عنوان مقاله:

Algorithm Design and Theoretical Analysis of a New Bit Forwarding Large Integer Modular Exponentiation Algorithm

محل انتشار:
دوفصلنامه علوم محاسباتی و مهندسی, دوره 2, شماره 2 (سال: 1401)

تعداد صفحات اصل مقاله: 12

نویسندگان:

Abdalhossein Rezai - Department of Electrical Engineering, University of Science and Culture, Tehran, Iran

Manizheh Abbasi - ACECR Institute of Higher Education, Isfahan Branch, Isfahan, Iran

Asghar Karimi - ACECR Institute of Higher Education, Isfahan Branch, Isfahan, Iran

خلاصه مقاله:

One of the most principal operations in many PKCs is Modular Exponentiation (ME). This operation is usually performed by successive modular multiplications. So, the efficiency of these PKCs is released on the efficiency of the Modular Multiplication (M۲) and modular exponentiation implementation. Therefore, it is essential to minimize the execution time of the M۲ and the number of required M۲ for performing the ME operation. This paper proposes a novel ME algorithm. In the developed algorithm, the Bit Forwarding (BF) and multibit-scan-multibit-shift techniques are employed for the performance improvement in the ME operation. The complexity analysis is accomplished to show that the developed exponentiation algorithm has benefit in the number of required multiplications. The results indicate that the presented algorithm improves the results compared to other modular .exponentiation algorithms by about ۱۱%-۸۵%

کلمات کلیدی:

Modular exponentiation, bit forwarding technique, modular multiplication, complexity analysis, multibit-scan-multibit-shift technique

لینک ثابت مقاله در پایگاه سیویلیکا: