**ИТОГОВЫЙ ОТЧЁТ**

**по проекту РФФИ 16-01-00196**

**Разработка теоретических основ проектирования алгоритмического и аппаратного обеспечения на основе схем обратимых логических элементов**

Основной код классификатора

01-217 Математические модели и методы защиты, преобразования и передачи информации

Дополнительные коды классификатора

01-114 Дискретная математика и математическая кибернетика

01-224 Математическое моделирование технических систем

Продолжительность 2016-2018, три года

Ключевые слова: обратимые вычисления, синтез схем, обратимые логические элементы

Номер ЦИТиС АААА-А16-116021510097-7

**Аннотация, публикуемая на сайте РФФИ**

Проект предполагает создание фундамента для глубоких исследований в области обратимости: теории и методов синтеза обратимых схем, в т. ч. сбоеустойчивых, обратимых алгоритмов решения прикладных задач, применения обратимых схем в современной криптографии и т. д.

За время выполнения проекта впервые систематически изучен вопрос синтеза схем из обратимых функциональных элементов при различном количестве используемых в схеме дополнительных входов (дополнительной памяти). Получены асимптотические оценки сложности, глубины и квантового веса обратимых схем и показано, что данные оценки существенно зависят от количества используемых дополнительных входов схемы.

Исследованы различные подходы к созданию алгоритмов синтеза обратимых схем, предложены и систематизированы различные способы снижения сложности обратимых схем, состоящих из обобщённых элементов Тоффоли. Разработан асимптотически оптимальный метод синтеза обратимых схем без дополнительных входов. Разработан новый быстрый алгоритм синтеза обратимой схемы, реализующей заданную чётную подстановку с малым числом подвижных точек. Также исследованы подходы к проблеме синтеза сбоеустойчивых обратимых схем (элементы с контролем чётности, с обеспечением самоконтролируемости обычных синтезированных схем и др.). Предложен метод синтеза сбоеустойчивых обратимых схем в пространствах Хэмминга.

Теоретически рассмотрено применение обратимых схем для решения задачи схемной реализации некоторых вычислительно асимметричных преобразований. Разработаны криптографические примитивы, которые обладают хорошими статистическими свойствами и могут применяться для построения систем симметричного шифрования, основанных на схемах из обратимых элементов. Предложены различные способы синтеза обратимых схем, реализующих алгоритм дискретного логарифмирования в конечном поле характеристики 2.

По результатам работ, выполненных в ходе выполнению проекта, один из исполнителей (Д. В. Закаблуков) в 2018 г. защитил кандидатскую диссертацию на соискание учёной степени кандидата физико-математических наук по специальности 01.01.09 дискретная математика и математическая кибернетика в учёном совете ВЦ им. А. А. Дородницына РАН ФИЦ «Информатика и управление». Руководитель – член коллектива исполнителей проекта А. Е. Жуков.

**Название Проекта (на англ. языке)**

Development of the theoretical bases of algorithms and hardware design based on schemes of reversible logic elements

**Аннотация, публикуемая на сайте РФФИ (на английском языке**

The project involves the creation of a foundation for deep research in the field of reversibility: the theory and methods for the synthesis of reversible schemes, including fault-tolerant, reversible algorithms for solving applied problems, the use of reversible schemes in modern cryptography, etc.

During the project, for the first time, the issue of synthesizing circuits from reversible functional elements was systematically studied with different numbers of additional inputs used in the circuit (additional memory). Asymptotic estimates are obtained for the complexity, depth, and quantum weight of reversible circuits, and it is shown that these estimates essentially depend on the number of used additional circuit inputs.

Various approaches to the creation of algorithms for the synthesis of reversible circuits are explored, and various ways of reducing the complexity of reversible circuits consisting of generalized elements of Toffoli are proposed and systematized. An asymptotically optimal method for the synthesis of reversible circuits without additional inputs has been developed. A new fast algorithm for the synthesis of a reversible scheme that implements a given even substitution with a small number of moving points has been developed. Also studied are approaches to the problem of synthesis of fail-safe reversible schemes (elements with parity control, ensuring the self-control of conventional synthesized schemes, etc.). A method for the synthesis of fault-tolerant reversible schemes in Hamming spaces is proposed.

Theoretically considered is the use of reversible schemes for solving the problem of the circuit implementation of some computationally asymmetric transformations. Cryptographic primitives have been developed that possess good statistical properties and can be used to build symmetric encryption systems based on schemes of reversible elements. Various methods for synthesizing reversible circuits that implement the discrete logarithm algorithm in a finite field of characteristic 2 are proposed.

**Цель и задачи фундаментального исследования (указать как в заявке)**

Фундаментальной целью проекта является разработка методов синтеза обратимых логических схем и их применение к задачам обратимости и однонаправленности.   
Задачи проекта:

1) создание методов и практических алгоритмов и синтеза схем из обратимых элементов.

2) исследование понятий однонаправленности и обратимости в математической кибернетике.

**Важнейшие результаты, полученные при реализации Проекта**

**1.** Проведены исследования обратимых схем, доказаны некоторые теоретические результаты, связанные с их свойствами. Впервые систематически изучен вопрос синтеза схем из обратимых функциональных элементов при различном количестве используемых в схеме дополнительных входов (дополнительной памяти). 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. Для сложности таких схем удалось получить эквивалентные с точность до порядка верхние и нижние оценки как в случае использования дополнительных входов в схеме, так и в случае их отсутствия. Особо стоит отметить установление в общем случае существенной зависимости характеристик обратимых схем от количества дополнительных входов, не характерной для схем из классических, необратимых функциональных элементов, а именно: увеличение количества дополнительных входов в обратимой схеме почти всегда позволяет снизить ее сложность, глубину и квантовый вес.

**2.** Исследованы различные существующие алгоритмы синтеза обратимых схем: переборные алгоритмы, непереборные быстрые алгоритмы, алгоритмы снижения сложности обратимой схемы. 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. Разработан новый быстрый алгоритм синтеза обратимой схемы, реализующей заданную чётную подстановку с малым числом подвижных точек. Доказано, что в сравнении с известными алгоритмами синтеза время работы данного алгоритма и требуемый им объём памяти асимптотически меньше. Разработан быстрый, асимптотически оптимальный метод синтеза обратимых схем без дополнительных входов, состоящих из функциональных элементов NOT, CNOT и 2-CNOT.

**3.** Исследованы подходы к проблеме синтеза сбоеустойчивых обратимых схем (элементы с контролем чётности, с обеспечением самоконтролируемости обычных синтезированных схем и др.). Предложен метод синтеза сбоеустойчивых обратимых схем в пространствах Хэмминга. Конкретно были также реализованы элементы HCNOT (управляемое отрицание), HLTG (гейт Тоффоли в хэмминговом пространстве), HFRG (гейт Фредкина в хэмминговом пространстве), HADD (обратимый сбоеустойчивый сумматор). Предложенные сбоеустойчивые схемы уже являются важными для обратимой схемотехники. Рассмотрены модификации схем в поляризованном хэмминговом пространстве.

**4.** Разработаны криптографические примитивы (блочный шифр, удовлетворяющий перспективным требованиям по скорости и криптостойкости, генератор псевдослучайных последовательностей и др.). Данные примитивы обладают хорошими статистическими свойствами и могут применяться для построения систем симметричного шифрования, основанных на схемах из обратимых элементов. Теоретически рассмотрено применение обратимых схем для решения задачи схемной реализации некоторых вычислительно асимметричных преобразований. Предложены различные способы синтеза обратимых схем, реализующих алгоритм дискретного логарифмирования в конечном поле характеристики 2. 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.

**5.** Применение полученных методов синтеза и способов снижения сложности обратимых схем позволило разработать программное обеспечение по синтезу обратимых схем [Zakablukov, D.V.: ReversibleLogicGenerator Software.

<https://github.com/dmitry-zakablukov/ReversibleLogicGenerator>], с помощью которого были получены схемы, имеющие существенно лучшие показатели по сравнению с известными ранее по таким показателям, как сложность и глубина схемы, число дополнительных линий (дополнительная память), квантовая стоимость. Данное программное обеспечение может быть применено в будущем при решении задач синтеза квантовых схем малой сложности.

Полученные в результате работы над проектом результаты можно использовать для анализа сложности различных отображений, а также для проектирования перспективных 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. Кроме того, сама суть обратимой логики предлагает новые интересные подходы, возможность иного взгляда, позволяющего решать важные фундаментальные задачи из сферы информационных технологий. В частности, этот подход дает возможность взглянуть с принципиально иной точки зрения на вопросы сложности вычислений, в том числе вопросы однонаправленности.

**Сопоставление результатов, полученных при реализации с мировым уровнем**

Тематика асимптотической сложности и глубины обратимых схем малоисследована и в отечественной и в зарубежной литературе. В процессе работы над проектом впервые систематически изучен вопрос синтеза схем из обратимых функциональных элементов при различном количестве используемых в схеме дополнительных входов (дополнительной памяти). Установлена в общем случае существенная зависимость характеристик обратимых схем от количества дополнительных входов, совершенно не характерная для схем из классических, необратимых функциональных элементов. Все полученные в ходе выполнения проекта результаты находятся на мировом уровне.

То же относится и к теоретическим исследованиям по применению обратимых схем для решения задач схемной реализации преобразований. Разработан единственный известный на сегодняшний день асимптотически оптимальный метод синтеза обратимых схем без дополнительных входов, состоящих из функциональных элементов NOT, CNOT и 2-CNOT. В результате были получены схемы, имеющие существенно лучшие показатели по сравнению с известными ранее по таким показателям, как сложность и глубина схемы, число дополнительных линий (дополнительная память), квантовая стоимость.

Предложенный метод синтеза сбоеустойчивых обратимых схем в пространствах Хэмминга оригинален и не по зарубежной литературе известен в применении к обратимым схемам.

Разработанные криптографические примитивы (блочный шифр, генератор псевдослучайных последовательностей) оригинальны. Данные исследования находятся на мировом уровне.

Часть результатов опубликована в зарубежных изданиях из базы данных «SCOPUS». Доклад, содержащий результаты, полученные в ходе работы над проектом, был включен в программу международной конференции «RC 2016, the 8th Conference on Reversible Computation», проходившей в 2016 г. в Болонье (Италия).

**Методы и подходы, использованные при реализации Проекта**

При исследованиях асимптотической сложности и глубины обратимых схем применялись методы дискретной математики, математической кибернетики, математической статистики, теории групп подстановок.

В ходе разработки алгоритмов синтеза обратимых схем (в том числе и методов синтеза сбоеустойчивых обратимых схем) использовались все вышеперечисленные методы, а также сравнительный анализ и математические моделирование.

При рассмотрении применения обратимых схем для решения задачи схемной реализации вычислительно асимметричных преобразований и разработки метода синтеза сбоеустойчивых обратимых схем в пространствах Хэмминга применялись методы дискретной математики.

При разработке криптографических примитивов (блочных шифров, удовлетворяющих перспективным требованиям по скорости и криптостойкости, генераторов псевдослучайных последовательностей и др.) использовались методы математической кибернетики и криптоанализа.

В целом, применяемые методы являются традиционными, но с их помощью получены новые оригинальные результаты, находящиеся на уровне мировых результатов. Отметим, что практически отсутствуют отечественные разработки данной тематики.

**Участие в научных мероприятиях по тематике Проекта за период, на который предоставлен грант (каждое мероприятие с новой строки, указать названия мероприятий и тип доклада)**

1. 8th International Conference «Reversible Computation 2016», Bologna, Italy, July 7–8, 2016. (8-я международная конференция Reversible Computation 2016, Болонья, Италия, 7-8 июля 2016 г.). – Закаблуков Д.В., секционный доклад.
2. Международная конференция «XXVII Крымская Осенняя Математическая Школа-симпозиум по спектральным и эволюционным задачам» (КРОМШ-2016), г. Севастополь, 17-29 сентября 2016 г. Гуров С.И. руководство секцией Дискретная математика и информатика, секционный доклад.
3. 3. VII Всероссийская научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем – 2016» (МЭС-2016), г. Зеленоград, Москва, 3-7 октября 2016 г. Гуров С.И. секционный доклад.
4. XVIII научно-практическая конференция «РусКрипто’2016», посвященная различным аспектам криптографии, информационной безопасности и защиты информации прошла 22 ‑ 25 марта 2016 г., Подмосковье. Жуков А. Е. пленарный доклад.
5. II Черноморская международная научно-практическая конференция МГУ имени М.В. Ломоносова «Математические, естественные и гуманитарные науки: совместные ответы на вызовы перспективных технологий», 24-27 мая 2017 г., г. Севастополь, филиал МГУ. Гуров С.И. секционный доклад, Жуков А.Е., секционный доклад.
6. Крымская осенняя математическая школа-симпозиум (КРОМШ-2017), 17-29 сентября 2017 г., г. Севастополь (Б/О «Чайка»). Гуров С.И. – руководство секцией Дискретная математика и информатика, Гуров С. И., секционный доклад.
7. XIX научно-практическая конференция «РусКрипто’2017», посвященная различным аспектам криптографии, информационной безопасности и защиты информации прошла 21 ‑ 24 марта 2017 г., Подмосковье. Жуков А. Е. пленарный доклад.
8. Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 29.01.2018 – 1.02.2018, 2018 IEEE Conference of Russian. – IEEE, Piscataway, NJ, United States, 2018. – С. 1430‑1433. Гуров С. И., секционный доклад.
9. XXVI Международная конференция «Математика. Экономика. Образование». Х международный симпозиум «Ряды Фурье и их приложения». Молодёжная школа-конфе-ренция по гармоническому анализу. 27 мая – 3 июня 2018 г. Краснодарский край, пос. Дюрсо. Гуров С. И., секционный доклад.
10. VIII Всероссийская научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем ‑ 2018» (МЭС-2018). Гуров С. И., секционный доклад.
11. XXVI Международная конференция «Математика. Экономика. Образование». Х международный симпозиум «Ряды Фурье и их приложения». Молодёжная школа‑конференция по гармоническому анализу. 27 мая – 3 июня 2018 г. Краснодарский край, пос. Дюрсо. Гуров С. И., секционный доклад.
12. Дискретные модели в теории управляющих систем: X Международная конференция, Москва и Подмосковье, 23-25 мая 2018 г. Закаблуков Д.В., секционный доклад.
13. XX юбилейная научно-практическая конференция «РусКрипто’2018», 20 ‑ 23 марта 2018 г., Подмосковье. Жуков А. Е. пленарный доклад.

**Публикации за 2018 г.**

1. Первый автор Alexander Stempkovskiy

Другие авторы D. Telpukhov, S. Gurov, T. Zhukova, A. Demeneva

Название R-code for Concurrent Error Detection and Correction in the Logic Circuits

Язык публикации английский

Издание Conference of Russian Young Researchers in Electrical and Electronic Engineering (EICon-Rus), 29.01.2018 – 1.02.2018, 2018 IEEE Conference of Russian.

Тип публикации Статья в журнале

Состояние опубликовано

Страницы 140-143

Краткий реферат

В настоящее время вопросы, связанные с синтезом отказоустойчивых комбинационных схем, приобретают особую актуальность. Этому способствуют различные факторы развития микроэлектронной промышленности, в том числе переход к нанометровым измерениям конструкции, а также разработка современных методов и средств автоматизации. Эти факторы вместе приводят к тому, что именно комбинационные области становятся наиболее уязвимой областью штампа. Решение этой проблемы часто связано с использованием избыточного кодирования, которое традиционно используется в системах хранения и передачи данных. Однако стандартные помехозащищённые коды часто неэффективны из-за особенностей конструкции комбинационной схемы, и ошибки в них игнорируются. Мы предлагаем новый подход к построению отказоустойчивых комбинационных схем с использованием избыточного кодирования на основе спектрального R-кода. Этот код исправляет единичные и обнаруживает двойные ошибки. Мы применяем методы технологической защиты для части декодера, код исправляет любую единственную ошибку в комбинационной схеме, и мы получаем меньшую структурную избыточность по сравнению с тройной модульной избыточности. В статье представлена серия численных экспериментов, демонстрирующих высокую эффективность предлагаемого подхода.

1. Первый автор Гуров Сергей Исаевич

Другие авторы Жукова Татьяна Дмитриевна

Название Сбоеустойчивая обратимая логика

Язык публикации русский

Издание XXVI Международная конференция «Математика. Экономика. Образование». Х международный симпозиум «Ряды Фурье и их приложения». Молодёжная школа-конференция по гармоническому анализу. 27 мая – 3 июня 2018 г. Краснодарский край, пос. Дюрсо. Материалы

Тип публикации Тезисы доклада

Состояние опубликовано

Страницы

Краткий реферат

В докладе рассмотрены основные понятия обратимой схемотехники, при этом основное внимание уделено существующим моделям построения сбоеустойчивых обратимых схем и методам их тестирования. На сегодняшний день стал уже очевиден кризис специализированных классических информационных технологий на элементной базе интегральных микросхем (ИМС), которые перестают отвечать возрастающим требованиями по быстродействию, объёмам используемой памяти, плотности элементов на кристалле, надёжности вычислений и др. В связи с этим понятны причины активизации в последнее время интереса к развитию методов синтеза обратимых схем. На этом пути, однако, возникает проблемы надёжности функционирования ИМС, и, в первую очередь - проблема их устойчивости к кратковременным самоустраняемым отказам или *сбоям* (SEU, single event upsets). Причинами сбоев являются воздействия на схему различных видов помех: радиационных, скачков напряжений питания, деградаций сигналов во времени и др. В связи с данной проблемой в докладе рассматриваются основные понятия обратимой схемотехники и методы синтеза сбоеустойчивых обратимых схем. Предложен оригинальный подход к указанной проблеме, основанный на помехоустойчивом кодировании в конечном Хэмминговом пространстве. Конкретно, представлена сбоеустойчивая модификация элемента Тоффоли, синтезированная в рамках предлагаемого подхода.

1. Первый автор Гуров Сергей Исаевич

Другие авторы Кормаков Георгий Владимирович

Название Сбоеустойчивые обратимые схемы и метод их синтеза в пространстве Хемминга

Язык публикации русский

Издание Прикладная математика и информатика: Труды факультета Вычислительной математики и кибернетики

Тип публикации Статья в журнале

Состояние опубликовано

Номер издания 57

Страницы 21-35

Краткий реферат

На сегодняшний день стал уже очевиден кризис классических информационных технологий на элементной базе интегральных микросхем (ИМС), которые перестают отвечать возрастающим требованиями по быстродействию, объёмам используемой памяти, плотности элементов на кристалле, надёжности вычислений и др. Основными недостатками классических методов вычислений является чрезмерное выделение тепла при обеспечении указанных требований и недостаточная устойчивость специализированных ИМС к внешним воздействиям. Известно, что выполнении логических операций классическими схемами при потере одного бита информации выделяется энергия *ε0* *=k·T·ln 2* [Дж], где *k* - постоянная Больцмана, T - температура в градусах Кельвина В пересчете на процессор суммарная рассеиваемая мощность вырастает уже до величин порядка 1 Вт. На практике, с учётом активных сопротивлений реальных полупроводников, получаем процессоры, которые по тепловыделению обгоняют утюги. Эту ситуацию можно назвать «тепловым проклятием» существующей парадигмы ВТ. В известной статье Р. Меркля и К. Дрекслера «Спиральная логика» отмечалось, что есть только два способа, как обеспечить рассеивание энергии ниже ε0: проводить вычисления при низких температурах, уменьшая *kT*, или использовать обратимую логику. При этом низкотемпературная работа не уменьшает общую рассеиваемую энергию, а просто переносит её затраты на холодильное оборудование. Ч. Беннетт в 1973 г. показал, как можно построить обратимый компьютер, рассеивающий энергию, значительно меньшую, чем *ε0* на каждую элементарную операцию, а в идеале и иметь нулевое рассеивание энергии. В связи с этим понятны причины активизации в последнее время интереса к развитию методов синтеза обратимых схем, как комбинационных, так и последовательностных. На этом пути, однако, возникает проблема надёжности функционирования ИМС, и, в первую очередь проблема их устойчивости к кратковременным самоустраняемым отказам или сбоям (SEU, single event upsets), второй из указанных выше недостатков. При уменьшении проектных норм до десятков и единиц нанометров, энергия активации, вызывающая ошибки, уменьшается. Поэтому сбоеустойчивость является важнейшим требованием к аппаратуре, работающей, например, в тяжелых условиях космоса. В настоящее время в мире активно развивается направление радиационно-стойкого проектирования (RHBD, Radiation Hardening By Design) основанное на использовании схемотехнических, топологических и алгоритмических методов повышения сбоеустойчивости. В данной статье рассмотрены основные существующие модели построения сбоеустойчивых обратимых схем и предложен новый подход к данной проблеме.

1. Первый автор Гуров Сергей Исаевич

Название Конечные поля и группы перестановок: приложения в теории кодирования и комбинаторике

Язык публикации русский

Издание КДУ

Тип публикации Монография

Состояние опубликовано

Страницы 190

1. Первый автор Тельпухов Дмитрий Владимирович

Другие авторы Жукова Татьяна Дмитриевна, Гуров Сергей Исаевич

Название Схема функционального контроля для комбинационных схем на основе R-кода

Язык публикации русский

Издание VIII Всероссийская научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем - 2018» (МЭС-2018). Сборник трудов / под общ. ред. академика РАН А. Л. Стемпковского.

Тип публикации Статья в сборнике

Состояние опубликовано

Том издания IV

Страницы 98-103

Краткий реферат

В настоящее время особую актуальность приобретают вопросы, связанные с синтезом комбинационных схем, устойчивых к одиночным эффектам. Этому способствуют как совокупность различных факторов развития микроэлектронной промышленности, так и современное состояние в области разработки средств автоматизации проектирования. Такие факторы, как переход к нанометровым нормам проектирования, увеличение тактовых частот, понижение напряжения питания в совокупности приводят к тому, что наиболее уязвимой частью интегральных схем становятся именно комбинационные участки. Часто для решения проблемы обеспечения сбоеустойчивости привлекают методы избыточного кодирования, которое традиционно используется в системах хранения и передачи данных. Однако стандартные помехоустойчивые коды обычно малоэффективны из-за специфики конструкции и функционирования комбинационных схем. В рамках данной работы был предложен новый подход к построению сбоеустойчивых комбинационных схем с использованием избыточного кодирования на основе спектрального R-кода. Применение методов технологической защиты для части кодера позволяет данному коду помимо всего прочего исправлять любую однократную ошибку в комбинационной схеме, а также обнаруживать в ней двукратную ошибку. В результате полученная схема обладает меньшей структурной избыточностью по сравнению с тройным модульным резервированием. В статье представлены результаты серии численных экспериментов, демонстрирующих высокую эффективность предлагаемого подхода. Ключевые слова — сбоеустойчивость комбинационных схем, информационная избыточность, избыточное кодирование, R-код.

1. Первый автор Гуров Сергей Исаевич

Название Использование информационной избыточности при построении сбоеустойчивых комбинационных схем

Язык публикации русский

Издание Таврический вестник информатики и математики

Тип публикации Статья в журнале

Состояние опубликовано

Номер издания 2

Страницы 29-44

Краткий реферат

В статье на основе проведенного анализа специфики задачи повышения сбоеустойчивости комбинационных интегральных схем методами избыточного кодирования формулируются и требования к такому коду. Предлагается линейный нециклический код с проверками на четность, удовлетворяющий данным требованиям. Код исправляет одиночные ошибки, обнаруживает двойные и обладает преимуществами, существенными для рассматриваемой задачи. Дана оценка эффективности предложенного кода.

1. Первый автор Жуков Алексей Евгеньевич

Другие авторы Гуров Сергей Исаевич

Название Обратимые вычисления и криптография

Язык публикации русский

Издание Защита информации. INSIDE

Тип публикации Статья в журнале

Состояние опубликовано

Том издания 6

Номер издания 84

Страницы 74-79

Краткий реферат

Обратимые вычисления – новая, активно развивающаяся парадигма вычислений. К середине XXI века ожидается переход всей ИТ-технологии на реализацию обратимых вычислений что, помимо всего прочего, заставит пересмотреть как существующие криптографические примитивы, так и многие фундаментальные принципы их построения. Кроме того, сама суть обратимой логики предлагает новые интересные подходы, дает возможность взглянуть с принципиально иной точки зрения на вопросы сложности вычислений, в том числе вопросы однонаправленности.

1. Первый автор Гуров Сергей Исаевич

Другие авторы Кормаков Георгий Владимирович, Жукова Татьяна Дмитриевна

Название Сбоеустойчивые обратимые схемы

Язык публикации русский

Издание XXVI Международная конференция «Математика. Экономика. Образование». Х международный симпозиум «Ряды Фурье и их приложения». Молодёжная школа-конференция по гармоническому анализу. 27 мая – 3 июня 2018 г. Краснодарский край, пос. Дюрсо. Сборник трудов.

Тип публикации Статья в сборнике

Состояние принято в печать

Том издания

Краткий реферат

Современные возрастающие требования по быстродействию, объёмам используемой памяти, плотности элементов на кристалле, надёжности вычислений и др. приводят к тому, что классические информационные технология на элементной базе интегральных микросхем ИМС перестают им отвечать. Основной из недостатков связан с тем, что обеспечение указанных требований ведёт к значительному выделению тепла. Современная цифровая электроника изготавливается на основе металл-оксидных полевых транзисторов (MOSFET). В последнее активизировались исследования по разработки синтеза обратимых схем, как комбинационных, так и последовательностных. Второй важной проблемой современной ВТ является надёжность функционирования ИМС, причём на первый план здесь выходит задача обеспечения их устойчивости к кратковременным самоустраняемым отказам или *сбоям* (SEU, single event upsets). Современные специализированные вычислительные устройства часто работают в условиях воздействия внешней радиации. До 50% отказов в современном оборудовании, работающем в условиях воздействия внешней радиации, связаны с влиянием дозовых и однократных радиационных эффектов. При уменьшении проектных норм до нанометров, энергия активации, вызывающая ошибки, уменьшается. Поэтому сбоеустойчивость является важнейшим требованием к аппаратуре, работающей, например, в тяжелых условиях космоса. Это вызвало появление и активное развитие направления радиационно-стойкого проектирования (RHBD, Radiation Hardening by Design) основанное на использовании различных методов повышения сбоеустойчивости ИМС. В данной статье рассмотрены основные существующие модели построения сбоеустойчивых обратимых комбинационных схем и предложен новый подход к данной проблеме.

1. Первый автор Гуров Сергей Исаевич

Другие авторы Жуков Алексей Евгеньевич, Закаблуков Дмитрий Владимирович, Кормаков Георгий Владимирович

Название Обратимые вычисления: обзор проблемы

Язык публикации русский

Издание Автоматика и телемеханика

Тип публикации Статья в журнале

Состояние сдано в редакцию

Краткий реферат

Интерес к обратимым вычислениям и реализующим их схемам из обратимых элементов возник в начале 1960-х г., когда был сформулирован казавшийся сначала парадоксальным принцип Неймана-Ландауэра: в любой вычислительной системе, независимо от её физической реализации, при потере одного бита информации выделяется теплота в количестве не менее kT ln 2 Дж (k - постоянная Больцмана, T -абсолютная температура. В 2012 г. в эксперименте с коллоидной частицей эффект Ландауэра удалось обнаружить на практике. В пересчете на процессор суммарная рассеиваемая мощность вырастает уже до величин порядка 1 Вт. Данная ситуация выглядит как конец развития вычислительной техники в рамках существующих технологий из-за «теплового проклятия». Выход видят в переходе к вычислительным устройствам, реализующим обратимые вычисления, позволяющие обойти ограничение, устанавливаемое принципом Ландауэра. При обратимых вычислениях информация не теряется, откуда следуют (теоретически) нулевые потери энергии на её обработку. Важным является то, что обратимость необходимо поддерживать на всех уровнях вычислений: физической модели, архитектуры вычислителя, языков программирования высокого уровня и реализуемых алгоритмов: Ч. Беннетт указал, что необратимость хотя бы на одном уровне полностью разрушает положительные эффекты остальных. Отсюда следует, что для создания парадигмы обратимых вычислений требуется разработать следующие новые направления: • теорию (алгебру и логику) обратимых вычислений; • языки и парадигмы обратимого программирования; • методы реализации прикладных программ и алгоритмы обратимого программирования; • обратимую схемотехнику; физическую реализацию обратимых элементов. В статье дан краткий обзор основных понятий, связанных с обратимостью, рассмотрены вопросы построения схем из функциональных обратимых элементов, в том числе сбоеустойчивых и предложены основные такие элементы. Указаны направления и результаты применения схем из обратимых логических элементов в криптографии.

1. Первый автор Жуков Алексей Евгеньевич

Название Один подход к изучению однонаправленности

Язык публикации русский

Издание Information Security/ Информационная безопасность

Тип публикации Статья в журнале

Состояние опубликовано

Том издания 1

Страницы 40-43

Краткий реферат

Понятие однонаправленной функции является одним из важнейших для современной криптографии. Однако строгих доказательств существования или возможности построения таких функций в настоящее время нет. В работе рассматривается один подход, позволяющий новым образом взглянуть на явление однонаправленности. Суть подхода заключается в применении обратимых схем для реализации вычислительно асимметричных преобразований. На примере обратимых схем, реализующих линейные асимметричные преобразования, показывается, что разница в сложности прямого и обратного преобразований в некоторых случаях связана с разницей в сложности соответствующих подсхем по уборке вычислительного мусора. На основании рассмотренных обратимых схем делается предположение о структуре вычислительно асимметричных преобразований.

1. Первый автор Закаблуков Дмитрий Владимирович

Название О зависимости сложности и глубины обратимых схем, состоящих из функциональных элементов NOT, CNOT и 2-CNOT, от количества дополнительных входов

Язык публикации русский

Издание Дискретная математика

Тип публикации Статья в журнале

Состояние сдано в редакцию

URL: [https://arxiv.org/abs/1702.08045](https://mail.rambler.ru/m/redirect?url=https%3A//arxiv.org/abs/1702.08045&hash=8163c7bd5111fca5ae8743f73b170bb1) (дата обращения: 20.07.2018).

Краткий реферат

В работе рассматривается вопрос сложности и глубины обратимых схем, состоящих из функциональных элементов NOT, CNOT и 2-CNOT, в условиях ограничения на количество используемых дополнительных входов. Изучаются функции Шеннонa сложности и глубины обратимой схемы, реализующей отображение , при условии, что количество дополнительных входов находится в диапазоне . Для указанного диапазона значений доказываются асимптотические верхние оценки:

и

.

1. Первый автор Закаблуков Дмитрий Владимирович

Название Методы синтеза обратимых схем из функциональных элементов NOT, CNOT и 2-CNOT

Язык публикации русский

Издание Диссертация на соискание учёной степени кандидата физико-математических наук: 01.01.09 – ВЦ РАН ФИЦ «Информатика и управление» РАН, Москва, 2018

Тип публикации Монография

Состояние опубликовано

Страниц 151

Краткий реферат

Основными целями диссертации являются изучение обратимых схем из функциональных элементов NOT, CNOT и 2-CNOT, разработка новых методов синтеза таких схем и изучение зависимости их сложности и глубины от количества используемых дополнительных входов схемы.

В диссертации впервые систематически изучается вопрос синтеза схем из обратимых функциональных элементов при различном количестве используемых в схеме дополнительных входов (дополнительной памяти). Разработан новый быстрый алгоритм синтеза обратимой схемы, реализующей заданную чётную подстановку с малым числом подвижных точек. Предложены и систематизированы различные способы снижения сложности обратимых схем, состоящих из обобщённых элементов Тоффоли. Получены асимптотические оценки сложности, глубины и квантового веса обратимых схем и показано, что данные оценки существенно зависят от количества используемых дополнительных входов схемы. Разработан асимптотически оптимальный метод синтеза обратимых схем без дополнительных входов. Предложены различные способы синтеза обратимых схем, реализующих алгоритм дискретного логарифмирования в конечном поле характеристики 2.

Предложенные методы синтеза и способы снижения сложности обратимых схем были реализованы в программном обеспечении по синтезу обратимых схем без дополнительных входов. Данное программное обеспечение может быть применено при решении задач синтеза квантовых схем малой сложности. С другой стороны, разработанные методы снижения сложности обратимых схем позволяют изучать структуру подстановок на множестве двоичных векторов при помощи изучения структуры реализующих их обратимых схем.

1. Первый автор Закаблуков Дмитрий Владимирович

Название Обзор методов синтеза обратимых схем с ограниченной памятью

Язык публикации русский

Издание Дискретные модели в теории управляющих систем: X Международная конференция, Москва и Подмосковье, 23-25 мая 2018 г.: Труды

Тип публикации Статья в сборнике

Состояние опубликовано

Страницы 125-128

Краткий реферат

Приводится обзор полученных автором результатов по синтезу схем из обратимых функциональных элементов при различном количестве используемых в схеме дополнительных входов (дополнительной памяти). Приводятся асимптотические оценки сложности и глубины обратимых схем и показано, что данные оценки существенно зависят от количества используемых дополнительных входов схемы.

1. Первый автор Тельпухов Дмитрий Владимирович

Другие авторы Надоленко Владимир Владимирович, Гуров Сергей Исаевич

Название Вычисление наблюдаемости элементов комбинационных логических схем с использованием бит-параллельного моделирования

Язык публикации русский

Издание Прикладная математика и информатика: Труды факультета Вычислительной математики и кибернетики

Тип публикации Статья в журнале

Состояние опубликовано

Номер издания 59

Страницы 94-110

Краткий реферат

В данной работе рассмотрены методы определения наблюдаемости элементов комбинационной логической схемы, опирающиеся на векторные вычисления (бит-параллельное моделирование). Результатом таких вычислений является набор ODC (observability don’t care) всех узлов для заданного набора состояний схемы. Эти данные позволяют оценить вероятность логического маскирования случайного сбоя в схеме. Сравнение методов по точности и временным затратам подкреплено результатами тестирования на схемах ISCAS’85. Ключевые слова: наблюдаемость, бит-параллельное моделирование, комбинационные схемы, ODC

1. Первый автор Закаблуков Д.В.

Название О сложности обратимых схем, состоящих из функциональных элементов NOT, CNOT и 2-CNOT.

Язык публикации русский

Издание Дискретная математика, 2016. Т. 28, №2. С. 12–26.

Рассматривается вопрос о сложности обратимых схем, состоящих из функциональных элементов NOT, CNOT и 2-CNOT. Определяется функция Шеннонa сложности обратимой схемы, реализующей отображение , как функция от и количества дополнительных входов схемы.