Device-Independent QKD with Spin-Coupled Cavities

Alejandro Mattar, Jonatan Bohr Brask, Antonio Acín

Phys. Rev. A, 88, 062319, 2013.

DIQIP Meeting, Brussels, May 2014

Notes:

Notes:

Notes:

Device-Independent Quantum Key Distribution (DIQKD)

- Provides a very high level of security. Security can be guaranteed with minimal assumptions on the implementation when the observed statistics is nonlocal.
- Requires violation of a Bell inequality. The violation must be free of the detection loophole.

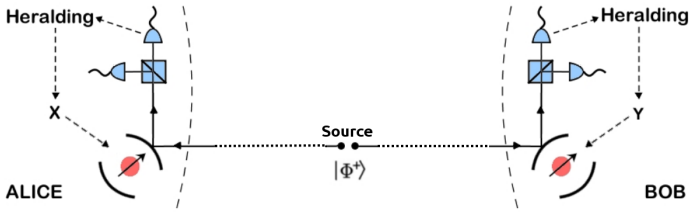
Challenge : Closing the detection loophole over relevant distances

- In standard schemes for Bell inequality violation, entangled photons are distributed from a source to Alice and Bob, then measured. The fraction of runs where photons reach both Alice and Bob decreases exponentially due to channel loss.
- There is a maximal distance for violation. Beyond this, DIQKD is impossible.
- Violation can be restored by assuming that the coincidence counts are representative of the entire data set (fair sampling). However, this is not justified for cryptography.
- No detection-loophole-free violations have been demonstrated so far, beyond a few tens of metres. Relevant distances for KD are kilometres and beyond.

Notes:

Possible solutions

- Distribute entanglement over long distances using quantum repeaters. Requires good quantum memory and many components.
- Perform quantum non-demolition measurement of incoming photons to confirm arrival.
- Single-photon qubit amplifier (Gisin, Pironio, Sangouard, Phys. Rev. Lett. 105, 070501, 2010).
- **Here : Heralded mapping of photonic entanglement onto spins in cavities.**
  - could be e.g. quantum dots, NV-centers, single atoms.



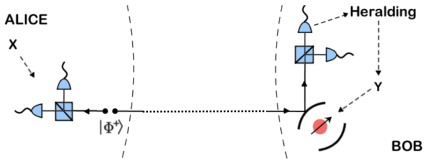
Notes:

- Heralding is a pre-selection and does not open any loopholes.
- Read-out of the spin can be very efficient.
- Eliminates dependence of Bell violation on channel loss.
- Only local heralding required, so spin decoherence is independent of distance.

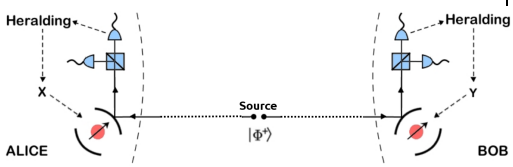
↓

Positive key rate over any distance.

Asymmetric protocol



Symmetric protocol



Notes:

Basis for the scheme : Coupling of light to spins in cavities

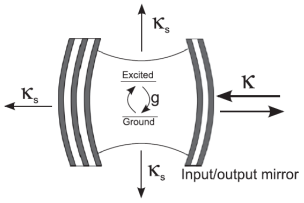
The presence of a dipole in the cavity can strongly modify the reflectivity.

For resonance scattering

$$g^2 = \frac{\gamma(\kappa + \kappa_s)}{4}$$

The reflectivities for coupled (full) or uncoupled (empty) cavities are given by

$$r_f = \frac{1}{1 + \kappa/\kappa_s} \qquad r_e = \left| \frac{1 - \kappa/\kappa_s}{1 + \kappa/\kappa_s} \right|$$



Young, Hu, Rarity, Phys. Rev. A, 87, 012332, 2013.

Here we consider spin-coupled cavities - one dipole transition for each spin state (e.g. a degenerate lambda transition). Light of different polarisation couples differently to the two spin states.

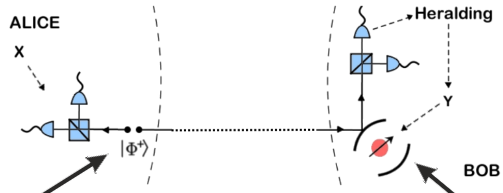
$$|R\rangle|\uparrow\rangle \rightarrow r_f|R\rangle|\uparrow\rangle \qquad |L\rangle|\uparrow\rangle \rightarrow r_e|L\rangle|\uparrow\rangle$$
$$|R\rangle|\downarrow\rangle \rightarrow r_e|R\rangle|\downarrow\rangle \qquad |L\rangle|\downarrow\rangle \rightarrow r_f|L\rangle|\downarrow\rangle$$

For $\kappa/\kappa_s \gg 1$ this gives a probabilistic, entangling interaction.

Notes:

Protocol operation

1. Initialisation of spins, probabilistic production of photonic entanglement.
2. Heralding measurement (+ Alice's measurement for asymmetric scheme).
3. Upon successful herald, readout of spin.



$|vac\rangle + \sqrt{p}(\frac{|RR\rangle + |LL\rangle}{\sqrt{2}}) + O(p)$ $\frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$

In the ideal case of without spin decoherence and multiphoton contributions,
the state after light-cavity interaction is (asymmetric protocol)

$$|\psi^A\rangle = \frac{1}{2}\begin{cases} |H\rangle \otimes [r_e|\Psi^+\rangle + r_f|\Phi^+\rangle] \\ + \\ i|V\rangle \otimes [r_e|\Psi^-\rangle + r_f|\Phi^-\rangle] \end{cases}$$

Notes:

E. Hänggi and R. Renner 2010,
L. Masanes et al. 2011, Pironio et al. 2013

Two different levels of security

- Bounded Quantum Storage (stronger, but realistic under current technology) :
  The devices may have memory, but Eve has limited quantum memory.
- Collective Attacks (weaker) : The devices are memoryless. Eve has unlimited memory.

In general, a positive key rate is possible whenever the uncertainty of Eve is larger
than the amount of public communication required for error correction.

$$H_E(S) - H(A|B) > 0$$

For different levels of security, we have different lower bounds on Eve's uncertainty
in terms of the Bell violation. For the CHSH inequality

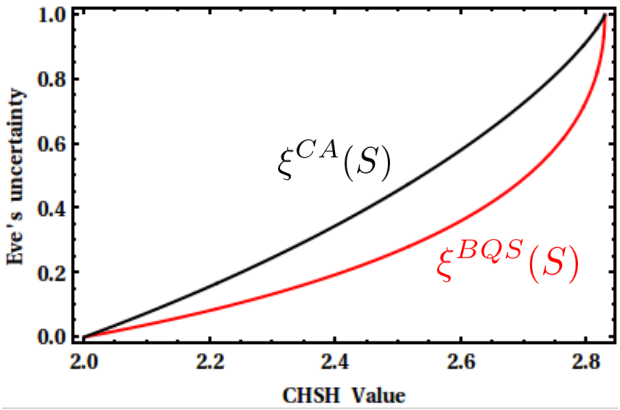
$$H_E^{BQS} \geq \xi^{BQS}(S) = -\log_2\left[\frac{1+\sqrt{2-(S/2)^2}}{2}\right]$$

$$H_E^{CA} \geq \xi^{CA}(S) = 1 - h\left[\frac{1+\sqrt{(S/2)^2-1}}{2}\right]$$

The conditional entropy is given by the quantum bit error rate (uniform marginals)

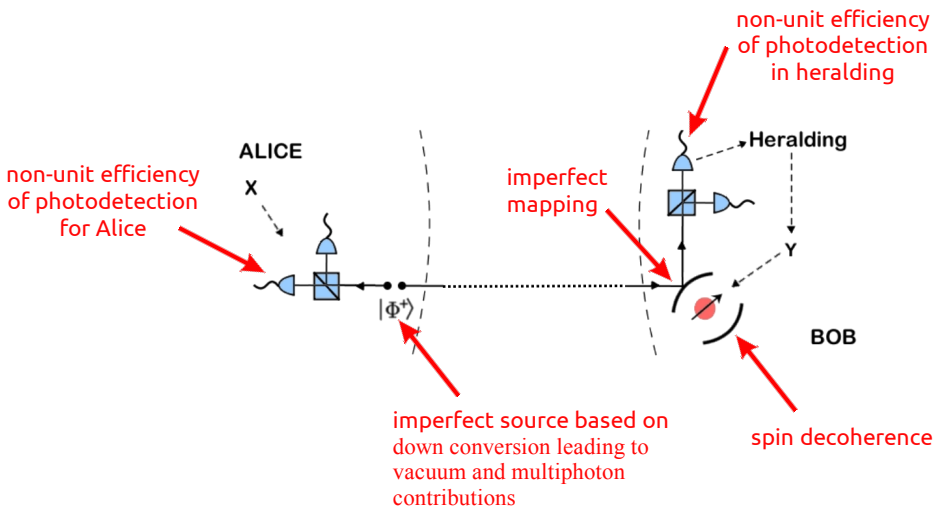
$$H(A|B) = h(Q)$$

Notes:



Notes:

Imperfections



Notes:

Noise : spin decoherence, multiphoton events, imperfect spin-light interation

Spin decoherence : model as a depolaring channel (worst case)

$$\xi(\rho) = \frac{1}{4}[1 + 3e^{-t/\tau}]\rho + \frac{1}{4}[1 - e^{-t/\tau}]\sum_{i=1}^{3}\sigma_i\rho\sigma_i$$

The spin decoheres between the heralding event and the end of the spin measurement, so the amount of decoherence depends on the ratio read out time / decoherence time.

Multiphoton contributions : we assume (worst case) that the cavity reflectivity is unity and that the output state after successful heralding is completely mixed.

Imperfect interaction : because of cavity loss, entanglement between light and spins is not perfect. Also, heralding outcomes are not communicated, but a local phase flip is applied if the herald is "V". The effective heralded state is an incoherent mixture of

$|\Psi^+\rangle \pm \frac{r_f}{r_e}|\Phi^+\rangle$ (asymmetric)

$|\Psi^+\rangle$ and $|\Psi^+\rangle \pm \frac{2r_f r_e}{r_e^2 + r_f^2}|\Phi^+\rangle$ (symmetric)

The ideal limit is $\kappa/\kappa_s \gg 1$ where $r_e \to 1, \quad r_f \to 0$

Notes:

Loss : channel loss, heralding detector, and Alice's detector inefficiency

Channel losses and heralding inefficiency only lower the rate postselection.

Detector inefficiency for Alice in the asymmetric protol creates inconclusive events. We need to bound the actual Bell violation considering all events in terms of the observed violation from the conclusive events. Two strategies for Eve:

- Conclusive outcomes for all settings. Bounded by quantum mechanics. $CHSH = S_q$
- Inconclusive outcome for at least one setting. Could have full information. $CHSH \leq 4$

$$H_E(S) \geq \xi(S) \quad \to \quad H_E(S) \geq (1-\mu)\xi\left(\frac{S - 4\mu}{1-\mu}\right)$$

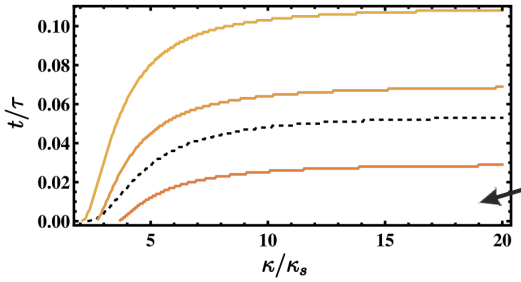
fraction of inconclusive to conclusive events $\mu \sim (1 - \eta_d^A)/\eta_d^A$

Gisin, Pironio, Sangouard, Phys. Rev. Lett. 105, 070501, 2010

Notes:

Feasible parameter ranges

- Important parameters are readout time / spin decoherence rate, cavity outcoupling/loss rate, and optical detection efficiency (for asymmetric scheme).
- Note that requirements for positive key rate do not depend on distance.



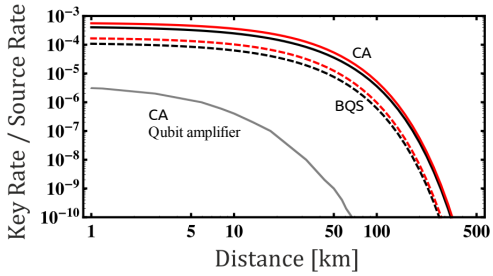
$\eta_d^A = 1.0, 0.9, 0.8$

Key rate positive under the curves.

- For QD's in micropillar cavities: Young, et al., PRA (2013), Reithmaier et al., Nature(2004) $\kappa/\kappa_s \sim 13$ $t/\tau \sim 0.1$
- For NV centers : Brunner, et al., NJPhys. (2013), Riedrich-Möller et al., Nat. Nano. (2012) $\kappa/\kappa_s \sim 2$ $t/\tau \sim 10^{-4}$
- For atoms : Brunner, et al., NJPhys. (2013), S. Ritter et al., Nature (2012) $\kappa/\kappa_s \sim 6$ $t/\tau \sim 10^{-3}$

Notes:

Achievable secret key rate



$\kappa/\kappa_s = 6$
$t/\tau = 0.01$
$\eta_d = 0.855$
$\eta_{her} = 0.855$
$L_{att} = 22\text{km}$

- Compare with optical qubit amplifier scheme. Gisin, Pironio, Sangouard, PRL (2010).
- Large improvement in rate/source use - around 5 orders of magnitude at 75km.
- Somewhat stricter requirements on source bandwidth in present scheme as it must match the cavity linewidth. Range from 0.1-100 of MHz, depending on implementation. For purely optical system, up to 10GHz may be achievable.
- Qubit amplifier curve assumes two single photons on demand. For probabilistic sources rate is reduced another 2-3 orders of magnitude.

Summary

We have described a new protocol for DIQKD based on heralded mapping of photonic entanglement to spins in cavities.

The protocol could be implemented using quantum dots in micropillar cavities, NV centers in photonic crystal cavities, or single atoms.

For realistic parameter values achievable with current or slightly improved technology, we find key rates on the order of 100 bits/s at 100km.

Outlook

Investigate which physical system is best suited for implementation.

Other Bell inequalities.

Other ways of heralding.
(e.g. via Stokes photons from atoms in free space, Sangouard et al., NJPhys 2013).

Notes:

Thank you.

Notes: