
Article:
Mountogiannakis, Alexander G. and Pirandola, Stefano (2026) Optimizing Epsilon Security Parameters in QKD. Physica Scripta. 325101. ISSN: 0031-8949

https://doi.org/10.1088/1402-4896/ae8db2

PAPER • **OPEN ACCESS**

Optimizing epsilon security parameters in QKD

To cite this article: Alexander G Mountogiannakis and Stefano Pirandola 2026 *Phys. Scr.* **101** 325101

Physica Scripta

PAPER

Optimizing epsilon security parameters in QKD

Alexander G Mountogiannakis[1,2] and Stefano Pirandola[1,*]

[1] Department of Computer Science, University of York, York YO10 5GH, United Kingdom
[2] nodeQ, 71-75 Shelton Street, Covent Garden, London WC2H 9JQ, United Kingdom
[*] Author to whom any correspondence should be addressed.

E-mail: stefano.pirandola@york.ac.uk

Keywords: QKD, quantum security, quantum cryptography, discrete variables, continuous variables, genetic optimization, composable security

OPEN ACCESS

RECEIVED
17 April 2026

REVISED
4 May 2026

ACCEPTED FOR PUBLICATION
14 July 2026

PUBLISHED
6 August 2026

Abstract

We investigate the optimization of ε-security parameters in quantum key distribution, aiming to improve the achievable secure key rate under a fixed overall composable security level. For this purpose, we employ a continuous genetic algorithm (CGA) to optimize the ε-security components of two representative protocols: the homodyne protocol from the continuous-variable family and the BB84 protocol from the discrete-variable family. We detail the CGA configuration, summarize the derivation of the composable key rate, and emphasize the role of the ε-parameters in both protocols. We then compare key rates obtained with optimized ε-values against those derived from standard and randomized choices. Our results demonstrate substantial key rate improvements at high security levels, where the key rate typically vanishes, and uncover positive-rate regimes that are inaccessible without optimization.

1. Introduction

Quantum key distribution (QKD) attempts to enable two parties to securely generate and share a secret cryptographic key by exploiting the principles of quantum mechanics [1–8] while being affected by a fundamental rate limitation [9, 10]. As the security of QKD is based on physics and not computational complexity, it is often described as providing "unconditional security" [11]. The original QKD paper was presented in 1984 [12] and, since then, the field has grown substantially, with numerous theoretical advancements, experimental implementations, and the development of multiple security proofs against various types of attacks. The field is generally divided into discrete-variable (DV) [13–21] and continuous-variable (CV) QKD [22–45].

Initially, QKD relied on the notion of the asymptotic key rate, which examines the protocol behavior, when an infinite number of quantum states are transmitted [14]. As the practical demonstration of QKD protocols unfolded, security solely in the asymptotic regime became obsolete. Finite-size effects, such as the number of generated states or the deviation between estimated and actual values, started to be incorporated into security proofs. However, these proofs remained incomplete, as practical implementations involve hidden imperfections in various components of the protocols that reduce their security. To mitigate the effects of these imperfections, the concept of composability was introduced to QKD [5].

Composability is associated with building systems, whose security is preserved, when protocols are composed with other protocols or used as components in larger applications [21]. In the context of quantum cryptographic systems, a protocol is ε-secure, when [5]

$$\mathcal{D} = (\rho_{ABE}, \sigma_{\mathrm{AB}} \otimes \rho_E) \leqslant \varepsilon, \tag{1}$$

where $\mathcal{D}$ is the trace distance [46], ρ_{ABE} is the joint output state of Alice, Bob, and Eve, and $\sigma_{\mathrm{AB}} \otimes \rho_E$ is the ideal secret state (describing two identical key strings completely decoupled from Eve).

2. Epsilon security in QKD

The epsilon security ε can be decomposed into individual parameters, found at various stages throughout the protocol, each associated with an imperfection. Typically, five components have been distinguished:

- **Parameter estimation (PE) error** $\varepsilon_{\mathrm{PE}}$. This is the probability that the estimated channel parameters do not belong in the marked out confidence region, laid out by the worst-case scenario estimators.
- **Entropy estimation error** $\varepsilon_{\mathrm{ent}}$. It is associated with the impact of finite samples on the entropy estimation of key generation sequences. This is only present in CV-QKD protocols.
- **Correctness** $\varepsilon_{\mathrm{cor}}$. It represents the hash collision probability of a family of universal hash functions used during the verification stage of error correction (EC). It is related to the probability of having different key strings after EC.
- **Smoothing error** ε_{s}. It quantifies how close the smoothed key distribution is allowed to be to the true one. In other words, it bounds the probability that the true state lies outside the neighborhood of size ε_{s} used for smoothing in the security analysis.
- **Hashing error** ε_{h}. This indicates the collision probability of the universal hash function used at the privacy amplification (PA) stage.

Note that the latter two parameters are included in the secrecy parameter $\varepsilon_{\mathrm{sec}}$, which characterizes the overall probability of failure associated with PA, i.e.

$$\varepsilon_{\mathrm{sec}} = \varepsilon_{\mathrm{s}} + \varepsilon_{\mathrm{h}}. \tag{2}$$

More specifically, the ε-secrecy parameter bounds the trace distance of the final state (after PA) from the ideal state, where Eve's is completely decoupled.

In CV-QKD protocols, the total epsilon security can be written as follows [43]

$$\varepsilon = 3\varepsilon_{\mathrm{PE}} + \varepsilon_{\mathrm{cor}} + \varepsilon_{\mathrm{sec}}, \tag{3}$$

where the factor 3 before $\varepsilon_{\mathrm{PE}}$ is due to the estimation of two different channel parameters, i.e. transmissivity and excess noise, plus to simplify the optimization process, we take the entropy estimation penalty as $\varepsilon_{\mathrm{ent}} = \varepsilon_{\mathrm{PE}}$. For the single-photon BB84, the epsilon security is

$$\varepsilon = \varepsilon_{\mathrm{PE}} + \varepsilon_{\mathrm{cor}} + \varepsilon_{\mathrm{sec}}. \tag{4}$$

3. Composable key rates

In this section, the review the composable secret key rate for both CV- and DV-QKD. We are interested in the conditional key rate, that is, the rate from a single block of a QKD session, assuming successful EC. The analysis can be easily extended to the unconditional key rate, where we average the performance by considering the probability of success of EC.

3.1. CV-QKD composable key rate

We consider CV-QKD with Gaussian-modulated coherent states (with variance μ_{sig}) and homodyne detection, with efficiency η and electronic noise ν_{el}. In our setting, the quantum channel between Alice and Bob is implemented by a fiber link. For a fiber of length L and attenuation A, the transmissivity is given by

$$T = 10^{-\frac{AL}{10}}. \tag{5}$$

To define the composable key rate R, we start with the asymptotic key rate as [43]

$$R_{\infty} = \beta I(\mathbf{x}:\mathbf{y}) - \chi(E:\mathbf{y}), \tag{6}$$

where β is the reconciliation efficiency (heuristically set to values $\leqslant 1$), $I(\mathbf{x}:\mathbf{y})$ is Alice and Bob's mutual information, and $\chi(E:\mathbf{y})$ is Eve's Holevo information on Bob's variable. With the introduction of estimators for the transmissivity $T \to \hat{T}$ and the excess noise $\xi \to \hat{\xi}$, obtained during the parameter estimation stage, the rate shown in equation (6) becomes

$$R_{\mathrm{PE}} = \beta I\left(\widehat{T},\widehat{\xi}\right) - \chi\left(T_{\mathrm{wc}},\xi_{\mathrm{wc}}\right), \tag{7}$$

where T_{wc} and ξ_{wc} denote the worst-case scenario estimators, provided by

$$T_{\mathrm{wc}} = \hat{T} - w\sigma_{\hat{T}},\ \xi_{\mathrm{wc}} = \hat{\xi} - w\sigma_{\hat{\xi}}. \tag{8}$$

Here, σ stands for the variance of the respective channel parameter and parameter w is related to the parameter estimation error by

$$w = \sqrt{2\ln\left(\frac{1}{\varepsilon_{\mathrm{PE}}}\right)}. \tag{9}$$

Given that m states are sacrificed for PE, i.e.

$$m = r_{\mathrm{PE}}N \tag{10}$$

where r_{PE} is the sacrificed state fraction for PE, only $n = N - m$ states will be used for key generation. This means that a factor n/N will multiply the key rate. The composable key rate is given by [47]

$$R = \frac{1}{N}\left(nR_{\mathrm{PE}} - F\right), \tag{11}$$

where F accounts for finite-size terms [48]

$$\begin{aligned} F = {} & \left(\sqrt{n}\log_2 n\right)\sqrt{2\ln\left(\frac{2}{\varepsilon_{\mathrm{PE}}}\right)} + 4\sqrt{n}\log_2\left(\sqrt{2^D}+2\right) \\ & \times\sqrt{\log_2\left(\frac{8}{\varepsilon_{\mathrm{sec}}^2}\right)} - \log_2\left(\frac{\varepsilon_{\mathrm{sec}}^2\varepsilon_{\mathrm{cor}}}{2}\right), \end{aligned} \tag{12}$$

with D being the discretization parameter, i.e. the number of bins used to map continuous quadrature outcomes to discrete values for key extraction. For a source with a repetition rate clk, measured in uses/sec, we can write a rate in bits/sec as

$$R \to \mathrm{clk}R. \tag{13}$$

3.2. DV-QKD composable key rate

In the single-photon BB84 protocol, the composable key rate in uses/sec is given by [47]

$$R = \kappa r. \tag{14}$$

To begin with, the transmissivity in equation (5) combines with the detector efficiency η to give the overall efficiency

$$\eta_{\mathrm{tot}} = \eta T. \tag{15}$$

In equation (14), κ stands for the raw key rate as

$$\kappa = (1 - r_{\mathrm{PE}})\, p_{\mathrm{sift}} Q_1, \tag{16}$$

where r_{PE} is the sacrificed state ratio for parameter estimation, p_{sift} is the sifting probability, calculated from the probability of the X-basis, p_X, as

$$p_{\mathrm{sift}} = p_X^2 + (1 - p_X)^2, \tag{17}$$

and Q_1 is Bob's detection probability, given by

$$Q_1 = \eta_{\mathrm{tot}} + (1 - \eta_{\mathrm{tot}})\, p_{\mathrm{dc}} \tag{18}$$

with p_{dc} denoting the dark-count probability.

Assuming a block of size $N = n + m$, where m points are for PE and n are used for key generation, the secret fraction r is given by

$$r = 1 - h\left(\tilde{E}\right) - f_{\mathrm{EC}} h\left(\hat{E}\right) + \frac{1 + \log_2\left(\varepsilon_{\mathrm{cor}}\varepsilon_{\mathrm{h}}^2\right)}{n} - \frac{\Delta_{\mathrm{AEP}}\left(\varepsilon_{\mathrm{s}}\right)}{\sqrt{n}}. \tag{19}$$

Here the asymptotic equipartition property (APE) term reads

$$\Delta_{\mathrm{AEP}}\left(\varepsilon_{\mathrm{s}}\right) = 7\sqrt{\log_2\left(\frac{2}{\varepsilon_{\mathrm{s}}}\right)}, \tag{20}$$

$f_{\mathrm{EC}} > 1$ is the reconciliation efficiency, and, finally, $\hat{E}$ and $\tilde{E}$ stand for the estimated and worst-case QBER respectively, with

$$\tilde{E} = \hat{E} + \sqrt{\frac{2}{m}\ln\left(\frac{m+1}{\varepsilon_{\mathrm{PE}}}\right)}. \tag{21}$$

To convert R into a rate in bits per second, both the repetition rate clk and the detector dead time t_{dt} must be taken into account, as

$$R \to c_{\mathrm{dt}}\mathrm{clk}R, \tag{22}$$

where c_{dt} is a reduction factor accounting for the detector dead time, given by

$$c_{\mathrm{dt}} = \frac{1}{1 + Q_1 t_{\mathrm{dt}}\mathrm{clk}}. \tag{23}$$

4. The continuous genetic algorithm (CGA)

The CGA [49–51] is an evolutionary optimization technique inspired by natural selection. It generalizes the traditional genetic algorithm by allowing parameters to take continuous values, making it well-suited for optimal control problems.

4.1. General description

In this framework, a chromosome is a candidate solution represented as a vector of continuous parameters. The quality of each chromosome is measured by a fitness function, which encodes the objective of the optimization. The algorithm evolves a population of chromosomes over successive generations through the following steps:

- **Initialization**: Randomly generate an initial population of candidate solutions.
- **Selection**: Evaluate the fitness of each chromosome and retain the best-performing ones.
- **Pairing**: Select pairs of parent chromosomes probabilistically according to fitness, ensuring fitter candidates reproduce more often.
- **Crossover (Mating)**: Combine parent parameters to generate offspring by forming weighted mixtures of the parent values. In the CGA, unlike in discrete genetic algorithms, these weights are typically chosen randomly from the interval $[0, 1]$. This allows the offspring to explore not only the parameter values present in the parents, but also any continuous value between them. This way, the search space is expanded.
- **Mutation**: Randomly replace some parameter values with new random values to maintain diversity and avoid local optima.
- **Elitism**: The best chromosome is preserved unchanged to guarantee non-decreasing maximum fitness across generations.

This iterative process continues until convergence or until a satisfactory fitness level is reached. As the CGA is inherently stochastic, it cannot guarantee the identification of the global optimal value in a finite amount of time. However, it reliably improves candidate solutions, as generations progress.

4.2. Algorithm formulation

Depending on the protocol of interest, the security parameters $\varepsilon_{\mathrm{PE}}$, $\varepsilon_{\mathrm{cor}}$ and $\varepsilon_{\mathrm{sec}}$ must satisfy a total epsilon security constraint. For CV-QKD, this constraint is shown in equation (3), while for DV-QKD it is given in equation (4). In our setting, only the $\varepsilon_{\mathrm{PE}}$ and $\varepsilon_{\mathrm{cor}}$ components are treated as optimization variables. The $\varepsilon_{\mathrm{sec}}$ component is reconstructed from the input ε plus the two security components. It is important to emphasize that the choice of optimization variables is irrelevant to the optimization problem, because the security parameters are constrained by a single linear condition and any two of them uniquely determine the third. Therefore, optimizing over $\varepsilon_{\mathrm{PE}}$ and $\varepsilon_{\mathrm{cor}}$ while solving for $\varepsilon_{\mathrm{sec}}$ is fully equivalent to optimizing over all three variables, subject to the same constraint.

In practice, the genetic algorithm operates in a normalized search space. A chromosome is described by a vector $\mathbf{C}$ of two normalized components (the 'genes') p_1 and p_2, i.e.

$$\mathbf{C} = (p_1, p_2) \in [-1, 1]^2 .$$

The genes are mapped to the physical domain by the linear transformation

$$x_i = \frac{p_i + 1}{2} (b_i - a_i) + a_i, \tag{24}$$

where $x_i \in [a_i, b_i]$ is the physical parameter associated with the gene p_i. In particular, we have $x_1 = \varepsilon_{\mathrm{PE}}$ and $x_2 = \varepsilon_{\mathrm{cor}}$. In our application, each of these physical parameters falls within the range $[a_i, b_i] = [10^{-21}, \varepsilon)$.

Each chromosome $\mathbf{C}$ is assigned a fitness value, defined as the secret key rate produced by the corresponding QKD model. Formally, the fitness function is

$$f(\mathbf{C}) = R\left(\varepsilon_{\mathrm{PE}}, \varepsilon_{\mathrm{cor}}, \varepsilon_{\mathrm{sec}}\right), \tag{25}$$

where the key rate R is computed on the physical variables $\varepsilon_{\mathrm{PE}}$ and $\varepsilon_{\mathrm{cor}}$, together with the value of $\varepsilon_{\mathrm{sec}}$ resulting from the relevant epsilon security constraint.

More specifically, for each generation with population size N_{pop}, the CGA consists of the following steps:

1. **Initialization:** We randomly generate each chromosome $\mathbf{C}$, by choosing its genes p_1 and p_2 from a uniform distribution over $[-1, 1]^2$.
2. **Evaluation:** For each chromosome, we map the genes into the physical parameters $x_1 = \varepsilon_{\mathrm{PE}}$ and $x_2 = \varepsilon_{\mathrm{cor}}$ according to equation (24) where the range is determined by the input epsilon security ε. The additional epsilon parameter $\varepsilon_{\mathrm{sec}}$ is built in such a way to satisfy the relevant constraint, expressed by equation (3) or (4). If this constraint is violated (e.g. this may happen when $\varepsilon_{\mathrm{PE}}$ and $\varepsilon_{\mathrm{cor}}$ are too close to $\varepsilon_{\mathrm{sec}}$), the chromosome is assigned the worst possible fitness value and therefore effectively discarded during selection.
3. **Selection:** For each chromosome, we compute the value of the fitness function according to equation (25). Then, the chromosomes are sorted by order of fitness and the top

$$N_{\mathrm{parents}} = \lfloor N_{\mathrm{pop}} \rho_{\mathrm{parent}} \rfloor \tag{26}$$

individuals create the parent pool. Here, ρ_{parent} stands for the parent selection rate. Then, the number of parents that survive onto the next generation can be determined by

$$N_{\mathrm{survivors}} = \max\left\{1, \lfloor N_{\mathrm{parents}} \rho_{\mathrm{survival}} \rfloor\right\}, \tag{27}$$

where ρ_{survival} is the survival rate.

4. **Pairing:** From the parent pool, mother–father pairs $(\mathbf{C}^{(m)}, \mathbf{C}^{(f)})$ are drawn using fitness-proportional softmax sampling. A mother chromosome $\mathbf{C}^{(m)}$ is randomly selected from the parent pool according to the softmax distribution

$$\Pr(m = j) = \frac{e^{f_j}}{\sum_{k=1}^{N_{\mathrm{parents}}} e^{f_k}}, \tag{28}$$

where $f_j := f(\mathbf{C}^{(j)})$ is the fitness of the jth chromosome $\mathbf{C}^{(j)}$. For each chosen mother, the father is sampled from the parent pool according to a conditional softmax distribution obtained by excluding the mother, i.e.

$$\Pr(f = j \mid m) = \frac{e^{f_j}}{\sum_{k=1,k\neq m}^{N_{\text{parents}}} e^{f_k}}, \tag{29}$$

where $j \neq m$. This ensures that the two parents in each pair are distinct while still favoring higher-fitness individuals. Note that higher-fitness chromosomes are more likely, but not guaranteed, to be selected.

5. **Crossover:** Offspring chromosomes are generated in the normalized domain $[-1,1]$ by forming convex combinations of the parent genes $\mathbf{C}^{(m)} = (p_1^m, p_2^m)$ and $\mathbf{C}^{(f)} = (p_1^f, p_2^f)$. For each offspring and each gene index i,

$$p_i = \begin{cases} \gamma\, p_i^{(m)} + (1-\gamma)\, p_i^{(f)} & \text{with } \Pr = \frac{1}{2}, \\ p_i^{(m)} & \text{otherwise}, \end{cases} \tag{30}$$

where each γ is sampled independently from the uniform distribution on $(0,1)$.

6. **Mutation and Elitism:** With rate ρ_{mutation}, the normalized genes p_i of the newly generated offspring and the surviving parents are perturbed by adding Gaussian noise with mean 0 and standard deviation 0.2. The mutated values are then clipped to remain in the range $[-1,1]$, which means that any value larger than 1 is set to 1 and any value smaller than -1 is set to -1 [52]. Mutation is applied to prepare candidate solutions for the next iteration. However, the best chromosome in the population is excluded from mutation and is carried over unchanged to the next generation. At least one chromosome must be preserved.

Steps 2–6 of this process are repeated for a set number of iterations N_{iter} to produce an approximate maximizer of the key rate R. After N_{iter} iterations, the optimization outcome is the best chromosome, for which we provide the value of the fitness (the highest fitness) and also the values of the optimal/near-optimal physical parameters.

4.3. Suitability

Various optimization techniques have previously been used in QKD parameter studies, including local numerical search methods, joint scanning strategies, machine-learning-based parameter prediction, and numerical security-proof-based optimization frameworks [53–56]. Here, the CGA is chosen not because it is claimed to be universally superior over all optimization methods, but because the present ε-allocation problem is nonlinear, threshold-sensitive, and not naturally suited to gradient-based or analytical optimization [57]. Although the admissible ε-security domain is defined by a simple linear budget constraint, the corresponding composable finite-size key rate depends on the constituent ε-parameters through logarithmic corrections, square-root finite-size terms, and worst-case estimators. In stringent-security regimes, small changes in the allocation of the constituent terms may determine whether the resulting key rate is positive or effectively zero. We stress that this optimization does not alter the underlying security definition or relax the security level; it only redistributes a fixed total ε-budget among the ε-constituent terms. For this reason, the CGA provides a fast, convenient, and derivative-free framework across different protocol models.

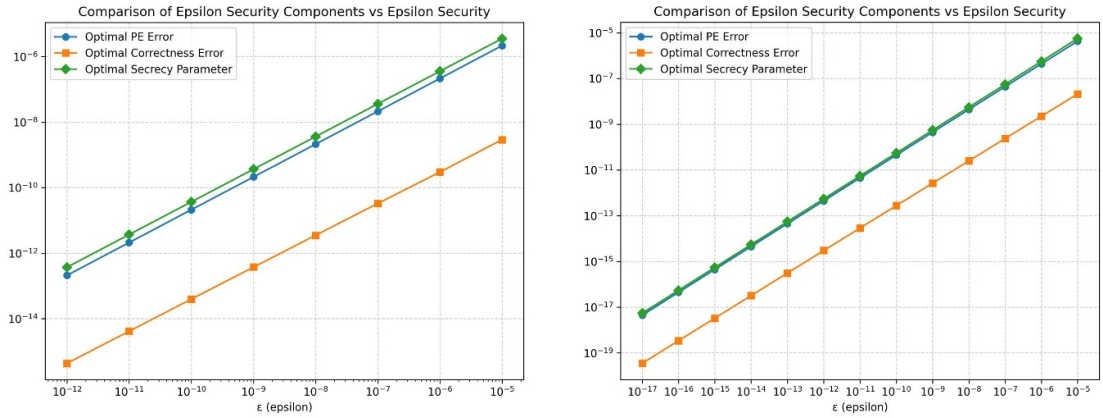
5. Case studies

For all simulations, the following optimization parameters were used in the CGA:

- Population Size $N_{\text{pop}} = 200$
- Iterations $N_{\text{iter}} = 300$
- Mutation Rate $\rho_{\text{mutation}} = 0.5$
- Parent Rate $\rho_{\text{parent}} = 0.5$
- Survival Rate $\rho_{\text{survival}} = 1$

Table 1. Representative computational cost of the CGA optimization for the CV-QKD and DV-QKD case studies.

Item/Quantity	CV-QKD	DV-QKD
CPU model	AMD EPYC 7763 (8 vCPUs)	
Implementation language	Python 3.10	
Population size N_{pop}	200	
Maximum generations N_{iter}	300	
Fitness evaluations per run	6×10^4	
Approximate runtime per fitness evaluation (ms)	0.2	0.1
Average runtime per generation (ms)	40	20
Typical stabilization generation range	20–40	20–50



(a) CV-QKD homodyne protocol. (b) DV-QKD BB84 protocol.

Figure 1. Optimized epsilon security component values vs. epsilon security, for CV-QKD and DV-QKD protocols. For both figures, both axes are plotted on a logarithmic scale.

Our practical observations indicate that these values are sufficient to achieve optimal outcomes. Increasing the number of iterations or the population size yields negligible improvement, while considerably slowing down the simulation.

Given that each run requires approximately $N_{\text{pop}}N_{\text{iter}} = 6 \times 10^4$ fitness evaluations, the computational cost is low, and a complete optimization run is typically finished in a few seconds on standard CPU hardware. More specifically, the implementation was carried out in Python 3.10 and executed on an AMD EPYC 7763 with 8 vCPUs. The approximate runtime per fitness evaluation was found to be 0.2 ms for the CV-QKD case and 0.1 ms for the DV-QKD case. These times correspond to average runtimes per generation of about 40 ms and 20 ms, respectively (see also table 1). We define stabilization as the stage where the best-so-far secret key rate improves by less than 10^{-2} bits/sec over 20 consecutive generations. Under this criterion, optimizations for both protocols typically began to stabilize after about 20 generations. However, the maximum generation budget was conservatively set to $N_{\text{iter}} = 300$, in order to maintain a uniform stopping rule across all runs and to accommodate the small late-stage improvements observed in some cases.

5.1. Epsilon optimization in CV-QKD

For any fixed epsilon security ε, we compare the rate from the optimized parameters ε_{PE}, ε_{cor} and ε_{sec} with that from two other cases (one symmetric and the other asymmetric, randomly chosen):

- when $\varepsilon_{\text{PE}} = \varepsilon_{\text{cor}} = \varepsilon_{\text{sec}} = \frac{\varepsilon}{5}$ and
- when $\varepsilon_{\text{PE}} = \frac{\varepsilon}{10}$, $\varepsilon_{\text{cor}} = \frac{2\varepsilon}{5}$ and $\varepsilon_{\text{sec}} = \frac{3\varepsilon}{10}$.

Both sets satisfy equation (3). The values used for the epsilon security range from $\varepsilon = 10^{-12}$ to 10^{-5} in steps of one order of magnitude. The resulting optimized epsilon parameters are plotted for these security levels in figure 1(a). It is noteworthy that the optimal values of ε_{PE} and ε_{sec} are extremely close, while ε_{cor} is consistently smaller by about two orders of magnitude across all security levels. The rest of the input parameters and their respective values are listed in table 2.

Table 2. Input parameters for the CV-QKD homodyne protocol.

Parameter	Description	Value
L	Channel length (km)	4
A	Fiber attenuation (dB/km)	0.2
η	Detector efficiency	0.85
ξ	Excess Noise	0.01
v_{el}	Electronic Noise	0.1
μ_{sig}	Signal Variance	25
N	Total number of pulses	4×10^5
β	Reconciliation efficiency (<1)	0.95
D	Discretization Parameter	7
r_{PE}	PE ratio	0.3
clk	Repetition rate (Hz)	1×10^9

Table 3. Input parameters for the DV-QKD protocol (single-photon BB84).

Parameter	Description	Value
L	Channel length (km)	100
A	Fiber attenuation (dB/km)	0.2
η	Detector efficiency	0.92
E	Quantum bit error rate	$\approx$0.05
p_X	X-basis state probability	0.5
N	Total number of pulses	3×10^7
p_{dc}	Dark count probability	1×10^{-3}
f_{EC}	Reconciliation efficiency (>1)	1.25
r_{PE}	PE state ratio	0.25
clk	Repetition rate (Hz)	2×10^9
t_{dt}	Detector dead-time (s)	2×10^{-6}

The rate results are displayed in figure 2(a). As seen in the figure, the percentage increase is much higher when the security is also higher, i.e. at lower ε. For very low ε values, the absolute advantage in the key rate that we obtained by optimizing is minimal. However, as the key rate is closer to zero, even a tiny absolute improvement translates into a large relative percentage gain. By contrast, when the baseline key rate is already high, the change is negligible in percentage terms.

This effect is depicted more clearly in figure 2(b), where we focus on the interval from 10^{-13} to 10^{-12} in order to closely examine the behavior in this region. Within this range, the benefits of optimization are evident: it significantly outperforms the case of the randomly-chosen asymmetric parameters and shows a substantial improvement compared to the 'division by 5' approach. Moreover, for $\varepsilon = 4 \times 10^{-13}$ and 5×10^{-13} optimization yields positive rates, which are unattainable in the other two scenarios. At $\varepsilon = 5 \times 10^{-13}$, our optimized approach provides a key rate of about 2 Mbit/s instead of zero.

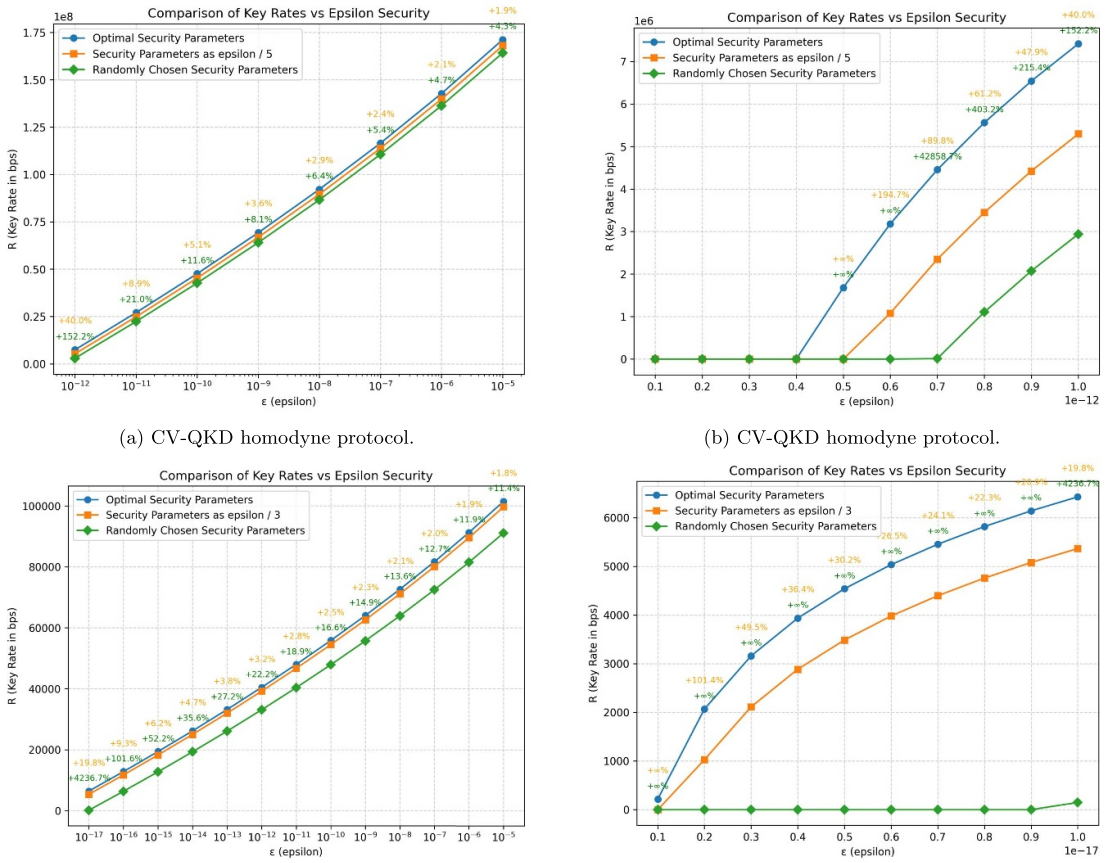
5.2. Epsilon optimization in DV-QKD

We will compare the key rate produced by the optimal epsilon parameters with the rates of two additional sets of suboptimal parameters that satisfy equation (4), i.e.

- $\varepsilon_{\text{PE}} = \varepsilon_{\text{cor}} = \varepsilon_{\text{sec}} = \frac{\varepsilon}{3}$ and
- $\varepsilon_{\text{PE}} = \frac{5\varepsilon}{99.5}$, $\varepsilon_{\text{cor}} = \frac{90\varepsilon}{99.5}$, $\varepsilon_{\text{sec}} = \frac{4.5\varepsilon}{99.5}$.

A comprehensive table of all input parameters that we used can be found in table 3. All results are evaluated for a long channel distance of $L = 100$ km. The examined security region spans from $\varepsilon = 10^{-17}$ to 10^{-5} in decade steps. The values of the optimized epsilon parameters for every security level are shown in figure 1(b). Similarly to the CV-QKD case, the optimal values of ε_{PE} and ε_{sec} are nearly identical for every level of ε. In contrast, ε_{cor} remains on the order of 10^{-2} times the values of ε_{PE} and ε_{sec} across the entire security range.

The composable rate R results are shown in figure 2(c). Again, simply dividing the ε-parameters by a common factor produces results that are close to optimal, though optimization provides a slight improvement. As the key rate approaches zero, optimization achieves increasingly greater percentage gains. This trend becomes particularly evident, when examining the region from 10^{-18} to 10^{-17},



(a) CV-QKD homodyne protocol.

(b) CV-QKD homodyne protocol.

(c) DV-QKD BB84 protocol.

(d) DV-QKD BB84 protocol.

Figure 2. Composable key rate (bits/sec) vs. epsilon security, for CV-QKD and DV-QKD protocols. For (a) and (c), the x-axis is plotted on a logarithmic scale. For (b) and (d), the x-axis is plotted on a linear scale.

as shown in figure 2(d). There, the set of optimized ε-parameters is the only one capable of achieving a positive rate at $\varepsilon = 10^{-18}$. For security levels from $\varepsilon = 2 \times 10^{-18}$, the equal values set for the epsilon security constituents can also achieve a positive rate, although it is much smaller. In contrast, the randomly-chosen asymmetric parameters achieve a positive rate only at $\varepsilon = 10^{-17}$, showing the importance of optimization in this context.

6. Conclusion

We have presented an application of a CGA for the optimization of composable security parameters in QKD protocols. In our formulation, each chromosome encodes three ε-security parameters, specifically the parameter estimation error $\varepsilon_{\mathrm{PE}}$, the correctness error $\varepsilon_{\mathrm{cor}}$ and the secrecy parameter $\varepsilon_{\mathrm{sec}}$ within their admissible domain, and the fitness function is given by the secret key rate R. This setting allows us to systematically explore the parameter space and identify configurations that maximize the key rate for fixed overall epsilon security.

For both CV-QKD and DV-QKD BB84 protocols, the same effects were observed by optimizing the ε-parameters. The optimized values of $\varepsilon_{\mathrm{PE}}$ and $\varepsilon_{\mathrm{sec}}$ are nearly identical, whereas $\varepsilon_{\mathrm{cor}}$ remains notably smaller at every considered security level. In addition, while already high key rates at high values of ε-security do not benefit significantly, rates at lower values of ε-security can experience massive improvements. Here ε-parameter optimization can achieve positive rates in regimes where a random or a standard choice fail.

Acknowledgments

UKRI supported this work through the Integrated Quantum Networks (IQN) Research Hub (EPSRC, Grant No. EP/Z533208/1).

Data availability statement

The data cannot be made publicly available upon publication because they contain commercially sensitive information. The data that support the findings of this study are available upon reasonable request from the authors.

ORCID iDs

Alexander G Mountogiannakis 0000-0003-1864-5643
Stefano Pirandola 0000-0001-6165-5615

References

[1] Pirandola S *et al* 2020 Advances in quantum cryptography *Adv. Opt. Photon.* **12** 1012–236
[2] Xu F, Ma X, Zhang Q, Lo H-K and Pan J-W 2020 Secure quantum key distribution with realistic devices *Rev. Mod. Phys.* **92** 025002
[3] Tomamichel M A 2012 Framework for non-asymptotic quantum information theory *PhD Thesis Zurich* (arXiv:1203.2142)
[4] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 The security of practical quantum key distribution *Rev. Mod. Phys.* **81** 1301–50
[5] Renner R 2005 Security of quantum key distribution *PhD Dissertation* ETH Zürich
[6] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography *Rev. Mod. Phys.* **74** 145
[7] Usenko V C *et al* 2025 Continuous-variable quantum communication (arXiv:2501.12801)
[8] Fletcher A I, Harney C, Ghalaii M, Papanastasiou P, Mountogiannakis A, Spedalieri G, Hajomer A A E, Gehring T and Pirandola S 2025 An overview of CV-MDI-QKD *Rep. Prog. Phys.* **88** 084001
[9] Pirandola S, García-Patrón R, Braunstein S L and Lloyd S 2009 Direct and reverse secret-key capacities of a quantum channel *Phys. Rev. Lett.* **102** 050503
[10] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 Fundamental limits of repeaterless quantum communications *Nat. Commun.* **8** 15043
Pirandola S, Laurenza R, Ottaviani C, and Banchi L, Fundamental limits of repeaterless quantum communications 2015 (arXiv:1510.08863)
[11] Mayers D 2001 Unconditional security in quantum cryptography *J. ACM* **48** 351–406
[12] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (IEEE)* pp 175–9
[13] Ekert A K 1991 Quantum cryptography based on Bell's theorem *Phys. Rev. Lett.* **67** 661–3
[14] Shor P W and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol *Phys. Rev. Lett.* **85** 441–4
[15] Gottesman D and Lo H-K 2003 Proof of security of quantum key distribution with two-way classical communications *IEEE Trans. Inf. Theory* **49** 457–75
[16] Kraus B, Gisin N and Renner R 2005 Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication *Phys. Rev. Lett.* **95** 080501
[17] Renner R, Gisin N and Kraus B 2005 Information-theoretic security proof for quantum-key-distribution protocols *Phys. Rev. A* **72** 012332
[18] Lim C C W, Curty M, Walenta N, Xu F and Zbinden H 2014 Concise security bounds for practical decoy-state quantum key distribution *Phys. Rev. A* **89** 022307
[19] Portmann C and Renner R 2014 Cryptographic security of quantum key distribution (arXiv:1409.3525)
[20] Yin H L, Zhou M G, Gu J, Xie Y M, Lu Y S and Chen Z B 2020 Tight security bounds for decoy-state quantum key distribution *Sci. Rep.* **10** 14312
[21] Canetti R 2020 Universally composable security *J. ACM* **67** 28
[22] Ralph T C 1999 Continuous variable quantum cryptography *Phys. Rev. A* **61** 010303(R)
[23] Hillery M 2000 Quantum cryptography with squeezed states *Phys. Rev. A* **61** 022309
[24] Cerf N J, Levy M and Van Assche G 2001 Quantum distribution of Gaussian keys using squeezed states *Phys. Rev. A* **63** 052311
[25] Ralph T C 2000 Security of continuous-variable quantum cryptography *Phys. Rev. A* **62** 062306
[26] Grosshans F and Grangier P 2002 Continuous variable quantum cryptography using coherent states *Phys. Rev. Lett.* **88** 057902
[27] Navascues M, Grosshans F and Acin A 2006 Optimality of Gaussian attacks in continuous-variable quantum cryptography *Phys. Rev. Lett.* **97** 190502
[28] Pirandola S, Braunstein S L and Lloyd S 2008 Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography *Phys. Rev. Lett.* **101** 200504
[29] Leverrier A and Grangier P 2010 Simple proof that Gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a Gaussian modulation *Phys. Rev. A* **81** 062314
[30] Leverrier A, Grosshans F and Grangier P 2010 Finite-size analysis of a continuous-variable quantum key distribution *Phys. Rev. A* **81** 062343
[31] Leverrier A, Alléaume R, Boutros J, Zémor G and Grangier P 2010 Multidimensional reconciliation for a continuous-variable quantum key distribution *Phys. Rev. A* **81** 062343
[32] Ruppert L, Usenko V C and Filip R 2014 Long-distance continuous-variable quantum key distribution with efficient channel estimation *Phys. Rev. A* **90** 062310
[33] Usenko V C and Grosshans F 2015 Unidimensional continuous-variable quantum key distribution *Phys. Rev. A* **92** 062337
[34] Leverrier A 2015 Composable security proof for continuous-variable quantum key distribution with coherent states *Phys. Rev. Lett.* **114** 070501
[35] Usenko V C and Filip R 2016 Trusted noise in continuous-variable quantum key distribution: a threat and a defense *Entropy* **18** 20

[36] Zhang Y *et al* 2020 Long-distance continuous-variable quantum key distribution over 202.81 km of fiber *Phys. Rev. Lett.* **125** 10502
[37] Leverrier A 2017 Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction *Phys. Rev. Lett.* **118** 200501
[38] Pirandola S 2021 Limits and security of free-space quantum communications *Phys. Rev. Res.* **3** 013279
[39] Pirandola S 2021 Composable security for continuous-variable quantum key distribution: trust levels and practical key rates in wired and wireless networks *Phys. Rev. Res.* **3** 043014
[40] Mountogiannakis A G, Papanastasiou P, Braverman B and Pirandola S 2022 Composably secure data processing for Gaussian-modulated continuous-variable quantum key distribution *Phys. Rev. Res.* **4** 013099
[41] Mountogiannakis A G, Papanastasiou P, Braverman B and Pirandola S 2022 Data postprocessing for the one-way heterodyne protocol under composable finite-size security *Phys. Rev. A* **106** 042606
[42] Papanastasiou P, Mountogiannakis A G and Pirandola S 2023 Composable security of CV-MDI-QKD with secret key rate and data processing *Sci. Rep.* **13** 11636
[43] Pirandola S and Papanastasiou P 2024 Improved composable key rates for CV-QKD *Phys. Rev. Res.* **6** 023321
[44] Mele F A, Lami L and Giovannetti V 2025 Maximum tolerable excess noise in continuous-variable quantum key distribution and improved lower bound on two-way capacities *Nat. Photon.* **19** 329–34
[45] Usenko V C *et al* 2026 Continuous-variable quantum communication *Rev. Mod. Phys.* **98** 015003
[46] Simeone O 2026 *Classical and Quantum Information Theory: Uncertainty, Information and Correlation* (Cambridge University Press)
[47] Pirandola S, Harney C and Spedalieri G 2025 Security-rate trade-off in quantum key distribution: from individual links to large-scale networks
[48] This rate can be written under the assumptions of $\varepsilon_{\rm s} = \varepsilon_{\rm h} = \varepsilon_{\rm sec}/2$ and $\varepsilon_{\rm PE} = \varepsilon_{\rm ent}$
[49] Chelouah R and Siarry P 2000 A continuous genetic algorithm designed for the global optimization of multimodal functions *J. Heuristics* **6** 191–213
[50] Bunnag D and Sun M 2005 Genetic algorithm for constrained global optimization in continuous variables *Appl. Math. Comput.* **171** 604–36
[51] Brown J, Paternostro M and Ferraro A 2023 Optimal quantum control via genetic algorithms for quantum state engineering in driven-resonator mediated networks *Quantum Sci. Technol.* **8** 025004
[52] Note that, because mutation takes place in the normalized domain, where the constraints in equations (3) or (4) are not enforced, infeasible physical parameters may arise after mapping. Such chromosomes are detected during the evaluation step of the next iteration and effectively discarded by being assigned the worst possible fitness value.
[53] Jiang C, Yu Z-W, Hu X-L and Wang X-B 2021 Higher key rate of measurement-device-independent quantum key distribution through joint data processing *Phys. Rev. A* **103** 012402
[54] Wang W and Lo H-K 2019 Machine learning for optimal parameter prediction in quantum key distribution *Phys. Rev. A* **100** 062334
[55] Xu F, Xu H and Lo H-K 2014 Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution *Phys. Rev. A* **89** 052333
[56] Kanitschar F and Pacher C 2022 Optimizing continuous-variable quantum key distribution with phase-shift keying modulation and postselection *Phys. Rev. Appl.* **18** 034073
[57] Arqub O A and Abu-Hammour Z S 2014 Numerical solution of systems of second-order boundary value problems using continuous genetic algorithm *Inf. Sci.* **279** 396–415