Robust Interior Point Method for Quantum Key Distribution Rate Computation

Hao Hu[1], Jiyoung Im[1], Jie Lin[2], Norbert Lütkenhaus[2] and Henry Wolkowicz[1]

1 Department of Combinatorics and Optimization, Faculty of Mathematics, University of Waterloo, Waterloo, ON, Canada N2L 3G1

2 Institute for Quantum Computing and Department of Physics & Astronomy, University of Waterloo, Waterloo, ON, Canada N2L 3G1

Our paper [1] is available on arXiv: 2104.03847. Code is available at https://www.math.uwaterloo.ca/~hwolkowi/henry/reports/ZGNQKDmainsolverUSEDforPUBLCNJuly31/.

INTRODUCTION

Security proof methods for quantum key distribution (QKD) based on numerical key rate calculation [2] can be powerful in principle. However, the practicality of the methods are limited by computational resources and the efficiency and accuracy of the underlying algorithms for convex optimization.

BACKGROUND: Numerical Security Proof Method

Asymptotic key rate:

$$R^{\infty} = p_{\text{pass}}[\min_{\rho \in S} H(\mathbf{Z}|\mathbf{E}) - \boldsymbol{\delta}_{\mathbf{EC}}]$$

Devetak-Winter formula [3]

$$= \min_{\rho_{AB} \in S} D(\mathcal{G}(\rho_{AB}) || \mathcal{Z}(\mathcal{G}(\rho_{AB}))) - p_{\text{pass}} \boldsymbol{\delta}_{\mathbf{EC}}$$

Ref. [2]

where $\boldsymbol{\delta}_{\mathbf{EC}}$ is the cost of error correction per signal and $D(\cdot \,||\, \cdot)$ is the quantum relative entropy function.

Key rate optimization:

minimize $D(\mathcal{G}(\rho_{AB}) || \mathcal{Z}(\mathcal{G}(\rho_{AB})))$

subject to: $\mathbf{Tr}[\rho_{AB} \Gamma_i] = \gamma_i$ → observational constraints & reduced density operator constraints

$\rho_{AB} \geq \mathbf{0}, \mathbf{Tr}[\rho_{AB}] = \mathbf{1}$ → ρ_{AB} is a density operator

$\mathcal{G}(\sigma) = \sum_i \boldsymbol{K}_i \sigma \boldsymbol{K}_i^{\dagger}$: completely positive map that models postprocessing steps of a QKD protocol

$\mathcal{Z}(\sigma) = \sum_j \boldsymbol{Z}_j \sigma \boldsymbol{Z}_j$: a quantum pinching channel that is related to key map of the protocol. Each $\boldsymbol{Z}_j$ is a projector.

MOTIVATION

- Previous formulation is ill-posed and numerically challenging: optimal solution is usually on boundary of SDP cone.
- We aim at a reliable, efficient numerical method for calculating key rates for QKD protocols.

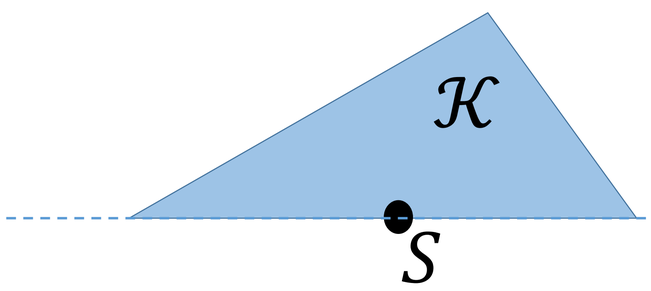
OUR CONTRIBUTIONS

We utilize the accumulated experience within the field of numerical convex optimization to reformulate the problems in order to obtain faster converging, stable approaches for solving the given convex optimization problem numerically. Our work is reported in Ref. [1]. Specifically, we

- Regularize the problem using **facial reduction** on both constraints and nonlinear objective
- Apply **Gauss-Newton interior point** approach on regularized problem
- Avoid the perturbation approach used in previous works to get $\rho_{AB} > \mathbf{0}$
- Provide theoretically proven lower bounds

BACKGROUND: Facial Reduction

Facial reduction is a general technique to preprocess an optimization problem.



Facial reduction finds a subspace $\mathcal{H}$ containing our feasible set S that intersects the (semidefinite) cone $\mathcal{K}$

Figure reproduced from [4]

We use facial reduction to remove redundant constraints and redundant unknown variables that always take a fixed value (in particular zero) in the entire feasible set.

BACKGROUND: Interior-Point Method

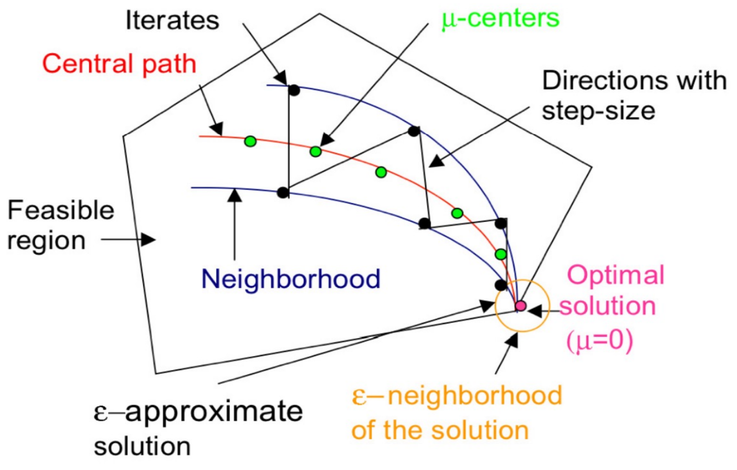


Figure taken from [5]

ALGORITHM FEATURES

- Based on a standard primal-dual interior-point approach applied to the facial reduced problem
- Modify the primal feasibility to use a nullspace representation
- Use a projected Gauss-Newton search direction to account for overdetermined least squares problem arising from the optimality conditions
- Exploit the exact feasibility of linear constraints after a step length one for the Gauss-Newton method
- Use a modified form of the dual to obtain a lower bound along with an upper bound from the objective function to stop the algorithm when the duality gap is provably small

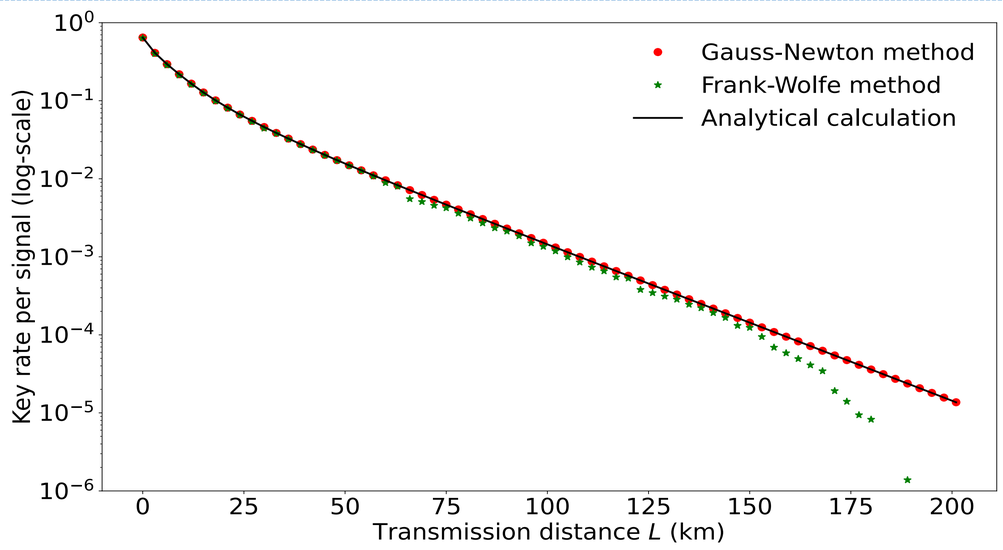
NUMERICAL TESTS

Problem Data			Gauss-Newton		Frank-Wolfe with FR		Frank-Wolfe w/o FR		cvxquad with FR	
protocol	parameter	size	gap	time	gap	time	gap	time	gap	time
ebBB84	(0.50,0.05)	(4,16)	5.98e-13	0.63	1.01e-04	84.39	1.17e-04	94.71	5.46e-01	216.37
ebBB84	(0.90,0.07)	(4,16)	2.33e-13	0.25	2.32e-04	85.09	2.54e-04	113.20	7.39e-01	647.60
pmBB84	(0.50,0.05)	(8,32)	5.51e-13	0.24	3.13e-05	1.85	6.47e-04	1.47	5.26e-01	170.12
pmBB84	(0.90,0.07)	(8,32)	1.01e-12	0.17	7.31e-05	1.04	6.25e-04	31.77	6.84e-01	235.89
mdiBB84	(0.50,0.05)	(48,96)	7.86e-13	1.08	9.62e-05	1.54	5.39e-04	134.79	1.82e-01	588.71
mdiBB84	(0.90,0.07)	(48,96)	2.96e-13	1.12	1.51e-04	101.84	3.48e-03	408.26	4.57e-01	574.31
TFQKD	(0.80,100,0.70)	(12,24)	7.67e-13	1.20	1.98e-04	96.08	1.55e-03	179.57	3.98e-03	990.92
TFQKD	(0.90,200,0.70)	(12,24)	3.42e-12	0.96	1.92e-05	2.07	1.65e-04	2.15	2.26e-04	875.44
DMCV	(10,60,0.05,0.35)	(44,176)	2.74e-09	510.66	2.44e-06	1015.14	3.36e-06	1709.65	**	0.86
DMCV	(11,120,0.05,0.35)	(48,192)	3.23e-09	720.61	2.60e-06	348.81	1.98e-06	628.25	**	1.24
dprBB84	(1,0.08,30)	(12,48)	4.92e-13	0.93	3.79e-06	77.86	9.38e-05	108.50	**	119.20
dprBB84	(2,0.14,30)	(24,96)	1.04e-12	10.07	6.19e-06	15.61	3.62e-06	27.79	**	105.40
dprBB84	(3,0.10,30)	(36,144)	4.96e-13	61.32	6.48e-04	7.89	2.08e-02	28.46	**	614.71
dprBB84	(4,0.12,30)	(48,192)	1.13e-12	272.09	4.41e-05	15.28	9.79e-04	184.42	**	3397.34

- ebBB84(p_z,e): entanglement-based qubit BB84 protocol with the probability p_z to choose Z basis and error rate e.
- pmBB84(p_z,e): prepare & measure qubit BB84 protocol with the probability p_z to choose Z basis and error rate e.
- mdiBB84 (p_z,p): qubit-based MDI BB84 protocol with the probability p_z to choose Z basis; simulation is done a qubit depolarizing channel with depolarizing probability p.
- TFQKD(q, L, p_x): Protocol 1 of Ref. [6]. The parameter q is the probability that a source emits single photons. L the distance between Alice and Bob. The parameter q is the probability to choose x basis.
- DMCV(N_c,L, ξ,α): Discrete-modulated CVQKD [7] with a photon-number cutoff N_c, transmission distance L, channel excess noise ξ and coherent-state amplitude α.
- dprBB84(c, α, L): discrete-phase-randomized weak-coherent-pulse BB84 [8] with c discrete global phases, coherent-state amplitude α and transmission distance L.

Size refers to the dimensions of $\boldsymbol{\rho_{AB}}$ and $\mathcal{G}(\boldsymbol{\rho_{AB}})$.
Gauss-Newton is our algorithm applied to the facial reduced problem. Frank-Wolfe is the algorithm in Ref. [2] either with our facial reduction formulation or without. The header cvxquad with FR refers to the algorithm provided by [9] with facial reduction formulation. ** indicates that a certain algorithm fails to give a reasonable answer within a reasonable amount of time. See our paper [1] for more details.

Gauss-Newton performs significantly better in terms of accuracy of the results and running time in most cases.



Comparison of key rate for discrete-modulated continuous-variable QKD among our Gauss-Newton method [1], the Frank-Wolfe method [2] and analytical key rate [7] for the noise = 0 case.

FUTURE DIRECTIONS

- The algorithm can still be improved. For example, one may combine the Hessian calculation from [10] with our method.
- We would like to extend our algorithm to perform the finite key analysis [11].

REFERENCES

[1] H. Hu, J. Im, J. Lin, N. Lütkenhaus and H. Wolkowicz, arXiv: 2104.03847
[2] A. Winick, N. Lütkenhaus, and P. J. Coles, Quantum 2, 77 (2018), arXiv: 1710.05511
[3] I. Devetak and A. Winter, Proc. R. Soc. A 461, 207 (2005), arXiv: quant-ph/0306078
[4] F. N. Permenter, PhD thesis, MIT, Cambridge, MA, USA (2017)
[5] G. Lesaja, The Open Operational Research Journal 3, 1-12 (2009)
[6] M. Curty, K. Azuma, and H.-K. Lo, npj. Quantum Inf. 5, 64 (2019)
[7] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Phys. Rev. X 9, 041064 (2019), arXiv: 1905.10896
[8] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, New J. Phys. 17, 053014, (2015)
[9] H. Fawzi, J. Saunderson, and P.A. Parrilo. Foundations of Computational Mathematics 19, 259-296 (2019). Package cvxquad at https://github.com/hfawzi/cvxquad.
[10] L. Faybusovich and C. Zhou, arXiv:1906.00037
[11] I. George, J. Lin and N. Lütkenhaus, Phys. Rev. Research 3, 013274, arXiv: 2004.11865

Discovery Grants Program: Grant No. 341495
Collaborative Research and Development Program, Grant No. CRDP J 522308-17

Financial support for this work has been partially provided by Huawei Technologies Canada Co., LTD.