3rd International Conference on

Cryptography, Cyber Security and Information Warfare

(3rd CryCybIW)

Hellenic Military Academy

26th -27th May 2016

Abstracts

Editor: Nicholas J. Daras

Cryptographic Techniques for Secure Linear Computations in the Supply Chain Management

Iris-Pandora Krommyda[1], Gerasimos C. Meletiou[2],
Demetrius S. Triantafyllou[3] and Michael N. Vrahatis[4]

[1] Department of Business Administration of Food and Agricultural Enterprises,
University of Western Greece, GR-30100 Agrinio, Greece,
E-mail: ikrommyd@cc.uoi.gr

[2]A.T.E.I. of Epirus, P.O.110, GR-47100 Arta, Greece,
E-mail: gmelet@teiep.gr

[3]Department of Mathematics and Engineering Sciences, Hellenic Military Academy,
Vari, GR-16673, Greece
E-mail: dtriant@math.uoa.gr

[4]Computational Intelligence Laboratory, Department of Mathematics,
University of Patras, GR-26110 Patras, Greece,
E-mail: vrahatis@math.upatras.gr [4]

Key words: *supply chain management • optimization • linear programming • secure linear computations*

Abstract Optimization problems encountered in a supply chain can often be modeled as linear programming problems, whose objective function and constraints combine data from several parties. However, this approach requires private data and sensitive information that the involved parties are often unwilling and hesitant to exchange and reveal to each other. In order to tackle these two conflicting goals, namely, the information sharing and protecting confidentiality, various cryptographic techniques for secure linear computations have been developed. These techniques ensure that the several parties can compute any function without any party to disclose its input to another. An overview of various efficient techniques for securely solving linear programming problems is presented. □

References

[1] B. Boutsinas, G.C. Meletiou and M.N. Vrahatis: *Mining encrypted data*, in **Supply Chain and Finance**, P.M. Pardalos, A. Migdalas and G. Baourakis (eds.), Chapter 16, pp.273–281, World Scientific Publishing (Computers and Operations Research series, vol. 2), River Edge, NJ, U.S.A., 2004

[2] O. Catrina and S. de Hoogh: *Secure multiparty linear programming using fixed-point arithmetic*, Lecture Notes in Computer Science 6345(2010), pp. 134–150

[3] R. Cramer and I. Damgård: *Secure distributed linear algebra in a constant number of rounds*, Lecture Notes in Computer Science 2139(2001), pp. 119–136

[4] Y. Hong and J. Vaidya: *An inference-proof approach to privacy-preserving horizontally partitioned linear programs*, Optimization Letters 8(1)(2014), pp. 267–277

[5] Y. Hong and J. Vaidya and H.-B. Lu: *Secure and efficient distributed linear programming*, Journal of Computer Security 20(2012), pp. 583–634

[6] Y. Hong and J. Vaidya and S. Wang: *A survey of privacy-aware supply chain collaboration: From theory to applications*, Journal of Information Systems 28(1)(2014), pp. 243–268

[7] M.G. Karagiannopoulos, M.N. Vrahatis and G.C. Meletiou: *A note on a secure voting system on a public network*, Networks 432(4)(2004), pp. 224–225

[8] E. Kiltz, P. Mohassel, E. Weinreb and M. Franklin: *Secure linear algebra using linearly recurrent sequences*, Lecture Notes in Computer Science 4392(2007), pp. 291–310

[9] E. C. Laskari, G.C. Meletiou, D.K. Tasoulis and M.N. Vrahatis: *Privacy preserving electronic data gathering*, Mathematical and Computer Modelling 42(7-8)(2005), pp. 739–746

[10] E. C. Laskari, G.C. Meletiou and M.N. Vrahatis: *Recent approaches to electronic data gathering with privacy*, in Proceedings of the First International Conference From Scientific Computing to Computational Engineering (IC-SCCE 2004), September 8–10, 2004, Athens, Greece, pp.1–7, 2004

[11] J.-T. Li and M.J. Atallah: *Secure and private collaborative linear programming*, in Proceedings of the International Conference on Collaborative Computing:

Networking, Applications and Worksharing (CollaborateCom 2006), November 17–20, 2006, Atlanta, GA, U.S.A., pp.1–8, 2006

[12] O. L. Mangasarian: *Privacy-preserving linear programming*, Optimization Letters 5(1)(2011), pp. 165–172

[13] G.C. Meletiou, A.D. Koutsodimas and I.P. Krommyda: *Secure supply chain collaboration using cryptographic techniques*, in Proceedings of the 4th International Symposium and 26th National Conference on Operational Research, June 4–6, 2015, Chania, Greece, pp.68–72, 2015

[14] J. Vaidya: *Privacy-preserving linear programming*, Proceedings of the ACM symposium on Applied Computing (SAC 2009), March 8–2, 2009, Honolulu, HI, U.S.A., pp.2002–2007, 2009

[15] A.C.-C. Yao: *How to generate and exchange secrets*, in Proceedings of the 27th Annual Symposium on Foundations of Computer Science (SFCS 1986), October 27–29, 1986, Toronto, ON, Canada, pp. 162-167, 1986