3rd International Conference on

Cryptography, Cyber Security and Information Warfare

(3rd CryCybIW)

Hellenic Military Academy

26th -27th May 2016

Abstracts

Editor: Nicholas J. Daras

Secret Sharing Schemes through Structured Matrices

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,
E-mails: alekst@master.math.upatras.gr [1] and vrahatis@math.upatras.gr [4]

[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

Key words: *Secret sharing schemes • structured matrix triangularization • LU factorization • matrix convolution*

Abstract Secret sharing schemes through matrices of special structure are presented. The secret S, formulated by a matrix, is shared among n participants in such a way that the ith participant receives from the dealer a part of the secret S encrypted as a convolution of several matrices:

$$M_i = S * \prod_j P_j, \quad \text{for all} \quad i = 1, 2, \ldots, n, \quad j = 1, 2, \ldots, i\text{-}1, i\text{+}1, \ldots, n,$$

where $\prod$ indicates matrix convolution and P_i represents the secret matrix of the ith participant which is also known to the dealer. The secret S can be derived through numerical linear algebra techniques and more precisely through matrix factorization. The usage of well known and widely used methods such as the LU factorization with partial pivoting can guarantee the stability of the procedure. We show that a specific group of participants are in a position to construct a block banded matrix, by properly shearing their own information and by applying the LU factorization with partial pivoting, they can retrieve and extract the secret S. □

References

[1] A. Beimel: *Secret-sharing schemes: A survey*, Lecture Notes in Computer Science 6639(2001), pp. 11–46

[2] M. Bläser: *Fast matrix multiplication*, in **Theory of Computing**, Graduate Surveys 5(2013), pp. 1–60

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

[4] A. Danelakis, M. Mitrouli and D.S. Triantafyllou: *Blind image deconvolution using a banded matrix method*, Numerical Algorithms 64(2013), pp. 43–72

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

[6] J.M. Landsberg and G. Ottaviani: *New lower bounds for the border rank of matrix* multiplication, Theory of Computing 11(11)(2015), pp. 285–298

[7] E.C. Laskari, G.C. Meletiou, D.K. Tasoulis and M.N. Vrahatis: *Transformations of two cryptographic problems in terms of matrices*, ACM SIGSAM Bulletin 39(4) (2005), pp. 127–130

[8] V.E. Markoutis, G.C. Meletiou, A.N. Veneti and 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

[9] G.C. Meletiou, E.C. Laskari, D.K. Tasoulis and M.N. Vrahatis: *Matrix representation of cryptographic functions*, Journal of Applied Mathematics and Bioinformatics 3(1)(2013), pp. 205–213

[10] G.C. Meletiou, D.S. Triantafyllou and M.N. Vrahatis: *Handling problems in cryptography with matrix factorization*, Journal of Applied Mathematics and Bioinformatics 5(3)(2015), pp. 37–48

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