Quantum Key Distribution

Maximal violation of symmetric measurement protocol with simplex bell inequality and self-testing.

Jam Kabeer Ali Khan
Supervisor: Professor Ravishankar Ramanathan

The University of Hong Kong
Department of Computer Science
CS Research Internship

September 12, 2024

Contents

1. Background
2. Motivation
3. Result and Methods
4. Conclusion

Background

Background

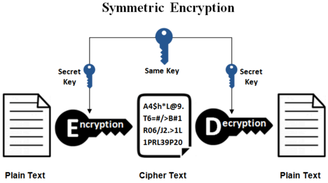


Figure: Symmetric Key Distribution

1. Key Distribution: Securely transferring the secret key between parties in Cryptography protocols.
2. Random Number Generation (RNG): Generating a sequence of numbers that are predicted best by random chance, most are Psuedo Random Number Generators (PRNG) using deterministic algorithms. Strong application in crytographic key generation.
3. Quantum Key Distribution (QKD) involves delivery of secret keys through an insecure quantum channel by parties performing measurment on entangled state.(Zapatero et al., 2023)
4. QRNG: Generating truely random numbers based on the phenomena of Quantum Physics. More secure than PRNG.
5. Device-Independent QKD does not depends on the implementation of the QKD device, treating it as a blackbox, and it certifies the security based upon the input-output measurement statistics of Alice and Bob (Zapatero et al., 2023).

Device-Independence

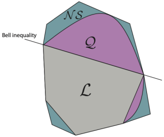


Figure: Sketch of Polytope Brunner et al. (2014)

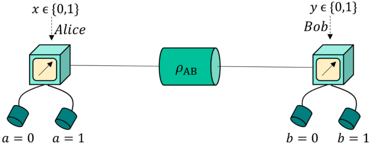


Figure: CHSH test setup Zapatero et al. (2023)

1. Bell's Theorem: Predictions made by Quantum Theory can not be predicted by any Local Theory.
2. CHSH Bell Inequality: $\langle A_0 B_0 \rangle + \langle A_1 B_0 \rangle + \langle A_1 B_1 \rangle - \langle A_0 B_1 \rangle \leq 2$
3. Device-Independent QKD is the gold standard for secure key exchange, allowing information-theoretic security. It does not depend on the implementation of the device.
4. Performance of DI-QKD can be quantified by the key rate (# of reliable bits per unit time).

Motivation

Problem

Objective: We want to design a DI-QKD protocol with improved key rate by shifting basis.

Method: Using the same measurment settings for Alice and Bob.

Why does it improves the key rate?
Eavesdropper strategy for one measurment basis may not be the best for another basis, which makes it harder

How many measurement settings do we need? At least 3

lemma 1.1
If $\{p(ab|xy)\}$ is a non-local behavior such that Alice and Bob use the same measurements, where x ∈ X, y ∈ Y s.t. $|X| = |Y| = n$, then $n \geq 3$.

lemma 1.2
Local correlation polytope for 3-measurement settings is maximally violated by the simplex projections, where Alice and Bob use the same settings: $A_i = B_i \ \forall \ i \in \{0, 1, 2\}$.

lemma 1.1

$$\langle A_x B_y \rangle = \sum_{a,b\in\{-1,+1\}} ab\, P(ab|xy)$$

$$\langle A_x \rangle = \sum_{a\in\{-1,+1\}} a\, P(a|x)$$

$$\langle B_y \rangle = \sum_{b\in\{-1,+1\}} b\, P(b|y)$$

	B_0	$\mathbb{1} - B_0$	B_1	$\mathbb{1} - B_1$
A_0	$\frac{1}{2}$	0	T_1	$\frac{1}{2} - T_1$
$\mathbb{1} - A_0$	0	$\frac{1}{2}$	$\frac{1}{2} - T_1$	T_1
A_1	T_2	$\frac{1}{2} - T_2$	$\frac{1}{2}$	0
$\mathbb{1} - A_1$	$\frac{1}{2} - T_2$	T_2	0	$\frac{1}{2}$

$0 \le T_1, T_2 \le \frac{1}{2}$

Suppose $n = 2$. So, $A_1 = B_1$ and $A_2 = B_2$ as Alice and Bob use the same measurements. We can show the following correlation, under no-signalling constraints and the eq (1)

We will show that in the above case, CHSH is not violated and hence, 2 measurement settings with $A_1 = B_1$ and $A_2 = B_2$ is not enough.

$$\begin{aligned}
&\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \\
&= 1 + (4T_1 - 1) + (4T_2 - 1) - 1 \\
&= 4(T_1 + T_2) - 2 \\
&\le 2
\end{aligned}$$

CHSH is not violated by the above case and therefore, we need a minimum of 3 measurement settings. In the case of 3 measurement settings, we have the simplex bell inequality violation.

lemma 1.2

A Local behaviour $\{P(ab|xy)\}$ with 2-outcomes and 3 measurement settings will have 36 conditional probabilities.

Taking into account No-signaling constraints, it can be represented using 15 correlators in the correlator format.

$$\{\langle A_0\rangle, \langle A_1\rangle, \langle A_2\rangle, \langle B_0\rangle, ..., \langle A_0 B_0\rangle, ..., \langle A_2 B_2\rangle\}$$

$$\begin{aligned}\langle A_x\rangle &= P(+|x) - P(-|x) = 0\\ \langle B_y\rangle &= P(+|y) - P(-|y) = 0\\ \langle A_i B_i\rangle &= 1\end{aligned}$$

We project the polytope into lower dimension and solve it to get the following facets:

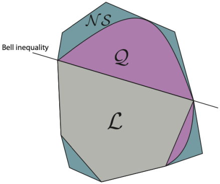
$$\begin{aligned}-\langle A_1 B_0\rangle - \langle A_2 B_0\rangle - \langle A_2 B_1\rangle &\leq 1\\ \langle A_1 B_0\rangle + \langle A_2 B_0\rangle - \langle A_2 B_1\rangle &\leq 1\\ \langle A_1 B_0\rangle - \langle A_2 B_0\rangle + \langle A_2 B_1\rangle &\leq 1\\ -\langle A_1 B_0\rangle + \langle A_2 B_0\rangle + \langle A_1 B_2\rangle &\leq 1\end{aligned}$$

lemma 1.2

We want to maximize the quantum violation. Using Born's rule, $\langle A_i B_j \rangle = \hat{n_i}.\hat{n_j}$ This leads to the following optimization problem, where

$$A_i = B_i = \hat{n_i}.\sigma = \cos\theta_i \cos\phi_i \sigma_x + \cos\theta_i \sin\phi_i \sigma_y + \sin\theta_i \sigma_z \quad \forall i$$

where $\sigma_x, \sigma_y, \sigma_z$ are Pauli matrices.



$$\max_{\hat{n_0},\hat{n_1},\hat{n_2}} -\hat{n_0}.\hat{n_1} - \hat{n_0}.\hat{n_2} - \hat{n_1}.\hat{n_2}$$

$$\text{where } \hat{n_1} = (1,0,0)$$
$$\hat{n_2} = (\cos\theta_1 \cos\phi_1, \cos\theta_1 \sin\phi_1, \sin\theta_1)$$
$$\hat{n_3} = (\cos\theta_2 \cos\phi_2, \cos\theta_2 \sin\phi_2, \sin\theta_2)$$

$$\iff \max_{\theta_1,\phi_1,\theta_2,\phi_2} -(\cos\theta_1 \cos\phi_1 + \cos\theta_2 \cos\phi_2 + \cos\theta_1 \cos\theta_2 \cos\phi_1 \cos\phi_2 + \cos\theta_1 \cos\theta_2 \sin\phi_1 \sin\phi_2 + \sin\phi_1 \sin\phi_2)$$

Solving the problem gives the simplex projections.

$$A_0 = B_0 = \sigma_z$$
$$A_1 = B_1 = \cos(\frac{2}{3}\pi)\sigma_z + \sin(\frac{2}{3}\pi)\sigma_x$$
$$A_2 = B_2 = \cos(\frac{4}{3}\pi)\sigma_z + \sin(\frac{4}{3}\pi)\sigma_x$$

Result and Methods

Finding the Simplex Bell Inequality

	B_0	$\mathbb{1} - B_0$	B_1	$\mathbb{1} - B_1$	B_2	$\mathbb{1} - B_2$
A_0	$\frac{1}{2}$	0	$\frac{1}{8}$	$\frac{3}{8}$	$\frac{1}{8}$	$\frac{3}{8}$
$\mathbb{1} - A_0$	0	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{1}{8}$	$\frac{3}{8}$	$\frac{1}{8}$
A_1	$\frac{1}{8}$	$\frac{3}{8}$	$\frac{1}{2}$	0	$\frac{3}{8}$	$\frac{1}{8}$
$\mathbb{1} - A_1$	$\frac{3}{8}$	$\frac{1}{8}$	0	$\frac{1}{2}$	$\frac{1}{8}$	$\frac{3}{8}$
A_2	$\frac{1}{8}$	$\frac{3}{8}$	$\frac{1}{8}$	$\frac{3}{8}$	$\frac{1}{2}$	0
$\mathbb{1} - A_2$	$\frac{3}{8}$	$\frac{1}{8}$	$\frac{3}{8}$	$\frac{1}{8}$	0	$\frac{1}{2}$

Probability Box for Simplex Measurmements on maximally entangled state.

Finding the Simplex Bell Inequality

From the lemma 1.2, we know that the Simplex Projections maximally violate the local correlation polytope. Now, we want to find a Bell Inequality that is maximally violated by the simplex projections.

Seesaw Method:

M matrix represents the co-efficients for the Bell Inequality.

$$\text{maximize } M.\hat{\pi}$$

$$\text{subject to } \text{M.P}^{L_i} \leq 1$$

Introduce additional constraint: $M.\hat{\pi} \geq M.p$ If required, we intoduce further additional constraints, e.g. $A_1 = B_1$

We get the maximum quantum violation for the specific M by solving the following problem using NPA Hierarchy Navascués et al. (2008) using QETLAB Johnston (2016).

$$\text{maximize } M.p$$

$$\text{subject to } \text{p} \in Q_{1+AB}$$

Other Methods:

1. Solving the following linear program using *Sequential Least Squares Programming (SLSQP)* (Gómez et al., 2021).
2. Let $\beta(P_q)$ and $\beta(P_c)$ be the Bell expressions for quantum correlation P_q and classical correlation P_c, respectively. We need to find a general Bell expression s.t.

$$\text{maximize } (\min\ (\beta(P_q) - \beta(P_c)))$$

Key Rate and Randomness

Bell Inequality:

$$\begin{aligned} B_q = {} & 2\langle A_0 B_0\rangle - 3\langle A_0 B_1\rangle - 3\langle A_0 B_2\rangle \\ & + 2\langle A_1 B_1\rangle - 3\langle A_1 B_0\rangle - 3\langle A_1 B_2\rangle \\ & + 2\langle A_2 B_2\rangle - 3\langle A_2 B_0\rangle - 3\langle A_2 B_1\rangle \leq 12 \end{aligned}$$

where Maximum local violation is 12 and maximum Quantum violation is 15

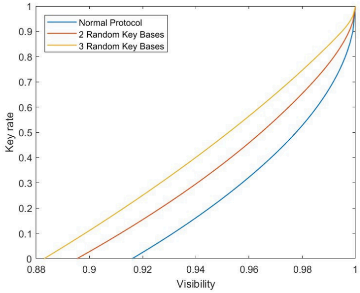


Figure: Key Rate

In order to calculate guessing probability, we will use the method in Acín et al. (2016) where we introduce a 3-outcome POVM A_3 on the Alice's side where each outcome corresponds to a guess on Bob's measurement.

$$P_{guess} = max \sum_{a \in \{0,1,2\}} P(a, (e = a)|x = 3)$$

$$\text{min-entropy} = \text{- } \log_2(P_{guess})$$

$$\mathrm{B}_q' = B_q - k \sum_{i=0}^{2} P(a = i, b = +1|x = 3, y = i) \leq 15$$

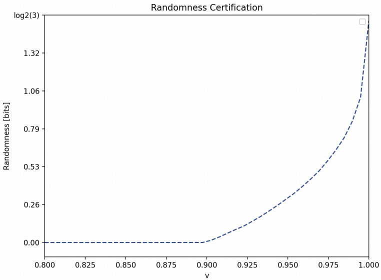


Figure: Min-Entropy Curve

Bell Inequality for Simplex Projectors of General d

Bell-Inequality for general d maximally violated by simplex projectors.

$$
\begin{aligned}
&d: \text{ dimension of the simplex projectors}\\
&n: \text{ number of settings of each player}\\
&n = \text{ d + 1}\\
&I = \sum_{i=1}^{n}\langle A_i B_i\rangle - \sum_{i,j=1;i\neq j}^{n}\langle A_i B_j\rangle - \frac{d^2-d-2}{d}(\sum_{i=1}^{n}\langle A_i\rangle + \sum_{j=1}^{n}\langle B_j\rangle)
\end{aligned}
$$

1. Allows to certify $\log(d+1)$ bits of randomness for d-dimensional quantum system.

Self-testing and SWAP Gate

Self-testing of states and measurements. Correlations $p(a,b|x,y)$ self-test the state and measurements $|\psi_{A'B'}\rangle, \{A_i^{'}\}, \{B_i^{'}\}$, if there exists a local isometry:

$$\Phi_A \otimes \Phi_B \otimes \mathbb{1}[A_i^{'} \otimes B_j^{'} \otimes \mathbb{1} |\psi_{AB}\rangle] = (A_i \otimes B_j |\phi^+\rangle) \otimes |\epsilon\rangle$$

How to show existence of an Isometry?

We show construction of the following Partial SWAP Gate.

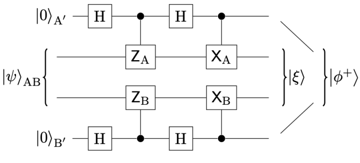


Figure: Partial SWAP gate isometry for self-testing Šupić and Bowles (2020)

Z_A, Z_B, X_A, X_B must satisfy the following properties:

1. $Z_A |\psi\rangle = Z_B |\psi\rangle$
2. $X_A |\psi\rangle = X_B |\psi\rangle$
3. $Z_A X_A |\psi\rangle = -X_A Z_A |\psi\rangle$
4. $Z_B X_B |\psi\rangle = -X_B Z_B |\psi\rangle$

SOS-Decompositions

Let Z and X operators be defined as follows:

$$Z_A = A_0 \qquad\qquad Z_B = B_0$$

$$X_A = \frac{A_1 - \cos\frac{2\pi}{3}A_0}{\sin\frac{2\pi}{3}} \qquad\qquad X_B = \frac{B_1 - \cos\frac{2\pi}{3}B_0}{\sin\frac{2\pi}{3}}$$

Show $Z_A\left|\psi\right\rangle = Z_B\left|\psi\right\rangle$.

It is equivalent to showing $(A_0 - B_0)\left|\psi\right\rangle = 0$ by simplification.
We perform SOS decomposition on the $I_B^{''}$ following: $I_B^{'} = I_B^{''} + \alpha(A_0 - B_0)^2 \succeq 0$ by solving it as an SDP with basis $\{A_0, A_1, A_2, B_0, B_1, B_2\}$, where $I_B^{'} = 15\mathbb{1} - B_q$ and x is the basis vector.

Results: Let $\alpha = 0.05$

$$I_B^{''} = Tr[(\sum_i \lambda_i \upsilon_i \upsilon_i^{\dagger})Q], \text{ where } Q = x.x^{\dagger}$$

$$\lambda_0 = 0.46617 \quad \lambda_1 = 4.5 \quad \lambda_2 = 4.93383 \quad \lambda_3 = 5.00000$$

$$\upsilon_0 = \begin{bmatrix} 0.41432 \\ 0.40518 \\ 0.40518 \\ -0.41432 \\ -0.40518 \\ -0.40518 \end{bmatrix} \upsilon_1 = \begin{bmatrix} 0.40825 \\ 0.40825 \\ 0.40825 \\ 0.40825 \\ 0.40825 \\ 0.40825 \end{bmatrix} \upsilon_2 = \begin{bmatrix} -0.57301 \\ 0.29297 \\ 0.29297 \\ 0.57301 \\ -0.29297 \\ -0.29297 \end{bmatrix} \upsilon_3 = \begin{bmatrix} 0 \\ -0.5 \\ 0.5 \\ 0 \\ 0.5 \\ -0.5 \end{bmatrix}.$$

SOS-Decomposition (continued)

Show $X_A |\psi\rangle = X_B |\psi\rangle$.

It is equivalent to showing $(A_1 - B_1)|\psi\rangle = 0$ by simplification.
We perform SOS decomposition on the I''_B following: $I'_B = I''_B + \alpha(A_1 - B_1)^2 \succeq 0$ by solving it as an SDP with basis $\{A_0, A_1, A_2, B_0, B_1, B_2\}$, where $I'_B = 15\mathbb{1} - B_q$ and x is the basis vector.

Results:

$$I''_B = Tr[(\sum_i \lambda_i v_i v_i^\dagger)Q], \text{ where } Q = x.x^\dagger$$

$$\lambda_0 = 0.46617 \quad \lambda_1 = 4.5 \quad \lambda_2 = 4.93383 \quad \lambda_3 = 5.00000$$

$$v_0 = \begin{bmatrix} -0.40518 \\ -0.41432 \\ -0.40518 \\ -0.40518 \\ -0.41432 \\ -0.40518 \end{bmatrix} v_1 = \begin{bmatrix} 0.40825 \\ 0.40825 \\ 0.40825 \\ 0.40825 \\ 0.40825 \\ 0.40825 \end{bmatrix} v_2 = \begin{bmatrix} -0.29297 \\ 0.57301 \\ -0.29297 \\ 0.29297 \\ -0.57301 \\ 0.29297 \end{bmatrix} v_3 = \begin{bmatrix} -0.5 \\ 0 \\ 0.5 \\ 0.5 \\ 0 \\ -0.5 \end{bmatrix}.$$

Show $Z_A X_A |\psi\rangle = -X_A Z_A |\psi\rangle$; $Z_B X_B |\psi\rangle = -X_B Z_B |\psi\rangle$

We show it using the properties of the operators.

Conclusion

Further Direction

1. Design the DI-QKD Protocol with shifting basis.
2. Find more robust Bell-Inequality for the general d.
3. Potentially, submit a research paper to *Quantum Journal*

Thanks to Prof. Ravishankar Ramanathan for the opportunity and guidance.

Thanks to Yuan Liu for her constant support.

Thanks to all the members of *Quantum Information and Computation Lab* for their support.

Reference

Acín, A., Pironio, S., Vértesi, T., and Wittek, P. (2016). Optimal randomness certification from one entangled bit. *Phys. Rev. A*, 93:040102.

Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V., and Wehner, S. (2014). Bell nonlocality. *Reviews of Modern Physics*, 86(2):419–478.

Gómez, S., Uzcátegui, D., Machuca, I., and et al. (2021). Optimal strategy to certify quantum nonlocality. *Scientific Reports*, 11:20489.

Johnston, N. (2016). QETLAB: A MATLAB toolbox for quantum entanglement, version 0.9. https://qetlab.com.

Navascués, M., Pironio, S., and Acín, A. (2008). A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013.

Zapatero, V., van Leent, T., Arnon-Friedman, R., Liu, W.-Z., Zhang, Q., Weinfurter, H., and Curty, M. (2023). Advances in device-independent quantum key distribution. *npj Quantum Information*, 9(1).

Šupić, I. and Bowles, J. (2020). Self-testing of quantum systems: a review. *Quantum*, 4:337.