A Triple Hill Cipher Algorithm Proposed to Increase the Security of Encrypted Binary Data and its Implementation Using FPGA

Ashraf A.M. Khalaf *, Mona S. Abd El-karim *, Hesham F. A. Hamed*
**Department of Electronics & Communications Engineering, Faculty of Engineering, Minia University, Minia, Egypt*
ashkhalaf@yahoo.com , engmona1889@gmail.com , hfah66@yahoo.com

Abstract—Encrypted binary data security is an important task in the field of data communication systems since many decades. In this paper,we study the security problem and present a proposed triple hill cipher algorithm and its implementation on FPGA to encrypt any binary data such as images, audio, video … etc. The proposed algorithm uses three stages of a modified hill cipher to make the algorithm more robust and gives high level security of the data,each stage is considered a block cipher with a block length of 128 bits and key length of 256 bits. The message to be encrypted is processed by this block cipher in three stages. The keys are taken from random number generator. The proposed algorithm is promising to give better security.

Keyword—Hill cipher , 256 bit key ,cryptography, VHDL, FPGA.

Ashraf A. M. Khalaf (M'98) received his B.Sc. and M.sc. degrees in electrical engineering from Minia university, Egypt, in 1989 and 1994 respectively. Hereceived his Ph.D in electrical engineering from GraduateSchool of Natural Science and Technology, Kanazawa university, Japan, in Marsh, 2000. He is currently works as an associate professor at electronics andcommunications engineering Department, Minia university, Egypt.. His research interest includes digital signal processing and its applications in communications, neural networks, and optical communications.

Mona S. Abd El-karim She is currently a master course student for M.Sc. degree in Electrical Engineering (Communication and Electronics), Faculty of Engineering, Minia University, El-Minia, Egypt.

Hesham F.A. Hamed received the B.Sc. degree in Electrical Engineering, the M.Sc. and Ph.D. degrees in Electronics a nd Communications Engineering from EL-Minia University, ELMinia, Egypt, in 1989, 1993, and 1997 respectively. He currentlyis Professor and a Vice Dean for Postgraduate Studies & Researchers faculty of Engineering EL-Minia University. From 1989 to 1 993 he worked as a Teacher Assistant in the Electrical Engineering Department, ELMinia University. From 1993 to 1995, he wa s a visiting scholar at Cairo University, Cairo, Egypt. From 1995 to 1997, he was a visiting scholar at Texas A&M University, College Station, Texas (with the group of VLSI). From 1997 to 2003, he was an Assistant Professor in the Electrical Engineerin g Department, EL-Minia University. From 2003 to 2005, he was Associate Professor in the same University. From 2005 to 2007 , he was a Visiting Researcher at Ohio University, Athens, Ohio. He has published more than 65 papers and one book chapter. His research interests include analog and mixed-mode circuit design, low voltage low power analog circuits, current mode circuit s, nano- scale analog and digital integrated circuits design, and FPGA.