Mathematical Problems of Computer Science 33, 121--126, 2010.

Linear Cryptanalysis of Block Ciphers in the Cluster Computational Environment

Melsik Kyuregyan, Ofelya Manukyan and Edita Harutyunyan

Institute for Informatics and Automation Problems of NAS of RA
e-mail: melsik@ipia.sci.am, manofa81@yahoo.com

Abstract

This paper presents some results concerning synthesis of new cryptosystems equivalent to SAFER+ and SAFER++ to perform their linear cryptanalysis in the cluster computational environment. A parallel software package "LinearCryptanalyser" is developed to find such "Armenian Shuffles" which were chosen as secure against differential cryptanalysis and now will be checked if they are also secure against linear cryptanalysis. The research is focused on both theoretical and practical aspects of existence of linked I/O sums. The software package "LinearCryptanalyser" analyzes the existence of linked I/O sums and the absence of such sums will indicate cryptoresistance of block ciphers against last-round attack.

.

References

1. J. L. Massey, G. H. Khachatrian and M. K. Kuregian, ``Nomination of SAFER+ as Candidate algorithm for the Advanced Encryption Standard (AES)", Submission document from Cylink Corporation to NIST, June 1998.
2. J. L. Massey, G. H. Khachatrian and M. K. Kuregian, ``Nomination of SAFER++ as Candidate Algorithm for the New European Schemes for Signatures, Integrity, and Encryption (NESSIE)", Submission document from Cylink Corporation, 2000.
3. C. Harpes, ``Cryptanalysis of iterated block ciphers", ETH Series in Information Processing, editor: James L. Massey. v. 7, Hartung-Gorre Verlang Konstanz, 1996.
4. C. Harpes, G. G. Kramer and J. L. Massey, ``A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma", Presented at Eurocrypt '95.
5. C. Harpes, ``A generalization of linear cryptanalysis applied to SAFER", Signal and Info. Proc. Lab., CH-8092 Zurich, March 9, 1995.

Բլոկային ծածկագրման համակարգերի գծային վերծանումը կլաստերային հաշվողական համակարգում

Մ. Կյուրեղյան, Օ. Մանուկյան և Է. Հարությունյան

Ամփոփում

Աշխատանքում նկարագրված են արդյունքներ SAFER+ և SAFER++ բլոկային ծածկագրման համակարգերի նոր տարբերակի կառուցման վերաբերյալ: Ստեղծվել է զուգահեռ հաշվարկների “LinearCryptanalyser” ծրագրաշար, որի օգնությամբ փնտրվում են այնպիսի "Armenian Shuffle" կոորդինատային տեղափոխություններ, որոնց համապատասխան բլոկային ծածկագրման համակարգերը կլինեն կայուն դիֆերենցիալ և գծային վերլուծությունների նկատմամբ: Հետազոտությունները կատարվել են կապակցված մուտք/ելք գումարների գոյության ինչպես տեսական, այնպես էլ կիրառական տեսանկյուններից: “LinearCryptanalyser” զուգահեռ հաշվարկների ծրագրաշարը թույլ է տալիս ուսումնասիրել կապակցված մուտք/ելք գումարների գոյության հարցը, իսկ նման կապակցված գումարների բացակայությունը վկայում է ուսումնասիրվող բլոկային ծածկագրման համակարգերի կայունության մասին գծային կրիպտոանալիզի նկատմամբ: