Probing the role of LG inequality for quantum key distribution

Quantum Information Processing and

Applications - HRI, Allahabad

Dec 7, 2013

R. Srikanth, PPISR, Bangalore

Collaborators

H. Akshata Shenoy, IISc, Bangalore

Arvinda S, Poornaprajna Institute of Scientific Research, B'lore

Prof. D. Home, Bose Institute, Kolkata

Crypto-wars: A Nonlocal hope

QKD: Distant parties (Alice and Bob) share private random bit string, whose security against Eve is based on quantum features like no-cloning (Bennett and Brassard 1984).

Quantum nonlocality (Bell 1964) can also be the basis of security (Ekert 1991). Basic intuition: monogamy of nonlocal correlations (CKW 2000).

Extendable to multi-partite quantum secret sharing exploiting monogamy of multipartite correlations (Scarani & Gisin 2001).

More generally: cryptographic benefits of any non-signaling, nonlocal theory include impossibility of perfect cloning, monogamy & privacy of correlations, complementarity etc. (Masanes, Acin and Gisin 2005).

Separability strikes back

Nonlocality as invoked above can equally be reproduced by protocols based on separable states (Bennett, Brassard & Mermin 1992).

The basic reason for this: single-particle properties like no-cloning and complementarity are consequences of non-signaling nonlocality (MAG 2005).

It would thus seem that nonlocality/entanglement gives no additional benefit to cryptography.

The Return of Nonlocality

Conventional QKD schemes implicitly assume devices can be trusted. But what if correlations are established via side-channels between encoded state (e.g., polarization in BB84) and another degree of freedom (e.g., frequency)?

Device independent (DI) scenario: security guaranteed via certain statistical checks and without detailed characterization of devices (Mayers & Yao 1998).

Necessary condition for security in this more stringent requirement: $P(a,b|x,y) \neq \sum_\lambda P(a|x,\lambda)P(b|y,\lambda)p_\lambda$, since Eve may possess a copy of $\lambda \Rightarrow P(a,b)$ must violate a Bell inequality. sufficiently highly: security not just against a quantum mechanical Eve, but even arbitrary non-signaling Eve. (BHK06, AGM06).

Insecurity of BB84 in DI scenario

$$\begin{aligned} P(a=b|x=y) &= 1 \\ P(a=b|x\neq y) &= \frac{1}{2} \end{aligned} \tag{1}$$

for which the CHSH inequality

$$E(0,0)+E(0,1)-E(1,0)+E(1,1)=2\leq B_{\mathsf{LR}}$$

The correlations (1) can be reproduced by:

$$\rho_{AB}=\frac{1}{4}(|00\rangle_{AB}\langle 00|+|11\rangle_{AB}\langle 11|)_z\otimes(|00\rangle_{AB}\langle 00|+|11\rangle_{AB}\langle 11|)_x.$$

Accessing higher dimensions undermines BB84.

Non-signaling: Eve has full info after PAB.

Back to separability? Temporal considerations, OK?

Conventional DI QKD assumes $P(a, b|x, y)$ must be *spatial*. Formally, violation of a correlation inequality indicates lack of joint distribution – basis of unification of spatial, temporal and contextuality inequalities (Markiewicz et al. 2013; DASH 2013).

What about replacing spatial with temporal correlations? Does it make sense?

Idea suggestive but not obvious, mainly for various reasons:
(1) BB84 is a Prepare-and-Measure protocol, involves quantum communication, whereas above attack is *static*;
(2) Temporal correlations, unlike spatial, are signaling.
(3) 'temporal entanglement' quite different from spatial
(4) So too with monogamy of temporal entanglement

What LGI based cryptography can hope for

Consider attack using cheat state $\rho_{\mathcal{A}B}$. If **m** and **n** denote the Bloch vectors of the state of two uncorrelated particles, and measurements **x** and **y** are performed on them, then $E(\mathbf{x},\mathbf{y}) \propto (\mathbf{x}\cdot\mathbf{m})(\mathbf{y}\cdot\mathbf{n})$. Such 'separable' correlations cannot violate LGI.

Therefore, LGI serves as a *sameness check*: entity authentication: to ascertain that it was prepared in the previous step by Alice (barring singlet correlations).

(Analogously, the Bell test of a conventional DI protocol constitutes a check on dimensionality of the system.)

First issue: including BB84 emissions

However: if the hi-dim attack is coupled with standard BB84 emissions, then the sameness check does not help!

Thus we must either (A) abandon prepare-and-measure cryptographic strategies for entanglement-based ones OR (B) enhance prepare-and-measure strategies OR (C) find reasons to restrict Eve's power just enought to suit us!

Moral: no easy way to go from spatial to temporal correlations in **cryptography:**

Here we opt for (C)

A bit like saying Eve can carry a tera-watt laser weapon but not a torch light!

Technically: static BHK attack with standard BB84 emission becomes *signaling* (if Alice's device is in the state $|0\rangle$ OR $|-\rangle$, and Eve measures in the computational basis and find $|1\rangle$, she knows Alice's basis choice to be the diagonal basis, implying a signaling side-channel which we rule out by assumption).

With arbitrary side-channels, QKD is a lost hope. "Eve is not God" – but a powerful human being!

2nd issue: Temporal correlations are signaling.

Correlations for sequential measurements on qubit $\hat{x}$ then $\hat{y}$:

$$
\begin{aligned}
P_{\alpha\beta|\hat{x}\hat{y}} &= \mathrm{Tr}\left(\frac{1+\beta\hat{y}}{2}\frac{1+\alpha\hat{x}}{2}\rho\frac{1+\alpha\hat{x}}{2}\right) = \frac{1}{4} + \frac{\alpha}{4}\mathrm{Tr}(\hat{x}\rho) + \frac{\beta}{8}\mathrm{Tr}(\hat{y}\rho) \\
&+ \frac{\beta}{8}\mathrm{Tr}(\hat{x}\hat{y}\hat{x}\rho) + \frac{\alpha\beta}{8}\mathrm{Tr}(\{\hat{x},\hat{y}\}\rho), \qquad (2)
\end{aligned}
$$

where $\alpha, \beta = \pm 1$.

Bob's marginal $P_{\beta|xy} = \sum_\alpha P_{\alpha\beta|xy} = \frac{1}{4} + \frac{\beta}{8}\mathrm{Tr}(\hat{y}\rho) + \frac{\beta}{8}\mathrm{Tr}(\hat{x}\hat{y}\hat{x}\rho)$ depends on Alice's setting (converse not true).

On the other hand, correlator

$$\langle\hat{x}\hat{y}\rangle = \sum_{\alpha,\beta} \alpha\beta P_{\alpha\beta|\hat{x}\hat{y}} = \frac{1}{2}\langle\{\hat{x}\hat{y}\}\rangle = \vec{x}\cdot\vec{y}, \qquad (3)$$

same as with spatial correlations $\Rightarrow$ same Tsirelson bound.

3rd issue: temporal 'entanglement' & monogamy

In quantum mechanics: Three consecutive measurements $\hat{x}$, $\hat{y}$ and $\hat{z}$ are performed at t_1, t_2 and t_3 ($t_1 < t_2 < t_3$) respectively:

$$\begin{aligned} \langle \hat{x}, \hat{z} \rangle &= \sum_{m,n,o=\pm 1} mo \; \mathrm{Tr}\left[\rho \Pi_{\mathbf{x}}^{m}\right] \mathrm{Tr}\left[\Pi_{\mathbf{x}}^{m} \Pi_{\mathbf{y}}^{n}\right] \mathrm{Tr}\left[\Pi_{\mathbf{y}}^{n} \Pi_{\mathbf{z}}^{o}\right] \\ &= (\mathbf{x} \cdot \mathbf{y})(\mathbf{y} \cdot \mathbf{z}), \end{aligned} \tag{4}$$

Third correlatum is *disentangled* from first, when second is projective measurement. (By contrast, a W state lacks this feature).

Formally, lhs of (4) like measurement on product state of identical copies with Bloch vector **y**.

Separable bound for CHSHI

For separable states, $\Lambda \leq \sqrt{2}$. (Local bound is 2.) Bound reached with e.g., $\mathbf{x}'$, $\mathbf{z}$, $\mathbf{x}$ and $\mathbf{z}'$ be coplanar, separated by angle $\pi/4$, with $\mathbf{y} = \mathbf{z}$.

$$\begin{aligned} \vec{a}_1 &= \hat{i}, \vec{a}_2 = \hat{j}, \vec{a}_3 = \frac{1}{\sqrt{2}}\hat{i} + \frac{1}{\sqrt{2}}\hat{j}, \\ \vec{b}_1 &= \frac{1}{\sqrt{2}}\hat{i} + \frac{1}{\sqrt{2}}\hat{j}, \vec{b}_2 = \frac{-1}{\sqrt{2}}\hat{i} + \frac{1}{\sqrt{2}}\hat{j}, \vec{b}_3 = \hat{j} \end{aligned} \tag{5}$$

which are used for evaluating one of the following Bell correlations

$$\Lambda = E(\vec{a}_1, \vec{b}_1) + E(\vec{a}_2, \vec{b}_1) + E(\vec{a}_1, \vec{b}_2) - E(\vec{a}_2, \vec{b}_2). \tag{6}$$

Most general separable state

$$\rho_{sep} = \int \int \sigma(\vec{n}_a, \vec{n}_b) |n_a\rangle\langle n_a| \otimes |n_b\rangle\langle n_b| d\vec{n}_a d\vec{n}_b, \tag{7}$$

where $\int\int \sigma(\vec{n}_a, \vec{n}_b) d\vec{n}_a d\vec{n}_b = 1$ and

$$\begin{aligned} \vec{n}_a &= \sin\theta_a \cos\phi_a \hat{i} + \sin\theta_a \sin\phi_a \hat{j} + \cos\theta_a \hat{k} \\ \vec{n}_b &= \sin\theta_b \cos\phi_b \hat{i} + \sin\theta_b \sin\phi_b \hat{j} + \cos\theta_b \hat{k} \end{aligned} \tag{8}$$

$$E(\vec{a}_i, \vec{b}_j) = \mathrm{Tr}[\rho_{sep} \vec{\sigma}.\vec{a}_i \otimes \vec{\sigma}.\vec{b}_j] \tag{9}$$

$$\begin{aligned} \Lambda &= \sqrt{2} \int\int\int\int \sigma(\theta_a, \theta_b, \phi_a, \phi_b) \sin^2\theta_a \sin^2\theta_b \sin(\phi_a + \phi_b) d\theta_a d\theta_b d\phi_a d\phi_b \\ &\Rightarrow -\sqrt{2} \le S \le \sqrt{2}, \end{aligned} \tag{10}$$

which is less than the local-realist bound 2.

Monogamy and signaling are related

No-signaling + nonlocality $\Rightarrow$ no-cloning, monogamy etc (MAG 2006).

Nonlocality + some signaling $\Rightarrow$ weakened no-cloning, monogamy etc (AS 2013).

Alice and Bob share a non-signaling correlation given by $a \oplus b = x \cdot y$ – violates CHSH inequality to the algebraic maximum of 4.

Suppose Charlie interacts with Bob, and becomes correlated with Alice by: $a \oplus c = x \cdot z$.

Adding up: $b \oplus c = x \cdot (y \oplus z)$, 1-bit signal from Alice to Bob-Charlie

More generally: Charlie's attempt to generate correlation leads to convex combination of PR + local box along both arms:

$$\Lambda_{\mathcal{A}B} + \Lambda_{\mathcal{A}C} \leq 2 \times (2(1-\mu) + 4\mu) = 4\mu + 4, \tag{11}$$

$\mu = 0 \Rightarrow$ no-signaling bound (Toner 2006). No bound when $\mu = 1$.

Probability that Bob-Charlie deduce Alice's input is thus $\mu^2 + \frac{1}{2}(1-\mu^2) = \frac{1}{2}(1+\mu^2) \equiv \sigma$.

Signal $S \equiv 2\sigma - 1 = \mu^2 \in [0,1]$ so that:

$$\Lambda_{\mathcal{A}B} + \Lambda_{\mathcal{A}C} \leq 4(1+\sqrt{S}), \tag{12}$$

showing how signaling weakens monogamy.

Larger the signaling, smaller the gap $C - S$, and more classical the correlations (AS 2013).

4th issue: Monogamy of temporal correlations

Given sequential measurements A, B, C, we have by virtue of Eqs. (4) and (10) Monogamy for temporal qubit correlations:

$$\Lambda_{\mathcal{A}B} + \Lambda_{\mathcal{A}C} \leq 2\sqrt{2} + \sqrt{2} = 3\sqrt{2} > 4,$$

no-signaling bound.

Implications studied under two protocols:
(1) LG protocol: Where secret bit generation based on monogamy: nonlocal case secure, whereas temporal case almost not.
(2) LG-BB84 protocol: Where LG mode used for entity authentication, while BB84 mode used for secret bit generation.

LG protocol: Rendered almost insecure through weakened monogamy

On particle transmitted from Alice to Bob, both randomly perform LGI measurements.

Basis reconciliation: Bob announces bases; Alice keeps her outcome as-is except flips last case (settings (1,1)).

Violation of LGI guarantees mostly correlated than anti-correlated.

Secure in non-signaling case, and **just** secure under above signal-weakened monogamy,

LG/CHSH in probability form: $\mathcal{B} \equiv \frac{1}{4}\sum_{x,y} P(a \oplus b = xy|x,y) \leq \frac{3}{4}$.

Monogamy: $\mathcal{B}_{\mathcal{AB}} + \mathcal{B}_{\mathcal{AE}} \leq \frac{3\sqrt{2}}{8} + 1 \equiv \frac{3}{2} + \epsilon$, where $\epsilon = \frac{3}{4\sqrt{2}} - \frac{1}{2}$ is the weakening of monogamy beyond the no-signaling limit.

From Pawlowski (2010) for individual attacks: Bob knows Alice's bit with probability $p_B = \mathcal{B}_{AB}$, while Eve knows Alice's bit with probability $p_E \leq 2\mathcal{B}_{AE} - \frac{1}{2}$.

By virtue of monogamy $p_B + \frac{1}{2}p_E + \frac{1}{4} \leq \frac{3}{2} + \epsilon$, therefore $p_B \geq p_E$ if $\mathcal{B}_{AB} \geq \frac{5}{6} + \frac{2\epsilon}{3}$, or, in correlation terms $\Lambda_{\mathcal{AB}} \geq \frac{8}{3}(1 + 2\epsilon)$, which is precisely $2\sqrt{2}$ for the above value of ϵ.

LG-BB84 protocol

$M_\pm \equiv \frac{1}{\sqrt{2}}(X \pm Z)$.

Alice transmits Bob randomly one of the 8 states: eigenstates of $X, Z, M_+ \equiv \{|\underline{0}\rangle, |\underline{1}\rangle\}, M_- \equiv \{|\underline{+}\rangle, |\underline{-}\rangle\}$.

Bob randomly measures: $X, Z, M_\pm$.

BB84 mode: When bases match $\Rightarrow$ secret bit.

LG mode: Alice measures X/Z, Bob measures $M_\pm$, or vice versa, outcome data is used to check for violation of LGI. (for *entity authentication*)

Higher-dimensional attack cheat state $\rho_{\mathcal{A}B}$ here would be: $\rho'_{\mathcal{A}B} = \frac{1}{16}\left(\Pi^{(12)}_{00} + \Pi^{(12)}_{11}\right) \otimes \left(\Pi^{(34)}_{++} + \Pi^{(34)}_{--}\right) \otimes \left(\Pi^{(56)}_{\underline{00}} + \Pi^{(56)}_{\underline{11}}\right) \otimes \left(\Pi^{(78)}_{\underline{++}} + \Pi^{(78)}_{\underline{--}}\right)$.

$\rho'_{\mathcal{A}B}$ passes the BB84 test, but maximally fails LG test ($\Lambda = 0$)

Eve mixes fraction f of device attack (via $\rho'_{\mathcal{A}B}$) with channel attack with prob $1 - f$ (producing error rate η).

Alice and Bob find

$$\begin{aligned} \Lambda_0 &\equiv 2\sqrt{2}(1-f)(1-\eta), \\ e &\equiv (1-f)\eta \end{aligned} \tag{13}$$

Single-qubit attack

Our protocol is equivalent to Alice transmitting half a singlet to Bob, and measuring her qubit in LG-BB84 basis (Scarani and Gisin 2005):

For privacy amplification (as against advantage distillation) in QKD (Csizar & Körner 1989):

$$I(A:B) > I_E \equiv \min[I(A:E), I(B:E)].$$

Eve's optimal individual attack (maximizing I(A:E) for given disturbance), parametrized by $\theta \in [0, \pi/2]$ (Niu & Griffiths 2000):

$$\begin{aligned} U|00\rangle_{BE} &= |00\rangle_{BE} \\ U|10\rangle_{BE} &= \cos\theta|10\rangle_{BE} + \sin\theta|01\rangle_{BE}, \end{aligned} \quad (14)$$

$$|\Psi(\theta)\rangle_{ABE} = \frac{1}{\sqrt{2}}(|000\rangle + \cos\theta|110\rangle) + \sin\theta|101\rangle$$

Calculation with $\rho_{AB}, \rho_{AE}, \rho_{BE}$ shows that the error statistics (matches vs mismatches in outcomes) are the same for any measurement basis. Moreover, error is binary symmetric.

$e_{AB} = (1 - \cos\theta)/2;\ e_{AE} = (1 - \sin\theta)/2;\ e_{BE} = (1 - \sin 2\theta)/2;$

In each case, $I(\cdot : \cdot) = 1 - H(e_\alpha)$.

Plotting I_{AB} vs I_E, one finds

$$I_{AB} \geq I_E \Longleftrightarrow \theta \leq \pi/4 \tag{15}$$

Nonlocality

Two-qubit mixed state density operator $\rho = \frac{1}{4}[I \otimes I + (\vec{r} \cdot \sigma) \otimes I + I \otimes (\vec{s} \cdot \sigma) \sum_{n,m=1}^{3} t_{mn}(\sigma_m \otimes \sigma_n)]$, $\Lambda_{\text{max}}(\rho) = 2\sqrt{M(\rho)}$. Thus ρ violates CHSHI iff $M(\rho) > 1$, where $M(\rho) = \max(e_j + e_k)$, e_j, e_k being eigenvalues of matrix $T^{\dagger}T$, where $T = \{t_{mn}\}$ is the correlation matrix (Horodecki family (1995)).

$\Lambda_{\text{max}}(\rho_{AB}) = 2\sqrt{2}\cos\theta$; $\Lambda_{\text{max}}(\rho_{AE}) = 2\sqrt{2}\sin\theta$; $\Lambda_{\text{max}}(\rho_{BE}) = \sqrt{2}\sin 2\theta$;

Thus ρ_{AB} is nonlocal iff $\theta > \pi/4$ By Eq. (15),
security $\Longleftrightarrow$ nonlocality.

By our reduction: security $\Longleftrightarrow$ violation of LG inequality.

Thank you!