Abstract

Cryptography is a technique that protects the information, which is in transit or in storage, from unauthorized or unexpected reveals. This paper demonstrates a Secure Hash Algorithm-3 (SHA-3) called Keccak, and also proposed a hardware architecture for the Keccak to support high speed security application. Since SHA-3 supports high level of parallelism, the proposed hardware architecture brings higher speed, in terms of bit rate and capacity, and also provides better security demanded by Internet of Things. This paper also demonstrates the architectural attributes of popular and real life cryptography techniques such as, Secure Hash Algorithm-1 (SHA-1), Secure Hash Algorithm-2 (SHA-2) and Advanced Encryption Standard (AES). In this research, the security techniques AES, SHA-1, SHA-2 and SHA-3 has been implemented on Virtex-5 FPGA device and their architectural attributes were captured. Finally, the proposed architecture of SHA-3 is compared with architecture of contemporary security techniques (AES, SHA-1, and SHA-2) in terms of speed, area and power. The comparison results shown that the SHA-3 architecture brought optimum performance over its contemporary security techniques.
High Speed Architecture for KECCACK Secure Hash Function

References

6. Marc Stevens hash clash, “Framework for MD5 & SHA-1 Differential Path Construction and Chosen-Prefix Collisions for MD5”.
10. ChristofPaar, Jan Pelzl, "Introduction to Public-Key Cryptography", Chapter 6 of "Understanding Cryptography, A Textbook for Students and Practitioners" (companion web site contains online cryptography course that covers public-key cryptography), Springer, 2009.
Volume 26, Number 3, pp. 18-22, April 2011.


20. AUTHORS PROFILE

21. Pasupuleti Sailaja received her MSc(Tech) in VLSI from Andhra University in 2013. She is currently pursuing her M.Tech (Communication Systems) in Christ University, Bangalore. Her area of interests are VLSI and Cryptography.

22. Mahendra Vucha received his B. Tech in Electronics & Communication Engineering from JNTU, Hyderabad in 2007 and M. Tech degree in VLSI and Embedded System Design from MANIT, Bhopal in 2009. He also received Ph. D degree in Electronic and Communication Engineering from MANIT, Bhopal (M.P), India. He is currently working as Asst. Prof in Department of Electronic and Communication Engineering at Faculty of Engineering, Christ University, Bangalore. His areas of interest are Hardware Software Co-Design, Analog Circuit design, Digital System Design and Embedded System Design.

Index Terms

Computer Science          Security

Keywords

Internet of Things, Secure Hash Algorithm, Filed Programmable Gate Array.