{tag} {/tag}

IJCA Special Issue on International Conference on Electronics, Communication and Information systems

ICECI - Number 3

Year of Publication: 2012

Authors:

M. Rajaram

M. Arul Then Mathi

{bibtex}iceci1025.bib{/bibtex}

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

- Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender
- NIST, "Announcing the secure hash standard," FIPS 180-2, Technical report, 2002
- R. Lien, T. Grem bowski, and K. Gaj, "A 1 Gbit/s partially unrolledarchitecture of hash functions SHA-1 and SHA-512," in Topics in Cryptology - CT-RSA 2004, ser. Lecture Notes in Computer Science , vol. 2964. Springer Berlin / Heidelberg, 2004.
- X. Wang and H. Yu, "How to break MD5 and other hash functions, "in Advances in Cryptology - EUROCRYPT 2005, ser. Lecture Notes inComputer Science, vol. 3494. Springer Berlin / Heidelberg, 2005, pp. 19–35
- C. D. Cannière and C. Rechberger, "Finding SHA-1 characteristics: General results and applications," in Advances in Cryptology – ASIA CRYPT2006, ser. Lecture Notes in Computer Science, vol. 4284. SpringerBerlin / Heidelberg, 2006, pp. 1–20
- J. -P. Aumasson, L. Henzen, W. Meier, and R. C. -W. Phan, "SHA-3 proposal BLAKE," Submission to NIST, 2008, http://131002. net/blake/
- Luca Henzen, Student Member, IEEE, Jean-Philippe Aumasson, Willi Meier, andRaphael C. -W. Phan, Member, IEEE "VLSI Characterization of the Cryptographic Hash Function BLAKE" Oct. 2011
- D. J. Bernstein, "Cha-cha, a variant of Salsa20," 2007, http://cr. yp. to/ chacha. html
- "Call for a new cryptographic hash algorithm (SHA-3) family," Federal Register, Vol. 72, No. 212, 2007, http://www. nist. gov/hash-competition

Index Terms

Computer Science Security

Keywords

Sha-3 Blake 64 Low Power Cryptography Hash Function Encryption