On new one-way ring homomorphisms

Bachuki Mesablishvili

e-mail: bachuki.mesablishvili@tsu.ge

Department of Mathematics,

Faculty of Exact and Natural Sciences,
Ivane Javakhishvili Tbilisi State University,

2 Chavchavadze Avenue, Tbilisi 0179.

Annotation: New one-way ring homomorphisms from one-way (non-abelian) group Homomorphisms are constructed. A multiple digital signature scheme is also given as an application of our one-way ring homomorphisms.

References:

[1] I. Anshel, *An algebraic method for public-key cryptography,* Math. Res. Lett. ***6*** (1999), 287-291.
[2] W. Diffie and M.E. Hellman, *New directions in cryptography,* Information Theory ***22*** (1976), 644-654.
[3] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms,* Advances in cryptology |CRYPTO '84, Lecture Notes in Comp. Sci. 196, Springer, 1985, 10-18.
[4] R.C. Merkle, *A certified digital signature,* Advances in cryptology, CRYPTO '89, Lecture Notes in Comput. Sci. 435, Springer, 1989, pp. 218-238.
[5] M.O. Rabin, *Digitalized signatures,* Academic Press (1978), 155-168.