Quick multiplying multidigit number with use the modification of the algorithm fast transformation Fourier

Kyantai Abdikalikov[a]

[a] *Aktobe Regional State University by K. Zhubanov, Kazakhstan*

[a] *abdikalikov@mail.ru*

Abstract: In this study, we develop approach Shtrassen [1] to quick multiplying multidigit number in a part of the use for its realization of the original modification algorithm of the fast transformation Fourier (FTF) [2].

For realization on computer asymmetric cryptographic algorithm it is necessary to have a library effective on speed algorithm and programs of the execution operation with multidigit number.

Time to operations of the multiplying on processor with fixed by length of the word is proportional to the square of the length operand $O(n)^2$. By construction of consecutively-parallel hardware provision, that time can be reduced to $O(n)$. In this case amount of required logical elements will be proportional to a length operand $O(n)$. Time of the work for the most high-speed realization is proportional to $O(\log n)$, but it requires $O(n)^2$ logical elements.

For the method Karacuby, its difficulty is $O(n^{\log_2 3})$, where $\log_2 3 \approx 1.58$ [3]. The method polynomial since running time of the order $n^{1+\varepsilon}, (\varepsilon > 0)$. The algorithm Tooma-Kuka has difficulty of the order $O(n2^{\sqrt{2\log_2 n}} \log_2 n)$ [4]. The algorithm Shenhage – Shtrassen allows to multiply two -n a class numbers, executing for $O(n \log n \log\log n)$ step (the bit operation) [1].

Note that these methods are based on the information of the multiplying n- a class numbers to multiplying numbers with smaller number category.

Keywords: multidigit number, modification, cryptographic, hardware provision.

References:

[1] A. Shanhage, V. Shtrassen, Quick multiplying greater nembers, Cybernetics collection, issue 10, pp. 87-98, 1973.

[2] K.A. Abdikalikov, V.K. Zadiraka, Elements modern cryptology and methods of security to bank information, Almaty, Gylym,1999.

[3] A.A. Karacuba, Y.P. Ofman, Multiplying multidigit numbers on automaton, DAN USSR, vol, 145, pp. 293-294, 1962.

[4] S.A. Kun, S.O. Anderaa, About minimum time of the calculation to functions, Cybernetics collection, issue 8, pp. 293-294, 1971.