Abstract

A novel encryption system to increase security in a three tier manner without any additional complexity is proposed in this paper. The encryption block here is a Shrinking generator which is a Linear Feedback Shift Register (LFSR) based stream cipher system in which controlled randomness provides security. The channel coding technique used is Turbo code that performs very well and provides results near Shannon's Limit. The design of interleaver used in turbo code provides security while channel coding. Puncturing pattern designed for channel coding further increases the security of the system and improves the code rate also. Security of the system is achieved by hiding the keys used in code generation and puncturing from unintended users. For an intended user, performance of the channel coding system is further improved by using Soft Input Decryption (SID) technique. The hardware complexity of the proposed Shrinking Generator Based Cipher (SGBC) is compared with joint coding cryptographic schemes available in literature. Improved Linear Consistency Attack is mounted to analyze the security of the proposed system and the results show that a significant increase in security could be achieved without any additional increase in complexity.
References


- Qian Mao; Longji Sun; ChuanQin: "Joint Error Correction and Encryption Scheme"

- Silvio A. Abrantes, “From BCJR to turbo decoding: MAP algorithms made easier © Silvio A. Abrantes, April 2004

**Index Terms**

Computer Science  
Security

**Keywords**

Turbo code  
Puncturing  
Soft Input Decryption  
Improved Linear Consistency  
Attack