A Message Encryption Scheme Using Idempotent Semirings

M. Durcheva

Technical University of Sofia, Bulgaria, mdurcheva66@gmail.com

Symmetric-key and public-key encryption have a number of complementary advantages. Symmetric key cryptography is faster and more efficient than asymmetric (public key) cryptography, but it lacks security when exchanging keys over unsecured channels. Furthermore, in symmetric key cryptography sound cryptographic practice dictates that the key be changed frequently whereas in public key cryptography a private key/public key pair may remain unchanged for considerable periods of time (see [3]).

In the present work a message encryption scheme based on public key establishment is proposed. For key exchanging phase we suggest using idempotent semirings [1, 2].

References

[1] M. Durcheva, *Public Key Cryptosystem Based on Two Sided Action of Different Exotic Semirings*, in Journal of Mathematics and System Science 4, pp. 6-13 (2014).

[2] M. Durcheva, *An application of different dioids in public key cryptography*, in AIP Conference Proceedings 1631, pp. 336-343 (2014).

[3] A. Menezes, P. vanOorschot and S. Vanstone *Handbook of Applied Cryptography*, CRC Press (1996).