Федеральное агентство связи
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)

ОТЗЫВ

на выпускную квалификационную работу магистранта гр. МГ-171 Чусовитина А.Р.
по теме «Реализация и исследование поточного шифра на основе шифра Шеннона»

В 2016 году были теоретически описаны и строго доказаны свойства двух шифров Шеннона, однако в исходном виде эти шифры предполагались для шифрования исключительно текстов на английском языке. Поэтому адаптация одного из этих шифров к реальным данным, передаваемым по сети, разработка на его основе поточного шифра и исследование его свойств являются важными и актуальными задачами для современной криптографии. Важно отметить, что одной из особенностей шифра Шеннона является высокое быстродействие его реализации.

Перед Чусовитиным А.Р. стояла задача разработки на основе шифра Шеннона поточного шифра, работающего с реальными данными, передаваемыми по сети. Кроме того, необходимо было проверить получаемые в результате шифрования последовательности при помощи общепризнанных статистических тестов NIST и «стопка книг», а так же оценить быстродействие разработанной реализации и сравнить её с действующим стандартом поточного шифрования RC4.

Автором работы были выполнены все поставленные перед ним задачи, результаты исследования показали высокую надёжность шифра и подтвердили теоретические обоснования. Кроме того, было показано, что предложенный шифр работает на порядок быстрее действующего стандарта. Работа выполнялась в рамках гранта № ГР АААА-Б19-219020490005-8, а результаты были представлены на международных и всероссийских конференциях.

Существенных замечаний к оформлению нет, все этапы работы выполнены в срок и на высоком уровне. По результатам проверки на сайте antiplagiat оригинальность работы составляет 79,42%, что полностью соответствует требованиям, предъявляемым к ВКР. Поэтому работу магистранта Чусовитина А.Р. оцениваю на **«отлично»** и рекомендую для публикации в рецензируемом научном издании. Считаю, что Чусовитин А.Р. заслуживает присвоения квалификации «магистр» по направлению 09.04.01 - «Информатика и вычислительная техника» и рекомендую его для поступления в аспирантуру.

Компетенции		Уровень сформированности компетенций		
		высокий	Средний	низкий
Общекультурные	ОК-1 Способность совершенствовать и развивать свой интеллектуальный и общекультурный уровень	+		
	ОК-3 Способность к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности	+		
	ОК-4 Способность заниматься научными исследованиями	+		
	ОК-5 Использование на практике умений и навыков в организации исследовательских и проектных работ, в управлении коллективом	+		
	ОК-6 Способность проявлять инициативу, в том числе в ситуациях риска, брать на себя всю полноту ответственности	+		
	ОК-9 Умение оформлять отчеты о проведенной научно-исследовательской работе и подготавливать публикации по результатам исследования	+		
Общепрофессиональные	ОПК-3 Способность анализировать и оценивать уровни своих компетенций в сочетании со способностью и готовностью к саморегулированию дальнейшего образования и профессиональной мобильности	+		
	ОПК-5 Владение методами и средствами получения, хранения, переработки и трансляции информации посредством современныхкомпьютерных технологий, в том числе в глобальных компьютерных сетях	+		
Профессиональные	ПК-2 знанием методов научных исследований и владение навыками их проведения	+		
	ПК-7 применением перспективных методов исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники и информационных технологий	+		
	ПК-17 способностью к организации промышленного тестирования создаваемого программного обеспечения	+		

Работа имеет практическую ценность	+	Тема предложена предприятием	
Работа имеет теоретическую значимость	+	Тема предложена студентом	
Работа внедрена		Тема является фундаментальной	+
Рекомендую работу к опубликованию	+	Рекомендую студента в аспирантуру	+
Работа выполнена в рамках гранта НИОКР	+	Имеются публикации по теме работы	+

Доц. каф. ПМиК, к.т.н._____Ракитский Антон Андреевич

Должность руководителя подпись ФИО руководителя