УТВЕРЖДАЮ

Первый проректор — проректор по научной работе МГТУ им. Н. Э. Баумана,

д. т. н., профессор

_____ Зимин В. Н.

«11» декабря 2017 г.

# ЗАКЛЮЧЕНИЕ

Федерального государственного бюджетного образовательного учреждения высшего профессионального образования

«Московский государственный технический университет им. Н. Э. Баумана»

Диссертация «Методы синтеза обратимых схем из функциональных элементов NOT, CNOT и 2-CNOT» выполнена на кафедре «Информационная безопасность» Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Московский государственный технический университет им. Н. Э. Баумана».

В период подготовки диссертации соискатель Закаблуков Дмитрий Владимирович **работал** в Обществе с ограниченной ответственностью «Дотпром» в должности программиста.

В 2012 г. **окончил** Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Московский государственный технический университет им. Н. Э. Баумана» по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем».

**Удостоверение о сдаче кандидатских экзаменов** выдано в 2015 г. Федеральным государственным бюджетным образовательным учреждением высшего профессионального образования «Московский государственный технический университет им. Н. Э. Баумана».

**Научный руководитель** — Жуков Алексей Евгеньевич, кандидат физико-математических наук, доцент кафедры ИУ-8 «Информационная безопасность» Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Московский государственный технический университет им. Н. Э. Баумана».

По итогам обсуждения принято следующее заключение:

Диссертационная работа Закаблукова Д. В. посвящена актуальной проблеме синтеза и сложности управляющих систем в классе схем из обратимых функциональных элементов.

Наиболее существенные **научные результаты**, полученные лично автором, заключаются в следующем:

1. Получены верхние и нижние асимптотические оценки сложности, глубины и квантового веса обратимых схем, состоящих из функциональных элементов NOT, CNOT и 2-CNOT. Доказана существенная зависимость данных оценок от количества дополнительных входов в схеме.

2. Предложены и систематизированы различные способы снижения сложности обратимых схем, состоящих из обобщённых элементов Тоффоли.

3. Разработан новый быстрый алгоритм синтеза обратимой схемы, реализующей заданную чётную подстановку с малым числом подвижных точек.

4. Разработан быстрый, асимптотически оптимальный метод синтеза обратимых схем без дополнительных входов, состоящих из функциональных элементов NOT, CNOT и 2-CNOT.

5. Предложены различные способы синтеза обратимых схем, реализующих алгоритм дискретного логарифмирования в конечном поле характеристики 2.

**Достоверность** результатов работы обеспечивается строгостью применения математических моделей, корректностью математических доказательств, непротиворечивостью полученных результатов с известными, подтверждается результатами расчётов, компьютерным моделированием и апробацией предложенных в диссертации методов.

**Научная новизна** *первого* результата заключается в том, что определён порядок роста сложности обратимых схем, состоящих из функциональных элементов NOT, CNOT и 2-CNOT; доказаны верхние и нижние асимптотические оценки глубины и квантового веса таких схем. Доказана существенная зависимость полученных оценок от количества дополнительных входов в схеме, а именно: увеличение количества дополнительных входов в обратимой схеме почти всегда позволяет снизить ее сложность, глубину и квантовый вес.

Научная новизна *второго* результата состоит в том, что систематизированы существующие и предложены новые способы снижения сложности обратимых схем, состоящих из обобщённых элементов Тоффоли. Показано, что многие эквивалентные замены в обратимых схемах можно описать при помощи операций на множествах. Также получен новый критерий коммутируемости двух обобщённых элементов Тоффоли.

Научная новизна *третьего* результата заключается в том, что для случая чётной подстановки с малым числом подвижных точек предложен быстрый алгоритм синтеза реализующей эту подстановку обратимой схемы. Доказано,

что в сравнении с известными алгоритмами синтеза время работы данного алгоритма и требуемый им объём памяти асимптотически меньше.

Научная новизна *четвертого* результата состоит в том, что разработан единственный известный на сегодняшний день асимптотически оптимальный метод синтеза обратимых схем без дополнительных входов, состоящих из функциональных элементов NOT, CNOT и 2-CNOT.

Научная новизна *пятого* результата заключается в том, что доказана верхняя асимптотическая оценка сложности обратимых схем, состоящих из функциональных элементов NOT, CNOT и 2-CNOT и реализующих алгоритм дискретного логарифмирования в конечном поле характеристики 2. Данная оценка асимптотически меньше верхней оценки сложности обратимых схем в общем случае.

**Практическая значимость**. Полученные в диссертационном исследовании результаты можно использовать для анализа сложности различных отображений, а также для проектирования современных энергоэффективных вычислительных устройств, предназначенных для работы в условиях ограниченной памяти и ресурсов. Разработанные методы синтеза обратимых схем могут стать основой для дальнейших исследований в данной области и войти в состав учебных материалов и лекций по синтезу и сложности управляющих систем на факультетах соответствующего профиля высших учебных заведений.

**Ценность** научных работ соискателя состоит в разработке новых, асимптотически оптимальных методов синтеза обратимых схем, состоящих из функциональных элементов NOT, CNOT и 2-CNOT, для широкого диапазона значений количества дополнительных входов в схеме.

Тема и содержание диссертационной работы **соответствуют** специальности 01.01.09 – «Дискретная математика и математическая кибернетика».

Результаты диссертации **полностью изложены** в 12 печатных трудах, из которых 5 статей опубликовано в рецензируемых научных изданиях из перечня ВАК (выделены полужирным шрифтом).

1. Жуков А. Е., Закаблуков Д. В., Засорина Ю. В., Чикин А. А. «*Вычислительно асимметричные преобразования и схемы из обратимых элементов*» // Вопросы кибербезопасности, 2015, №2(10). С. 49-55.
2. Закаблуков Д. В. «*Асимптотическая сложность и глубина обратимых схем из элементов NOT, CNOT и 2-CNOT*» // Дискретные модели в теории управляющих систем: IX Международная конференция, Москва и Подмосковье, 20-22 мая 2015 г.: Труды / Отв. ред. В. Б. Алексеев, Д. С. Романов, Б. Р. Данилов. – М.: МАКС Пресс, 2015. – С. 82-84.
3. **Закаблуков Д. В. «*Быстрый алгоритм синтеза обратимых схем на основе теории групп подстановок*» // Прикладная дискретная математика, 2014, №2. С. 101-109.**
4. **Закаблуков Д. В. «*Вентильная сложность обратимых схем как мера сложности четных подстановок*» // Вестник МГТУ им. Н. Э. Баумана, серия «Приборостроение», 2015, №1(100). С. 67-82.**
5. Закаблуков Д. В., Жуков А. Е. «*Исследование схем из обратимых логических элементов*» // Информатика и системы управления в XXI веке: Сборник трудов №9 молодых ученых, аспирантов и студентов. – М.: МГТУ им. Н. Э. Баумана, 2012. – С. 148-157.
6. **Закаблуков Д. В. «*О сложности обратимых схем, состоящих из функциональных элементов NOT, CNOT и 2-CNOT*» // Дискретная математика, 2016. Т. 28, №2. С. 12-26.**
7. **Закаблуков Д. В. «*Оценка глубины обратимых схем из функциональных элементов NOT, CNOT и 2-CNOT*» // Вестник Московского университета, серия «Математика. Механика», 2016, №3. С. 3-12.**

8. Закаблуков Д. В. «*Синтез схем из обратимых элементов*» // Тезисы доклада XX Всероссийской научно-практической конференции «Проблемы информационной безопасности в системе высшей школы», МИФИ, 2013. – С. 100-101.

9. Закаблуков Д. В. «*Синтез обратимых схем на основе теории групп подстановок*» // «Безопасные информационные технологии». Сборник трудов Пятой Всероссийской научно-технической конференции / под ред. Матвеева В. А., – М.: НИИ Радиоэлектроники и лазерной техники МГТУ им. Н. Э. Баумана, 2015. – С. 84-85.

10. **Закаблуков Д. В. «*Снижение вентильной сложности обратимых схем без использования таблиц эквивалентных замен композиций вентилей*» // Наука и образование. МГТУ им. Н. Э. Баумана. Электрон. журн. 2014. №3. DOI: 10.7463/0314.0699195.**

11. Zakablukov D. V. «*Application of Permutation Group Theory in Reversible Logic Synthesis*» // In book: Devitt S., Lanese I. (eds) Reversible Computation – RC 2016. (Series: Lecture Notes in Computer Science). Springer Cham, 2016. Vol. 9720. Pp. 223-238. DOI: 10.1007/978-3-319-40578-0_17.

12. Zakablukov D. V. «*On Asymptotic Gate Complexity and Depth of Reversible Circuits Without Additional Memory*» // Journal of Computer and System Sciences, 2017. Vol. 84. Pp. 132-143. DOI: 10.1016/j.jcss.2016.09.010.

Диссертация «Методы синтеза обратимых схем из функциональных элементов NOT, CNOT и 2-CNOT» Закаблукова Дмитрия Владимировича удовлетворяет всем требованиям, предъявляемым к диссертациям на соискание учёной степени кандидата физико-математических наук по специальности 01.01.09 – «Дискретная математика и математическая кибернетика» и **рекомендуется** к защите на соискание учёной степени кандидата физико-математических наук по указанной специальности.

Заключение принято на заседании кафедры «Информационная безопасность» МГТУ им. Н. Э. Баумана. Присутствовало на заседании 27 чел. Результаты голосования: «за» — 27 чел., против и воздержавшихся нет, протокол №03.02.01.08-10/4 от 14 ноября 2017 г.

Заведующий кафедрой «Информационная безопасность»

д. ф.-м. н., профессор _____ / Басараб М. А. /