Experimentally feasible quantum-key-distribution scheme using qubit-like qudits and its comparison with existing qubit- and qudit-based protocols

H. F. Chau,[1,2,*] Qinan Wang,[1] and Cardythy Wong[1]

[1]*Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong*

[2]*Center of Theoretical and Computational Physics, University of Hong Kong, Pokfulam Road, Hong Kong*

(Received 14 March 2016; published 7 February 2017)

Recently, Chau [Phys. Rev. A **92**, 062324 (2015)] introduced an experimentally feasible qudit-based quantum-key-distribution (QKD) scheme. In that scheme, one bit of information is phase encoded in the prepared state in a 2^n-dimensional Hilbert space in the form $(|i\rangle \pm |j\rangle)/\sqrt{2}$ with $n \geqslant 2$. For each qudit prepared and measured in the same two-dimensional Hilbert subspace, one bit of raw secret key is obtained in the absence of transmission error. Here we show that by modifying the basis announcement procedure, the same experimental setup can generate n bits of raw key for each qudit prepared and measured in the same basis in the noiseless situation. The reason is that in addition to the phase information, each qudit also carries information on the Hilbert subspace used. The additional $(n-1)$ bits of raw key comes from a clever utilization of this extra piece of information. We prove the unconditional security of this modified protocol and compare its performance with other existing provably secure qubit- and qudit-based protocols on market in the one-way classical communication setting. Interestingly, we find that for the case of $n = 2$, the secret key rate of this modified protocol using nondegenerate random quantum code to perform one-way entanglement distillation is equal to that of the six-state scheme.

DOI: 10.1103/PhysRevA.95.022311

I. INTRODUCTION

Prepare-and-measure-based quantum-key-distribution (PM-QKD) protocol is a class of practical schemes in which the sender Alice prepares a quantum state and sends it through an insecure channel to the receiver Bob, who measures the received state so as to establish a shared raw key. Then, they apply classical post-processing to the raw key to distill a secure final key [1]. While early PM-QKD protocols such as the well-known BB84 scheme [2] use unentangled qubits as quantum information carriers, various authors proposed using qudits instead [1,3–8]. Generally speaking, qudit-based schemes are more error tolerant than qubit-based ones. However, qudit-based schemes are generally very hard to implement in practice partly because of the difficulty in preparing a general qudit state with high fidelity. Two notable exceptions are the recently proposed round-robin differential-phase-shift (RRDPS) scheme [8] and the so-called Chau15 scheme [3].

Recall that for the Chau15 scheme, Alice randomly picks two distinct elements i, j from the Galois field GF(2^n) with $n \geqslant 2$ and prepares a state in the form $(|i\rangle \pm |j\rangle)/\sqrt{2}$, where $\{|i\rangle : i \in \mathrm{GF}(2^n)\}$ is an orthonormal basis of the 2^n-dimensional Hilbert space. After receiving this state from Alice, Bob randomly picks two distinct elements $i', j' \in \mathrm{GF}(2^n)$ and projectively measures the state along $\{(|i'\rangle \pm |j'\rangle)/\sqrt{2}$. The Chau15 scheme is experimentally feasible because in the time bin representation, the preparation and measurement procedures are almost identical to those for diagonal basis qubits [3]. In this regard, we call these preparation and measurement states qubit-like. The security of the Chau15 scheme originates from the fact that for $n \geqslant 2$, the values of i, j, i', j' used, and hence the Hilbert subspace picked during the preparation and measurement of these qubit-like states, are withheld from the eavesdropper Eve until after Bob's measurement. Clearly, Alice and Bob should get a shared raw bit of key encoded in the phase of the prepared qudit should $\{i, j\} = \{i', j'\}$. In other words, the Chau15 scheme is able to generate one bit of raw secret key per successful transfer of each 2^n-dimensional qudit provided that it is prepared and measured in the same Hilbert subspace [3].

Here we show that the Chau15 scheme can be modified so that the number of raw secret bits generated per each such successful qudit transfer can be increased from 1 to n. We do it by replacing the announcement procedures for the Hilbert subspaces used to the preparation and measurement bases. In this way, the $(n-1)$ classical bits used to describe the Hilbert subspace information of each prepare and measure qubit-like qudit state, which is also withheld from Eve until Bob's measurement, can then be used to generate part of the raw key. More importantly, there is no need to change the hardware setup of the Chau15 scheme in this modification.

In Sec. II, we first introduce an entanglement-distillation-based quantum-key-distribution (ED-QKD) protocol known as Scheme A. Then, we use Shor-Preskill argument [1,9] to show that Scheme A can be reduced to two equally secure PM-QKD protocols known as Schemes B and C. In particular, the state preparation and measurement procedures in Scheme C are identical to that of the Chau15 scheme. We then prove the unconditional security of Scheme A and give key rate formulas under one-way entanglement distillation for Schemes A–C in Sec. III. We also compare the performance of our schemes to various provably secure qubit- and qudit-based PM-QKD schemes in the literature using one-way entanglement distillation in Sec. III. In particular, we find that for the case of $n = 2$, the secret key rate of Scheme B is equal to that of the six-state scheme [10] when both use nondegenerate random quantum codes to perform one-way entanglement distillation. Finally, we briefly discuss the experimental feasibility of Schemes B and C.

[*] hfchau@hku.hk

II. THE MODIFIED SCHEMES

A. The entanglement-distillation-based scheme known as Scheme A

Let $N \equiv 2^n$ with $n \geqslant 2$ and consider the following ED-QKD scheme known as Scheme A.[1] (The description below extensively uses a lot of finite field arithmetic. Readers may consult Ref. [11] for an introduction.)

The modified ED-QKD scheme (Scheme A).

(1) Alice secretly and randomly picks $[a] \in \text{GF}(N)/\text{GF}(2)$ and $\lambda \in \text{GF}(N)^* \equiv \text{GF}(N) \setminus \{0\}$. She prepares the state $\sum_{\bar{i}\in\text{GF}(2)} |\bar{i} + [a]\rangle_\text{A} \otimes |\bar{i} + [a]\rangle_\text{B}/\sqrt{2}$, where all arithmetic in the ket state are performance in the finite field GF(N). She applies the linear transformation $L_\lambda|i\rangle \mapsto |\lambda i\rangle$ for all $i \in \text{GF}(N)$ to the second qudit before sending it through an insecure quantum channel to Bob.

(2) Upon reception of the state from Alice, Bob secretly and randomly picks $\lambda' \in \text{GF}(N)$ and applies the linear transformation $L_{\lambda'}^{-1}$ to his received state.

(3) Alice and Bob jot down the joint measurement result along the basis,

$$\mathcal{B} = \left\{ \frac{1}{\sqrt{2}} \sum_{\bar{i}\in\text{GF}(2)} (-1)^{\bar{i}\bar{c}} |\bar{i} + [a]\rangle_\text{A} \otimes |\bar{i} + [a] + b\rangle_\text{B} \right. \\ \left. : [a] \in \text{GF}(N)/\text{GF}(2), b \in \text{GF}(N),\ \bar{c} \in \text{GF}(2) \right\} \\ \equiv \{|\Phi_{[a],b,\bar{c}}\rangle\}, \tag{1}$$

to their shared quantum state. Then, they publicly announce the values of λ,λ' used and keep the state only if $\lambda = \lambda'$. They repeat steps 1–3 until they have enough shared pairs.

(4) Alice and Bob pick a random sample from their remaining measured states and reveal the values of b and $\bar{c}$ obtained for each of the selected states for various λ's and $[a]$'s to estimate the error rate of the channel. Specifically, let $\tilde{e}_{b\bar{c}}$ be the probability that Alice prepares the state $|\Phi_{[a],0,0}\rangle$ and that the resultant state measured by Alice and Bob is $|\Phi_{[a],b,\bar{c}}\rangle$ for some $[a] \in \text{GF}(N)/\text{GF}(2)$. Then, by revealing the values of b and $\bar{c}$ from a random sample of those shared states to which Alice and Bob have applied $I \otimes L_\lambda$ and $I \otimes L_\lambda^{-1}$, they obtain an estimate of the value of $\tilde{e}_{\lambda[b],\bar{c}} + \tilde{e}_{\lambda([b]+1),\bar{c}}$ for all $[b] \in \text{GF}(N)/\text{GF}(2)$ and $\bar{c} \in \text{GF}(2)$. They proceed only if the error rate is sufficiently small. (We shall discuss the smallness criterion later on in the unconditional security proof in Sec. III.)

(5) Alice and Bob apply one- or two-way entanglement distillation similar to the ones used in Refs. [3,7,9,12,13] to the remaining states to distill out almost perfect EPR-like states each in the form $|\Phi_{[a],0,0}\rangle$. For instance, they apply a Calderbank-Shor-Steane (CSS) quantum error-correcting code [14–17] that could correct the measured spin-flip and phase errors of the channel in step 4. (Note that such a CSS code is constructed using a classical N-ary code C_1 and a classical binary code C_2 obeying $\{0\} \subset C_2 \subset C_1$ via the standard CSS construction. This is possible for a binary code can be regarded as an N-ary code by extending the linear coding space over the field GF(2) to the linear space over the field GF(N). In fact, we may extend the dual code of the binary code C_2 to an N-ary code with the same minimum distance using the same trick. In this way, C_1 and C_2 can be used to correct spin-flip and phase errors in this noisy and insecure channel, respectively. More importantly, the choice of C_1 could depend on the error syndrome measurement results of the code C_2 just like the one used by Lo in Ref. [12].)

(6) Finally, Alice and Bob separately measure each of their share of the almost perfect EPR-like states along the basis B_1, where

$$B_\lambda = \left\{ \frac{1}{\sqrt{2}} \sum_{\bar{i}\in\text{GF}(2)} (-1)^{\bar{i}\bar{c}} |\lambda(\bar{i} + [a])\rangle \right. \\ \left. : [a] \in \text{GF}(N)/\text{GF}(2), \bar{c} \in \text{GF}(2) \right\} \tag{2}$$

for all $\lambda \in \text{GF}(N)^*$. In this way, they obtain n bits of shared secret key per EPR-like state measured—1 bit comes from the phase information $\bar{c}$ and $(n-1)$ bits come from the value of $[a] \in \text{GF}(N)/\text{GF}(2)$.

We remark that in the absence of noise and Eve, Alice and Bob should get $b = \bar{c} = 0$ for each pair of tested quantum particles in step 4. And in this case, they share a copy of the EPR-like state $|\Phi_{[a],0,0}\rangle$ per qudit transfer just after step 3. A simple-minded way to understand the origin of security of this scheme is that as Alice puts each shared EPR-like state in a Hilbert subspace, which is not known to Eve, she has a non-negligible chance of disturbing the signal if she guesses this subspace incorrectly.

B. Reduction to two prepare-and-measure-based schemes known as Schemes B and C

Consider the unitary operation BADD for Alice and Bob to separately add their first qudit to their second qudit in the computational basis. Clearly,

$$\text{BADD}(|\Phi_{[a],b,\bar{c}}\rangle \otimes |\Phi_{[a'],b',\bar{c}'}\rangle) \\ = |\Phi_{[a],b,\bar{c}-\bar{c}'}\rangle \otimes |\Phi_{[a]+[a'],b+b',\bar{c}'}\rangle. \tag{3}$$

Consider also the unitary operation that acts on the computational basis according to

$$H(|b\rangle) = \begin{cases} (|b\rangle + |b+1\rangle)/\sqrt{2} & \text{if } b \in \text{GF}(N)/\text{GF}(2), \\ (-|b\rangle + |b+1\rangle)/\sqrt{2} & \text{otherwise.} \end{cases} \tag{4}$$

Then

$$H \otimes H(|\Phi_{[a],b,\bar{c}}\rangle) = (-1)^{\bar{b}_0}|\Phi_{[a],b+\bar{b}_0+\bar{c},\bar{b}_0}\rangle \\ = (-1)^{\bar{b}_0}|\Phi_{[a],[b]+\bar{c},\bar{b}_0}\rangle, \tag{5}$$

up to a global phase, where $\bar{b}_0 \in \text{GF}(2)$ denotes the constant term of the degree-$(n-1)$ polynomial expression for b in

[1] From now on, we use the convention that a variable in Roman, square-bracketed, overbarred, and Greek alphabet are in GF(N), GF(N)/GF(2), GF(2), and GF(N)*, respectively.

GF(2)[x]. Clearly, both $H \otimes H$ and BADD map basis states in $\mathcal{B}$ to itself up to an overall phase. Since the error correction and privacy amplification procedure using the specially designed CSS code in step 5 of Scheme A involves $H \otimes H$, BADD, standard basis measurement plus local quantum operation by Bob only, therefore Alice may push her final measurement forward in time. By the Shor-Preskill argument [7,9], we obtain an equally secure PM-QKD scheme that we called Scheme B.

To find the corresponding channel error estimation method for this equally secure Scheme B, we consider the linear operators [16,17]:

$$\mathtt{X}_u|i\rangle = |i+u\rangle \text{ and } \mathtt{Z}_u|i\rangle = (-1)^{\mathrm{Tr}(ui)}|i\rangle, \tag{6}$$

for all $u \in \mathrm{GF}(N)$, where $\mathrm{Tr}(i) = i + i^2 + i^4 + \cdots + i^{N/2}$ is the absolute trace of i. Then

$$L_\lambda^{-1}\mathtt{X}_u\mathtt{Z}_v L_\lambda = \mathtt{X}_{\lambda^{-1}u}\mathtt{Z}_{\lambda v}. \tag{7}$$

Recall that in Scheme A, Alice first prepares the state $|\Phi_{[a],0,0}\rangle$. Consider those shared states to which Alice and Bob have applied the operations $I \otimes L_\lambda$ and $I \otimes L_\lambda^{-1}$, respectively. Suppose Alice and Bob separately measure these shared states after passing through the insecure channel in the B_1 basis. Suppose further that Alice informs Bob of her measurement outcomes. Then from Eqs. (2) and (5)–(7), Bob could deduce $[\lambda^{-1}u] + \mathrm{Tr}(\lambda v)$ and hence both $[\lambda^{-1}u]$ and $\mathrm{Tr}(\lambda v)$ as these two variables are linearly independent over GF(2). Since the solution of the equation $[\lambda^{-1}u] = [b]$ is $u = \lambda[b]$ or $u = \lambda([b]+1)$, the outcomes of the above measurement by Alice and Bob give estimates of $\tilde{e}_{\lambda[b],\bar{c}} + \tilde{e}_{\lambda([b]+1),\bar{c}}$ for all $\lambda \in \mathrm{GF}(N)^*$, $[b] \in \mathrm{GF}(N)/\mathrm{GF}(2)$, and $\bar{c} \in \mathrm{GF}(2)$. Hence, our ED-QKD Scheme A can be reduced to the following equally secure PM-QKD Scheme B.

The modified PM-QKD scheme (Scheme B).

(1) Alice randomly picks $\lambda \in \mathrm{GF}(N)^*$ and prepares one of the basis states in B_λ by randomly selecting the parameters $[a]$ and $\bar{c}$. He sends the state to Bob.

(2) Upon reception, Bob randomly picks $\lambda' \in \mathrm{GF}(N)^*$ and measures his received state in the $B_{\lambda'}$ basis.

(3) They publicly announce the values of λ,λ' used and keep their state only if $\lambda = \lambda'$. They add the parameters $([a],\bar{c})$ describing their prepared and measured states to their raw key string. They repeat steps 1–3 until they have a sufficiently long raw key.

(4) They estimate the values of $\tilde{e}_{\lambda[b],\bar{c}} + \tilde{e}_{\lambda([b]+1),\bar{c}}$ by revealing (and discarding) a random sample of dits from the raw key to which Alice and Bob have applied $I \otimes L_\lambda$ and $I \otimes L_\lambda^{-1}$, respectively. They proceed only if the error rate is sufficiently small.

(5) Alice and Bob apply classical error correction and privacy amplification to their remaining raw keys based on the classical N-ary code C_1 and classical binary code C_2 obeying $\{0\} \subset C_2 \subset C_1$. Moreover, C_1 may be picked depending on the error syndrome of C_2 just like the privacy amplification procedure reported in Ref. [12]. Specifically, we denote the $(N/2)$-ary vector formed by the $[a]$'s and the binary vector formed by the $\bar{c}$'s in Alice's remaining raw key by $\vec{a}$ and $\vec{c}$, respectively. Alice announces the error syndromes for C_1 of $\vec{a}$ and C_2 of $\vec{c}$. Bob subtracts them from his corresponding measured error syndromes and then uses the subtracted results to perform classical error corrections using codes C_1 (C_2) on his remaining raw key $\vec{a}'$ ($\vec{c}'$). For a sufficiently low noise level, the Bob's raw key after error correction should agree with Alice's. They now use the cosets $\vec{a} + C_1$ and $\vec{c} + C_2$ as their shared final key.

Note that Scheme B is analogous to the Chau15 scheme in Ref. [3]. The most notable difference is that unlike the Chau15 scheme, the two-dimensional Hilbert subspaces used in state preparation and measurement are not revealed in Scheme B.

Since each element in B_λ can be rewritten in the form $(|i\rangle \pm |j\rangle)/\sqrt{2}$ for some $i \neq j \in \mathrm{GF}(N)$, the state preparation of Scheme B in step 1 is exactly the same as that of the Chau15. While the state measurement procedure of Scheme B in step 2 is a complete measurement and is different from the incomplete measurement used in the Chau15, we could further change this step in Scheme B to step 2' below so that the hardware setup is identical to that of the Chau15 scheme. We call this further modified protocol Scheme C.

The further modified PM-QKD scheme (Scheme C).

(2′) Upon reception, Bob randomly picks $\lambda' \in \mathrm{GF}(N)^*$, $[a'] \in \mathrm{GF}(N)/\mathrm{GF}(2)$ and measures his received state along $\{|\lambda'[a']\rangle \pm |\lambda'(1+[a'])\rangle\}/\sqrt{2}$. (Clearly, this is equivalent to randomly picking $i' \neq j' \in \mathrm{GF}(N)$ and measuring the received state along $(|i'\rangle \pm |j'\rangle)/\sqrt{2}$ as in the measurement step in the Chau15 scheme.) Bob informs Alice to ignore her parameters λ, $[a]$, and $\bar{c}$ and repeat her state preparation and sending procedures in step 1 of Scheme B in case his measurement fails.

Note that Schemes B and C are equally secure. The reason is that Eve's action on the qudits cannot depend on the values of λ''s and $[a]$'s used for she has no knowledge of them when the qudits pass through the insecure quantum channel. Consequently, the error rates $\tilde{e}_{b\bar{c}}$ experienced by the $|\Phi_{[a],0,0}\rangle$'s in the corresponding ED-QKD Scheme A for those discarded and undiscarded qudits are the same. In summary, this further modification in Scheme C allows easier experimental implementation than Scheme B because complete measurement in the $B_{\lambda'}$ basis even for $N = 4$ is not trivial. However, the key rate of Scheme C will be lower than that of Scheme B since more signals have to be discarded in step 2'. We shall get back to this point in Sec. III B below.

Finally, we remark that it is possible to apply two-way error correction and privacy amplification in Schemes A–C similar to the one used in the Chau15 scheme [3]. In fact, the conclusions on the error-tolerable capability of the Chau15 scheme using two-way entanglement purification in Ref. [3] is directly applicable to our three schemes. In what follows, however, we focus on the performance of Schemes A–C using the more practical one-way entanglement purification procedure [9], which gives a higher key rate when the channel noise is low at the expense of having a lower error-tolerable rate.

III. SECURITY AND PERFORMANCE ANALYSIS

A. The unconditional security proof Of Scheme A

Recall that in Scheme A, Eve sees the same completely mixed density matrix for the quantum state that Alice sends to Bob in step 1 irrespective of the value of λ

used. So the quantum operation $\rho \mapsto \mathcal{E}(\rho) = \sum_i K_i \rho K_i^\dagger$ Eve applies to the insecure quantum channel is independent of λ, where each Kraus operator used can be written as $K_i = \sum_{u,v\in\text{GF}(N)} g_{iuv} \mathtt{X}_u \mathtt{Z}_v$ for some $g_{iuv} \in \mathbb{C}$. Since $\sum_i K_i^\dagger K_i = I$ and $\mathtt{Z}_v \mathtt{X}_u = (-1)^{\text{Tr}(uv)} \mathtt{X}_u \mathtt{Z}_v$ [7,17], we have $\sum_{i,u,v} |g_{iuv}|^2 = 1$ and $\sum_{i,u,v} g^*_{iuv} g_{i,u,v+w} = 0$ for all $w \neq 0$. Consequently,

$$\begin{aligned} \tilde{e}_{b,\bar{c}} &= \langle \Phi_{[a],b,\bar{c}}|\mathcal{E}(|\Phi_{[a],0,0}\rangle\langle\Phi_{[a],0,0}|)|\Phi_{[a],b,\bar{c}}\rangle \\ &= \sum_i \sum_{v,v'}{}' g^*_{ibv} g_{ibv'} = \sum_i \sum_v{}' |g_{ibv}|^2 \equiv \sum_v{}' e_{bv}, \end{aligned} \tag{8}$$

where the primed sum is over those variables v and/or $v' \in \text{GF}(N)$ satisfying $\text{Tr}(v) = \text{Tr}(v') = \bar{c}$. Note that $I \otimes \mathtt{X}_u \mathtt{Z}_v |\Phi_{[a],b,\bar{c}}\rangle = I \otimes \mathtt{X}_{u'} \mathtt{Z}_{v'} |\Phi_{[a],b,\bar{c}}\rangle$ up to an irrelevant phase whenever $u = u'$ and $\text{Tr}(v) = \text{Tr}(v')$. Combined with Eq. (8), we conclude that Eve's attack through $\mathcal{E}$ is equivalent to the quantum operation $\rho \mapsto \sum_{u,v} e_{uv} \mathtt{X}_u \mathtt{Z}_v \rho (\mathtt{X}_u \mathtt{Z}_v)^\dagger$. In this regard, we may interpret e_{uv} as the probability that the qudit has experienced $\mathtt{X}_u \mathtt{Z}_v$ in the insecure quantum channel.

Recall that we obtain estimates of $\tilde{e}_{\lambda[b],\bar{c}} + \tilde{e}_{\lambda([b]+1),\bar{c}}$ for $[b] \in \text{GF}(N)/\text{GF}(2)$, $\lambda \in \text{GF}(N)^*$, and $\bar{c} \in \text{GF}(2)$ in step 4 of Scheme A. In the infinite key length limit, these estimates are exact. More importantly, e_{uv}'s must be consistent with these estimates through Eq. (8). The dimension of each qudit received by Bob is $N = 2^n$. So quantum Gilbert-Varshamov bound [14,15] tells us that the CSS code needed to perform the entanglement distillation in step 5 of Scheme A exists provided that [12]

$$\begin{aligned} K &= n - \max h_2(\{e_{uv}\}_{u,v\in\text{GF}(N)}) \\ &\equiv n + \max \sum_{u,v\in\text{GF}(N)} e_{uv} \log_2 e_{uv} > 0, \end{aligned} \tag{9}$$

where the maximum is over all e_{uv}'s in $[0,1]$ that are consistent with the error rate estimates, namely, $\tilde{e}_{\lambda[b],\bar{c}} + \tilde{e}_{\lambda([b]+1),\bar{c}}$ for $[b] \in \text{GF}(N)/\text{GF}(2)$, $\lambda \in \text{GF}(N)^*$ and $\bar{c} \in \text{GF}(2)$. Once this (random) CSS code exists, Alice and Bob can almost surely distill out almost perfect states each in the form $|\Phi_{[a],0,0}\rangle$.

There are a few ways to define the key rate for a QKD protocol. Here we extend the one used for qubit transfer in Ref. [1], which is experimentally meaningful, to qudit transfer by defining the secret key rate as the number of provably secure dits distilled divided by the number of qudit transferred in the limit of an arbitrary large number of qudit transfer. In the case of a lossless channel and perfect detectors, the secret key rates for Scheme A and hence also Scheme B equal

$$R_\text{A} = R_\text{B} = \max(0, K/\{n(N-1)\}). \tag{10a}$$

Note that in the above expression, the $1/(N-1)$ factor is the probability that Alice's λ agrees with Bob's λ'; and the $1/n$ factor converts the number of secret bits to dits. To summarize, both Schemes A and B can distill out a secret key provided that Eq. (9) holds for all e_{uv}'s given that they obey the constraints coming from the measurement statistics in step 4 of Scheme A. Clearly, the resultant secret key is composable [18,19]. This completes our proof of the unconditional security.

Finally, we remark that for Scheme C, Alice and Bob will add n bits to their raw keys if $\lambda = \lambda'$ and Bob's measurement in step 2' is successful. As a result, the secret key rate for Scheme C equals

$$R_\text{C} = 2R_\text{B}/N = \max(0, 2K/\{nN(N-1)\}). \tag{10b}$$

Here, the extra factor of $2/N$ is the probability of having a successful measurement in step 2'.

B. Key rate formulas for Schemes A–C

One may study the performance of Schemes A–C using all the parameters obtained from step 4 to constrain e_{uv}'s. But this approach is not very fruitful. Since the secret key comes from both $[a]$ and $\bar{c}$, it makes sense to gauge the performance of our QKD scheme by one of the following two sets of parameters. The first set is the average bit error rate $e_{\bar{c}}$ of the $\bar{c}$'s and the average dit error rate $e_{[a]}$ of the $[a]$'s in the raw key. (Note that both $e_{\bar{c}}$ and $e_{[a]}$ are averaged over λ.) The second set is simply the bit error rate of the raw bit key string e_raw.

Note that permuting the nonzero u and v indices in e_{uv}'s does not change the values $e_{\bar{c}}$, $e_{[a]}$, and e_raw. Combined with the convexity of h_2, we conclude that the maximum in the right-hand side of Eq. (9) is reached only if $e_{\mu 0} = e_{\mu' 0}$, $e_{0\nu} = e_{0\nu'}$, and $e_{\mu\nu} = e_{\mu'\nu'}$ for all $\mu,\mu',\nu,\nu' \in \text{GF}(N)^*$. This observation greatly simplifies the computation of K in Eq. (9) as it becomes the easily manageable optimization problem involving four unknowns, namely, $A \equiv e_{00}$, $B \equiv \sum_{\nu\in\text{GF}(N)^*} e_{0\nu}/(N-1)$, $C \equiv \sum_{\mu\in\text{GF}(N)^*} e_{\mu 0}/(N-1)$, and $D \equiv \sum_{\mu,\nu\in\text{GF}(N)^*} e_{\mu\nu}/(N-1)^2$ under the constraints,

$$0 \leqslant A,B,C,D \leqslant 1, \tag{11a}$$

$$1 = A + (N-1)(B+C) + (N-1)^2 D, \tag{11b}$$

$$e_{\bar{c}} = \frac{N}{2}\{B + (N-1)D\}, \tag{11c}$$

$$e_{[a]} = (N-1)\{C + (N-1)D\}, \tag{11d}$$

for the case of finding $R_\text{B}(e_{\bar{c}}, e_{[a]})$. And by putting in the additional constraint,

$$e_\text{raw} = \frac{1}{n}\left\{ e_{\bar{c}} + \frac{(n-1)N e_{[a]}}{(N-1)(N-2)} \right\}, \tag{11e}$$

one could determine $R_\text{B}(e_\text{raw})$. Note that the first term in the curly bracket in the right-hand side of Eq. (11e) comes from the fact that $1/n$ of the raw bits originates from the values of $\bar{c}$'s. For the second term, $\sum_{v\in\text{GF}(N)} e_{\mu v} = e_{[a]}/(N-1)$ for all $\mu \in \text{GF}(N)^*$ so that each type of dit error in $[a]$ occurs at a rate of $2e_{[a]}/(N-1)$. Converting the dit $[a]$ to $(n-1)$ bits, the corresponding bit error rate becomes $2e_{[a]}/(N-1) \times (N/4)/(N/2-1)$. Hence, the second term in Eq. (11e) corresponds to the contribution of bit error rate in the value of $[a]$.

Figure 1 plots the secret key rate R_B of Scheme B for $N = 4$ using one-way classical communication for fixed $e_{\bar{c}}$ and $e_{[a]}$ by numerically optimizing Eqs. (9) and (10a) subject to the constraints in Eqs. (11a)–(11d). It shows that the maximum tolerable error rate $e_{\bar{c}}$ ($e_{[a]}$) can be very high when $e_{[a]}$ ($e_{\bar{c}}$) is low. So, when $e_{[a]}$ is small, Alice and Bob may drop all the raw bits originated from $[a]$'s and use only the raw bits originated from $\bar{c}$'s to distill the secret key similar to the method used in Ref. [3]. In this way, the maximum tolerable $e_{\bar{c}}$ can be as

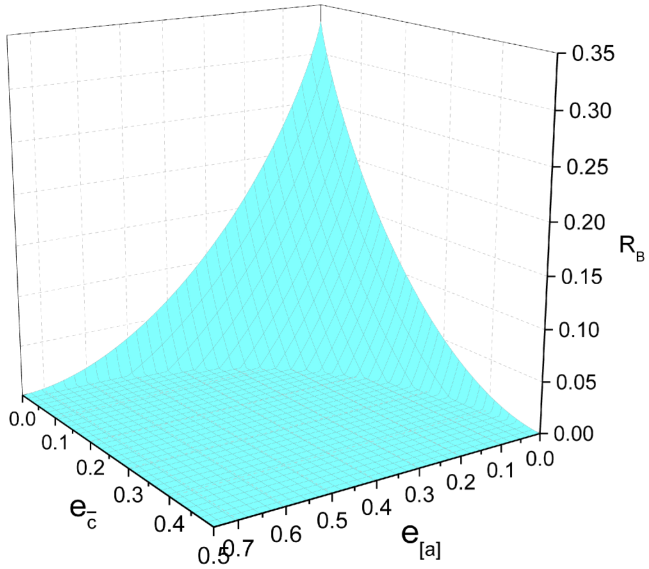

FIG. 1. The secret key rate R_{B} of Scheme B as a function of $e_{[a]}$ and $e_{\bar{c}}$ for $N = 4$ using one-way entanglement distillation.

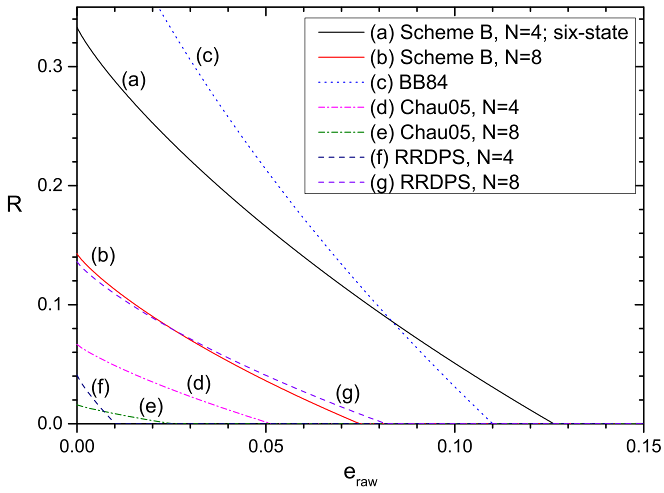

FIG. 2. The secret key rates R as a function of the bit error rate of the raw bit string e_{raw} for various PM-QKD schemes in the one-way communication setting. Scheme B, BB84, Chau05, and RRDPS are shown in solid, dot, dash-dot, and dash curves, respectively. Note that the six-state scheme here uses nondegenerate quantum code for entanglement distillation.

large as 1/2 at the expense of having a very low secret key rate. Similar conclusion is drawn when $e_{\bar{c}}$ is small as Alice and Bob may keep only those raw bits generated from the measurement of $[a]$'s. However, we shall not pursue further along this direction here.

C. Comparison with other provably secure PM-QKD schemes

We now compare the performance of Scheme B with a few well-known qubit- and qudit-based PM-QKD schemes. And we focus our comparison for the case when the quantum channel is lossless and that the detectors are prefect without dark counts and dead time in the limit of an infinitely long raw key. (We shall briefly discuss photon insertion loss in the experimental apparatus toward the end of this subsection.) In addition, we only consider the case of one-way privacy amplification. For qubit-based schemes, we choose the BB84 [2] and the six-state schemes [10]. Note that for qudit-based PM-QKD schemes, unconditional security proofs are known only for a few of them. The representative examples are the Chau05 scheme [7] and the RRDPS scheme [8]. That is why we choose these two in our comparison.

Figure 2 depicts the secret key rates R for various PM-QKD schemes using one-way entanglement distillation with nondegenerate quantum code as a function of e_{raw}. And Table I summarizes the values of R when $e_{\mathrm{raw}} = 0$ as well as the maximum provably secure bit error rate of the raw key for these schemes. For the cases of $N = 4$ and 8 in Scheme B, the secret key rates are computed by a similar numerical optimization procedure used to obtain Fig. 1. (For Scheme C in both cases, the rate is one-half of that for Scheme B.) It shows that the maximum provably secure bit error rate e_{raw} decreases as N increases.

The most eye-catching feature in Fig. 2 is that the secret key rates of the six-state scheme [10] and Scheme B for $N = 4$ seem to agree. (That is to say, for $N = 4$, Scheme B and hence Scheme C can tolerate up to 12.6% bit error rate [12].) Here we prove that it is indeed the case.

First, there is a unique property for $N = 4$, namely, that the bit error rate of the raw key e_{raw} in Eq. (11e) is unaltered by swapping $e_{\mu 0}$ with $e_{0\mu}$ for all $\mu \in \mathrm{GF}(N)^*$ although this swapping may change the values of $e_{\bar{c}}$ and $e_{[a]}$. By convexity of h_2, the value of K in Eq. (9) is minimized only if $B = C$. Thus, Eq. (9) can be written as an extremization over a single variable D after eliminating A and B via the constraints given by Eqs. (11b)–(11e). By finding the turning point of the resultant expression as a function of D, we conclude that K is minimized when $D = e_{\mathrm{raw}}^2/4$ [and hence $B = C = e_{\mathrm{raw}}/2 - 3e_{\mathrm{raw}}^2/4 = (e_{\mathrm{raw}}/2)(1 - 3e_{\mathrm{raw}}/2)$ and $A = 1 - 3e_{\mathrm{raw}} + 9e_{\mathrm{raw}}^2/4 = (1 - 3e_{\mathrm{raw}}/2)^2$]. Upon simplification,

TABLE I. Performance of various PM-QKD schemes using one-way entanglement distillation. Here, the $e_{\mathrm{raw}}^{\max}$ for the six-state scheme is for the case of using degenerate quantum code to perform entanglement distillation.

Scheme	N[a]	$R(0)$[b]	$e_{\mathrm{raw}}^{\max}$[c]
BB84 [2,9]	2	1/2	11.0%
Six-state [10,12]	2	1/3	12.7%
Chau05 [7]	4	1/15	5.1%
	8	1/63	2.5%
RRDPS [8]	4	0.041	1.0%
	8	0.136	8.2%
Scheme B	4	1/3	12.6%
	8	1/7	7.5%
Scheme C	4	1/6	12.6%
	8	1/28	7.5%

[a] The Hilbert space dimension of the quantum information carrier.
[b] The secret key rate in the noiseless and lossless situation.
[c] The maximum provably secure bit error rate of the raw key.

we have

$$\begin{aligned} K &= 2 + A\log_2 A + 3B\log_2 B + 3C\log_2 C + 9D\log_2 D \\ &= 2\left\{1 + \left(1 - \frac{3e_{\text{raw}}}{2}\right)\log_2\left(1 - \frac{3e_{\text{raw}}}{2}\right)\right. \\ &\quad \left. + \frac{3e_{\text{raw}}}{2}\log_2\left(\frac{e_{\text{raw}}}{2}\right)\right\}. \end{aligned} \tag{12}$$

From Eq. (10a), we conclude that the secret key rate of Scheme B as a function of e_{raw} is the same as that of the six-state scheme by one-way entanglement distillation using nondegenerate codes [12]. We do not believe that this is coincidental for these two very different schemes to have the same secret key rate. But we have no idea why.

The most error-tolerant PM-QKD scheme using N-dimensional qudits is the Chau05 scheme, which can tolerate up to $e_{\text{raw}} = 35.6\%$ using two-way classical communication for $N = 4$ [7]. To find the maximum tolerable error rate using one-way communication for the Chau05 scheme, we use the fact that the scheme effectively depolarizes the quantum error so that $e_{uv} = e_{u'v'}$ for all $(u,v),(u',v') \neq (0,0)$. Hence, Eq. (9) becomes

$$K = n + e_{00}\log_2 e_{00} + (1 - e_{00})\log_2\left(\frac{1 - e_{00}}{N^2 - 1}\right). \tag{13}$$

When $N = 4$, $K = 0$ at $e_{00} = 0.710$. Thus, the Chau05 scheme using one-way entanglement distillation can tolerate up to $(1 - e_{00})N/(N^2 - 1) \times (N/2)/(N - 1) = 5.1\%$ bit error rate for $N = 4$. By the same analysis, the Chau05 scheme using one-way entanglement distillation can tolerate up to 2.5% bit error rate.

For the RRDPS scheme using N-dimensional qudits with one-way privacy amplification, the secret key rate is given by [8]

$$R_{\text{RRDPS}} = \frac{1}{\log_2 N}\left\{1 - h_2\left(\frac{1}{N - 1}\right) - h_2(e_{\text{raw}})\right\}, \tag{14}$$

where $h_2(e) = -e\log_2 e - (1 - e)\log_2(1 - e)$. (Note that the extra $1/\log_2 N$ factor, which does not appear in Ref. [8], converts the number of bits to the number of dits in the raw key.) That is to say, it can tolerate up to a bit error rate of 1.0% and 8.2% for $N = 4$ and 8, respectively.

These findings are summarized in Fig. 2 and Table I. They show that, for both $N = 4$ and 8, the error-tolerant capability of Schemes B and C using one-way classical communication is better than the Chau05 [7] and the RRDPS [8] schemes. Table I also shows the secret key rate in the noiseless situation. In this situation, and for $N = 4$, the secret key rate of Scheme B is the same as that of the six-state scheme and is much higher than those of the Chau05 [7] and the RRDPS [8] schemes but lower than the BB84 [2]. All in all, we conclude that in terms of the secret key rate in the noiseless limit and the maximum tolerable provably secure bit error rate of the raw key using one-way entanglement distillation, both Schemes B and C can be ranked among the best all-rounded PM-QKD schemes for $N = 4$. Therefore, from Fig. 2, when restricted to one-way entanglement distillation, the most economical way for Alice and Bob to share their secret key is to use the BB84 in case the channel noise is low (when $e_{\text{raw}} \lesssim 9\%$) and either the six-state scheme or Scheme B with $N = 4$ if the channel noise is high (when $9\% \lesssim e_{\text{raw}} \lesssim 12\%$) provided that errors and losses in the labs of Alice and Bob are negligibly small.

For actual experimental setup, we have already pointed out that the state preparation of Schemes B and C is the same as that of the Chau15 scheme in Ref. [3]. For Scheme B, the measurement is more complicated than in Ref. [3] for the present scheme requires complete measurement. The measurement can either be done by active or passive basis selection; the latter case can be done by adapting the method used by Muller *et al.* in Ref. [20] using $(N - 1)N$ photon detectors, which is barely feasible though not very economical for $N = 4$ due to the large number of detectors required. Whereas for Scheme C, the measurement can be done in exactly the same way as in the Chau15 scheme [3], which can be directly adapted from the measurement part of various RRDPS experiments [21–23]. It is instructive to carry out actual experiments using Schemes B and C and compare their performances with that of the six-state scheme, and we are going to do so.

ACKNOWLEDGMENTS

This work is supported in part by the RGC Grant 17304716 of the HKSAR Government. We would like to thank Tieqiao Huang and H.-K. Lo for their discussions.

[1] See, for example, V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009), and references cited therein.

[2] C. H. Bennett and G. Brassard, in *Proceedings IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179, reprinted with corrections in Theo. Comp. Sci. **560**, 7 (2014).

[3] H. F. Chau, Phys. Rev. A **92**, 062324 (2015).

[4] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).

[5] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).

[6] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[7] H. F. Chau, IEEE Trans. Inf. Theory **51**, 1451 (2005).

[8] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature (London) **509**, 475 (2014).

[9] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[10] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).

[11] S. Lin and D. J. Costello Jr., in *Error Control Coding*, 2nd ed. (Prentice Hall, Upper Saddle River, 2004), Chap. 2.2–2.6.

[12] H.-K. Lo, Quantum Inf. Comput. **1**, 81 (2001).

[13] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).

[14] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).

[15] A. M. Steane, Proc. R. Soc. London A **452**, 2551 (1996).

[16] E. M. Rains, IEEE Trans. Inf. Theory **45**, 1827 (1999).

[17] A. Ashikhmin and E. Knill, IEEE Trans. Inf. Theory **47**, 3065 (2001).

[18] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in *Theory Of Cryptography: Second Theory Of Cryptography Conference, TCC2005*, edited by J. Killian (Springer, Berlin, 2005), pp. 386–406.

[19] R. Renner and R. König, in *Theory Of Cryptography: Second Theory Of Cryptography Conference, TCC2005*, edited by J. Killian (Springer, Berlin, 2005), pp. 407–425.

[20] A. Muller, J. Breguet, and N. Gisin, Europhys. Lett. **23**, 383 (1993).

[21] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Nature Photonics **9**, 827 (2015).

[22] S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, H.-W. Li, L.-J. Zhang, Z. Zhou, G.-C. Guo, and Z.-F. Han, Nature Photonics **9**, 832 (2015).

[23] Y.-H. Li, Y. Cao, H. Dai, J. Lin, Z. Zhang, W. Chen, Y. Xu, J.-Y. Guan, S.-K. Liao, J. Yin, Q. Zhang, X. Ma, C.-Z. Peng, and J.-W. Pan, Phys. Rev. A **93**, 030302(R) (2016).