Quantum private states are the states that represent some amount of perfect secure key. A simple symmetry of any generalised private quantum state (i.e., the states that represent perfect key but not fully random) is provided and extended on Devetak-Winter so called ccq (classical-classical-quantum) and cqq (classical-quantum-quantum) lower bound on secure key. This symmetry is used to develop a practical method of estimating the Alice measurement that is optimal from the perspective of single shot Devetak-Winter lower bound on secure key. The method is particularly good when the noise does not break the symmetry of the state with respect to the lower bound formula. It suggests a general paradigm for quick estimation of quantum communication rates under the symmetry of a given resource like state and/or channel.

I. INTRODUCTION

Entanglement is considered as a resource in quantum communication and computing. It has many intriguing properties that make in some cases quantum physics predictions drastically different from classical ones (see [1]). Any BB84 type protocol [2] is formally equivalent to some version of entangled based protocol of the type E91 [3]. On the level of uncorrelated sources Bennett et al. pointed out this fact on specific scheme [4] which was later naturally extended to a quantum privacy amplification QPA [5] based entanglement distillation protocol [6]. The general intrinsic connection between BB84 secret key generation and possibility of maximal entanglement distillation from correlated sources of noisy entanglement was provided explicitly by elegant error correction type analysis [7] which in particular illuminated this aspect hidden in previous proofs. However the fundamental intuition behind the BB84 secret key generation - entanglement distillation equivalence is already present in the case of uncorrelated source for which QPA protocol works. The latter is a protocol that distills maximally entangled states out of a mixed states in a well defined way. In QPA it is eavesdropper that is representing the noise and the distillation procedure is aimed at remove the correlations with eavesdropper in the process that produces a pure output state - maximally entangled state that is a source of perfect key. It seemed that this QPA is necessary to get privacy. However there exists nondistillable entanglement called bound entanglement [8] for which by the very definition QPA in its original form can not work. It turns out that there is another possibility of distilling secret key by distilling private states [9] that are generalisations of maximally entangled states - they provide secret key under the measurement in a fixed basis on some part of the system. The measurement basis may be unique and that is what makes the private states more general form maximally entangled ones for which there are infinite many pairs of local bases that provide secure key. The distillation of private states allow to provide secret key form bound entanglement (see [9]) showing in particular a possibility of drastic separation between amount of pure entanglement that can be distilled from a quantum state (called distillable entanglement and denoted by D) and amount of secret key that can be distilled from the same state (called distillable secret key and denoted by K). Recently the separation $D < K$ was experimentally demonstrated together with the illustration how inefficient may be the original entanglement distillation based scheme, if compared with p-bit based protocols [10].

In this article we present the new symmetry of the states with perfect secure key called generalized private states, which states that in the most popular Devetak-Winter protocol secret key rate is invariant in both scenarios of CCQ and CQQ type if the measurement bases, chosen in a wrong way, are rotated around the axis corresponding to the secure basis by any angle. Then we use this symmetry to propose a new method of searching the optimal basis, which allows to obtain optimal amount of distillable key with respect to the Devetak-Winter secret key rate, in the case when a state possessing this symmetry was rotated by an unknown angle. We investigate the influence of various qubit channels on the result of the method and show that the proposed method is an optimal one as long as a channel is bistochastic. Finally we derive the error estimation of numerical implementation of the procedure and show examples of the results.

II. A USEFUL SYMMETRY OF THE GENERALIZED PRIVATE STATES

According to [11] any state containing perfectly secure key corresponds to a pure state shared by three parties Alice, Bob and Eve. Unlike the eavesdropper subsystem E with a Hilbert space $H_E$ the subsystems of Alice and Bob
are composite and correspond to the tensor products of Hilbert spaces $\mathcal{H}_A \otimes \mathcal{H}_A'$ and $\mathcal{H}_B \otimes \mathcal{H}_B'$ respectively. We call the subsystem corresponding to the pair $A,B$ the key part since this is the part that is used for key generation by local von Neumann measurements while the pair $A'B'$ is called the shield part since it is in a sense responsible for protecting the key. The above structure allows to write explicitly the pure state of the three parties which represents a perfectly secure random a perfectly secure random statistics.

Before proving some new property let us remind that the so called CQQ state with respect to the basis $|q\rangle$ present here. Before proving some new property let us remind that the so called CQQ state with respect to the basis $|q\rangle$ present here. Before proving some new property let us remind that the so called CQQ state with respect to the basis $|q\rangle$ present here. Before proving some new property let us remind that the so called CQQ state with respect to the basis $|q\rangle$ present here.

We have a natural definition of the key rates in one-way protocols obtained by measuring the state first in some basis since after performing the local von Neumann measurements in that basis Alice and Bob share the correlated statistics. The above structure allows to write explicitly the pure state of the three parties which represents a perfectly secure random a perfectly secure random statistics.
B. General symmetry rule and its simple application

In what follows we shall use the notation $\hat{U}(X) = UXU^\dagger$ and $\hat{M}(\{P_k\})(X) = \sum_k P_k XP_k$ with a projectors $P_k = P(e_k) = |e_k\rangle\langle e_k|$ for any orthonormal basis $\{e_k\}$. We have a simple

*Observation.* Consider a function $f$ defined on any CQ state on the composite system $XY$

$$\sigma_{XY}^{CQ} = \sum_k P_k \otimes \sigma_k$$

Assume that the function $f$ is invariant under some subgroup $R_X$ of unitary operations $R_X \in R_X$ on the system $X$ ie.

$$\forall R_X \in R_X f(\hat{R}_X \otimes I_Y(\sigma_{XY}^{CQ})) = f(\sigma_{XY}^{CQ})$$

Given any state $\rho_{XY}$ which is invariant in an analogous way

$$\forall R_X \in R_X \hat{R}_X \otimes I_Y(\rho_{XY}) = \rho_{XY}$$

we have the following identity

$$f([\hat{M}_X(\{\hat{R}_X(P_k)\}) \otimes I_Y](\rho_{XY})) = f([\hat{M}_X(\{P_k\}) \otimes I_Y](\rho_{XY}))$$

for all $R_X \in R_X$ and all $\{P_k\}$ constructed from any orthonormal bases $\{e_k\}$.

*Proof.* It is obvious to see that ,,internal'' $\hat{R}_X$ is absorbed by the $QQ$ state $\rho_{XY}$ while the external conjugated one $\hat{R}_X$ is absorbed by the invariance of the function $f$.

We have immediate conclusion:

*Conclusion.* The functions $\{4\}$ and $\{5\}$, if calculated on a given generalized private state $\{2\}$, are invariant under the rotations $\hat{R}_A \otimes I_{BE}$ and $\hat{R}_A \otimes \hat{R}_B \otimes I_E$ respectively where $R_A, R_B$ are any unitary operations which are diagonal in the local bases $|i\rangle_A, |j\rangle_B$ forming a secure basis of the states $\{2\}$.

*Proof.* The role of the pair of the subsystems $\{X,Y\}$ is played by $\{A, BE\}$ or $\{AB, E\}$ respectively and the role of the subgroup are all the unitary operations diagonal in the bases described in the conclusion.

C. Consequences

In the case, when the key part dimension $d = 2$, this feature can be interpreted graphically. Let us consider CQQ case. Then Alice can choose two angles $(\theta, \varphi)$ to determine her measurement basis using the eigenvectors of the $\sigma_n$ operator

$$|e_0(\theta, \varphi)\rangle = \left[ \cos \frac{\theta}{2} e^{i\varphi} \sin \frac{\theta}{2} \right], |e_1(\theta, \varphi)\rangle = \left[ \sin \frac{\theta}{2} e^{-i\varphi} \cos \frac{\theta}{2} \right].$$

We define the function $K_D(\theta, \varphi) = K_D^{DW}(\rho_{\text{priv}}^{C(\theta, \varphi)QQ})$. Here superscript $C(\theta, \varphi)$ denotes that to calculate CQQ state base vectors determined by angles $(\theta, \varphi)$ were used. In spherical coordinate system, in which $|e_0(0,0)\rangle, |e_1(0,0)\rangle$ coincide with the base vectors used in $\{2\}$ the function $K_D(\theta, \varphi)$ is $\varphi$ independent, i.e. becomes function only of $\theta$ angle.

III. PROCEDURE

As follows from the previous section, points on the sphere$^{[10]}$ possessing the same value of $K_D$ establish a circle, whose center is located at intersection of $Z$ axis and the sphere. Moreover, each circle has a center in the same point (all circles are concentric). At this point value of $K_D$ is maximal. Using facts presented in Subsection II.C one is able to find such angles $\theta_{\text{Max}}, \varphi_{\text{Max}}$, for which the measurement in basis given by $^{[10]}$ will lead to the maximal value of $K_D$, without a priori knowledge of this basis or rotations by which the state was changed. Suppose that the original ideal state was rotated by unknown transformation $U_A \otimes I_{B' A'}$ which eventually changed its optimal measurement basis on Alice side from $\{|0\rangle_A, |1\rangle_A\}$ to $\{|0\rangle_n, |1\rangle_n\}$ where we define $\hat{n} = O\hat{z}$ as:

$$|0\rangle_n \langle 0\rangle_n = U|0\rangle \langle 0\rangle |U^\dagger = \frac{1}{2}(I + (O\hat{z})\hat{\sigma})$$

$$|1\rangle_n \langle 1\rangle_n = U|1\rangle \langle 1\rangle |U^\dagger = \frac{1}{2}(I - (O\hat{z})\hat{\sigma}).$$

(11)
The procedure is as follows.

1. First one chooses arbitrary values of angles $\theta_0$, $\varphi_0$ and establishes two base vectors $|e_0 (\theta_0, \varphi_0)\rangle$ and $|e_1 (\theta_0, \varphi_0)\rangle$. This basis is used to perform measurement and to obtain value of $K_D (\theta_0, \varphi_0) = K_{D0}$.

2. Then one changes the value of $\theta_0$ to $\theta_1$ and creates a set of base vectors $\{ |e_0 (\theta_1, \varphi_i)\rangle, |e_1 (\theta_1, \varphi_i)\rangle \}_{i=1}^{N}$. Vectors from this set differ in the value of $\varphi_i$ angle by arbitrary constant factor $\frac{2\pi}{N}$ so that $0 \leq \varphi_i < 2\pi$. One can ascribe each vector from the set to a corresponding point on the sphere. These points lay on a circle, whose centre is located at the point ascribed to vector $|e_0 (\theta_0, \varphi_0)\rangle$.

3. Subsequently, using the vectors from the set, the measurements are performed and for each pair of vectors $|e_0 (\theta_1, \varphi_i)\rangle, |e_1 (\theta_1, \varphi_i)\rangle$ the value of $K_{D1i}$ is calculated. A set of values $K_{D,N} = \{ K_{D1}, \ldots, K_{DN} \}$ is created. The aim of these measurements is to find two points laying on a chosen circle, characterized by values of $\varphi_i$ angle, for which value of $K_{D1i}$ is equal to earlier calculated value $K_{D0}$. It is not difficult to see that it is always possible to achieve this purpose when we assume continuity of $\varphi$ (or arbitrary small resolution in $\varphi_i$). According Subsection [II C] because the sphere is covered with circles with the same value of $K_D$, any other circle laying on the sphere can have 0, 1, 2 or infinity intersection points. Thus it is always possible to find such values of $\theta_0, \theta_1$, which ensure that points with the same value of $K_D$ are found. Just as for a plane, three points on the sphere are enough to unambiguously determine the circle. The radius and the centre of the circle are found solving the system of equations:

$$d(\theta_{Max}, \varphi_{Max}, \theta_0, \varphi_0) = R$$
$$d(\theta_{Max}, \varphi_{Max}, \theta_1, \varphi_1) = R$$
$$d(\theta_{Max}, \varphi_{Max}, \theta_1, \varphi_2) = R,$$

where $d$ is spherical distance defined as [13]:

$$d = \arccos (\mathbf{P} \cdot \mathbf{Q}) ,$$

here $\mathbf{P}, \mathbf{Q}$ are two points on the sphere characterized by angles $\theta_i, \varphi_i$ and $\theta_j, \varphi_j$, respectively. In therms of Cartesian coordinates ($x = \sin \theta \cos \varphi, y = \sin \theta \sin \varphi$ and $z = \cos \theta$) expression (15) is of a form:

$$d(\theta_i, \varphi_i, \theta_j, \varphi_j) =$$
$$= \arccos (\sin \theta_i \sin \theta_j \cos (\varphi_i - \varphi_j) + \cos \theta_i \cos \theta_j).$$

According to Subsection [II C] centre of the circle determined in this way is associated with the basis (characterized by angles $\theta_{Max}, \varphi_{Max}$), in which $K_D (\theta, \varphi)$ has maximal value. Fig. [I] presents main ideas of the proposed procedure.

The proposed procedure can be slightly modified. Finding two points with value of $K_{D1}$ exactly equal $K_{D0}$ can cause a problem and such solution is not a practical one. To overcome this difficulty, instead of finding two points with the same value of $K_D$, one finds points $K_{D1}, K_{D2}$ from the set $K_{D,N}$, for which the values of $K_{D1}, K_{D2}$ are the closest to the $K_{D0}$ i.e. for which $\Delta K_{D1} = K_{D0} - K_{D1}$ and $\Delta K_{D2} = K_{D0} - K_{D2}$ are minimal. Subsequently the interpolating function $I_{\{K_{D,N}\}} (\theta, \varphi)$ from the set $K_{D,N}$ is created. To construct the interpolation function Hermite polynomials of a required order are used. Thus one can write for $i = \{1, 2\}$:

$$K_{D0} =$$
$$= K_{D1} + \Delta K_{D1} =$$
$$= K_D (\theta_1, \varphi_i) + \frac{\partial I_{\{K_{D,N}\}} (\theta_1, \varphi)}{\partial \varphi} \bigg|_{\varphi = \varphi_i} \Delta \varphi_i$$
$$+ \frac{\partial^2 I_{\{K_{D,N}\}} (\theta_1, \varphi)}{\partial \varphi^2} \bigg|_{\varphi = \varphi_i} \Delta \varphi_i^2 =$$

$$= I_{\{K_{D,N}\}} (\theta_1, \varphi_i) + \frac{\partial I_{\{K_{D,N}\}} (\theta_1, \varphi)}{\partial \varphi} \bigg|_{\varphi = \varphi_i} \Delta \varphi_i$$
$$+ \frac{\partial^2 I_{\{K_{D,N}\}} (\theta_1, \varphi)}{\partial \varphi^2} \bigg|_{\varphi = \varphi_i} \Delta \varphi_i^2 ,$$

(17)
where we use the fact that $I_{(K,D,N)} (\theta_i, \varphi_i) = K_{Di}$ (i.e. the interpolation function reproduces the values of $K_{Di}$ from the set $K_{D,N}$ in the probe points). One solves equation $\{17\}$ for $\Delta \varphi_i$, $i \in \{1, 2\}$. In general, equation $\{17\}$ can have two different solutions. However, in such a case one chooses smaller $\Delta \varphi_1$ and $\Delta \varphi_2$ (because equation $\{17\}$ is Taylor expansion of function $I_{(K,D,N)} (\theta, \varphi)$ near $\varphi = \varphi_i$). By solving modified systems of equations:

$$d(\theta_{Max}, \varphi_{Max}, \theta_0, \varphi_0) = R \quad \text{(18)}$$
$$d(\theta_{Max}, \varphi_{Max}, \theta_1, \varphi_1 + \Delta \varphi_1) = R \quad \text{(19)}$$
$$d(\theta_{Max}, \varphi_{Max}, \theta_1, \varphi_2 + \Delta \varphi_2) = R, \quad \text{(20)}$$

one obtains values of $\theta_{Max}, \varphi_{Max}$.

The proposed approach enables to find the basis optimizing the value of $K_D$ by performing only local measurements.

**IV. ERROR ESTIMATION**

Due to approximation (finite sum) and possible numerical errors, it is never possible to solve $\{17\}$ exactly. As a result angles $\theta'_i, \varphi'_i$ will not lead to the maximal value of distillable key. In this section the estimation of this error is provided. Let us denote (see Fig. 2):

$$\hat{\varphi}_1 = \varphi_1 + \Delta \varphi_1 = \varphi'_1 + \Delta \varphi'_1$$
$$\hat{\varphi}_2 = \varphi_2 + \Delta \varphi_2 = \varphi'_2 + \Delta \varphi'_2$$
$$\theta_M + \Delta \theta_M = \theta'_M$$
$$\varphi_M + \Delta \varphi_M = \varphi'_M. \quad \text{(21)}$$

Without loss of generality, we can arrange $\hat{\varphi}_1, \hat{\varphi}_2$ so that $\hat{\varphi}_1 > \hat{\varphi}_2$. Spherical distance between points characterized by angles $(\theta_i, \varphi_i)$, $(\theta_j, \varphi_j)$ is given by $\{15\}$. We assume that $(\theta_i, \varphi_i) = (0, 0)$, so

$$\arccos [\cos \theta'_M] = R \quad \text{(22)}$$
$$\arccos [\sin \theta_1 \sin \theta'_M \cos (\hat{\varphi}_1 - \varphi'_M) + \cos \theta_1 \cos \theta'_M] = R \quad \text{(23)}$$
$$\arccos [\sin \theta_1 \sin \theta'_M \cos (\hat{\varphi}_2 - \varphi'_M) + \cos \theta_1 \cos \theta'_M] = R. \quad \text{(24)}$$

Combining $\{23\}$ and $\{24\}$ we get:

$$\cos (\hat{\varphi}_1 - \varphi'_M) = \cos (\hat{\varphi}_2 - \varphi'_M). \quad \text{(25)}$$

Because $\hat{\varphi}_1 \neq \hat{\varphi}_2$ and $\varphi'_M \in (0, 2\pi)$ there are two possibilities: $\hat{\varphi}_1 - \varphi'_M = -(\hat{\varphi}_2 - \varphi'_M)$ or $\hat{\varphi}_1 - \varphi'_M = - (\hat{\varphi}_2 - \varphi'_M - 2\pi)$. We set $\varphi'_M := \varphi'_M \bmod 2\pi$

$$\varphi'_M = \frac{\hat{\varphi}_1 + \hat{\varphi}_2}{2}$$
$$\varphi_M + \Delta \varphi_M = \frac{\varphi_1 + \varphi_2}{2} + \frac{\Delta \varphi_1 + \Delta \varphi_2}{2}, \quad \text{(26)}$$

so $\Delta \varphi_M = \frac{\Delta \varphi_1 + \Delta \varphi_2}{2}$.

However, we know only $\varphi'_i$, $\Delta \varphi'_i$ but we can estimate (see Fig. 2) as $|\Delta \varphi_i| < \Delta \varphi - |\Delta \varphi'_i|$. As a result

$$\Delta \varphi_M < \frac{2\Delta \varphi - |\Delta \varphi'_1| - |\Delta \varphi'_2|}{2}. \quad \text{(27)}$$

Combining equations $\{22\}$ and $\{23\}$

$$\cot \theta'_M = \cot \frac{\theta_i}{2} \cos (\hat{\varphi}_1 - \varphi'_M). \quad \text{(28)}$$

As a consequence of the equality

$$\cos (\hat{\varphi}_1 - \varphi'_M) = \cos \left(\varphi_1 + \Delta \varphi_1 - \frac{\varphi_1 + \Delta \varphi_1 + \varphi_2 + \Delta \varphi_2}{2}\right) = \cos \left(\frac{\varphi_1 + \Delta \varphi_1 - \varphi_2 - \Delta \varphi_2}{2}\right), \quad \text{(29)}$$
we obtain the following relation
\[
\theta_M = \arccot \left[ \cot \frac{\theta_1}{2} \cos \left( \frac{\varphi_1 - \varphi_2}{2} \right) \right]
\]  
(30)
and
\[
\theta_M + \Delta \theta'_M = \arccot \left[ \cot \frac{\theta_1}{2} \cos (\tilde{\varphi}_1 - \varphi'_M) \right].
\]  
(31)
In order to obtain the upper bound on \(\Delta \theta'_M\) we have to find \(\tilde{\theta}_M\) - an lower bound on \(\theta_M\). Then the following relation holds:
\[
\tilde{\theta}_M + \Delta \theta'_M < \theta_M + \Delta \theta'_M = \arccot \left[ \cot \frac{\theta_1}{2} \cos (\tilde{\varphi}_1 - \varphi'_M) \right],
\]  
(32)
so \(\Delta \theta'_M < \arccot \left[ \cot \frac{\theta_1}{2} \cos (\tilde{\varphi}_1 - \varphi'_M) \right] - \theta_M\). We have to estimate the difference \(\varphi_1 - \varphi_2\) using known quantities \(\tilde{\varphi}_1, \tilde{\varphi}_2\). There are two different possibilities: in the first one \(\varphi_1 - \varphi_2 < \pi\) whereas in the second \(\varphi_1 - \varphi_2 > \pi\). Let us consider the first one. Because \(\arccot x \in (-\frac{\pi}{2}, \frac{\pi}{2})\) is a decreasing function for \(x \in (-\infty, 0) \cup (0, \infty)\), in order to find \(\tilde{\theta}_M\) we have to increase \(\cos (\frac{\varphi_1 - \varphi_2}{2})\). For our purposes we shall assume the worst case, namely \(\varphi_1 < \varphi_1\) and \(\varphi_2 > \varphi_2\). Then \(\varphi_1 - \varphi_2 > \varphi_1 - \varphi_2\). From previous considerations the following relation holds: \(\varphi_1 + \Delta \varphi > \varphi_2 > \varphi_1 - \Delta \varphi\). As a result \(\varphi_1 - \varphi_2 + 2\Delta \varphi > \varphi_1 - \varphi_2 > \varphi_1 - \varphi_2\). Using this inequality we get
\[
\theta_M > \tilde{\theta}_M 1 = \arccot \left[ \cot \frac{\theta_1}{2} \cos \left( \frac{\varphi_1 - \varphi_2 + 2\Delta \varphi}{2} \right) \right].
\]  
(33)
If \(\varphi_1 - \varphi_2 > \pi\) the similar line of reasoning leads to
\[
\theta_M > \tilde{\theta}_M 2 = \arccot \left[ \cot \frac{\theta_1}{2} \cos \left( \frac{\varphi_1 - \varphi_2 - 2\Delta \varphi}{2} \right) \right].
\]  
(34)
Finally one gets
\[
\Delta \theta'_M < \arccot \left[ \cot \frac{\theta_1}{2} \cos (\tilde{\varphi}_1 - \varphi'_M) \right] - \tilde{\theta}_M, i = 1, 2
\]  
(35)
where \(\tilde{\theta}_M, i = 1, 2\) is given by (33) or (34). Using perturbed points \((\varphi_i, \tilde{\varphi}_i)\) one obtains the point \((\theta_M + \Delta \theta_M, \varphi_M + \Delta \varphi_M)\) which differ from the real point \((\theta_M, \varphi_M)\) by \((\Delta \theta_M, \Delta \varphi_M)\), where \(\Delta \theta_M, \Delta \varphi_M\) are given by (31) and (27). In the new coordinate system associated with the point \((\theta_M + \Delta \theta_M, \varphi_M + \Delta \varphi_M)\) the error is given by:
\[
\Delta \theta = \arccos \left[ \sin \theta'_M \sin (\theta'_M - \Delta \theta_M) \cos \Delta \varphi_M + \cos \theta'_M \cos (\theta'_M - \Delta \theta_M) \right].
\]  
(36)

V. CONDITIONS FOR INVARIANCE OF KEY RATE IN CASE OF LOCAL ACTION OF PAULI CHANNELS

According to [11], using appropriate unitary operation \(U = 1_A \otimes \sum_i |i\rangle \langle i| \otimes U^i_{AB}^{(i)}\) (called twisting) it is possible to write a particular private state as:
\[
\rho_{pri} = |\Psi_+\rangle \langle \Psi_+|_{AB} \otimes \sigma_{A'B'},
\]  
(37)
where \(|\Psi_+\rangle\) is one of the four Bell states \(|\Psi_{\pm}\rangle, |\phi_{\pm}\rangle\)
\[
|\Psi_{\pm}\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \quad |\phi_{\pm}\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}.
\]  
(38)
After sending (37) down the channel \(A \otimes I\) where \(A(\cdot) = \sum_i p_i K_i(\cdot) K_i^\dagger\) with \(K_i = \{I, \sigma_x, \sigma_y, \sigma_z\}\) (note that twisting commutes with the action of the channel) one obtains a state
\[
\tilde{\rho}_{pri} = (p_1 |\Psi_+\rangle \langle \Psi_+|_{AB} + p_4 |\Psi_-\rangle \langle \Psi_-|_{AB}) \\
+ (p_2 |\phi_+\rangle \langle \phi_+|_{AB} + p_3 |\phi_-\rangle \langle \phi_-|_{AB}) \otimes \sigma_{A'B'},
\]  
(39)
The purification of this state is given by

$$\left| \tilde{\Psi}_{\text{priv}} \right> = \left[ \frac{p_1}{\sqrt{2}} (|00\rangle_{AB} + |11\rangle_{AB}) |0\rangle_E \right. \\
\frac{p_3}{\sqrt{2}} (|00\rangle_{AB} - |11\rangle_{AB}) |1\rangle_E \\
\frac{p_2}{\sqrt{2}} (|01\rangle_{AB} + |10\rangle_{AB}) |2\rangle_E \\
\left. \frac{p_3}{\sqrt{2}} (|01\rangle_{AB} - |10\rangle_{AB}) |3\rangle_E \right] \otimes |\psi\rangle_{A'B'E},$$

where $E,E$ denote Eves’ subsystem. It follows from \[4\] that we can trace over subsystems A’E (due to additivity of Von Neumann entropy for tensor product states $K_{DW}^{B}$ is independent of subsystems A’E). In order to find the value of the key rate due to Devetak - Winter protocol \[4\] we calculate the cqq state using base vectors defined by \[10\]. The nonzero elements of the reduced AB matrix are given by

$$\begin{align*}
\frac{1}{2} a_{0000} &= \cos^2 \frac{\theta}{2} (p_1 + p_4) + \sin^2 \frac{\theta}{2} (p_2 + p_3) \\
\frac{1}{2} a_{0101} &= \sin^2 \frac{\theta}{2} (p_1 + p_4) + \cos^2 \frac{\theta}{2} (p_2 + p_3) \\
\frac{1}{2} a_{1010} &= \sin^2 \frac{\theta}{2} (p_1 + p_4) + \cos^2 \frac{\theta}{2} (p_2 + p_3) \\
\frac{1}{2} a_{1111} &= \cos^2 \frac{\theta}{2} (p_1 + p_4) + \sin^2 \frac{\theta}{2} (p_2 + p_3) \\
\frac{1}{2} a_{0001} &= a_{0100}^* = e^{i\varphi} \sin \frac{\theta}{2} \cos \frac{\theta}{2} (p_1 - p_4) + e^{-i\varphi} \sin \frac{\theta}{2} \cos \frac{\theta}{2} (p_2 - p_3) \\
\frac{1}{2} a_{1011} &= a_{1101}^* = e^{i\varphi} \sin \frac{\theta}{2} \cos \frac{\theta}{2} (p_4 - p_1) + e^{-i\varphi} \sin \frac{\theta}{2} \cos \frac{\theta}{2} (p_3 - p_2).
\end{align*}$$

As a result entropies of Alice and Bob are equal $S_A = S_B = 1$. The reduced AB matrix is block diagonal so its eigenvalues are

$$\begin{align*}
\lambda_{1,2} &= \frac{1}{4} \left( 1 + \sqrt{\cos^2 \theta (p_1 + p_4 - p_2 - p_3)^2} + \sin^2 \theta |e^{i\varphi} (p_1 - p_4) + e^{-i\varphi} (p_2 - p_3)|^2 \right) \\
\lambda_{3,4} &= \frac{1}{4} \left( 1 - \sqrt{\cos^2 \theta (p_1 + p_4 - p_2 - p_3)^2} + \sin^2 \theta |e^{i\varphi} (p_1 - p_4) + e^{-i\varphi} (p_2 - p_3)|^2 \right).
\end{align*}$$

As a consequence, $I_{A:B}$ will be independent of $\varphi$ angle if and only if $p_1 - p_2$ or $p_2 - p_3$. In order to minimize joint entropy $S_{A:B}$ one has to set $\theta = 0$ or $\theta = \frac{\pi}{2}$ depending on $\{p_1,p_2,p_4\}$ or $\{p_1,p_2,p_3\}$. Setting $\theta = 0$ will be optimal if $(p_1 + p_4 - 2p_2) > 0$ for $p_2 = p_3$ or $(p_2 + p_3 - 2p_1) > 0$ for $p_1 = p_4$, otherwise $\theta = \frac{\pi}{2}$. In order to show that $I_{A:E}$ is independent of $\varphi$ and let us consider a state resulting from the measurement performed on $E$ subsystem. This operation does not increase the value of $I_{A:E}$ which we denote as $I_{A:E}^M$ so we have $I_{A:E} \geq I_{A:E}^M$ and due to \[4\]

$$K_{DW}^{B} (\hat{\rho}_{\text{priv}}) = I_{A:B} - I_{A:E} \geq I_{A:B} - I_{A:E}^M.$$  

After measurement the reduced $AE$ matrix has following eigenvalues $\lambda_{1,2} = \frac{p_1}{2}$, $\lambda_{3,4} = \frac{p_2}{2}$, $\lambda_{5,6} = \frac{p_3}{2}$, $\lambda_{7,8} = \frac{p_4}{2}$ whereas the eigenvalues of $E$ matrix are given by $\lambda_1 = p_1$, $\lambda_2 = p_2$, $\lambda_3 = p_3$, $\lambda_4 = p_4$ so we obtain that $I_{A:E}$ is independent of $\theta$. As a result if $p_1 = p_4$ or $p_2 = p_3$ the distillable key will preserve its invariance and the proposed procedure will be valid.
VI. NUMERICAL RESULTS

In this section we provide some examples of the results obtained by implementing the above procedure numerically.

Rotated $\rho_{SWAP}$ state. - Consider a private state introduced in [9] and realized experimentally [12]

$$\rho_{SWAP} = \frac{1}{4} |\Psi_-\rangle\langle\Psi_-|_{AB} \otimes |\Psi_-\rangle\langle\Psi_-|_{A'B'} +$$

$$\frac{1}{4} |\Psi_+\rangle\langle\Psi_+|_{AB} \otimes I_{A'B'}$$

$$- \frac{1}{4} |\Psi_+\rangle\langle\Psi_+|_{AB} \otimes |\phi_\perp\rangle\langle\phi_\perp|_{A'B'}.$$  \hspace{1cm} (44)

This state was rotated and then the optimizing procedure was applied. The example of the results is shown in Fig. 3.

Depolarizing channel. - The procedure was checked using the rotated state $\tilde{\rho}_{SWAP} = \Lambda_A \otimes I_{BA'B'}$, where $\Lambda(\rho) = p\frac{1}{2} + (1 - p)\rho$. The example of the results is shown in Fig. 4.

Phase flip channel. - Another test was performed using the rotated $\tilde{\rho}_{SWAP} = \Lambda_A \otimes I_{BA'B'}$, where $\Lambda(\rho) = pp + (1 - p)\sigma_z \rho \sigma_z$. The example of the results is shown in Fig. 5.

Rotated mixture of $\rho_{SWAP}$ and $\rho_{MSWAP}$ states. - Another example of the private states is a state

$$\rho_{MSWAP} = \frac{1}{2} |\phi_\perp\rangle\langle\phi_\perp| \otimes \left( \frac{1}{2} |00\rangle\langle00| + |\Psi_+\rangle\langle\Psi_+| \right) +$$

$$+ \frac{1}{2} |\phi_\perp\rangle\langle\phi_\perp| \otimes \left( \frac{1}{2} |11\rangle\langle11| - |\Psi_-\rangle\langle\Psi_-| \right).$$  \hspace{1cm} (45)

This state plays a role in bound entangled secure key [11]. We checked the procedure using rotated mixture of two private states $\rho_{priv} = p\rho_{SWAP} + (1-p)\rho_{MSWAP}$ and the rotated $\tilde{\rho}_{SWAP} = \Lambda_A \otimes I_{BA'B'}$, where $\Lambda(\rho) = pp + (1 - p)\sigma_z \rho \sigma_z$. The example of the results is shown in Fig. 6.

Qubit channel with trigonometrical parametrisation. - Consider a channel given by the Kraus operators [15]

$$K_1 = \begin{bmatrix} \cos \frac{u}{2} \cos \frac{v}{2} \\ \sin \frac{u}{2} \sin \frac{v}{2} \end{bmatrix} I + \begin{bmatrix} \sin \frac{u}{2} \sin \frac{v}{2} \\ \cos \frac{u}{2} \cos \frac{v}{2} \end{bmatrix} \sigma_z$$

$$K_2 = \begin{bmatrix} \cos \frac{u}{2} \sin \frac{v}{2} \\ \sin \frac{u}{2} \cos \frac{v}{2} \end{bmatrix} \sigma_x - i \begin{bmatrix} \sin \frac{u}{2} \cos \frac{v}{2} \\ \cos \frac{u}{2} \sin \frac{v}{2} \end{bmatrix} \sigma_y$$ \hspace{1cm} (46)

which transforms the Bloch vector $\vec{r} = [r_x, r_y, r_z]^T$ of the state into $\vec{r}' = [\cos ur_x, \cos vr_y, \cos u \cos vr_z + \sin u \sin v]^T$. It follows from Section VII that in general this channel does not preserve the invariance of distillable key. In this case the procedure fails. The example of the results is shown in Fig. 7.

VII. CONCLUSIONS

In the present paper the new symmetry of the states with perfect secure key called generalized private states have been provided which says that the most popular Devetak-Winter protocol secret key rate is invariant in both scenarios of CCQ and CQQ type if the measurement bases, chosen in a wrong way, are rotated (in a sense of angular momentum) around the axis corresponding to the secure basis by any angle. The symmetry has a particularly good interpretation when seen on a sphere since then the wrong is any basis corresponding to $\hat{n}$ with an angle $\theta$ to the $\hat{z}$ axis (corresponding to the secure basis) while the symmetry rotation is just the rotation by the angle $\phi$ around the $\hat{z}$ axis. We have also proven that for the qubit key part the optimality of the $\hat{z}$ axis as the secure basis is preserved after the action of any bistochastic channel (i.e. the one represented by random Pauli rotations).

The symmetry of the ideal p-bit lead us to the heuristic scheme of estimation of the optimal axis (with respect to the Devetak-Winter secret key rate $K_{DW}$) which is valid for any state that has this type of symmetry of the key rate under the rotation around the optimal basis. Namely given the density matrix, may be even in a numerical form, instead of searching over all sphere Alice may perform the analysis of the key over a ring around some chosen axis $\hat{z}'$ on the sphere and guess the optimal measurement axis only on the data based on this ring.

The method generally has a „dualistic” character with respect to the channel action. If the Alice subsystem as the direction of the optimal axis unperturbed, than the results are good if the $\hat{z}'$ is chosen to be far form the (unknown) optimal one $\hat{z}$ while if there is a perturbation of the optimal direction $\hat{z}$ (in a sense of the shrinking of that direction on a Bloch sphere) then the closer is the chosen axis to the original one the result is better. Basing on the polynomial approximation of the key function on the chosen ring there is also the possibility of the derivation of the error bar.
FIG. 1: Local Alice’s sphere with two different coordinate systems. Z axis corresponds to $\theta_{\text{Max}}$, $\varphi_{\text{Max}}$ angles whereas $Z'$ to $\theta_0$, $\varphi_0$ angles. Black circle shows the path along which angle $\varphi$ changes. At the intersection point between Z axis and the sphere $K_D(\theta_{\text{Max}}, \varphi_{\text{Max}}) = K_D^{\text{Max}}$. The intersection point between $Z'$ axis and the sphere is denoted by $(\theta_0, \varphi_0)$. At this point $K_D(\theta_0, \varphi_0) = K_D^0$. Points with the same value of $K$ (laying on a circle, whose center is located at the point $K_D^0$) are denoted by $(\theta_1, \varphi_1)$ and $(\theta_1, \varphi_2)$. At the first point $K_D(\theta_1, \varphi_1) = K_D^1$, whereas at the second point $K_D(\theta_1, \varphi_2) = K_D^2$.

FIG. 2: Starting point for the procedure $(\theta_0, \varphi_0)$, in which $K(\theta_0, \varphi_0) = K_D^0$. Point $(\theta_1, \varphi_1)$, $K_D^0 = K(\theta_1, \varphi_1)$ is closest to the point $(\theta_0, \varphi_0)$ in the given set because $\Delta K_D^1 = |K_D^0 - K_D^1|$ is minimal (see text for details). Using the interpolation function one obtains that $K(\theta_1, \varphi_1 + \Delta \varphi_1) = K(\theta_0, \varphi_0)$ really holds. The case of the second point $(\theta_1, \varphi_2 + \Delta \varphi_2)$ is similar. The error of the procedure is given by (36).

of the procedure. The analysis of examples shows that the error bar in general bounds the actual value of the error made in the procedure.

We believe that the present method may be especially useful when the large sample of data are provided and quick estimation of optimal Alice measurement is needed.

Acknowledgments. We thank Ewa and Jędrzej Tuziemscy for help in preparation of Figures. Calculations were carried out at the Academic Computer Center in Gdańsk. This work was supported by 7th Framework Programme Future and Emerging Technologies project Q-ESSENCE.

[1] R. Horodecki, P. Horodecki, M. Horodecki and K. Horodecki, Rev. Mod. Phys. 81, 865 (2009).
[2] C. H. Bennett and G. Brassard, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing IEEE Computer Society, New York, 1984, pp. 175179.
[3] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[4] C. H. Bennett, G. Brassard, and N. D. Mermin, 1992, Phys. Rev. Lett. 68, 557 (1992).
[5] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. 77, 2818 (1996).
[6] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. 76, 722 (1996).
[7] P. W. Shor, J. Preskill, Phys. Rev. Lett. 85, 441 (2000)
[8] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. 80, 5239 (1998).
[9] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. 94, 160502 (2005).
[10] K. Dobek, M. Karpinski, R. Demkowicz-Dobrzański, K. Banaszek, P. Horodecki, Phys. Rev. Lett. 106, 030501 (2011).
[11] K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim IEEE Trans. Inf. Theory 55, 1898 (2009).
[12] K. Dobek, M. Karpinski, R. Demkowicz-Dobrzański, K. Banaszek, P. Horodecki Phys. Rev. Lett. 106, 030501 (2011).
[13] T. Rowland Spherical Distance. MathWorld–A Wolfram Web Resource, created by Eric W. Weisstein. http://mathworld.wolfram.com/SphericalDistance.html
[14] K. Horodecki, P. Pankowski, M. Horodecki, P. Horodecki IEEE Trans. Inf. Theory 54, 2621 (2008).
[15] M. B. Ruskai, S. Szarek, E. Werner Lin. Alg. Appl. 347, 159 (2002).
[16] Points on the sphere correspond to angles used in [10]. The term sphere should not be confused with the Bloch sphere of the state.
FIG. 3: The estimated error of the procedure (using formula (36)) - left plot, and the error of the procedure (absolute value of the difference between rotation angle and the angle calculated by the procedure $\Delta \theta = |\theta - \theta_{M'}|$) - right plot vs. the number of points $r=10n$ ($n=1$ denotes that 10 points were used) for the rotated $\rho_{SWAP}$ state. Rotation angle $\theta = \frac{\pi}{3}$. Different colors correspond to different choices of $\theta_1$ angle in (20): blue - $\theta_1 = 0.0025 \pi$, red - $\theta_1 = 0.005 \pi$, orange - $\theta_1 = 0.0075 \pi$, red - $\theta_1 = 0.01 \pi$. In agreement with (36), for all cases the estimated error of the procedure constitute an upper bound on the error. The error of the procedure is orders of magnitude smaller than its estimated value.

FIG. 4: The estimated error of the procedure (using formula (36)) - left plot and, the error of the procedure (absolute value of the difference between rotation angle and the angle calculated by the procedure $\Delta \theta = |\theta - \theta_{M'}|$) - right plot vs. the number of points $r=10n$ ($n=1$ denotes that 10 points were used) for the state $\tilde{\rho}_{SWAP} = \Lambda A \otimes I_{BA'B'}$, where $\Lambda (\rho) = p \rho + (1 - p) \sigma_z \rho \sigma_z$. Rotation angle $\theta = \frac{\pi}{4}$, $p = \frac{1}{10}$. Different colors correspond to different choices of $\theta_1$ angle in (20): blue - $\theta_1 = 0.0025 \pi$, red - $\theta_1 = 0.005 \pi$, orange - $\theta_1 = 0.0075 \pi$, red - $\theta_1 = 0.01 \pi$. In agreement with (36), for all cases the estimated error of the procedure constitute an upper bound on the error. The error of the procedure is orders of magnitude smaller than its estimated value.

FIG. 5: The estimated error of the procedure (using formula (36)) - left plot and the error of the procedure (absolute value of the difference between rotation angle and the angle calculated by the procedure $\Delta \theta = |\theta - \theta_{M'}|$) - right plot vs. the number of points $r=10n$ ($n=1$ denotes that 10 points were used) for the state $\tilde{\rho}_{SWAP} = \Lambda A \otimes I_{BA'B'}$, where $\Lambda (\rho) = p \rho + (1 - p) \sigma_z \rho \sigma_z$. Rotation angle $\theta = \frac{\pi}{7}$, $p = \frac{3}{10}$. Different colors correspond to different choices of $\theta_1$ angle in (20): blue - $\theta_1 = 0.0025 \pi$, red - $\theta_1 = 0.005 \pi$, orange - $\theta_1 = 0.0075 \pi$, red - $\theta_1 = 0.01 \pi$. In agreement with (36), for all cases the estimated error of the procedure constitute an upper bound on the error. The error of the procedure is orders of magnitude smaller than its estimated value.
FIG. 6: The estimated error of the procedure (using formula (36)) - left plot and the error of the procedure (absolute value of the difference between rotation angle and the angle calculated by the procedure $\Delta \theta = |\theta - \theta_{M'}|$) - right plot vs. the number of points $r=10n$ ($n=1$ denotes that 10 points were used) for the state $\rho_{\text{priv}} = p\rho_{\text{SWAP}} + (1-p)\rho_{\text{MSWAP}}$. Rotation angle $\theta = \frac{\pi}{8}$, $p = \frac{2}{5}$. Different colors correspond to different choices of $\theta_1$ angle in (20): blue - $\theta_1 = 0.0025 \pi$, red - $\theta_1 = 0.005 \pi$, orange - $\theta_1 = 0.0075 \pi$, red - $\theta_1 = 0.01 \pi$. In agreement with (36), for all cases the estimated error of the procedure constitute an upper bound on the error. The error of the procedure is orders of magnitude smaller than its estimated value.

FIG. 7: The estimated error of the procedure (using formula (36)) and the error of the procedure (absolute value of the difference between rotation angle and the angle calculated by the procedure $\Delta \theta = |\theta - \theta_{M'}|$) vs. the number of points $r=10n$ ($n=1$ denotes that 10 points were used) for the state $\rho_{\text{priv}} = (\Lambda A \otimes 1_{B'BA'})\rho_{\text{SWAP}}$, $\Lambda_A(\rho) = K_1^\dagger \rho K_1 + K_2^\dagger \rho K_2$ where $K_i$ are given by (46). Rotation angle $\theta = \frac{\pi}{8}$, $u=0.1 \pi$, $v=0.05 \pi$. Different colors correspond to different choices of $\theta_1$ angle in (20): blue - $\theta_1 = 0.0025 \pi$, red - $\theta_1 = 0.005 \pi$, orange - $\theta_1 = 0.0075 \pi$, red - $\theta_1 = 0.01 \pi$. As discussed in Sec. V in this case proposed estimation scheme is no longer valid. The error of the procedure can be greater than its estimated value.