Abstract

Hash functions form an important category of cryptography, which is widely used in a great number of protocols and security mechanisms. In this paper the VLSI implementation of one of the 14 "second-round" candidates BLAKE for 64 bit and the round rescheduling technique design are proposed by using modulo 2n adder and adiabatic multiplexer for high throughput when compared to SHA 2.

References

Index Terms

Computer Science Security

Keywords
Sha-3 Blake 64 Low Power Cryptography Hash Function Encryption