ОТЗЫВ

официального рецензента на диссертационную работу

Сақан Қайрат Сақанұлы на тему «Разработка алгоритмов хеширования на основе итеративных блочных шифров и исследование их криптостойкости», предоставленную на соискание степени доктора философии (PhD) по образовательной программе «8D06301 – Системы информационной безопасности».

№п/п	Критерии	Соответствие критериям (необходимо отметить один из вариантов ответа)	Обоснование позиции официального рецензента
1.	Тема диссертации (на дату ее утверждения) соответствует направлениям развития науки и/или государственным программам	1.1 Соответствие приоритетным направлениям развития науки или государственным программам:	Диссертационная работа на тему «Разработка алгоритмов хеширования на основе итеративных блочных шифров и исследование их криптостойкости» соответствует приоритетным направлениям развития науки «Информационные, коммуникационные и космические технологии» и «Национальная безопасность и оборона», а также «Информационной доктрины» Республики Казахстан, утвержденной Указом Президента Республики Казахстан от 20 марта 2023 года № 145.
		1) **Диссертация выполнена в рамках проекта или целевой программы, финансируемого(ой) из государственного бюджета (указать название и номер проекта или программы)** 2) Диссертация выполнена в рамках другой государственной программы (указать название программы) 3) Диссертация соответствует приоритетному направлению развития науки, утвержденному Высшей научно-технической комиссией при Правительстве Республики Казахстан (указать направление)	Данная работа выполнена в рамках научно-исследовательских работ проекта программно-целевого финансирования МОН РК «Разработка и исследование алгоритмов хеширования произвольной длины для цифровых подписей и оценка их стойкости», реализованного в период 2021-2022 гг. (ГРН – OR11465439, научный руководитель – д.т.н., доцент С.Е. Нысанбаева).
2.	Важность для науки	**Работа вносит**/не вносит **существенный вклад в науку, а ее важность хорошо раскрыта**/не раскрыта	Результаты работы вносят существенный вклад в области обеспечения информационной безопасности, в том числе защиты информации. Разработанный алгоритм может быть применен в сфере обеспечения целостности, достоверности, подлинности и неотказуемости от авторства информации. Кроме того, он может быть использован при разработке алгоритмов подписей в постквантовой криптографии и технологии блокчейн.

3.	Принцип самостоятельности	Уровень самостоятельности: **1) <u>Высокий;</u>** 2) Средний; 3) Низкий; 4) Самостоятельности нет	Работа обладает высоким уровнем творческой самостоятельности, при выполнении которой наблюдается конкретность, системность, организованность и творческий подход к решению научных проблем. Диссертация написана единолично автором, содержит новые научные результаты в области исследования. Стоит отметить, что работа является результатом практической деятельности непосредственного участия диссертанта в научном проекте, указанном в диссертации, а также на это указывают публикации в высокорейтинговых журналах, доклады на международных конференциях, научных семинарах и полученные авторские права.
4.	Принцип внутреннего единства	4.1 Обоснование актуальности диссертации: **1) <u>Обоснована;</u>** 2) Частично обоснована; 3) Не обоснована.	Бурное развитие цифровых технологий открыло огромное количество новых каналов коммуникаций. В итоге, на информационном пространстве появились новые направления, которые коренным образом изменили процесс обмена информацией и соответственно возникла необходимость формирования безопасного информационного общества и защищенного обмена электронных данных. Поэтому, актуальность диссертации основывается именно на формировании и использовании крипторафических систем и средств, обеспечивающих конфиденциальность, целостность и установление и неотрицание авторства электронных данных.
		4.2 Содержание диссертации отражает тему диссертации: **1) <u>Отражает;</u>** 2) Частично отражает; 3) Не отражает	Содержание диссертации отражает ее тему. В ней соискатель предлагает новый алгоритм хеширования данных HBC-256, где в качестве сжимающей функцией рассматривается симметричный алгоритм блочного шифрования CF. В работе подробно описывается схема алгоритма, а основные его параметры выбираются на основе научных подходов. Последующие разделы работы посвящаются исследованию безопасности разработанного алгоритма и его эффективности в практическом применении.
		4.3. Цель и задачи соответствуют теме диссертации: **1) <u>соответствуют;</u>** 2) частично соответствуют; 3) не соответствуют	В работе поставлена конкретная цель, вытекающая из проблематики в данной области исследования, а задачи, которые необходимо выполнить для ее достижения, определены и сформулированы из принципа последовательности и полноты действий.
		4.4 Все разделы и положения диссертации логически взаимосвязаны: **1) <u>полностью взаимосвязаны;</u>** 2) взаимосвязь частичная; 3) взаимосвязь отсутствует	Разделы диссертационной работы логически структурированные и четко взаимосвязаны между собой. Задачи, определенные для достижения поставленной цели, выполняются последовательно и характеризируются своей полнотой. Диссертационная работа считается завершенным научным исследованием.
		4.5 Предложенные автором новые	Достоверность каждого научного результата, выводы и решения подтверждены в

		решения (принципы, методы) аргументированы и оценены по сравнению с известными решениями: **1) <u>критический анализ есть;</u>** 2) анализ частичный; 3) анализ представляет собой не собственные мнения, а цитаты других авторов	виде научных статьей, авторскими свидетельствами, заключениями независимых зарубежных экспертов (Летняя школа-семинар по криптографии, г. Новосибирск, Россия) и протоколами научных семинаров, ведущих ВУЗ и профильных научных организаций зарубежья (НАУ, г.Киев, Украина; БГУ, г.Минск, Беларусь; Университет Халифа, г. Абу-Даби, ОАЭ).
5.	Принцип научной новизны	5.1 Научные результаты и положения являются новыми? **<u>1) полностью новые;</u>** 2) частично новые (новыми являются 25-75%); 3) не новые (новыми являются менее 25%)	Научные результаты диссертации являются новыми и дополняют известные. В работе предложены следующие новые научные положения: - построена новая схема совместимого применения четырех 4-битных S-блоков в зависимости от местоположения элемента в квадратной матрице; - с целью минимизации количества раундов предложена новая схема применения нелинейного преобразования в функции сжатия; - в зависимости объема хешируемых данных предложен выбор параметра *k*, адаптированного для параллельного вычисления.
		5.2 Выводы диссертации являются новыми? **<u>1) полностью новые;</u>** 2) частично новые (новыми являются 25-75%); 3) не новые (новыми являются менее 25%)	Выводы диссертации являются новыми, они сопровождаются теоретическими и практическими обоснованиями. Все три новых научных подхода, перечисленных в пункте 5, показывают свою актуальность и уникальность, а также их преимущества подтверждаются результатами сравнительного анализа.
		5.3 Технические, технологические, экономические или управленческие решения являются новыми и обоснованными: **<u>1) полностью новые;</u>** 2) частично новые (новыми являются 25-75%); 3) не новые (новыми являются менее 25%)	Технические, технологические, экономические или управленческие решения являются новыми для решения комплекса задач, связанных с формированием открытого информационного пространства, и являются одними из ключевых направлений обеспечения информационной безопасности страны.

6.	Обоснованность основных выводов	Все основные выводы основаны/не основаны на весомых с научной точки зрения доказательствах либо достаточно хорошо обоснованы (для qualitative research и направлений подготовки по искусству и гуманитарным наукам)	Все полученные научные результаты в диссертационной работе основаны на научных доказательствах. Каждый результат получен путем обоснования, выбора параметров, сравнения с имеющимися экспериментальными данными и с результатами других исследований. Сравнения показывают достоверность, согласованность и обоснованность выводов, указанных в диссертации. Имеются протоколы зарубежных научных семинаров и статьи в рейтинговых журналах и на международных конференциях, где докладывались результаты.
7.	Основные положения, выносимые на защиту	Необходимо ответить на следующие вопросы по каждому положению в отдельности: 7.1 Доказано ли положение? 1) доказано; 2) скорее доказано; 3) скорее не доказано; 4) не доказано 7.2 Является ли тривиальным? 1) да; 2) нет 7.3 Является ли новым? 1) да; 2) нет 7.4 Уровень для применения: 1) узкий; 2) средний; 3) широкий 7.5 Доказано ли в статье? 1) да; 2) нет	**Положение 1.** Разработан новый алгоритм хеширования на основе блочного шифра, адаптированный для параллельных вычислений и программно-аппаратной реализации; 7.1 доказано; 7.2 нет; 7.3 да; 7.4 средний; 7.5 да. **Положение 2.** Предложена новая схема сопряженного применения четырех 4-битных S-блоков относительно индексов элемента матрицы, применение которой позволит повысить безопасность алгоритма и более эффективно использовать память микросхемы в аппаратной реализации; 7.1 доказано; 7.2 нет; 7.3 да; 7.4 широкий; 7.5 да. **Положение 3.** Предложена новая схема применения нелинейного преобразования в функции сжатия, которая позволяет уменьшить количество раундов; 7.1 доказано; 7.2 нет; 7.3 да; 7.4 широкий; 7.5 да. **Положение 4.** Предложена возможность выбора k частей блока хеширования относительно размера исходного хешируемого сообщения, что в свою очередь, повышает производительность вычислений (k=3, …, 8). 7.1 доказано; 7.2 нет; 7.3 да; 7.4 широкий; 7.5 да.
8.	Принцип достоверности Достоверность источников и предоставляемой	8.1 Выбор методологии - обоснован или методология достаточно подробно описана **1) да;** 2) нет	Выбор методологии исследования обоснован. В работе в достаточном объеме для проведения исследования описаны все основные теоретические и эмпирические методы.

	информации	8.2 Результаты диссертационной работы получены с использованием современных методов научных исследований и методик обработки и интерпретации данных с применением компьютерных технологий: **1) да;** 2) нет	Результаты диссертационной работы были получены с использованием основных методов научных исследований и методик обработки. Исследовательская работа проводилась в таких областях как теория булевых функций, линейная алгебра, теория вероятности и математическая статистика, методы криптографического анализа и типы атак для исследования хеш-функций, лавинный эффект. Вместе с тем, для интерпретации и обработки данных широко применялись современные компьютерные технологий и языки программирования, а также ПЛИС – для программно-аппаратной реализации предложенного алгоритма.
		8.3 Теоретические выводы, модели, выявленные взаимосвязи и закономерности доказаны и подтверждены экспериментальными исследованиями (для направлений подготовки по педагогическим наукам результаты доказаны на основе педагогического эксперимента): **1) да;** 2) нет	Теоретические выводы и выявленные закономерности были доказаны и подтверждены экспериментальными исследованиями. Результаты экспериментальных исследований получены и оценены компьютерными программами лаборатории информационной безопасности Института информационных и вычислительных технологий КН МНВО РК.
		8.4 **Важные утверждения подтверждены**/частично подтверждены/не подтверждены **ссылками на актуальную и достоверную научную литературу**	Во всех разделах важные утверждения подтверждаются ссылками на актуальную и достоверную научную литературу. При оформлении диссертации соблюдены все нормы научной этики и академической чесности.
		8.5 **Использованные источники литературы достаточны**/не достаточны **для литературного обзора**	При написании диссертационной работы использовано достаточное количество источников литературы, большинство из них не более 5–10-летней давности, что еще раз свидетельствует об актуальности темы исследования.
9	Принцип практической ценности	9.1 Диссертация имеет теоретическое значение: **1) да;** 2) нет	Диссертация имеет теоретическое значение. Результаты работы будут способствовать развитию криптологии и созданию новых подходов защиты данных, расширению теории создания еще более эффективные хеш-функций, отвечающих всем требованиям нынешнего технологического прогресса.
		9.2 Диссертация имеет практическое значение и существует высокая вероятность применения полученных результатов на практике: **1) да;** 2) нет	Полученные результаты исследовательской работы имеют высокую практическую ценность и могут быть использованы для обеспечения защиты, верификации (авторизация и аутентификация) данных в инфокоммуникационных системах и сетях.

		9.3 Предложения для практики являются новыми? 1) полностью новые; **2) частично новые (новыми являются 70%);** 3) не новые (новыми являются менее 25%)	Разработан новый алгоритм хеширования данных на основе блочного шифра, который может быть использован для обеспечения информационной безопасности страны и ее граждан, преотвращения и своевременного реагирования на информационные вызовы и риски.
10.	Качество написания и оформления	Качество академического письма: **1) высокое;** 2) среднее; 3) ниже среднего; 4) низкое.	Диссертационная работа оформлена и подготовлена в соответствии с предъявляемыми требованиями. Считается, что умение выражать и обосновывать умозаключение соискателя посредством краткого, достаточно убедительного научного текста на высоком уровне. В работе соблюдается научный стиль (еще точнее академический подстиль), учитывается общепринятая терминология рассматриваемой предметной области.

В отзывах официальные рецензенты указывают одно из следующих решений:

1) **присудить степень доктора философии (PhD) или доктора по профилю;**
2) направить диссертацию на доработку (кроме случаев защиты диссертации в форме серии статей);
3) отказать в присуждении степени доктора философии (PhD) или доктора по профилю.

Официальный рецензент:
PhD, Директор института информационных технологий
НАО Алматинского университета энергетики и связи имени Г. Даукеева **А. А. Абдукаримова**

Персоналды басқару жөніндегі бөлім
Отдел по управлению персоналом

Қолтаңбаны растаймын
Подпись заверяю
қызметі аты-жөні
«21» 07 2023 ж.