Breaking an orbit-based symmetric cryptosystem

Ercan Solak\textsuperscript{a,}\textsuperscript{*}, Rhouma Rhouma\textsuperscript{b}, Safya Belghith\textsuperscript{b}

\textsuperscript{a} Computer Science and Engineering, Isik University, Turkey
\textsuperscript{b} Syscom Laboratory, Ecole Nationale d'Ingénieurs de Tunis, Tunisia

\begin{abstract}
We report a break for a recently proposed class of cryptosystems. The cryptosystem uses constant points of a periodic secret orbit to encrypt the plaintext. In order to break the system, it suffices to sort the constant points and find the initial fixed point. We also report breaks for modified versions of the cryptosystem. In addition, we discuss some efficiency issues of the cryptosystem.
\end{abstract}

1. Introduction

Chaos-based cryptography has attracted increasing research effort during the last decade. Many proposals have been made with different architectures, including stream ciphers, block ciphers, search-based ciphers, image ciphers, and public-key ciphers. At a higher level of classification, we can separate chaos cryptography into analog and digital architectures. A more elaborate classification can be found in [1].

Chaotic stream ciphers use chaotic systems to generate pseudo-random sequences which are then used to algebraically mask the plaintext sequence. Chaotic block ciphers inject a plaintext block into a chaotic system and use a transformation of the state variables as the ciphertext.

Search-based chaotic cryptosystems were first proposed by Baptista in [2]. In this scheme, a plaintext character is encrypted into the number of iterations required to reach the set corresponding to the particular character. Several variations of Baptista-type cryptosystems have been proposed [3–6]. However, many of these proposals were found to be weak against simple types of attack [7–10].

As chaos-based cryptography has grown through many proposals [11–13], there has also been a dual development of the cryptanalyses of these proposals [7–10]. Some basic frameworks and requirements in the design of chaos-based cryptosystems are investigated in [14,15], and some analyses and new design of digital chaotic ciphers are investigated in [1].

In this work, we cryptanalyze a cryptosystem recently proposed in [16]. The cryptosystem under study uses a nonlinear dynamical system. The cryptosystem exploits the idea of nonlinear mappings and their fixed points to encrypt information. In particular, the plaintext consists of symbols (characters) from a known alphabet (e.g. ASCII), while the ciphertext consists of constant points of the orbit. The secret key of the algorithm is the ordering of the constant points of a periodic orbit. In its most basic form, the chaotic system is iterated as many times as the plaintext character and the state of the chaotic system is sent as the ciphertext.

\textsuperscript{*} Corresponding author.
E-mail address: ercan@isikun.edu.tr (E. Solak).

0895-7177/ – see front matter © 2011 Elsevier Ltd. All rights reserved.