Experimental Quantum Communication without Shared Reference Frame

Teng-Yun Chen¹*, Jun Zhang¹*, J.-C. Boileau², Xian-Min Jin¹,
Bin Yang¹, Qiang Zhang¹,³, Tao Yang¹,³, R. Laflamme², and Jian-Wei Pan¹,³
¹ Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics,
University of Science and Technology of China, Hefei, Anhui 230026, China.
² Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada.
³ Physikalisches Institut, Universität Heidelberg, Philosophenweg 12, 69120 Heidelberg, Germany
(Dated: April 1, 2022)

We present an experimental realization of a robust quantum communication scheme [Phys. Rev.
Lett. 93, 0220501 (2004)] using pairs of photon entangled in polarization and time. The scheme
overcomes errors due to collective rotation of the polarization modes (for example, birefringence in
optical fiber or misalignment), is insensitive to phase’s fluctuation of the interferometer and does
not require precise timing. No shared reference frame is required except from the need to label the
different photons. We use this scheme to implement a robust variation of the Bennett-Brassard 1984
quantum key distribution protocol (BB84) over 1km of optical fiber. We conclude by discussing and
solving the unconditional security of our protocol.

PACS numbers: 03.67.Dd, 03.65.Ud, 03.67.Pp

Quantum cryptography [1], whose security is based on
the fundamental principles of quantum mechanics, is a
fast expanding field of quantum information both theo-
retically and experimentally [2]. Recently, many quan-
tum key distribution (QKD) experiments have been re-
alized through optical fiber and free space using weak-
coherent source or entangled photon pairs. The maxi-
mum distances of free space QKD using weak-coherent
source and entangled photons pairs. The maximum
distances of free space QKD using weak-coherent
source and entangled photons are 23.4km by Kurtsiefer
et al. [3] and 13km by Peng et al. [4], respectively. Their
aim was to try to validate the feasibility of quantum com-
munication with satellites. Despite some security flaws,
fiber-based QKD over 100km has been achieved [5].

Polarization and phase-time are most common cod-
ing methods to implement QKD. Although polarization
can be suitable for free space QKD, it is generally not
suitable for fiber-based QKD because of the time and
wavelength dependences of birefringence which will de-
polarize the photons. Experimentally, active feedback or
self-compensation could be applied to solve these prob-
lems [6], but it is efficient only when the thermal and
mechanical fluctuations are rather slow. A popular alter-
native to polarization coding is phase-time coding using
unbalanced interferometers [7, 8]. However, phase-time
coding can be very sensitive to the phase’s fluctuations
between the two arms of the interferometers and requires
thermal stability. Some ingenious tricks like two-way
communication [9] are insensitive to phase’s fluctuation,
but have themselves disadvantages like being incompati-
bly with perfect single photon sources and being sensitive
to backscattering light.

To overcome the problems mentioned above, Walton
et al. proposed a scheme based on decoherence-free sub-
space (DFS) which required encoding qubits using phase
and time entanglement between two photons [10]. Then
Boileau et al. [11] proposed a variation of that proto-
col that use a combination of time bins and polarization
modes for coding. These schemes are insensitive to
phase’s fluctuations of the interferometer and robust
against collective rotation induced by birefringence or
misalignment. In single photon QKD protocol, a pre-
cisely synchronized clock is necessary to reduce the time
window to minimize the contribution of dark counts.
However, it is not the case for coding schemes using pho-
ton pairs, because the photons simultaneously originating
from the pair can provide precise time references for each
other. The fact that no synchronized clock is necessary
could be useful if the arrival time of photon fluctuates.

The obvious disadvantages of two photon schemes are
that they are much more sensitive to photon loss and
seem much inefficient than the single photon schemes.
However, it would be possible to reduce the qubit losses
to a level comparable to single photon schemes by us-
ing post-selection, entanglement swapping and quantum
memory devices [12]. As a step forward in that direction,
we implemented a variation of the BB84 protocol based
on the robust scheme of Boileau et al. [11], and realized
an efficient quantum communication without any shared
reference frame.

Our experimental scheme is illustrated in Fig. 1
On Alice’s side, polarization-entangled photon pairs are
generated via type-II spontaneous parametric down-
conversion (SPDC) [13]. The two photons of each pair are
labelled by passing two arms with 1.8m length difference.
In the long arm, two Pockel cells (POC1 and POC2),
driven by high voltage pulse generators gated with ran-
dom number signal, are used to produce the four states
similar to that of BB84: |HV⟩ + |VH⟩, |HV⟩ − |VH⟩,
|HV⟩ + i|VH⟩ and |HV⟩ − i|VH⟩, where H and V stand
for horizontal and vertical polarization mode, respec-
tively.

The two entangled photons can be combined into the

*These authors contributed equally to this work.
same path in the beam-splitter BS1 with a probability of 1/4. Afterward, the vertically polarized photons are firstly tagged with a delay $T$ in an unbalanced interferometer composed of two polarizing beam-splitters (PBS1 and PBS2) with a 1.2m difference between the two pathes’ length. The POC3 is added to perform a random collective rotation of polarization before the photons are collected into the fiber coupler (FC1). Then, the photons are sent to Bob directly or through a 1 km single mode optical fiber. A polarization rotator (PR) is used to simulate the collective rotation noise. On Bob’s side, the received horizontally polarized photons are tagged with the same delay $T$. To make the two timing tags exactly the same, a right-angled prism (Delay in Fig. 1) is used to adjust the path length precisely.

Using notation introduced in Ref. [11] and supposing that the initial state was of the form $\alpha |HV\rangle + \beta |VH\rangle$, the resulting state can be written as:

\[
\begin{align*}
((\delta_1 + 1)/2)(\alpha |H_T'V_T'\rangle + \beta |V_T'H_T'\rangle) \\
+((\delta_1 - 1)/2)(\alpha |V_T'H_T'\rangle + \beta |H_T'T_T'\rangle) \\
+((\delta_2 + \delta_3)/2)(\alpha |H_T'H_T'\rangle + |H_T'T_T'\rangle) \\
+((\delta_2 - \delta_3)/2)(\alpha |V_T'H_T'\rangle + |V_T'T_T'\rangle),
\end{align*}
\]

where $|H\rangle$ and $|V\rangle$ represent Bob’s polarization basis frame which can be different from Alice’s one. The subscripts T and TT mean that the photon has been tagged once and twice, respectively. The $\delta_j$’s are parameters that depend directly on the collective rotation of the polarization mode. They satisfy the following relation: $|\delta_1|^2 + |\delta_2|^2 + |\delta_3|^2 = 1$. Giving the arrival time of the photons, the final state is projected to the original state with a probability $p_s = \|\delta_3 - 1\|^2$. The $p_s$ could be anything between 0 and 1. To make $p_s$ independent of the environment or any misalignment of the reference frame, Alice or Bob could apply a random unitary transformation $B^{s2}$ between the two tagging operations. If $B$ is chosen from the uniform distribution over $U(2)$, then $p_s$ is in average equal to $\frac{1}{2}$ whatever is the collective rotation. Because it’s difficult to realize random transformation $B$ over the whole $U(2)$ space experimentally, we simplify the experimental set-up by using only one POC (POC3 in Fig.1). Making it do nothing half of the time, and a bit-flip operation otherwise, $p_s$ could also average to a non-zero value, $\frac{1}{2} \leq p_s \leq \frac{3}{4}$.

The received photons are split at BS2. The two half-wave plates HW1 and HW2 are set such that they perform as Hadamard gates on the polarization. By switching POC4 such that it do nothing or act as a QWP at 90°, we can select a random measurement basis (either $\{|H_T'V_T'\rangle + |V_T'H_T'\rangle, |H_T'T_T'\rangle - |V_T'H_T'\rangle\}$ or the $\{|H_T'V_T'\rangle + i|V_T'H_T'\rangle, |H_T'T_T'\rangle - i|V_T'H_T'\rangle\}$). By post-selecting the cases where each of two photons exit from different outputs of BS2 and their arrival time difference is 6ns (which is related to the 1.8m time label), the states are differentiated according to their polarization (the same or different) [11]. The detection events within the 3ns coincident time window are recorded to generate quantum key bits.

For the measurement to succeed, it is crucial to observe two photons interference after the timing tags. It requires to match accurately the difference of the path’s lengths of the two interferometers by adjusting the prism on Bob’s side (see Fig. 1). The curve in Fig. 2 shows an interference fringe with a visibility of above 95%. The fact that interference is observed over a large length interval (of about one hundred micrometers) clearly implies that the interference is robust against the phase instability of the interferometers as claimed in Ref. [10, 11].

In order to demonstrate the robustness of the protocol in principle, we first use a 4m optical fiber to implement the QKD protocol. Approximately 12,000Hz polarization-entangled pairs are detected behind a interference filter (IF) of 1.6nm FWHM. The entangled photon pairs are transferred to one of the four states randomly and sent to Bob. Due to the photon losses in the BSs and the fiber connectors, only a maximum of 140Hz coincidences can be registered on Bob’s side after calibrating the PR. We then rotate the angle of the first QWP of the PR to simulate the degree of collective rotation noise. In the experiment, five settings are selected for particular angles of the QWP. The first setting corresponds to the case where there is no collective rotation and coincidence is maximal. The last setting corresponds to a collective bit-flip. The other settings are chosen via rotating the angle of QWP with equal intervals between the best and the worst settings. We investigated the change of error rates and coincidences under these conditions with or without random rotation implemented by POC3.

As shown in Fig.3, the coincidence without random ro-
The 2000 Hz single count rate of each detector and the accidental coincidence counts in function of the angle of the collective rotation with or without random rotations.

The QBER of each states was measured in 20 minutes without (a) or with random rotations (b). The average QBER over all states with and without the random rotations are compared in (c). In (d), we give the normalized coincidence counts in function of the angle of the collective rotation with or without random rotations.

The QBER measured under different collective rotations (as in Fig. 3) and with a 1km single mode fiber. The average QBER over all states with and without the random rotations are compared in (c). In (d), we give the normalized coincidence counts in function of the angle of the collective rotation with or without random rotations.

The average QBER over all states with and without the random rotations are compared in (c). In (d), we give the normalized coincidence counts in function of the angle of the collective rotation with or without random rotations.
can be estimated from the identity \( e^p \) and proof \[16\] bound Eve’s information after bit error correction since privacy amplification \[14, 15\] can be used for the measurement of \( p^S \) close to \( e^p \). Remark that the number of pairs required for the measurement of \( p^S \) is asymptotically negligible.

To obtain a secure key, it is necessary and sufficient to bound Eve information about the key after bit error correction since privacy amplification \[14, 13\] can be used to reduce asymptotically that information to zero with a key’s lost proportional to Eve’s information. For the qubits projected outside \( S \), Alice and Bob assume the worst case scenario and suppose that Eve has full information about the results corresponding to these states. For the qubits projected inside \( S \), Shor and Preskill’s proof \[10\] bound Eve’s information after bit error correction by \( H(e^x) \). Consequently, the secret key generation rate is at least \( p^S - H(e^x) - p^S H(e^x) \) of the conclusive results. Note that, \( H \) is the Shannon entropy, \( e^x \) and \( e^S_x \) are the bit error rate over all conclusive results and over the conclusive results that were projected inside \( S \), respectively. A conclusive result is defined as any measurement that gives a bit to the key before error correction and privacy amplification.

Since both \( e^x \) and \( p^S \) can be measured directly by using a sample of test bits, to estimate the secret key generation rate, Alice and Bob only need an upper bound for \( e^S_x \). \( e^S_x \) can be estimated from the identity \( e^S_x = p^S e^S_x + (1 - p^S) e^S_x \), where \( e^S_x \) is the error rate of the conclusive results corresponding to the states projected outside \( S \). As a consequence of Bobs random choice of \( \Phi \) for \( M_\Phi \) and the fact that the coefficients of the density matrix \( \rho \) corresponding to \( |V_1 V_1^\dagger\rangle \langle H' H'| \) and \( |H' H'| \langle V_1^{\dagger} V_1 | \) are zeros, \( e^S_x \) asymptotically. In the experiment, we measured \( p^S \) using the method explained above. In the case with \( 4 \) m fiber, \( p^S \) is measured to be \( 97\% \) and in the case with \( 1 \) km fiber \( p^S \) is \( 91\% \). With the help of random rotations, the \( e^S_x \)’s observed in both cases (see Figs.\[3\] and \[4\]) are sufficient to guarantee secure key distribution.

Any coherent attack from an eavesdropper was considered in our security analysis. However, we assumed perfect state preparation and measurements, and that Eve’s has no access whatsoever to Alice and Bob’s lab. For a more realistic security analysis, considerations as the ones treated in Ref. \[17\] \[18\] would be necessary.

In summary, we have realized one of the first efficient quantum communication protocols without shared spatial and reference frame including no time reference, except to label the qubits. It could be useful for free-space transmission in the case where the receiver and the sender are moving relative to each other. It could also be useful to avoid birefringence effect in optical fiber and would be a possible solution to the phase instability of interferometers. Our experiment is a first step toward more efficient robust quantum communication since it is only an example of a series of more complex quantum communication schemes exploiting the decoherence-free subsystem of the collective noise and time tags.\[19\]. We also showed the unconditional security of a robust quantum key distribution protocol based of BB84. We conclude with the remarks that technological advances of entangled photon sources and quantum memories would greatly enhance our results.

This work was supported by the CAS, the NNSFC, the NSERC and the PCSIRT. This work was also supported by the Alexander von Humboldt Foundation, the Marie Curie Excellence Grant of the EU and the government of Ontario.

---

[1] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp.175-179 (1984).
[2] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002).
[3] C. Kurtsiefer et. al., Nature (London) 419, 450 (2002).
[4] C.-Z. Peng et. al., Phys. Rev. Lett. 94, 150501 (2005).
[5] C. Gobby, Z. L. Yuan and A. J. Shields, Appl. Phys. Lett. 84, 3762 (2004); T. Kimura et. al., [quant-ph/0303104].
[6] J.D. Franson and B.C. Jacobs, Electron. Lett. 31, 232 (1995).
[7] C. H. Bennett, Phys. Rev. Lett. 68, 3121 (1992).
[8] R. Hughes, G. Morgan and C. Peterson, J. Mod. Opt. 47, 533 (2000); G. Ribordy et. al., ibid. 47, 517 (2000); W. Tittel, J. Brendel, H. Zbinden and N. Gisin, Phys. Rev. Lett. 84, 4737 (2000).
[9] A. Muller et. al., Appl. Phys. Lett. 70 793(1997); D. Stucki et. al., New J. Phys. 4, 41 (2002).
[10] Z.D. Walton et. al., Phys. Rev. Lett. 91, 087901 (2003).
[11] J.-C. Boileau, R. Laflamme, M. Laforest and C. R. Myers, Phys. Rev. Lett. 93, 220501 (2004).
[12] J.-C. Boileau, D. Poulin, K. Tamaki and R. Laflamme, to be published).
[13] P.G. Kwiat et. al., Phys. Rev. Lett. 75, 4337 (1995).
[14] C. H. Bennett, G. Brassard and J.-M. Robert, SIAM Journal on Computing, 17(2): 210, (1988).
[15] R. Renner and R. König, In Theory of Cryptography-TCC 2005, LNCS(Springer, Berlin, 2005), p.407.
[16] P. W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (2000).
[17] D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill, Quant. Info. and Comp. Vol.4, No. 5, 325 (2004).
[18] N. Gisin et. al., Phys. Rev. A 73, 022320 (2006).
[19] J. L. Ball and K. Banaszek, Open Syst. Inf. Dyn. 12, 121 (2005).