Conditions for counter measure against one time pad attack on Baptista type cryptosystem

ABSTRACT

In 1998, M.S. Baptista proposed a chaotic cryptosystem using the ergodicity property of the simple low-dimensional and chaotic logistic equation Xn+1=bXn+(1-Xn)where X0 and b are the secret keys. This cryptosystem hasthe ability to prevarious ciphers responding to the same message input. Since then, many cryptosystems based on Baptista's work has been proposed. However, over the years research has showand vulnerable to attacks and is widely discussed. Among the weaknesses are the non-uniform distribution of ciphertexts and succumbing to the one-time pad attack(a type of chosen plaintext attack). The one-time pad attack which was constructed by Alvarez (2003) proved that the ergodic cipher put forward by Baptista behaves as a one-time pad which reuses its key, and as a result, is easy to break. The method of attack is based on the symbolic dynamics of one dimensional quadratic map. The focus of our research is to overcome the one-time pad attack. As pointed out by Alvarez, obtaining the one-time pad is as good as knowing the key (i.e. 0X and b), making the system 100% vulnerable. We give a formal treatment for the one-time pad attack. We derive definitions and give mathematical explanations for this phenomenon. Finally, we give a theorem, if satisfied by a "counter measure" method, would result in this cryptosystem being invulnerable against the one-time pad attack.

Keyword: Chaotic cryptosystem; Ergodicity; Cryptanalysis; Logistic map