Multimed Tools Appl
DOI 10.1007/s11042-013-1790-4

Security analysis and improvement of a partial encryption scheme

Oussama Benrhouma · Houcemeddine Hermassi · Safya Belghith

Abstract This paper proposes to cryptanalyze a partial image encryption scheme. Security weaknesses were found in the cryptosystem consisting in the generation of the keystream. We then propose a modified version of the partial encryption scheme to enhance its security together with keeping the benefit of encrypting a reduced amount of data. Our contributions can be resumed in two points : we will first show the insecurity of the cryptosystem under study then we will propose a remedy to resist the described attacks.

Keywords WSN · Partial encryption · Security · Attacks

1 Introduction

In constrained environments devices such as Wireless Sensor Network (WSN) nodes, energy and memory. Time is considered as a very limited resource, hence cryptographic algorithms such as digital chaotic ciphers like those in [1, 12, 27] and traditional cryptographic techniques such as AES (Advanced Encryption Standard), IDEA(International Data Encryption Algorithm) and RSA(Rivest Shamir Adleman) are no longer suitable for practical encryption in a real time communication scenario. These constrained environments devices need some lightweight schemes to be implemented in order to reduce the memory and the energy needed, and to speed up the whole process. That's why, classical schemes of encrypting the raw data cannot be used in such environments. The best alternatives remaining are : 1) to design a special encryption algorithm for constrained devices such as Ultra-lightweight block ciphers like PRESENT [4] which occupies a reduced area requiring only 1570 gate equivalents (GEs). or Piccolo [24] which achieves both high security and notably compact implementation in hardware and only requires from 683 to 758 gate equivalents (GEs). 2) The use of joint encryption and compression schemes to combine the coding stage to the encryption stage in order to gain time and make the attackers' job harder. 3) The design of partial encryption schemes in order to reduce the amount of

O. Benrhouma (✉) · H. Hermassi · S. Belghith
SysComLab, Ecole Nationale d'Ingnieurs de Tunis (ENIT), Tunis, Tunisia
e-mail: oussama.benrhoumaa@gmail.com

Published online: 12 December 2013