rangle, \qquad j \in \mathbb{F}_d.$$

BB84 protocol

(i) The sender, Alice, and the receiver, Bob, do steps (ii)–(iv) for each $i = 1,\ldots,m$.
(ii) Alice chooses a random bit a_i. She prepares her system in one state that is chosen uniformly randomly from the Z-basis if a_i is 0, or in one from the X-basis if a_i is 1.
(iii) Alice sends the prepared state to Bob.
(iv) Bob chooses another random bit b_i, and receives the state, performs the Z-basis measurement if b_i is 0, or the X-basis measurement if b_i is 1.

(v) Alice and Bob announce $\mathsf{a} = (\mathsf{a}_1, \ldots, \mathsf{a}_m)$ and $\mathsf{b} = (\mathsf{b}_1, \ldots, \mathsf{b}_m)$, respectively.

(vi) Alice and Bob discard any results where $\mathsf{a}_i \neq \mathsf{b}_i$. Alice draws another string of random bits $\mathsf{c} = (\mathsf{c}_1, \ldots, \mathsf{c}_m)$, and sends it to Bob through a public channel. They decide that those d-ary digits with the accompanying c_i being 0 will be the code digits, i.e., will be used for the key transmission with a CSS code. In the case where $d = 2$, it is assumed that the number of the code digits is even (if not, they divert one digit chosen in an arbitrary manner to the estimation of the noise level in the following step).

(vii) Alice and Bob announce the values of their non-code digits which are accompanied by $\mathsf{c}_i = 1$, and from these and a_i $(= \mathsf{b}_i)$, estimate the noise level, and decide on a secure transmission rate, and a CSS code, i.e., a pair (C, Γ), to be used (the exact meaning will be clear in section 6).

(viii) Alice announces the coset $y + C^\perp$, where y $(= w + v + x)$ is the string consisting of the remaining code digits. In other words, she announces the coset representative $x \in \mathbb{F}_d^n / C^\perp$ of the coset $y + C^\perp$, or equivalently, the syndrome $(y \cdot g_j)_{j=1}^{j=\kappa}$.

(ix) Bob subtracts the coset representative $x \in \mathbb{F}_d^n / C^\perp$ from his code digits, $y - e$, and corrects the result $y - x - e$ to a codeword u in $C^\perp$, where he uses the decoder such that $u = y - x$ if $e \in \Gamma$.

(x) Alice uses the coset $(y - x) + C \in C^\perp / C$, and Bob uses $u + C \in C^\perp / C$ as the key.

In step (viii), $x \in \mathbb{F}_d^n / C^\perp$ means that x is chosen from the transversal of $\mathbb{F}_d^n / C^\perp$ shared by Alice and Bob, which may be assumed to be Γ. In short, by the law of large numbers, about $[(1 - p_\mathrm{a})p_\mathrm{b} + p_\mathrm{a}(1 - p_\mathrm{b})]m$ copies of states are discarded, about $(1 - p_\mathrm{c})[(1 - p_\mathrm{a})(1 - p_\mathrm{b}) + p_\mathrm{a}p_\mathrm{b}]m$ copies are used for the transmission of the key with CSS codes, the reliability of which was evaluated in section 3, and the about $p_\mathrm{c}[(1 - p_\mathrm{a})(1 - p_\mathrm{b}) + p_\mathrm{a}p_\mathrm{b}]m$ remaining copies are used for the estimation of the noise level, which will be described in section 5.

In what follows, we will analyse the security of the protocol under the 'individual attack' assumption that Eve obtains data by an identical measurement on each particle. Especially, this assumption includes that Eve cannot change her measurement according to the value of a_i or b_i. A measurement is modelled as a completely positive (CP) instrument whose measurement result belongs to a finite or countable set (e.g., [12–16]). We also assume that the channel noises $\mathcal{N}, \mathcal{N}'$ are tensor products of identical copies of a CP map. Namely, we assume a state $\rho \in \mathsf{L}(\mathsf{H})$ of each particle suffers a change $\rho \mapsto \sum_i A_i \rho A_i^\dagger$, and Eve obtains i, or part of it, with probability $\mathrm{Tr} A_i^\dagger A_i \rho$ as information on this particle.

We remark that some quantities such as $\mathsf{Z} = z$ and the quantum code $(\mathcal{Q}_{xz}, \mathcal{R})$ are artifices that have been introduced only to establish the security, and are not needed for practice. For example, in the protocol, only half of the decoding operation $\mathcal{R}$ (the part where a half of the syndrome, namely, $(x \cdot g_i)_{i=1}^{\kappa}$ in (6) matters) is performed. This can be viewed as the decoding for the classical code $C^\perp$ (more precisely, the coset code $y + C^\perp$), and the decoding error probability of this classical code $C^\perp$, together with $1 - \mathbb{E}F_{\mathsf{XZ}}$ for the corresponding CSS code $\mathsf{CSS}(C, \Gamma)$, has been upper-bounded exponentially in theorem 1.

5. Estimation of channel parameters

Roughly speaking, the BB84 protocol consists of CSS coding and estimation of channel parameters. This section describes how the estimation works in the present case of individual attacks.

Since Alice and Bob use the X-basis or Z-basis at random, the change suffered by a transmitted state, if it is assumed to be a Z-basis element $|j\rangle$ initially, is either $\mathcal{A}$ or

$\mathcal{A}' = \mathcal{U}^{-1}\mathcal{A}\mathcal{U}$ accordingly as the Z-basis ($a_i = b_i = 0$) or the X-basis ($a_i = b_i = 1$) is used, where $\mathcal{A}$ represents Eve's action plus the channel noises for each digit sent, and $\mathcal{U}$ denotes the Fourier transform

$$\mathcal{U}(\rho) = U\rho U^{\dagger}$$

with

$$U = d^{-1/2} \sum_{j,l \in \mathbb{F}_d} \omega^{jl} |j\rangle\langle l|.$$

Note that the X-basis $\{|j\rangle'\}$ and Z-basis $\{|j\rangle\}$ are related by

$$|j\rangle' = U|j\rangle, \qquad j \in \mathbb{F}_d.$$

We use the following well-known one-to-one map of Choi [42] between the CP maps on $\mathsf{L}(\mathsf{H}^{\otimes n})$ and the positive semi-definite operators in $\mathsf{L}(\mathsf{H}^{\otimes n} \otimes \mathsf{H}^{\otimes n})$:

$$\mathsf{M}_n(\mathcal{V}) = [\mathcal{I} \otimes \mathcal{V}](|\Psi\rangle\langle\Psi|), \tag{25}$$

where $\mathcal{I}$ is the identity map on $\mathsf{L}(\mathsf{H}^{\otimes n})$, and $|\Psi\rangle$ is a maximally entangled state given by

$$|\Psi\rangle = \frac{1}{\sqrt{d^n}} \sum_{l \in \mathcal{B}} |l\rangle \otimes |l\rangle$$

with some orthonormal basis $\mathcal{B} = \{|l\rangle\}$ of $\mathsf{H}^{\otimes n}$. Choi introduced $d^n \mathsf{M}_n(\mathcal{V})$ in matrix form to yield fundamentals of CP maps.

In the present case, we assume $|l\rangle = |l_1\rangle \otimes \cdots \otimes |l_n\rangle$, $l = (l_1, \ldots, l_n) \in \mathbb{F}_d^n$, and let

$$|\Psi_y\rangle = \frac{1}{\sqrt{d^n}} \sum_{l \in \mathbb{F}_d^n} |l\rangle \otimes N_y|l\rangle, \qquad y \in \mathcal{X}^n. \tag{26}$$

These $2n$ vectors form an orthonormal basis of $\mathsf{H}^{\otimes n} \otimes \mathsf{H}^{\otimes n}$ (e.g., [43]). Recall that a symplectic code has a collection of subspaces $\{\mathcal{Q}_\xi\}$ and recovery operators $\mathcal{R}_\xi$ for each ξ, where ξ corresponds to the syndrome and has been written as xz for CSS codes. It is known that an N_J-correcting symplectic code $(\mathcal{Q}_\xi, \mathcal{R}_\xi)$, used on a channel $\mathcal{V}_n : \mathsf{L}(\mathsf{H}^{\otimes n}) \to \mathsf{L}(\mathsf{H}^{\otimes n})$, has entanglement fidelity, averaged over all ξ with equal probabilities, not smaller than $\sum_{y \in J} P_{\mathcal{V}_n}(y)$:

$$\mathbb{E}_\xi F_{\mathrm{e}}\big(\pi_{\mathcal{Q}_\xi}, \mathcal{R}_\xi \mathcal{V}_n\big) \geqslant \sum_{y \in J} P_{\mathcal{V}_n}(y), \tag{27}$$

where $P_{\mathcal{V}_n}(x)$ is associated with the channel $\mathcal{V}_n$ via

$$P_{\mathcal{V}_n}(x) = \langle \Psi_x | \mathsf{M}_n(\mathcal{V}_n) | \Psi_x \rangle, \qquad x \in \mathcal{X}^n, \tag{28}$$

and $\mathbb{E}_\xi$ is the expectation operator. This bound is implicit in [7] as explained in appendix A; the bound is tight for the largest choice of J [27].

Our channel to be analysed has the product form $\mathcal{V}_n = \mathcal{M}^n$, and hence $P_{\mathcal{V}_n}$ also has the product form

$$P_{\mathcal{V}_n} = P_{\mathcal{M}}^n.$$

Here, we have assumed that Alice and Bob do not use the values of $\mathsf{a}_i (= \mathsf{b}_i)$ for coding, which implies that $\mathcal{M}$ can be regarded as the mixture

$$\mathcal{M} = (1 - r)\mathcal{A} + r\mathcal{A}'.$$

Note, especially in the case where $d = 2$, $P_{\mathcal{A}}$ and $P_{\mathcal{A}'}$ are related by

$$P_{\mathcal{A}'}(s, t) = P_{\mathcal{A}}(t, s), \qquad s, t \in \mathbb{F}_d, \tag{29}$$

since X and Z switch with each other by $\mathcal{U}$. More generally, we have

$$P_{\mathcal{A}'}(s,t) = P_{\mathcal{A}}(t,-s), \qquad s,t \in \mathbb{F}_d, \tag{30}$$

which is proved in appendix A.

The quantity $P_{\mathcal{A}}(s,t)$ is the probability of obtaining (s,t) with a measurement $\{|\Psi_{(s,t)}\rangle\langle\Psi_{(s,t)}|\}_{(s,t)\in\mathbb{F}_d^2}$ on the system in the state $\mathsf{M}_1(\mathcal{A})$. However, this seems hard to implement, so that we divide the problem. We measure either s or t per sample of the state $\mathsf{M}_1(\mathcal{A})$. To do this, note that

$$Z \otimes Z^{-1}|\Psi_{(s,t)}\rangle = \omega^s|\Psi_{(s,t)}\rangle \tag{31}$$

for $(s,t) \in \mathbb{F}_d^2$. This implies that measuring eigenvalues of $Z \otimes Z^{-1}$, i.e., performing the measurement $\left\{\sum_{t\in\mathbb{F}_d}|\Psi_{(s,t)}\rangle\langle\Psi_{(s,t)}|\right\}_{s\in\mathbb{F}_d}$ in the state $\mathsf{M}_1(\mathcal{A})$, gives the result s with probability $\overline{P_{\mathcal{A}}}(s)$. Measuring eigenvalues of $Z \otimes Z^{-1}$ is still imaginary, but measuring eigenvalues of $Z \otimes I$ and then $I \otimes Z^{-1}$ is completely simulated by sending one of the eigenstates of Z at random (according to the uniform distribution) through $\mathcal{A}$ and measuring Z^{-1} at the receiver's end, and $\overline{P_{\mathcal{A}}}(s)$ equals the probability that the difference $l - l'$ between the sent digit l and the received one l' is s. For a natural estimate of $\overline{P_{\mathcal{A}}}(s)$ needed in the BB84 protocol, we use the relative frequency of the appearances of $s \in \mathbb{F}_d$ in the sequence of the observed differences $l_i - l_i'$. In words, we use the type P_{U} of U for the estimate of $\overline{P_{\mathcal{A}}}$, where the random variable U is the sequence of the differences $l_i - l_i'$ and we use only the digits l_i and l_i' accompanied by $(\mathsf{a}_i, \mathsf{b}_i, \mathsf{c}_i) = (0,0,1)$. Noting (30), we use similar estimates, say, P_{W}, for $\overline{\overline{P_{\mathcal{A}}}}$, which is obtained from the sequence W of the differences $l_i' - l_i$ of those l_i and l_i' accompanied by $(\mathsf{a}_i, \mathsf{b}_i, \mathsf{c}_i) = (1,1,1)$.

6. Security of the Bennett–Brassard 1984 protocol

In this section, finally, we will establish the security of the BB84 protocol for high rates using theorem 1. This should be done in terms of the random variables involved with the protocol, namely, Alice's sent digits $\boldsymbol{\eta}^{\mathrm{A}} = \left(\eta_1^{\mathrm{A}}, \ldots, \eta_m^{\mathrm{A}}\right)$, Bob's received digits $\boldsymbol{\eta}^{\mathrm{B}} = \left(\eta_1^{\mathrm{B}}, \ldots, \eta_m^{\mathrm{B}}\right)$, C, X, V, a, b, c, E, and T defined below.

In the BB84 protocol, we should consider the possibility of Eve's obtaining knowledge on the key from the data sent through the public channel, i.e., X, C, a, b and c and the non-code digits used for the noise estimation (in our scheme, Γ is determined from C, so that it need not be sent). For the purpose of analysis, we convert (a, b) into $(\mathsf{a}, \mathsf{d} = \mathsf{b} - \mathsf{a})$, where we regard a, b and $\mathsf{d} = (\mathsf{d}_1, \ldots, \mathsf{d}_m)$ as vectors over $\mathbb{F}_2$. Let a' denote the subsequence a_{T} of a (appendix D), where $\mathsf{T} = \{i \mid \mathsf{c}_i = 0 \text{ and } \mathsf{d}_i = 0\}$, the set of the positions of the code digits (with the one element thrown away if $d = 2$ and $n = |\mathsf{T}|$ is initially odd); let a'' denote the subsequence $\mathsf{a}_{\mathsf{T}^{\mathrm{c}}}$ where $\mathsf{T}^{\mathrm{c}} = \{1, \ldots, m\} \setminus \mathsf{T}$; we let Y_{A} [Y_{B}] denote the string of publicly announced non-code (estimation) digits of Alice [Bob], which is a subsequence of $\boldsymbol{\eta}^{\mathrm{A}}$ [$\boldsymbol{\eta}^{\mathrm{B}}$]. Denote the septuple of random variables $(C, \mathsf{a}'', \mathsf{d}, \mathsf{c}, \mathsf{T}, \mathsf{Y}_{\mathrm{A}}, \mathsf{Y}_{\mathrm{B}})$ by S. One criterion for security that takes S into account is $I(\mathsf{V}; \mathsf{EXa}'|\mathsf{S} = s) \approx 0$ for (almost) every definite value of $\mathsf{S} = s$. The rationale hereof is that we should evaluate the security for any definite values of as many parameters as possible. To show that our scheme fulfils this criterion, we modify the argument in section 4.1 as follows.

The argument in section 4.1 is applicable to the above protocol if we add the conditioning on a' and S to the mutual information I. Specifically, we begin with $I(\mathsf{V}; \mathsf{E}|\mathsf{X} = x, \mathsf{Z} = z, \mathsf{a}' = a', \mathsf{S} = s) \leqslant S_{xz,a',s}$ instead of (19). Note that what we have evaluated above is the fidelity $\mathbb{E}_{\mathsf{XZa}'} F_{\mathsf{XZ},\mathsf{a}',s}$ (and the decoding error probability for key transmission) of the codes used on the channel $\mathcal{M}^{\otimes n}$, where $S_{xz,a',s}$ and $F_{xz,a',s}$ are the obvious replacements for S_{xz} and F_{xz} with

conditioning on $\mathsf{a}' = a'$ and $\mathsf{S} = s$, and $\mathbb{E}_{\mathsf{Y}}$ denotes the expectation operator with respect to a random variable Y. Then, in this case, we can replace (22) with

$$I(\mathsf{V}; \mathsf{E}|\mathsf{XZa}', \mathsf{S} = s) \leqslant 2d^{-nE+o(n)}[n(E+R) - o(n)] \tag{32}$$

using the bound $1 - \mathbb{E}F_{\mathsf{XZa}',s} \leqslant d^{-nE(R,\overline{P},\overline{\overline{P}})+o(n)}$ in theorem 1. From the chain rule of mutual information [17, 23], we have

$$I(\mathsf{V}; \mathsf{EXZa}'|\mathsf{S} = s) = I(\mathsf{V}; \mathsf{XZa}'|\mathsf{S} = s) + I(\mathsf{V}; \mathsf{E}|\mathsf{XZa}', \mathsf{S} = s),$$

where $I(\mathsf{V}; \mathsf{XZa}'|\mathsf{S} = s) = 0$ due to the mutual independence of V from $\mathsf{X}, \mathsf{Z}, \mathsf{a}'$ given $\mathsf{S} = s$, and hence, $I(\mathsf{V}; \mathsf{EXa}'|\mathsf{S} = s) \leqslant I(\mathsf{V}; \mathsf{EXZa}'|\mathsf{S} = s) = I(\mathsf{V}; \mathsf{E}|\mathsf{XZa}', \mathsf{S} = s)$. Combining this with (32), we obtain

$$I(\mathsf{V}; \mathsf{EXa}'|\mathsf{S} = s) \leqslant 2d^{-nE+o(n)}[n(E+R) - o(n)]. \tag{33}$$

Note that n is also a random variable, which is a function of m and $\mathsf{S} = s$.

Now it is time to clarify the meaning of what is stated in step (vii) of the BB84 protocol in section 4. Recall our assumption $p_{\mathrm{a}}, p_{\mathrm{b}}, p_{\mathrm{c}} \in (0, 1)$ and (24), which imply

$$0 < r < 1,$$

as well as that the channel $\mathcal{M} = (1-r)\mathcal{A} + r\mathcal{A}'$ stands for Eve's action, which implies $\overline{P_{\mathcal{M}}} = (1-r)\overline{P_{\mathcal{A}}} + r\overline{\overline{P_{\mathcal{A}}}^{\mathsf{f}}}$ and $\overline{\overline{P_{\mathcal{M}}}} = (1-r)\overline{\overline{P_{\mathcal{A}}}} + r\overline{P_{\mathcal{A}}}$, where the operation f on probability distributions is defined by

$$q^{\mathsf{f}}(t) = q(-t), \qquad t \in \mathbb{F}_d.$$

Let Alice and Bob choose a moderate number $E > 0$ as a wanted speed of convergence of the amount of the possible information leakage $I(\mathsf{V}; \mathsf{EXa}'|\mathsf{S} = s)$ as well as a sufficiently small positive constant ε. They use the estimate P_{U} of $\overline{P_{\mathcal{A}}}$ and the estimate P_{W} of $\overline{\overline{P_{\mathcal{A}}}}$ in section 5. Let $\mathcal{G}$ consist of triples (α, p, q), where $0 \leqslant \alpha \leqslant 1$, and p, q are distributions on $\mathbb{F}_d$. With a triple $(\alpha, p, q) \in \mathcal{G}$, we associate a probability distribution on $\{0, 1\} \times \mathbb{F}_d$, which we denote by $Q_{\alpha,p,q}$ and specify by $Q_{\alpha,p,q}(0, x) = (1-\alpha)p(x)$ and $Q_{\alpha,p,q}(1, x) = \alpha q(x)$, $x \in \mathbb{F}_d$. Let λ_m [λ'_m] denote the number of samples used for the estimation of $\overline{P_{\mathcal{A}}}$ [$\overline{\overline{P_{\mathcal{A}}}}$], and put $\nu = \lambda_m + \lambda'_m$.

In step (vii), they choose a rate R such that $E(R, (1-\alpha)p + \alpha q^{\mathsf{f}}, (1-\alpha)q + \alpha p) \geqslant E$ for any triple $(\alpha, p, q) \in \mathcal{G}$ such that $\|Q_{\alpha,p,q} - Q_{\lambda'_m/\nu,\mathsf{P}_{\mathsf{U}},\mathsf{P}_{\mathsf{W}}}\|_1 \leqslant \varepsilon$, and a code of rate R and fidelity not smaller than $1 - d^{-nE(R,\overline{P_{\mathcal{L}}},\overline{\overline{P_{\mathcal{L}}}})+o(n)}$ for any channel $\mathcal{L}$, the existence of which is ensured by theorem 1. (The function $o(n)$ is explicitly given in remark 4 to theorem 1.)

For simplicity, we restrict our attention to the almost sure event where $\nu/m \to [(1-p_{\mathrm{a}})(1-p_{\mathrm{b}}) + p_{\mathrm{a}}p_{\mathrm{b}}]p_{\mathrm{c}} > 0$ as $m \to \infty$, which directly follows from the strong law of large numbers applied to $(\mathsf{d}_i, \mathsf{c}_i), i = 1, 2, \ldots$ (e.g., [44]). For any m, if $\left\| Q_{r,\overline{P_{\mathcal{A}}},\overline{\overline{P_{\mathcal{A}}}}} - Q_{\lambda'_m/\nu,\mathsf{P}_{\mathsf{U}},\mathsf{P}_{\mathsf{W}}} \right\|_1 \leqslant \varepsilon$, then $E(R, \overline{P_{\mathcal{M}}}, \overline{\overline{P_{\mathcal{M}}}}) \geqslant E$ as desired. Owing to (12), the probability (conditioned on specific values of d, c) of the event of estimation failure where $\left\| Q_{r,\overline{P_{\mathcal{A}}},\overline{\overline{P_{\mathcal{A}}}}} - Q_{\lambda'_m/\nu,\mathsf{P}_{\mathsf{U}},\mathsf{P}_{\mathsf{W}}} \right\|_1 > \varepsilon$ is upper-bounded by

$$d^{-\nu \min_{Q:\|Q-Q_{r,\overline{P_{\mathcal{A}}},\overline{\overline{P_{\mathcal{A}}}}}\|_1 \geqslant \varepsilon} D(Q\|Q_{r,\overline{P_{\mathcal{A}}},\overline{\overline{P_{\mathcal{A}}}}})+o(m)}, \tag{34}$$

and this goes to zero with probability one in our almost sure event.

Hence, the above version of the BB84 protocol is secure in the sense that with Eve's attack modelled as a tensor product form of identical copies of a CP instrument, for any such instrument, either 'the mutual information between the key and the eavesdropper's obtained data, together with the decoding error probability for the key transmission, is upper-bounded by $d^{-nE+o(n)}$, where E is positive' or 'the probability that the detection of eavesdroppers fails

is exponentially close to zero'. Especially, reliable and secure key transmission is possible with this protocol at any rate below

$$(1-p_{\rm c})(1-p_{\rm a}-p_{\rm b}+2p_{\rm a}p_{\rm b})[1-2\max\{H((1-r)\overline{P_{\mathcal{A}}}+r\overline{\overline{P_{\mathcal{A}}}}^{\rm f}),\, H((1-r)\overline{\overline{P_{\mathcal{A}}}}+r\overline{P_{\mathcal{A}}})\})], \tag{35}$$

where the rate indicates the ratio of the length of the key to the number of uses of the channel, rather than to the code length of the incorporated CSS code.

7. Discussions

The achievability of the rate $[1-2h(\delta_X+\delta_Z)]/4$, where $\delta_X=\overline{\overline{P_{\mathcal{A}}}}(1), \delta_Z=\overline{P_{\mathcal{A}}}(1)\leqslant 1/2$ may be implicit in [6] though their error rates may differ from our δ_X and δ_Z. This bound can be understood to be obtained by using the exponent $E_{\rm GV}(R,P_{\mathcal{M}})=\min_{1-2h(\overline{Q}(1)+\overline{\overline{Q}}(1))\leqslant R \text{ or } \overline{Q}(1)+\overline{\overline{Q}}(1)\geqslant 1} D(Q\|P_{\mathcal{M}})$ in place of $E(R,\overline{P_{\mathcal{M}}},\overline{\overline{P_{\mathcal{M}}}})$ of theorem 1. Specifically, this follows from the Gilbert–Varshamov bound for CSS codes [10] and Sanov's theorem in large deviation theory (e.g., [22, 23]) or (12). (For the present purpose, we need only the upper bound on the probability in question, so that half of Sanov's theorem, namely, (12), is enough.) Shor and Preskill [6] also mentioned a higher rate which corresponds to $[1-2h((\delta_X+\delta_Z)/2)]/4$, i.e., (35) with $p_{\rm a}=p_{\rm b}=p_{\rm c}=1/2$ or

$$[1-2H(P_{\mathcal{M}})]/4 \qquad (d=2). \tag{36}$$

This rate is established by theorem 1 (section 3) rigorously. Another achievable rate is presented in appendix B. Several other achievable rates (or tolerable error rates) have been mentioned in the literature (e.g., [7, equation (38)], [45, 46]) without details on their code structures.

8. Conclusion

In summary, we have established achievable rates in the BB84 protocol. This improves the one based on the Gilbert–Varshamov bound for CSS codes, which may be implicit in Shor and Preskill's security proof. Specifically, in this paper the existence of a version of the BB84 protocol with exponential convergence of the mutual information between Alice and Eve to zero for any rate below the number in (35) was proved. Several issues lacking in the literature were pointed out and resolved (cf criticisms of Yuen [48, appendix A] on other security proofs). Namely, the existence of CSS codes robust against fluctuations of channel parameters was proved, and the decoding error probability for key transmission, together with the mutual information, was shown to decrease exponentially. Especially, it was proved that codes of 'balanced' weight spectra (corollary 2) achieve the coding rate $1-2h((\delta_X+\delta_Z)/2)$ for $d=2$, where $\delta_X=\overline{\overline{P_{\mathcal{A}}}}(1), \delta_Z=\overline{P_{\mathcal{A}}}(1)$. A proof of the security of a BB84-type protocol for joint attacks is given in appendix C.

In a seemingly less practical but theoretically interesting setting where Eve's attack is known to Alice and Bob beforehand, the optimum rate has recently been obtained in [49].

Acknowledgments

The author appreciates a comment of Masahito Hayashi on an earlier version of this paper that the security proof should extend to the case of joint attacks as well as valuable discussions with him. The author is grateful to Hiroshi Imai for the support.

Appendix A. Proofs of subsidiary results

A.1. Proof of the fidelity bound (27)

The bound directly follows from the argument in the two paragraphs containing equations (18)–(24) of [7, section III-B] for $d = 2$. The entanglement distillation protocol they used is the same as Shor and Preskill's [6] and can be interpreted as follows for our purposes. Given a bipartite state $\overline{\mathsf{M}}_n(\mathcal{V}_n) = [\mathcal{I} \otimes \mathcal{V}_n](|\overline{\Psi}\rangle\langle\overline{\Psi}|)$, where $|\overline{\Psi}\rangle = d^{-n/2} \sum_{\xi,y} |\overline{\xi, y}\rangle \otimes |\overline{\xi, y}\rangle$, where $\{|\overline{\xi, y}\rangle\}_y$ is an orthonormal basis of $\mathcal{Q}_\xi$. Alice performs the local measurement $\{\Pi_\xi\}$ on the first half of the system, where Π_ξ denotes the projection onto the code space $\mathcal{Q}_\xi$, and Bob performs the recovery operation for the N_J-correcting code $\mathcal{Q}_\xi$ knowing that Alice's measurement result is ξ. Since Alice obtains each result ξ with equal probability, the lower bound of [7] serves as that on the average entanglement fidelity of the code $(\mathcal{Q}_\xi, \mathcal{R}_\xi)$ in question.

The bound (27) for $d \geqslant 2$, together with its tightness, follows from the formula for 'discrete twirling' ([50] and references therein) and the properties of the symplectic codes [27]. It is remarked that a similar bound was given by the present author [25, lemma 5]; we can rephrase this bound in terms of the entanglement fidelity F_e using the relation

$$K(K+1)^{-1}[1 - F_\mathrm{e}(K^{-1}I, \mathcal{A})] = 1 - \mathbb{E}_\varphi \langle\varphi|\mathcal{A}(|\varphi\rangle\langle\varphi|)|\varphi\rangle,$$

where $\mathcal{A}$ is a CP map on $\mathsf{L}(H)$ with $\dim H = K$, and $\mathbb{E}_\varphi$ denotes the expectation operator with $\varphi = |\varphi\rangle$ regarded as uniformly distributed over all unit vectors in H [51], though the resulting bound has the form $1 - F'_\mathrm{e} \leqslant (K+1)K^{-1} \sum_{y \in J^\mathrm{c}} P_{\mathcal{V}_n}(y)$, which is weaker than (27) by the asymptotically negligible factor of $(K+1)K^{-1}$.

A.2. Proof of (30)

First, observe, by the definition of M_1 in (25) and that of $|\Psi_y\rangle$ in (26), that $P_\mathcal{A}(s,t)$ can be written as

$$P_\mathcal{A}(s,t) = \sum_i \left|d^{-1}\mathrm{Tr} A_i^\dagger X^s Z^t\right|^2, \qquad s,t \in \mathbb{F}_d$$

for a CP map $\mathcal{A}(\sigma) = \sum_i A_i \sigma A_i^\dagger$. Then, for $\mathcal{A}' = \mathcal{U}^{-1}\mathcal{A}\mathcal{U}$, we have

$$\begin{aligned} P_{\mathcal{A}'}(s,t) &= \sum_i |d^{-1}\mathrm{Tr}(U^\dagger A_i U)^\dagger X^s Z^t|^2 \\ &= \sum_i \left|d^{-1}\mathrm{Tr} A_i^\dagger U X^s U^\dagger U Z^t U^\dagger\right|^2 \\ &= \sum_i \left|d^{-1}\mathrm{Tr} A_i^\dagger Z^{-s} X^t\right|^2 \end{aligned}$$

where we used the relations $UXU^\dagger = Z^{-1}$ and $UZU^\dagger = X$ for the last equality. Since $Z^{-s}X^t$ is the same as $X^t Z^{-s}$ up to a phase factor, ω^{st}, by the commutation relation $XZ = \omega ZX$ or (3), we have $P_{\mathcal{A}'}(s,t) = P_\mathcal{A}(t,-s)$, as promised.

A.3. Proof that $\overline{P}^n(\Gamma'^\mathrm{c}_n)$ is the decoding error probability for key transmission

The probability in question has the form $[p_1 \cdots p_n](T)$, where p_i are probability distributions on $\mathbb{F}_d$ and $T \subseteq \mathbb{F}_d^n$ (in the present case, p_i are identically equal to $\overline{P}$), while the ith transmitted digit suffers the probabilistic change described by a channel matrix, say, $Q_i(y_i|x_i)$ with $p_i(z_i) = d^{-1}\sum_{x_i \in \mathbb{F}_d} Q_i(x_i - z_i|x_i)$ as already argued in section 5. Putting

$q_i(z_i|x_i) = Q_i(x_i - z_i|x_i)$, $[q_1 \cdots q_n](z_1, \ldots, z_n|x_1, \ldots, x_n) = q_1(z_1|x_1) \cdots q_n(z_n|x_n)$, and recalling the decoding procedure in steps (viii)–(x) of the protocol, we see the decoding error probability is given by $d^{-n} \sum_{x \in \mathbb{F}_d^n} [q_1 \cdots q_n](T|x) = [p_1 \cdots p_n](T)$, as desired.

Appendix B. Minimum conditional entropy decoding

In this appendix, a decoding strategy for CSS codes in the BB84 protocol that results in an improvement on the achievable rate, especially when $r = 1/2$, is proposed.

Define μ_m and μ'_m by $\mu_m = |\{i|\, 1 \leqslant i \leqslant m, (\mathsf{a}_i, \mathsf{b}_i, \mathsf{c}_i) = (0, 0, 0)\}|$ and $\mu'_m = |\{i \mid 1 \leqslant i \leqslant m, (\mathsf{a}_i, \mathsf{b}_i, \mathsf{c}_i) = (1, 1, 0)\}|$, where m is the number of whole sent digits. In the proposed scheme, Alice and Bob use $\min\{\mu_m, \mu'_m\}$ digits with $(\mathsf{a}_i, \mathsf{b}_i, \mathsf{c}_i) = (0, 0, 0)$ and the same number of digits with $(\mathsf{a}_i, \mathsf{b}_i, \mathsf{c}_i) = (1, 1, 0)$ for CSS coding discarding excessive digits if they exist. If $r = 1/2$, the loss of digits in this process is small by the strong law of large numbers.

In the conventional decoding schemes for CSS codes in the BB84 protocol [6–8] or that in section 6, Bob does not use the information as to whether $\mathsf{a}_i = \mathsf{b}_i = 0$ or $\mathsf{a}_i = \mathsf{b}_i = 1$ has occurred; he considers the channel as the mixture of $\mathcal{A}$ and $\mathcal{A}' = \mathcal{U}^{-1}\mathcal{A}\mathcal{U}$. To improve on the achievable rates in (35) for $r = 1/2$, we employ a decoding strategy that uses the information on a_i $(= \mathsf{b}_i)$, minimum conditional entropy decoding, so to speak. Specifically, we associate each word xx', where xx' denotes the concatenation of $x \in \mathbb{F}_d^\nu$ and $x' \in \mathbb{F}_d^\nu$, and x $[x']$ is composed of the digits for which $\mathsf{a}_i = 0$ $[\mathsf{a}_i = 1]$, with the conditional entropy

$$h_{\mathrm{c}}(x, x') = \frac{H(\mathsf{P}_x) + H(\mathsf{P}_{x'})}{2}, \tag{B.1}$$

and *choose a word that minimizes the conditional entropy h_{c} in each coset in $\mathbb{F}_d^n \big/ C^\perp$ to obtain a transversal* Γ. The quantity $h_{\mathrm{c}}(x, x')$ can be written solely with P_x and $\mathsf{P}_{x'}$, so that we will occasionally denote $h_{\mathrm{c}}(x, x')$ by $h_{\mathrm{c}}(\mathsf{P}_x, \mathsf{P}_{x'})$.

Theorem 2. *Let a number $0 \leqslant R \leqslant 1$ be given. There exists a sequence of pairs $\{(C_\nu, \Gamma_\nu)\}_{\nu \in \mathbb{N}}$, each consisting of a self-orthogonal code $C_\nu \subseteq \mathbb{F}_d^{2\nu}$ with $2\nu - 2\dim C_\nu \geqslant 2\nu R$ and a set Γ_ν of coset representatives of $\mathbb{F}_d^{2\nu} \big/ C_\nu^\perp$ such that for any pair of probability distributions P_0 and P_1 on $\mathcal{X}$,*

$$P_0^\nu P_1^\nu (J(\Gamma'_\nu)^{\mathrm{c}}) \leqslant \overline{P_0}^\nu \overline{P_1}^\nu \left(\Gamma_\nu'^{\mathrm{c}}\right) + \overline{\overline{P_0}}^\nu \overline{\overline{P_1}}^\nu \left(\Gamma_\nu'^{\mathrm{c}}\right) \leqslant d^{-2\nu E_{\mathrm{c}}(R, P_0, P_1) + o(\nu)},$$

where

$$\Gamma'_\nu = \Gamma_\nu + C_\nu,$$

$$E_{\mathrm{c}}(R, P_0, P_1) = \min\{E^*(R, \overline{P_0}, \overline{P_1}), E^*(R, \overline{\overline{P_0}}, \overline{\overline{P_1}})\},$$

$$E^*(R, p_0, p_1) = \min_{Q_0, Q_1} [D(Q_0 \| p_0) + D(Q_1 \| p_1) + |1 - 2h_{\mathrm{c}}(Q_0, Q_1) - R|^+]/2,$$

and the minimization with respect to (Q_0, Q_1) is taken over all pairs of probability distributions on $\mathbb{F}_d$.

The proof is similar to that of theorem 1. In this case, we pair up digits in a sequence $xy = (x_1, \ldots, x_\nu, y_1, \ldots, y_\nu)$ as $(x_1, y_1), \ldots, (x_\nu, y_\nu)$ to regard it as a sequence from $\mathcal{X}^\nu$, $\mathcal{X} = \mathbb{F}_d \times \mathbb{F}_d$. Then, to evaluate the fidelity of the codes, we use the existence proof of 'balanced' codes in section 3, which is clearly valid if we use types in $\mathcal{P}_\nu(\mathcal{X})$ in place of types in $\mathcal{P}_n(\mathbb{F}_d)$, and the similarly modified permutation argument for sequences in $\mathcal{X}^\nu$. By this theorem with $P_0 = P_{\mathcal{A}}$ and $P_1 = P_{\mathcal{U}^{-1}\mathcal{A}\mathcal{U}}$, the rate $(1 - p_{\mathrm{c}})[1 - H(\overline{\mathcal{A}}) - H(\overline{\overline{\mathcal{A}}})]/2$ is achievable with the BB84 protocol. The result extends to an arbitrary rational r; for example, for $r = 1/3$, we can use types in $\mathcal{P}_\nu\left(\mathbb{F}_d^3\right)$.

Appendix C. Security against joint attacks

In this appendix, we will prove the security of the following modified BB84 protocol against any joint attack through this paper's approach. Especially, an exponential upper bound on the information leakage to Eve, which holds for finite m and n, will be established. This modification to the protocol is essentially due to [46], and its main idea is as follows. In the protocol, about $p_{\mathrm{a}}p_{\mathrm{b}}m$ digits with $\mathsf{a}_i = \mathsf{b}_i = 1$ are used for estimation of the level of errors caused by the Weyl unitary Z, the same number of randomly chosen digits with $\mathsf{a}_i = \mathsf{b}_i = 0$ are used for estimation of those caused by X, and the about $[(1 - p_{\mathrm{a}})(1 - p_{\mathrm{b}}) - p_{\mathrm{a}}p_{\mathrm{b}}]m$ remaining digits with $\mathsf{a}_i = \mathsf{b}_i = 0$ are used for CSS coding. In this paper, we assume that the parameters $p_{\mathrm{a}} = \Pr\{\mathsf{a}_i = 1\}$, $p_{\mathrm{b}} = \Pr\{\mathsf{b}_i = 1\} \in (0, 1/2)$ are independent of m in order that the law of large numbers (or any other refined law such as Sanov's theorem) is applicable to $\{(\mathsf{a}_i, \mathsf{b}_i)\}$; in [46], it is assumed p_{a}, p_{b} depend on m so that r in (24) goes to 0 as m goes to infinity (seemingly only for the purpose of analysis of security); Hayashi [52] described an idea for a possible proof of security of this protocol using the codes in theorem 1 (in fact, the modification for $d = 2$ in section 3.2) for small enough r.

Let $\mathcal{S}_n$ be the symmetric group on $\{1, \ldots, n\}$ as before. For the proof for joint attacks, we should be more specific about the expression of the key. Given a self-orthogonal code C, the key, which is actually a string of $k = n - 2\kappa$ digits, is encoded into $C^{\perp}/C$. The encoding map, $f_{C,h_1,\ldots,h_k}$, can be given as $f_{C,h_1,\ldots,h_k} : (\sigma_1, \ldots, \sigma_k) \mapsto C + \sigma_1 h_1 + \cdots + \sigma_k h_k$, where $\{h_1, \ldots, h_k\}$, together with a basis of C, gives a basis of $C^{\perp}$. Thus, Alice and Bob specify their cryptographic code by $(g_1, \ldots, g_\kappa; h_1, \ldots, h_k; \Gamma)$; in this appendix, we always assume $g_1, \ldots, g_\kappa$ form a basis of C. We use the syndromes $\mathsf{X}', \mathsf{Z}' \in \mathbb{F}_d^\kappa$ for the code $C^{\perp}$ and the coset representatives X, Z for $\mathbb{F}_d^n / C^{\perp}$ interchangeably since they are in one-to-one correspondence with each other once the generator $g_1, \ldots, g_\kappa$ of C is fixed: $\mathsf{X}H^{\mathrm{T}} = \mathsf{X}'$, where $H^{\mathrm{T}} = \left[g_1^{\mathrm{T}} \cdots g_\kappa^{\mathrm{T}}\right]$. In places where we want to distinguish a random variable from its realization, we use sanserif or bold font for the former and italic font for the latter as in the text.

Modified BB84 protocol

(i) The sender, Alice, and the receiver, Bob, do steps (ii)–(iv) for each $i = 1, \ldots, m$.
(ii) Alice chooses a random bit a_i. She prepares her system in one state that is chosen uniformly randomly from the Z-basis if a_i is 0, or in one from the X-basis if a_i is 1.
(iii) Alice sends the prepared state to Bob.
(iv) Bob chooses another random bit b_i, and receives the state, performs the Z-basis measurement if b_i is 0, or X-basis measurement if b_i is 1.
(v) Alice and Bob announce $\mathsf{a} = (\mathsf{a}_1, \ldots, \mathsf{a}_m)$ and $\mathsf{b} = (\mathsf{b}_1, \ldots, \mathsf{b}_m)$, respectively.
(vi) Alice and Bob discard any results where $\mathsf{a}_i \neq \mathsf{b}_i$. Let $\mathsf{T}_{\mathrm{sift}} = \{i | \mathsf{a}_i = \mathsf{b}_i\}$ (the remaining places) and $\boldsymbol{\mu} = |\mathsf{T}_{\mathrm{sift}}|$. (In the case where $d = 2$, it is assumed that $\boldsymbol{\mu}$ is even; if not, they disregard another place chosen randomly from $\{i | \mathsf{a}_i = \mathsf{b}_i\}$.) Put $\mathsf{n} \stackrel{\mathrm{def}}{=} \boldsymbol{\mu} - 2|\{i | \mathsf{a}_i = \mathsf{b}_i = 1\}|$. If $\mathsf{n} \leqslant 0$ or $\mathsf{n} = \boldsymbol{\mu}$, they abort the protocol. To divide $\mathsf{T}_{\mathrm{sift}} = \{i | \mathsf{a}_i = \mathsf{b}_i\}$ into two parts, i.e., that for CSS coding T, and that for estimation for the noise level $\mathsf{T}_{\mathrm{sift}} \backslash \mathsf{T}$, they do the following. From $\{i | \mathsf{a}_i = \mathsf{b}_i = 0\}$, Alice randomly chooses (according to the uniform distribution over all possible choices) $(\boldsymbol{\mu} - \mathsf{n})/2 = |\{i | \mathsf{a}_i = \mathsf{b}_i = 1\}|$ places where digits are to be used for the estimation of the level of errors caused by the Weyl unitary X, and tells the choice to Bob. The set of the remaining n places with $\mathsf{a}_i = \mathsf{b}_i = 0$ constitutes T. The digits with $\mathsf{a}_i = \mathsf{b}_i = 1$ will also be used for the noise estimation.

(vii) Alice and Bob announce the values of their estimation digits thus chosen (which will be Y_A and Y_B below) and from these, estimate the noise level, and decide on a secure transmission rate, and a CSS code $(g_1, \ldots, g_\kappa; h_1, \ldots, h_k; \Gamma)$ to be used.

(viii) Alice chooses a random permutation π from $\mathcal{S}_\mathsf{n}$ according to the uniform distribution, and tells the choice to Bob.

(ix) Alice announces the coset $y+\pi(C^\perp)$, where y $(= w+v+x)$ is the string consisting of the remaining code digits. In other words, she announces the syndrome $\mathsf{X}' = (y \cdot \pi(g_j))_{j=1}^{j=\kappa}$, which is in one-to-one correspondence with the coset representative $x \in \mathbb{F}_d^n / \pi(C^\perp)$ of the coset $y + \pi(C^\perp)$.

(x) Bob subtracts the coset representative $x \in \mathbb{F}_d^n / \pi(C^\perp)$ from his code digits, $y - e$, and corrects the result $y - x - e$ to a codeword u in $\pi(C)^\perp$, where he uses the decoder such that $u = y - x$ if $e \in \pi(\Gamma)$.

(xi) Alice uses $\boldsymbol{\sigma} = f^{-1}_{\pi(C),\pi(h_1),\ldots,\pi(h_k)}[y-x+\pi(C)]$ and Bob uses $\boldsymbol{\sigma}' = f^{-1}_{\pi(C),\pi(h_1),\ldots,\pi(h_k)}[u+\pi(C)]$ as the key.

Let a TPCP map $\mathcal{A} : \mathsf{L}(\mathsf{H}^{\otimes m}) \to \mathsf{L}(\mathsf{H}^{\otimes m})$ represent the whole action of Eve (plus the other environment). This means that there exists a decomposition (CP instrument) $\{\mathcal{A}_i\}_i$ such that $\mathcal{A} = \sum_i \mathcal{A}_i$, where $\mathcal{A}_i$ are trace-nonincreasing CP maps, and when the initial state of the system of the whole sent digits is ρ, Eve obtains data $\mathsf{E} = i$ with probability $\mathrm{Tr}\mathcal{A}_i(\rho)$ leaving the system in state $\mathcal{A}_i(\rho)/\mathrm{Tr}\mathcal{A}_i(\rho)$. Here, the decomposition may depend on the other random variables available to Eve. However, the proof relies on the assumption that $\mathcal{A}$ does not depend on a, b, which is needed to use lemma 5. Recalling the interpretation of the $Z \otimes Z^{-1}$ measurement in section 5 and using the $\overline{U} \otimes U$-invariance of $|\Psi\rangle$, where $U = d^{-1/2} \sum_{j,l \in \mathbb{F}_d} \omega^{jl} |j\rangle\langle l|$ and $\overline{U} = U^{-1}$, and the relation $X \otimes X |\Psi_{(s,t)}\rangle = \omega^t |\Psi_{(s,t)}\rangle$ in addition to (31), we note that Alice's sent digits $\boldsymbol{\eta}^\mathrm{A} = \left(\eta_1^\mathrm{A}, \ldots, \eta_m^\mathrm{A}\right)$ and Bob's received digits $\boldsymbol{\eta}^\mathrm{B} = \left(\eta_1^\mathrm{B}, \ldots, \eta_m^\mathrm{B}\right)$ are mathematically equivalent to the results of the following fictional measurements. We imagine that Alice and Bob have a bipartite system in state $\mathsf{M}_m(\mathcal{A})$, and observe $O_{a_i}^{(i)}$, $i = 1, \ldots, m$, and $O_{b_i}^{(i)}$, $i = 1, \ldots, m$, respectively, where $O_{a_i}^{(i)} = I^{\otimes(i-1)} \otimes O_{a_i} \otimes I^{\otimes(m-i)} \in \mathsf{L}(\mathsf{H}^{\otimes m})$. Here, O_0 is the 'observable' Z to distinguish the eigenvalues of Z (more precisely, the Z-basis measurement $\{|i\rangle\langle i|\}_{i=0}^{d-1}$), and O_1 denotes X, i.e, $\{|i\rangle'\langle i|'\}_{i=0}^{d-1}$. Then, $\boldsymbol{\eta}^\mathrm{A}$ and $\boldsymbol{\eta}^\mathrm{B}$ are the same as the sequence of the measurement results of Alice and that of Bob, respectively, for $d = 2$ (and this is true if each digit $t \in \mathbb{F}_d$ of $\boldsymbol{\eta}^\mathrm{A}$ with $\mathsf{a}_i = 1$ is replaced by $-t$ for $d > 2$). Moreover, we can relate $\boldsymbol{\eta}^\mathrm{A}$ and $\boldsymbol{\eta}^\mathrm{B}$ to the classical random variables $(\boldsymbol{\xi}_i, \boldsymbol{\zeta}_i)$, $i = 1, \ldots, m$, which are drawn according to $P_\mathcal{A}$ defined by (28) as follows. We have $\boldsymbol{\xi}_{\mathsf{T}_0} = \boldsymbol{\eta}^\mathrm{A}_{\mathsf{T}_0} - \boldsymbol{\eta}^\mathrm{B}_{\mathsf{T}_0}$ for the subsequence $\boldsymbol{\xi}_{\mathsf{T}_0}$ of $\boldsymbol{\xi} = \boldsymbol{\xi}_1 \cdots \boldsymbol{\xi}_m$ (appendix D), where $\mathsf{T}_0 = \{i \,|\, \mathsf{a}_i = \mathsf{b}_i = 0\}$, and $\boldsymbol{\zeta}_{\mathsf{T}_1} = \boldsymbol{\eta}^\mathrm{B}_{\mathsf{T}_1} - \boldsymbol{\eta}^\mathrm{A}_{\mathsf{T}_1}$, where $\mathsf{T}_1 = \{i \,|\, \mathsf{a}_i = \mathsf{b}_i = 1\}$.

In what follows, we evaluate the fidelity, $F_{(T_\mathrm{sift},\mu,n)}$ defined below, of the symplectic code underlying the protocol, which is, in essence, the CSS code $(g_1, \ldots, g_\kappa; h_1, \ldots, h_k; \Gamma)$. As before, the fidelity can be written in terms of the classical random variables $\boldsymbol{\xi}, \boldsymbol{\zeta}$. (In fact, the underlying code is the combined system of this CSS code $\mathsf{CSS}(C, \Gamma)$ and a trivial symplectic code, which conveys no information (i.e., protects only a one-dimensional subspace of $\mathsf{H}^{\otimes(m-n)}$), where each code does its job independently. The trivial code is the collection of simultaneous eigenspaces of $\left\{O_{a_i}^{(i)'} \mid i \in \{1, \ldots, m\} \setminus \mathsf{T}\right\}$, where $O_{a_i}^{(i)'} \in \mathsf{L}(\mathsf{H}^{\otimes(m-n)})$ is obtained from $O_{a_i}^{(i)} = I^{\otimes(i-1)} \otimes O_{a_i} \otimes I^{\otimes(m-i)} \in \mathsf{L}(\mathsf{H}^{\otimes m})$ by neglecting I on the systems for T. The combined code is an $N_{J(\Gamma) \times \mathbb{F}_d^{2(m-n)}}$-correcting symplectic code. Here, the appropriate permutation on $\{1, \ldots, m\}$ is to be understood.)

Let Y_A [Y_B] denote the string of publicly announced estimation digits of Alice [Bob], which is a subsequence of $\boldsymbol{\eta}^\mathrm{A}$ [$\boldsymbol{\eta}^\mathrm{B}$]; assume, say, the first half of Y_A [Y_B] consists of the digits accompanied by $\mathsf{a}_i = \mathsf{b}_i = 0$ and the latter half is for $\mathsf{a}_i = \mathsf{b}_i = 1$. Recall

$\mathsf{T} \subseteq \{1, \ldots, m\}$ denotes the set of the positions of the code digits. Eve can have access to a, b, X', $\mathsf{S}' = (\mathsf{T}_{\rm sift}, \boldsymbol{\mu}, \mathsf{n})$, $\mathsf{Y}_{\rm A}$, $\mathsf{Y}_{\rm B}$, T, k, $\mathsf{C}' = (g_1, \ldots, g_\kappa; h_1, \ldots, h_k; \Gamma)$ and $\boldsymbol{\pi}$. In what follows, with $m > 0$ and the realization $\mathsf{S}' = (T_{\rm sift}, \mu, n)$ arbitrarily fixed, we will upper-bound $I(\boldsymbol{\sigma}; \mathsf{E}\mathsf{X}'\mathsf{Y}_{\rm A}\mathsf{Y}_{\rm B}\boldsymbol{\pi}\mathsf{T}\mathsf{a}\mathsf{b}\mathsf{C}'|\mathsf{k}, \mathsf{S}' = (T_{\rm sift}, \mu, n))$ and the probability of key disagreement $\Pr\{\boldsymbol{\sigma} \neq \boldsymbol{\sigma}'|\mathsf{S}' = (T_{\rm sift}, \mu, n)\}$ simultaneously.

In step (vii), Alice and Bob choose the code in the following manner. With a sufficiently small constant $\gamma > 0$ chosen beforehand, they set

$$R(n, \mu, \mathsf{Y}_{\rm A}, \mathsf{Y}_{\rm B}) = 1 - 2\max\left\{H\left(\mathsf{P}_{\boldsymbol{\xi}_{\rm est}}\right), H\left(\mathsf{P}_{\boldsymbol{\zeta}_{\rm est}}\right)\right\} - 2\gamma, \tag{C.1}$$

where $\boldsymbol{\xi}_{\rm est}$ and $\boldsymbol{\zeta}_{\rm est}$ represent the first half of $\mathsf{Y}_{\rm A} - \mathsf{Y}_{\rm B}$ and the second half of $\mathsf{Y}_{\rm B} - \mathsf{Y}_{\rm A}$, respectively, calculate the minimum k of the possible code size k' with $k'/n \geqslant R(n, \mu, Y_{\rm A}, Y_{\rm B})$, set $\mathsf{k} = k$, and choose a code $(g_1, \ldots, g_\kappa; h_1, \ldots, h_k; \Gamma)$ from the shared list of codes satisfying the property of corollary 2. Note that $\boldsymbol{\xi}_{\rm est} = \boldsymbol{\xi}_{\mathsf{T}'}$, where $\mathsf{T}' \subseteq \{i \mid \mathsf{a}_i = \mathsf{b}_i = 0\}$ stands for the places for the estimation, and $\boldsymbol{\zeta}_{\rm est} = \boldsymbol{\zeta}_{\mathsf{T}_1}$ with $\mathsf{T}_1 = \{i \mid \mathsf{a}_i = \mathsf{b}_i = 1\}$.

Let $F_{k,(T_{\rm sift},\mu,n)}$ be $|\mathcal{S}_n|^{-1}\sum_{\pi\in\mathcal{S}_n} P_{[\boldsymbol{\xi}_{\rm code},\boldsymbol{\zeta}_{\rm code}]|\mathsf{k}=k,\mathsf{S}'=(T_{\rm sift},\mu,n)}\{J[\pi(\Gamma+C)]\}$, where $\boldsymbol{\xi}_{\rm code} = \boldsymbol{\xi}_{\mathsf{T}}$ and $\boldsymbol{\zeta}_{\rm code} = \boldsymbol{\zeta}_{\mathsf{T}}$. Then,

$$1 - F_{k,(T_{\rm sift},\mu,n)} \leqslant B\left(P_{\boldsymbol{\xi}_{\rm code}|\mathsf{k}=k,\mathsf{S}'=(T_{\rm sift},\mu,n)}\right) + B\left(P_{\boldsymbol{\zeta}_{\rm code}|\mathsf{k}=k,\mathsf{S}'=(T_{\rm sift},\mu,n)}\right), \tag{C.2}$$

where $B(Q) = |\mathcal{S}_n|^{-1}\sum_{\pi\in\mathcal{S}_n} Q[\pi(\Gamma + C)^{\rm c}]$. The part bounding $B(p)$ in section 3 (the last paragraph in section 3.1), as well as its modification for $d = 2$ in section 3.2, applies verbatim to the present case, where we want to upper-bound $B\left(P_{\mathsf{G}|\mathsf{k}=k,\mathsf{S}'=(T_{\rm sift},M,n)}\right)$ for $\mathsf{G} = \boldsymbol{\xi}_{\rm code}, \boldsymbol{\zeta}_{\rm code}$, if we replace p^n, $B(p)$ in (16) and $d^{-nD(p\|Q)}$ in (18) by $P_{\mathsf{G}|\mathsf{k}=k,\mathsf{S}'=(T_{\rm sift},\mu,n),(\mathsf{Y}_{\rm A},\mathsf{Y}_{\rm B})=(Y_{\rm A},Y_{\rm B})}$, $B\left(P_{\mathsf{G}|\mathsf{k}=k,\mathsf{S}'=(T_{\rm sift},\mu,n),(\mathsf{Y}_{\rm A},\mathsf{Y}_{\rm B})=(Y_{\rm A},Y_{\rm B})}\right)$ and $P_{\mathsf{G}|\mathsf{k}=k,\mathsf{S}'=(T_{\rm sift},\mu,n),(\mathsf{Y}_{\rm A},\mathsf{Y}_{\rm B})=(Y_{\rm A},Y_{\rm B})}\left(\mathcal{T}_Q^n\right)$, respectively. Thus, we have

$$\begin{aligned}
&B\left(P_{\boldsymbol{\xi}_{\rm code}|\mathsf{k}=k,\mathsf{S}'=(T_{\rm sift},\mu,n),(\mathsf{Y}_{\rm A},\mathsf{Y}_{\rm B})=(Y_{\rm A},Y_{\rm B})}\right)\\
&\quad\leqslant |\mathcal{P}_n| \sum_{Q\in\mathcal{P}_n} P_{\boldsymbol{\xi}_{\rm code}|\mathsf{k}=k,\mathsf{S}'=(T_{\rm sift},\mu,n),(\mathsf{Y}_{\rm A},\mathsf{Y}_{\rm B})=(Y_{\rm A},Y_{\rm B})}\left(\mathcal{T}_Q^n\right)\\
&\qquad\times \min\left\{\sum_{Q':H(Q')\leqslant H(Q)} d^{nH(Q')-\frac{n-k}{2}-1}, 1\right\}\\
&\quad\leqslant d^d|\mathcal{P}_n|^2 \sum_{Q\in\mathcal{P}_n} \Pr\left\{\mathsf{P}_{\boldsymbol{\xi}_{\rm code}} = Q|\mathsf{k}=k, \mathsf{S}' = (T_{\rm sift}, \mu, n), (\mathsf{Y}_{\rm A}, \mathsf{Y}_{\rm B}) = (Y_{\rm A}, Y_{\rm B})\right\}\\
&\qquad\times d^{-n|1-R(n,\mu,Y_{\rm A},Y_{\rm B})-2H(Q)|^+/2}
\end{aligned}$$

for any k and $(Y_{\rm A}, Y_{\rm B})$ with $\Pr\{\mathsf{k} = k, (\mathsf{Y}_{\rm A}, \mathsf{Y}_{\rm B}) = (Y_{\rm A}, Y_{\rm B})|\mathsf{S}' = (T_{\rm sift}, \mu, n)\} > 0$, as well as the counterpart for $\boldsymbol{\zeta}_{\rm code}$. Substituting (C.1) into these estimates, applying the operation $A \mapsto \sum_{(Y_{\rm A},Y_{\rm B}),k} \Pr\{(\mathsf{Y}_{\rm A}, \mathsf{Y}_{\rm B}) = (Y_{\rm A}, Y_{\rm B}), \mathsf{k} = k|\mathsf{S}' = (T_{\rm sift}, \mu, n)\}A$, and combining them with (C.2), we have the following bound on $F_{(T_{\rm sift},\mu,n)} = \sum_{k=0}^n \Pr\{\mathsf{k} = k|\mathsf{S}' = (T_{\rm sift}, \mu, n)\}F_{k,(T_{\rm sift},\mu,n)}$:

$$\begin{aligned}
1 - F_{(T_{\rm sift},\mu,n)} &\leqslant d^d|\mathcal{P}_n|^2 \sum_{Q\in\mathcal{P}_n, Q'\in\mathcal{P}_{(\mu-n)/2}} \Pr\left\{\mathsf{P}_{\boldsymbol{\xi}_{\rm code}} = Q \text{ and } \mathsf{P}_{\boldsymbol{\xi}_{\rm est}} = Q'|\mathsf{S}' = (T_{\rm sift}, \mu, n)\right\}\\
&\quad\times d^{-n[|H(Q')-H(Q)+\gamma|^+]} + d^d|\mathcal{P}_n|^2 \sum_{Q\in\mathcal{P}_n, Q'\in\mathcal{P}_{(\mu-n)/2}}\\
&\quad\times \Pr\left\{\mathsf{P}_{\boldsymbol{\zeta}_{\rm code}} = Q \text{ and } \mathsf{P}_{\boldsymbol{\zeta}_{\rm est}} = Q'|\mathsf{S}' = (T_{\rm sift}, \mu, n)\right\}d^{-n[|H(Q')-H(Q)+\gamma|^+]}\\
&\leqslant 4d^d|\mathcal{P}_n|^3|\mathcal{P}_{(n+\mu)/2}|^3 d^{-nE_1(\gamma,\alpha)},
\end{aligned} \tag{C.3}$$

where $\alpha = (\mu - n)/(\mu + n)$,

$$E_1(\gamma, \alpha) = \min_{0 \leqslant \varepsilon \leqslant 2} \{(1-\alpha)^{-1}[g(\alpha)\varepsilon]^2/(2\ln d) + |\gamma - \theta(\varepsilon)|^+\},$$

$$\theta(x) = \begin{cases} 0 & \text{for} \quad x = 0 \\ -x \log_d (x/d) & \text{for} \quad 0 < x \leqslant 1/2 \\ 1 & \text{for} \quad 1/2 < x, \end{cases}$$

and

$$g(\alpha) = \frac{\sqrt{\alpha(1-\alpha)}}{\sqrt{\alpha} + \sqrt{1-\alpha}}.$$

To see the last inequality in (C.3), we need the next lemma with $\mathcal{Y} = \mathbb{F}_d$ and $N = (\mu + n)/2$ as well as the continuity of entropy, i.e., that $\|Q - Q'\|_1 \leqslant \varepsilon$ implies $|H(Q) - H(Q')| \leqslant \theta(\varepsilon)$ [17]; we have upper-bounded each summation on the right-hand side by $\sum_\varepsilon 2|\mathcal{P}_N|^2 d^{-N[g(\alpha)\varepsilon]^2/(2\ln d)} d^{-n|\gamma - \theta(\varepsilon)|^+}$ using the lemma, where ε ranges over $\{\varepsilon \mid \exists Q \in \mathcal{P}_n,\ Q' \in \mathcal{P}_{(\mu-n)/2},\ \|Q - Q'\|_1 = \varepsilon\}$, which is not greater than $2|\mathcal{P}_n||\mathcal{P}_N|^3 d^{-nE_1(\gamma,\alpha)}$.

Lemma 5 (random sampling)**.** *Let a finite alphabet $\mathcal{Y}$ and positive integers n and N, $0 < n < N$, be given. Put $\alpha = (N-n)/N$. Assume that Y is an arbitrary random variable taking values in $\mathcal{Y}^N$ and we choose n symbols from Y uniformly randomly. Denote the resulting string by Y' (arranged in an arbitrary order, which does not matter) and the string of the remaining digits by Y''. Then the probability that $\|\mathsf{P}_{\mathsf{Y}'} - \mathsf{P}_{\mathsf{Y}''}\|_1 \geqslant \varepsilon$ is upper-bounded by $2|\mathcal{P}_N(\mathcal{Y})|^2 d^{-N[g(\alpha)\varepsilon]^2/(2\ln d)}$.*

Proof. For a fixed realization y of Y, denote the conditional probability $\Pr\{\mathsf{P}_{\mathsf{Y}'} = Q \text{ and } \mathsf{P}_{\mathsf{Y}''} = Q' | \mathsf{Y} = y\}$ by $W(Q, Q'|y)$ (W is a classical channel). For now imagine that Y is the sequence of independent random variables identically distributed according to $Q \in \mathcal{P}_N(\mathcal{Y})$, and let $(Q^N \times W)[A]$, or the $Q^N \times W$-probability of A, denote the probability of the event A under this condition. The $Q^N \times W$-probability that $\|\mathsf{P}_{\mathsf{Y}'} - \mathsf{P}_{\mathsf{Y}}\|_1 \geqslant \varepsilon'/\sqrt{1-\alpha}$ or $\|\mathsf{P}_{\mathsf{Y}''} - \mathsf{P}_{\mathsf{Y}}\|_1 \geqslant \varepsilon'/\sqrt{\alpha}$ is upper-bounded by $2|\mathcal{P}_N(\mathcal{Y})| d^{-N\varepsilon'^2/(2\ln d)}$ by large deviation theory, i.e., by (12), and Pinsker's inequality $D(Q\|Q') \geqslant \|Q - Q'\|_1^2/(2\ln d)$ [17]. In other words, the probability that $\|\mathsf{P}_{\mathsf{Y}'} - \mathsf{P}_{\mathsf{Y}}\|_1 < \varepsilon'/\sqrt{1-\alpha}$ and $\|\mathsf{P}_{\mathsf{Y}''} - \mathsf{P}_{\mathsf{Y}}\|_1 < \varepsilon'/\sqrt{\alpha}$ is lower-bounded by $1 - 2|\mathcal{P}_N(\mathcal{Y})| d^{-N\varepsilon'^2/(2\ln d)}$. By the triangle inequality, this immediately implies $(Q^N \times W)[\|\mathsf{P}_{\mathsf{Y}'} - \mathsf{P}_{\mathsf{Y}''}\|_1 < (1/\sqrt{\alpha} + 1/\sqrt{1-\alpha})\varepsilon'] \geqslant 1 - 2|\mathcal{P}_N(\mathcal{Y})| d^{-N\varepsilon'^2/(2\ln d)}$. Note that $W(\cdot, \cdot|y)$ is the same for all $y \in \mathcal{Y}^N$ of a fixed type, and hence, $\forall Q', Q'', W(Q', Q''|y) \leqslant (Q^N \times W)[\mathsf{P}_{\mathsf{Y}'} = Q' \text{ and } \mathsf{P}_{\mathsf{Y}''} = Q'']/Q^N\big(\mathcal{T}_Q^N\big)$, where $Q = \mathsf{P}_y$, for any y. Since for any $Q \in \mathcal{P}_N(\mathcal{Y})$, $Q^N\big(\mathcal{T}_Q^N\big) \geqslant |\mathcal{P}_N(\mathcal{Y})|^{-1}$ (in fact, $\max_{P \in \mathcal{P}_N(\mathcal{Y})} Q^N\big(\mathcal{T}_P^N\big) = Q^N\big(\mathcal{T}_Q^N\big)$ [17]), we have $\Pr\{\|\mathsf{P}_{\mathsf{Y}'} - \mathsf{P}_{\mathsf{Y}''}\|_1 \geqslant (1/\sqrt{\alpha} + 1/\sqrt{1-\alpha})\varepsilon' | \mathsf{Y} = y\} \leqslant 2|\mathcal{P}_N(\mathcal{Y})|^2 d^{-N\varepsilon'^2/(2\ln d)}$. Noting this bound is independent of y, we obtain the lemma. □

Remark. In the above application of this lemma, Y' and Y'' are the code digits and estimation digits, respectively. This ensures that $\mathsf{P}_{\mathsf{Y}'}$ and $\mathsf{P}_{\mathsf{Y}''}$ are close with high probability. In the binary case where $\mathcal{Y} = \{0, 1\}$, upper bounds of the form $\exp\{-(N-n)K\varepsilon^2\}$, with some constant K, for the probability that $\mathsf{P}_y(1) - \mathsf{P}_{\mathsf{Y}''}(1) = \varepsilon$ has long been known [53] and most security proofs for QKD use this type of bound (e.g., [5, appendix M, e-Print], [46, lemma 1], [7, equation (25)], [54, appendix, property 16], [55, p 589, exercise 12.27], [52]). An advantage of the above lemma is the applicability to the case where $|\mathcal{Y}| > 2$.

The rest of the task is to relate the fidelity bound in (C.3) to the mutual information as we did in section 6 for individual attacks. In the present case, we initially have

$$I(\boldsymbol{\sigma}; \mathsf{E}|\mathsf{X}'\mathsf{Z}'\mathsf{Y}_\mathrm{A}\mathsf{Y}_\mathrm{B}\pi\mathsf{TabC}'\mathsf{k}, \mathsf{S}' = (T_{\mathrm{sift}}, \mu, n)) \leqslant 2d^{-nE_1(\gamma,\alpha)+o_1(n,\mu)}[n(E_1(\gamma,\alpha)+1) - o_1(n,\mu)]$$

with a negligible function $o_1(n, \mu)$. Note that $\boldsymbol{\sigma}$ is independent of $\mathsf{X}', \mathsf{Z}', \mathsf{Y}_\mathrm{A}, \mathsf{Y}_\mathrm{B}, \pi, \mathsf{T}, \mathsf{a}, \mathsf{b}$ and C' conditionally on k (i.e., $\mathsf{S}''' = (\mathsf{X}', \mathsf{Z}', \mathsf{Y}_\mathrm{A}, \mathsf{Y}_\mathrm{B}, \pi, \mathsf{T}, \mathsf{a}, \mathsf{b}, \mathsf{C}')$, k and $\boldsymbol{\sigma}$ form a Markov chain in this order [17]) given $\mathsf{S}' = (T_{\mathrm{sift}}, \mu, n)$ since the probability of $\boldsymbol{\sigma}$ conditioned on $\mathsf{k} = k, \mathsf{S}''' = s'''$ and $\mathsf{S}' = (T_{\mathrm{sift}}, \mu, n)$ is uniform over $\mathbb{F}_d^k$. By the chain rule for mutual information, again, this implies

$$I(\boldsymbol{\sigma}; \mathsf{EX}'\mathsf{Y}_\mathrm{A}\mathsf{Y}_\mathrm{B}\pi\mathsf{TabC}'|\mathsf{k}, \mathsf{S}' = (T_{\mathrm{sift}}, \mu, n)) \leqslant d^{-nE_1(\gamma,\alpha)+o(m)}$$

[cf (33)], where $o(m)$ can be explicitly given as $3\log_d 2 + d + 6(d-1)\log_d m + \log_d[m(\gamma+1)]$. This simultaneously upper-bounds $\Pr\{\boldsymbol{\sigma} \neq \boldsymbol{\sigma}'|\mathsf{S}' = (T_{\mathrm{sift}}, \mu, n)\}$ since the argument in section A.3 also extends to the present case trivially. The bound is valid for m finite and is also meaningful in the limit of m large since α goes to r in (24) almost surely by the law of large numbers applied to the stochastic process $\{(\mathsf{a}_i, \mathsf{b}_i)\}_i$. In fact, for the almost sure event where $\alpha \in [r_0, r_1]$ for all large enough m, where $r_0 < r < r_1$, the bound is true with $E_1(\gamma, \alpha)$ replaced by

$$E_2(\gamma, r_0, r_1) = \min_{0 \leqslant \varepsilon \leqslant 2} [G\varepsilon^2/(2\ln d) + |\gamma - \theta(\varepsilon)|^+].$$

Here $G = \min_{r_0 \leqslant \alpha \leqslant r_1} (1-\alpha)^{-1}[g(\alpha)]^2$ can be made positive so that $E_2(\gamma, r_0, r_1)$ is positive by choosing r_0, r_1 and γ appropriately.

This protocol achieves the rate $(1 - p_\mathrm{a} - p_\mathrm{b})[1 - 2\max\{H(\overline{P_\mathcal{A}}), H(\overline{\overline{P_\mathcal{A}}})\}]$ for an individual attack $\mathcal{A}$, as can be checked by modifying the argument in section 6 more easily.

Appendix D. Nomenclature

Several symbols often used in this paper are listed below.

Strings, probability distributions and the Weyl unitary basis

- $0^n = (0, \ldots, 0) \in \mathbb{F}_d^n$, $1^n = (1, \ldots, 1) \in \mathbb{F}_d^n$
- $\mathcal{X} = \mathbb{F}_d^2 = \mathbb{F}_d \times \mathbb{F}_d$
- $[u, w] = ((u_1, w_1), \ldots, (u_n, w_n)) \in \mathcal{X}^n$ for $u = (u_1, \ldots, u_n)$, $w = (w_1, \ldots, w_n) \in \mathbb{F}_d^n$
- $N_{[u,w]} = X^u Z^w$, where $X^u = X^{u_1} \otimes \cdots \otimes X^{u_n}$ and $Z^w = Z^{w_1} \otimes \cdots \otimes Z^{w_n}$
- P_y: type of string y, defined by (10)
- $\mathcal{P}(\mathcal{Y})$: the set of all probability distribution on $\mathcal{Y}$
- $\mathcal{P}_n(\mathcal{Y})$: the set of all types of sequences in $\mathcal{Y}^n$ [$\mathcal{P}_n(\mathcal{Y}) \subseteq \mathcal{P}(\mathcal{Y})$]
- $[PQ](x, y) = P(x)Q(y)$
- $\overline{Q}(s) = \sum_{t\in\mathcal{Y}} Q(s,t)$, $\overline{\overline{Q}}(s) = \sum_{t\in\mathcal{Y}} Q(t,s)$
- s_T: subsequence $s_{j_1} \cdots s_{j_n}$ of $s_1 \cdots s_m$, where $T = \{j_1, \ldots, j_n\} \subseteq \{1, \ldots, m\}$ and $j_1 < \cdots < j_n$.

Standard notation in information theory

- Entropy: $H(P) = -\sum_{y\in\mathcal{Y}} P(y)\log_d P(y)$
- Kullback–Leibler information: $D(P\|Q) = \sum_{y\in\mathcal{Y}} P(y)\log_d \frac{P(y)}{Q(y)}$

- Mutual information: for random variables X and Y, $I(\mathsf{X};\mathsf{Y}) = D(P_{\mathsf{XY}} \| P_{\mathsf{X}} P_{\mathsf{Y}})$, where P_{W} denotes the probability distribution of W for an arbitrary discrete random variable W; $I(\mathsf{X};\mathsf{Y}|\mathsf{Z}=z) = D(P_{\mathsf{XY}|\mathsf{Z}=z} \| P_{\mathsf{X}|\mathsf{Z}=z} P_{\mathsf{Y}|\mathsf{Z}=z})$, where the probability that $\mathsf{W}=w$ conditional on the event $\mathsf{Z}=z$ is denoted by $P_{\mathsf{W}|\mathsf{Z}=z}(w)$, and $I(\mathsf{X};\mathsf{Y}|\mathsf{Z})$ stands for the expectation $\sum_z P_{\mathsf{Z}}(z) I(\mathsf{X};\mathsf{Y}|\mathsf{Z}=z)$.
- $h(x) = -x \log_2 x - (1-x)\log_2(1-x)$, $0 \leqslant x \leqslant 1$

CSS codes

- Γ: transversal (set of coset representatives in which each coset has exactly one representative) of $\mathbb{F}_d^n / C^\perp$
- $\mathsf{CSS}(C,\Gamma)$: $N_{J(\Gamma)}$-correcting CSS code made from a self-orthogonal C with basis $g_1, \ldots, g_\kappa$, where $J(\Gamma)$ is given in (8)
- Letters v, x, z as coset representatives (after [6]): $v + C \in C^\perp/C$, $x + C^\perp \in \mathbb{F}_d^n / C^\perp$, $z + C^\perp \in \mathbb{F}_d^n / C^\perp$

Parameters in the BB84 protocol

- m: total number of d-ary digits transmitted in the BB84 protocol
- n: code-length of CSS code
- $\kappa = \dim_{\mathbb{F}_d} C$
- $k = n - 2\kappa = \log_d \dim_{\mathbb{C}} \mathcal{Q}_{xz}$ ($\mathcal{Q}_{xz}$: quantum CSS codes)

References

[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing (Bangalore, India)* pp 175–9

[2] Wiesner S 1983 Conjugate coding *SIGACT News* **15** 78–88

[3] Mayers D 1996 Quantum key distribution and string oblivious transfer in noisy channels *Advances in Cryptography: Proc. Crypto'96* pp 343–57

[4] Mayers D 2001 Unconditional security in quantum cryptography *J. Assoc. Comput. Mach.* **48** 351–406

[5] Biham E, Boyer M, Boykin P O, Mor T and Roychowdhury V 2000 A proof of the security of quantum key distribution *Proc. 32nd Annual ACM Symp. on Theory of Computing* pp 715–24 (1999 *Preprint* quant-ph/9912053 LANL)

[6] Shor P and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol *Phys. Rev. Lett.* **85** 441–4

[7] Gottesman D and Preskill J 2001 Secure quantum key distribution using squeezed states *Phys. Rev.* A **63** 022309

[8] Gottesman D, Lo H-K, Lütkenhaus N and Preskill J 2002 Security of quantum key distribution with imperfect devices *Preprint* quant-ph/0212066, LANL

[9] Tamaki K, Koashi M and Imoto N 2003 Unconditionally secure key distribution based on two nonorthogonal states *Phys. Rev. Lett.* **90** 167904

[10] Calderbank A R and Shor P W 1996 Good quantum error correcting codes exist *Phys. Rev.* A **54** 1098–105

[11] Steane A M 1996 Multiple particle interference and quantum error correction *Proc. R. Soc.* A **452** 2551–77

[12] Holevo A S 2001 *Statistical Structure of Quantum Theory* (Berlin: Springer)

[13] Kraus K 1971 General state changes in quantum theory *Ann. Phys., NY* **64** 311–35

[14] Hellwig K-E 1995 General scheme of measurement processes *Int. J. Theor. Phys.* **34** 1467–79
Hellwig K-E 2000 General scheme of measurement processes *Quantum Computation and Quantum Information Theory* ed C Macchiavello *et al* (Singapore: World Scientific) (Reprint)

[15] Kraus K 1983 *States, Effects, and Operations (Lecture Notes in Physics* vol 190) (Berlin: Springer)

[16] Preskill J 1998 *Lecture Notes for Physics 229: Quantum Information and Computation* Available at http://www.theory.caltech.edu/people/preskill/ph229

[17] Csiszár I and Körner J 1981 *Information Theory: Coding Theorems for Discrete Memoryless Systems* (New York: Academic)

[18] Csiszár I and Körner J 1981 Graph decomposition: a new key to coding theorems *IEEE Trans. Inf. Theory* **27** 5–12

[19] Calderbank A R, Rains E M, Shor P W and Sloane N J A 1997 Quantum error correction and orthogonal geometry *Phys. Rev. Lett.* **78** 405–8

[20] Calderbank A R, Rains E M, Shor P W and Sloane N J A 1998 Quantum error correction via codes over GF(4) *IEEE Trans. Inf. Theory* **44** 1369–87
[21] Gottesman D 1996 Class of quantum error-correcting codes saturating the quantum Hamming bound *Phys. Rev.* A **54** 1862–8
[22] Dembo A and Zeitouni O 1998 *Large Deviations Techniques and Applications* 2nd edn (Berlin: Springer)
[23] Cover T M and Thomas J A 1991 *Elements of Information Theory* (New York: Wiley)
[24] Hamada M 2002 Exponential lower bound on the highest fidelity achievable by quantum error-correcting codes *Phys. Rev.* A **65** 052305 (2001 *Preprint* quant-ph/0109114 LANL)
[25] Hamada M 2002 Lower bounds on the quantum capacity and highest error exponent of general memoryless channels *IEEE Trans. Inf. Theory* **48** 2547–57 (2001 *Preprint* quant-ph/0112103 LANL)
[26] Hamada M 2002 Information rates achievable with algebraic codes on quantum discrete memoryless channels *Preprint* quant-ph/0207113 LANL
[27] Hamada M 2003 Notes on the fidelity of symplectic quantum error-correcting codes *Int. J. Quantum Inf.* vol 1 443–63 (*Preprint* quant-ph/0311003 LANL)
[28] Schumacher B 1996 Sending entanglement through noisy quantum channels *Phys. Rev.* A **54** 2614–28
[29] Gottesman D and Lo H-K 2003 Proof of security of quantum key distribution with two-way classical communications *IEEE Trans. Inf. Theory* **49** 457–75 (2001 *Preprint* quant-ph/0105121 LANL)
[30] Steane A M 1999 Efficient fault-tolerant quantum computing *Nature* **399** 124–6
[31] Gottesman D 1997 Stabilizer codes and quantum error correction *PhD Thesis*, California Institute of Technology (*Preprint* quant-ph/9705052 LANL)
[32] Weyl H 1928 *Gruppentheorie und Quantenmechanik* (Leipzig: Verlag von S Hirzel)
Weyl H 1950 *The Theory of Groups and Quantum Mechanics* Reprint 2nd edn (1931) (New York: Dover) (Engl. Transl.)
[33] Knill E and Laflamme R 1997 Theory of quantum error-correcting codes *Phys. Rev.* A **55** 900–11
[34] Artin E 1957 *Geometric Algebra* (New York: Interscience)
[35] Serre J-P 1977 *Cours d'Arithmétique* 2nd edn (Paris: Presses Universitaires des France)
[36] Aschbacher M 2000 *Finite Group Theory* 2nd edn (Cambridge: Cambridge University Press)
[37] Grove L C 2001 *Classical Groups and Geometric Algebra* (Providence, RI: American Mathematical Society)
[38] Ashikhmin A E, Barg A M, Knill E and Litsyn S N 2000 Quantum error detection II *IEEE Trans. Inf. Theory* **46** 789–800
[39] Barg A 2002 A low-rate bound on the reliability of a quantum discrete memoryless channel *IEEE Trans. Inf. Theory* **48** 3096–100
[40] Lo H-K and Chau H F 1999 Unconditional security of quantum key distribution over arbitrarily long distances *Science* **283** 2050–56
[41] Holevo A S 1973 Bounds for the quantity of information transmitted by a quantum communication channel *Probl. Inf. Trans.* **9** 177–83 (Translated from *Problemy Peredachi informatsii* pp 3–11)
[42] Choi M-D 1975 Completely positive linear maps on complex matrices *Linear Algebr. Appl.* **10** 285–90
[43] Werner R F 2001 All teleportation and dense coding schemes *J. Phys. A: Math. Gen.* **34** 7081–94
[44] Billingsley P 1995 *Probability and Measure* 3rd edn (New York: Wiley)
[45] Lo H-K 2001 Proof of unconditional security of six-state quantum key distribution scheme *Quantum Inform. Comput.* **1** 81–94
[46] Lo H-K, Chau H F and Ardehali M 2000 Efficient quantum key distribution scheme and proof of its unconditional security *Preprint* quant-ph/0011056 LANL
[47] Biham E and Mor T 1997 Secure of quantum cryptography against collective attacks *Phys. Rev. Lett.* **78** 2256–9
[48] Yuen H P 2003 KCQ: A new approach to quantum cryptography: I. General principles and qubit key *Preprint* qunat-ph/0311061 LANL
[49] Devetak I 2003 The private classical information capacity and quantum information capacity of a quantum channel *Preprint* qunat-ph/0304127 LANL
[50] Hamada M 2003 Teleportation and entanglement distillation in the presence of correlation among bipartite mixed states *Phys. Rev.* A **68** 012301–1–7 (*Preprint* quant-ph/0302054 LANL)
[51] Horodecki M, Horodecki P and Horodecki R 1999 General teleportation channel, singlet fraction, and quasidistillation *Phys. Rev.* A **60** 1888–98
[52] Hayashi M 2003 Private communication
[53] Hoeffding W 1963 Probability inequalities for sums of bounded random variables *Am. Stat. Assoc. J.* **58** 13–30
[54] Inamori H, Lütkenhaus N and Mayers D 2001 Unconditional security of practical quantum key distribution *Preprint* qunat-ph/0107017 LANL
[55] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)