Iraqi J. Laser, Issue 2, Vol.18, pp.47-54 (2019)

IRAQI JOURNAL OF LASER

Optimizing the Secure Key Rate of a Single Sequential Quantum Repeater with Two Different Quantum Memories

Marwa A. Khaled [(1)] and **Jawad A. Hasan**[(2)]

(1) University of Baghdad, Baghdad, Iraq
(2) Institute of Laser for Postgraduate Studies, University of Baghdad, Baghdad, Iraq

(Received 11 September 2019; accepted 29 October 2019)

Abstract: Quantum channels enable the achievement of communication tasks inaccessible to their classical counterparts. The most famous example is the distribution of secret keys. Unfortunately, the rate of generation of the secret key by direct transmission is fundamentally limited by the distance. This limit can be overcome by the implementation of a quantum repeater. In order to boost the performance of the repeater, a quantum repeater based on cut-off with two different types of quantum memories is suggestd, which reduces the effect of decoherence during the storage of a quantum state.

Keywords: quantum repeater, quantum key distribution, quantum memories, quantum communication, quantum network

Introduction

The entanglement distribution over long distances is difficult because of unavoidable transmission losses and the no-cloning theorem [1] which is impossible to make an exact copy of an unknown quantum state, so the use of quantum repeaters [2] is one possible solution for this problem. Quantum repeater is a device that enhances the performance more than can be achieved by direct communication channel alone. This performance is measured differently for different tasks, such as secret key generation [3] or transmission of quantum information [4]. An original scheme is [2] based on dividing the whole communication distance into smaller segments connected by quantum repeaters to generate entanglement over those segments then applying the entanglement swapping operation at each intermediate node in a nested way, to establish long-distance entanglement. Many quantum repeater schemes require significant resources so they are not under experimental reach. However, the progress in recent experiments of the development of quantum memories [5, 6] has brought the realization of quantum repeaters closer than ever. One of the setups is that proposed in [7] which is based on single sequential quantum repeater located in the middle distance of the optical fiber that separates Alice and Bob and depends on the concept of cut off. The quantum repeater sends photons entangled with QM1 to Alice through the optical fiber. After many trials, Alice will receive one photon and performs a BB84 measurement [8]. After Alice has measured a photon and communicated her success to the quantum repeater, the quantum repeater tries to send a photon entangled with the QM2 to Bob through the optical fiber. If Bob does not receive a photon within some pre-defined amount of trials (the cut-off n*), the round will terminate and starts again. This is done to prevent the state in the QM1 from decoherence extremely. If Bob succeeds, the quantum repeater makes a Bell state measurement (BSM) on the two quantum memories. The round will complete performing

one a bit of the secret key. To make this protocol cut-off, the probability of Bob must be ≥ the probability of Alice [7], Since for probability of Alice > probability of Bob this will be equivalent to the state that the quantum repeater is positioned closer to Alice than Bob and this may reduce the overall distance which defeat the purpose of initiate the quantum repeater. When using the same type of quantum memory in quantum repeater, the probabilities of Alice and Bob (P_A, P_B) are equal .In order to increase the P_B, a quantum repeater based on different quantum memories is proposed. As shown in Figure (1). The QM1 is Nitrogen-Vacancy center (NV center) [9] which emits a single photon to Alice through an optical fiber with a transmissivity δ_A and QM2 is a trapped ion [10] embedded into high finesse cavities that emits a single photon to Bob through an optical fiber with a transmissivity δ_B. Alice and Bob each use a detector setup consisting of an optical element that can distinguish photonic qubit states in the X and Z bases (like a polarizing beam splitter for polarization qubits) and two threshold detectors that signals the absence or presence of photons. Alice and Bob choose the basis on which to measure. Each detector has dark count probability and detector efficiency. The secret key rate is used to estimate the performance of the quantum repeater and compared it with the key rate of direct transmission and R_{TGW}

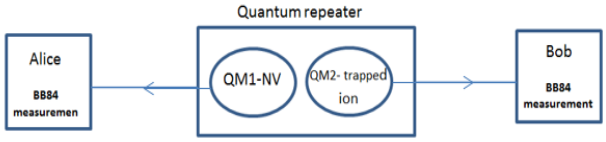


Figure (1):Schematic of the proposed protocol. (QM1) sends entangled photons to Alice, the other to Bob in sequantional manner. Once both parties successfully measure photons using BB84 measurements, a Bell measurement is performed on the QMs, if Bob doesn't receive the photon before n* the round will abort and start over again.

Methodology

The proposed protocol depends on using two different quantum memories in a central station (QR) placed between Alice and Bob, who wish to share a secret key via QKD. The quantum repeater is coupled to an optical fiber with low attenuation of 0.1419dB/km at wavelength of 1560nm [11] to achieve long distance, but Nitrogen-Vacancy center emits a photon with a wave length of 637 nm [12] and the trapped ion emits a photon with a wave length of 854 nm [13] so frequency conversion is needed to enhance the distance. Polarization encoding had been used to encode qubits. Both Alice and Bob have measurement apparatuses that allow them to measure incoming photons in X and Z bases in BB84. Then Bell state measurement can be applied between two different QMs. The scheme also needs coupling and high detection probability. Equation (1) is used to assign the performance of the scheme [14],

$$R = \frac{Y}{2}\left(1 - h(e_z) - h(e_x)\right) \quad \ldots\ldots (1)$$

Where (R) is the secret key rate, Y is the yield that is the probability Alice and Bob to detect a signal per round, h(e) is the binary entropy function where h (e) = -e $\log_2$(e) - (1 - e) $\log_2$ (1 - e) , e_x and e_z are the quantum bit error rates (QBERs) between Alice and Bob in the X and Z bases, and the factor of 1/2 comes from the fact that the protocol requires the use of two optical modes.

The yield Y is inversely proportional with the number of channels used [14],

$$Y = \frac{P_{bsm}}{E[\max(N_A; N_B)]} \quad \ldots\ldots (2)$$

P_{bsm}: the probability of Bell state measurement, NA is the number of photons that need to be sent to Alice so that her detector clicks once and NB is denoted by the number of photons that need to be sent to Bob so that his detector clicks once. The average number of channel uses required for both Alice and Bob's detectors to click is E [max (NA; NB)] where E is the expected value operator. The cut off increases the average number of channel uses because when Bob reaches n* trials, Alice and Bob abort the round and start over again; therefore the expected value is [7]:

$$E[\max(N_A, N_B)] \approx \begin{cases} \dfrac{1}{P_A(1-(1-P_B)^{n^*})} & \dfrac{1}{P_A} > n^* \\ \dfrac{1}{P_A}+\dfrac{1}{P_B}-\dfrac{1}{P_A+P_B-P_AP_B} & \dfrac{1}{P_A} \le n^* \end{cases} \quad \ldots..(3)$$

For $\frac{1}{P_A} \le n^*$ low losses regime is considered [14] where n* doesn't affect the secret key rate. When $\frac{1}{P_A} > n^*$is high loss regime where n* affects the key rate. So the high loss regime is used to study the effect of n* on key rate when using two different memories.

The probability of photon that is emitted from the NV center memory and detected by Alice can be denoted by P_A^* which is equal to [14]:

$$P_A^* = P_{em/A}\, Fc_A\; P_{c/A}\delta_A P_{det} \quad \ldots..(4)$$

Due to the dark count the probability of Alice will be:

$$P_{A,BB84} = 1-(1-P^*_A)(1-P_d)^2 \quad \ldots\ldots(5)$$

Also, the probability that a photon is emitted from the trapped ion and detected by Bob can be denoted by P_B^* which it is equal to:

$$P_B^* = P_{em/B}\, Fc_B\; P_{c/B}\delta_B P_{det} \quad \ldots\ldots.(6)$$

Due to the dark count, the probability of Bob detector to click will be:

$$P_{B,BB84} = 1-(1-P^*_B)(1-P_d)^2 \ldots\ldots(7)$$

$P_{c/A}$, $P_{c/B}$ is the probability of couplling quantum memory with the optical fiber for Alice side and Bob side respectively, Fc_A is the frequency conversion of the photon that is emited from NV center memmory, Fc_B is the frequency conversion of the photon that is emited from trapped ion memory, δ_A is the transmissivity of the optical fiber that connects Alice with QR = $e^{-L_A/L_{att}}$, δ_B is the transmissivity of the optical fiber that connects Bob with QR =$e^{-L_B/L_{att}}$ where the L_{att} equals to the attenuation length of the optical fiber , $P_{em/A}$ is the is the probability of generating a photon from NV center into the optical fiber, $P_{em/B}$ is the the probability of generating a photon from trapped ion into the optical fiber, P_{det} is the the probability of photons to produce a click in the detector and p_d is the is the probability of measuring a dark count.

The noise due to QMs must be introduced. The decoherence is modeled by a decay of the fidelity with the number of trials n*. This decoherence in QM is caused by two effects, the first one is the decoherence due to QM1 attempt to generate entangled state which can be quantified by a_0 and b_0, and the second is due to storage state until QM2 makes entangled photon with memory and sends the photon and gets a reply to confirm connection. This makes noise that can be quantified by a_1 and b_1. The quantum state ρ, that is exposed with those impacts given by the dephasing and depolarising channels with $\lambda_1 = (1+e^{-an})/2$ and $\lambda_2 = e^{-bn}$. Where $\lambda_1 = F_{prep}$ which is the dephasing parameter of preparation fidelity of memory photon entangled state and λ_2= is F_{gm} which is depolarizing parameter that describes the noise introduced by imperfect gates and measurements between the quantum memories the two parameters a and b are given by [7]:

$$a = a_0 + a_1\left(\frac{2n_rL_B}{c} + t_{prep}\right) \quad \ldots\ldots(8)$$

$$b = b_0 + b_1\left(\frac{2n_rL_B}{c} + t_{prep}\right) \quad \ldots\ldots(9)$$

The n_r is the refractive index of the optical fiber, L_B is the distance between the quantum repeater and Bob, c is the speed of light in the space, t_{prep} is the time to prepare for the emission of an entangled photon. The expression for the secret key fraction depends on the error rates in the X, Y and Z bases, which it is denoted by e_x, e_Y and e_z.

$$e_X = e_Y = e_{XY} = 0.5 - 0.5\, F_{gm} \propto_A \propto_B \left(2F_{prep}-1\right)^2 < e^{-(a+b)n} > \ldots(10)$$

$$e_Z = 0.5 - 0.5\, F_{gm} \propto_A \propto_B < e^{-bn} > \quad \ldots\ldots \quad (11)$$

Where α_A, α_B is depolarising parameters due to the noise that is achieved by the dark counts at Alice's or Bob's detector respectively

$$\propto_A = \frac{P^*{}_A(1-P_d)}{P_A} \ldots\ldots (12)$$

$$\propto_B = \frac{P^*{}_B(1-P_d)}{P_B} \ldots\ldots (13)$$

$$< e^{-cn} >= \frac{P_B\, e^{-c}}{1-(1-P_B)^{n^*}} \frac{1-(1-P_B)^{n^*} e^{-cn}}{1-(1-P_B)\, e^{-c}} \ldots\ldots (14)$$

Where $< e^{-cn} >$ is the average of the exponential e^{-cn} over a geometric distribution over the first n* trials. To assign the key rate of quantum repeater it must be compared with direct transmission benchmarks, because the quantum repeater is a source of additional losses. The first bench mark is called the Takeoka-Guha-Wilde (TGW) bound, which shows that the secret key rate of any QKD protocol performed over such a pure-loss bosonic channel cannot exceed this bound [15] :

$$R_{TGW} = log_2(\frac{1+\delta}{1-\delta})$$

Where $\delta = e^{-L/L_{att}}$

The second benchmark is related to the transmissivity when it is equal to transmissivity of fiber, filters and Alice's and Bob's apparatus, so it will become

$$\delta = \delta_{Fiber}\, P_{em} P_{det}\, P_c\, Fc$$

Results and discussion

The following parameters values were used for the results in this section. Python 3 is used for the programming of the calculations. The parameters are:

a_0: dephasing due to interaction (NV center) =1/2000 per attempt [16]
a_1: dephasing with time (NV center) =1/3 per second [17]
b_0: depolarisation due to interaction (NV center) =1/5000 per attempt [16]
b_1: depolarisation with time (NV center) =1/3 per second [17]
t_{prep}: memory-photon entanglement preparation time (trapped ion) = 210 μs [18]
$P_{em/A}$: probability of emission (NV center) = 0.49 [19]
$P_{c/A}$: probability of coupling (NV center) = 0.46 [20]
Fc_A: frequency conversion (NV center) = 0.3 [21]
Fc_B: frequency conversion (trapped ion) = 0.5 [22]
$p_{em/B}$: probability of emission (trapped ion) = 0.9 [23]
$P_{c/B}$: probability of coupling (trapped ion) = 0.4 [24]
P_{det}: detector efficiency = 0.8 [19]
P_d: probability of dark count =$3*10^{-7}$ [19]
L_0: attenuation length = 22km [19]
p_{bsm}: Bell state measurement success probability = 1 [25]
n_r: refractive index of the optical fibre =1.44 [26].

For these experimental data Figure (2) shows the secret key rate of quantum repeater based on NV center. When n*= 5, 50 the secret key rate increases and the distance crossers 400Km until n*is higher than 50 the losses increase and reduce the distance that the secret key rate can achieve. The decrease in distance and rate continue as long as n* increases.

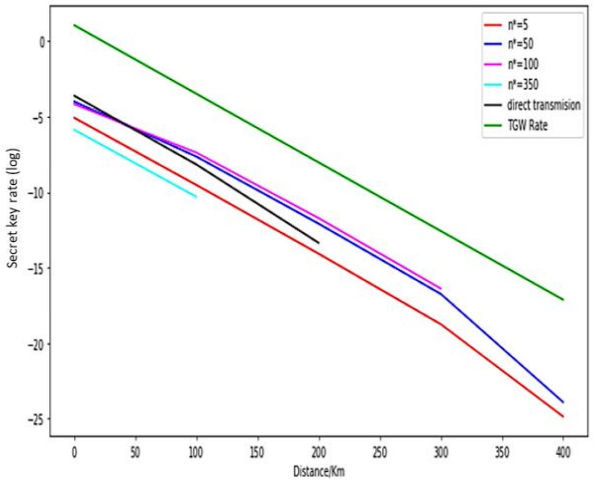


Figure (2): Secret key rate of quantum repeater based on NV center (probability of dark count= $3*10^{-7}$).

The probability of Bob may increase by shifting the quantum repeater towards Bob, so Figure (3) shows the effect of reducing the distance between Bob and the quantum repeater to increase the probability of detection. The secret key rate will decay rapidly when the quantum repeater is closer to Bob than Alice more than the secret key rate of the repeater when it is in middle of the distance that separate Alice and Bob at same n*.Figure (3) shows that the best secret key rate can be achieved when the quantum repeater position is in the middle of the distance.

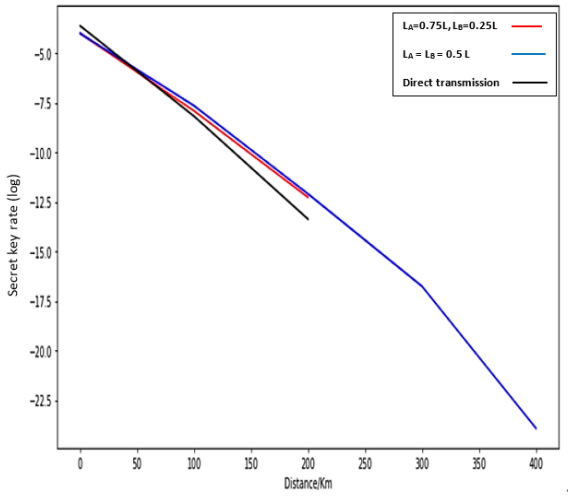


Fig. (3): Different positions of quantum repeater based on NV center quantum memory when n*=50

In order to increase Bob's probability ,the quantum repeater based on NV center -trapped ion quantum memories is proposed .Figure(4) shows the enhancement of the protocol because the P_B is greater than P_A this will make efficient secret key rate but still difficult to cross R_{TGW}.

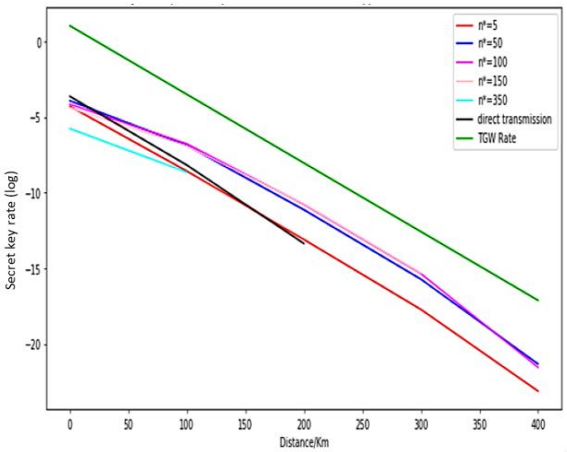


Fig.(4): Secret key rate of quantum repeater based on NV centre -trapped ion quantum memories (probability of dark count = $3*10^{-7}$).

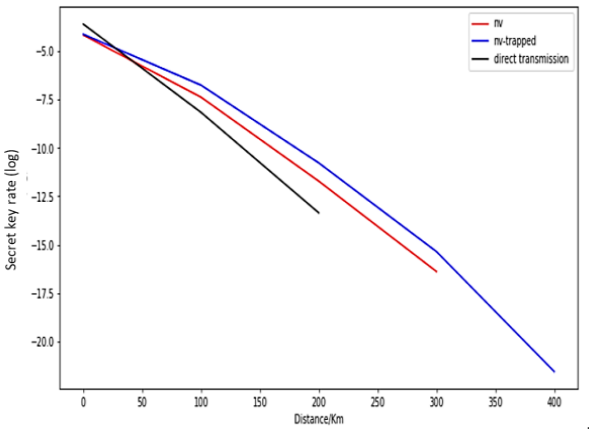


Fig. (5): Secret key rate of quantum repeater based on NV center and NV center - trapped ion when n*=100 (probability of dark count= $3*10^{-7}$).

Figure (5) shows achievement of higher secret key rate of quantum repeater based on NV center - trapped ion than a quantum repeater based on NV center because of high probability of emission and coupling of trapped ion quantum memory with the optical fiber.

In Figure (6) shows the use of trapped ion quantum memory effects on raising the probability of Bob more than the probability of Alice.

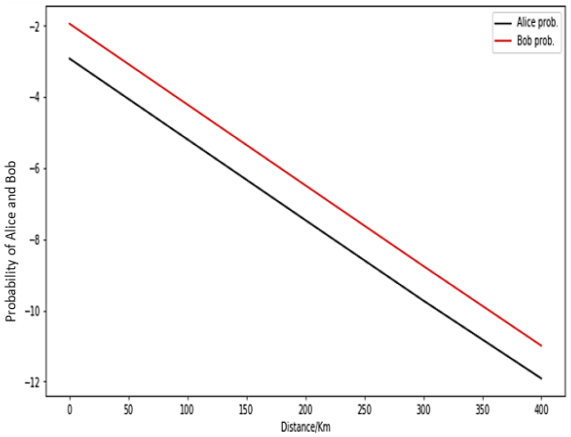


Fig. (6): Probability of Alice and Bob in quantum repeater based on NV center - trapped ion when n*=100 (probability of dark count= $3*10^{-7}$).

Figure (7): shows the secret key rate that can be achieved from quantum repeater based on NV center - trapped ion. A higher key rate is obtained compared to that obtained from quantum repeater based on NV center with the same number of n*, this is due to using different quantum memories when the distance that separates Alice and Bob equal to (100 Km),

(200 Km) as shown in (a), (b) respectively. This means the decrease in the n* that is needed to get a higher secret key rate.

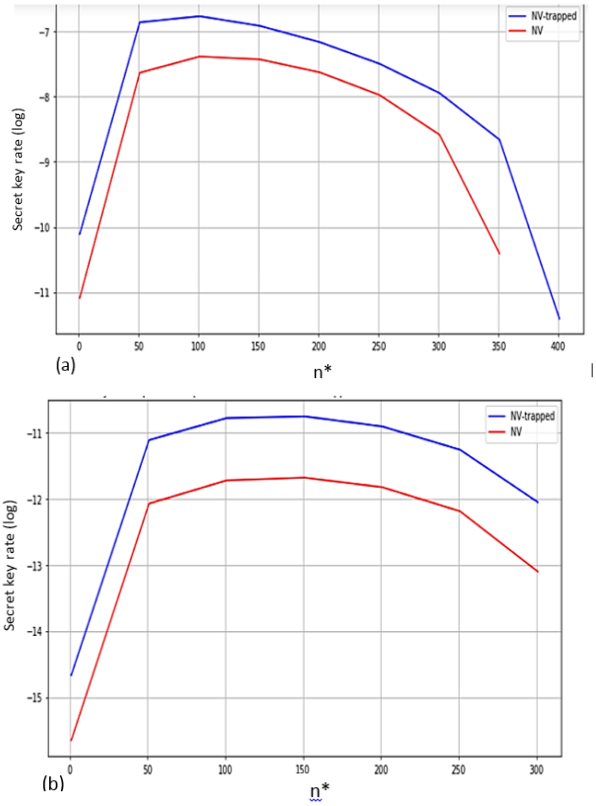
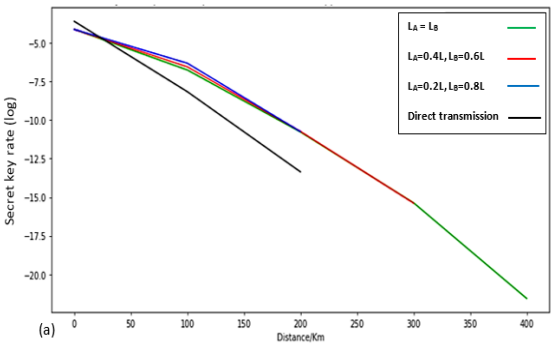


Fig. (7): The secret key rate of quantum repeater based on NV center - trapped ion when (a) L=100Km (b) L=200Km (probability of dark count= $3*10^{-7}$).

Figure (8) shows the effect of quantum repeater's position based on NV center - trapped ion on the secret key rate. When the position of quantum repeater is closer to Alice than Bob, the secret key rate with blue and red curves rapidly decrease to short distance more than the green curve which is the quantum repeater is in middle of the distance as shown in (a). In (b) the quantum repeater's position is closer to Bob than Alice, also the secret key rate with blue and red curves decrease to short distance more than the other, this shows that the best position of the quantum repeater is when L_A=L_B.



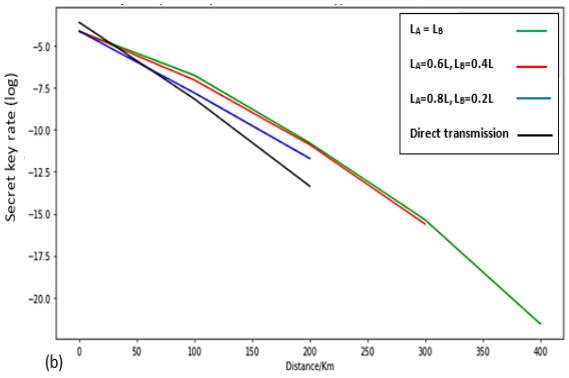


Fig. (8): (a) The positions of quantum repeater based on NV center - trapped ion closer to Alice than Bob (b) The positions of quantum repeater based on NV center - trapped ion closer to Bob than Alice (n*=100)

The dark count rate is another factor that affects the secret key rate as shown in Figure (9). At (a) the secret key rate reaches 500 Km when the probability of the dark count equal to 10^{-8}, but the secret key rate decreases rapidly when probability of the dark count is equal to 10^{-6} as shown in (b) because the dark count makes additional losses.

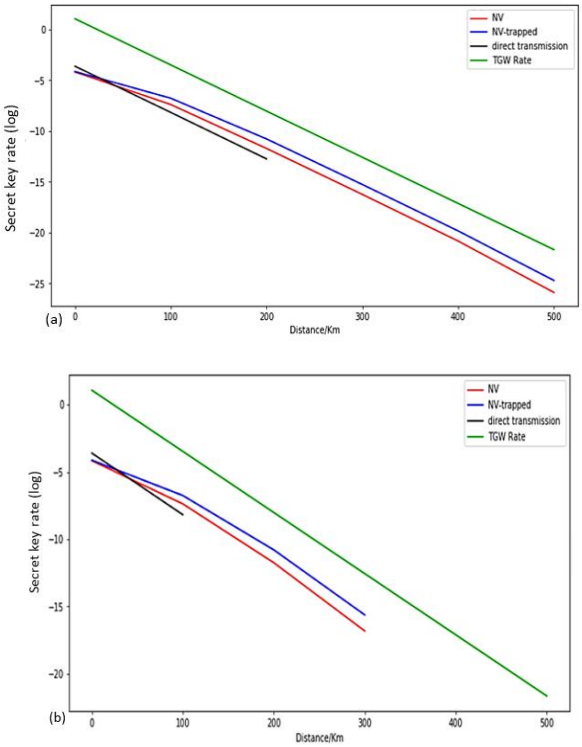


Fig. (9): Secret key rate of quantum repeater based on NV center and NV center –trapped ion at n*=100 when (a) probability of dark count = 10^{-8} (b) probability of the dark count = 10^{-6}

Conclusion

Alice and Bob exchange signals with a central station consisting of two different quantum memories, the Nitrogen-Vacancy center and trapped ion, which satisfy the condition ($P_B > P_A$). this increases the secret key rate and reduces the number of trails n* .Also, the scheme shows that the best position of the quantum repeater is in the middle of the distance that separates Alice and Bob to maximize the secret key rate with distances.

References:

[1] J. L. Park, Foundation of Physics,Vol.1, No.1, 23-33, (1970)
[2] H-J Briegel, W. Dür, J. I. Cirac and Zoller P., Phys. Rev. Lett. ,81, 5932 (2008)
[3] D. Gottesman, H-K Lo, N. L¨utkenhaus , J. Preskill., arXiv preprint quant-ph/0212066 (2004)
[4] I. Devetak, P. W. Shor., arXiv preprint quant-ph/0311131 (2008)
[5] M. P. Hedges, J. J. Longdell, Y. Li, M. J., Nature, vol.465, pages1052–1056 (2010)
[6] A. I. Lvovsky, B. C. Sanders, Nature Photonics, vol. 3, pages706–714 (2009)
[7] F. Rozpędek, K. Goodenough, J. Ribeiro, N. Kalb, V. C. Vivoli, A. Reiserer, R. Hanson, S. Wehner, D. Elkouss., Quantum Sci. Technol., vol. 3, no 3 (2018)
[8] S. Kuppam, arXiv preprint 1612.03706 (2016)
[9] C. Kurtsiefer, S. Mayer, P. Zarda, H. Weinfurter, Physical Review Letters, vol. 85, 290 (2000)
[10] T. P. Harty, D. T. C. Allcock, C. J. Ballance, L. Guidoni, H. A. Janacek, N. M. Linke, D. N. Stacey, D. M. Lucas., Physical Review Letters, PRL 113, 220501 (2014)
[11] Y. Tamura, H. Sakuma, K. Morita, M. Suzuki, Y. Yamamoto, K. Shimada, Y. Honma, K. Sohma, T. Fujii , T. Hasegawa. Lowest-ever , Optical Fiber Communication Conference (Washington, DC: Optical Society of America) pp Th5D–1 (2017)
[12] C. Simon, M. Afzelius, J. Appel, A. B. Giroday and et al, The European Physical Journal D, 58, 1–22 (2010)
[13] M. Bock, P. Eich, S. Kucera, M. Kreis, A. Lenhard, C. Becher, J. Eschner, Nature Communication, 9:1998(2018)
[14] D. Luong, L. Jiang, J. Kim, N. L¨utkenhaus, Applied Physics B, 122:96. (2016)
[15] M. Takeoka, S. Guha, M. M. Wilde, IEEE, 60, 4987 (2014)
[16] A. Reiserer, N. Kalb, M. S. Blok, K. J. M. Bemmelen, T. H. Taminiau Hanson R., Physical Review X 6, 021040 (2016)
[17] P. C. Maurer, G. Kucsko, C. Latta, L. Jiang, N. Y. Yao, S. D. Bennett and et al., Science ,vol. 336, Issue 6086, pp. 1283-1286 (2012)
[18] A. D. Pfister, M. Salz and et al., Appl. Phys. B, 122:89 (2016)
[19] B. Hensen, H. Bernien and et al., Nature, 15759 (2015)
[20] D. Riedel, I. Söllner, B. J. Shields, S. Starosielec, P. Appel, E. Neu, P. Maletinsky, R. J. Warburton, Physical Review X 7, 031040 (2017)
[21] S. Zaske and et al.,Phys. Rev. Lett.,109, 147404 (2012)
[22] T. Walker, K. Miyanishi, R. Ikuta and et al, Phys. Rev. Lett., 120, 203601(2018)
[23] B. Darqui ´ e, MP. Jones, J. Dingjan, J. Beugnon, S. Bergamini, Y. Sortais, G. Messin, A. Browaeys, P. Grangier, Science, 309, 5733, 454-456(2005)
[24] B. Brandstätter, A. McClung, K. Schüppert, B. Casabone and et al., Review of scientific instruments, 84, 123104 (2013)
[25] Pfaff W. and et al., Science, 345, 6196, 532-535(2014)
[26] R. Paschotta Article on ‘fibers’ in Encyclopedia of Laser Physics and Technology Available online: https://rp-photonics.com/fibers.html

تحسين معدل المفتاح في المكرر الكمي المتسلسل باستخدام ذاكرتين كموميتين مختلفتين

مروة أسعد خالد جواد عبدالكاظم حسن

معهد الليزر للدراسات العليا, جامعة بغداد, بغداد, العراق

الخلاصة: تتيح القنوات الكمومية إنجاز مهام الاتصال التي يتعذر الوصول إليها مع نظيراتها الكلاسيكية. المثال الأكثر شهرة هو توزيع مفاتيح سرية. لسوء الحظ ، فإن معدل توليد المفتاح السري عن طريق النقل المباشر محدود بشكل أساسي من خلال المسافة. يمكن التغلب على هذا الحد من خلال تنفيذ مكرر الكم. من أجل تعزيز أداء المكرر ، فقد اقترح مكرر كمي مع نوعان مختلفان من الذاكرة الكمومية يعتمد على مفهوم الانقطاع ، مما يقلل من ازالة الترابط الكمي أثناء تخزين الحالة الكمومية.