Abstract

In 2007 NIST announced a public competition to develop a new cryptographic hash algorithm. This competition was announced due to the fact that in recent years, several successful attacks have been reported against SHA-1, thus raised significant alarming conditions against SHA-2. This new algorithm will replace the SHA-2 and can be used in various security applications in the information infrastructure. This paper focuses on efficient implementation of one of the SHA-3 candidates and round-3 finalist Grøstl on FPGA. The aim of this work is to achieve high throughput to area ratio (TPA) simultaneously by achieving high throughput by considering tradeoff between area and speed. The design is implemented as fully autonomous with both permutations P and Q are executed in parallel, and are equipped with I/O wrapper. The developed hardware has two designs, first with S-box is implemented using Look-Up-Table (LUT) or Distributed Memory and second with S-box implemented as Block RAM (BRAM). The implementation results obtained using virtex-5, when S-box is implemented as LUT has a throughput of 9.360Gbps and occupied 2253 Slices including I/O wrapper, thus achieves TPA of 4.154 and when S-box implemented as BRAM has throughput of 5.565Gbps and occupied 1356 Slices with wrapper, thus achieves 4.104 throughput per unit area (TPA).


citations

- SHA-3 Hardware Implementations: http://ehash.iaik.tugraz.at/wiki/SHA-3_Hardware-Implementations
- SHA-3 HARDWARE IMPLEMENTATION, Research Center for Information Security http://www.rcis.aist.go.jp/project/index-en.html
Efficient Hardware Implementation of SHA-3 Candidate Grøstl using FPGA

18-25.
- Vincent Rijmen, "Efficient implementation of the Rijndael S-box", Katholieke University Leuven, Dept. ESAT. Belgium.

Index Terms

Computer Science Security

Keywords