عنوان مقاله:

FPGA-Based Efficient Hardware Implementation of Fault Tolerant Gaussian Normal Basis and Redundant Basis Multipliers

محل انتشار:

دومین همایش ملی پژوهش های نوین در مهندسی و علوم کاربردی (سال: 1398)

تعداد صفحات اصل مقاله: 11

نویسنده:

Bahram Rashidi - *Faculty of Engineering, Ayatollah Boroujerdi University, Boroujerd, Iran*

خلاصه مقاله:

This paper presents an efficient FPGA implementation of fault tolerant bit-serial Gaussian normal basis (GNB) and redundant basis multipliers over the binary finite fields. The efficiency of the proposed method is based on and depends on the regularity of the circuit architecture. The hardware architectures of multipliers, which are employed here, consist of GNB and type-2 redundant basis. These structures have inherent regularity and similarity in their circuits, compatible to the fault tolerant design method presented here. In the proposed method a common circuit with a relatively low hardware, which is extracted from the main circuit, is used for fault tolerant design. This work has been successfully verified and implemented using Xilinx ISE 14.2 by Virtex-5 XC5VLX110 FPGA. The hardware implementation allows validation of the proposed structures for practical fault tolerant cryptographic applications. The .results show that the proposed fault tolerant bit-serial GNB and redundant basis multipliers have low area overhead

کلمات کلیدی:

.Fault Tolerant, bit-serial multiplier, Gaussian normal basis, Redundant basis, Hardware implementation, FPGA

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/1034481