A new approach to data encryption based on the synchronous stream cipher with bit-level diffusion

ABSTRACT

Most proposed stream ciphers are cracked through vulnerability of input and output. This paper is focused on the encryption function and the security tradeoff between pseudorandom number generators and the encryption function. Despite the focus on the security of the key generation, there is still considerable potential for attacks on the secret key as long as the encryption function leaks valuable information about the key to the attacker. Hence, it is important to study the possibility of constructing a new encryption model based on a stream cipher, while considering security and throughput tradeoffs. In this paper a new approach to data encryption based on its integration with a synchronous stream cipher is presented. This new approach is named the "Permuted Synchronous Stream Cipher" (PSSC). The sophisticated design of the PSSC for providing diffusion to stream ciphers allows it to be easily incorporated into most of the existing proposed stream ciphers to provide better security. The PSSC key stream is constructed from two parts, namely the key- bits and a corresponding diffusion maps. The method involves inserting random bits into the ciphertext followed by bit rotation and XORing bitwise. Therefore, any statistical pattern or information about the secret key that may be reflected in or leaked into the cipher's output can be masked by performing simple bit diffusion on the ciphertext based on a pseudorandom sequence of diffusion maps. We believe that the proposed method can achieve a throughput rate that is fast enough for real-time data protection with better security.

Keyword: Diffusion; Diffusion map; Stream cipher; PSSC