
Supplementary information

Experimental demonstration of memory-enhanced quantum communication

In the format provided by the authors and unedited

M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev & M. D. Lukin✉

SUPPLEMENTARY INFORMATION

I. THEORETICAL DESCRIPTION OF ASYNCHRONOUS BELL STATE MEASUREMENT

Here we give a theoretical description of how the sequence depicted in Fig. 3a corresponds to an asynchronous BSM between two photonic time-bin qubits. Below, we also describe how this enables the experimental observation of the violation of the Bell-CHSH inequality.

Due to the critical coupling of the nanocavity, the memory node only reflects photons when the SiV spin is in the state $|\uparrow\rangle$. The resulting correlations between the spin and the reflected photons can still be used to realize a BSM between two asynchronously arriving photonic time-bin qubits using an adaptation of the well known proposal of Duan and Kimble for entangling a pair of photons incident on an atom-cavity system [29]. As a result of the critical coupling, we only have access to two of the four Bell states at any time, with the inaccessible Bell states corresponding to photons being transmitted through the cavity (and thus lost from the detection path). Depending on whether there was an even or odd number of π -pulses on the spin between the arrival of the two heralded photons, we distinguish either the $\{|\Phi_{\pm}\rangle\}$ or $\{|\Psi_{\pm}\rangle\}$ states (defined below). For the sake of simplicity, we first describe the BSM for the case when the early time bin of Alice's and Bob's qubits both arrive after an even number of microwave π pulses after its initialization. Thereafter we generalize this result and describe the practical consequences for the quantum communication protocol.

The sequence begins with a $\pi/2$ microwave pulse, preparing the spin in the state $|\psi_i\rangle = (|\uparrow\rangle + |\downarrow\rangle)/\sqrt{2}$. In the absence of a photon at the device, the subsequent microwave π -pulses, which follow an XY8-N type pattern, decouple the spin from the environment and at the end of the sequence should preserve the spin state $|\psi_i\rangle$. However, reflection of Alice's photonic qubit $|A\rangle = (|e\rangle + e^{i\phi_1}|l\rangle)/\sqrt{2}$ from the device results in the entangled spin-photon state $|\psi_A\rangle = (|\uparrow e\rangle + e^{i\phi_1}|\downarrow l\rangle)/\sqrt{2}$. The full system is in the state

$$|\psi_A\rangle = \frac{|+x\rangle(|\uparrow\rangle + e^{i\phi_1}|\downarrow\rangle) + |-x\rangle(|\uparrow\rangle - e^{i\phi_1}|\downarrow\rangle)}{2}. \quad (1)$$

Regardless of the input photon state, there is equal probability to measure the reflected photon to be $|\pm x\rangle$. Thus, measuring the photon in X basis (through the TDI) does not reveal the initial photon state. After this measurement, the initial state of the photon $|A\rangle$ is teleported onto the spin: $|\psi_{m_1}\rangle = (|\uparrow\rangle + m_1 e^{i\phi_1}|\downarrow\rangle)/\sqrt{2}$, where $m_1 = \pm 1$ denotes the detection outcome of the TDI [19, 41]. The quantum state of Alice's photon is now stored in the spin state, which is preserved by the dynamical decoupling sequence.

Reflection of the second photon $|B\rangle = (|e\rangle + e^{i\phi_2}|l\rangle)/\sqrt{2}$ from Bob results in the spin-photon state $|\psi_{m_1,B}\rangle = (|\uparrow e\rangle + m_1 e^{i(\phi_1+\phi_2)}|\downarrow l\rangle)/\sqrt{2}$. This state now has a phase that depends on the initial states of both photons, enabling the photon-photon BSM measurements described below. Rewriting Bob's reflected photon in the X basis, the full system is in the state

$$|\psi_{m_1,B}\rangle = \frac{|+x\rangle(|\uparrow\rangle + m_1 e^{i(\phi_1+\phi_2)}|\downarrow\rangle) + |-x\rangle(|\uparrow\rangle - m_1 e^{i(\phi_1+\phi_2)}|\downarrow\rangle)}{2}. \quad (2)$$

The second measurement result m_2 once again contains no information about the initial state $|B\rangle$, yet heralds the final spin state $|\psi_{m_1,m_2}\rangle = (|\uparrow\rangle + m_1 m_2 e^{i(\phi_1+\phi_2)}|\downarrow\rangle)$ as described in the main text. When this state lies along the X axis of the Bloch sphere ($\phi_1 + \phi_2 = \{0, \pi\}$), the final result of the X basis measurement on the spin state m_3 has a deterministic outcome, dictated by all values of the parameters $\{\phi_1, \phi_2\}$ (known only to Alice and Bob) and $\{m_1, m_2\}$ (which are known to Charlie, but are completely random). Conversely, all information available to Charlie $\{m_1, m_2, m_3\}$ only contains information on the correlation between the photonic qubits, not on their individual states. The resulting truth table for different input states is given in Extended Data Table 3. For all input states, there is equal probability of measuring ± 1 for each individual measurement m_i . However, the overall parity of the three measurements $m_1 m_2 m_3$ depends on whether or not the input photons were the same, or opposite, for inputs $|A\rangle, |B\rangle \in |\pm x\rangle$ or $|\pm y\rangle$.

We now address the fact that the BSM distinguishes either between $\{|\Phi_{\pm}\rangle\}$ or $\{|\Psi_{\pm}\rangle\}$ if there was an even or odd number of microwave π pulses between incoming photons respectively. This effect arises because each π pulse in the dynamical decoupling sequence toggles an effective frame change: $Y \leftrightarrow -Y$. The impact on this frame change on the BSM can be seen by writing the pairs of Bell states $(|\Phi_{\pm}\rangle = (|ee\rangle \pm |ll\rangle)/\sqrt{2})$ and $(|\Psi_{\pm}\rangle = (|el\rangle \pm |le\rangle)/\sqrt{2})$ in the X and Y bases, where we have

$$|\Phi_{\pm}\rangle^{(X)} = (|+x\rangle|\pm x\rangle + |\mp x\rangle|\mp x\rangle)/\sqrt{2} \quad (3)$$

$$|\Phi_{\pm}\rangle^{(Y)} = (|+y\rangle|\mp y\rangle + |\pm y\rangle|\mp y\rangle)/\sqrt{2} \quad (4)$$

$$|\Psi_{\pm}\rangle^{(X)} = (|+x\rangle|\pm x\rangle - |\mp x\rangle|-x\rangle)/\sqrt{2} \quad (5)$$

$$|\Psi_{\pm}\rangle^{(Y)} = i(|+y\rangle|\pm y\rangle - |\mp y\rangle|-y\rangle)/\sqrt{2} \quad (6)$$

For X basis inputs, as seen by Eq. 3 and 5, switching between $\{|\Phi_{\pm}\rangle\}$ and $\{|\Psi_{\pm}\rangle\}$ measurements does not affect the inferred correlation between input photons. For Y basis inputs however, this does result in an effective bit flip in the correlation outcome (see Eq. 4 and 6). In practice, Alice and Bob can keep track of each Y photon sent and apply a bit flip accordingly, as long as they have the appropriate timing information about MW pulses applied by Charlie. If Charlie does not give them the appropriate information, this will result in an increased QBER which can be detected.

As an additional remark, this scheme also works for pairs of photons that are not both in the X or Y basis but still satisfy the condition $\phi_1 + \phi_2 = 0$. For example, $|a\rangle$ and $|b\rangle$ from Fig. 3b satisfy this condition. In this case, adequate correlations can still be inferred about the input photons, although they were sent in different bases.

Finally, we would like to note that this asynchronous scheme for performing a BSM between two pulses has an important advantage over the synchronous, linear-optical implementation. In the case where Alice and Bob use attenuated laser pulses to encode photonic qubits, which is by far the most technologically simple implementation, there is an inherent QBER of 25% for photons sent in the X and Y bases. This is because the linear-optical implementation relies on the pulses to overlap on a beamsplitter and interfere via the Hong-ou-Mandel effect, which has a finite visibility of 50% for coherent pulses [22]. Intuitively, this finite error arises from a fundamental inability to distinguish between detection outcomes where two individual single-photons arrived from Alice and Bob versus a two-photon component from either Alice or Bob in the synchronous scheme. In the asynchronous scheme, since pulses do not arrive at the same time from Alice and Bob, this error is mitigated. As a result, for ideal quantum memory operation and sufficiently attenuated laser pulses, the ultimate limit to the QBER is zero.

In order to perform a test of the Bell-CHSH inequality [14], we send input photons equally distributed from all states $\{|\pm x\rangle, |\pm y\rangle, |\pm a\rangle, |\pm b\rangle\}$ (Fig. 3b). We select for cases where two heralding events arise from input photons $\{A, B\} = \pm 1$ that are either 45° or 135° apart from one another. Conditioned on the parity outcome of the BSM (± 1), the Bell-CHSH inequality bounds the correlations between input photons as

$$S_{\pm} = |\langle A \cdot B \rangle_{xa} - \langle A \cdot B \rangle_{xb} - \langle A \cdot B \rangle_{ya} - \langle A \cdot B \rangle_{yb}| \leq 2, \quad (7)$$

where the subscripts denote the bases the photons were sent in. The values of each individual term in Eq. 7, denoted as “input correlations,” are plotted in Fig. 3d for positive and negative parity outcomes.

II. ANALYSIS OF QUANTUM COMMUNICATION EXPERIMENT.

For each experiment, we estimate the QBER averaged over all relevant basis combinations. This is equivalent to the QBER when the random bit string has all bases occurring with the same probability, (an unbiased and independent basis choice by Alice and Bob). We first note that the QBER for positive and negative parity announcements are not independent. We illustrate this for the example, that Alice and Bob send photons in the X basis. We denote the probability P that Alice sent qubit $|\psi\rangle$, Bob sent qubit $|\xi\rangle$ and the outcome of Charlie’s parity measurement is m_C , conditioned on the detection of a coincidence, as $P(\psi_A \cap \xi_B \cap m_C)$. We find for balanced inputs $P(+X_A \cap -X_B) = P(-X_A \cap +X_B)$ that $P(E_{XX}|+C) = P(E_{XX}|-C)$ with E_{XX} denoting the occurrence of a bit error in the sifted key of Alice and Bob. We thus find for the posterior probability L for the average QBER for XX coincidences

$$L(P(E_{XX})) = L(P(-C|+X_A \cap +X_B)) * L(P(+C|+X_A \cap -X_B)) \\ * L(P(+C|-X_A \cap +X_B)) * L(P(-C|-X_A \cap -X_B)). \quad (8)$$

Note that this expression is independent of the actual distribution of $P(\psi_A \cap \xi_B)$. Here, the posterior probability $L(P(+C|+X_A \cap -X_B))$ is based on the a binomial likelihood function $P(N_{m_C \cap \psi_A \cap \xi_B} | N_{\psi_A \cap \xi_B}, L)$, where N_C denotes the number of occurrences with condition C . Finally the posterior probability of the unbiased QBER is $L(P(E)) = L(P(E_{XX})) * L(P(E_{YY}))$. All values presented in the text and figures are maximum likelihood values with bounds given by the confidence interval of $\pm 34.1\%$ integrated posterior probability. Confidence levels towards a specific bound (for example, unconditional security [3]) are given by the integrated posterior probability up to the bound.

To get the ratio of the distilled distilled key rate with respect to the sifted key rate by (ideal) error correction and privacy amplification, we use the bounds given by difference in information by Alice and Bob with respect to a potential eavesdropper who performs individual attacks: $r_s = I(A, B) - I(A/B, E)^{\max}$ [4]. We use the full posterior probability

distribution of QBER (which accounts for statistical and systematic uncertainty in our estimate) to compute the error bar on r_s , and correspondingly, the error bars on the extracted distilled key rates plotted in Fig. 4.

