Measurement-device-independent quantum private queries by rotation-invariant twisted photons

Sijia Sun^{1,*}, Yuguang Yang¹

¹College of Computer Science and Technology, Beijing University of Technology, 100124 Beijing, China

Abstract. Quantum private query is an important cryptography protocol aiming to protect both user's and database's privacy. However, to execute even the simplest quantum private queries, one must establish and maintain a shared reference frame. Here we propose a rotation-invariant Measurement-device-independent quantum private queries with hybrid encoding approach, combined polarization and transverse spatial modes to overcome the polarization misalignment associated with random rotations in long-distance transmission. The initial encoding and final decoding of information in our protocol can be conveniently performed in the polarization space. Furthermore, our hybrid encoding approach only needs to insert four q-plates in practical experiment and to overcome the polarization misalignment problem.

1 Introduction

A symmetrically private information retrieval protocol (SPIR) [1] allows a user say Alice to retrieve an element of a database held by a database provider, Bob, but does not want him to learn anything about the item Alice is interested in. Meanwhile, Alice cannot get other items except the one she wanted. A SPIR problem is a 1-out-of-N oblivious transfer (OT) [2] protocol essentially.

Classical solutions to the SPIR problem are generally based on some computational complexity theoretic assumption, which might be susceptible to the strong ability of quantum computation. The SPIR problem also has solutions in the quantum scenarios, like the quantum symmetrically private information retrieval (QSPIR), namely quantum private queries (QPQ) [3]. Unfortunately, Lo has proven that quantum mechanics alone cannot provide unconditionally secure perfect quantum oblivious transfer [4], this implies the impossibility of perfect quantum SPIR. It can be concluded from Lo's proof that if a quantum SPIR has perfect user privacy, then Alice can perform an attack to access the entire database without being detected.

A feasible workaround is to require that Alice can elicit sufficiently little content of the database, or at least cannot get the whole database in any way, meanwhile, Bob would be detected with nonzero probability if he tries to know Alice's retrieval address.

Giovannetti et al. proposed a novel cheat-sensitive QPQ protocol (GLM-protocol) [6], where the database is represented by a unitary operation and it is performed on the two coming query states. GLM protocol can guarantee perfect database security because Alice can obtain at most two elements even if she performs dishonest queries. Compared with previous schemes, GLM-protocol shows an exponential reduction in both communication and computational complexity. Furthermore, the security analysis and proof-of-principle experimental realization of GLM-protocol were done in refs. [7-8].

Though the GLM-protocol exhibit significant advantages in theory, it is difficult to implement because when large database is concerned the dimension of the oracle operation will be very high. To solve this problem, Jakobi et al. proposed an interesting strategy (J-protocol) [9] based on SARG04 protocol [10]. Using SARG04 protocol, an asymmetric key can be distributed between Alice and Bob, which is used to encrypt the whole database. Alice only knows few bits of the key, which ensures the database privacy. J-protocol can be easily generalized to large database.

Though the security of QKD has been rigorously proven based on the laws of quantum mechanics, owing to the imperfections in real-life implementations, a large amount of quantum hacking

* Corresponding author: sunsj_1@163.com

like detector side channel attacks[11] have been proposed. The QKD-based QPQ also suffer this attack.

Recently, measurement-device-independent quantum key distribution (MDI-QKD) that removes all detector side channel attacks has been proposed by Lo et al. [12]. In the protocol, Alice and Bob send signal pulses to a third party, who is supposed to perform local Bell state measurement and announce the results public, so that Alice and Bob can distill secret keys according to measurement results by operating their bits. Zhao et al. proposed measurement-device-independent QPQ which remove all the known and unknown detector side channels [13].

Practical QKD protocol proposed have in common the need for a shared reference frame between Alice and Bob, which requires the transmission of an infinite amount of information. A possible solution is encoding logical qubits in multi-qubit states with appropriate symmetry properties, so that the states are rotationally invariant [14]. However, detection and production multi-photon state is a technological challenge. A more efficient way to circumvent misalignments is provided by exploiting multiple degrees of freedom of single photons.

In this paper, we show that it is possible to encode logical qubits into single photons using polarization and transverse spatial modes. Just as the circular polarization states are eigenstates of the spin angular momentum(SAM), the helical-wavefront Laguerre-Gaussian modes eigenstates of the spin angular momentum(SAM), the helical-wavefront Laguerre-Gaussian modes are eigenmode of its orbital angular momentum(OAM). The SAM and first order OAM are defined with respect to the same reference frame, they suffer exactly the same transformation under coordinate rotation. Therefore, they constituting an ideal pair to carry rotationally invariant hybrid qubits. Inspired by the work of Zhao et al [13], we propose a rotation-invariant MDI-QPQ protocol, which do not need shared reference frame, overcome serious obstacles in the particular situations where the users are very far apart from each other. In particular, our method only needs to insert q-plates in transmittance procedure. This in turn means that encoding and decoding procedure in our protocol can be convenient performed in the polarization space, while the transmission is done in the rotation invariant hybrid space.

2 Rotation-invariant MDI-QPQ

In this section, we focus on the rotation-invariant MDI-QPQ system and primarily analyze logical qubits

encoding technique. The schematic of our protocol is shown in Fig. 1.

Fig. 1. Schematic diagram of rotation-invariant MDI-QPQ for the honest parties. The BS represents 50:50 beam splitter, and PBS stands for polarization beam splitter.

2.1. Logical qubit encoding

As circular polarization states are eigenstates of the spin angular momentum(SAM), the helical-wavefront Laguerre-Gaussian modes are eigenmodes of its orbital angular momentum(OAM). The SAM and first order OAM eigenstates suffer exactly the same transformation under coordinate rotation. Therefore, our logical qubit basis is defined by hybrid polarization-OAM single-photon states.

$$\begin{aligned} \{0,1\}^Z &= \{ |L\rangle_\pi |r\rangle_o, |R\rangle_\pi |l\rangle_o \} \\ \{0,1\}^X &= \{ \cos\theta |L\rangle_\pi |r\rangle_o + \sin\theta |R\rangle_\pi |l\rangle_o, \\ &\quad \sin\theta |L\rangle_\pi |r\rangle_o - \cos\theta |R\rangle_\pi |l\rangle_o \} \end{aligned} \quad (1)$$

subscript π denotes the polarization Hilbert space, subscript o denotes the OAM bidimensional subspace, arbitrary rotations around the propagation direction by any angle φ , circular polarization states and OAM eigenmodes acquire equivalent phase factors

$$|L/R\rangle_\pi \rightarrow e^{\mp i\varphi} |L/R\rangle_\pi, |l/r\rangle_o \rightarrow e^{\mp i\varphi} |l/r\rangle_o \quad (2)$$

As our logical qubit combinations with opposite handedness, the phase term cancel each other and the composite states remain intact. So our scheme is immune to all possible reference frame misalignments.

2.2 State encoder/decoder

After determining logical qubits, the next question is how to prepare them. A nature choice is q-plate[11] that can maps polarization qubit into qubits encoded in hybrid polarization-OAM states of the same photon. When a circularly polarized light beam traverses the q-plate, an $\pm 2q$ amount of OAM is transferred into the beam

$$(\alpha |R\rangle + \beta |L\rangle)_\pi |0\rangle_o \xrightarrow{\text{q-plate}} \alpha |L\rangle_\pi |-2q\rangle_o + \beta |R\rangle_\pi |+2q\rangle_o$$

(3)

$|L\rangle_\pi$ and $|R\rangle_\pi$ are eigenstates of SAM with eigenvalues $\hbar$ and $-\hbar$, since the subspace spanned by our logical qubit has zero total angular momentum along the propagation axis, the amount of OAM per photon should equal to $\hbar$ and $q = 0.5$, therefore light beam traverses the q-plate gives rise to the following transformations

$$|R\rangle_\pi |0\rangle_o \xrightarrow{\text{q-plate}} |L\rangle_\pi |r\rangle_o, |L\rangle_\pi |0\rangle_o \xrightarrow{\text{q-plate}} |R\rangle_\pi |l\rangle_o \quad (4)$$

$|l\rangle_o$ and $|r\rangle_o$ are eigenstates of OAM with eigenvalues $\hbar$ and $-\hbar$. Before performing a partial BSM on the received pulses, a second q-plate transformed the rotation invariant hybrid states back in the original polarization states

$$\begin{aligned} |R\rangle_\pi |0\rangle_o &\xrightarrow{\text{q-plate}} |L\rangle_\pi |r\rangle_o \xrightarrow{\text{q-plate}} |R\rangle_\pi |0\rangle_o \\ |L\rangle_\pi |0\rangle_o &\xrightarrow{\text{q-plate}} |R\rangle_\pi |l\rangle_o \xrightarrow{\text{q-plate}} |L\rangle_\pi |0\rangle_o \end{aligned} \quad (5)$$

The superposition state transforms

$$\begin{aligned} |0_i^x\rangle_\pi |0\rangle_o &\xrightarrow{\text{q-plate}} \sin \theta_i |L\rangle_\pi |r\rangle_o + \cos \theta_i |R\rangle_\pi |l\rangle_o \\ &\xrightarrow{\text{q-plate}} \sin \theta_i |R\rangle_\pi |0\rangle_o + \cos \theta_i |L\rangle_\pi |0\rangle_o = |0_i^x\rangle_\pi |0\rangle_o \quad (6) \\ |1_i^x\rangle_\pi |0\rangle_o &\xrightarrow{\text{q-plate}} \sin \theta_i |R\rangle_\pi |l\rangle_o - \cos \theta_i |L\rangle_\pi |r\rangle_o \\ &\xrightarrow{\text{q-plate}} \sin \theta_i |L\rangle_\pi |0\rangle_o - \cos \theta_i |R\rangle_\pi |0\rangle_o = |1_i^x\rangle_\pi |0\rangle_o \end{aligned}$$

2.3 The protocol

(1) Bob prepares one of the four polarized states $|L\rangle$, $|R\rangle$ and $|0_b^x\rangle = \cos \theta_b |L\rangle + \sin \theta_b |R\rangle$, $|1_b^x\rangle = \sin \theta_b |L\rangle - \cos \theta_b |R\rangle$ randomly, where $\theta_b \in (0, \frac{\pi}{2})$ and can be adjusted to make the protocol have different degree of security. The basis firstly pass through a q-plate, then sends to Alice. The basis $|0_b^x\rangle, |1_b^x\rangle$ corresponds to the raw key bit, and the basis $|L\rangle, |R\rangle$ encodes the raw key bit 0.

(2) Alice prepares one of the four polarized states $|L\rangle, |R\rangle$ and $|0_a^x\rangle = \cos \theta_a |L\rangle + \sin \theta_a |R\rangle$, $|1_a^x\rangle = \sin \theta_a |L\rangle - \cos \theta_a |R\rangle$ randomly and independently of Bob, also pass through a q-plate. Before, she projects her and Bob's states into a Bell state another q-plate transforms the hybrid states back in the original polarization states. If the BSM does not output a Bell state, then Alice asks Bob to restart step(1) Otherwise, Alice records the measurement result. In fact, she needs to identify only the Bell state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, which means that the

BSM can be built with only linear optical elements. Theoretical probabilities of obtaining the projection $|\Psi^-\rangle$ for different combinations of the honest states are shown in Table 1. Repeat steps (1) and (2) until $k \times N$ successful BSMs are made, where k is a natural number determined by the security analysis and N is the number of database's bits.

(3) For each time Alice obtained a Bell state, Bob announces bit 0 to Alice if he has sent states $|0_b^x\rangle$ or $|L\rangle$, announces bit 1 if he has sent states $|1_b^x\rangle$ or $|R\rangle$.

(4) Alice decodes Bob's states to acquire the corresponding raw key bits. It can be done depending on her state and the bit Bob announces in step (3). For example, if Bob sends state $|0_b^x\rangle$ and declare bit 0, which mean may send $|0_b^x\rangle$ or $|L\rangle$, Alice can rule out $|L\rangle$ and conclude that the raw key is 0.

(5) certainly only if she prepared the state $|L\rangle$ according to Table 1, both the conclusive and inconclusive raw key are retained.

(6) length N , and add these substrings bitwise, obtaining the final key K with length N .

(7) Now, a raw key string with length $k \times N$ are shared between Bob and Alice, where Bob knows every bit value and Alice knows partially. Then, cuts the raw key into k substrings of length N , and add these substrings bitwise, obtaining the final key K with length N .

(8) Bob encrypts his database and Alice obtains the item she wanted with one of her known bits in K . In particular, suppose Alice knows the j th bit K_j and wants the i th bit of the database X_i . She declares the number $s = j - i$, then, Bob shifts K by s , and using the obtained key K' to encrypt his database in the manner of one-time pad. Thus X_i is encrypted by K_j and consequently can be correctly obtained by Alice when she gets the encrypted database.

2.4 Discussion

To make the protocol work correctly, it can be seen from Table 1 that the absolute value of the difference between θ_a and θ_b should satisfy $\Delta\theta = |\theta_a - \theta_b| = 0$ or $\frac{\pi}{2}$. We make an example to show how Alice obtains a conclusive raw key in the honest protocol. For $\Delta\theta = 0$, if Bob has sent state $|0_b^x\rangle$, after Alice records the measurement result, Bob announced bit 0, according to Table 1, Alice can identify Bob's state is $|0_b^x\rangle$, only if she has prepared state $|L\rangle$, and thus the raw key 0

with certainty. She will obtain an inconclusive result if she prepared states $|1_a^x\rangle$ or $|R\rangle$.

Table 1. Theoretical probability of obtaining $|\Psi^-\rangle$ in the honest protocol

probabilit y	$ 0_b^x\rangle$	$ 1_b^x\rangle$	$ L\rangle$	$ R\rangle$
$ 0_a^x\rangle$	$\frac{1}{2}\sin^2(\theta_b - \theta_a)$	$\frac{1}{2}\cos^2(\theta_b - \theta_a)$	$\frac{1}{2}\sin^2\theta_a$	$\frac{1}{2}\cos^2\theta_a$
$ 1_a^x\rangle$	$\frac{1}{2}\cos^2(\theta_b - \theta_a)$	$\frac{1}{2}\sin^2(\theta_b - \theta_a)$	$\frac{1}{2}\cos^2\theta_a$	$\frac{1}{2}\sin^2\theta_a$
$ L\rangle$	$\frac{1}{2}\sin^2\theta_b$	$\frac{1}{2}\cos^2\theta_b$	0	$\frac{1}{2}$
$ R\rangle$	$\frac{1}{2}\cos^2\theta_b$	$\frac{1}{2}\sin^2\theta_b$	$\frac{1}{2}$	0

As Alice selects the four states randomly, in the absence of noise, the probability that BSM yields the above conclusive raw key is $p_c = \frac{1}{2}\sin^2\theta_b$, for both

$\Delta\theta=0$ and $\frac{\pi}{2}$. After adding the substrings in step(5), Alice will on average know $\bar{n} = N(p_c)^k$ bits and the probability that she will know none query key is $P_0 = [1 - (p_c)^k]^N$, it implies that the correctness of our protocol is the same with refs.[4] in the noiseless channel. We can choose suitable k for different database size to keep both $\bar{n}$ and P_0 in a suitable level.

3 Security analysis

Now we consider the security of our protocol. To realize a secure QPQ protocol, two security requirements should be satisfied, that is, the database privacy and user privacy.

3.1 Database security

If Alice is dishonest and she wants to obtain more items in Bob's database, she has to try to obtain more key bits in the raw key. To attain this aim Alice can storing the received photons in quantum memories and performing the USD measurements after step (3) to distinguish which state Bob really sent. The success probability of this USD measurement is bounded by $1 - F(\rho_0, \rho_1)$, where $F(\rho_0, \rho_1)$ is the fidelity between the two states to be discriminated. In our protocol this probability is $p^{USD} = 1 - \langle 0_b^x | L \rangle = 1 - \sin\theta_b$. The relation between p_c and p^{USD} are shown in Fig.1, it can be seen

that Bob will obtain better database privacy when $\theta_b > \frac{\pi}{4}$.

Fig. 2. The probabilities of Alice acquiring a conclusive raw key in the honest protocol and in the USD attack in different for different θ_b .

Dishonest Alice can also perform joint measurement on the k qubits which contribute to an element of the final key. By this means she wants to obtain the bit value of the final key directly without distinguishing the individual bit values of the raw key. An example for this is Helstrom's minimal error-probability measurement, i.e., the measurement that distinguishes two quantum states with the highest information gain. To distinguish two equally likely quantum state ρ_0 and ρ_1 , the probability to guess the state correctly is bounded by $p_{guess} = 0.5 + 0.5 \times D(\rho_0, \rho_1)$, where $D(\rho_0, \rho_1)$ is the trace distance between ρ_0 and ρ_1 . In our protocol, therefore, Alice can correctly guess a final key bit with the probability at most $p_{guess} = 0.5 + 0.5 \times \sin^k\theta$. So the more substrings are added to generate the final key, the harder it is for her to guess the bit value.

To sum up, when $\theta_b > \frac{\pi}{4}$ and a large k is chosen in our protocol it exhibits a better performance in terms of the database security.

3.2 User security

In the following we briefly discuss the probability with which Bob can obtain the conclusiveness of any of Alice's bits in the raw key. Similar to the analysis in Ref.[10], instead of transmitting the honest states to Alice in step (1), Bob can get the conclusiveness of Alice's one bit with the optimal probability by sending the middle state $|0_b^x\rangle (|1_b^x\rangle)$ and announcing 1(0). here

$$\begin{aligned} |0_b^x\rangle &= \cos\frac{\theta_b}{2} |L\rangle + \sin\frac{\theta_b}{2} |R\rangle \\ |1_b^x\rangle &= \sin\frac{\theta_b}{2} |L\rangle - \cos\frac{\theta_b}{2} |R\rangle \end{aligned} \quad (7)$$

When $\Delta\theta = |\theta_a - \theta_b| = 0$, the theoretical probabilities for the middle states and Alice's honest states being projected into Bell state $|\Psi^-\rangle$ are shown in Table 2. Take the example that Bob sends

state $|0_b^x\rangle$ and announces bit 1. From Table 2 and 1, it can be seen that Alice will obtain a conclusive raw key if she prepares states $|1_a^x\rangle$ or $|R\rangle$. Because Alice prepares the states randomly, as shown in Table 2, the probability of obtaining a conclusive raw key in both cases is $p_{c_1}^{mid} = \cos^2\frac{\theta_b}{2}$. If Bob wants Alice to obtain an inconclusive raw key, he sends state $|0_b^x\rangle (|1_b^x\rangle)$ and announcing 0(1). Now, Alice will get a conclusive result with probability $p_{c_2}^{mid} = \sin^2\frac{\theta_b}{2}$.

Bob can increase or decrease the conclusiveness of Alice's raw key in the middle-state attack. Once Bob tries to gather more information on Alice's query item than the honest protocol, it will make him loss the information on the raw key bit value, Bob's final key is still not exactly the same with Alice's corresponding query key at last, which means that he may provide wrong answers. And it can be detected by Alice at a later time with a probability.

Table 2. Theoretical probability of obtaining $|\Psi^-\rangle$ with Bob's middle-state attack

probability y	$ 0_a^x\rangle$	$ 1_a^x\rangle$	$ L\rangle$	$ R\rangle$
$ 0_b^x\rangle$	$\frac{1}{2}\sin^2(\frac{\theta_b}{2} - \theta_a)$	$\frac{1}{2}\cos^2(\frac{\theta_b}{2} - \theta_a)$	$\frac{1}{2}\sin^2\frac{\theta_b}{2}$	$\frac{1}{2}\cos^2\frac{\theta_b}{2}$
$ 1_b^x\rangle$	$\frac{1}{2}\cos^2(\frac{\theta_b}{2} - \theta_a)$	$\frac{1}{2}\sin^2(\frac{\theta_b}{2} - \theta_a)$	$\frac{1}{2}\cos^2\frac{\theta_b}{2}$	$\frac{1}{2}\sin^2\frac{\theta_b}{2}$

4 Conclusions

We present a practical QKD-based QPQ system with hybrid qubits. A hybrid encoding approach combined polarization qubit with orbital angular momentum qubit is adopted to overcome the polarization misalignment associated with random rotations in long-distance quantum private queries. The initial encoding and final decoding of information in our MDI-QPQ implementation protocol can be conveniently performed in the polarization space, while the transmission is done in the rotation invariant hybrid space. Furthermore, our hybrid encoding approach only needs to insert four q-plates in practical experiment.

References

1. Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin, J COMPUT SYST SCI **60**, 592-629 (2000)
2. I. Kerenidis, R. De Wolf, Inform. Process. Lett. **90**, 109-114 (2004)
3. H. K Lo, Phys. Rev. A **56**, 1154-1162 (1997)
4. V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. Lett. **100**, 230502 (2008)
5. M. Jakobi, C. Simon, N. Gisin, J. D. Bancal, C. Branciard, N. Walenta, and H. Zbinden, Phys. Rev. A **83**, 022301 (2011)
6. V. Scarani, A. Acin, G. Ribordy and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004)
7. B. Qi, C.H.F. Fung, H. K Lo, and X. Ma, Quantum Inf. Comput. **7**, 73-82 (2007)
8. H. K Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012)
9. L. Y. Zhao, Z. Q. Yin, W. Chen, Y. J. Qian, C. M. Zhang, and G. C. Guo, Sci. Rep. **7** 39733 (2017)
10. Z. D. Walton, A. F. Abouraddy, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, Phys. Rev. Lett. **91**, 087901 (2003)
11. L. Marrucci, C. Manzo, and D. Paparo, Phys. Rev. Lett. **96**, 163905 (2006)