



Review on the abstract of the PhD thesis of Perov Artem
for the PhD degree in technical sciences on the speciality
05.13.17 - Theoretical foundations of computer science

To whom it may concern,

This is a review report on the abstract of the PhD thesis of Perov Artem titled

Universal method of constructing decisive rules using convolutional neural networks for analysis of pseudo-random sequence generators based on iterative block ciphers

The main idea in the thesis of Perov A. is devoted to the problems of analyzing the output sequences of pseudo-random number generators, which have important applications in different computer science areas. In the thesis, Perov A. has developed a new approach to the process of analyzing pseudorandom sequence generators, and shown that the approach can significantly reduce the sampling length for statistical analysis. The proposed method is based on the recognition of output sequences that are transformed to digital images, which can be classified by convolutional neural networks with high accuracy. The proposed method is novel in the sense that inception V3, ResNet, and EfficientNet architectures usually do not solve such tasks. This methodology allows for evaluating the sample entirely, without taking into account separate values. According to the comparison with previously known results, it is confirmed the suitability of the proposed method and some advantages over analytical and empirical statistical methods. The generators proposed in the thesis are solid algorithms, of which the effectiveness has been previously proven in many scientific papers. The proposed method in the thesis re-confirm the effectiveness of those generators, which validates the idea. The research in the thesis is an interesting and successful piece of scientific work. It is worth noting that the approach of the thesis is generic and could be applied in other iterative generators, like hash functions, pseudorandom generators in programming languages, etc..

In my opinion, the thesis of A. Perov is a completed scientific research with certain scientific novelty. I consent to the inclusion of my personal review in documents related to the defence of the thesis of Perov A. and their further processing.

Yours sincerely,

A handwritten signature in black ink, appearing to read "Chunlei Li".

Chunlei Li
Associate Professor,

The Selmer Center on Secure Communications,
Department of Informatics, University of Bergen, Norway
Phone: (+47) 55584013



[Эмблема: Бергенский
университет]

Бергенский университет
Кафедра информатики
Центр передовых технологий
N-5020 Берген, Норвегия

Отзыв на автореферат диссертации Артёма Перова,
на соискание ученой степени кандидата технических наук по специальности
05.13.17 – Теоретические основы информатики

Вниманию всех заинтересованных лиц.

Настоящий документ является отзывом на автореферат диссертации Артёма Перова

Универсальный метод построения решающих правил с использованием сверточных нейронных сетей для анализа генераторов псевдослучайных последовательностей на основе итеративных блочных шифров

Основная идея диссертации А. Перова посвящена проблемам анализа выходных последовательностей генераторов псевдослучайных чисел, которые являются важным приложением в различных областях компьютерных наук. В работе А. Перов разработал новый подход к процессу анализа генераторов псевдослучайных последовательностей, и показал, что этот подход позволяет сократить длину выборки для статистического анализа. Предлагаемый метод основан на распознавании выходных последовательностей, преобразованных в цифровые изображения, которые могут распознаваться с помощью сверточной нейронной сети с высокой точностью. Предлагаемый метод является новым в том смысле, что архитектуры Inception V3, ResNet и EfficientNet обычно не решают таких задач. Эта методология позволяет полностью оценить выборку, не принимая во внимание отдельные значения счётчика. По сравнению с ранее известными результатами подтверждают пригодность предложенного метода и наличие некоторых преимуществ перед аналитическими и эмпирическими статистическими методами. Генераторы, предложенные в диссертации, представляют собой известные алгоритмы, эффективность которых ранее была доказана во многих научных статьях. Предлагаемый в автореферате метод повторно подтверждает эффективность этих генераторов. Научное исследование, выполненное в диссертации, является интересным и законченным. Стоит отметить, что подход, реализованный в диссертации, универсален и может быть применен к разным итеративным генераторам, таким как хеш-функции, псевдослучайные генераторы в языках программирования и т. д.

На мой взгляд, диссертация А. Перова – законченное научное исследование с определенной научной новизной. Я согласен на включение моих персональных данных в документы, связанные с защитой диссертации Перова А. и сопутствующими процессами.

Искренне ваш,

[Подпись]

Чанли Ли (Chunlei Li),

Доцент

Центр по безопасной связи Сельмера

Кафедра информатики, Бергенский университет, Норвегия

Тел. (+47) 55584013

[Печать: Бергенский университет* Кафедра информатики]

Перевод с английского языка на русский верен

Переводчик отдела переводов ДМС СФУ

Тел: +7 (391) 206-27-99; E-mail: AZhigalova@sfu-kras.ru

Жигалова А.И.

