Geometric Perspective on Quantum Key Distribution

Georgi **BEBROV**

Technical University of Varna

GIQ (2026)

Outline/Agenda

Motivation

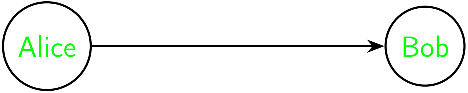
- **Establishing a bridge between geometry and QKD (information theory)**.
  Linking geometric to informational quantities.
- **Systematization**—representing distinct QKD processes within a unified geometric framework. Consequence: proper comparison of QKD processes.
- Introducing new perspective on the QKD processes—for visualizing, interpreting, and intuition purposes.

Essentials

Definition (Quantum Key Distribution, QKD)

Communication process in which two or more parties establish a common cryptographic key whose security is based on the principles of quantum mechanics.

Bipartite QKD are considered in this talk: two parties are involved in the QKD process.



legitimate (communicating) parties

Essentials

A QKD is completely described by its *secret key rate* $\mathbf{R}$

$$\mathbf{R} = \left(1 - \underbrace{H(e)}_{\text{eavesdropper}} - \underbrace{H(e)}_{\text{noise}}\right) \quad \textbf{BB84-QKD} \tag{1}$$

or

$$\begin{aligned}\mathbf{R} &= \left(1 - \underbrace{\chi}_{\text{eavesdropper}} - \underbrace{H(8p)}_{\text{noise}}\right) \quad \textbf{RQKD} \\ &= \left(1 - \underbrace{\chi}_{\text{eavesdropper}} - \underbrace{H(e)}_{\text{noise}}\right)\end{aligned} \tag{2}$$

e—error rate; p—interception rate; χ—Holevo information; $H(\bullet)$—Shannon entropy.

Essentials

Generalization of $\mathbf{R}$:

$$\boxed{\mathbf{R} = (1 - \mathbf{F})} \tag{3}$$

where

$$\mathbf{F} = H(e) + H(e) \tag{4}$$

or

$$\mathbf{F} = \chi + H(e) \tag{5}$$

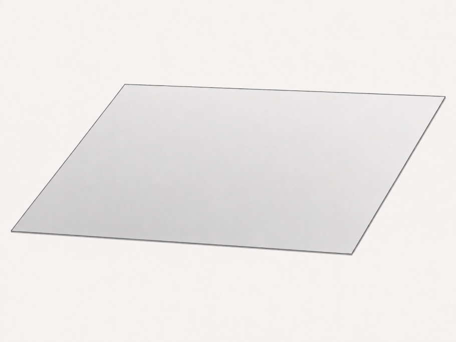
$\boxed{\mathbf{F} \text{ — key-rate } \textit{reduction}}$

Behavior of QKD is usually quantified (evaluated) by

rate-error relation $\mathbf{R}(e)$

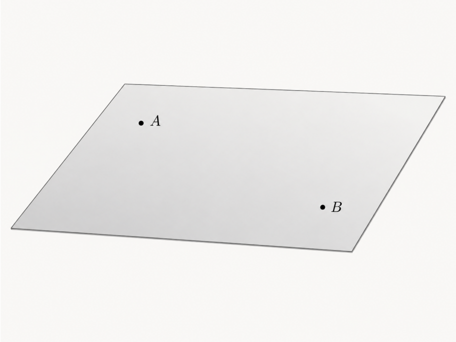
Geometric Model

1. communication process $\Rightarrow (M, g)$ 2-dimensional Riemannian manifold



Geometric Model

1. communication process $\Rightarrow$ (M, g) 2-dimensional Riemannian manifold
2. communicating parties $\Rightarrow$ distant points on the manifold ($A, B \in M$, $A \neq B$)



Geometric Model

Interception (or noise) — presence of a <u>field</u> distorting the manifold.

1. radially symmetric source (field) - scalar field $\phi : M \to \mathbb{R}$ (isotropic)

Geometric Model

Interception (or noise) — presence of a field distorting the manifold.

1. radially symmetric source (field) - scalar field $\phi : M \to \mathbb{R}$ (isotropic)
2. placed at the center between A and B

Geometric model

Metric:

$$g_{ij} = e^{2\phi}\delta_{ij},\ i,j \in \{1,2\}$$

ϕ — source field

$$g_{ij} \to \Gamma^k_{ij} \to R^i{}_{jkl}$$

Connections:

$$\Gamma^k_{ij} = \frac{1}{2} g^{kl}\left(\partial_i g_{lj} + \partial_j g_{li} - \partial_l g_{ij}\right),\ \partial_i = \frac{\partial}{\partial x^i}$$

Riemann tensor:

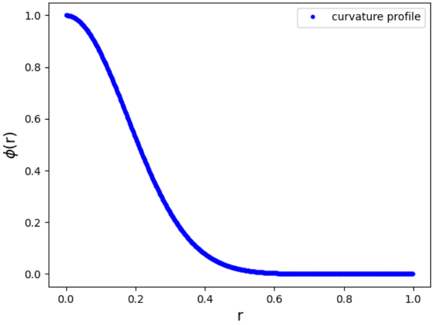
$$R^i{}_{jkl} = \partial_k \Gamma^i_{lj} - \partial_l \Gamma^i_{kj} + \Gamma^i_{km}\Gamma^m_{lj} - \Gamma^i_{lm}\Gamma^m_{kj}$$

Geometric Model

Bell-shaped field

$$\phi(r) = \sqrt{a} \times \mathrm{e}^{-\frac{r^2}{R^2}}$$

a — source intensity (noise or interception intensity);
R — width/scale of the source (bell shape)



$(a = 1,\ R = 0.25)$

Geometric Model

Given $\phi(r)$ (polar coordinates)

Metric

$$g_{ij} = e^{2\phi}\delta_{ij},\, i,j \in \{r,\theta\} \Rightarrow g_{rr} = e^{2\phi(r)},\; g_{\theta\theta} = e^{2\phi(r)}r^2$$

symmetric

Connections

$$\Gamma^k_{ij} \Rightarrow \Gamma^r_{rr} = \phi'(r),\; \Gamma^r_{\theta\theta} = -r(1 + r\phi'(r)),\; \Gamma^\theta_{r\theta} = \Gamma^\theta_{\theta r} = \frac{1}{r} + \phi'(r)$$

$\phi'(r) = \frac{\mathrm{d}\phi}{\mathrm{d}r}$

Riemann tensor

$$R^i{}_{jkl} \Rightarrow R^r{}_{\theta r\theta} = -r\phi'(r) - r^2\phi'(r)$$

only one independent element due to symmetry

Geometric Model

Geometric evaluation of a QKD behavior:

1. **geodesic length** (radial geodesic)

$$\mathcal{L} = \int_{\lambda_1}^{\lambda_2} \sqrt{g_{ij} \frac{\mathrm{d}x^i}{\mathrm{d}\lambda} \frac{\mathrm{d}x^j}{\mathrm{d}\lambda}} \mathrm{d}\lambda \Rightarrow \int_{r_1}^{r_2} \mathrm{e}^{\phi(r)} \mathrm{d}r \Rightarrow 2 \int_{0}^{r_0} \mathrm{e}^{\phi(r)} \mathrm{d}r = \mathcal{L}(a)$$

λ—geodesic parameter
$\mathrm{d}s^2 = \mathrm{e}^{2\phi(r)} \left(\mathrm{d}r^2 + r^2 \mathrm{d}\theta^2 \right)$
r_0—radial distance from the source; <u>source placed at $r = 0$</u>

Geometric Model

Geometric evaluation of a QKD behavior:

1. **geodesic length** (radial geodesic)

$$\mathcal{L} = \int_{\lambda_1}^{\lambda_2} \sqrt{g_{ij} \frac{\mathrm{d}x^i}{\mathrm{d}\lambda} \frac{\mathrm{d}x^j}{\mathrm{d}\lambda}} \mathrm{d}\lambda \Rightarrow \int_{r_1}^{r_2} \mathrm{e}^{\phi(r)} \mathrm{d}r \Rightarrow 2 \int_{0}^{r_0} \mathrm{e}^{\phi(r)} \mathrm{d}r = \mathcal{L}(a)$$

λ—geodesic parameter
$\mathrm{d}s^2 = \mathrm{e}^{2\phi(r)} \left(\mathrm{d}r^2 + r^2 \mathrm{d}\theta^2\right)$
r_0—radial distance from the source; source placed at $r = 0$

2. **Gaussian curvature**

$$K = \frac{R_{r\theta r\theta}}{\det g} = \frac{R_{r\theta r\theta}}{g_{rr} g_{\theta\theta}} \Rightarrow \frac{4\sqrt{a}}{R^2} \mathrm{e}^{-2\phi(r)} \mathrm{e}^{-\frac{r^2}{R^2}} \left(1 - \frac{r^2}{R^2}\right) = K(r, a)$$

$R_{r\theta r\theta} = g_{rn} R^{n}_{\ \theta r\theta}$

Geometric Model

Key rate in terms of $\mathcal{L}$

$$\begin{gathered}\mathbf{R} = 1 - \mathbf{F} \\ \Downarrow \\ \mathbf{R}_{\mathsf{G}}(a) = \mathcal{L} - \mathbf{F}_{\mathsf{G}}\end{gathered} \tag{6}$$

$\boxed{\mathcal{L}}$—geodesic length in the absence of a source (interception) ($r_0 = 0.5$, $\mathcal{L} = 1$)

$\boxed{\mathcal{L}_{\mathsf{dist}}}$—geodesic length in the presence of a source (interception)

$\boxed{\mathbf{F}_{\mathsf{G}} = \mathcal{L}_{\mathsf{dist}}(a) - \mathcal{L}}$—distortion length ($\mathbf{F}_{\mathsf{G}} \geq 0$)

Geometric Model

Key rate in terms of K

$$\mathbf{R} = 1 - \mathbf{F}$$
$$\Downarrow \tag{7}$$
$$\mathbf{R}_{\mathsf{G}}(a) = 1 - \left(\frac{K(0,a)}{K(0,1)}\right)^{\gamma}$$

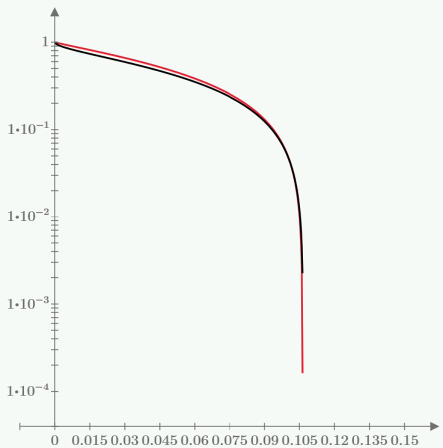
$a = 1$—reference intensity a.

$\boxed{\frac{K(0,a)}{K(0,1)}}$—normalized curvature ($r = 0$, curvature at the center, maximum curvature for certain a)

$\boxed{\gamma}$—power rescaling (shape-calibration exponent)

Results

$\mathcal{L}$-based approach:



Reconstructing RQKD rate-error function

Intensity a is related to p (interception probability).

black line—

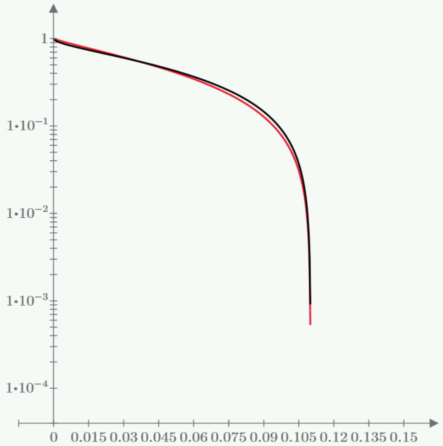
$\mathbf{R}_{\mathsf{G}} = \mathcal{L} - (\mathcal{L}_{\mathsf{dist}}(16.56 \times a) - \mathcal{L})$

red line—

$\mathbf{R}_{\mathsf{RQKD}} = (1 - \chi - H(8 \times a))$

Results

$\mathcal{L}$-based approach:



Reconstructing BB84-QKD rate-error function

Intensity a is related to e (error rate).

black line—

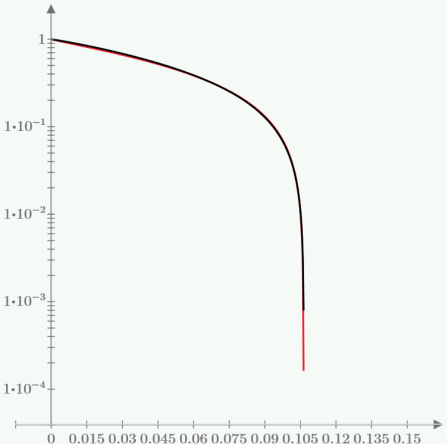
$\mathbf{R}_{\mathsf{G}} = \mathcal{L} - (\mathcal{L}_{\mathsf{dist}}(7.75 \times a) - \mathcal{L})$

red line—

$\mathbf{R}_{\mathsf{BB84}} = (1 - 2H(a))$

Results

K-based approach:



Reconstructing RQKD rate-error function

Intensity a is related to p (interception probability).

black line—

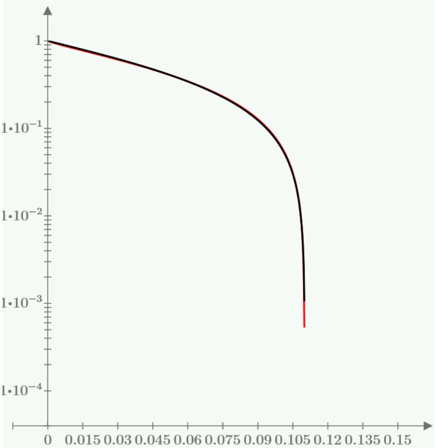
$$\mathbf{R}_{\mathsf{G}} = 1 - \left(\frac{K(0{,}0.388\times a)}{K(0{,}1)}\right)^{2.264}$$

red line—

$$\mathbf{R}_{\mathsf{RQKD}} = (1 - \chi - H(8 \times a))$$

Results

K-based approach:



Reconstructing BB84-QKD rate-error function

Intensity a is related to e (error rate).

black line—

$$\mathbf{R}_{\mathsf{G}} = 1 - \left(\frac{K(0{,}0.375\times a)}{K(0{,}1)}\right)^{2.135}$$

red line—

$$\mathbf{R}_{\mathsf{BB84}} = (1 - 2H(a))$$

$$\boxed{\mathbf{R}_{\mathsf{G}} \approx \mathbf{R}_{\mathsf{BB84}}}$$

Results

The above result implies

$$\left(\frac{K(0, 0.375 \times e)}{K(0,1)}\right)^{2.135} = 2H(e)$$

That is

$$\frac{1}{2}\left(\frac{K(0, 0.375 \times e)}{K(0,1)}\right)^{2.135} = H(e)$$

Hence

$$\chi = \frac{K(0, 0.388 \times e)}{K(0,1)}^{2.264} - \frac{1}{2}\left(\frac{K(0, 0.375 \times e)}{K(0,1)}\right)^{2.135}$$

since $F = \chi + H(e)$. Also $C = 1 - H(e)$ (information capacity of a *binary symmetric channel*) can thus be recast as

$$C = 1 - \frac{1}{2}\left(\frac{K(0, 0.375 \times e)}{K(0,1)}\right)^{2.135}$$

Results

Reconstructing rate-distance relation

Single-repeater bound (SRB) — $SRB \propto \sqrt{\eta}$ $\left(\eta = 10^{-\alpha L/10}\right)$:

$$SRB = \log_2\left(1 - \sqrt{10^{-\alpha L/10}}\right)$$

PLOB bound $(PLOB)$ — $PLOB \propto \eta$ $\left(\eta = 10^{-\alpha L/10}\right)$:

$$PLOB = \log_2\left(1 - 10^{-\alpha L/10}\right)$$

$\mathbf{R}_{\mathsf{G}} = 1 - \ln\left(\sqrt{\frac{K(0,a/20)}{K(0,32)}}\right)$ for η relation and

$\mathbf{R}_{\mathsf{G}} = 1 - \ln\left(\sqrt{\frac{K(0,a/20)}{K(0,58)}}\right)$ for $\sqrt{\eta}$ relation

Results

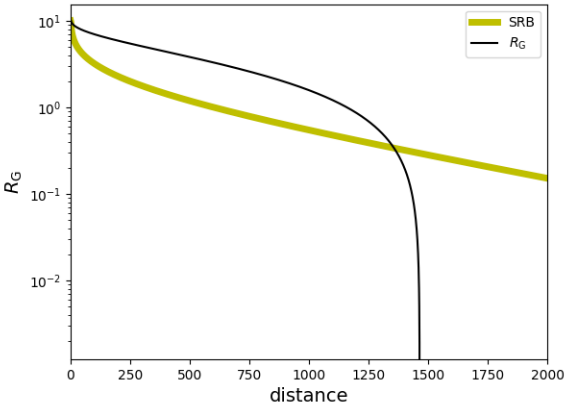


Figure: Rate-distance relation $\propto \sqrt{\eta}$

Results

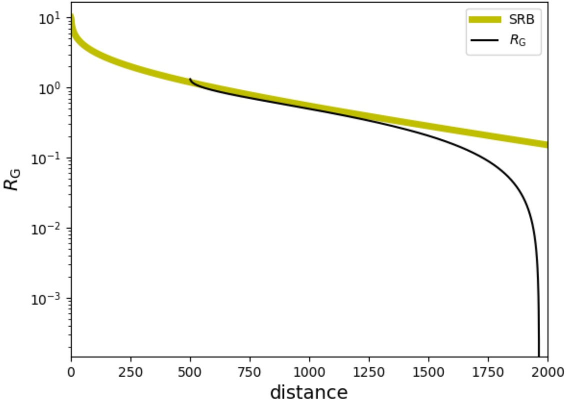


Figure: Rate-distance relation $\propto \sqrt{\eta}$

Results

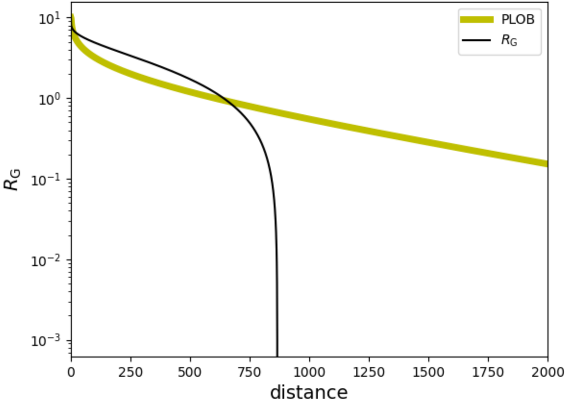


Figure: Rate-distance relation $\propto \eta$

Results

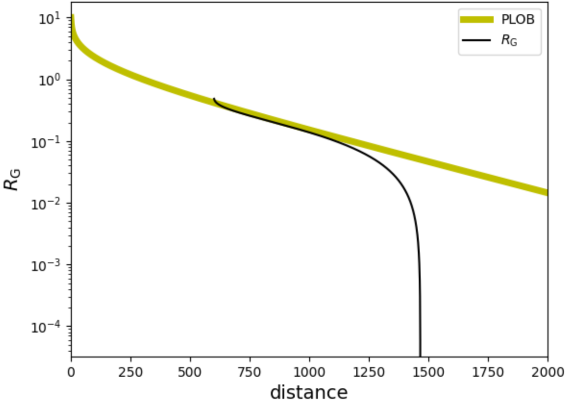


Figure: Rate-distance relation $\propto \eta$

Results

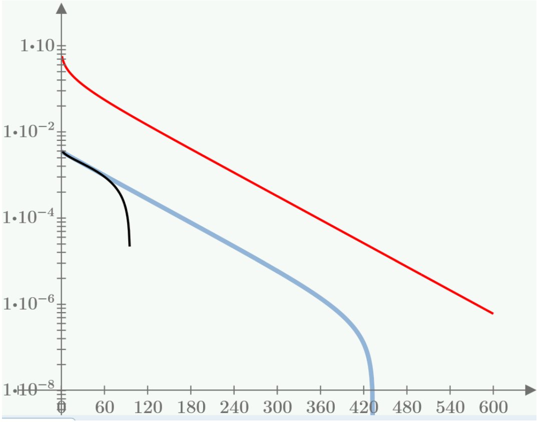


Figure: Rate-distance relation of a PM-QKD (blue line)

Remarks

- A geometric-based model of a QKD process was introduced.
- The QKD behavior is quantified by either geodesic length $\mathcal{L}$ or curvature K.
- Tha approach based on $\mathcal{L}$ fails to deliver desired results.
- The approach based on K delivers appropriate results. A link between geometry and classical information theory was presented (capacity C is completely derived in terms of K).

Thank you for your attention!