عنوان مقاله:

Throughput Improvement of RIPEMD-۱۶۰ Design using Unfolding Transformation Technique

محل انتشار:

دوفصلنامه بهینه سازی در مهندسی صنایع, دوره 15, شماره 1 (سال: 1401)

تعداد صفحات اصل مقاله: 10

نویسندگان:

Shamsiah binti Suhaili - *Faculty of Engineering, Universiti Malaysia Sarawak, ۹۴۳۰۰ Kota Samarahan, Sarawak, ,Malaysia*

Takahiro Watanabe - *Graduate School of Information, Production and Systems, Waseda University, ۲-۷ Hibikino, Wakamatsu-ku, Fukuoka ۸۰۸-۰۱۳۵, Japan*

Norhuzaimin Julai - *Faculty of Engineering, Universiti Malaysia Sarawak, ۹۴۳۰۰ Kota Samarahan, Sarawak, Malaysia*

خلاصه مقاله:

RIPEMD-۱۶۰ hash functions are widely used in many applications of cryptography such as digital signature, Hash Message Authentication Code (HMAC) and other data security application. There are three proposed RIPEMD-۱۶۰ design namely RIPEMD-۱۶۰ iterative design, RIPEMD-۱۶۰ unfolding with factor two and RIPEMD-۱۶۰ unfolding design with factor four. These techniques were applied to RIPEMD-۱۶۰ designs to examine the inner structure of RIPEMD-۱۶۰ in terms of area, maximum frequency and throughput of the design. In this project, RIPEMD-۱۶۰ hash function using unfolding transformation technique with factor four provided high throughput implementation. The throughput of the RIPEMD-۱۶۰ unfolding design increase significantly. The objective of this project is to enhance the performance of RIPEMD-۱۶۰ in terms of throughput. By using unfolding transformation factor four technique, the throughput of RIPEMD-۱۶۰ can be improved which is about ۱۷۵۳.۵۰ Mbps. The percentage of performance to area ratio of RIPEMD-۱۶۰ unfolding with factor four designs increase ۱.۵۱% if compared with RIPEMD-۱۶۰ design. The results show performance of proposed designs give the highest value compare with other designs. The simulation results were obtained from ModelSim Altera-Quartus II to verify the correctness of the RIPEMD-۱۶۰ designs in terms of functional .and timing simulations

کلمات کلیدی:

FPGA, Hash Function, RIPEMD-۱۶۰, throughput, Unfolding