Key transformation approach for Rijndael security.

ABSTRACT

The aim of the study is to improve the security of Rijndael key scheduling by increasing the bit contusion and diffusion of the Rijndael subkey, Rijndael is a block cipher designed by Joan Daemen and Vincent Rijmen. It is a combination of security, performance, efficiency, implementability and flexibility that makes it the best selection for Advanced Encryption Standard (AES). However, the 128 bit Rijndael key schedule does not satisfy the frequency (bit confusion) test for majority of subkeys and does not satisfy the avalanche (bit diffusion) test for any subkeys. These contribute to some attacks in the key schedule. Thus, a new transformation method which is called Shiftrow is proposed into the 128-bit Rijndael Key Schedule based upon information principles (bit confusion and diffusion properties). The new method has shown positive results in terms of the bit confusion and diffusion of subkey and it has increased bit confusion and diffusion compared to the subkey of the original Rijndael key schedule.

Keyword: Cryptography; Rijndael algorithm; Key transformation approach.