*Review of a Doctoral Thesis at FIT BUT*

**Doctoral thesis** (hereinafter referred to as "thesis"), title of the thesis:
**Evolution of Cryptographically Sound Boolean Functions**

**Name of the doctoral student** (hereinafter referred to as "student"), name and surname:
**Jakub Husa**

---

**Name and institution of the reviewer** (full name of the reviewer, full name and country of the institution):

Domagoj Jakobović (full professor)

University of Zagreb, Faculty of Electrical Engineering and Computing

Unska 3, 10000 Zagreb, Croatia

---

## Overview

The thesis under consideration deals with the heuristic design of Boolean functions with good cryptographic properties using evolutionary algorithms. I am pleased to report that the thesis is very well written and demonstrates the candidate's ability to conduct independent research. The candidate has accurately described the research problem, objectives and methodology and has ensured that the material is presented in a comprehensive and easy to understand manner. After a thorough review, I am confident that the dissertation fulfils all requirements within the doctoral degree study. In the following sections, a more detailed assessment will be made according to the template provided.

## I. Thesis

### Appropriateness and relevance

The field of optimising Boolean functions in connection with applications in cryptography is certainly not new, as many researchers have worked on this problem. However, the cryptographic community has long been satisfied with the existing solutions with scarce attempts to improve the current state of the art. Most of the available results in the field of cryptography have been obtained using exact mathematical methods such as primary algebraic constructions. The disadvantages of this approach include the fact that only a tiny fraction of the possible solutions are obtained and that one is not able to directly create functions with combinations of the desired properties.

The application of metaheuristic algorithms, which iteratively improve the solution by navigating the search space in an efficient way, proves to be a viable alternative to the usual approach. In this context, the thesis presents a detailed motivation for the application of evolutionary algorithms, and in particular genetic programming, to the design of Boolean functions. The candidate correctly identifies two facets of the problem; the first is the one inherent to the domain, where there are no techniques that can guarantee solutions of even better quality, especially considering many possible optimisation criteria that cannot be handled with algebraic constructions. The candidate selects and describes relevant properties of Boolean functions and their combinations in two application areas of cryptography.

The second relevant problem addressed in the thesis is the relative lack of insight into the effectiveness of the evolutionary approaches applied to the problem. In addition, the thesis identifies alternative evolutionary techniques that might be well suited to Boolean optimisation and suggests suitable modifications for their application in this area. All of this makes the material presented relevant within the research field, as the findings of the thesis can make future research efforts much more effective.

A summary of the contributions of the thesis

The design of Boolean functions for cryptography covers many different applications and use case scenarios. Due to a large amount of existing research, it is not trivial to assess the significance of new findings, as only certain function properties and their combinations are relevant for the target application. In this thesis, the candidate has identified potential application scenarios in which certain Boolean function properties are of interest and has presented the corresponding properties and their combinations. This is a thankless task as cryptography standards are a moving target and previously relevant cryptographic primitives and their properties may no longer be relevant in the near future. However, the motivation for the identified target applications is clearly stated in the thesis and can also serve as a guide for other researchers.

Another line of research is concerned with the application of previously unused variants of genetic programming in the design of Boolean functions. The candidate has identified the current disadvantages of commonly used approaches and proposed alternative techniques to overcome these difficulties. Many researchers tend to focus on the methods that have been successful in the past and may overlook the advantages of previously unused methods. In the application of evolutionary computation, as well as all metaheuristics, this includes the data structure and associated (genetic) operators that are able to represent the target solution and traverse the enormously large problem search space effectively. The thesis presents a detailed description of these alternative methods, such as linear genetic programming, and all the necessary steps required for their application in the Boolean domain.

Since evolutionary algorithms are based on repeated objective evaluation, usually in very large numbers, the execution of the algorithm is associated with high computational costs. This hinders the applicability of evolutionary algorithms in cases where the objective evaluation is the most time-consuming part of the algorithm loop, as is the case when designing Boolean functions. Given today's computational resources, parallelisation of population-based algorithms is a viable option. In this thesis, different levels of parallelisation are investigated and applied to the problem at hand, achieving significant performance improvements. The types of parallelisation – an implicit bit-level parallelisation, explicit parallelisations such as the island model or the master-worker model - are described in detail and their relative efficiency is compared with the sequential implementation of algorithms.

Evaluating the efficiency of different algorithms and their components on a real-world problem is never trivial, and much effort is devoted to predicting the performance of algorithms on unknown problem instances belonging to known problem classes. Within the scope of this thesis, a diverse benchmark suite for Boolean problems is proposed, along with baseline results for algorithm comparison. The benchmark suite includes problems for designing Boolean functions for cryptographic domains of varying size and complexity. The key feature of this problem category is that the optimal input-output mapping is not known, as is the case for the other problem classes. This feature and the variety of properties that need to be optimised simultaneously make this benchmark problem very difficult and its inclusion significantly increases the overall benefit of the proposed benchmark suite.

An important subclass of cryptography-relevant functions are bent Boolean functions, which achieve the highest possible nonlinearity. Directly evolving bent Boolean functions in a larger number of variables has proven to be difficult, as it requires a non-scalable amount of computational time to achieve the required – partly still unknown – levels of nonlinearity. Taking advantage of the inherent properties of Boolean nonlinearity, such as affine invariance and the ability to construct bent functions from smaller functions with fewer variables, the candidate has developed a directed mutation operator. The operator can be considered semantic as it takes into account the nonlinearity property in its application. In fact, the operator consists of several actions applied randomly, but with additional information to guide the changes in the individual. Unlike some general-purpose crossover or mutation operators, the proposed mutation operator has achieved excellent results considering the evolution of bent functions, with performance improvements even exceeding the parallelisation effects on multiple processing elements.

Novelty and significance:

The contributions achieved offer many new research opportunities and provide valuable information for other researchers in this field.

The results in optimising certain cryptographic properties of Boolean functions have surpassed those found in previous publications, demonstrating the merits of the methods presented in this thesis. The inclusion of alternative variants of genetic programming, which have not yet been investigated in this context, has shown that the different GP representations compete with each other. No single representation dominates over all others for all optimisation criteria, and they require different evolutionary parameters to achieve the best possible results. These findings are discussed in detail, which should be helpful for future applications of genetic programming to this problem.

Several parallel evolutionary models were used in this thesis. However, not all types of parallelisation are equally effective or even useful for this problem, as the results show. These results point out the efficient ways to speed up the execution of the algorithm and report on the scenarios where parallelisation is not recommended. In particular, the island model has been shown to be more efficient than the master-worker model, but only for a two-dimensional communication pattern. Parallelisation at bit level can be combined with both explicit models and is always advantageous.

The development of metaheuristics is usually not guided by their direct application to real-world problems, but by assessing the performance of different prototypes on commonly agreed sets of benchmark problems. One of the indirect results of this thesis is the inclusion of cryptographically sound Boolean functions in the general benchmark suite for Boolean functions, making them more visible to researchers from the EA community. Since these functions are the only black-box problem in this benchmark, we can expect that new research will provide even better results than the currently best-known ones.

The new mutation operator developed to optimise the nonlinearity of Boolean functions could significantly influence future research in this direction. Besides providing superior performance, an additional advantage is the fact that it is compatible with all genetic programming variants used in this thesis and in the relevant literature. Since it can significantly reduce the computational effort required to obtain solutions of the desired quality, it could be incorporated into other algorithm variants used in similar projects in this research area.

Evaluation of the formal aspects of the thesis:

The structure of the thesis is well organised and easy to follow. The research background can serve as an excellent introduction to the topic for all interested researchers; it is detailed and comprehensive and contains all relevant references up to the current year of publication. The research summary serves as an overview of the topics investigated in the thesis and provides enough information to adequately describe the contributions achieved.

The language used in the thesis is of a very high standard, with only a few minor errors, which are negligible. The writing quality is excellent throughout and contributes to the overall coherence and readability of the manuscript.

Quality of publications

The results of the research carried out as part of the doctoral study have been published in several different venues. The candidate has presented a solid number of publications, several of which have appeared in internationally recognised journals and at relevant conferences. The dissertation lists all relevant details of each publication as well as the conference rank or impact factor of the journal. The chosen venues adequately reflect the topic of the dissertation and are published in relevant areas of computer science. The visibility of these publications is evident and the candidate has already attracted the attention of other researchers working on similar topics. Of particular note is the publication in a prestigious CORE A-rank FOGA conference, written in collaboration with high-level researchers in the field.

## II. Student's overall achievements

Overall R&D activities evaluation:

The manuscript of the thesis contains all the necessary background information on the research topic and serves as an excellent source for the introduction to the problem at hand. The dissertation refers to the relevant literature and manages to comprehensively explain the current state of the art approaches and possible future avenues of research.

During the doctoral studies leading to this thesis, the candidate has conducted research on several relevant topics in this area. The results of his research have been published in a number of high quality publications and given in several conference presentations, some of which I have attended myself. Publishing results that represent the intersection of two different fields – in this case cryptography and evolutionary computation – is generally more difficult than reporting research that is confined to a specific field. The candidate successfully overcame this challenge and managed to make an active contribution to an already competitive topic.

Assessment of other characteristics (optional):

The candidate has participated in publication of papers with several international coauthors and has been included in collaboration with scientists and research groups from different universities.

## III. Conclusion

The motivation and research questions of the thesis are clearly formulated, and the experimental investigation is well defined and detailed. The text is clearly written and easy to follow. Overall, the research objectives have been met and the contributions are evident. The results published as part of this PhD thesis may be of use to other practitioners in the field and promote the application of genetic programming in the design of cryptographically sound Boolean functions. The proposed methods have shown that the candidate has a strong background in the field and is able to take advantage of different methods to develop appropriate solutions to the given problem. The candidate has demonstrated the required qualities for obtaining a doctorate degree by conducting independent research in an already competitive application area. In conclusion, I am confident that the candidate's thesis and achievements satisfy all the requirements for the award of an academic degree in doctoral studies.

Zagreb, 20. 09. 2024

Signature of the reviewer: