JMCS
Journal of Mathematics and Computer Science

All Fields | Paper Title | Author | Search

Efficient and verifiable outsourcing computation of large-scale nonlinear programming

Volume 21, Issue 4, pp 335--343

http://dx.doi.org/10.22436/jmcs.021.04.06 (http://dx.doi.org/10.22436/jmcs.021.04.06)

Publication Date: May 15, 2020

Submission Date: January 09, 2020

Revision Date: February 04, 2020

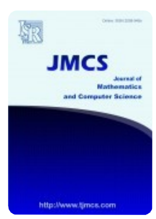
Accteptance Date: April 08, 2020

Download PDF (https://www.isr-publications.com/jmcs/8780/download-efficient-and-verifiable-outsourcing-computation-of-large-scale-nonlinear-programming)

Download XML (https://www.isr-publications.com/jmcs/articles-8780-efficient-and-verifiable-outsourcing-computation-of-large-scale-nonlinear-programming/xml)

Check for updates

Export citations



Authors

Nedal M. Mohammed (mailto:dr.nedal.mohammed@gmail.com)
- Department of Computer Science, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, India.

Ali N. AL-Seadi
- Department of Computer Science, Thi-Qar University, Thi-Qar, Iraq.

Santosh S. Lomte
- Department of Computer Science, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, India.

Poonam M. Rokade
- Department of Computer Science, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, India.

Ahmed A. Hamoud
- Department of Mathematics, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, India.

Abstract

Nonlinear programming (NLP) problems arise in various fields, such as transport, financial engineering, logistics, urban planning, supply chain management, and power system control. Solving large-scale NLPs are usually so computationally expensive for resource-constrained users within a feasible time. The cost-effective solution is computation outsourcing, but this raises security concerns such as the input and output privacy of the customers, and cheating behaviors of the cloud since NLP problems always carry sensitive information. In this paper, we develop a practical secure and verifiable schema for solving outsourcing large-scale (NLP) with the GRG method. Also, we apply approximate KKT conditions for verifying the optimality of the result returned by the GRG algorithm. We implement the proposed schema on the customer side laptop and using AWS compute domain elastic compute cloud (EC2) for the cloud side.

Share and Cite

ISRP Style

Nedal M. Mohammed, Ali N. AL-Seadi, Santosh S. Lomte, Poonam M. Rokade, Ahmed A. Hamoud, Efficient and verifiable outsourcing computation of large-scale nonlinear programming, Journal of Mathematics and Computer Science, 21 (2020), no. 4, 335--343

AMA Style

Mohammed Nedal M., AL-Seadi Ali N., Lomte Santosh S., Rokade Poonam M., Hamoud Ahmed A., Efficient and verifiable outsourcing computation of large-scale nonlinear programming. J Math Comput SCI-JM. (2020); 21(4):335--343

Chicago/Turabian Style

Mohammed, Nedal M., AL-Seadi, Ali N., Lomte, Santosh S., Rokade, Poonam M., Hamoud, Ahmed A.. "Efficient and verifiable outsourcing computation of large-scale nonlinear programming." Journal of Mathematics and Computer Science, 21, no. 4 (2020): 335--343

Keywords

Cloud computing | *secure computation outsourcing* | *verifiable computing* | *security and privacy nonlinear programming problems*

MSC

68Q99 **90C30**

References

[1] R. Andreani, G. Haeser, J. M. Martinez, On sequential optimality conditions for smooth constrained optimization, Optimization, 60 (2011), 627--641
View Article (https://doi.org/10.1080/02331930903578700) **MathSciNet** (http://www.ams.org/mathscinet-getitem?mr=2801388)
Google Scholar (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=On+sequential+optimality+conditions+for+smooth+constrained+optimization&btnG=)
MATH (https://zbmath.org/?q=an%3A1225.90123)

[2] E. B. Bajalinov, Linear-fractional programming theory, methods, applications and software, Springer Science & Business Media, Berlin (2013)

Google Scholar (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Linear-fractional+programming+theory%2C+methods%2C+applications+and+software&btnG=)
MATH (https://zbmath.org/?q=an%3A1067.90154)

[3] M. S. Bazaraa, H. D. Sherali, C. M. Shetty, Nonlinear programming: theory and algorithms, John Wiley & Sons, New York (2013)
View Article (https://books.google.com/books?hl=en&lr=&id=nDYz-NIpIuEC&oi=fnd&pg=PT10&dq=Nonlinear+programming:+theory+and+algorithms&ots=qNnV-grizg&sig=a0lksFOMH2GMWAXgIEAfnZGoIKg)
Google Scholar (https://scholar.google.com/scholar?cluster=2560831763233758074&hl=en&as_sdt=0,5)

[4] D. P. Bertsekas, Nonlinear programming, Athena scientific, Belmont (1999)
MathSciNet (http://www.ams.org/mathscinet-getitem?mr=3444832)
Google Scholar (https://scholar.google.com/scholar?as_q=&as_epq=Nonlinear+programming&as_oq=&as_eq=&as_occt=title&as_sauthors=Bertsekas&as_publication=&as_ylo=&as_yhi=&hl=en&as_sdt=0%2C5)
MATH (https://zbmath.org/?q=an%3A1015.90077)

[5] J. Dutta, K. Deb, R. Tulshyan, R. Arora, Approximate KKT points and a proximity measure for termination, J. Glob. Optim., 56 (2013), 1463--1499
View Article (https://doi.org/10.1007/s10898-012-9920-5) **MathSciNet** (http://www.ams.org/mathscinet-getitem?mr=3078314)
Google Scholar (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Approximate+KKT+points+and+a+proximity+measure+for+termination&btnG=)
MATH (https://zbmath.org/?q=an%3A1297.90150)

[6] C. Gentry, Computing arbitrary functions of encrypted data, Comm. ACM, 53 (2010), 97--105
View Article (https://doi.org/10.1145/1666420.1666444)
Google Scholar (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Computing+arbitrary+functions+of+encrypted+data&btnG=)
MATH (https://zbmath.org/?q=an%3A1315.94074)

[7] A. A. Hamoud, K. H. Hussain, N. M. Mohammed, K. P. Ghadle, Solving Fredholm integro-differential equations by using numerical techniques, Nonlinear Funct. Anal. Appl., 24 (2019), 533--542
View Article (http://nfaa.kyungnam.ac.kr/journal-nfaa/index.php/NFAA/article/view/1202)
Google Scholar (https://scholar.google.com/scholar?cluster=14633388168661900218&hl=en&as_sdt=0,5)
MATH (https://zbmath.org/?q=an%3A07132873)

[8] A. A. Hamoud, N. M. Mohammed, K. P. Ghadle, A study of some effective techniques for solving Volterra-Fredholm integral equations, Dyn. Contin. Discrete Impuls. Syst. Ser. A Math. Anal., 26 (2019), 389--406
View Article (http://online.watsci.org/abstract_pdf/2019v26/v26n6a-pdf/2.pdf)
MathSciNet (http://www.ams.org/mathscinet-getitem?mr=4043528)
Google Scholar (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=A+study+of+some+effective+techniques+for+solving+Volterra-Fredholm+integral+equations&btnG=)
MATH (https://zbmath.org/?q=an%3A07162576)

[9] C. Hu, A. Alhothaily, A. Alrawais, X. Cheng, C. Sturtivant, H. Liu, A secure and verifiable outsourcing scheme for matrix inverse computation, IEEE INFOCOM'17 (Atlanta, GA, U.S.A.), 4 (2017), 2304--2312
View Article (https://ieeexplore.ieee.org/abstract/document/8057199/)
Google Scholar (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=A+secure+and+verifiable+outsourcing+scheme+for+matrix+inverse+computation&btnG=)

[10] K. H. Hussain, A. A. Hamoud, N. M. Mohammed, Some new uniqueness results for fractional integro-differential equations, Nonlinear Funct. Anal. Appl., 24 (2019), 827--836
View Article (http://www.academia.edu/download/61493958/1238-3667-1-PB20191212-70309-ebw24u.pdf)
Google Scholar (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=allintitle%3A+%22Some+new+uniqueness+results+for+fractional+integro-differential+equations%22&btnG=)
MATH (https://zbmath.org/?q=an%3A07178041)

[11] J. Katz, Y. Lindell, Introduction to modern cryptography, CRC press, Boca Raton (2015)
View Article (https://books.google.com/books?hl=en&lr=&id=OWZYBQAAQBAJ&oi=fnd&pg=PR2&dq=Introduction+to+modern+cryptography&ots=BcsiwPS_20&sig=J8yyZXyTNozk5EHteZGNmCIKQDk)
MathSciNet (http://www.ams.org/mathscinet-getitem?mr=3287369)
Google Scholar (https://scholar.google.com/scholar?cluster=9960286068443096605&hl=en&as_sdt=0,5)

MATH (https://zbmath.org/?q=an%3A1323.94001)

[12] A. Li, W. Du, Q. Li, Privacy-preserving outsourcing of large-scale nonlinear programming to the cloud, Int. Conf. Security Privacy Comm. Syst. (Springer), 2018 (2018), 569--587
View Article (https://link.springer.com/chapter/10.1007/978-3-030-01701-9_31)
Google Scholar (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Privacy-preserving+outsourcing+of+large-scale+nonlinear+programming+to+the+cloud&btnG=)

[13] D. G. Luenberger, Y. Ye, Linear and nonlinear programming, Springer, New York (2008)
View Article (https://link.springer.com/content/pdf/10.1007/978-3-319-18842-3.pdf)
MathSciNet (http://www.ams.org/mathscinet-getitem?mr=2423726)
Google Scholar (https://scholar.google.com/scholar?cluster=12564808631807863828&hl=en&as_sdt=0,5)

[14] N. M. Mohammed, S. S. Lomte, Recent advances on secure computations outsourcing in cloud computing, Asian J. Math. Comput. Res., 24 (2017), 192--205
View Article (http://ikprress.org/index.php/AJOMCOR/article/view/1069)
Google Scholar (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Recent+advances+on+secure+computations+outsourcing+in+cloud+computing&btnG=)

[15] N. M. Mohammed, S. S. Lomte, Secure computations outsourcing of mathematical optimization and linear algebra tasks: Survey, National Conference on Recent Innovation in Computer Science & Electronics, 2019 (2019), 6 pages
View Article (https://pdfs.semanticscholar.org/0466/9589fa05b2a50f06b900a70a9aa43b5e8468.pdf)
Google Scholar (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Secure+computations+outsourcing+of+mathematical+optimization+and+linear+algebra+tasks%3A+Survey&btnG=)

[16] N. M. Mohammed, S. S. Lomte, Secure and efficient outsourcing of large scale linear fractional programming, Adv. Intel. Syst. Comput., 2020 (2020), 277--286
View Article (https://link.springer.com/chapter/10.1007/978-981-32-9515-5_26)
Google Scholar (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Secure+and+efficient+outsourcing+ +of+large+scale+linear+fractional+programming&btnG=)

[17] N. M. Mohammed, S. S. Lomte, Verifiable secure computation of linear fractional programming using certificate validation, Int. J. Power Electron. Drive Syst., 11 (2020), 284--290
View Article (http://search.proquest.com/openview/eefaee9f1d309fb8439eb90c0936c3da/1?pq-origsite=gscholar&cbl=1686343)
Google Scholar (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Verifiable+secure+computation+of+linear+fractional+programming+ +using+certificate+validation&btnG=)

[18] N. M. Mohammed, L. Sultan, S. S. Lomte, Privacy preserving outsourcing algorithm for two-point linear boundary value problems, Indonesian J. Ele. Eng. Comput. Sci., 16 (2019), 1065--1069
Google Scholar (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Privacy+preserving+outsourcing+algorithm+for+two-point+linear+boundary+value+problems&btnG=)

[19] J. B. Rosen, The gradient projection method for nonlinear programming. I: Linear constraints, J. Soc. Indust. Appl. Math., 8 (1960), 181--217
View Article (https://doi.org/10.1137/0108011) **MathSciNet** (http://www.ams.org/mathscinet-getitem?mr=112750)
Google Scholar (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=The+gradient+projection+method+for+nonlinear+programming.+ +Part+I%3A+Linear+constraints&btnG=)
MATH (https://zbmath.org/?q=an%3A0099.36405)

[20] J. B. Rosen, The gradient projection method for nonlinear programming. II. Nonlinear constraints, J. Soc. Indust. Appl. Math., 9 (1961), 514--532
View Article (https://doi.org/10.1137/0109044) **MathSciNet** (http://www.ams.org/mathscinet-getitem?mr=135991)
Google Scholar (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=The+gradient+projection+method+for+nonlinear+programming.+ +Part+I%3A+Linear+constraints&btnG=)
MATH (https://zbmath.org/?q=an%3A0231.90048)

[21] W. Shen, B. Yin, X. H. Cao, Y. Cheng, X. S. Shen, A distributed secure outsourcing scheme for solving linear algebraic equations in ad hoc clouds, IEEE Trans. Cloud Comput., 4 (2017), 415--430
View Article (https://doi.org/10.1109/TCC.2016.2647718)
Google Scholar (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=A+distributed+secure+outsourcing+scheme+for+solving+linear+algebraic+equations+in+ad+hoc+clouds&btnG=)

[22] R. Tulshyan, R. Arora, K. Deb, J. Dutta, Investigating EA solutions for approximate KKT conditions in smooth problems, Proceedings of Annual Conference on Genetic and Evolutionary Computation, 2010 (2010), 689--696
View Article (https://dl.acm.org/doi/abs/10.1145/1830483.1830609)
Google Scholar (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Investigating+EA+solutions+for+approximate+KKT+conditions+in+smooth+problems&btnG=)

[23] K. Zhou, J. Ren, CASO: Cost-aware secure outsourcing of general computational problems, IEEE Tran. Services Comput., 2018 (2018), 13 pages
View Article (https://doi.org/10.1109/TSC.2018.2814991)
Google Scholar (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Cost-aware+secure+outsourcing+of+general+computational+problems&btnG=)