HELLENIC REPUBLIC
National and Kapodistrian University of Athens
EST. 1837

UNIVERSITÉ DU LITTORAL CÔTE D'OPALE

NASCA23

Numerical Analysis and Scientific Computation with Applications

Book of Abstracts

3-6 July 2023,
Athens, Greece

Edited by

Mustapha Hached
Khalide Jbilou
Christos Koukouvinos
Marilena Mitrouli

Structured Ramp Secret Sharing Schemata

Gerasimos C. Meletiou[1], Nikolaos K. Papadakis[2], Dimitrios S. Triantafyllou[3], Michael N. Vrahatis[4]

[1] *University of Ioannina, School of Agriculture, GR-47100 Arta, Greece, e-mail: gmelet@uoi.gr*

[2] *Department of Mathematics and Engineering Sciences, Hellenic Military Academy, GR-16673 Vari, Greece, e-mail: npapadakis@sse.gr*

[3] *Department of Mathematics and Engineering Sciences, Hellenic Military Academy, GR-16673 Vari, Greece, e-mail: dtriant@sse.gr and Department of Civil Engineering, University of West Attica, GR-12241 Athens, Greece, e-mail: dtriant@uniwa.gr*

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

Abstract

Secret sharing schemata using computational techniques of Linear Algebra are proposed and analyzed. Specifically, (s, t, n) - threshold *Ramp Secret sharing* schemata are presented, where s and t are positive integers, while n denotes the number of *participants* of a secret sharing scheme. Any set of h participants, $0 < h < s$, are not able to retrieve any information about the secret, while any set of h' participants, $s \leq h' < t$, are able to retrieve only a part of the secret and any set of h'' participants, $t \leq h'' \leq n$, retrieve the whole secret. The person that manipulates the secret sharing procedure, named *dealer*, constructs a polynomial $p(x)$ of degree k, in which the secret is properly hidden. Next, the dealer creates a set of r *structured levels* $L_i,\ i = 1, 2, \ldots, r$ and shares a polynomial to each participant at every level. Several specified by the dealer participants from levels $L_i,\ L_j,\ i, j \in \{1, 2, \ldots, r\}, i \neq j$, must cooperate revealing their shares (represented by polynomials) and compute the *Greatest Common Divisor* of polynomials to retrieve the secret. To compute the greatest common divisor of polynomials, the participants can use direct methods for matrices factorization, for instance the well-known and widely used LU or QR factorization procedures. Our approaches are studied in respect of error analysis and complexity. Furthermore, indicative numerical examples are presented to facilitate the proposed schemata.

References

[1] S. Barnett, Greatest common divisor of several polynomials, Linear Multilinear A, 8, 271-279, (1980).

[2] G.R. Blakley, C. Meadows, Security of ramp schemes, in Advances in Cryptology, Lect. Notes Comput. Sci., 196, 242–268, (1984).

[3] A.K. Lenstra, H.W. Lenstra, Jr., L. Lovász, Factoring polynomials with rational coefficients, Math. Ann., 261, 515–534, (1982).

[4] G. C. Meletiou, D. S. Triantafyllou, M. N. Vrahatis, First study for ramp secret sharing schemes through greatest common divisor of polynomials, Lect. Notes Comput. Sci., 159, 247–259, (2020).

[5] D.R. Stinson, Ideal ramp schemes and related combinatorial objects, Discrete Math., 341, 299–307, (2018).