A Novel Method of Creating Block Ciphers Provably Immune to Linear and Differential Cryptanalysis

Perlicki, Szymon (School: Szkola Podstawowa nr 28 im. Generala Leopolda Okulickiego we Wroclawiu)

It is often the case that the size of some data is fixed and it might be encrypted all at once. Currently, in such a situation, we use a stream cipher or a block cipher with some mode of operation which has to be implemented additionally. Both of these options require storing additional information such as an IV, a nonce or a MAC, which might be a significant part of the data, if the data size is small. Unfortunately, up to now, ciphers with a larger block size have required a larger diffusion layer, which have taken up a lot of memory and made the cipher implementation harder. In this study a new method of constructing block ciphers is proposed. The presented construction consists of parallel SP-networks which recursively interchange data using a small diffusion layer, the size of which is recursively doubled by a presented algorithm. The method enables the creation of ciphers provably resistant to linear and differential cryptanalysis. These would be easy to parallelize and would make it possible to use a small, easy to store diffusion layer. The minimum required number of rounds for this method is derived. A proof is conducted, so that every encryption algorithm created using this method is resistant to linear and differential cryptanalysis under the given minimum required number of rounds.

Awards Won:

King Abdulaziz &amp

his Companions Foundation for Giftedness and Creativity: On-line Mawhiba Universal Enrichment Program

King Abdulaziz &amp

his Companions Foundation for Giftedness and Creativity: Award of $500

Association for Computing Machinery: Second Award of $3,000