2nd International Conference on

Cryptography, Network Security and Applications in the Armed Forces

Hellenic Military Academy

April 2, 2014

Abstracts

Editor: Nicholas J. Daras

Hierarchical Secret Sharing through Multivariate Birkhoff Interpolation

Vassileios Markoutis[1], Gerasimos C. Meletiou[2] and Michael N. Vrahatis[3]

[1]Department of Mathematics, University of Patras, GR-26110 Patras, Greece,
E-mail: billmarku@yahoo.gr

[2]A.T.E.I. of Epirus, P.O.110, GR-47100 Arta, Greece,
and
University of Patras Artificial Intelligence Research Center, University of Patras,GR-26110 Patras, Greece
E-mail: gmelet@teiep.gr

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

Abstract The Shamir's well-known threshold secret sharing scheme ([1], [2]) is been generalized by Tassa ([3], [4]). The set of participants is divided into levels and a hierarchical structure is introduced. In this paper Lagrangian interpolation is replaced by Birkhoff interpolation (a generalization of Lagrange and Hermite) and this is the novelty of the scheme.

In this presentation, we introduce Birkhoff interpolation over multivariate polynomials. Again the set of participants is divided into levels. However the hierarchical relation between levels is a kind of partial order. □

References

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

[2] G. J. Simmons: *How to (really) share a secret*, Advances in Cryptology – CRYPTO 88, LNCS 403 (1990) pp. 390–448.

[3] Tassa Tamir: *Hierarchical Threshold Secret Sharing*, J. Cryptology 20(2007), pp. 237–264.

[4] Tassa Tamir and Dyn Nira: *Multipartite Secret Sharing by Bivariate Interpolation*, J. Cryptology 22(2009), pp. 227–258.