Supplementary Materials: Low-Dimensional Reconciliation for Continuous-Variable Quantum Key Distribution

Laszlo Gyongyosi and Sandor Imre

S.1. Preliminaries

S.1.1. Spherical Code

A \( d \)-dimensional spherical code \( \mathcal{X} \) is defined over the \( d \)-dimensional unit sphere \( \Gamma^{d-1} \), given by \( \Gamma^{d-1} = \{ x = (x_0, x_1, \ldots, x_{d-1}) \in \mathbb{R}^d : \| x \| = 1 \} \), and \( \| x \| = 1 \) is the unit norm. The \( (d-1) \)-dimensional surface \( \mathcal{S}(\Gamma^{d-1}) \) of \( \Gamma^{d-1} \) is defined as \( \mathcal{S}(\Gamma^{d-1}) = 2\pi^{d/2}/\mathcal{G}(d/2) \), where \( \mathcal{G}(d/2) = \int_0^\infty t^{(d/2)-1}e^{-t}dt \) is the gamma function [24]. The number of codewords of the code is \( |\mathcal{X}| \), the smallest dimension \( d_{\text{min}} \) of any Euclidean space for the spherical code \( \mathcal{X} \) is \( d_{\text{min}} = \dim|\mathcal{X}| \), while the minimum distance between any two elements \( x \) and \( y \) of \( \mathcal{X} \subseteq \Gamma^{d-1} \), \( x \neq y \), is \( D = \min \{ \| x - y \| \} \).

S.1.2. Gaussian Random Spherical Vectors

Let \( \mathcal{X} = (X_0, \ldots, X_{d-1})^T \in \mathbb{R}^d \) be a Gaussian random vector with independent components, and with norm \( \| \mathcal{X} \| \) drawn from an \( \mathcal{N}(0, \sigma^2) \) memoryless Gaussian source. Over the \( d \)-dimensional unit sphere \( \Gamma^{d-1} \), spherical Gaussian random vector \( \mathcal{X} \in \Gamma^{d-1} \in \mathbb{R}^d \) has radius \( r = \mathbb{E}\| \mathcal{X} \| \) where \( \mathbb{E} \) is the mean of the norm \( \| \mathcal{X} \| \), defined [24] as

\[
\mathbb{E}\| \mathcal{X} \| = \frac{\sqrt{2\pi^d\mathcal{G}(\frac{d}{2})}}{\mathcal{G}(\frac{d-1}{2})} = \frac{\sqrt{2\pi^d}}{\mathcal{G}(\frac{d-1}{2})}
\]

(1)

where \( \beta(x, y) = \frac{\mathcal{G}(x)\mathcal{G}(y)}{\mathcal{G}(x+y)} \) is the beta function, while \( \mathbb{E}\| \mathcal{X} \|^k \) = \( d\sigma^2 \). The Gaussian random vector \( \mathcal{X} \in \mathbb{R}^d \) over \( \Gamma^{d-1} \) has a probability density function

\[
f(\mathcal{X}) = \frac{2^d\sigma^d\mathcal{G}(\frac{d}{2})}{\mathcal{G}(\frac{d-1}{2})(2\sigma^2)^d},
\]

(2)

and variance

\[
\text{var}[\mathcal{X}] = d\sigma^2 - \frac{2\pi\sigma^2}{\mathcal{G}(\frac{d+1}{2})}
\]

(3)

For \( d \to \infty \), \( \mathbb{E}\| \mathcal{X}/\sqrt{d\sigma^2} \| \to 1 \), and \( r = \lim_{d \to \infty} \mathbb{E}\| \mathcal{X}/\sqrt{d\sigma^2} \| \to 1 \). The distribution of \( r \) approximates the Dirac distribution \( \mathcal{P}_d(x) \), and gets to arbitrary close for \( d \to \infty \).

S.2. Notations

The notations of the manuscript are summarized in Table S1.
Table S1. Summary of the notations.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\varphi_i$</td>
<td>The first mode of the combined beam, phase space vector, where $x_{A,i}, x'<em>{B,i}$ and $p</em>{A,i}, p'_{B,i}$ are the position and momentum quadratures.</td>
</tr>
<tr>
<td>$\phi_i$</td>
<td>The second mode of the combined beam, phase space vector, transmitted to Bob, where $x_{A,i}, x'<em>{B,i}$ and $p</em>{A,i}, p'_{B,i}$ are the position and momentum quadratures.</td>
</tr>
<tr>
<td>$\xi_i$</td>
<td>The noisy version of phase space state $\left</td>
</tr>
</tbody>
</table>

$X$ Alice’s $N$-unit length raw data generated by $N$ random quadrature measurements. Binary string, consists of $N/d$ number of $d$-dimensional Gaussian random vectors $X_j \in \mathbb{R}^d$. 

$X'$ Bob’s $N$-unit length raw data generated by $N$ random quadrature measurements. Binary string, consists of $N/d$ number of noisy $d$-dimensional Gaussian random vectors $X'_j \in \mathbb{R}^d$. 

$X_i = x_{A,i} + x'_{B,i}$, $X_i = p_{A,i} + p'_{B,i}$ Alice’s raw data unit, obtained from a random quadrature measurement, where $x_{A,i}, x'_{B,i}$ and $p_{A,i}, p'_{B,i}$ are the position and momentum quadratures. 

$X'_i = x'_{A,i} + x''_{B,i}$, $X'_i = p'_{A,i} + p''_{B,i}$ Bob’s noisy raw data unit, obtained from a random quadrature measurement and by a correction $+2x_{B,i}$ or $+2p_{B,i}$, while $x'_{A,i}, x'_{B,i}$ and $p'_{A,i}, p'_{B,i}$ are the noisy position and momentum quadratures. 

$X_j \in \mathbb{R}^d : \{X_{j,0}, X_{j,1}, \ldots, X_{j,d-1}\}$ Alice’s $d$-dimensional Gaussian random vector ($d$ unit length Gaussian random vector), where $X_{j,i}$ is a Gaussian random variable. 

$X_{j,d} \in \mathbb{R}, \quad X'_{j,d} \in \mathbb{R}$ The $i$-th unit of $j$-th vector $X_j$ and $X'_j$. 

$X'_j \in \mathbb{R}^d : \{X'_{j,0}, X'_{j,1}, \ldots, X'_{j,d-1}\}$ Bob’s noisy $d$-dimensional Gaussian random vector ($d$ unit length vector), where $X'_{j,i} = x'_{A,i} + x''_{B,i}$ or $X'_{j,i} = p'_{A,i} + p''_{B,i}$ is a Gaussian random units obtained from a quadrature measurement. 

$K = \{U_0 \ldots U_{(N/d)-1}\} \in \mathbb{R}^{N/d}$, $U_j \in \{U_{j,0}, U_{j,1}, \ldots, U_{j,d-1}\} \in \mathbb{R}^d$, $U_j \in \{a, b\} \in \mathbb{R}$ Bob’s secret key vector. The full key is granulated into $N/d$ number of $U_j \in \mathbb{R}^d$ vectors. 

$X'_jU_j \in \mathbb{R}^d$ Bob’s $d$-dimensional vector sent to the classical channel. 

$X'_{j,d}U'_{j,d} \in \mathbb{R}$ A unit of Bob’s $d$-dimensional message sent to the classical channel. 

$C(\cdot)$ The Gaussian CDF function. 

$\mathcal{C}(\cdot)$ Covariance matrix. 

$\mathcal{D}_d(\cdot)$ Dirac distribution of a $d$-dimensional vector. 

$\mathcal{L}$ Lyapunov coefficient, $\mathcal{L} > 0$. 


$U'_j = \sum_{i=0}^{d-1} U'_{j,i}$

$U'_{j,i} = \left( C \left( X'_j U_j \right) U_j \right) \frac{1}{C(\lambda_i)}$

The noisy version of Bob's secret $U_j$, and its unit $U_{j,i}$.

$\delta_{j,i}$, $\delta'_{j,i}$

Noise on $U'_j = \sum_{i=0}^{d-1} U'_{j,i}$, and on unit $U_{j,i}$.

$\eta = \sqrt{\left( \sigma_{\delta_j}^2 \right)_d}$

Standard deviation of the noise vector $\delta_{j,i}$.

$\Lambda_j = \mathbb{N}\left(0,1\right)_d \in \mathbb{R}^d$, $\Lambda_{j,i} = \mathbb{N}\left(0,1\right) \in \mathbb{R}$

Standard Gaussian random noise vector, and the noise of the $i$-th unit of the $j$-th block $X_{j,i}$.

$\Delta_j = \mathbb{N}\left(0,\sigma_j^2\right)_d \in \mathbb{R}^d$

Gaussian random noise vector of the quantum channel $\mathcal{N}_2$ on $X_j$.

$\Delta_{j,i} = \mathbb{N}\left(0,\sigma_j^2\right) \in \mathbb{R}$

The $i$-th unit of $j$-th noise vector, that results raw data unit $X'_{j,i} = X_{j,i} + \Delta_{j,i}$.

### S.3. Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWGN</td>
<td>Additive White Gaussian Noise</td>
</tr>
<tr>
<td>BAWGN</td>
<td>Binary Additive White Gaussian Noise</td>
</tr>
<tr>
<td>BS</td>
<td>Beam Splitter</td>
</tr>
<tr>
<td>BSC</td>
<td>Binary Symmetric Channel</td>
</tr>
<tr>
<td>CDF</td>
<td>Cumulative Distribution Function</td>
</tr>
<tr>
<td>CLT</td>
<td>Central Limit Theorem</td>
</tr>
<tr>
<td>CV</td>
<td>Continuous-Variable</td>
</tr>
<tr>
<td>DPR</td>
<td>Differential Phase Reference</td>
</tr>
<tr>
<td>DV</td>
<td>Discrete-Variable</td>
</tr>
<tr>
<td>LDPC</td>
<td>Low Density Parity Check</td>
</tr>
<tr>
<td>PM</td>
<td>Prepare-and-Measure: entanglement-free protocol</td>
</tr>
<tr>
<td>RR</td>
<td>Reverse Reconciliation</td>
</tr>
<tr>
<td>SNR</td>
<td>Signal-to-Noise Ratio</td>
</tr>
</tbody>
</table>