4th International Conference on

Operational Planning, Technological Innovations and Mathematical Applications (OPTIMA)

Hellenic Military Academy

25th -26th May 2017

Abstracts

Editor: Nicholas J. Daras

Bottom-up hierarchical ramp secret sharing scheme

Stamatios-Aggelos N. Alexandropoulos[1], Gerasimos C. Meletiou[2],

Demetrius S. Triantafyllou[3] and Michael N. Vrahatis[4]

[1,4]Computational Intelligence Laboratory, Department of Mathematics,

University of Patras, GR-26110 Patras, Greece

[2]A.T.E.I. of Epirus, P.O.110, GR-47100 Arta, Greece

[3]Department of Mathematics and Engineering Sciences
Hellenic Military Academy
GR-16673 Vari, Greece

E-mails: [1] alekst@master.math.upatras.gr , [2] gmelet@teiep.gr

[3] vrahatis@math.upatras.gr and [4] dtriant@math.uoa.gr

Key words: ramp secret sharing scheme • information sharing • bottom-up hierarchy • bottom-up sharing

ABSTRACT

Secret sharing schemes have attracted the attention of many scientists aiming to distribute a secret among a group of participants each of which has been given a share of the secret. To this end, in this study, a hierarchical ramp secret sharing scheme is proposed. In the proposed approach, the dealer distributes to each one of n participants a share of the secret along with other unrelated items in an encrypted form. None of the participants alone (or in smaller groups) is able to

obtain the secret. In order to decrypt the secret, all the participants have to perform a pairwise cooperation using numerical methods. The proposed scheme is such as to allow the dealer to share the secret in a way that the most significant participant holds the most meaningful share. The participants are arranged in a bottom-up hierarchical structure. Any small group of $k < n$ participants is not in a position to reconstruct the secret. The proposed scheme can be applied to various issues related to transmission of encrypted messages where a hierarchy is required. □

References

[1] S.-A.N. Alexandropoulos, G.C. Meletiou, D.S. Triantafyllou, M.N. Vrahatis: Transformations of cryptographic schemes through interpolation techniques, In: *Computation, Cryptography, and Network Security*, N.J. Daras and M.Th. Rassias (eds.), Chapter **1**, pp. 1-17, Springer International Publishing, Switzerland, 2015

[2] G.R. Blakley: Safeguarding cryptographic keys, In: *Proceedings of the 1979 AFIPS National Computer Conference*, vol.**48**, AFIPS Press, Montvale, NJ, USA, pp. 313-317, 1979

[3] R.L. Burden, J.D. Faires: *Numerical Analysis*, Brooks / Cole Publishing Company, Pacific Grove, CA, USA, 6th edition, 1997

[4] B.N. Datta: *Numerical Linear Algebra and Applications*, SIAM, Philadelphia, PA, USA, 2nd Edition, 2010

[5] V.E. Markoutis, G.C. Meletiou, A.N. Veneti, M.N. Vrahatis: Threshold secret sharing through multivariate Birkhoff interpolation, In: *Computation, Cryptography, and Network Security, N.J.*

Daras and M.Th. Rassias (eds.), Chapter **14**, pp. 331-350, Springer International Publishing, Switzerland, 2015

[6] A. Shamir: How to share a secret, *Communications of the ACM*, **22**(11)(1979), pp. 612-613

[7] D.R. Stinson: An explication of secret sharing schemes, *Designs, Codes and Cryptography*, **2**(1992), pp. 357-390

[8] T. Tassa: Hierarchical threshold secret sharing, *Journal of Cryptology*, **20**(2) (2007), pp. 237-264.