Matrix algorithms of processing of the information flow in computer systems based on theoretical and numerical Krestenson's basis

Ihor Yakymenko, Mykhajlo Kasyanchuk, Yaroslav Nykolajchuk

Abstract – **This paper considers algorithms for matrix multiplication and modular exponentiation. Shown that algorithms are effectively implemented using appropriate tables, which allows to replace the operation of multiplication into operation of addition.**

Keywords – **Multiplication, exponentiation, Rademacher's basis, Krestenson's basis, matrix.**

I. INTRODUCTION

The operations of modular multiplication and exponentiation underlying the most common public-key cryptosystems (RSA, El Gamal, etc.), algorithms for digital signatures [1], determine the stability of elliptic curves by finding their order through the Shuf's algorithm [2], etc. Existing algorithms (fast multiplication, Blakey, Montgomery, binary, etc.) have significant computational complexity. In this paper, the algorithms proposed modular multiplication and exponentiation in the Krestenson's basis using matrix computations.

II. ALGORITHM Multiplication

It is well-known in the Krestenson's basis any decimal integer N is presented as a set of remnants of his division on fixed modules p_i, and $0 \le N \le \prod_{i=1}^{n} p_i - 1$ [3]. Reverse conversion to decimal number system is much more difficult. Since the operations performed in computer systems in the Rademacher's basis, the problem of direct referrals from the Krestenson's base into Rademacher's base and vice versa, effectively implemented through matrix calculations.

Consider two n-bit numbers $a=a_{n-1}2^{n-1}+\ldots+ \ +a_i2^i+\ldots+ a_12+a_0$ and $b=b_{n-1}2^{n-1}+\ldots+ +b_i2^j+\ldots+ b_12+b_0$, where a_i, b_j = 0, 1, n-digit module p. For purpose to find the results of their multiplication of modul p build the matrix presented in the table 1, where $c_{ij}=2^{i+j}$mod p. The product numbers a and b obtain the following formula $a \cdot b = \left(\sum_{m,k=1}^{n-1} c_{mk} \right) \bmod \ p$, where a_m, b_k=1, those c_{mk} located at the intersection of column and row for which the corresponding a_i and b_j are equal to 1.

Thus, could replace the multiplication operation, which has a quadratic computational complexity of adding with linear complexity.

Ihor Yakymenko, Mykhajlo Kasyanchuk, Yaroslav Nykolajchuk – Carpathians State center of informative tools and technologies of NASU. Ivano-Frankivsk, Pashnyckogo Str 43, UKRAINE.
E-mail:kasyanchuk@ukr.net; iyakymenko@mail.ru

TABLE 1

MULTIPLICATION MATRIX IN THE RADEMACHER-KRESTENSON'S BASIS

	b_{n-1}	…	b_j	…	b_1	b_0
a_{n-1}	$c_{n-1\ n-1}$	…	$c_{n-1\ j}$	…	$c_{n-1\ 1}$	$c_{n-1\ 0}$
…	…	…	…	…	…	…
a_i	$c_{i\ n-1}$	…	c_{ij}	…	c_{i1}	c_{i0}
…	…	…	…	…	…	…
a_1	$c_{1\ n-1}$	…	c_{1j}	…	c_{11}	c_{10}
a_0	$c_{0\ n-1}$	…	c_{0j}	…	c_{01}	c_{00}

III. ALGORITHM Exponentiation

For modular exponentiation a^xmod p will use the intermediate matrix presented in the table 2. Its dimension is n-range module p. In column of matrix the values a^{2^i} mod p in the Rademacher basis, a_{ij}=0, 1. Then any degree of x can be written in powers of 2 and the desired result can be obtained by multiple appropriate number of columns for a table 1.

TABLE 2

EXPONENTIATION MATRIX IN THE RADEMACHER-KRESTENSON'S BASIS

$a_{n-1\ n-1}$	…	$a_{i\ n-1}$		$a_{1\ n-1}$	$a_{0\ n-1}$
…	…	…	…	…	…
$a_{n-1\ j}$	…	$a_{i\ j}$	…	$a_{1\ j}$	$a_{0\ j}$
…	…	…	…	…	…
$a_{n-1\ 1}$	…	$a_{i\ 1}$	…	$a_{1\ 1}$	$a_{0\ 1}$
$a_{n-1\ 0}$	…	$a_{i\ 0}$	…	$a_{1\ 0}$	$a_{0\ 0}$
$a^{2^{n-1}}$	...	a^{2^i}	...	a^{2^1}	a^{2^0}

IV. CONCLUSION

In this work matrix algorithms for modular multiplication and exponentiation for replace the multiplication operation, which has a quadratic computational, complexity of adding with linear complexity.

REFERENCES

[1] Zadiraka V.K., Oleksyuk O.S. Computer arithmetic of multidecimal numbers – К.: 2003. – 264 p.

[2] Vasylenko O.M. Theoretic-numbers basis in cryptography. – M.: MCNMO, 2003. –328 p.

[3] Nykolajchuk Ya.M. The theory of information source. – Ternopil: TNEU, 2008. – 536 p.