A faster version of rijndael cryptographic algorithm using cyclic shift and bit wise operations

ABSTRACT

Doing arithmetic in finite field is the key part to the implementation of communication and coding system including the newly developed Rijndael the Advanced Encryption Standard (AES). This encryption standard uses KeyExpansion, ByteSub, Mixcolumn and Shiftrow functions which consists of XOR, inverse, multiplying and swap modules. Among them, inverse and multiplier are the most complex modules with longer delay. These modules are included in the Mixcolumn function. From the proposal of AES, the Mixcolumn function was suggested to solve the problem of delay by using look-up tables. This function can be integrated into a bigger table to replace the calculations of inverse and multiply operations, if it provides enough memory. In fact, too many tables are needed for various irreducible polynomials that this system is not flexible and expandable. The area for lookup tables becomes huge when multiple round units are implemented. This research proposes the use of cyclic shift and bit wise XOR operation as new approach to replace the lookup table. The principle benefit of using this new approach over the transform from Rijndael block cipher is speed. This new approach has shown the excellent result, which faster then Rijndael. The new approach algorithm speed increment has consistently increased in between 18% to 22% microsecond for encryption and 30% to 34% for decryption compared to Rijndael algorithm depending upon the key length.

Keyword: AES, speed, cyclic shift, exclusive OR, mixcolumn transformation,table lookup