ABSTRACT

The FPGA based crypto systems employed as a co-processing unit with the main system, is a good replacement for software security solution, in terms of performance, throughput and power. The crypto systems employed for high altitude applications are prone to SEUs.

Therefore, the problem has been identified to design, implement and analyze the performance of an adaptive crypto system for SEU mitigation. To design an adaptive crypto system to mitigate SEU requires

i. A high performance architectures for the security primitives

ii. A secure and random key generation to provide keys to the crypto system

iii. An effective SEU detection hardware

iv. Recovery circuitry to recover from the SEU errors.

The specific research objectives are:

a) To design a high performance architecture for the security primitives namely TEA, XTEA and RC5 primitives.

b) To formulate a key generation for the crypto system using genetic crossover methods.

c) To design and configure different switching modes in a multi primitive crypto system using multiple security primitives.
d) To analyze the performance of the adaptive crypto system for single event upset mitigation.

e) To propose a low cost crypto system implementation with TEA and XTEA security primitives.

The security primitives TEA, XTEA and RC5 are chosen to implement the adaptive crypto system. The architectures of TEA, XTEA and RC5 are designed, simulated and implemented in Xilinx 10.1 ISE tool on the target device XC4Vfx12-12sf363. The TEA and XTEA primitive are operated for an invariant 32 rounds, whereas RC5 primitive is operated for 12 rounds. All the three primitives handle a 64 bit plaintext P and a 128 bit key K. The slices utilized, frequency, power are the parameters obtained from the device utilization and the timing reports of the implementation process. The throughput, throughput / slice, energy and energy efficiency are the performance metrics which are evaluated from the obtained parameters.

Three different architectures namely, multiplexer based, structural and sub program architectures are analyzed for TEA primitive. The throughput of multiplexer based TEA architecture is 10.3% greater than structure based and 30.3% greater than the subprogram based architectural designs. Hence, multiplexer based architectural design was carried out for XTEA primitive, which is an extended version of TEA.

The multiplexer based, pipeline and sliding window architectures are proposed for a 12 round RC5 primitive. The device utilization of the pipeline architecture of RC5 primitive is 0.004% greater than the multiplexer based architecture of RC5. However, the throughput of pipeline is 8.95 Gbps, which is 14.1 times higher
than the multiplexer based architecture and 1.23 times higher than the sliding window architecture of RC5.

Several methods are available to generate keys for the crypto system. In this work, a new key generation method called LCG – SRC method is proposed. The keys generated using LCG – SRC method is stored and used for the adaptive crypto system. A new crossover operator called as Spin Ring Crossover (SRC) operator is proposed based on genetic principles. The characteristics and the performance of the SRC operator is compared with the other crossover operators. The SRC operation is performed on the 3500 parents generated from the random function. The randomness of the offspring generated are validated with the NIST test suite.

The parent chromosome is binary encoded and represented with 8 genes and 10 chromosomes together form a generation. A set of 100 generations are iterated and the deviation between the generations is calculated. The chromosomal values for each generation, median of population, standard deviation of each population were studied to analyze the properties of the operation. The methodology of seed selection, crossover points and mutations are formulated using the LCG recurrence relations. The keys for the adaptive cryptosystem are derived from LCG – SRC method is validated by performing runs test for randomness.

The multiplexer based architectural design of TEA, XTEA primitives and pipeline architecture of RC5 primitives are configured in a single FPGA to function as a multi primitive crypto system. Different configurations namely, Fixed Primitive Switching Key (FPSK), Switching Primitive Fixed Key (SPFK) and Switching Primitive and Switching Key (SPSK) is proposed for the multi primitive crypto system. The FPSK switches the keys for a fixed primitive, SPFK switches the
primitive for the fixed key and SPSK switches both the primitive and the keys. The keys generated from the LCG – SRC method are employed in the proposed multi primitive crypto system. The throughput of RC5 primitive in the FPSK configuration is 11.7% greater than the RC5 primitive in the SPFK configuration and 24.2% greater than the RC5 primitive in SPSK configuration. However, the SPSK configuration offers more security as it switches the primitive and key for each plaintext.

The multi primitive crypto system is SEU mitigated to form an adaptive crypto system with time multiplexed SEU mitigation in RC5 and XTEA primitive. The error detection hardware introduced in the input, output and at every intermediate output of RC5 primitive execution. The Vote Before Read (VBW) and Vote After Write (VAW) voting schemes are used with both single and triple voter schemes. If an SEU is detected in RC5 operation, then, the recovery control circuit switches the encryption operation to XTEA primitive. The XTEA primitive is mitigated for SEU with time multiplexed method and the recovery control circuit switches to TEA primitive on detecting a SEU in XTEA operation.

A cost efficient crypto system architecture using TEA and XTEA security primitives is designed using AT89C51 controller. The architectures are designed, simulated with Keil IDE and implemented in AT89C51. A new key generation method is proposed with the timers T0 and T1 of the controller. The key generation architectures using different ways of seeding the timers are discussed. The context switching is introduced to switch the primitives from TEA to XTEA and vice versa. The timer based key generation is tested for serial and RF modes of communication.