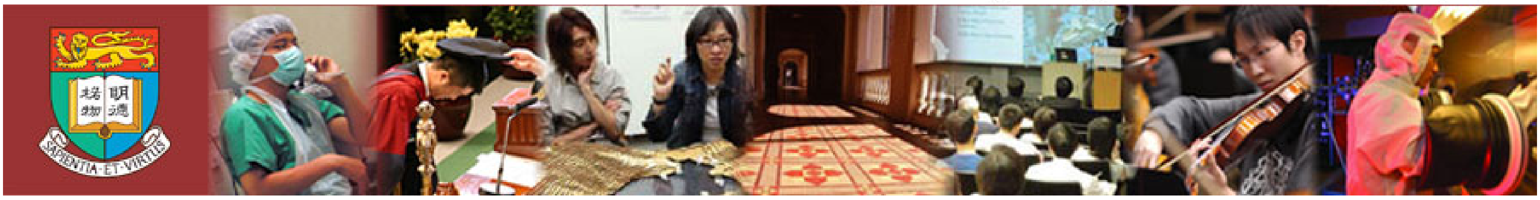

Unconditionally Secure Key Distribution in Higher Dimensions by Depolarization

Hoi Fung Chau, *Member, IEEE*

***Abstract*—This paper presents a prepare-and-measure scheme using N-dimensional quantum particles as information carriers where N is a prime power. One of the key ingredients used to resist eavesdropping in this scheme is to depolarize all Pauli errors introduced to the quantum information carriers. Using the Shor–Preskill-type argument, we prove that this scheme is unconditionally secure against all attacks allowed by the laws of quantum physics. For $N = 2^n > 2$, each information carrier can be replaced by n entangled qubits. In this case, there is a family of eavesdropping attacks on which no unentangled-qubit-based prepare-and-measure (PM) quantum key distribution scheme known to date can generate a provably secure key. In contrast, under the same family of attacks, our entangled-qubit-based scheme remains secure whenever $2^n \geq 4$. This demonstrates the advantage of using entangled particles as information carriers and of using depolarization of Pauli errors to combat eavesdropping attacks more drastic than those that can be handled by unentangled-qubit-based prepare-and-measure schemes.**

***Index Terms*—Depolarization, entanglement purification, local quantum operation, Pauli error, phase error correction, quantum key distribution, Shor–Preskill proof, two-way classical communication, unconditional security.**

I. Introduction

KEY distribution is the art of sharing a secret key between two cooperative players Alice and Bob in the presence of an eavesdropper Eve. If Alice and Bob distribute their key by exchanging classical messages only, Eve may at least in principle wiretap their conversations without being caught. So, given unlimited computational resources, Eve can crack the secret key. In contrast, in any attempt to distinguish between two nonorthogonal states, information gain is only possible at the expense of disturbing the state [1]. Therefore, if Alice and Bob distribute their secret key by sending nonorthogonal quantum signals, any eavesdropping attempt will almost surely affect their signal fidelity. Consequently, a carefully designed quantum key distribution (QKD) scheme allows Alice and Bob to accurately determine the quantum error rate, which in turn reflects the eavesdropping rate. If the estimated quantum error rate is too high, Alice and Bob abort the scheme and start all over again. Otherwise, they perform certain privacy amplification procedures to distill out the final key [2]–[6]. It is, therefore, conceivable that a provably secure QKD scheme exists even when Eve has unlimited computational power.

With this belief in mind, researchers proposed many QKD schemes [6]. These schemes differ in many ways such as the Hilbert space dimension of the quantum particles used, as well as the states and bases Alice and Bob prepared and measured. The first QKD scheme, commonly known as BB84, was invented by Bennett and Brassard [7]. In BB84, Alice randomly and independently prepares each qubit in one of the following four states: $|0\rangle$, $|1\rangle$, and $(|0\rangle \pm |1\rangle)/\sqrt{2}$, and sends them to Bob. After receiving the qubits, Bob randomly and independently measures each qubit in either $\{|0\rangle, |1\rangle\}$ or $\{(|0\rangle \pm |1\rangle)/\sqrt{2}\}$ bases. In short, BB84 is an experimentally feasible prepare-and-measure (PM) scheme involving the transfer of unentangled qubits [7]. Later, Bruß introduced another experimentally feasible PM scheme known as the six-state scheme [8]. In this scheme, Alice randomly and independently prepares each qubit in one of the following six states: $|0\rangle$, $|1\rangle$, $(|0\rangle \pm |1\rangle)/\sqrt{2}$, and $(|0\rangle \pm i|1\rangle)/\sqrt{2}$; and Bob measures each of them randomly and independently in one of the following three bases: $\{|0\rangle, |1\rangle\}$, $\{(|0\rangle \pm |1\rangle)/\sqrt{2}\}$, and $\{(|0\rangle \pm i|1\rangle)/\sqrt{2}\}$. Although the six-state scheme is more complex and generates a key less efficiently, Bruß found that it tolerates higher noise level than BB84 if Eve attacks each qubit individually [8]. In addition to qubit-based schemes such as BB84 and the six-state scheme, a number of PM QKD schemes involving higher dimensional or continuous systems have been proposed [9]–[17]. Most importantly, compared with qubit-based PM schemes, studies showed that many PM schemes involving higher dimensional systems can generate secure keys when a higher fraction of particles is eavesdropped individually [13]–[16], [18].

Instead of using PM schemes, Alice and Bob may explicitly use their shared entanglement to create a secret key. The first such entanglement-based (EB) QKD scheme was proposed by Ekert [19]. This scheme makes use of the fact that measuring a singlet state $(|01\rangle - |10\rangle)/\sqrt{2}$ along a common axis produces a pair of anticorrelated random bits. Consequently, a common key can be established provided that Alice and Bob share singlets through a quantum communication channel. To ensure that the fidelity of the shared singlets is high, Alice and Bob check if certain Bell's inequalities are maximally violated in a randomly selected subset of their shared particles [19]. Comparing with PM schemes, a typical EB scheme generates a key more efficiently but is harder to implement experimentally.

Are these QKD schemes really secure? Is it true that the six-state scheme tolerates higher error level than BB84? The answers to these questions turn out to be highly nontrivial. Recall that the all-powerful Eve may choose to attack the transmitted

Manuscript received December 10, 2002; revised October 31, 2004. This work was supported in part by the Research Grant Council (RGC) under Grant HKU 7010/04P of the Hong Kong Special Administrative Region (HKSAR) government.

The author is with the Department of Physics and Center of Theoretical and Computational Physics, University of Hong Kong, Hong Kong (e-mail: hfchau@hkusua.hku.hk).

Communicated by E. H. Knill, Associate Editor for Quantum Information Theory.

Digital Object Identifier 10.1109/TIT.2005.844076

0018-9448/$20.00 © 2005 IEEE

qubits collectively by applying a unitary operator to entangle these qubits with her quantum particles. In this situation, most of our familiar tools such as classical probability theory do not apply to the resultant highly entangled nonclassical state. These make rigorous cryptanalysis of BB84, the six-state, and Ekert schemes extremely difficult.

In spite of these difficulties, air-tight security proofs against all possible eavesdropping attacks of BB84, the six-state, and Ekert schemes have been discovered. Rigorous proofs of QKD schemes with better error tolerance have also been found. Mayers [4] and Biham *et al.* [20] eventually proved the security of BB84 against all kinds of attacks allowed by the known laws of quantum physics. In particular, Mayers showed that in BB84 a provably secure key can be generated whenever the bit-error rate (BER) is less than about 7% [4]. (A precise definition of BER can be found in Definition 3 in Section IV-A. Moreover, we emphasize that, unless otherwise stated, all provably secure error rates quoted in this paper are provable lower bounds. A QKD scheme may generate a secure key at a higher error rate although a rigorous proof has not been found.) Along a different line, Lo and Chau [3] proved the security of an EB QKD scheme, which is similar to the Ekert scheme, that applies up to 1/3 BER by means of a random hashing technique based on entanglement purification [21]. Their security proof is conceptually simple and appealing. Nevertheless, their scheme requires quantum computers and hence is not practical yet. By ingeniously combining the essence of the Mayers and Lo–Chau proofs, Shor and Preskill gave a security proof of BB84 that applies up to 11.0% BER [22]. This is a marked improvement over the 7% bit error tolerance rate in Mayers' proof. Since then, the Shor–Preskill proof became a blueprint for the cryptanalysis of many QKD schemes. For instance, Lo [23] as well as Gottesman and Lo [24] extended it to cover the six-state QKD scheme. At the same time, the work of Gottesman and Lo also demonstrates that careful use of local quantum operation plus two-way classical communication (LOCC2) increases the error tolerance rate of QKD. Furthermore, they found that the six-state scheme tolerates a higher BER than BB84 because the six-state scheme gives better estimates for the three Pauli error rates [24]. In search of an unentangled-qubit-based (UQB) QKD scheme that tolerates higher BER, Chau recently discovered an adaptive entanglement purification procedure inspired by the technique used by Gottesman and Lo in [24]. He further gave a Shor–Preskill-based proof showing that this adaptive entanglement purification procedure allows the six-state scheme to generate a provably secure key up to a BER of $(5-\sqrt{5})/10 \approx 27.6\%$ [25], making it the most error-tolerant PM scheme involving the transfer of unentangled qubits to date.

Unlike various UQB QKD schemes, very little cryptanalysis against the most general type of eavesdropping attack on a QKD scheme involving the transfer of higher dimensional quantum systems or entangled qubits has been performed. The only relevant work to date seems to be the earlier version of this work [17]. In that manuscript, an unconditionally secure QKD scheme that generalized the six-state scheme by using conjugation to cyclically permute $\mathrm{O}(N)$ kinds of quantum errors that can occur in the N-dimensional quantum information carriers was reported. Moreover, the set of preparation and measurement bases used is mutually unbiased [17]. Probably because Pauli errors are not depolarized when $N > 2$, the error tolerance capability of that scheme is not particularly high under the most general type of attack when $2 < N \lesssim 16$. More importantly, that scheme does not conclusively demonstrate the superiority of using entangled qubits to combat Eve [17]. In contrast, almost all cryptanalysis suggests that QKD schemes involving higher dimensional systems are more error tolerant under individual particle attack [13]–[15], [18]. It is, therefore, instructive to find an unconditionally secure PM QKD scheme based on entangled qubits that stands up to more drastic eavesdropping attacks than all known UQB PM schemes known to date.

In this paper, we analyze the security and error tolerance capability of a PM QKD scheme involving the transmission of higher dimensional quantum particles or entangled qubits. In fact, this scheme makes use of N-dimensional quantum information carriers prepared and measured randomly in $N(N+1)$ different bases. (In the cases of $N = 2, 3, 5, 7, 11$, the number of bases used can be reduced to $(N+1)$.) Such a preparation and measurement procedure depolarizes all Pauli errors in the transmitted signal. This greatly restricts the form of errors occurring in the quantum signals and makes error estimation effective; hence, its error tolerance rate is high. Nonetheless, the high error tolerance rate comes with a price, namely, that the efficiency of the scheme drops.

This paper is organized as follows. We first review the general assumptions on the capabilities of Alice, Bob, and Eve, as well as a precisely stated security requirement for a general QKD scheme in Section II. Then we introduce an EB QKD scheme involving the transmission of N-dimensional quantum systems, where N is a prime power in Section III and prove its security against the most general eavesdropping attack in Section IV. By standard Shor and Preskill reduction argument, we arrive at the provably secure PM scheme using unentangled N-dimensional quantum particles in Section V. Since one may use n possibly entangled qubits to represent an N-dimensional quantum state whenever $N = 2^n$, we obtain an unconditionally secure entangled-qubit-based (EQB) PM QKD scheme. (See Section V for a discussion of a subtle point in constructing this EQB PM QKD scheme. Moreover, we emphasize that the term EQB means that the qubits used to transfer information between Alice and Bob are entangled. In contrast, the term EB means that entanglement shared between Alice and Bob is explicitly used to generate the secret key. Thus, an EQB scheme may not be an EB scheme.) This EQB PM QKD scheme offers a definite advantage over all currently known UQB ones used to combat Eve. Specifically, whenever the most error-tolerant UQB PM QKD scheme known to date (namely, the one introduced by Chau in [25]) can generate a provably secure key under an eavesdropping attack, this EQB scheme can also generate an equally secure key for any $2^n \geq 2$ under the same attack. Furthermore, there is a family of eavesdropping attacks that creates a BER too high for Chau's scheme in [25] to generate a provably secure key. In contrast, the same family of attacks does not prevent this EQB PM scheme from producing a secure key whenever $2^n \geq 4$. This observation convincingly demonstrates that using entangled particles as information carriers can increase error tolerance in QKD. Finally, we give a brief summary in Section VI.

II. General Features and Security Requirements for Quantum Key Distribution

In QKD, we assume that Alice and Bob have access to two communication channels. The first one is an insecure noisy quantum channel. The other one is an unjammable noiseless authenticated classical channel in which everyone, including Eve, can listen to, but cannot alter, the content passing through it. We also assume that Alice and Bob have complete control over their own apparatus. Everything else for the unjammable classical channel may be manipulated by the all-powerful Eve. We further make the most pessimistic assumption that Eve is capable of performing any operation in her controlled territory that is allowed by the known laws of quantum physics [5], [6].

Given an unjammable classical channel and an insecure quantum channel, a QKD scheme consists of three stages [2]. The first is the signal preparation and transmission stage in which quantum signals are prepared and exchanged between Alice and Bob. The second is the signal quality test stage in which a subset of the exchanged quantum signals is measured in order to estimate the eavesdropping rate in the quantum channel. The final phase is the signal privacy amplification stage in which a carefully designed privacy amplification procedure is performed to distill out an almost perfectly secure key.

No QKD scheme can be 100% secure as Eve may be lucky enough to guess the preparation or measurement bases for each quantum state correctly. Hence, it is more reasonable to demand that the mutual information between Eve's measurement results after eavesdropping and the final secret key is less than an arbitrary but fixed small positive number. Hence we adopt the following definition of security.

Definition 1 (Based on Lo and Chau [3]) : With the above assumptions on the unlimited computational power of Eve, a QKD scheme is said to be **unconditionally secure** with security parameters (ϵ_p, ϵ_I) provided that whenever Eve has a cheating strategy that passes the signal quality control test with probability greater than ϵ_p, the mutual information between Eve's measurement results from eavesdropping and the final secret key is less than ϵ_I.

III. An Entanglement-Based QKD Scheme

In this section, we generalize the six-state scheme in a new way. In Section III-A, we first identify each element in $SL(2,N)$, the special linear group of 2×2 matrices over the finite field GF$\,(N)$, with a distinct unitary operator in $U(N)$. It turns out that all Pauli errors occurring in the transmitted particles can be depolarized by conjugating each transmitted particle by a randomly and independently picked unitary operator to be constructed. Then, in Section III-B, we devise an EB QKD scheme based on this set of unitary operators.

A. Construction of the Unitary Operator $T(M)$

We begin with the following definitions.

Definition 2 (Ashikhmin and Knill [26]) : Let $a \in$ GF$\,(N)$ where $N = p^n$ with p being a prime. We define the unitary operators X_a and Z_a acting on an N-dimensional Hilbert space by

$$X_a|b\rangle = |a+b\rangle \tag{1}$$

and

$$Z_a|b\rangle = \chi_a(b)|b\rangle \equiv \omega_p^{\mathrm{Tr}(ab)}|b\rangle \tag{2}$$

where χ_a is an additive character of the finite field GF$\,(N)$, ω_p is a primitive pth root of unity, and

$$\mathrm{Tr}(a) = a + a^p + a^{p^2} + \cdots + a^{p^{n-1}}$$

is the absolute trace of $a \in$ GF$\,(N)$. Note that the arithmetic inside the state ket and in the exponent of ω_p is performed in the finite field GF$\,(N)$.

It is easy to see from Definition 2 that the set of all Pauli errors acting on an N-dimensional particle $\{X_a Z_b : a,b \in \mathrm{GF}\,(N)\}$ spans the set of all possible linear operators acting on that particle over $\mathbb{C}$. (Unless otherwise stated, all linear operators discussed in this paper are endomorphisms.) Besides, X_a and Z_b follow the algebra

$$X_a X_b = X_b X_a = X_{a+b} \tag{3}$$

$$Z_a Z_b = Z_b Z_a = Z_{a+b} \tag{4}$$

and

$$Z_b X_a = \omega_p^{\mathrm{Tr}(ab)} X_a Z_b \tag{5}$$

for all $a,b \in$ GF$\,(N)$, where arithmetic in the subscripts is performed in GF$\,(N)$.

One way to permute quantum errors is to construct a unitary operator that maps $X_a Z_b$ to $X_{a\alpha+b\beta} Z_{a\delta+b\gamma}$ modulo a phase factor by conjugation. Specifically, let

$$M = \begin{bmatrix} \alpha & \beta \\ \delta & \gamma \end{bmatrix} \in SL(2,N)$$

where $N = p^n$ is a prime power. We look for a unitary operator $T(M)$ satisfying

$$T(M)^{-1} X_a Z_b T(M) = \omega_p^{f_M(a,b)} X_{a\alpha+b\beta} Z_{a\delta+b\gamma} \tag{6}$$

for all $a,b \in$ GF$\,(N)$, where the arithmetic in the subscripts is performed in GF$\,(N)$ and the factor $\omega_p^{f_M(a,b)} \in \mathbb{C}$ satisfies $|\omega_p^{f_M(a,b)}| = 1$. When the matrix $M \in SL(2,N)$ is clearly known to the readers, we shall simply denote $T(M)$ by T and f_M by f.

The choice of T is not unique if it exists. This is because $e^{i\theta} X_c Z_d T$ also permutes quantum errors modulo a phase factor for all $\theta \in \mathbb{R}$ and $c,d \in$ GF$\,(N)$. (However, the phase $f(a,b)$ depends on the values c and d.)

An invertible T satisfying (6) does not exist in general. To see this, we use (3)–(6) to manipulate the expression $X_{a+c} Z_{b+d} T$. On the one hand

$$X_{a+c} Z_{b+d} T = \omega_p^{f(a+c,b+d)} T X_{(a+c)\alpha+(b+d)\beta} Z_{(a+c)\delta+(b+d)\gamma}.$$

On the other hand,

$$\begin{aligned} X_{a+c} Z_{b+d} T &= \omega_p^{-\mathrm{Tr}(bc)} X_a Z_b X_c Z_d T \\ &= \omega_p^{f(c,d)-\mathrm{Tr}(bc)} X_a Z_b T X_{c\alpha+d\beta} Z_{c\delta+d\gamma} \\ &= \omega_p^{f(a,b)+f(c,d)}\ \omega_p^{\mathrm{Tr}([a\delta+b\gamma][c\alpha+d\beta]-bc)} \\ &\quad \cdot T X_{(a+c)\alpha+(b+d)\beta} Z_{(a+c)\delta+(b+d)\gamma}. \end{aligned}$$

Thus, the above two ways of expressing $X_{a+c}Z_{b+d}T$ agree for all $a, b, c, d \in$ GF(N) is a necessary condition for the existence of T^{-1}; otherwise, T is not injective as it maps a nonzero vector to the zero vector.

It is tedious but straightforward to check that the phase factor given in (7), together with the three phase conventions shown later in (8)–(10) satisfy the necessary condition for the existence of T^{-1} stated in the above paragraph. More importantly, we prove in Theorem 1 that the phase factor $f_M(a,b)$ defined in this way makes $T(M)$ invertible for all $M \in SL(2,N)$. We begin by writing down this particular phase factor $f_M(a,b)$ as follows:

$$f_M(a,b) = \frac{1}{2}\mathrm{Tr}([a^2\alpha\delta + b^2\beta\gamma]) + \mathrm{Tr}(ab\beta\delta) + \Delta_{p2}\mathrm{Tr}\left(\sum_{i>j} g_i g_j [a_i a_j \alpha\delta + b_i b_j \beta\gamma]\right) \quad (7)$$

for all $a, b \in$ GF(N). Note that in (7),

$$a = \sum_{i=1}^{n} a_i g_i \quad \text{and} \quad b = \sum_{i=1}^{n} b_i g_i$$

where $\{g_1, g_2, \ldots, g_n\}$ is a fixed basis of GF(N) over the field GF(p) and $a_i, b_i \in$ GF(p). Moreover, $\Delta_{p2} = 1$ if $p = 2$ and $\Delta_{p2} = 0$ if $p \neq 2$ in the above equation is the Kronecker delta.

The phase conventions are chosen as follows. When $p > 2$ and hence N is odd, 2 is invertible in GF(N). Consequently, the phase $\omega_p^{f_M(a,b)}$ may be chosen from pth roots of unity. Following this convention requires

$$f_M(a,b) \in \mathbb{Z}/p\mathbb{Z} \text{ for any } a, b \in \mathrm{GF}(N) \text{ if } 2 \nmid N. \quad (8)$$

In contrast, when $p = 2$ and hence N is even, 2 is not invertible in GF(N). Consequently, $f_M(a,b)$ may be integral or half-integral; and $\omega_p^{f_M(a,b)} \in \{\pm 1, \pm i\}$. In this case, we use the convention

$$\omega_2^{\mathrm{Tr}\left(g_j^2 a_j^2 \alpha\delta\right)/2} = \begin{cases} 1, & \text{if } \mathrm{Tr}\left(g_j^2 a_j^2 \alpha\delta\right) = 0 \\ i, & \text{if } \mathrm{Tr}\left(g_j^2 a_j^2 \alpha\delta\right) = 1 \end{cases} \quad (9)$$

and

$$\omega_2^{\mathrm{Tr}\left(g_j^2 b_j^2 \beta\gamma\right)/2} = \begin{cases} 1, & \text{if } \mathrm{Tr}\left(g_j^2 b_j^2 \beta\gamma\right) = 0 \\ i, & \text{if } \mathrm{Tr}\left(g_j^2 b_j^2 \beta\gamma\right) = 1 \end{cases} \quad (10)$$

for all $a_j, b_j \in$ GF(p), where $j = 1, 2, \ldots, n$.

We explain why the last term in (7) is required. Recall that the identity

$$\mathrm{Tr}\left(a_i^2 + a_j^2\right)/2 + \mathrm{Tr}(a_i a_j) = \mathrm{Tr}([a_i + a_j]^2)/2$$

holds only for $p > 2$. In contrast

$$\mathrm{Tr}\left(a_i^2 + a_j^2\right) = \mathrm{Tr}([a_i + a_j]^2)$$

for $p = 2$. So, we cannot use the first identity to absorb the last term in (7) into the first term when $p = 2$.

Lemma 1: Suppose $T(M)$ is a nonzero linear operator obeying (7)–(10) as well as the equation

$$X_a Z_b\, T(M) = \omega_p^{f_M(a,b)} T(M)\, X_{a\alpha+b\beta} Z_{a\delta+b\gamma}$$

for all $a, b \in$ GF(N). Then $T(M)$ is invertible. Besides, $T(M)$ is unitary after a proper scaling. Specifically, $T(M)$ is unitary if and only if its operator norm satisfies $\|T(M)\| = 1$.

Proof: Clearly, T also satisfies the equation

$$T^\dagger Z_{-b} X_{-a} = \omega_p^{-f(a,b)} Z_{-a\delta-b\gamma} X_{-a\alpha-b\beta} T^\dagger.$$

From (7)–(10), we know that

$$\begin{aligned} &X_a Z_b T T^\dagger \\ &\quad = \omega_p^{f(a,b)} T X_{a\alpha+b\beta} Z_{a\delta+b\gamma} T^\dagger \\ &\quad = \omega_p^{f(a,b)-\mathrm{Tr}([a\alpha+b\beta][a\delta+b\gamma])} T Z^\dagger_{-a\delta-b\gamma} X^\dagger_{-a\alpha-b\beta} T^\dagger \\ &\quad = \omega_p^{f(a,b)+f(-a,-b)-\mathrm{Tr}(a^2\alpha\delta+b^2\beta\gamma)-2\mathrm{Tr}(ab\beta\delta)} T T^\dagger X_a Z_b \\ &\quad = T T^\dagger X_a Z_b \end{aligned}$$

for all $a, b \in$ GF(N). By the same argument

$$X_a Z_b T^\dagger T = T^\dagger T X_a Z_b$$

for all $a, b \in$ GF(N). Thus, $TT^\dagger$ and $T^\dagger T$ are nonzero operators belonging to the centralizer of $\left\{\sum_{a,b} \Lambda_{ab} X_a Z_b : \Lambda_{ab} \in \mathbb{C}\right\}$. In other words, $TT^\dagger$ and $T^\dagger T$ are nonzero constant multiples of the identity operator. Hence, T is invertible. Obviously, the invertible operator T is unitary if and only if $\|T\| = 1$. □

Theorem 1: Let $\{g_1, g_2, \ldots, g_n\}$ be a fixed basis of GF(N) over GF(p). For any

$$M = \begin{bmatrix} \alpha & \beta \\ \delta & \gamma \end{bmatrix} \in SL(2,N)$$

the unitary operator $T(M)$ satisfying (6)–(10) exists. A possible choice of $T(M)$ is

$$T(M) = \frac{e^{i\theta}}{N^{\dim(\mathrm{colspan}(M-I))/2}} \sum_{[a\ b] \in \mathrm{colspan}(M-I)} \omega_p^{\mathrm{Tr}(\varphi_M(a,b))} \times \omega_p^{\frac{1}{2}\mathrm{Tr}(\varphi'_M(a,b))} X_a Z_b \quad (11)$$

for some $\theta \in \mathbb{R}$, with colspan$(M - I)$ being the span of the columns of $(M - I)$. In the above equation, the functions $\varphi_M, \varphi'_M :$ GF$(N) \times$ GF$(N) \longrightarrow$ GF(N) are given by

$$\begin{aligned} \varphi_M(a,b) = {} & b[\alpha\tilde{a}(a,b) + \beta\tilde{b}(a,b)] - a\tilde{b}(a,b) - \alpha\delta\tilde{a}(a,b)^2 \\ & - \alpha(\gamma-1)\tilde{a}(a,b)\tilde{b}(a,b) - \beta(\gamma-1)\tilde{b}(a,b)^2 \\ & + \Delta_{p2}\sum_{i>j} g_i g_j [\alpha\delta\tilde{a}_i(a,b)\tilde{a}_j(a,b) \\ & + \beta\gamma\tilde{b}_i(a,b)\tilde{b}_j(a,b)] \end{aligned} \quad (12)$$

and

$$\varphi'_M(a,b) = \alpha\delta\tilde{a}(a,b)^2 + \beta\gamma\tilde{b}(a,b)^2 \quad (13)$$

respectively. In (12) and (13), $\tilde{a}(a,b), \tilde{b}(a,b) \in$ GF(N) and $\tilde{a}_i(a,b), \tilde{b}_i(a,b) \in$ GF(p) are the solutions of the system of equations

$$\sum_{i=1}^{n} g_i \tilde{a}_i(a,b) = \tilde{a}(a,b) \quad (14)$$

$$\sum_{i=1}^{n} g_i \tilde{b}_i(a,b) = \tilde{b}(a,b) \quad (15)$$

and

$$\begin{bmatrix} \alpha-1 & \beta \\ \delta & \gamma-1 \end{bmatrix} \begin{bmatrix} \tilde{a}(a,b) \\ \tilde{b}(a,b) \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}. \quad (16)$$

TABLE I
THE OPERATOR T FOR A FEW M'S IN THE CASE OF $N = 2, 3,$ AND 4. NOTE THAT $\omega \in \text{GF}(4)$ IN THE LAST ROW OF THE TABLE SATISFIES $\omega^2 + \omega + 1 = 0$

N	M	$T(M)$
2	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	$\frac{1}{2}(I + iX_1 + iZ_1 + X_1 Z_1)$
3	$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$	$\frac{1}{3}\sum_{a,b=0}^{2} \omega_3^{\Delta_{b0}-\Delta_{a0}} X_a Z_b$
3	$\begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix}$	$\frac{1}{3}\sum_{a,b=0}^{2} \omega_3^{\Delta_{a0}-\Delta_{b0}} X_a Z_b$
4	$\begin{bmatrix} 0 & 1 \\ 1 & \omega \end{bmatrix}$	$\frac{1}{4}\sum_{a,b\in GF(4)} (-1)^{\text{Tr}(\omega[a+b])/2+\text{Tr}(\omega^2[a+b+\tilde{b}_1\tilde{b}_2])} X_a Z_b$

Proof: We show the existence of T by explicitly constructing it. We write

$$T = \sum_{i,j \in GF(N)} \Lambda_{ij} X_i Z_j$$

for some $\Lambda_{ij} \in \mathbb{C}$. Substituting this T into (6) and equating the coefficient of $X_a Z_b$, we obtain

$$\Lambda_{ab} = \omega_p^{f(i,j)+\text{Tr}([i\alpha+j\beta]\{b-i\delta-j[\gamma-1]\}-aj)} \times \Lambda_{a-i(\alpha-1)-j\beta,b-i\delta-j(\gamma-1)} \quad (17)$$

for all $a, b, i, j \in \text{GF}(N)$. Using (7)–(10), it is tedious but straightforward to check that (17) consists of N^2, $N(N-1)$, and (N^2-1) independent equations when $(M-I)$ is of rank $0, 1$, and 2, respectively.

In what follows, we only consider the case $\det(M-I) \neq 0$. The other cases can be proven in a similar manner. Since $(M-I)$ is invertible, $\dim(\text{colspan}(M-I)) = 2$. Besides, the solution of

$$\tilde{a}(a,b), \tilde{b}(a,b) \in \text{GF}(N) \quad \text{and} \quad \tilde{a}_i(a,b), \tilde{b}_i(a,b) \in \text{GF}(p)$$

in the system of (14)–(16) exists and is unique for any given $a, b \in \text{GF}(N)$. Hence, by choosing these $\tilde{a}(a,b), \tilde{b}(a,b)$, $\tilde{a}_i(a,b), \tilde{b}_i(a,b)$, we may use the (N^2-1) independent equations taken from (17) to relate every Λ_{ab} to Λ_{00} for all $(a,b) \neq (0,0)$. In this way, we conclude that every Λ_{ab} is proportional to Λ_{00}. Besides, all $|\Lambda_{ab}|$'s are equal. Consequently, from Lemma 1, the unitarity of $T(M)$ implies that $|\Lambda_{00}| = 1/N$. Substituting $\tilde{a}(a,b), \tilde{b}(a,b)$ into (6)–(10) and (17), we arrive at (11)–(13). □

For the purpose of illustration, the unitary operators $T(M)$'s for a few M's computed by (8)–(13) are listed in Table I. Incidentally, the unitary operator $T(M)$ listed in Table I for $N = 2$ is, up to a global phase, the same as the one used by Lo in his security proof of the six-state scheme in [23]. Furthermore, it is shown in Theorem 8 in the Appendix that the first three operators listed in Table I are of great importance in the construction of QKD schemes for $N = 2, 3$.

The unitary operator $T(M)$ stated in Theorem 1 depends on the matrix $M \in SL(2,N)$. So we may regard T as a map from $SL(2,N)$ to $U(N)$. Let

$$M_i = \begin{bmatrix} \alpha_i & \beta_i \\ \delta_i & \gamma_i \end{bmatrix} \in SL(2,N)$$

for $i = 1, 2$. Suppose further that N is odd. From (7), it follows that

$$f_{M_1 M_2}(a,b) = f_{M_1}(a\alpha_2 + b\beta_2, a\delta_2 + b\gamma_2) + f_{M_2}(a,b)$$

for all $a, b \in \text{GF}(N)$. In other words

$$T(M_1 M_2) = T(M_2) T(M_1).$$

Hence, the map $T : SL(2,N) \longrightarrow U(N)$ defines a faithful transposed representation of $SL(2,N)$ for all odd N. As $SL(2,N)$ is generated by two elements for any prime power N [27], Alice and Bob may apply any $T(M)$ if they can apply the two specific unitary operators corresponding to the generators of $SL(2,N)$. In contrast, when N is even, T is not a group representation of $SL(2,N)$. Fortunately, readers will find out in Section III that the security of all the QKD schemes reported in this paper do not depend on the phase $f_M(a,b)$. Therefore, in practice, Alice and Bob may replace $T(M_1 M_2 \cdots M_k)$ used in the QKD schemes reported in this paper by $T(M_k)T(M_{k-1}) \cdots T(M_1)$ in which M_i's are chosen from the two generators of $SL(2,N)$. (Note that the unitary operator defined in this way may depend on the decomposition of a matrix in $SL(2,N)$ into factors of M_i's. However, the unitary operator defined by any such decomposition will work equally well.)

B. An Entanglement-Based QKD Scheme

EB QKD Scheme A

1) Let the Hilbert space dimension N of each quantum particle involved in this scheme be a prime power. Alice prepares $L \gg 1$ quantum particle pairs in the state $\sum_{i\in\text{GF}(N)} |ii\rangle/\sqrt{N}$. She randomly and independently applies a unitary transformation $T(M) \in T[SL(2,N)]$ to the second particle in each pair. She keeps the first particle and sends the second in each pair to Bob. Bob acknowledges the receipt of these particles and then applies a randomly and independently picked $T(M')^{-1}$ to each received particle. Now, Alice and Bob publicly reveal their unitary transformations applied to each particle. A shared pair is then kept and is said to be in the set S_M if Alice and Bob have applied $T(M)$ and $T(M)^{-1}$ to the second particle of the shared pair, respectively. Thus, in the absence of noise and Eve, each pair of shared particles kept by Alice and Bob should be in the state $\sum_{i\in\text{GF}(N)} |ii\rangle/\sqrt{N}$.
2) Alice and Bob estimate the channel error rate by sacrificing a few particle pairs. Specifically, they randomly pick $\text{O}([N+1]^2 \log\{N[N^2-1]/\epsilon\}/\delta^2 N^2)$ pairs from each of the $N(N^2-1)$ sets S_M and measure each particle of the pair in the $\{|i\rangle : i \in \text{GF}(N)\}$ basis, namely, the standard basis. They publicly announce and compare their measurement results. In this way, they know the estimated channel error rate to within δ with probability at least $(1-\epsilon)$. (A detailed proof of this claim can be found in [2]. A brief outline of the proof will also be given in Section IV-B for handy reference.) If the channel error rate is too high, they abort the scheme and start all over again.
3) Alice and Bob perform the following privacy amplification procedure. (It will be shown in Section IV that step 3a below reduces errors of the form $X_a Z_b$ with $a \neq 0$ at the expense of increasing errors of the form Z_c with $c \neq 0$. In contrast, step 3b below reduces errors of the

form $X_a Z_b$ with $b \neq 0$ at the expense of increasing errors of the form X_c with $c \neq 0$. Applying steps 3a and 3b in turn is an effective way to reduce all kinds of quantum errors provided that the error rate is not too high.)

a) Alice and Bob apply the entanglement purification procedure by two-way classical communication (LOCC2 EP) similar to the one reported in [21], [28]. Specifically, Alice and Bob randomly group their remaining quantum particles in tetrads where each tetrad consists of two pairs shared by Alice and Bob in step 1. Alice randomly picks one of the two particles in her share of each tetrad as the control register and the other as the target. She applies the following unitary operation to the control and target registers:

$$|i\rangle_{\text{control}} \otimes |j\rangle_{\text{target}} \longmapsto |i\rangle_{\text{control}} \otimes |j-i\rangle_{\text{target}} \quad (18)$$

where the subtraction is performed in the finite field GF(N). Bob applies the same unitary transformation to his corresponding share of particles in the tetrad. Then, they publicly announce the measurement results of their target registers in the standard basis. They keep their control registers only when the measurement results of their corresponding target registers agree. They repeat the above LOCC2 EP procedure until there is an integer $r > 0$ such that a single application of step 3b will bring the signal quantum error rate of the resultant particles down to less than ϵ_I/ℓ^2 for an arbitrary but fixed security parameter $\epsilon_I > 0$, where $r\ell$ is the number of remaining pairs they share currently. They abort the scheme either when r is greater than the number of remaining quantum pairs they possess or when they have used up all their quantum particles in this procedure.

b) They apply the majority vote phase error correction (PEC) procedure introduced by Gottesman and Lo [24]. Specifically, Alice and Bob randomly divide the resultant particles into sets each containing r pairs of particles shared by Alice and Bob. Alice and Bob jointly apply the $[r,1,r]_N$ phase error correction procedure to their corresponding shares of r particles in each set and retain their phase error corrected quantum particles. At this point, Alice and Bob should share ℓ almost perfect pairs $\sum_{i\in \text{GF}(N)} |ii\rangle/\sqrt{N}$ with fidelity at least $(1-\epsilon_I/\ell)$. By measuring their shared pairs in the standard basis, Alice and Bob obtain their common key. More importantly, Eve's information on this common key is less than the security parameter ϵ_I. (Proof of this claim can be found in Theorem 3 in Section IV-C below.)

One may simplify Scheme A by picking $T(M)$'s from $T[H]$, where H is a proper subgroup of $SL(2,N)$ whose number of elements divides (N^2-1). Theorem 8 in the Appendix tells us that the subgroup H exists if and only if $N = 2,3,5,7,11$ and $|H| = N^2-1$. From now on, we use the symbol G to denote either the entire group $SL(2,N)$ or the order (N^2-1) subgroup H of $SL(2,N)$.

In the case $N = 2$ and G equals the cyclic group of three elements, Scheme A is a variation of the six-state scheme introduced by Chau in [25]. The key difference is that, unlike the former one, the present scheme does not make use of the Calderbank–Shor–Steane quantum code after PEC.

Lemma 3 in Section IV-C shows that all Pauli errors in the quantum signal right after step 1 in Scheme A are depolarized. Furthermore, Theorem 8 in the Appendix shows that the same conclusion applies when Alice and Bob pick M from a subgroup H of $SL(2,N)$ of order (N^2-1).

IV. Cryptanalysis of the Entanglement-Based QKD Scheme

In this section, we present a detailed unconditional security proof of Scheme A in the limit of a large number of quantum particles L transmitted. We also investigate the maximum error tolerance rate of Scheme A against the most general type of eavesdropping attack allowed by the laws of quantum physics. With suitable modifications, the security proof reported here can be extended to the case of a small finite L. Nevertheless, working in the limit of large L makes the asymptotic error tolerance rate analysis easier.

The remainder of this section is organized as follows. In Section IV-A, we define various error rate measures and discuss how to fairly compare error tolerance capabilities between different QKD schemes. Then, in Section IV-B, we briefly explain why a reliable upper bound of the channel error can be obtained by randomly testing only a small subset of quantum particles in step 2 of Scheme A. Finally, in Section IV-C, we prove the security of the privacy amplification procedure in step 3 of Scheme A and analyze its error tolerance rate. This will complete the proof of unconditional security for EB Scheme A.

A. Fair Comparison of Error Tolerance Capability and Various Measures of Error Rates

Definition 3: Recall that Alice prepares L particle pairs each in the state $\sum_{i\in \text{GF}(N)} |ii\rangle/\sqrt{N}$ and randomly applies $T(M) \in T[G]$ to the second particle in each pair. We denote the resultant (pure) state of the pairs by $\bigotimes_{j=1}^{L} |\phi_j\rangle$. Then, she sends one particle in each pair through an insecure quantum channel to Bob; and upon receipt, Bob randomly applies $T(M')^{-1}$ to his share of the pair. The **channel quantum error rate** in this situation is defined as the marginal error rate of the measurement results if Alice and Bob were to make a hypothetical measurement on the jth shared quantum particle pair in the basis $\{I \otimes X_a Z_b |\phi_j\rangle : a,b \in \text{GF}(N)\}$ for all j. In other words, the channel quantum error rate equals $1/L$ times the expectation value of the cardinality of the set

$$\{j : \text{hypothetical measurement of the } j\text{th pair equals } I \otimes X_a Z_b |\phi_j\rangle \text{ with } (a,b) \neq (0,0)\}.$$

The **channel standard basis measurement error rate** is defined as $1/L$ times the expectation value of the cardinality of the set

$$\{j : \text{hypothetical measurement of the } j\text{th pair equals } I \otimes X_a Z_b |\phi_j\rangle \text{ with } a \neq 0\}.$$

The next two definitions concern only those quantum particle pairs retained by Alice and Bob in $\bigcup_{M\in G} S_M$. (That is, those that Alice and Bob have applied $T(M)$ and $T(M)^{-1}$ to the second particle of the shared pair for some $M \in G$, respectively.) In the absence of noise and Eve, all such particle pairs should be in the state $\sum_{i\in \mathrm{GF}(N)} |ii\rangle/\sqrt{N}$. The **signal quantum error rate** (or quantum error rate (QER) for short) in this situation is defined as the expectation value of the proportion of particle pairs in $\bigcup_M S_M$ whose measurement result in the basis

$$\left\{ \sum_{i\in \mathrm{GF}(N)} |i\rangle \otimes X_a Z_b |i\rangle/\sqrt{N} : a, b \in \mathrm{GF}(N) \right\}$$

equals $\sum_{i\in \mathrm{GF}(N)} |i\rangle \otimes X_a Z_b |i\rangle/\sqrt{N}$ for some $(a,b) \neq (0,0)$. The **signal standard basis measurement error rate** (or standard basis measurement error rate (SBMER) for short) is defined as the expectation value of the proportion of particle pairs in $\bigcup_M S_M$ whose measurement result in the basis

$$\left\{ \sum_{i\in \mathrm{GF}(N)} |i\rangle \otimes X_a Z_b |i\rangle/\sqrt{N} : a, b \in \mathrm{GF}(N) \right\}$$

equals

$$\sum_{i\in \mathrm{GF}(N)} |i\rangle \otimes X_a Z_b |i\rangle/\sqrt{N}$$

for some $a \neq 0$. In other words, SBMER measures the apparent error rate of the signal when Alice and Bob measure their respective shares of particles in the standard basis. In the special case of $N = 2^n$, any standard basis measurement result can be bijectively mapped to an n-bit string. Thus, it makes sense to define the **signal bit-error rate** (or BER for short) as the marginal error rate of the n-bit string resulting from a standard basis measurement of the signal at the end of the signal preparation and transmission stage.

Three important remarks are in place. First, SBMERs and BERs of QKD schemes using quantum particles of different dimensions as information carriers should *never* be compared directly. This is because the quantum communication channels used are different. In addition, the same eavesdropping strategy may lead to different error rates [13]–[16], [18]. It appears that the only sensible situation in which it is meaningful to compare the error tolerance capabilities of two QKD schemes is when the schemes are using the same quantum communication channel and are subjected to the same eavesdropping attack. Specifically, let Alice reversibly map every p^n-dimensional quantum state used in Scheme A into n possibly entangled p-dimensional quantum particles and send them through an insecure p-dimensional quantum particle communication channel to Bob. Moreover, since we assume that Alice and Bob do not have quantum storage capability, it is reasonable to require that Alice prepares and sends packets of n possibly entangled p-dimensional quantum particles one after another. In this way, Scheme A becomes an entangled-particle-based QKD scheme. More importantly, Eve may apply the same eavesdropping attack on the insecure p-dimensional quantum particle channel used by Alice and Bob irrespective of the value n. Thus, it is fair to compare the error tolerance capability between two entangled-particle-based QKD schemes derived from Scheme A using p^n- and $p^{n'}$-dimensional particles, respectively, against any eavesdropping attack on the p-dimensional quantum particle channel.

Second, the BER defined above for $N = 2^n$ with $n > 1$ depends on the bijection used. Fortunately, in Section IV-C, readers will find that the BER for the QKD scheme reported in this paper is independent of this bijection.

Third, Lemma 3 in Section IV-C and Theorem 8 in the Appendix show that Pauli errors that occurred in a collection of N-dimensional quantum registers are depolarized if we conjugate each register by a randomly and independently picked $T(M) \in T[G]$. Furthermore, the channel QER is equal to the QER of the signal. Roughly speaking, QER refers to the rate of any quantum error (phase shift and/or spin flip) occurring in the pair $\sum_{i\in \mathrm{GF}(N)} |ii\rangle/\sqrt{N}$ shared by Alice and Bob. In contrast, the depolarization of Pauli errors implies that the channel standard basis measurement error rate does not equal the SBMER in general.

B. Reliability of the Error Rate Estimation

In Scheme A, Alice and Bob keep only those particle pairs that are believed to be in the state $\sum_{i\in \mathrm{GF}(N)} |ii\rangle/\sqrt{N}$ at the end of step 1. Then, they measure some of them in the standard basis in the signal quality control test in step 2. More importantly, since all the LOCC2 EP and PEC privacy amplification procedures in step 3 map standard basis to standard basis, we can imagine that the final standard basis measurements of their shared secret key were performed right at the beginning of step 3. In this way, any quantum eavesdropping strategy used by Eve is reduced to a classical probabilistic cheating strategy. In other words, for any quantum eavesdropping strategy, one can always find an equivalent Pauli attack that has the same probability of passing the signal quality control test in step 2 and gives the same density matrix of the shared quantum particles just before the final standard basis measurement in step 3. Therefore, we need only to consider Pauli attack in the subsequent analysis [3].

Recall that in step 2, Alice and Bob do not care about the measurement result of an individual quantum register; they only care about the difference between the measurement outcome of Alice and the corresponding outcome of Bob. In other words, they apply the projection operator

$$P_a = \sum_{i\in \mathrm{GF}(N)} |i, i+a\rangle \langle i, i+a| \tag{19}$$

to each of the randomly selected quantum registers in the set $\bigcup_{M\in G} S_M$. The projection operator P_a can be rewritten in a form involving Bell-like states as follows. Define $|\Phi_{ab}\rangle$ to be the Bell-like state

$$\sum_{i\in \mathrm{GF}(N)} |i\rangle \otimes X_a Z_b |i\rangle/\sqrt{N} \equiv \sum_{i\in \mathrm{GF}(N)} \omega_p^{\mathrm{Tr}(ib)} |i, i+a\rangle/\sqrt{N}.$$

Then, P_a can be rewritten as

$$P_a = \sum_{b\in \mathrm{GF}(N)} |\Phi_{ab}\rangle \langle \Phi_{ab}|. \tag{20}$$

Since every particle pair in S_M is subjected to $T(M)$ and $T(M)^{-1}$ before and after passing through the insecure channel, respectively, P_a is a measure of whether an error of the form $T(M) X_a Z_b T(M)^{-1}$ for some $b \in \mathrm{GF}(N)$ has occurred in this pair. Recall that $M \in G$ is randomly and independently chosen for each pair. Moreover, such a choice is known to Eve after the second half of the particle pair has reached Bob. So, combined with (6) as well as (19) and (20), the signal quality control test in step 2 of Scheme A can be regarded as an effective random sampling test for the fidelity of the pairs as

$$|\Phi_{00}\rangle \equiv \sum_{i\in \mathrm{GF}(N)} |ii\rangle/\sqrt{N}.$$

At this point, classical sampling theory can be used to estimate the quantum channel error and hence the eavesdropping rate of the classical probabilistic cheating strategy used by Eve, as well as the fidelity of the remaining pairs as $|\Phi_{00}\rangle$.

Lemma 2 (Adapted From Lo, Chau, and Ardehali [2]): Suppose that immediately after step 1 in Scheme A, Alice and Bob share L_M pairs of particles in the set S_M, namely, those particles that were conjugated by $T(M)$. Suppose further that Alice and Bob randomly pick $\mathrm{O}(\log[1/\epsilon]/\delta^2) \lesssim 0.01L_M$ of the L_M pairs for testing in step 2. Define the estimated channel standard basis measurement error rate $\hat{e}_M$ to be the portion of tested pairs whose measurement results obtained by Alice and Bob differ. Denote the channel standard basis measurement error rate for the set S_M by e_M. Then, the probability that $|e_M - \hat{e}_M| > \delta$ is of the order of ϵ for any fixed $\delta > 0$.

Proof: Using earlier discussions in this subsection, the problem depicted in this lemma is equivalent to a classical random sampling problem without replacement whose solution follows directly from [2, Lemma 1]. □

Lemma 2 assures that by randomly choosing $\mathrm{O}(\log[1/\epsilon]/\delta^2)$ out of L_M pairs to test, the unbiased estimator $\hat{e}_M$ cannot differ significantly from the actual channel standard basis measurement error rate e_M. More importantly, the number of particle pairs they need to test is independent of L_M. Therefore, in the limit of large L_M (and hence large L), randomly testing a negligibly small portion of quantum particle pairs is sufficient for Alice and Bob to estimate the channel standard basis measurement error rate in the set S_M with high confidence [2]. In addition, the QER of the remaining untested particle pairs is the same as that of $\bigcup_{M\in G} S_M$ in the large L limit.

Theorem 2: Let G denote the group $SL(2,N)$ or its order (N^2-1) subgroup H reported in Theorem 8. Using the notation in Lemma 2, $(N+1)\langle\hat{e}_M\rangle/N$ is a reliable estimator of the upper bound of the QER, where $\langle\cdot\rangle$ denotes the mean averaged over all $M\in G$. Specifically, the probability that the QER exceeds $(N+1)(\langle\hat{e}_M\rangle+\delta)/N$ is less than $\epsilon|G|$.

Proof: Recall that Eve does not know the choice of unitary operators applied by Alice and Bob in step 1 in Scheme A. Consequently, by Lemma 3 in Section IV-C or Theorem 8 in the Appendix , step 1 in Scheme A depolarizes Pauli errors of the quantum particles. That is, in the limit of a large L, the X_aZ_b error rate in the set S_I is equal to that of $T(M)^{-1}X_aZ_bT(M)$ in the set S_M for all $M\in G$. Among the

$$T(M)^{-1}X_aZ_bT(M) \equiv \omega_p^{f_M(a,b)}X_cZ_d$$

errors occurring in the set S_M, only those with $c\neq 0$ can be recorded in step 2. Thus, the estimator for the QER equals

$$(N^2-1)\langle\hat{e}_M\rangle/N(N-1) = (N+1)\langle\hat{e}_M\rangle/N.$$

This theorem now follows directly from Lemma 2. □

To summarize, once the signal quality control test in step 2 of Scheme A is passed, Alice and Bob have high confidence (of at least $(1-\epsilon)$) that the QER of the remaining untested particle pairs is small enough for the signal privacy amplification stage in step 3 to handle. Moreover, the estimation given in Theorem 2 is independent of the phase $f_M(a,b)$ used by the unitary operator $T(M)$.

Before closing this subsection, we would like to point out that one can estimate the QER in a more aggressive way. Specifically, Alice and Bob do not only know whether the measurement results of each tested pair are equal, in fact they also know the difference between their measurement results in each tested pair. They may exploit this extra piece of information to better estimate the probability of X_aZ_b error in the signal for each $a,b\in \mathrm{GF}(N)$. Such estimation helps them to devise tailor-made privacy amplification schemes that tackle the specific kind of error caused by channel noise and Eve. While this methodology will be useful in practical QKD, we shall not pursue this further here as the aim of this paper is the worst case cryptanalysis in the limit of a large number of quantum particle transfers L.

C. Security of Privacy Amplification

Definition 4: We denote the X_aZ_b error rate of the quantum particles shared by Alice and Bob just before step 3 in Scheme A by $e_{a,b}$. When there is no possible confusion in the subscript, we shall write e_{ab} instead of $e_{a,b}$. Similarly, we denote the X_aZ_b error rate of the resultant quantum particles shared by them after k rounds of LOCC2 EP by $e_{a,b}^{k\mathrm{EP}}$ or $e_{ab}^{k\mathrm{EP}}$. Suppose further that Alice and Bob perform PEC using the $[r,1,r]_N$ majority vote code after k rounds of LOCC2 EP. We denote the resultant X_aZ_b error rate by $e_{a,b}^{\mathrm{PEC}}$ or e_{ab}^{PEC}.

Lemma 3: Let $G=SL(2,N)$. The signal quantum error suffered by quantum particle pairs in $\bigcup_{E\in SL(2,N)}$ can be regarded as depolarized. In other words, the QER satisfies

$$\sum_{i,j\in \mathrm{GF}(N)} e_{ij} = 1 \tag{21}$$

and

$$e_{ab} = e_{a'b'}, \quad \text{for all } (a,b),(a',b')\neq(0,0). \tag{22}$$

Proof: Recall that Alice and Bob randomly and independently apply $T(M)$ and $T(M')^{-1}$ to each transmitted quantum register. More importantly, their choices are unknown to Eve when the quantum particle is traveling in the insecure channel. Let $\mathcal{E}$ be the quantum operation that Eve applies to the quantum particles in the set $\bigcup_{M\in SL(2,N)} S_M$. (In other words, $\mathcal{E}$ is a completely positive convex-linear map acting on the set of density matrices describing the quantum particle pairs to which Alice and Bob have applied $T(M)$ and $T(M)^{-1}$, respectively, for some $M\in SL(2,N)$. Moreover, $0\leq \mathrm{Tr}(\mathcal{E}(\rho))\leq 1$ for any density matrix ρ.) After Alice and Bob have publicly announced their choices of quantum operations, every quantum particle pair in $\bigcup_M S_M$ has an equal chance of having experienced $\left[\otimes_j T(M_j)^{-1}\right]\mathcal{E}[\otimes_j T(M_j)]$ where $M_j\in SL(2,N)$. Note that the index j in the tensor product in the above expression runs over all particle pairs in $\bigcup_M S_M$. From the discussions in Section IV-B, we know that Eve's attack may be reduced to a classical probabilistic one. In other words, we may regard $\mathcal{E}$ as a Pauli error operator. Since $SL(2,N)$ is a group and the set

$$\{M \in SL(2,N) : M[a\ b]^t = [c\ d]^t\}$$

contains N elements for all $[a\ b], [c\ d] \neq [0\ 0]$, we conclude from (6) that the Pauli quantum error of the quantum particles in the set $\bigcup_{M\in SL(2,N)} S_M$ is depolarized. Hence, (21) and (22) apply. □

After establishing the initial conditions for the QER, we investigate the effect of LOCC2 EP on the QER.

Lemma 4: In the limit of a large number of transmitted quantum registers, $e_{ab}^{k\mathrm{EP}}$ is given by

$$e_{ab}^{k\mathrm{EP}} = \frac{\sum\limits_{c_0,\ldots,c_{2^k-2}} e_{ac_0} e_{ac_1} \cdots e_{ac_{2^k-2}} e_{a,b-c_0-c_1-\cdots-c_{2^k-2}}}{\sum\limits_{i\in\mathrm{GF}(N)} \left(\sum\limits_{j\in\mathrm{GF}(N)} e_{ij} \right)^{2^k}}. \tag{23}$$

In particular, if e_{ab}'s are given by (21) and (22), then

$$e_{00}^{k\mathrm{EP}} = \frac{[e_{00} + (N-1)e_{01}]^{2^k} + (N-1)\,(e_{00} - e_{01})^{2^k}}{N\left\{[e_{00} + (N-1)e_{01}]^{2^k} + (N-1)N^{2^k} e_{01}^{2^k}\right\}} \tag{24}$$

$$e_{0b}^{k\mathrm{EP}} = \frac{[e_{00} + (N-1)e_{01}]^{2^k} - (e_{00} - e_{01})^{2^k}}{N\left\{[e_{00} + (N-1)e_{01}]^{2^k} + (N-1)N^{2^k} e_{01}^{2^k}\right\}} \tag{25}$$

for all $b \neq 0$ and

$$e_{ab}^{k\mathrm{EP}} = \frac{N^{2^k} e_{01}^{2^k}}{N\left\{[e_{00} + (N-1)e_{01}]^{2^k} + (N-1)N^{2^k} e_{01}^{2^k}\right\}} \tag{26}$$

for all $a, b \in \mathrm{GF}\,(N)$ with $a \neq 0$.

Proof: Suppose that Bob's control and target registers experience $X_a Z_b$ and $X_{a'} Z_{b'}$ errors, respectively. (In contrast, those retained by Alice are error free as they never passed through the insecure noisy channel.) After applying the unitary operation in (18), the errors in the control and target registers become $X_a Z_{b+b'}$ and $X_{a'-a} Z_{b'}$, respectively.

Recall that the privacy amplification procedure in step 3 is performed irrespective of which set S_M the particle belongs to. So, in the limit of a large number of transmitted quantum registers, the covariance between probabilities of picking any two distinct quantum registers tends to zero. Likewise, the covariance between probabilities of picking any two distinct pairs of quantum registers also tends to zero. Hence, in this limit, the expectation value of the $X_a Z_b$ error rate just after applying the unitary operation in (18) can be computed by assuming that the error in every pair of control and target registers is independent. Moreover, the variance of the $X_a Z_b$ error rate tends to zero in this limit.

To show that (23) is valid, let us recall that Alice and Bob keep their control registers only when the measurement results of their corresponding target registers agree. In other words, they keep a control register only when $a = a'$. Thus, once the control register in Bob's laboratory is kept, it will suffer an error $X_d Z_c$ where $d = a$ and $c = b + b'$. Therefore, in the limit of a large number of transmitted quantum registers, the number of quantum registers remaining after $(k+1)$ rounds of LOCC2 EP is proportional to

$$\sum_{i\in\mathrm{GF}(N)} \left(\sum_{j\in\mathrm{GF}(N)} e_{ij}^{k\mathrm{EP}} \right)^2.$$

Similarly, the number of quantum registers suffering from $X_a Z_b$ errors after $(k+1)$ rounds of LOCC2 EP is proportional to

$$\sum_{c\in\mathrm{GF}(N)} e_{ac}^{k\mathrm{EP}} e_{a,b-c}^{k\mathrm{EP}}.$$

Furthermore, the two proportionality constants are the same. Therefore,

$$e_{ab}^{(k+1)\mathrm{EP}} = \frac{\sum_{c\in\mathrm{GF}(N)} e_{ac}^{k\mathrm{EP}} e_{a,b-c}^{k\mathrm{EP}}}{\sum_{i\in\mathrm{GF}(N)} \left(\sum_{j\in\mathrm{GF}(N)} e_{ij}^{k\mathrm{EP}} \right)^2} \tag{27}$$

for all $k \in \mathbb{N}$. Equation (23) can then be proven by mathematical induction on k. (It is easier to use mathematical induction to prove the validity of the numerator in (23) and then use (21) to determine the denominator.)

In particular, if the initial error rates e_{ab}'s are given by (21) and (22), then (24)–(26) can be proven by mathematical induction on k with the help of (27). □

Lemma 4 generalizes a similar result for qubits [24], [25]. In fact, the effect of LOCC2 EP is to reduce errors of the form $X_a Z_b$ with $a \neq 0$ at the expense of possibly increasing errors of the form Z_c with $c \neq 0$. We further remark that in the case where L is finite, $e_{ab}^{k\mathrm{EP}}$ is determined by solving the classical problem of randomly pairing N^2 kinds of balls in an urn containing $2r\ell$ balls. Therefore, $e_{ab}^{k\mathrm{EP}}$ is related to the so-called multivariate hypergeometric distribution whose theory is reviewed extensively in [29].

Lemma 5: In the limit of a large number of quantum particles transmitted from Alice to Bob, the $X_a Z_b$ error rate after PEC e_{ab}^{PEC} using $[r,1,r]_N$ majority vote code satisfies

$$\sum_{a\neq 0} \sum_{b\in\mathrm{GF}(N)} e_{ab}^{\mathrm{PEC}} \leq r \sum_{a\neq 0} \sum_{b\in\mathrm{GF}(N)} e_{ab}^{k\mathrm{EP}}. \tag{28}$$

Moreover, if e_{ab}'s satisfy (21), (22), and $e_{00} > e_{01}$, then

$$\sum_{a\in\mathrm{GF}(N)} \sum_{b\neq 0} e_{ab}^{\mathrm{PEC}} \leq (N-1) \left\{ 1 - \frac{N\,(e_{00} - e_{01})^{2^{k+1}}}{4\,[e_{00} + (N-1)e_{01}]^{2^{k+1}}} \right\}^r \tag{29}$$

as $k \to \infty$. This inequality also holds if r depends on k.

Proof: Recall that the parity-check matrix of the $[r,1,r]_N$ majority vote code is

$$\begin{bmatrix} 1 & -1 & & & \\ 1 & & -1 & & \\ \vdots & & & \ddots & \\ 1 & & & & -1 \end{bmatrix}. \tag{30}$$

Therefore, after measuring the (phase) error syndrome, the Z_b error stays with the control register whereas the X_a error propagates from the control as well as all target registers to the resultant control quantum register [30]. Specifically, let the error in the ith quantum register be $X_{a_i}Z_{b_i}$ for $i = 1, 2, \ldots, r$. Then, after measuring the error syndrome, the resultant error in the remaining control register equals $X_{a_1+\cdots+a_r}Z_{b_1}$. Consequently, after PEC, the error in the remaining register is $X_{a_1+\cdots+a_r}Z_b$ where b is the majority of b_i $(i = 1, 2, \ldots, r)$. In other words, after PEC, spin flip error rates are increased by at most r times. Hence, (28) holds.

By the same argument used in Lemma 4, in the limit of a large number of transferred quantum registers, the rate of any kind of phase error after PEC, $\sum_{a\in\mathrm{GF}(N)}\sum_{b\neq 0} e_{ab}^{\mathrm{PEC}}$, satisfies

$$\sum_{a\in\mathrm{GF}(N)}\sum_{b\neq 0} e_{ab}^{\mathrm{PEC}} \leq (N-1)\max\{\Pr(\text{the number of registers suffering from error of the form } X_iZ_1 \text{ is greater than or equal to those suffering from error of the form } X_i \text{ when drawn from a random sample of } r \text{ registers, given a fixed } e_{00})\} \tag{31}$$

where the maximum is taken over all possible probabilities with different e_{ab}'s satisfying the constraints in (21) and (22). We denote the sum $\sum_{a\in\mathrm{GF}(N)} e_{ab}^{k\mathrm{EP}}$ by $e_{Z_b}^{k\mathrm{EP}}$. Then

$$\begin{aligned}
&\sum_{a\in\mathrm{GF}(N)}\sum_{b\neq 0} e_{ab}^{\mathrm{PEC}}\\
&\leq (N-1)\max\Bigg\{\sum_{s=0}^{r}\binom{r}{s}\left(1-e_{Z_0}^{k\mathrm{EP}}-e_{Z_1}^{k\mathrm{EP}}\right)^{r-s}\\
&\qquad\times\left(e_{Z_0}^{k\mathrm{EP}}+e_{Z_1}^{k\mathrm{EP}}\right)^{s}\Pr(\text{the number of registers suffering from error of the form } X_iZ_1 \text{ is greater than or equal to those suffering from error of the form } X_i \text{ when drawn from a random sample of } s \text{ registers, given that these } s \text{ registers are suffering from error of the form } X_iZ_b \text{ for } b=0,1, \text{for a fixed } e_{00})\Bigg\}\\
&\leq (N-1)\max\Bigg\{\sum_{s=0}^{r}\binom{r}{s}\left(1-e_{Z_0}^{k\mathrm{EP}}-e_{Z_1}^{k\mathrm{EP}}\right)^{r-s}\\
&\qquad\times\left(e_{Z_0}^{k\mathrm{EP}}+e_{Z_1}^{k\mathrm{EP}}\right)^{s}\\
&\qquad\times\exp\left[-2s\left(\frac{1}{2}-\frac{e_{Z_1}^{k\mathrm{EP}}}{e_{Z_0}^{k\mathrm{EP}}+e_{Z_1}^{k\mathrm{EP}}}\right)^{2}\right]\Bigg\}\\
&= (N-1)\max\Bigg\{\Bigg\{1-\left(e_{Z_0}^{k\mathrm{EP}}+e_{Z_1}^{k\mathrm{EP}}\right)\\
&\qquad\times\left[e^{-2\left[1/2-e_{Z_1}^{k\mathrm{EP}}/\left(e_{Z_0}^{k\mathrm{EP}}+e_{Z_1}^{k\mathrm{EP}}\right)\right]^2}-1\right]\Bigg\}^{r}\Bigg\}\\
&\leq (N-1)\max\Bigg\{\Bigg[1-2t\left(e_{Z_0}^{k\mathrm{EP}}+e_{Z_1}^{k\,\mathrm{EP}}\right)\\
&\qquad\times\left(\frac{1}{2}-\frac{e_{Z_1}^{k\mathrm{EP}}}{e_{Z_0}^{k\mathrm{EP}}+e_{Z_1}^{k\mathrm{EP}}}\right)^{2}\Bigg]^{r}\Bigg\}
\end{aligned}\tag{32}$$

where $t \to 1$ as $k \to \infty$. Note that we have used [31, eq. (1.2.5)] to arrive at the second inequality above. (That equation is applicable because the assumption that $e_{00} > e_{01}$ leads to $e_{Z_0}^{k\mathrm{EP}} > e_{Z_1}^{k\mathrm{EP}}$ for a sufficiently large k.) It is straightforward to check that (32) remains valid if r depends on k.

Since $e_{00} > e_{01}$

$$\left(\sum_{b\in\mathrm{GF}(N)} e_{0b}\right)^{2^k} = \left[e_{00}+(N-1)e_{01}\right]^{2^k}$$

is the dominant term in the common denominator of (24)–(26) when k is sufficiently large, (29) follows directly from (24)–(26) and (32). □

The preceding theorem tells us that the effect of PEC is to reduce errors of the form X_aZ_b with $b \neq 0$ at the expense of possibly increasing errors of the form X_c with $c \neq 0$. For this reason, powerful signal privacy amplification procedures can be constructed by suitably combining LOCC2 EP and PEC.

Now, we prove the unconditional security of Scheme A.

Theorem 3: Let $N = p^n$ be a prime power, and let ϵ_p, ϵ_I, and δ be three arbitrarily small but fixed positive numbers. Define

$$e^{\mathrm{QER}} = \frac{(N^2-1)(2N+1-\sqrt{5})}{2N(N^2+N-1)}. \tag{33}$$

The EB QKD Scheme A involving the transfer of N-dimensional quantum particles is unconditionally secure with security parameters (ϵ_p, ϵ_I) when the number of quantum register transfers $L \equiv L(\epsilon_p, \epsilon_I, \delta)$ is sufficiently large. Specifically, provided that Alice and Bob abort the scheme whenever the estimated QER in step 2 is greater than $(e^{\mathrm{QER}} - \delta)$, the secret key generated by Alice and Bob is provably secure in the $L \to \infty$ limit. In fact, if Eve uses an eavesdropping strategy with at least ϵ_p chance of passing the signal quality test stage in step 2, the mutual information between Eve's measurement results after eavesdropping and the final secret key is less than ϵ_I. In this respect, Scheme A tolerates asymptotically up to a QER of e^{QER}.

Proof: By picking $L \gg (N+1)^2|G|\log(|G|/\epsilon_p)/\delta^2N^2$ and applying Lemma 2 and Theorem 2, we conclude that by testing $\mathrm{O}([N+1]^2\log[\,|G|/\epsilon_p]/\delta^2N^2)$ pairs in each set S_M, any eavesdropping strategy that causes a QER higher than e^{QER} has less than ϵ_p chance of passing the signal quality test stage in step 2 of Scheme A. (Similarly, if the QER is less than $(e^{\mathrm{QER}}-2\delta)$, it has at least $(1-\epsilon_p)$ chance of passing step 2. As δ can be chosen to be arbitrarily small, the signal quality test stage in step 2 of Scheme A is not overly conservative.)

Now, suppose that Alice and Bob arrive at the signal privacy amplification stage in step 3 of Scheme A. Since $L \to \infty$, the quantum particle pairs used in the signal quality test stage in step 2 do not affect the error rates e_{ab}'s of the remaining untested particle pairs.

From the discussions in Section IV-B, we only need to consider the case when Eve uses a classical cheating strategy. Hence, the initial error rates e_{ab}'s satisfy (21) and (22). After applying k rounds of LOCC2 EP, Alice and Bob may consider picking r used in the majority vote PEC to be

$$r \approx \frac{\epsilon_I \left[e_{00} + (N-1)e_{01}\right]^{2^k}}{2\ell(N-1)N^{2^k} e_{01}^{2^k}} \tag{34}$$

where ℓ is the number of quantum particle pairs Alice and Bob share immediately after the PEC procedure in step 3b. Provided that $e_{00} > e_{01}$, in the $k \to \infty$ limit, $r \to \infty$. So, from (28) and (29) in Lemma 5, the QER of the remaining quantum registers after PEC, e^{final}, is upper-bounded by

$$e^{\mathrm{final}} < \frac{\epsilon_I}{2\ell} + (N-1) \times \exp\left\{ \frac{-\epsilon_I N (e_{00} - e_{01})^{2^{k+1}}}{8\ell(N-1)N^{2^k} e_{01}^{2^k} \left[e_{00} + (N-1)e_{01}\right]^{2^k}} \right\}. \tag{35}$$

In other words, $e^{\mathrm{final}} < \epsilon_I/\ell$ provided that

$$(e_{00} - e_{01})^2 > N e_{01} \left[e_{00} + (N-1)e_{01}\right]. \tag{36}$$

This condition is satisfied if and only if

$$e_{00} > \frac{N^2 + 1 + (N^2-1)\sqrt{5}}{2N(N^2+N-1)}. \tag{37}$$

It is easy to verify that the constraint in (37) is consistent with the assumption that $e_{00} > e_{01}$. Hence, provided that the initial QER satisfies

$$\sum_{(a,b)\neq(0,0)} e_{ab} < \frac{(N^2-1)(2N+1-\sqrt{5})}{2N(N^2+N-1)} = e^{\mathrm{QER}} \tag{38}$$

the fidelity of the ℓ quantum particle pairs shared between Alice and Bob immediately before they perform standard basis measurements to obtain their secret key is at least $1 - e^{\mathrm{final}} > 1 - \epsilon_I/\ell$. By [3, Footnote 28], the mutual information between Eve's final measurement result after eavesdropping and the final secret key is at most ϵ_I. Thus, provided Alice and Bob abort the scheme if the estimated QER in step 2 exceeds $(e^{\mathrm{QER}} - \delta)$, the secret key generated is provably secure. That is, the scheme is unconditionally secure with security parameters (ϵ_p, ϵ_I). □

A few remarks are in order.

First, as Scheme A reduces any kind of eavesdropping attacks in the channel to a classical cheating strategy which in turn is reduced to depolarization of the quantum signal, the ratio of the QER to the SBMER is given by $(N+1):N$. From Theorem 3, the maximum tolerable SBMER for Scheme A equals

$$e^{\mathrm{SBMER}} = \frac{(N^2-1)(2N+1-\sqrt{5})}{2(N+1)(N^2+N-1)}. \tag{39}$$

In addition, if $p = 2$, Lemma 3 implies that no matter what bijective map Alice and Bob use to convert their standard basis 2^n-dimensional quantum particle measurement results into an n-bit string,the probability that exactly i out of n consecutive measured bits are in error equals $2^n e_{01}\binom{n}{i}$ for all $0 \leq i \leq n$. Consequently, the BER equals

$$2^n e_{01} \sum_{i=0}^{n} \binom{n}{i} i/n = 2^{2n-1} e_{01}$$

and the maximum tolerable BER for Scheme A is given by

$$e^{\mathrm{BER}} = \frac{N(2N+1-\sqrt{5})}{4(N^2+N-1)}. \tag{40}$$

TABLE II
THE TOLERABLE SBMER AND BER FOR SCHEME A AND HENCE ALSO SCHEMES B AND C FOR $N \leq 16$. AS POINTED OUT IN THE TEXT, THE VALUES OF SBMER AND BER SHOULD NOT BE COMPARED DIRECTLY

N	Tolerable SBMER	Tolerable BER
2	27.64%	27.64%
3	43.31%	N.A.
4	53.40%	35.60%
5	60.44%	N.A.
7	69.62%	N.A.
8	72.78%	41.59%
9	75.34%	N.A.
11	79.25%	N.A.
13	82.09%	N.A.
16	85.14%	45.41%

We tabulate the tolerable SBMER and BER in Table II. However, we must emphasize once again that according to the discussions in Section IV-A, we *cannot* deduce the relative error tolerance capability from Table II.

Second, we study the tolerable error rate of Scheme A as a function of N. Table II shows that the maximum tolerable BER e^{BER} for $N = 2$ is the same as the one obtained earlier by Chau in [25]. Additionally, e^{SBMER} increases as N increases. In fact, the tolerable SBMER and BER tend to 100% and 50%, respectively, as $N \to \infty$. More precisely, as $n \to \infty$, the tolerable BER for Scheme A using 2^n-level quantum particles scales as $\approx 1/2 - (1+\sqrt{5})/2^{n+2}$. If N is a prime power, e^{SBMER} for Scheme A using N-level quantum particles scales as $\approx 1 - (3+\sqrt{5})/2N$ as $N \to \infty$. On the other hand, the following lemma sets the upper limit for the tolerable SBMER for Scheme A.

Lemma 6: The tolerable SBMER for Scheme A is upper-bounded by $(N-1)/(N+1)$. In fact, this bound is set by the following interpret-and-resend strategy: for each N-dimensional particle in the insecure quantum channel, Eve randomly and independently picks $M \in SL(2,N)$ and measures the particle in the basis $\{T(M)|i\rangle : i \in \mathrm{GF}(N)\}$. Then, she records the measurement result and resends the measured particle to Bob.

Proof: The proof follows the idea reported in [24]. Clearly, using this intercept-and-resend strategy, no quantum correlation between Alice and Bob can survive and hence no provably secure key can be distributed. Thus, this eavesdropping strategy sets the upper bound for the tolerable SMBER and BER for Scheme A. If the quantum particle is prepared by Alice and measured by Eve in the same basis, that particle will suffer Z_a error with equal probability for all $a \in \mathrm{GF}(N)$. As Scheme A depolarizes Pauli errors, we know that e_{00} induced by this eavesdropping strategy equals $1/N$. Therefore, the SBMER for this strategy is

$$[(1-1/N)/(N^2-1)] \times N(N-1) = (N-1)/(N+1). \ \square$$

Thus, the difference between the tolerable SBMER and its theoretical upper bound tends to zero in the limit of large N. So in this limit, the error tolerance capability of Scheme A approaches its maximally allowable value.

Third, readers may wonder why Scheme A is highly error tolerant especially when N is large. Every quantum cheating strategy can be reduced to a classical one. Furthermore, Lemma 3 tells us that Scheme A depolarizes the errors caused by any classical cheating strategy in the transmitted quantum signals. This greatly restricts the types of quantum errors we need to consider. The LOCC2 EP becomes a powerful tool to reduce spin errors at the expense of increasing phase errors. Furthermore, $e_{Z_0}^{k\mathrm{EP}} > e_{Z_b}^{k\mathrm{EP}}$ for all $b \neq 0$ provided that $e_{00} > e_{01}$. In other words, the dominant kind of phase error is having no phase error at all. Thus, the majority vote PEC procedure is effective in bringing down the phase error. This is the underlying reason why Scheme A is so powerful that, in the limit $N \to \infty$, $e^{\mathrm{SBMER}} \to 1^-$.

Fourth, the unconditional security proof in Theorem 3 does not depend on the phase $f_M(a,b)$ used in (6). Recall from the discussions in Section III-A that $T : SL(2,2^n) \longrightarrow U(2^n)$ is not a group representation. So, in practice, Alice and Bob may replace $T(M_1 M_2 \cdots M_k)$ used in Scheme A by $T(M_k)T(M_{k-1})\cdots T(M_1)$, in which the M_i's are chosen from the two generators of $SL(2,2^n)$.

Fifth, the privacy amplification performed in Scheme A is based entirely on entanglement purification and phase error correction. In fact, the key ingredient in reducing the QER used in the proof of Theorem 3 is the validity of the condition stated in (36). Nonetheless, there is no need to bring down the QER to the small security parameter ϵ_I. One may devise an equally secure scheme by following the adaptive procedure introduced by Chau in [25] instead. That is, Alice and Bob may switch to a concatenated Calderbank–Shor–Steane quantum code when the PEC brings down the QER to about 5%. The strategy of adding an extra step of quantum error correction toward the end of the privacy amplification procedure may increase the key generation rate. To understand why, let us consider the proof of Theorem 3 together with (34). They tell us that in order to bring the QER down to less than ϵ after k rounds of LOCC2 EP, Alice and Bob have to choose r and hence the number of quantum registers needed in PEC to be $\sim\epsilon c^{2^k}$ for some constant $c > 1$. In contrast, by randomizing the quantum registers, the QER after each application of Steane's seven quantum register code is reduced quadratically whenever the QER is less than about 5%. Consequently, Alice and Bob may increase the key generation rate by performing fewer rounds of LOCC2 EP, choosing $\epsilon \approx 0.01$, and finally adding a few rounds of the Calderbank–Shor–Steane code quantum error correction procedure.

V. Reduction to the PM Scheme

Finally, we apply the standard Shor and Preskill proof [22] to reduce the EB Scheme A to two provably secure PM schemes in this section. Let us first write down the detail procedures of Schemes B and C before showing their security.

PM QKD Scheme B

1) Alice randomly and independently prepares $L \gg 1$ quantum particles in the standard basis. She randomly and independently applies a unitary transformation $T(M) \in T[G]$ to each quantum particle, where G equals $SL(2,N)$ or an order (N^2-1) subgroup of $SL(2,N)$ (if it exists). Alice records the states and transformations she applied and then sends the states to Bob. Bob acknowledges the receipt of these particles and then applies a randomly and independently picked $T(M')^{-1}$ to each received particle. Now, Alice and Bob publicly reveal the unitary transformations they applied to each particle. A particle is kept and is said to be in the set S_M if Alice and Bob have applied $T(M)$ and $T(M)^{-1}$ to it, respectively. Bob measures the particles in S_M in the standard basis and records the measurement results.
2) Alice and Bob estimate the channel quantum error rate by sacrificing a few particles. Specifically, they randomly pick $\mathrm{O}([N+1]^2 \log[\,|G|/\epsilon]/\delta^2 N^2)$ pairs from each of the $|G|$ sets S_M and publicly reveal the preparation and measured states for each of them. In this way, they obtain the estimated channel error rate to within δ with probability at least $(1-\epsilon)$. If the channel error rate is too high, they abort the scheme and start all over again.
3) Alice and Bob perform the following privacy amplification procedure.
   a) They apply the privacy amplification procedure with two-way classical communication similar to the ones reported in [24], [25]. Specifically, Alice and Bob randomly group their corresponding remaining quantum particles in pairs. Suppose the jth particle of the ith pair was initially prepared in the state $|s_{i_j}\rangle$. Then, Alice publicly announces the value $s_{i_1} - s_{i_2} \in \mathrm{GF}(N)$ for each pair i. Similarly, Bob publicly announces the value $s'_{i_1} - s'_{i_2}$ where $|s'_{i_j}\rangle$ is the measurement result of the jth particle in the ith pair. They keep one of their corresponding registers of the pair only when their announced values of the corresponding pairs agree. They repeat the above procedure until there is an integer $r > 0$ such that a single application of step 3b will bring the signal quantum error rate of the resultant particles down to ϵ_I/ℓ^2 for a fixed security parameter $\epsilon_I > 0$, where $r\ell$ is the number of remaining quantum particles they have. They abort the scheme either when r is greater than the number of remaining quantum particles they possess or when they have used up all their quantum particles in this procedure.
   b) They apply the majority vote phase error correction procedure introduced by Gottesman and Lo [24]. Specifically, Alice and Bob randomly divide their corresponding resultant particles into sets each containing r particles. They replace each set by the sum of the values prepared (by Alice) or measured (by Bob) of the r particles in the set. These replaced values are bits of their final secure key string.

EQB PM QKD Scheme C $[2^n, n_{\mathrm{ns}}]$

1) Alice and Bob agree on a bijection mapping GF (2^n) to an n-bit string. Alice prepares $L \gg 1$ sets; and each set contains n qubits that are randomly and independently prepared in the standard basis $\{|i\rangle : i \in \mathrm{GF}\,(2^n)\}$ identified through their mutually agreed bijection. She records the state of each set in the form of an n-bit string. Then, she randomly and independently applies $T(M) \in T[G]$ to each set of qubits, where G equals $C_3 < SL(2,2)$ and $SL(2,2^n)$ for $n = 1$ and $n > 1$, respectively. She permutes the n qubits in each set with n_{ns} randomly prepared nonsignaling qubits and sends them to Bob. (In the upcoming analysis, one finds that for a fixed n, the tolerable BER of this scheme increases with n_{ns}. However, the number of nonsignaling qubits used is limited by the absence of quantum storage capability.) After Bob has received these qubits, Alice tells him which of the n qubits belong to a set that will be used to generate the key. Bob measures and discards the n_{ns} nonsignaling qubits and applies a randomly and independently picked $T(M')^{-1}$ to each of the n qubits in the set that will be used to generate the key. Now, Alice and Bob publicly reveal their unitary transformations applied to each set. A set is kept and is said to be in S_M if Alice and Bob have applied $T(M)$ and $T(M)^{-1}$ to it, respectively. Bob records the standard basis measurement results identified through their mutually agreed on bijection in the form of an n-bit string for each set in S_M. At this point, Alice and Bob should each have $|G|$ families of n-bit strings; each family contains the prepare state/measurement result of qubits in S_M. Moreover, in the absence of noise and Eve, the corresponding bit strings in Alice's and Bob's hands should agree.
2) Alice and Bob regard their $|G|$ families of n-bit strings as states in the standard basis $\{|i\rangle : i \in \mathrm{GF}\,(N)\}$ and follow steps 2 and 3 in Scheme B to obtain their secret key.

Note that in Scheme C $[2^n, n_{\mathrm{ns}}]$ (or Scheme C for short if the values of n and n_{ns} are clearly known to the readers), apart from the possibly entangled qubits that are used to generate the secret key, Alice and Bob have to create and send random nonsignaling qubits through the insecure channel. The proofs of Theorems 4 and 5 tell us that while the use of nonsignaling qubits does not change the tolerable BER, it is essential for Scheme C to tolerate more drastic eavesdropping attacks.

Theorem 4 (Based on Shor and Preskill [22]) : The tolerable BER of Scheme A in Section III-B as well as Schemes B and C above are equal. Thus, the conclusion of Theorem 3 is also applicable to Schemes B and C.

Proof: Recall from [22] that Alice may measure all her share of quantum registers right at step 1 in Scheme A without affecting the security of the scheme. Besides, LOCC2 EP and PEC procedures in Scheme A simply permute the measurement basis. Also, the final secret key generation does not make use of the phase information of the transmitted quantum registers. Hence, the Shor–Preskill argument in [22] can be applied to Scheme A, giving us equally secure PM Schemes B and C. (Note that the introduction of random nonsignaling qubits does not affect the tolerable BER of Scheme C as these qubits are discarded after being measured and are not used to generate the secret key.) □

As discussed in Section IV-A, we *cannot* compare the error-tolerant capability of Scheme B that uses unentangled quantum particles of different dimensions as information carriers. Nonetheless, we can compare the error-tolerant capability of the EQB PM QKD Scheme C against the same eavesdropping attack.

Theorem 5: For any fixed n, the error-tolerant capability of Scheme C $[2^n, n_{\mathrm{ns}}]$ increases with n_{ns} in the limit of a large

$$\sum_{M\in SL(2,2^n)} |S_M|.$$

Besides, in the limits of a large $\sum_{M\in SL(2,2^n)} |S_M|$ and a large n_{ns}, the error-tolerant capability of Scheme C $[2^n, n_{\mathrm{ns}}]$ increases with n. That is, for any fixed n and in the limit of a large n_{ns}, whenever Scheme C $[2^n, n_{\mathrm{ns}}]$ generates a provably secure key under an eavesdropping attack, so does Scheme C $[2^{n'}, n_{\mathrm{ns}}]$ under the same attack for any $n' > n$. Furthermore, there is a family of eavesdropping attacks that can be tolerated by Scheme C $[2^{n'}, n_{\mathrm{ns}}]$. However, no provably secure key is produced in Scheme C $[2^n, n_{\mathrm{ns}}]$.

Proof: Recall that Alice sends Bob packets of qubits each containing n signaling as well as n_{ns} nonsignaling qubits and that any eavesdropping strategy in Scheme C is equivalent to a classical probabilistic cheating strategy. Suppose that the channel quantum error rate is q. In other words, the probability that a randomly chosen qubit passing through the insecure channel is in error equals q. Let q_k denote the portion of packets that contains exactly k erroneous qubits. Then, q_k's satisfy the following three constraints:

$$\sum_{k=0}^{n+n_{\mathrm{ns}}} q_k = 1, \tag{41}$$

$$\sum_{k=0}^{n+n_{\mathrm{ns}}} k q_k = (n+n_{\mathrm{ns}})q, \tag{42}$$

and

$$0 \le q_k \le 1 \tag{43}$$

for $k = 0, 1, \ldots, n+n_{\mathrm{ns}}$. Clearly, the set of $(q_0, q_1, \ldots, q_{n+n_{\mathrm{ns}}})$ satisfying the above three constraints is convex.

Since Eve does not know which qubits are signaling before Bob has received them, the QER for the signaling qubits is given by

$$\begin{aligned} q_{\mathrm{QER}} &= \sum_{k=1}^{n+n_{\mathrm{ns}}} \left(1 - \prod_{i=0}^{k-1} \frac{n_{\mathrm{ns}} - i}{n + n_{\mathrm{ns}} - i} \right) q_k \\ &= 1 - \sum_{k=0}^{n+n_{\mathrm{ns}}} \left(q_k \prod_{i=0}^{n-1} \frac{n + n_{\mathrm{ns}} - k - i}{n + n_{\mathrm{ns}} - i} \right). \end{aligned} \tag{44}$$

We claim that for any q_k's satisfying the three constraints (41)–(43), q_{QER} is upper-bounded by

$$q_{\mathrm{QER}} \le 1 - \sum_{k=\lfloor (n+n_{\mathrm{ns}})q \rfloor}^{\lfloor (n+n_{\mathrm{ns}})q \rfloor + 1} \left(\tilde{q}_k \prod_{i=0}^{n-1} \frac{n + n_{\mathrm{ns}} - k - i}{n + n_{\mathrm{ns}} - i} \right) \tag{45}$$

where $\tilde{q}_k$'s are the (unique) solutions of the system of equations

$$\sum_{k=\lfloor (n+n_{\rm ns})q\rfloor}^{\lfloor (n+n_{\rm ns})q\rfloor+1} \tilde{q}_k = 1 \tag{46}$$

and

$$\sum_{k=\lfloor (n+n_{\rm ns})q\rfloor}^{\lfloor (n+n_{\rm ns})q\rfloor+1} k\tilde{q}_k = (n+n_{\rm ns})q. \tag{47}$$

In other words, we claim that among all strategies that cause a channel quantum error rate q, the one that causes either $\lfloor (n+n_{\rm ns})q\rfloor$ or $\lfloor (n+n_{\rm ns})q\rfloor + 1$ erroneous qubits in each packet produces the highest QER in the signaling qubits.

To show the validity of our claim, we rewrite (44) as

$$\begin{aligned} q_{\rm QER} = 1 &- \sum_{k=\lfloor (n+n_{\rm ns})q\rfloor}^{\lfloor (n+n_{\rm ns})q\rfloor+1} \left(\tilde{q}_k \prod_{i=0}^{n-1} \frac{n+n_{\rm ns}-k-i}{n+n_{\rm ns}-i} \right) \\ &- \sum_{k=0}^{n+n_{\rm ns}} \left(\Delta q_k \prod_{i=0}^{n-1} \frac{n+n_{\rm ns}-k-i}{n+n_{\rm ns}-i} \right) \end{aligned} \tag{48}$$

where $\Delta q_k = q_k - \tilde{q}_k$ if $k = \lfloor (n+n_{\rm ns})q\rfloor$ or $\lfloor (n+n_{\rm ns})q\rfloor + 1$, and $\Delta q_k = q_k$ otherwise. Since the set of $(q_0, \ldots, q_{n+n_{\rm ns}})$ satisfying (41)-(43) is convex, the claim is valid if we can show that the last term in (48) is nonpositive for all Δq_k's satisfying

$$\sum_k \Delta q_k = \sum_k k \Delta q_k = 0$$

and $\Delta q_j \geq 0$ whenever $j = \lfloor (n+n_{\rm ns})q\rfloor$ or $\lfloor (n+n_{\rm ns})q\rfloor + 1$.

There are three cases to consider. The first case is that $\Delta q_k \geq 0$ for all k. Clearly, this is possible only if $\Delta q_k = 0$ for all k. So in this case, the last term in (48) equals 0.

The second case is that exactly one $\Delta q_k < 0$. Without loss of generality, we may assume that the one is $\Delta q_{\lfloor (n+n_{\rm ns})q\rfloor}$. Observe that one can tune Λ_i's to make the auxiliary real-valued function ξ in the equation below two times differentiable and $\xi'' \geq 0$ in $(0, n+n_{\rm ns})$

$$\xi(k) = \begin{cases} \prod_{i=0}^{n-1} \Gamma(n+n_{\rm ns}-k-i+1), & \text{if } 0 \leq k \leq n_{\rm ns} \\ \sum_{i=0}^{3} \Lambda_i k^i, & \text{if } n_{\rm ns} < k < n_{\rm ns}+1 \\ 0, & \text{if } k \geq n_{\rm ns}+1. \end{cases} \tag{49}$$

Consequently, such a $\xi(k)$ is a convex function in the interval $[0, n+n_{\rm ns}]$. Since

$$\sum_{k \neq \lfloor (n+n_{\rm ns})q\rfloor} \Delta q_k = -\Delta q_{\lfloor (n+n_{\rm ns})q\rfloor} > 0$$

the convexity of ξ implies that the last term in (48) is nonpositive.

The last case is that exactly two $\Delta q_k < 0$, namely, for $k = \lfloor (n+n_{\rm ns})q\rfloor$ and $\lfloor (n+n_{\rm ns})q\rfloor + 1$. In this situation,

$$\sum_k \Delta q_k = \sum_k k\, \Delta q_k = 0$$

demands that there exist $\Delta q_{k_1}, \Delta q_{k_2} > 0$ for some $k_1 < \lfloor (n+n_{\rm ns})q\rfloor$ and $k_2 > \lfloor (n+n_{\rm ns})q\rfloor + 1$. Consequently, we may define $\Delta q'_j = \Delta q''_j = 0$ for $j = \lfloor (n+n_{\rm ns})q\rfloor$ and $\lfloor (n+n_{\rm ns})q\rfloor + 1$ and decompose Δq_k as $\Delta q'_k + \Delta q''_k$ for all $k \neq \lfloor (n+n_{\rm ns})q\rfloor, \lfloor (n+n_{\rm ns})q\rfloor + 1$ in such a way that $\Delta q'_k, \Delta q''_k \geq 0$ for all k and

$$\sum_k \Delta q'_k = -\Delta q_{\lfloor (n+n_{\rm ns})q\rfloor}$$

and

$$\sum_k \Delta q''_k = -\Delta q_{\lfloor (n+n_{\rm ns})q\rfloor+1}.$$

By means of this decomposition and the convexity of the function ξ, we conclude that the last term in (48) is nonpositive. Hence, the claim in (45) is valid.

From (45)–(47), it is easy to check that for a fixed n, tolerable BER of Scheme C $[2^n, n_{\rm ns}]$ increases with $n_{\rm ns}$. Combining with (39) and Table II, we conclude that for $n = 2$, $q \approx 1.5 \times 0.2764$ and $q_{\rm QER} \lesssim 1.25 \times 0.5340$, $n_{\rm ns} \geq 23$. Thus, Scheme C $[4, n_{\rm ns}]$ generates a provably secure key when the channel BER is slightly higher than 27.64% provided that $n_{\rm ns} \geq 23$. Thus, this scheme is more error resistant than any UQB QKD scheme known to date.

Note that as $n_{\rm ns} \to \infty$, the right-hand side of (45) becomes $1-(1-q)^n$. (A simple way to argue why this is the case is to observe that in the limit of a large number of random nonsignaling qubits used, Eve can do no better than guessing which of the n qubits in a packet are used to generate the secret key when these qubits are traveling in the insecure channel.) As the Pauli signal quantum error is depolarized, Lemma 3 demands that the error rates caused by this classical probabilistic strategy are given by

$$e_{ab} = \begin{cases} (1-q)^n, & \text{if } a = b = 0 \\ \frac{1-(1-q)^n}{2^{2n}-1}, & \text{otherwise.} \end{cases} \tag{50}$$

From (40), the final key is provably secure provided that the probability q satisfies

$$q < q_{\rm crit}(n) \equiv 1 - \frac{1}{2}\left[\frac{(1+\sqrt{5})2^{2n} - (\sqrt{5}-1)}{2(2^{2n}+2^n-1)} \right]^{1/n}. \tag{51}$$

Since $q_{\rm crit}(n)$ is a strictly increasing function of n, we conclude that the error-tolerant capability of Scheme C $[2^n, n_{\rm ns}]$ strictly increases with increasing n in the limit of large $n_{\rm ns}$. Hence, this theorem is proved. □

Since the most error-resistant UQB PM scheme known to date is the one offered by Chau in [25] (which is also equivalent to Scheme C $[2, 0]$), the above theorem clearly shows the advantage of using entangled qubits as information carriers provided that Alice and Bob can transmit a large number of qubits without requiring quantum storage. Specifically, no UQB PM scheme to date can generate a provably secure key if Eve randomly causes an error to a qubit in the insecure quantum channel with probability q satisfying $0.4146 \approx q_{\rm crit}(1) \leq q < q_{\rm crit}(2) \approx 0.4234$. In contrast, Scheme C $[2^n, n_{\rm ns}]$ tolerates such an attack for any $n \geq 2$ and for a sufficiently large $n_{\rm ns}$ depending on n.

We emphasize that the use of random nonsignaling qubits is vital in the proof of Theorem 5. Otherwise, Eve may cause 100% signal quantum error in Scheme C $[2^n, n_{\rm ns}]$ by creating an X error to every one out of n consecutive qubits that passes through the insecure quantum channel. However, we also have to stress that the presence of nonsignaling qubits lowers the key generation rate of Scheme C. In the absence of quantum storage, the number of nonsignaling qubits per packet $n_{\rm ns}$ is limited by the decoherence time of qubits and the qubit transmission rate in the channel. The proof of Theorem 5 tells us that for $n = 2$, Alice and Bob need to use $n_{\rm ns} = 23$ in order to generate a provably secure key at a channel BER slightly higher than that which can be tolerated by all UQB QKD schemes known to date. Clearly, Scheme C [4], [23] generates a key at a rate 8% that of Scheme C [2, 0]. Moreover, manipulating a packet of 25 qubits in the absence of quantum storage in Scheme C [4], [23] is challenging.

Now, we discuss the number of different kinds of states Alice and Bob have to prepare and measure in Schemes B and C.

Theorem 6: Suppose Alice and Bob follow Schemes B or C with $G = SL(2, N)$, so that they prepare and measure in $N(N+1)$ bases (and hence $N^2(N+1)$ different states). If they choose G to be an order (N^2-1) subgroup of $SL(2, N)$ instead, they need to prepare and measure in $(N+1)$ different bases (and hence $N(N+1)$ states).

Proof:

Case 1: $G = SL(2, N)$. Let G' be the subgroup

$$\{\mathrm{diag}(\alpha, \alpha^{-1}) : \alpha \in \mathrm{GF}\,(N)^*\}$$

of $SL(2, N)$. Let $g, g' \in G'$ and $h \in SL(2, N)$. From (6)–(7)

$$\begin{aligned}
&\langle i|T(gh)^{-1}T(g'h)|i'\rangle \\
&\quad = \omega_p^{-\mathrm{Tr}(i'k)}\langle i|T(gh)^{-1}T(g'h)Z_k|i'\rangle \\
&\quad = \omega_p^{-\mathrm{Tr}(i'k)}\langle i|Z_{k\beta^{-1}}T(gh)^{-1}T(g'h)|i'\rangle \\
&\quad = \omega_p^{\mathrm{Tr}([\beta^{-1}i-i']k)}\,\langle i|T(gh)^{-1}T(g'h)|i'\rangle
\end{aligned}$$

for all $k \in \mathrm{GF}\,(N)$, where $g'g = \mathrm{diag}(\beta, \beta^{-1})$. Therefore, $\langle i|T(gh)^{-1}T(g'h)|i'\rangle = 0$ if $i \neq i'\beta$. In other words, the bases $\{T(gh)|i\rangle : i \in \mathrm{GF}\,(N)\}$ and $\{T(g'h)|i\rangle : i \in \mathrm{GF}\,(N)\}$ are the same. Consequently, if Alice and Bob choose $G = SL(2, N)$ in Schemes B and C, they need to prepare and measure in $N(N^2-1)/(N-1) = N(N+1)$ bases (and hence, $N^2(N+1)$ different states).

Case 2: $N = 2$ and G is the order-3 subgroup of $SL(2, 2)$. Theorem 8 in the Appendix tells us that G is unique. It is clear that, in this case, Alice and Bob need to prepare and measure their quantum states in three different bases.

Case 3: $N > 2$ and G is the order (N^2-1) subgroup of $SL(2, N)$. Theorem 8 in the Appendix implies that $N = 3, 5, 7, 11$. Besides, G contains an order $(N-1)$ subgroup H' in the form

$$\{P^{-1}\mathrm{diag}(\alpha, \alpha^{-1})P : \alpha \in \mathrm{GF}\,(N)^*\}$$

for some $P \in SL(2, N)$. Recall from Section III-A that $T : SL(2, N) \longrightarrow U(N)$ in this case is a transposed representation. Hence, from (7)

$$\begin{aligned}
\langle i|T(gh)^{-1}T(g'h)|i'\rangle &= \langle i|T(g'g^{-1})|i'\rangle \\
&= \langle i|T(\mathrm{diag}(\beta, \beta^{-1}))|i'\rangle \\
&= \langle i|i'\beta^{-1}\rangle
\end{aligned}$$

for some $\beta \in \mathrm{GF}\,(N)^*$. Hence, Alice and Bob need to prepare and measure in $(N^2-1)/(N-1) = N+1$ different bases (and hence, $N(N+1)$ states). □

Since the maximum number of mutually unbiased bases equals $(N+1)$ for any prime power N [32]–[34], Scheme B shows that certain PM QKD schemes not using mutually unbiased bases can be more error tolerant.

VI. Discussion

In summary, we have introduced two PM QKD schemes (Schemes B and C) based on depolarization of Pauli errors and proved their unconditional security. In particular, we showed that for a sufficiently large Hilbert space dimension of quantum particles N used, Scheme B generates a provably secure key close to 100% SBMER or 50% BER. This result demonstrates the advantages of using unentangled higher dimensional quantum particles as signal carriers as well as depolarizing Pauli errors in QKD. It also shows that, for $N > 2$, the use of certain nonmutually unbiased bases increases the error tolerance capability of QKD. In addition, Scheme C shows that the ability to create and transfer, but not to store entangled qubits is advantageous in quantum cryptography.

There is a tradeoff between the error tolerance rate and key generation efficiency, however. It is clear from the proof of Theorem 3 that r, and hence, the number L of quantum particles transferred from Alice and Bob, scales as 2^k. Besides, the probability that the measurement results agree and hence the control quantum register pairs are kept in LOCC2 EP equals $\approx 1/N$ in the worst case. As a result, while Schemes B and C are highly error tolerant, they generate a secret key with exponentially small efficiency in the worst case scenario. Fortunately, the adaptive nature of Schemes B and C makes sure that this scenario will not happen when the error rate of the channel is small. To conclude, in most practical situations, Alice and Bob should choose the smallest possible N whose corresponding $e^{\rm SBMER}$ is slightly larger than the channel standard basis measurement error rate. In this way, they can generate their provably secure key at the highest possible rate.

Appendix

This appendix discusses the possibility of depolarizing Pauli error using proper subgroups of $SL(2, N)$. The analysis makes use of the Dickson theorem [35] on the subgroup classification of projective special linear groups over finite fields. The version of the Dickson theorem listed below is due to Huppert in [36, Hauptsatz 8.27].

Theorem 7 (Dickson): Let $N = p^n$. Subgroups of $PSL(2, N)$ are isomorphic to one of the following families of groups.

1) elementary Abelian p-groups;
2) cyclic groups C_z of order z, where z is a divisor of $(N \pm 1)/(N - 1, 2)$;
3) dihedral groups D_z of order $2z$, where z is as defined in 2);
4) alternating group A_4 (this can occur only for $p > 2$ or when $p = 2$ and $n \equiv 0 \bmod 2$);
5) symmetric group S_4 (this can occur only if $N^2 \equiv 1 \bmod 16$);
6) alternating group A_5 (this can occur only if $p = 5$ or $N^2 \equiv 1 \bmod 5$);
7) a semidirect product of an elementary Abelian group of order p^m with a cyclic group of order t, where t is a divisor of $(p^m - 1, N - 1)$;
8) the group $PSL(2, p^m)$ for m a divisor of n, or the group $PGL(2, p^m)$ for $2m$ a divisor of n.

In addition to the Dickson theorem, the following lemma is also needed.

Lemma 7: If N is odd, $-I$ is the only element in $SL(2, N)$ whose order is 2.

Proof: Let

$$M = \begin{bmatrix} \alpha & \beta \\ \delta & \gamma \end{bmatrix}$$

be an order–2 element in $SL(2, N)$. $M^2 = I$ implies $\beta(\alpha + \gamma) = \delta(\alpha + \gamma) = 0$ and $\alpha^2 + \beta\delta = 1$. If $\alpha + \gamma = 0$, $\det M = -\alpha^2 - \beta\delta = 1$ is consistent with $\alpha^2 + \beta\delta = 1$ only if N is even. So, $\alpha + \gamma$ must be equal to 0. Hence, $\beta = \gamma = 0$ and $M = \pm I$. As N is odd, $-I$ is the only order–2 element in $SL(2, N)$. □

We examine the possibility of using a smaller group to depolarize Pauli error in step 1. Specifically, we look for subgroups H of $SL(2, N)$ to do the job. Clearly, the order of the subgroup H must be a multiple of $(N^2 - 1)$.

Theorem 8: Proper subgroups H of $SL(2, N)$ satisfying $(N^2 - 1) \mid |H|$ exist only for $N = 2, 3, 5, 7, 11$ and $|H| = N^2 - 1$. Specifically, we note the following.

1) When $N = 2$, $H \cong C_3$. Moreover, this subgroup is unique and is generated by one element. In fact

$$H = \left\langle \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right\rangle.$$

2) When $N = 3$, $H \cong Q_8$. Moreover, this subgroup is unique and is generated by two elements. In fact

$$H = \left\langle \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix} \right\rangle.$$

3) When $N = 5$, $H/\{\pm I\} \cong A_4$. Moreover, H is generated by two elements. One possible choice of H is

$$\left\langle \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \right\rangle.$$

4) When $N = 7$, $H/\{\pm I\} \cong S_4$. Moreover, H is generated by two elements. One possible choice of H is

$$\left\langle \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \right\rangle.$$

5) When $N = 11$, $H/\{\pm I\} \cong A_5$. Moreover, H is generated by two elements. One possible choice of H is

$$\left\langle \begin{bmatrix} 2 & 0 \\ 0 & 6 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \right\rangle.$$

Furthermore, $|\{M \in H : M[a\ b]^t = [c\ d]^t\}| = 1$ for all $[a\,b], [c\,d] \neq [0\,0]$. Thus, replacing $SL(2, N)$ by H in Scheme A also depolarizes Pauli errors.

Proof: From the Dickson theorem, it follows that $SL(2, N)$ does not contain a proper subgroup H whose order divides $(N^2 - 1)$ if $N \neq 2, 3, 5, 7, 11$. Moreover, if H exists for $N = 2, 3, 5, 7, 11$, $|H| = N^2 - 1$. In what follows, we are going to show that such H indeed exist for $N = 2, 3, 5, 7, 11$.

Case 1: When $N = 2$, the Dickson theorem implies that if H exists, $H \cong C_3$. Since the only order–3 elements of $SL(2, 2)$ are

$$M_{21} \equiv \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \text{ and } M_{21}^2$$

the order 3 subgroup H of $SL(2, 2)$ exists and is unique. An explicit expression for $T(M_{21})$ is given in Table I for reference.

Case 2: When $N = 3$, the Dickson theorem implies that if H exists, $H/\{\pm I\} \cong D_2 \cong C_2 \times C_2$. H cannot be Abelian as H would then be isomorphic to $C_2 \times C_2 \times C_2$, contradicting Lemma 7. Since H is a non-Abelian group of order 8, H is generated by two elements. By Lemma 7 and [37, proof of Proposition 6.3], we conclude that the two elements generating H are both of order 4. Hence, $H \cong Q_8$. Note that the only order–4 elements of $SL(2, 3)$ are

$$M_{31} \equiv \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, \ -M_{31},$$
$$M_{32} \equiv \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix}, \ -M_{32}, \ M_{31}M_{32}, \text{and } M_{32}M_{31}.$$

Therefore, $\langle M_{31}, M_{32} \rangle$ is the only order-$(N^2 - 1)$ subgroup of $SL(2, 3)$. Explicit expressions for $T(M_{31})$ and $T(M_{32})$ are given in Table I for reference.

Case 3: When $N = 5$, the Dickson theorem implies that if H exists, $H/\{\pm I\} \cong A_4$ or D_6. Satz 8.13 in [36] says that $PSL(2, 5) \cong A_5$. Hence, the only possibility is that $H/\{\pm I\} \cong A_4$. Since A_4 can be generated by two elements, one of order 2 and the other of order 3, $H/\{\pm I\} = \langle M_{51}/\{\pm I\}, M_{52}/\{\pm I\} \rangle$ for some $M_{51}, M_{52} \in SL(2, 5)$ provided that H exists. Moreover, $M_{51}/\{\pm I\}$ and $M_{52}/\{\pm I\}$ are of order 2 and 3, respectively. We may assume that $M_{52}^3 = -I$, for otherwise replace M_{52} by $-M_{52}$. Consequently, the subgroup H, if it exists, is equal to $\langle -I, M_{51}, M_{52}\rangle = \langle M_{51}, M_{52}\rangle$. Thus, H can be generated by two elements in $SL(2,5)$. From Lemma 7, the order of M_{51} is equal to 4. By explicit search, H exists but is not unique. One possible H is

$$\left\{\begin{bmatrix}2 & 0\\ 0 & 3\end{bmatrix}, \begin{bmatrix}1 & 2\\ 1 & 3\end{bmatrix}\right\}.$$

Case 4: When $N = 7$, the Dickson theorem implies that if H exists, $H/\{\pm I\} \cong S_4$. Since S_4 is generated by two elements, namely, (1234) and (123), the subgroup $H/\{\pm I\}$, if it exists, equals $\langle M_{71}/\{\pm I\}, M_{72}/\{\pm I\}\rangle$. Moreover, using the same argument as in the proof of case 3), we may choose $M_{71}^4 = \pm I$ and $M_{72}^3 = -I$. Hence, H, if it exists, is equal to $\langle -I, M_{71}, M_{72}\rangle = \langle M_{71}, M_{72}\rangle$. By an explicit search, H exists but is not unique. One possible H is

$$\left\langle\begin{bmatrix}2 & 0\\ 0 & 4\end{bmatrix}, \begin{bmatrix}1 & 2\\ 1 & 3\end{bmatrix}\right\rangle.$$

Case 5: When $N = 11$, the Dickson theorem implies that if H exists, $H/\{\pm I\} \cong A_5$. Since A_5 is generated by two elements, namely, (12345) and (123), using the same argument as in the proof of cases 3) and 4), we conclude that H, if it exists, can be generated by two elements. An explicit search tells us that H exists but is not unique, and one possible H is

$$\left\langle\begin{bmatrix}2 & 0\\ 0 & 6\end{bmatrix}, \begin{bmatrix}1 & 1\\ 1 & 2\end{bmatrix}\right\rangle.$$

To show that $|\{M \in H : M[a\ b]^t = [c\ d]^t\}| = 1$ for all $[a\ b], [c\ d] \neq [0\ 0]$, we observe from our discussion of the structure of H above, that H contains an order-$(N-1)$ proper subgroup H'. Since $H' < SL(2,N)$

$$H' = \{P^{-1}\mathrm{diag}(\alpha, \alpha^{-1})P : \alpha \in \mathrm{GF}(N)^*\}$$

for some $P \in SL(2,N)$. As all order (N^2-1) subgroups of $SL(2,N)$ are conjugate to each other, it suffices to show the validity for $P = I$. As $N \nmid |H| = N^2 - 1$, H does not contain elements of the form

$$\begin{bmatrix}\alpha & \beta\\ 0 & \alpha^{-1}\end{bmatrix} \quad \text{or} \quad \begin{bmatrix}0 & \alpha\\ -\alpha^{-1} & \beta\end{bmatrix}$$

for some $\beta \neq 0$. Therefore, for any

$$\begin{aligned} M &= \begin{bmatrix}\alpha & \beta\\ \delta & \gamma\end{bmatrix} \in SL(2,N)\\ |\{H'MH'\}| &= |\{M'MM'' : M', M'' \in H'\}|\\ &= \begin{cases} N-1, & \text{if } \alpha = 0 \text{ or } \delta = 0\\ (N-1)^2, & \text{if } \alpha, \delta \neq 0.\end{cases} \end{aligned} \tag{52}$$

Also, the first column of matrices in $H'MH'$ are all distinct. Since $|H| = N^2 - 1$, (52) requires that the first columns of the matrices in H are all distinct. Hence, $|\{M \in H : M[a\ b]^t = [c\ d]^t\}| = 1$ for all $[a\ b], [c\ d] \neq [0\ 0]$. Combining with the fact that H' is a group, Scheme A depolarizes Pauli errors. □

REFERENCES

[1] C. H. Bennett, G. Brassard, R. Jozsa, D. Mayers, A. Peres, B. Schumacher, and W. K. Wootters, "Reduction of quantum entropy by reversible extraction of classical information," *J. Mod. Opt.*, vol. 41, no. 12, pp. 2307–2314, 1994.

[2] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and proof of its unconditional security," *J. Crypt.*. quant-ph/0011056v2, to be published.

[3] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, 1999.

[4] D. Mayers, "Unconditional security in quantum cryptography," *J. Assoc. Comput. Mach.*, vol. 48, no. 3, pp. 351–406, 2001.

[5] D. Gottesman and H.-K. Lo, "From quantum cheating to quantum security," *Phys. Today*, vol. 53, no. 11, pp. 22–27, 2000.

[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002.

[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing*, Bangalore, India, 1984, pp. 175–179.

[8] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Phys. Rev. Lett.*, vol. 81, no. 14, pp. 3018–3021, 1998.

[9] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A*, vol. 61, no. 1, pp. 010303(R):1–4, 2000.

[10] M. Hillery, "Quantum cryptography with sequeezed states," *Phys. Rev. A*, vol. 61, no. 2, pp. 022309:1–8, 2000.

[11] D. Gottesman and J. Preskill, "Secure quantum key distribution using squeezed states," *Phys. Rev. A*, vol. 63, no. 2, pp. 022309:1–18, 2001.

[12] H. Bechmann-Pasquinucci and A. Peres, "Quantum cryptography with 3-state systems," *Phys. Rev. Lett.*, vol. 85, no. 15, pp. 3313–3316, 2000.

[13] H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," *Phys. Rev. A*, vol. 61, no. 6, pp. 062308:1–6, 2000.

[14] M. Bourennane, A. Karlsson, and G. Björk, "Quantum key distribution using multilevel encoding," *Phys. Rev. A*, vol. 64, no. 1, pp. 012306:1–5, 2001.

[15] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," *Phys. Rev. Lett.*, vol. 88, no. 12, pp. 127902:1–4, 2002.

[16] M. Bourennane, A. Karlsson, G. Björk, N. Gisin, and N. J. Cerf, "Quantum key distribution using multilevel encoding: Security analysis," *J. Phys.: A*, vol. 35, no. 47, pp. 10065–10076, 2002.

[17] H. F. Chau, "Unconditionally Secure Key Distribution in Higher Dimensions," quant-ph/0212055v2, 2004.

[18] D. Bruß and C. Macchiavello, "Optimal eavesdropping in cryptography with three-dimensional quantum states," *Phys. Rev. Lett.*, vol. 88, no. 12, pp. 127901:1–4, 2002.

[19] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, 1991.

[20] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, "A proof of the security of quantum key distribution," in *Proc. 32nd Annu. ACM Symp. Theory of Computing (STOC2000)*. New York: ACM Press, 2000, pp. 715–724.

[21] C. H. Bennett, D. A. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A*, vol. 54, no. 5, pp. 3824–3851, 1996.

[22] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, 2000.

[23] H.-K. Lo, "Proof of unconditional security of six-state quantum key distribution scheme," *Quant. Inf. and Comp.*, vol. 1, no. 2, pp. 81–94, 2001.

[24] D. Gottesman and H.-K. Lo, "Proof of security of quantum key distribution with two-way classical communications," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 457–475, Feb. 2003.

[25] H. F. Chau, "Practical scheme to share a secret key through a quantum channel with a 27.5% bit error rate," *Phys. Rev. A*, vol. 66, no. 6, pp. 060302(R):1–4, 2002.

[26] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3065–3072, Nov. 2001.

[27] A. A. Albert and J. Thompson, "Two-element generation of the projective unimodular group," *Illinois J. Math.*, vol. 3, pp. 421–439, 1959.

[28] G. Alber, A. Delgado, N. Gisin, and I. Jex, "Efficient bipartite quantum state purification in arbitrary dimensional hilbert spaces," *J. Phys.: A*, vol. 34, no. 42, pp. 8821–8833, 2001.

[29] N. L. Johnson, S. Kotz, and N. Balakrishnan, *Discrete Multivariate Distributions*. New York: Wiley, 1997, ch. 39.

[30] D. Gottesman, "Fault-tolerant quantum computation with higher-dimensional systems," *Chaos, Solitons & Fractals*, vol. 10, no. 10, pp. 1749–1758, 1999.

[31] S. Roman, *Coding and Information Theory*. Berlin: Springer-Verlag, 1992, pp. 26–26.

[32] W. K. Wootters and B. D. Fields, "Optimal state-determination by mutually unbiased measurements," *Ann. Phys.*, vol. 191, no. 2, pp. 363–381, 1989.

[33] J. Lawrence, C. Brukner, and A. Zeilinger, "Mutually unbiased binary observable sets on N qubits," *Phys. Rev. A*, vol. 65, no. 3, pp. 032320:1–5, 2002.

[34] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, "A new proof for the existence of mutually unbiased bases," *Algorithmica*, vol. 34, no. 4, pp. 512–528, 2002.

[35] L. E. Dickson, *Linear Groups: With an Exposition of the Galois Field Theory*. New York: Dover, 1958, pp. 260–260.

[36] B. Huppert, *Endliche Gruppen I*. Berlin: Springer-Verlag, 1967, pp. 198–198.

[37] T. W. Hungerford, *Algebra*. Berlin: Springer-Berlag, 1974, pp. 97–98.