3rd International Conference on

Technology Trends and Scientific Applications in Artillery and other Military Science (TTSAAMS)

Hellenic Artillery School

Abstracts

Editor: Nicholas J. Daras

Studying Secret Sharing Schemes with Matrix Representations

Gerasimos C. Meletiou[1], Dimitrios S. Triantafyllou[2] and Michael N. Vrahatis[3]

[1]A.T.E.I. of Epirus, P.O.110, GR-47100 Arta, Greece, and
Computational Intelligence Laboratory, Department of Mathematics,
University of Patras, GR-26110 Patras, Greece
E-mail: gmelet@teiep.gr

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

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

Abstract We present and compare various secret sharing schemes. Firstly, we present the classical and widely used Shamir's scheme [4] which is based on Langrange interpolation as well as Blakley's scheme [1] which is based on hyperline geometry. We also present variations of these schemes [2,3] which improve the classical procedures leading to more effective algorithms.

Well known matrices such as Vandermonde's, Hilbert's and Pascal's matrix have been used for representing the domain of the shares, the interpolation process as well as the extraction of the secret. Also, numerical linear algebra methods for solving linear systems of equations in finite fields, such as LU factorization, have been applied.

We compare the presented schemes in respect of computational complexity, storage capacity and robustness. All the methods have been tested on various examples and the results are summarized in tables concluding to useful results. □

References

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

[2] X.-L. Hei, X.-J. Du, B.-H. Song: *Two matrices for Blakley's secret sharing scheme,* In: Proceedings of the 2012 IEEE International Conference on Communications (ICC), pp. 810-814, IEEE 2012.

[3] 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, Springer, New York, 2015, to appear.
[4] A. Shamir: *How to share a secret*, Communications of the ACM **22**(11) (1979), 612-613.