Отзыв на автореферат Алхуссайн Амани

«ВЕРОЯТНОСТНЫЙ АНАЛИЗ СТОЙКОСТИ ЗАЩИТЫ ИНФОРМАЦИИ МЕТОДОМ ЦЕЛОЧИСЛЕННОГО РАСЩЕПЛЕНИЯ СИМВОЛОВ»

Работа посвящена исследование свойств нового метода защиты текстовой информации с помощью целочисленного расщепления символов, что появляется актуальной задачей в области передачи информации.

Целочисленное расщепление является основой для создания новых модели и алгоритма защиты информации. Доказывается, что с ростом глубины расщепления вероятность несанкционированного восстановления символа экспоненциально убывает, что позволяет говорить об асимптотической стойкости расщепления. Разработан и построен новый метод шифрования, позволяющий управлять уровнем защиты информации с помощью генератора показано, что предложенный метод расщепления также существенно усложняет восстановление исходного текста несанкционированным пользователем опирающегося на семантическое содержание этого текста.

Достоверность полученных в диссертации результатов вытекает из использования математических методов модульной арифметики, методов теории вероятностей, методов теории информации и методов симметричной защиты информации с использованием генераторов псевдослучайных чисел. В работе доказан ряд теорем, обосновывающих основные положения диссертации.

По теме диссертации опубликовано 24 работы, результаты неоднократно докладывались на российских и международных конференциях.

Судя по автореферату, работа полностью удовлетворяет требованиям к кандидатским диссертациям по теме «Теоретическая информатика, кибернетика (по физико-математическим наукам)».

Доцент кафедры системного анализа и управления

Университета «Дубна», доцент, к.ф.-м.н. (01.01.09)

Аверкин А.Н.

15.09.2023

Подпись Аверкина А.Н. удостоверяю:
начальник отдела кадров федерального государственного бюджетного образовательного учреждения высшего образования «Университет «Дубна» (государственный университет «Дубна»)
В.А. Виноградова

Аверкин Алексей Николаевич, кандидат физико-математических наук, доцент кафедры системного анализа и управления

Федеральное государственное бюджетное образовательное учреждение высшего образования «Университет «Дубна», 141980 г. Дубна Московской обл., ул. Университетская, 19, Тел.: 8(916)635-4060, Email: averkin2003@inbox.ru

Отзыв

на автореферат диссертационной работы Алхуссайн Амани «Вероятностный анализ стойкости защиты информации методом целочисленного расщепления символов», представленной к защите в диссертационном совете ПДС 0200.006 при федеральном государственном автономном образовательном учреждении высшего образования «Российский университет дружбы народов имени Патриса Лумумбы» на соискание ученой степени кандидата физико-математических наук по специальности 1.2.3. Теоретическая информатика, кибернетика

По мере того, как информационные технологии охватывают все новые стороны жизни, возрастает важность защиты информации. Проблемы защиты информации привлекают внимание множества исследователей. Особенно интересны попытки создания принципиально новых и оригинальных методов решения этих проблем. В диссертационном исследовании Алхуссайн А. предложен оригинальный подход, основанный на операции, названной автором целочисленным расщеплением.

Работа содержит математическое исследование этой операции. В частности, доказано свойство асимптотической стойкости расщепления символов. Основываясь на реферате, можно заключить, что тематика диссертации соответствует специальности 1.2.3. Теоретическая информатика, кибернетика.

Достоверность полученных результатов подтверждается математическими доказвтельствами, проведенными с использованием теории вероятностей, методов теории информации. Работа также содержит описание подтверждающих результату экспериментов на компьютере.

Основные результаты, изложенные в диссертации, заключаются в следующем:

1. Предложены определения целочисленного расщепления числа и обобщённого целочисленного расщепления.
2. Изучены и доказаны утверждения, позволяющие использовать расщепление в области защиты информации.
3. Предложено новое математическое понятие символьного расщепления.
4. Исследовано поведение вероятности несанкционированного восстановления исходного теста по результату расщепления и обобщённого расщепления.

Все результаты логически обоснованы на современном уровне математической строгости.

Научная ценность результатов диссертации состоит в дальнейшем развитии теории защиты информации, заключающемся, в частности, в обобщении полученных результатов в соответствии с требованиями асимптотической стойкости..

Практическая ценность заключается в том, что разработанный алгоритм на основе предложенной процедуры расщепления может быть использован для встраивания новых защитных механизмов в комплексные средства обеспечения компьютерной безопасности и в реальных системах информационной безопасности.

Результаты диссертации соответствуют требованиям паспорта специальности 1.2.3. Теоретическая информатика, кибернетика. Они опубликованы в 25 работах, из которых 7

изданы в журналах, рекомендованных ВАК, 6 - в периодических научных изданиях, индексируемых в системе Scopus, 1 - патент на изобретение. Результаты представлялись на множестве международных и всероссийских конференций, а также обсуждались на научных семинарах. В публикациях отражены все основные результаты диссертации.

Положения, выносимые на защиту, соответствуют теме работы и решают задачи, поставленные в диссертации.

На основании автореферата и опубликованных работ Алхуссайн А. считаю, что диссертация соответствует всем требованиям, предъявляемым к диссертациям на соискание степени кандидата физико-математических наук, а её автор - Алхуссайн А.- заслуживает присуждения ей ученой степени кандидата физико-математических наук по специальности 1.2.3. Теоретическая информатика, кибернетика.

Старший научный сотрудник ИППИ РАН
д.ф.-м.-н (05.13.01),
"11" сентября 2023г.

Жожикашвили А. В.

Подпись Жожикашвили А.В.
УДОСТОВЕРЯЮ
Зав. канцелярией

Жожикашвили Александр Владимирович, старший научный сотрудник, д.ф.-м.н., с.н.с.
Федеральное государственное бюджетное учреждение науки Институт проблем передачи информации им. А.А. Харкевича Российской академии наук (ИППИ РАН)
127051, г. Москва, Большой Каретный переулок, д.19 стр. 1.
Телефон: +7 (495) 650-42-25, Email: director@iitp.ru

В диссертационный совет ПДС 0200.006 на базе ФГАОУ ВО «Российский университет дружбы народов имени Патриса Лумумбы»

ОТЗЫВ

на автореферат диссертации Алхуссайн Амани на тему «Вероятностный анализ стойкости защиты информации методом целочисленного расщепления символов», представленной на соискание учёной степени кандидата физико-математических наук по специальности 1.2.3. Теоретическая информатика, кибернетика

Широкомасштабное внедрение в различные сферы современного общества разнообразного спектра цифровых технологий требует совершенствования имеющихся и разработки новых подходов для обеспечения информационной безопасности. Одним из наиболее эффективных способов решения указанной проблемы является создание и использование различных криптографических алгоритмов. В диссертационной работе Алхуссайн А. предложен новый метод защиты информации, основанный на применении целочисленного расщепления символов.

Анализ автореферата позволяет сделать вывод о том, что диссертация Алхуссайн А. изложена с соблюдением четкости и последовательности всех ее составных частей. Поставленные во введении задачи исследования полностью решены. Диссертационная работа, несомненно, обладает научной новизной, теоретической и практической значимостью и тематика исследования соответствует специальности 1.2.3. Теоретическая информатика, кибернетика.

К важным пунктам научной новизны следует отнести следующие: а) предложены основные определения и понятия целочисленного расщепления; б) доказаны утверждения, позволяющие использовать метод целочисленного расщепления для защиты информации; в) предложено определение символьного расщепления для применения процедуры целочисленного расщепления при защите текстовой информации; г) представлены математические модели для метода защиты на основе символьного расщепления; д) проведен вероятностный анализ несанкционированного восстановления исходного теста по результату расщепления и обобщённого расщепления и получен результат асимптотической стойкости расщепления символов; ж) проведено сравнение метода расщепления с традиционными методами защиты информации, которые обладают свойствами или математическими операторами, соответствующими предлагаемому методу расщепления.

В автореферате представлен достаточный объём иллюстрированного материала, который наглядно демонстрирует содержание и результаты диссертации.

Наряду с положительными аспектами диссертационного исследования, отраженными в автореферате, имеют место и отдельные вопросы, требующие пояснения.

Для таблицы 1 (стр. 17 автореферата) «Сравнение расщепления с некоторыми синхро-потоковыми (синхронизационными) методами защиты)», желательно также представить различные дополнительные количественные оценки алгоритмов, например, производительность и требования к памяти. Указанные обстоятельства для сравнения рассмотренных различных методов защиты (Вернама, гаммирования, символьного расщепления) предполагают эффективное использование человеко-машинных многокритериальных методов для выбора наиболее предпочтительного подхода при решении конкретной практической задачи, чему в работе уделено мало внимания.

Перечисленные замечания не снижают общей положительной оценки результатов диссертационного исследования. Автореферат диссертации на тему «Вероятностный анализ стойкости защиты информации методом целочисленного расщепления символов» свидетельствует о завершенном самостоятельно выполненном исследовании, результаты которого имеют научную и практическую значимость, соответствующую требованиям паспорта специальности 1.2.3. Теоретическая информатика, кибернетика. По теме диссертации опубликовано 25 работ, из которых 8 в изданиях, рекомендованных ВАК, 6 - в периодических научных изданиях, индексируемых в системе Scopus, 1 - патент на изобретение. В публикациях отражены все основные результаты диссертации.

С учетом вышеизложенного, Алхуссайн А. заслуживает присуждения учёной степени кандидата физико-математических наук по специальности 1.2.3. Теоретическая информатика, кибернетика.

Кандидат технических наук
(шифр специальности 05.13.10),
доцент кафедры «Прикладной математики
и искусственного интеллекта» НИУ МЭИ _____ Ройзензон Г.В.

19 октября 2023

Ройзензон Григорий Владимирович
кандидат технических наук,
доцент кафедры «Прикладной математики и искусственного интеллекта»
ФГБОУ ВО Национального исследовательского университета
«Московский энергетический институт»

111250, Россия, г. Москва, ул. Красноказарменная, д. 14, стр. 1
тел.: 8(495)362-79-62
e-mail: RoyzenzonGV@mpei.ru

Подпись удостоверяю

Заместитель начальника
по работе с персоналом
Л.И. Полевая

142

ОТЗЫВ

на автореферат диссертационной работы Алхуссайн Амани «Вероятностный анализ стойкости защиты информации методом целочисленного расщепления символов», представленной к защите в диссертационном совете ПДС 0200.006 при Федеральном государственном автономном образовательном учреждении высшего образования «Российский университет дружбы народов имени Патриса Лумумбы» на соискание ученой степени кандидата физико-математических наук по специальности 1.2.3. Теоретическая информатика, кибернетика

Исследование проблем разработки, совершенствования и применения методов защиты информации в процессе ее хранения и передачи привлекает внимание множества исследователей, так как разработка новых и совершенствование имеющихся методов защиты имеет большое значение для развития инфокоммуникационных и информационных сред и систем. В диссертационном исследовании Алхуссайн А. предложена новая математическая процедура – целочисленное расщепление (представление числа в виде цепочки из целых чисел), доказаны утверждения, связанные с этой процедурой. На основе доказанных утверждений разработан способ расщепления символов.

Изучена возможность несанкционированного восстановления результата расщепления и доказано свойство асимптотической стойкости расщепления символов. Проведенное исследование математической модели защиты информации методом расщепления, анализ вероятностных характеристик этого метода и асимптотической стойкости расщепления, показали, что решаемая задача является актуальной.

Достоверность аналитических результатов подтверждается строгими математическими выкладками, выполненными с использованием теории вероятностей, методов теории информации и вычислительных экспериментов.

Диссертация содержит новые научные результаты, основные положения которых заключаются в следующем:

1. Предложены определения целочисленного расщепления символа и обобщенного целочисленного расщепления.

2. Изучены и доказаны утверждения, позволяющие использовать расщепление в области защиты информации.

3. Предложено новое математическое понятие символьного расщепления.

4. Исследовано поведение вероятности несанкционированного восстановления исходного теста по результату расщепления и обобщенного расщепления.

Автор корректно использует известные научные методы обоснования полученных результатов, которые подтверждаются строгим использованием теории вероятностей и

теории защиты информации. Все результаты логически обоснованы. Научная ценность результатов диссертации заключается в развитии теории защиты информации и данных, в обобщении полученных результатов в соответствии с требованиями асимптотической стойкости.

Практическая ценность заключается в том, что разработанный алгоритм на основе предложенной процедуры расщепления может быть встроен в комплексные средства обеспечения компьютерной безопасности реальных систем.

Тематика диссертации соответствуют специальности 1.2.3. Теоретическая информатика, кибернетика. Результаты опубликованы в 25 работах, из которых 7 изданы в журналах, рекомендованных ВАК, 6 – в периодических научных изданиях, индексируемых в системе Scopus, 1 – патент на изобретение. Результаты представлялись на множестве международных и всероссийских конференций, а также обсуждались на научных семинарах. В публикациях отражены все основные результаты диссертации.

В автореферате достаточно полно отражена актуальность темы диссертации, цель работы, научная новизна, теоретическая и практическая значимость. Положения, выносимые на защиту, соответствуют теме работы и решают задачи, поставленные в диссертации.

На основании автореферата и опубликованных работ Алхуссайн А. считаю, что диссертационная работа соответствует требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата физико-математических наук, а ее автор – Алхуссайн А. – заслуживает присуждения ей ученой степени кандидата физико-математических наук по специальности 1.2.3. Теоретическая информатика, кибернетика.

Ведущий научный сотрудник
ИПС им. А.К. Айламазяна РАН,
к.т.н. (шифр специальности 2.3.5) Фраленко Виталий Петрович

8.09.2023

Подлинность Фраленко В.П. подтверждаю:
начальник отдела кадров ИПС им. А.К. Айламазяна РАН Е.Г. Игнатьева

Фраленко Виталий Петрович, к.т.н., н.с. ИПС им.А.К.Айламазяна РАН
Федеральное государственное бюджетное учреждение науки Институт программных систем им. А.К.Айламазяна Российской академии наук
Адрес: 152021, Ярославская область, Переславский район, с. Веськово, ул. Петра Первого, д.4 «а». Телефон: (4852) 695-228, E-mail: psi@botik.ru

144