An algorithm for error-free calculation of convolution in extensions of finite fields

A.N. Kalugin [1]
[1] *Samara State Aerospace University*

Abstract

The paper considers an algorithm for error-free calculation of discrete circular convolution using number-theoretic transformations in the residue number system with an alternative factorization of the composite module in the extension of the residue class ring. An additional computational gain is provided by representing the input data and transformation parameters in canonical number systems.

Keywords: error-free calculation, finite field, discrete circular convolution, number-theoretic transformations, factorization, canonical number system.

Citation: Kalugin AN. An algorithm for error-free calculation of convolution in extensions of finite fields. Computer Optics 2003; 25: 134-140.

Access full text (in Russian)

References

[1] Schneier B. Applied cryptography: protocols, algorithms, and source code in C. 2nd ed. New York: John Wiley and Sons Inc; 1996.
[2] Menezes AJ, van Oorschot PC. Vanstone SA. Handbook of applied cryptography. Boca Raton: CRC Press, 1996.
[3] Chernov VM, Pershina MV. «Error-free» calculation of the convolution using generalized Mersenne and Fermat transforms over algebraic fields. In Book: Sommer G, Daniilidis K, Pauli J, eds. Computer analysis of images and patterns (CAIP'97). Berlin, Heidelberg: Springer; 2005: 621-628.
[4] Chernov VM. Synthesis of parallel algorithms of Fourier-Galois transforms in direct sums of finite rings. Proceedings of the Samara Scientific Center of Russian Academy of Sciences 2000; 2(1): 128-134.
[5] Kátai I, Kovács B. Canonical number systems in imaginary quadratic fields. Acta Mathematica Academiae Scientarium Hungarica 1981; 37(1-3): 159-164.
[6] Kátai I, Szabo J. Canonical number systems for complex integers. Acta Sci Math 1975; 37: 255-260.
[7] Thuswardner JM. Elementary properties of canonical number systems in quadratic fields. In Book: Bergum GE, Philippou AN, Horadam AF, eds. Applications of Fibonacci numbers. Vol 7. Dordrecht: Springer Science+Business Media; 1998: 405-415.
[8] Knut D. The art of computer programming. Vol. 2. Seminumerical algorithms. 3rd ed. Addison-Wesley Professional; 1997.
[9] Kovács A. Generalized binary number systems. Annales Univ Sci Budapest, Sect Comp 2001; 20: 195-206.
[10] Chernov VM. Factorization ambiguity, canonical number systems in quadratic rings and parallel algorithms for calculating convolutions. Proceedings of the 11th Conference "Mathematical methods for Pattern Recognition" (MMRO-11) 2003: 212-215.