Федеральное государственное бюджетное
учреждение науки
ИНСТИТУТ МАТЕМАТИКИ
им. С.Л. Соболева
Сибирского отделения
Российской академии наук
(ИМ СО РАН)
630090 Новосибирск, пр. Академика Коптюга, 4
Для телеграмм: Новосибирск, 90, Математика
Тел.: (8-383) 333-28-92. Факс: (8-383) 333-25-98
E-mail: im@math.nsc.ru
12.03.2021 № 250-2-35
На № 500 от 01.02.2021

УТВЕРЖДАЮ

Директор Института математики
им. С.Л.Соболева
ак. РАН, д.ф.-м.н.
Гончаров Сергей Савостьянович

_____

12 марта 2021 года.

ОТЗЫВ

ведущей организации на диссертацию

Перова Артёма Андреевича

«Универсальный метод построения решающих правил с использованием свёрточных нейронных сетей для анализа генераторов псевдослучайных последовательностей на основе итеративных блочных шифров»,

представленной на соискание ученой степени кандидата технических наук по специальности 05.13.17 – «Теоретические основы информатики»

Одной из наиболее актуальных задач криптографии – на протяжении достаточно долгого времени в прошлом (особенно стоит отметить вторую половину XX века) и особенно сейчас – является задача распознавания «меры случайности» той или иной криптографической последовательности. Исторически, эта задача возникала, например, при дешифровании текстов на естественном языке – необходимо было уметь статистически отличать дешифрованный текст от случайного, и тем самым находить правильный открытый текст. Последние 30-40 лет задача анализа псевдослучайных последовательностей стоит особенно остро. Она непосредственно связана *с возможностью атак на генераторы таких последовательностей*, повсеместно используемые в симметричной криптографии. По сути, каждый метод криптоанализа симметричных шифров из группы статистических методов (таких как, линейный, дифференциальный и другие), представляет собой конкретизированную *атаку различения*: различения последовательности шифртекстов и действительно случайной последовательности. Любое отличие рассматривается, как «зацепка», новая возможность для криптоаналитика. Соответственно, отсутствие отличия или обоснованная сложность

в его обнаружении естественным образом говорит о стойкости криптографической системы, построенной с использованием данного генератора. Следует отметить, что несмотря на большой интерес к данной задаче во всём мире, продвижения в её решении минимальны.

Диссертационная работа А.А.Перова посвящена новому подходу к анализу случайности последовательностей, порожденных с помощью итеративных блочных шифров. Рассматриваются последовательности шифртекстов, полученных после зашифрования некоторой исходной последовательности открытых текстов с помощью итеративного шифра с фиксированным числом раундов в режиме CTR. Последовательности анализируются с помощью специально обученной нейронной сети и после перевода их в графические изображения. Предложен ряд важных и универсальных новшеств, позволяющих добиться более эффективного анализа «неслучайности» рассматриваемых последовательностей.

В первой главе работы приводится краткий обзор использующихся в настоящее время статистических тестов и подходов, которые применяются для анализа случайности той или иной криптографической последовательности. Отдельное внимание уделяется методам порождения псевдослучайных последовательностей, основанным на использовании итеративных блочных шифров.

Вторая глава посвящена методу построения решающих правил для анализа генератора псевдослучайной последовательности на основе свёрточной нейронной сети MLSA. При этом активно анализируются не сами псевдослучайные последовательности, а графические изображения, полученные из них. Так, графические изображения, полученные из выходной последовательности блочного шифра с неполным (малым) числом раундов имеют выраженную текстуру, которая «улавливается» нейросетью. При этом закономерности «улавливаются» лучше, именно после перехода к графической интерпретации последовательности. Для анализа выбрана нейронная сеть Inception ResNet-V2, имеющая достаточно высокую производительность. Производилась генерация ряда случайных последовательностей с помощью разработанного программного комплекса «УНИБЛОКС-2015», перевод последовательностей в графическое представление с помощью разработанной программной утилиты на C++, обучение нейронной сети по различным сценариям и др.

В третьей главе приведено практическое тестирование методов, предложенных во второй главе, и описаны особенности новой разработанной информационно-аналитической системы. Рассмотрены основные приёмы программирования и результаты тестирования алгоритмов с помощью нового

метода, а также с помощью классических статистических тестов. В частности, отмечено, что метод MLSA, работающий по сценарию различения соседних раундов шифра, лучше находит отличия в последовательностях, сгенерированных с помощью шифра, чем группа классических статистических тестов. Предложен подход, позволяющий объединить в единую систему реализации алгоритмов и использовать методику, основанную на варьировании параметров генераторов псевдослучайных последовательностей. На основе экспериментов сделан вывод о целесообразности предложенного во второй главе метода.

В приложении приведены исходные коды библиотек «УНИБЛОКС-2015» и её модификации с тестами NIST, а также исходные коды утилит по преобразованию выходных последовательностей в графические изображения.

Диссертация содержит как теоретические, так и практические результаты (акты о внедрении имеются). Результаты без сомнения вызовут интерес у специалистов по стеганографии и математической криптографии и могут быть использованы в учебном процессе при разработке лекционных курсов для студентов, специализирующихся в различных областях информационных технологий и криптографии. Автореферат полностью соответствует содержанию диссертационной работы.

К автореферату и диссертации имеются следующие замечания:

- представляется излишним выносить в автореферат доказательство одной из теорем, содержащихся в диссертации;
- по отношению к статистическим тестам было бы интересно рассматривать не только тесты NIST, «стопка книг», «адаптивный критерий хи-квадрат», но и тесты Dieharder, TestU01 и др;
- не все обозначения последовательно вводятся перед использованием, например, R_{min} (минимальное число раундов шифрования);
- из текста не сразу становится понятно, что библиотека «УНИБЛОКС-2015», используемая для обучения нейронной сети, разработана непосредственно автором;
- имеется ряд стилистических неточностей.

Отмеченные недостатки не умаляют ценности проделанной работы и не влияют на общее положительное впечатление о диссертации.

Все результаты, представленные в диссертации, являются новыми, строго доказанными теоретически или экспериментально, прошедшими широкую апробацию на международных и российских конференциях и семинарах. Они вносят

определённый вклад в развитие фундаментальных основ криптографии и информационной безопасности. Диссертация Перова Артёма Андреевича имеет внутреннее единство и является завершённой научно-квалификационной работой, в которой на основании выполненных автором исследований содержится предложенное решение задачи анализа псевдослучайной последовательности, имеющей существенное значение для криптографии.

Диссертация соответствует требованиям п.9 "Положения о присуждении учёных степеней" постановления Правительства Российской Федерации от 24.09.2013 г. № 842, а её автор Перов Артём Андреевич заслуживает присуждения учёной степени кандидата технических наук. Отзыв на диссертацию и автореферат рассмотрен и одобрен на заседании лаборатории криптографии Международного математического центра в Академгородке (Институт математики СО РАН) 09.03.2021 г., протокол № 17.

Наталья Николаевна Токарева,
кандидат физико-математических наук,
старший научный сотрудник
лаборатории дискретного анализа
ИМ СО РАН
630090, Новосибирск, пр. Коптюга, 4.
Тел.: (8-383) 333-28-92, Факс: (8-383) 333-25-98,
Mail: im@math.nsc.ru, Web: www.math.nsc.ru

«12» марта 2021г.

подпись Н.Н. Токаревой
удостоверяю
Зав. орготделом Н.З. Кондалева
ИМ СО РАН
«12» марта 2021г.