2nd International Conference on

# Cryptography, Network Security and Applications in the Armed Forces

Hellenic Military Academy

April 2, 2014

# Abstracts

Editor: Nicholas J. Daras

# Orbit Computations and Matrix Factorization in Finite Fields

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

[1] 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

[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*** The Discrete Logarithm function and the Diffie-Hellman mapping are revisited. We use Vandermonde matrices for their representation. Both of the above mentioned cryptographic functions admit expression as a product of matrices.

First we consider orbits of repeated applications of the cryptographic transformations. The length of the orbit is related to the robustness of the cryptosystem. We determine it either by computational experiments or with theoretical tools. We investigate the behavior of powers of matrices constructed from the generators $a$ of multiplicative groups for several primes $p$ in $\mathbb{Z}_p$. We study the convergence of the powers of these matrices to the identity matrix in respect of the generator $a$, the prime numbers $p$ and the elements of the main diagonal of the matrices. Several examples and graphs are given concluding to useful remarks.

Finally, matrix factorization approach (LU factorization) is used. Obtaining lower bounds of the length of the orbits is one of our goals. Facing the computational equivalence of the Discrete Logarithm problem and the Diffie-Hellman problem is another goal. □

## References

[1] W. Diffie and M. Hellman: *New directions in cryptography*, IEEE Trans. Inf. Th., 22(6) (1976), pp. 644–654.

[2] L. Glebsky and I. Shparlinski: *Short Cycles in Repeated Exponentiation Modulo a Prime*, Des. Cod. Crypt., 56(1) (2009), pp. 35–42.

[3] B.N. Datta: Numerical Linear Algebra and Applications, *Second Edition, SIAM, United States of America, 2010*.

[4] G.H. and Van Loan, C.F.: Matrix Computations, *Third Edition, The John Hopkins University Press, Baltimore, London, 1989*.

[5] G. Meletiou and G. Mullen: *A note on Discrete Logarithms in finite fields*, A.A.E.C.C. 3 (1992), pp. 75–79.

[6] G. C Meletiou, E.C. Laskari, D.K. Tasoulis and M.N. Vrahatis: *Matrix representations of Cryptographic Functions*, Journal of Applied Mathematics and Bioinformatics, 3(1) (2013), pp, 205-213.

[7] G. Meletiou and A. Winterhof: *Interpolation of the Double Discrete Logarithm*, LNCS, 5130(2008), pp. 1–10.

[8] D. Triantafyllou, *Numerical Linear Algebra methods in Data Encoding and Decoding*, Journal of Applied Mathematics & Bioinformatics, 3(1) (2013), pp. 193-203.

[9] A. Winterhof: *A note on the interpolation of the Diffie-Hellman mapping*, Bull. Austral. Math. Soc., 64(3) (2001), pp. 475–477.