Vesna Dimitrova Ph.D., Associate proffesor
Faculty of Computer Science and Engineering
University Sts. “Cyril and Methodius” in Skopje, Macedonia
e-mail: vesna.dimitrova@finki.ukim.mk

OPINION

for the dissertation

STUDY OF THE CONDITIONS FOR LINEAR CRYPTANALYSIS IN FEISTEL NETWORKS

submitted by

Robert Yordanov Tsenkov,

“Државна агенција НАЦИОНАЛНА СИГУРНОСТ”, Sofia, Bulgaria,

for obtaining degree

Doctor of Informatics at Institute of Mathematics and Informatics,

Bulgarian Academy of Science

The thesis has 143 pages written in Bulgarian language. It consists of List of Figure (with 1 Figure), List of Tables (with 25 Tables), Introduction, five Chapters, Conclusion, Bibliography (with 131 Citations) and four Appendixes.

The motivation of doctoral thesis, actuality of the topic, goals and objectives of the thesis, research methodology, outcomes and structure of the thesis is given in Introduction.

In Chapter 1 a survey of basic concepts in cryptography and cryptanalysis is given. Here is presented fundamental aspects of cryptographic mechanisms, basic principles of construction of cryptographic algorithms, several types of cryptanalyses (linear, differential,..), description of Feistel networks, their properties and applications.

Chapter 2 contains notations, definitions, theorems and properties, directly concerned to the investigations in the thesis. Here is given description of DES algorithm, several properties of linear cryptanalyses, construction and complexity of linear attacks.

In Chapter 3, named “Modified family of algorithms”, modified DES algorithm with embedded parity check in the S-boxes is presented. Here, the influence of inserting a bit of additional linearity in the round's output of DES by embedding parity check in the outputs of all its S-boxes is discussed. The research is focused on finding best characteristics for 3 to 20 rounds of the modified cipher, when the parity bit position is the same in all S-boxes. It is given new search algorithm, named “Basic Search Algorithm (BSA)”. The aim of the BSA is to construct all *n*-round ($n \geq 3$) characteristics with non-zero linear bias. It is shown that such embedding reduces the effectiveness of optimal I-round and 3-round characteristics, but it is not true for greater number of rounds. At the end, it is concluded that the modification of this type does not necessarily mean a reduction or growth in the effectiveness of interest. So, successful attacks based on this approach have varying magnitude of complexity and at the same time they are not inevitably more efficient than the corresponding primary attacks towards the original cipher.

In Chapter 4 a linear cryptanalysis of a family of modified DES ciphers with even weight S-boxes is presented. Here is given the behavior (from the perspective of linear cryptanalysis) of a wider family of modified DES ciphers whose parity check position into each individual S-box is picked up arbitrarily and independently from those into the others is given. The research is focused on finding multi-round linear characteristics for thus modified DES ciphers having maximal effectiveness. The analysis of the experimental results leads to conclusion that ciphers derivable from the DES possess good resistance (in most cases even better than the DES itself) towards the primary attacks of indicated type.

In Chapter 5 the parity check is considered as a part of commonly defined affine transformation. Some properties of Linear Approximation Tables (LAT) are given and results are generalized.

Conclusions and further work is presented in Conclusion. Here is given thesis contribution, directions for practical applications of obtained results and some idea for further research.

At the end, four Appendixes: 1) LAT for first S-box of modified algorithm, 2) best multi-round linear characteristics, 3) additional details for 16-round's best approximative expressions and 4) complexity of the search algorithm – BSA are given.

The results of the dissertation "Study of the conditions for linear cryptanalysis in Feistel networks" are presented with talks given at several conferences and published in the following papers:

1. Y. Borissov, P. Boyvalenkov, R. Tsenkov. Linear cryptanalysis and modified DES with parity check in the S-boxes. *Second Conference on Cryptography and Information Security in the Balkans*, *LNCS* 9540, Springer-Verlag, 2016, pp. 60–78;

2. R. Tsenkov, Y. Borissov. Narrow sense linear cryptanalysis of a family of modified DES ciphers with even weight S-boxes. *Proceedings of Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory*, 2016, pp. 284–289.

3. Y. Borissov, P. Boyvalenkov, R. Tsenkov. On a Linear Cryptanalysis of a Family of Modified DES Ciphers with Even Weight S-boxes. *Cybernetics and Information Technologies*, 16(4), IICT-BAS, 2016, (in print).

Conclusion: The dissertation "Study of the conditions for linear cryptanalysis in Feistel networks" submitted by Robert Tsenkov is clear and readable. It gives valuable contributions in the field of cryptography and cryptanalyses. The results of this thesis are important for new research problems and they are a challenge for further investigations.

Having in mind the above considerations it is my pleasure to support Robert Tsenkov for obtaining the degree Doctor of Informatics.

25.01.2017 Member of Scientific council

Skopje Vesna Dimitrova