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

S.1.2. Gaussian Random Spherical Vectors

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

$$\mathbb{E}\left[\left\| \mathfrak{X} \right\| \right] = \frac{\sqrt{2\sigma^2} \mathcal{G}\left(\frac{d+1}{2} \right)}{\mathcal{G}\left(\frac{d}{2} \right)} = \frac{\sqrt{2\pi\sigma^2}}{\beta\left(\frac{d}{2}, \frac{1}{2} \right)} \tag{1}$$

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

$$f\left(\mathfrak{X} \right) = \frac{2r^{d-1} e^{\frac{-r^2}{2\sigma^2}}}{\mathcal{G}\left(\frac{k}{2} \right) \left(2\sigma^2 \right)^{k/2}}, \tag{2}$$

and variance

$$\mathrm{var}\left[\mathfrak{X} \right] = d\sigma^2 - \frac{2\pi\sigma^2}{\beta^2\left(\frac{d}{2}, \frac{1}{2} \right)} \tag{3}$$

For $d \to \infty$, $\mathbb{E}\left\| \mathfrak{X} / \sqrt{d\sigma^2} \right\| \to 1$, and $r = \lim_{d \to \infty} \left\| \mathfrak{X} / \sqrt{d\sigma^2} \right\| \to 1$. The distribution of r approximates the Dirac distribution $\mathcal{D}_d\left(x \right)$, 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.

Notation	Description
$\left\|\varphi_i\right\rangle = \left\|x_{A,i} + x'_{B,i} + i\left(p_{A,i} + p'_{B,i}\right)\right\rangle$	The first mode of the combined beam, phase space vector, where $x_{A,i}, x'_{B,i}$ and $p_{A,i}, p'_{B,i}$ are the position and momentum quadratures.
$\left\|\phi_i\right\rangle = \left\|x_{A,i} - x'_{B,i} + i\left(p_{A,i} - p'_{B,i}\right)\right\rangle$	The second mode of the combined beam, phase space vector, transmitted to Bob, where $x_{A,i}, x'_{B,i}$ and $p_{A,i}, p'_{B,i}$ are the position and momentum quadratures.
$\left\|\xi_i\right\rangle = \left\|x'_{A,i} - x''_{B,i} + i\left(p'_{A,i} - p''_{B,i}\right)\right\rangle$	The noisy version of phase space state $\left\|\phi_i\right\rangle$, with the noisy quadratures.
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 $\mathbf{X}_j \in \mathbb{R}^d$.
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 $\mathbf{X}'_j \in \mathbb{R}^d$.
$X_i = x_{A,i} + x'_{B,i}$, $X_i = p_{A,i} + p'_{B,i}$	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.
$\mathbf{X}_j \in \mathbb{R}^d : \left\{X_{j,0}, X_{j,1}, \ldots X_{j,d-1}\right\}$	Alice's *d*-dimensional Gaussian random *vector* (*d* unit length Gaussian random vector), where $X_{j,i}$ is a Gaussian random variable.
$X_{j,i} \in \mathbb{R}$, $X'_{j,i} \in \mathbb{R}$	The *i*-th unit of *j*-th vector $\mathbf{X}_j$ and $\mathbf{X}'_j$.
$\mathbf{X}'_j \in \mathbb{R}^d : \left\{X'_{j,0}, X'_{j,1}, \ldots X'_{j,d-1}\right\}$	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.
$\mathbf{K} = \left\{\mathbf{U}_0, \ldots \mathbf{U}_{(N/d)-1}\right\} \in \mathbb{R}^{N/d}$, $\mathbf{U}_j = \left\{U_{j,0}, U_{j,1}, \ldots U_{j,d-1}\right\} \in \mathbb{R}^d$, $U_j \in \left\{a, b\right\} \in \mathbb{R}$	Bob's secret key vector. The full key is granulated into N/d number of $\mathbf{U}_j \in \mathbb{R}^d$ vectors.
$\mathbf{X}'_j \mathbf{U}_j \in \mathbb{R}^d$	Bob's *d*-dimensional vector sent to the classical channel.
$X'_{j,i} U_{j,i} \in \mathbb{R}$	A unit of Bob's *d*-dimensional message sent to the classical channel.
$C(\cdot)$	The Gaussian CDF function.
$\mathfrak{C}(\cdot)$	Covariance matrix.
$\mathcal{D}_d(\cdot)$	Dirac distribution of a *d*-dimensional vector.
$\mathfrak{L}$	Lyapunov coefficient, $\mathfrak{L} > 0$.

$U'_j = \sum_{i=0}^{d-1} U'_{j,i}$, $U'_{j,i} = \left(C\left(X'_{j,i}\right)U_{j,i}\right)\frac{1}{C\left(X_{j,i}\right)}$	The noisy version of Bob's secret U_j, and its unit $U_{j,i}$.
δ_j, $\delta_{j,i}$	Noise on $U'_j = \sum_{i=0}^{d-1} U'_{j,i}$, and on unit $U_{j,i}$.
$\eta = \sqrt{\left(\sigma^2_{\delta_j}\right)_d}$	Standard deviation of the noise vector $\vec{\delta}_j$.
$\Lambda_j = \mathbb{N}\left(0,1\right)_d \in \mathbb{R}^d$, $\Lambda_{j,i} = \mathbb{N}\left(0,1\right) \in \mathbb{R}$	Standard Gaussian random noise vector, and the noise of the *i*-th unit of the *j*-th block $X_{j,i}$.
$\Delta_j = \mathbb{N}\left(0,\sigma_2^2\right)_d \in \mathbb{R}^d$	Gaussian random noise vector of the quantum channel $\mathcal{N}_2$ on $\mathbf{X}_j$.
$\Delta_{j,i} = \mathbb{N}\left(0,\sigma_2^2\right) \in \mathbb{R}$	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

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