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. Alexandropoulos¹, Gerasimos C. Meletiou², Demetrios S. Triantafyllou³ and Michael N. Vrahatis⁴

¹⁴Computational Intelligence Laboratory, Department of Mathematics, University of Patras, GR-26110 Patras, Greece

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

³Department 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


