На правах рукописи

Пестунов Андрей Игоревич

СТАТИСТИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ОЦЕНКИ ЗАЩИЩЁННОСТИ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ИТЕРАТИВНЫХ БЛОЧНЫХ ШИФРОВ

05.13.19 — Методы и системы защиты информации, информационная безопасность

Автореферат
диссертации на соискание учёной степени
кандидата физико-математических наук

Новосибирск 2013

Работа выполнена в федеральном государственном бюджетном учреждении науки Институте вычислительных технологий Сибирского отделения Российской академии наук (ИВТ СО РАН)

Научный руководитель:

Осипов Александр Леонидович, кандидат технических наук, старший научный сотрудник, заведующий кафедрой прикладных информационных технологий Новосибирского государственного университета экономики и управления "НИНХ"

Официальные оппоненты:

Воробейчиков Сергей Эрикович, доктор физико-математических наук, профессор кафедры высшей математики и математического моделирования Национального исследовательского Томского государственного университета

Токарева Наталья Николаевна, кандидат физико-математических наук, старший научный сотрудник лаборатории дискретного анализа Института математики им. С. Л. Соболева СО РАН

Ведущая организация: Федеральное государственное автономное образовательное учреждение высшего профессионального образования "Сибирский федеральный университет" (СФУ), г. Красноярск

Защита состоится "21" июня 2013 г. в 10.35 на заседании диссертационного совета Д 212.267.22 на базе федерального государственного бюджетного образовательного учреждения высшего профессионального образования "Национальный исследовательский Томский государственный университет" по адресу: 634050, г. Томск, пр. Ленина, 36 (учебный корпус №2, ауд. 212б).

С диссертацией можно ознакомиться в Научной библиотеке Томского государственного университета.

Автореферат разослан "20" мая 2013 г.

Учёный секретарь
диссертационного совета
кандидат технических наук,
доцент

Трепькаев В. Н.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Стремительное развитие информационных технологий привело к появлению новых угроз нарушения информационной безопасности, и, следовательно, разработка и совершенствование методов защиты информации в процессе её хранения и передачи в настоящее время является актуальной научно-технической проблемой. *Итеративные блочные шифры* являются одним из тех методов, которые часто используются в системах обеспечения информационной безопасности для защиты конфиденциальности данных, а также для построения хеш-функций и кодов аутентичности сообщений, защищающих информацию от подделок и модификаций.

Важным этапом создания новых и совершенствования существующих итеративных блочных шифров является оценка обеспечиваемой ими защищённости информации. Модели, в рамках которых такую оценку можно получить аналитически, применимы далеко не всегда, поэтому для комплексной оценки защищённости информации производится разработка и моделирование атак, направленных на вычисление секретного ключа или ключей раундов шифра. Научный интерес представляют атаки, оказывающиеся эффективнее существующих хотя бы по одному из общепринятых показателей.

Методы оценки защищённости информации, обеспечиваемой блочными шифрами, делятся на два класса: детерминированные и статистические. Одним из наиболее распространённых статистических методов является разностный анализ. Несмотря на большое число работ, посвящённых этому методу, в них используются понятия, связи и соотношения между которыми недостаточно формализованы. Кроме того, в рамках проблемы теоретического обоснования разностного анализа существует ряд других нерешённых задач, в том числе исследование того, как изменяется разность двух блоков после операций, используемых в раундовых функциях шифров.

С увеличением числа *раундов* — простых преобразований, итерация которых образует блочный шифр, — повышается степень защищённости, обеспечиваемая шифром, но вместе с тем снижается производительность реализующих его программно-аппаратных средств. Определение оптимального числа раундов является ключевой проблемой, связанной с блочными шифрами.

Итеративные блочные шифры используются для генерации псевдослучайных чисел, широко применяющихся в системах защиты информации. Отсюда вытекает проблема нахождения баланса не только между производительностью и уровнем защищённости, но и между производительностью и качеством генерируемых псевдослучайных чисел. Кроме того, шифры, обладающие неудовлетворительными статистическими свойствами, не могут обеспечить высокий уровень информационной безопасности.

Таким образом, теоретическое обоснование и применение статистических методов анализа блочных шифров, а также разработка и исследование эффективности статистических тестов имеет важное значение для оценки защи-

щённости информации, обеспечиваемой итеративными блочными шифрами. Несмотря на существующие российские и зарубежные стандарты на шифры, актуальность создания новых и совершенствования существующих блочных шифров по-прежнему высока. Это приводит к тому, что в последние годы активно проводятся международные проекты, направленные на их комплексный анализ и стандартизацию (AES, NESSIE, CRYPTREC).

Целью работы является разработка, теоретическое и экспериментальной обоснование и исследование эффективности статистических методов и средств оценки защищённости информации при использовании итеративных блочных шифров.

Для достижения этой цели были поставлены следующие **задачи**.

- Оценка защищённости информации, обеспечиваемой итеративными блочными шифрами, методом разностного анализа.
- Теоретическое обоснование метода разностного анализа и формализация связей и соотношений между его понятиями.
- Теоретическое и экспериментальное исследование эффективности статистических тестов и критериев.
- Оценка защищённости информации итеративными блочными шифрами при помощи статистических тестов и критериев; нахождение зависимости статистических свойств блочных шифров от числа раундов в них.

Объектом исследований являются статистические модели и методы оценки защищённости информации итеративными блочными шифрами; статистические тесты и критерии.

Предметом исследований являются статистические свойства итеративных блочных шифров; вероятность успеха и сложность атак на итеративные блочные шифры; ошибки первого и второго рода статистических тестов и критериев; разностные вероятностные характеристики и дифференциалы блочных шифров.

Методы исследований. Аппарат математического анализа, теории вероятностей и математической статистики; методы статистического моделирования и регрессионного анализа; технологии программирования на языках C, C++ и Java.

Научная новизна

1. Получены результаты, представляющие собой вклад в развитие теории разностного метода анализа итеративных блочных шифров.
   (а) Формализованы основные понятия данного метода и систематизированы связи между ними.
   (б) Теоретически определена зависимость между вероятностью сохранения разности двух величин после арифметических операций, используемых в блочных шифрах, от веса Хэмминга этой разности.

2. Методом разностного анализа проведена оценка защищённости информации кандидатами конкурса AES шифрами MARS и CAST-256.

   (а) Предложены разностные характеристики этих шифров и получены оценки их вероятностей, на основании чего разработаны атаки на данные шифры, являющиеся эффективнее существующих.

   (б) Получены оценки сложности разностной атаки в общем случае при различных параметрах итеративных блочных шифров.

3. Теоретически и экспериментально обоснована эффективность статистического теста "стопка книг".

   (а) Теоретически доказано, что для одного класса альтернативных гипотез тест "стопка книг" позволяет достичь заданных значений ошибок первого и второго рода при размере выборки $O(\sqrt{S})$, где S — размер алфавита, которому принадлежат элементы выборки.

   (б) Экспериментально показано, что для класса линейных конгруэнтных генераторов "стопка книг" эффективнее спектрального теста.

4. Проведено статистическое исследование защищённости информации итеративными блочными шифрами, заявленными на конкурс AES.

   (а) Определены зависимости от числа раундов длин последовательностей псевдослучайных чисел (генерируемых этими шифрами), при которых тест "стопка книг" отличает их от равномерно распределённых случайных чисел.

   (б) Найдено число раундов, при котором псевдослучайные числа, генерируемые рассматриваемыми шифрами, не отличаются от равномерно распредёленных случайных чисел.

Соответствие диссертации паспорту специальности. Диссертация соответствует п. 9 "Модели и методы оценки защищенности информации и информационной безопасности объекта" паспорта специальности 05.13.19.

Достоверность результатов обеспечена корректностью постановок задач, математическими доказательствами теоретических утверждений, экспериментальной проверкой теоретических результатов, сравнением полученных экспериментальных данных с эталонными.

Положения, выносимые на защиту.

1. Формализация основных понятий разностного метода и систематизация связей между ними.

2. Теоретически обоснованная зависимость вероятности сохранения разности двух величин после арифметических операций, используемых в блочных шифрах, от веса Хэмминга этой разности.

3. Разностные характеристики шифров MARS и CAST-256; атаки на эти шифры, основанные на предложенных характеристиках; оценки сложности разностной атаки в зависимости от параметров блочных шифров.
4. Теоретическое и экспериментальное обоснование эффективности статистического теста "стопка книг".
5. Зависимости от числа раундов длин псевдослучайных последовательностей, генерируемых шифрами-кандидатами AES, при которых тест "стопка книг" отличает их от равномерно распределённых случайных чисел. Минимальное число раундов, при котором эти последовательности обладают удовлетворительными статистическими свойствами.

Практическая ценность. Разработан программный комплекс для статистического оценивания защищённости информации при использовании итеративных блочных шифров "СКАБШ-2012". Найдены зависимости статистических свойств блочных шифров от числа раундов, что может служить рекомендацией к применению шифров для генерации псевдослучайных чисел.

Основные результаты работы использовались при выполнении базовых проектов ИВТ СО РАН по приоритетным направлениям фундаментальных исследований РАН (№№ гос. регистрации 01.2007.07871 и 01.2010.61308) и внедрены в учебный процесс Новосибирского государственного университета экономики и управления (НГУЭУ) при подготовке студентов по специальности "Организация и технология защиты информации" и направлению "Информационная безопасность".

Исследования по теме диссертации поддержаны грантом Лаврентьевского конкурса молодежных проектов СО РАН (2010–2011 гг.), грантом № 11-07-09299 Российского фонда фундаментальных исследований по программе "Мобильность молодых ученых" (2011 г.), грантом Фонда содействия отечественной науке в номинации "Лучшие аспиранты РАН" (2006–2007 гг.), стипендией администрации Новосибирской области в сфере научной деятельности (2006 г.) и частично грантами №№ НШ-931.2008.9 и НШ-6068.2010.9 Президентской программы "Ведущие научные школы РФ" (рук. академик Ю.И. Шокин).

Апробация работы. Результаты диссертации докладывались и обсуждались на следующих конференциях и семинарах: VII Intern. Conf. on Intelligent Information Hiding and Multimedia Signal Processing, Dalian, China, 2011; XII Всеросс. научно-практ. конф. "Проблемы информационной безопасности государства, общества и личности", Томск– Барнаул–Белокуриха, 2010; IX Сибирская науч. школа-семинар с междунар. участием "Компьютерная безопасность и криптография" (Sibecrypt-IX), Тюмень, 2010; IEEE Region 8 Intern. Conf. on Computational Technologies in Electrical and Electronic Engineering (Sibircon-2008), Novosibirsk, 2008; Российско-Казахстанское совещание рабочей группы, Новосибирск, 2007; XI Intern. Symp. on Problems of Redundancy in Information and Control Systems, Saint Petersburg,

2007; Междунар. конф. "Вычислительные и информационные технологии в науке, технике и образовании", Павлодар, 2006; VII Всеросс. конф. молодых ученых по матем. моделированию и информационным технологиям, Красноярск, 2006 Междунар. школа-конф. по приоритет. направл. развития науки и техники с участием молодых ученых, аспирантов и студентов, Москва, 2006; конф. "Информационная безопасность" в рамках науч. сессии НГУЭУ в 2010–2013 гг.; семинары ИВТ СО РАН: "Информационные технологии" (рук.: академик Ю.И. Шокин, чл.-корр. А.М. Федотов, д.ф.-м.н. С.К. Голушко), "Информационно-вычислительные технологии" (рук.: академик Ю.И. Шокин, д.ф.-м.н. В.М. Ковеня), "Информационно-вычислительные технологии в задачах поддержки принятия решений" (рук.: академик Ю.И. Шокин, д.ф.-м.н. Л.Б. Чубаров, д.ф.-м.н. М.П. Федорук); семинар каф. защиты информации и криптографии ТГУ (рук. д.т.н. Г.П. Агибалов), семинар "Криптография и криптоанализ" (рук. к.ф.-м.н. Н.Н. Токарева, ИМ СО РАН).

Публикации. По теме диссертации опубликовано 14 работ, в том числе 7 статей в журналах, рекомендованных ВАК, 4 работы в трудах международных конференций и 3 работы в тезисах конференций.

Личный вклад автора. Все результаты, выносимые на защиту, получены автором лично. В совместной работе [7] автор программно реализовал тест "стопка книг" и провел эксперименты по предложенной соавтором схеме.

Структура и объём работы. Диссертация включает введение, три главы, заключение и список литературы из 156 наименований. Основной текст работы, содержащий 32 таблицы и 11 рисунков, изложен на 124 страницах. Общий объём диссертации составляет 161 страницу.

Благодарность. Автор выражает глубокую благодарность директору Института вычислительных технологий СО РАН академику Ю.И. Шокину за постоянное внимание к работе и поддержку.

СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** обоснована актуальность выбранной темы, определены цель и задачи исследования, раскрыта научная новизна работы и практическая значимость полученных результатов. Сформулированы положения, выносимые на защиту, и кратко изложено содержание диссертации.

В **главе 1** представлен аналитический обзор по теме исследований, обозначены основные проблемы, связанные с оценкой защищённости информации при использовании итеративных блочных шифров, произведена постановка задач диссертации и обоснована их актуальность.

Глава 2 посвящена оценке защищённости информации, обеспечиваемой блочными шифрами, с использованием разностного метода анализа.

В **§2.1** описаны проблемы в существующей терминологии разностного анализа итеративных блочных шифров и предложен набор определений, образующих строгую единообразную терминологию, согласованную с существу-

ющими понятиями. В качестве основных проблем отмечены отсутствие строгих общепринятых терминов и отсутствие точных соответствий между понятиями характеристики, дифференциала, усечённой характеристики и усечённого дифференциала. Такая ситуация не позволяет проводить какие-либо рассуждения, применимые сразу для всех этих объектов, но требует рассмотрения частных случаев. Предложенный набор определений решает обозначенные проблемы и формирует терминологию, в рамках которой дифференциал, усечённый дифференциал и характеристика при определённых условиях являются усечёнными характеристиками. Показано, как вычисляется вероятность объединения усечённых характеристик для марковских шифров с использованием уравнения Колмогорова-Чепмена по аналогии с тем, как это сделано в статье К. Лэй и Дж. Мэсси для характеристик.

В **§2.2** теоретически исследована зависимость между весом Хэмминга разности и вероятностью её сохранения после арифметических операций по модулю 2^s. Результаты сформулированы в виде теорем и следствий. Пусть $\boxplus$, $\boxminus$ и $\circledast$ — соответственно сложение, вычитание и умножение по модулю 2^s, $\oplus$ — операция XOR, $\mathcal{U}\{0,1\}^s$ — равномерное распределение на множестве двоичных векторов длины s, $H(\cdot)$ — функция вычисления веса Хэмминга, $\Delta^{[s-1]}$ — $(s-1)$-ый (старший) бит величины Δ.

Теорема 2.1. Пусть X, $Z \sim \mathcal{U}\{0,1\}^s$ и $Y = X \oplus \Delta$, где $H(\Delta) = h$, $0 \le h \le s-1$ и $\Delta^{[s-1]} = 0$, тогда

$$\mathbf{P}\big((X \boxplus Z) \oplus (Y \boxplus Z) = \Delta\big) = 2^{-h}.$$

Утверждение 2.1. Пусть X, $Z \sim \mathcal{U}\{0,1\}^s$ и $Y = X \oplus \Delta$, где $H(\Delta) = h$, $1 \le h \le s$ и $\Delta^{[s-1]} = 1$, тогда

$$\mathbf{P}\big((X \boxplus Z) \oplus (Y \boxplus Z) = \Delta\big) = 2^{-(h-1)}.$$

Утверждение 2.2.

(а) Пусть X, $Z \sim \mathcal{U}\{0,1\}^s$ и $Y = X \oplus \Delta$, где $H(\Delta) = h$, $0 \le h \le s-1$ и $\Delta^{[s-1]} = 0$, тогда $\mathbf{P}\big((X \boxminus Z) \oplus (Y \boxminus Z) = \Delta\big) = 2^{-h}$.

(б) Пусть X, $Z \sim \mathcal{U}\{0,1\}^s$ и $Y = X \oplus \Delta$, где $H(\Delta) = h$, $1 \le h \le s$ и $\Delta^{[s-1]} = 1$, тогда $\mathbf{P}\big((X \boxminus Z) \oplus (Y \boxminus Z) = \Delta\big) = 2^{-(h-1)}$.

Утверждение 2.3. Пусть X, $Z \sim \mathcal{U}\{0,1\}^s$ и $Y = X \oplus 2^m$, тогда

(а) $\mathbf{P}\big((X \boxplus Z) \oplus (Y \boxplus Z) = 2^m\big) = 1/2$, если $m < s-1$,

(б) $\mathbf{P}\big((X \boxminus Z) \oplus (Y \boxminus Z) = 2^m\big) = 1/2$, если $m < s-1$,

(в) $\mathbf{P}\big((X \boxplus Z) \oplus (Y \boxplus Z) = 2^m\big) = 1$, если $m = s-1$,

(г) $\mathbf{P}\big((X \boxminus Z) \oplus (Y \boxminus Z) = 2^m\big) = 1$, если $m = s-1$.

Теорема 2.2 Пусть X, Y, $Z \in \{0,1\}^s$ и $X \oplus Y = 2^{s-1}$, причём младший бит Z равен 1, тогда

$$(X \circledast Z) \oplus (Y \circledast Z) = 2^{s-1}.$$

Все теоретические результаты подтверждены экспериментально, далее они используются при анализе защищённости информации шифрами MARS и CAST-256 разностным методом.

В **§2.3** анализируется 32-раундовый шифр MARS, который имеет 256-битовый секретный ключ и состоит из *"пред-отбеливания"*, *"пост-отбеливания"*, 16 *core* раундов и 16 *mixing* раундов. Развёрнутый ключ шифра состоит из 40 ключей раундов и имеет длину 1248 бит. В диссертации предложена разностная характеристика для 8 backward core раундов, которая выглядит следующим образом:

$$\begin{aligned}(0,0,0,2^{18}) \xrightarrow{\text{"пред-отбел."} + 3 \text{ раунда}} (2^{18},0,0,0) \xrightarrow{1 \text{ раунд}} (2^9,?,?,2^{31}) \xrightarrow{1 \text{ раунд}} \\ (?,?,?,2^{22}) = (0,0,0,2^{22}) \xrightarrow{3 \text{ раунда}} (2^{22},0,0,0).\end{aligned} \tag{1}$$

Вероятность этой характеристики составляет 2^{-98}.

На основе предложенной характеристики разработана атака, направленная на нахождение ключей раундов у шифра MARS, состоящего из "пред-" и "пост-отбеливаний", 8 backward core раундов и 8 backward mixing раундов. Обозначим такой вариант шифра через MARS_{16} и заметим, что его развёрнутый ключ имеет длину 752 бита, в то время как наиболее эффективная из существующих атак направлена на вариант шифра MARS с развёрнутым ключом длиной 682 бита (см. табл. 1). Значит, предложенная атака является более эффективной, чем существующие. В данном случае эффективность атаки определяется не числом раундов шифра, а количеством вычисленных битов ключа, поскольку раунды шифра MARS не являются равноправными в том смысле, что mixing раунды не зависят от ключа.

Разработанная атака состоит из двух этапов: вычисление ключей "пост-отбеливания" и вычисление оставшихся ключей (для core-раундов и "пред-отбеливания"). Рассмотрим четыре 32-битовых ключа "пост-отбеливания" как один 128-битовый, тогда атака, направленная на его нахождение будет иметь следующий вид.

Шаг 1. Сформировать 6 групп, состоящих из 2^{101} различных пар блоков с разностью $(0,0,0,2^{18})$; обозначим эти пары блоков через $(A_t^g,\ B_t^g)$, где $g = \overline{1,6}$, $t = \overline{1,2^{101}}$.

Таблица 1: Лучшие атаки на шифр MARS

Биты ключей	Раунды			"Отбеливания"		Сложность			Источник
	Всего	Core	Mixing	Пред-	Пост-	Блоки	Память (в байтах)	Шифрования	
566	21	5	16	+	+	2^3	2^{236}	2^{232}	Д. Келси и др.
566	21	5	16	+	+	2^{50}	2^{197}	2^{247}	— | —
628	12	6	6	+	+	2^{69}	2^{73}	2^{197}	— | —
682	11	11	0	−	−	2^{65}	2^{69}	2^{229}	— | —
752	16	8	8	+	+	$2^{104,6}$	$2^{108,6}$	$2^{231,6}$	**§2.3**

Шаг 2. Для каждой пары $(A_t^g,\ B_t^g)$ запросить пару шифрованных блоков $X_t^g = \mathrm{MARS}_{16}(A_t^g)$ и $Y_t^g = \mathrm{MARS}_{16}(B_t^g)$; полученные $6 \cdot 2^{101}$ пар шифрованных блоков сохранить в памяти.

Шаг 3. Перебрать все возможные значения вычисляемого ключа (обозначим его через k), $k = \overline{0, 2^{128} - 1}$, и для каждого из возможных значений выполнить следующие действия:

(а) $g := 1$;

(б) сохранённые пары шифрованных блоков из группы g расшифровать на "пост-отбеливание" с ключом k и на 8 backward mixing раундов; обозначим полученные пары через P_t^g и Q_t^g;

(в) если $P_t^g \oplus Q_t^g \neq (0, 0, 0, 2^{22})$ для всех $t = \overline{1, 2^{101}}$, то k — ложный ключ-кандидат; отбросить его и перейти на шаг (3), где выбрать следующий ключ-кандидат;

если $P_t^g \oplus Q_t^g = (0, 0, 0, 2^{22})$ выполняется хотя бы для одной из пар, то перейти на шаг (г);

(г) если $g < 6$, то $g := g + 1$ и перейти на шаг (б); иначе k — это истинный ключ.

Для реализации разработанной атаки требуется $2^{104,6}$ выбранных открытых текстов, $2^{108,6}$ байт памяти и $2^{231,6}$ операций шифрования, что является быстрее полного опробования 256-битовых ключей. Вероятность успеха атаки (вероятность вычислить истинный ключ) составляет приблизительно 99%.

В **§2.4** исследована защищённость информации при использовании шифра CAST-256. Предложена следующая разностная характеристика для 18 раундов этого шифра:

$$(\beta, \alpha, 0, 0) \xrightarrow{\text{2 раунда}} (0, 0, \beta, \alpha) \xrightarrow{\text{1 раунд}} (\alpha, 0, 0, 0) \xrightarrow{\text{15 раундов}} (?, ?, ?, \alpha),$$

где $\alpha = 29_x^{\lll n}$, $\beta = 60A40_x$, индекс x означает запись числа в шестнадцатеричном виде, n выбрано случайно из множества $\{0,1,\ldots,31\}$, а $y^{\lll n}$ — циклический сдвиг влево величины y на n бит. Согласно полученной оценке вероятность этой характеристики составляет 2^{-17}.

На основе предложенной характеристики разработана атака на CAST-256, состоящий из 24-х раундов. Схема атаки аналогична схеме атаки на MARS. Вычислительная сложность атаки на CAST-256 составляет приблизительно $2^{25,2}$ выбранных открытых текстов, $2^{29,2}$ байт памяти и $2^{245,2}$ операций шифрования. Это меньше сложности полного опробования 256-битовых ключей. Вероятность успеха атаки приблизительно равна 99%.

На шифр CAST-256 опубликованы две атаки (см. табл. 2): первая вычисляет ключ шифра, состоящего из 16 раундов, а вторая — для шифра, имеющего до 36 раундов, но только для одного класса слабых ключей. В частности, к 24-раундовому CAST-256 атака применима только для 2^{-30} части всех

Таблица 2: Лучшие атаки на шифр CAST-256

Кол-во атакованных раундов	Сложность атаки			Число ключей	Источник
	Кол-во блоков	Память (в байтах)	Кол-во шифрований		
16	$2^{49,3}$	не указано	не указано	**Все**	Д. Вагнер
24	не указано	не указано	не указано	$\mathbf{2^{-25}}$ **часть**	Х. Секи и др.
36	2^{123}	не указано	2^{100}	$\mathbf{2^{-35}}$ **часть**	Х. Секи и др.
24	$2^{25,2}$	$2^{29,2}$	$2^{245,2}$	**Все**	**§2.4**

ключей. Разработанная в диссертации атака применима ко всем ключам, следовательно, она более эффективна для 24 раундов шифра CAST-256.

Проведена экспериментальная проверка предложенных характеристик и разработанных атак на MARS и CAST-256 посредством их моделирования на ЭВМ. В **§2.6** атака описана в общем виде, и рассчитана её сложность в зависимости от параметров шифра для достижения вероятности успеха 99%.

В **главе 3** теоретически и экспериментально обоснована эффективность статистического теста "стопка книг", а также исследованы зависимости статистических свойств шифров участников конкурса AES от числа раундов.

Пусть некоторый источник порождает буквы из алфавита $A = \{a_1, \ldots, a_S\}$, и дана выборка $X = (x_1, \ldots, x_N)$ из этого алфавита. Тест "стопка книг" является критерием согласия с гипотезой H_0 о том, что элементы выборки имеют равномерное распределение, т. е.

$$P(x_n = a_i) = 1/S,\ n = \overline{1, N},\ i = \overline{1, S}.$$

При использовании теста "стопка книг" в алфавите A фиксируется некоторый произвольный порядок, который меняется после анализа каждого выборочного элемента x_n следующим образом: буква $a_i = x_n$ получает первый номер, номера тех букв, которые были меньше её номера, инкрементируются, а у остальных букв номера сохраняются. Формально эта процедура выглядит так: пусть $\omega^n(a)$ — номер буквы a после анализа элементов x_1, x_2, ..., x_n, и начальный порядок $\omega^0(\cdot)$ на буквах A задан произвольно, тогда после анализа элемента x_{n+1} буквы получат следующие номера:

$$\omega^{n+1}(a) = \begin{cases} 1, & \text{если } a = x_{n+1}; \\ \omega^n(a) + 1, & \text{если } \omega^n(a) < \omega^n(x_{n+1}); \\ \omega^n(a), & \text{если } \omega^n(a) > \omega^n(x_{n+1}). \end{cases} \qquad (2)$$

Перед тестированием множество номеров $\{1, \ldots, S\}$ разбивается на $l > 1$ частей

$$A_1 = \{1,\ 2, \ldots,\ K_1\},\ A_2 = \{K_1 + 1,\ K_1 + 2, \ldots,\ K_2\},$$

$$\ldots$$

$$A_l = \{K_{l-1} + 1,\ K_{l-1} + 2, \ldots,\ K_l = S\}.$$

Для этих подмножеств по выборке $(x_1, x_2, \ldots, x_N)$ подсчитываются числа ν_j, $j = \overline{1,l}$, каждое из которых означает, сколько номеров $\omega^n(x_{n+1})$ принадлежит подмножеству A_j. Далее вычисляется статистика

$$x^2 = \sum_{j=1}^{l} \frac{(\nu_j - NP_j)^2}{NP_j}, \text{ где } P_j = |A_j|/S, \tag{3}$$

и тест записывается в следующем виде:

$$\pi = \begin{cases} H_0, & \text{если } x^2 < \chi_{l-1;\alpha}; \\ \neg H_0, & \text{иначе.} \end{cases} \tag{4}$$

В **§3.2** эффективность статистического теста "стопка книг" обоснована теоретически при $l = 2$, т. е. множество номеров букв разбивается на две части размеров K и $S - K$ соответственно.

Для упрощения выкладок сформируем начальный порядок номеров не произвольно, а специальным образом на основе *подготовительной* выборки. Такая модификация позволит упростить выкладки, не меняя их сути. Вначале зафиксируем произвольный порядок, а затем обработаем подготовительную выборку, состоящую из K элементов, переупорядочивая номера букв согласно правилам (2). Выборку, по которой производится подсчёт величины ν, назовём *контрольной*.

Рассмотрим некоторую перестановку индексов $\sigma(t)$, $t = \overline{1,S}$ и соответствующую ей простую гипотезу $H^{\gamma,\delta}_{\sigma(t)}$ с параметрами $\gamma \in (0, 1/2]$ и $\delta \in (0, 1)$; она заключается в том, что

$$p_i = \mathbf{P}(x_n = a_{\sigma(i)}) = \begin{cases} 1/S(1+\delta), & \text{если } i = 1, \ldots, \gamma S; \\ 1/S(1-\delta), & \text{если } i = \gamma S + 1, \ldots, 2\gamma S; \\ 1/S, & \text{если } i = 2\gamma S + 1, \ldots, S. \end{cases}$$

Подобные варианты альтернативной гипотезы приведены в ряде источников (Б. Я. Рябко и др., М. Кендалл и А. Стьюарт). Параметр γ определяет долю букв, вероятность которых отлична от $1/S$, а параметр δ — величину отклонения этой вероятности. Гипотеза говорит о том, что вероятности появления некоторых букв равны $1/S$, а остальные либо больше этого значения, либо меньше, причём на одинаковую величину и таких значений поровну.

Теперь определим сложную гипотезу $\mathcal{H}^{\gamma,\delta}$ как множество $\{H^{\gamma,\delta}_{\sigma(t)}\}$ со всевозможными перестановками (всего их $S!$). Эта гипотеза говорит о том, что параметры δ и γ известны, но неизвестно, каким буквам какие вероятности соответствуют. Вместо сложной гипотезы $\neg H_0$ возьмём её сужение $\mathcal{H}^{\gamma,\delta}$ и критерий (4) преобразуем к виду

$$\hat{\pi} = \begin{cases} H_0, & \text{если } x^2 < \chi_{1;1-\alpha}; \\ \mathcal{H}^{\gamma,\delta}, & \text{иначе.} \end{cases}$$

Основным теоретическим результатом является следующая

Теорема. Для любых α и β из интервала $(0,1)$ существует константа $\hat{C} = \hat{C}(\alpha,\beta;\gamma,\delta) > 0$ такая, что при $K = \sqrt{S}$ и при размере контрольной выборки $N = \hat{C} \cdot K$ ошибки первого и второго рода критерия $\hat{\pi}$ асимптотически при $S \to \infty$ не превосходят α^* и β соответственно, где $\alpha^* \approx \alpha$ с точностью, удовлетворительной для практических целей.

Таким образом, тест "стопка книг" в некотором смысле предлагает группировку для критерия хи-квадрат, которая позволяет (согласно доказанной теореме) в случае рассмотренной альтернативной гипотезы использовать для тестирования выборку размера $O(\sqrt{S})$.

В **§3.3** эффективность теста "стопка книг" обоснована экспериментально для класса мультипликативных линейных конгруэнтных генераторов (МЛКГ), которые успешно прошли спектральный тест (работа P. L'Ecuyer), являющийся одним из наиболее эффективных критериев и, как отмечает Д. Кнут, хорошо подходит для тестирования генераторов именно этого типа. МЛКГ генерирует псевдослучайные числа согласно следующей формуле:

$$x_{i+1} = a \cdot x_i \bmod m,$$

где x_0, a и m — целочисленные константы, являющиеся параметрами МЛКГ. МЛКГ предназначен для получения целых чисел, равномерно распределённых на множестве $\{0,\dots,m-1\}$. В ряде источников отмечается, что младшие знаки таких чисел могут иметь неудовлетворительные статистические свойства, поэтому существует рекомендация использовать только старшие знаки. Согласно этой рекомендации выделяется старший бит или старший байт; в дальнейшем эти режимы обозначены R_1 и R_8 соответственно.

При проведении экспериментов последовательность полученных таким образом псевдослучайных бит разбивалась на блоки длины s и при тестировании рассматривалась как выборка из алфавита размера 2^s. Множество номеров в "стопке книг" разбивалось на две или на три части. Каждый генератор тестировался в режиме R_1 при разных размерах выборок; если удавалось найти размер выборки, при котором тест "стопка книг" отличал генерируемые числа от равномерно распределённых, то все вычисления повторялись при этой длине по другим 100 ранее не задействованным выборкам. При этом вычислялись величины U_α, равные количеству тех выборок, на которых критерий (4) отвергал гипотезу H_0 при уровне значимости α. Если отклонения определить не удавалось, то вычисления повторялись в режиме R_8.

В табл. 3 отражены результаты экспериментов, где № — это номер генератора, R — режим тестирования, a и m — параметры генератора, s — длина блока, N — размер выборки в словах, $N \cdot s$ — размер выборки в битах, K и L — соответственно размеры частей A_1 и A_2.

Непосредственным вычислением установлено, что, если $U_{0,05} > 12$ или $U_{0,5} > 73$, то с вероятностью $99,9\%$ распределение элементов тестируемых

Таблица 3: Результаты тестирования линейных конгруэнтных генераторов

№	R	m	a	s	N	$N \cdot s$	K	L	$U_{0,5}$	$U_{0,05}$
1	1	$2^8 - 5$	33	8	70	560	2^3	2^5	72	0
2	1	$2^9 - 3$	35	8	70	560	2^3	2^5	100	0
3	1	$2^{10} - 3$	65	8	100	800	2^3	2^5	95	4
4	1	$2^{11} - 9$	995	8	500	4000	2^5	2^7	73	18
5	1	$2^{12} - 3$	209	8	200	1600	2^5	2^7	71	21
6	1	$2^{13} - 1$	884	8	1000	8000	2^5	2^7	71	13
7	1	$2^{14} - 3$	572	16	1500	12000	2^{10}	2^{11}	85	3
8	1	$2^{15} - 19$	219	16	2000	32000	2^{13}	2^{13}	80	26
9	1	$2^{16} - 15$	17364	16	2000	32000	2^9	2^{14}	71	9
10	1	$2^{17} - 1$	43165	16	4000	60000	2^{12}	2^{14}	72	21
11	1	$2^{18} - 5$	92717	16	4000	64000	2^{11}	2^{13}	70	9
12	1	$2^{19} - 1$	283741	24	25000	600000	2^{13}	-	80	18
13	1	$2^{20} - 3$	380985	24	30000	720000	2^{13}	-	71	23
14	1	$2^{21} - 9$	360889	24	200000	4800000	2^{17}	-	80	24
15	1	$2^{22} - 3$	914334	24	100000	2400000	2^{13}	-	79	14
16	1	$2^{23} - 15$	653276	24	150000	3600000	2^{13}	-	67	24
17	8	$2^{24} - 3$	6423135	24	25000	600000	2^{14}	-	90	30
18	8	$2^{25} - 39$	25907312	24	35000	840000	2^{14}	-	72	14
19	8	$2^{26} - 5$	26590841	24	45000	1080000	2^{14}	-	66	13
20	8	$2^{27} - 39$	45576512	24	80000	1520000	2^{15}	-	66	16
21	8	$2^{28} - 57$	246049789	24	200000	4800000	2^{17}	-	84	29
22	8	$2^{29} - 3$	520332806	24	300000	7200000	2^{17}	-	66	13

выборок не является равномерным. Табл. 3 показывает, что для всех генераторов найдены параметры, при которых одно из этих условий выполняется, следовательно, тест "стопка книг" определяет отклонения от равномерного распределения для рассмотренных генераторов, а спектральный тест — нет.

Корректность реализации теста "стопка книг" проведена посредством тестирования генераторов, классифицированных Д. Кнутом как "удовлетворительные", "находящиеся на грани" и "неудовлетворительные". Результаты их анализа тестом "стопка книг" согласуются с данной классификацией: "удовлетворительные" генераторы прошли тестирование успешно, а "находящиеся на грани" и "неудовлетворительные" — нет, причём у "неудовлетворительных" генераторов отклонения фиксировались на выборках меньшей длины, чем у "находящихся на грани".

В **§3.4** при помощи теста "стопка книг" проведён статистический анализ защищённости информации при использовании блочных шифров, заявленных на конкурс AES.

- Статистически исследована зависимость от числа раундов размера выборки, при котором псевдослучайные последовательности, генерируемые блочными шифрами, отличаются от равномерно распределённых случайных чисел.

- Определены минимальные значения числа раундов шифров, при которых обеспечиваются удовлетворительные статистические свойства этих последовательностей.
- Построен прогноз, распространяющий экспериментально найденные зависимости на большее число раундов, когда выборка становится настолько велика, что её невозможно обработать практически.

Опишем метод генерации псевдослучайных бит с помощью блочного шифра и схему экспериментов. Представим 128-битовый блок в виде четырех 32-битовых подблоков, занумерованных 0, 1, 2, 3 от старшего к младшему. Рассмотрим последовательность блоков $X_i^u, u \in \{0,1,2,3\}$, у которых подблок с номером u равен i, а остальные — нулевые, i пробегает значения $0,1,...,N-1$. Например, $X_7^0 = (7,0,0,0)$, а $X_5^3 = (0,0,0,5)$. Обозначим через $y_i^{u,v}$ 32-битовый подблок зашифрованного блока X_i^u с номером v. Например, зашифровав X_7^0, получаем блок $(y_7^{0,0}, y_7^{0,1}, y_7^{0,2}, y_7^{0,3})$. Любую часть такого блока можно взять в качестве псевдослучайного числа.

Экспериментальный анализ состоит из двух этапов: подбор подходящих параметров и тестирование. Цель первого этапа — определить параметры u, v, s, K и N, при которых тест "стопка книг" отличает генерируемую последовательность от последовательности равномерно распределенных случайных чисел. Здесь s — размер слова, K — размер верхней части "стопки книг", N — длина последовательности. На втором этапе с помощью 100 случайных ключей генерируются 100 последовательностей с выбранными на первом этапе параметрами. Для каждой из последовательностей вычисляются значения x^2 согласно формуле (3), и подсчитывается величина $U_{0,01}$, означающая, сколько раз из 100 значения x^2 превысили квантиль распределения хи-квадрат уровня 0,01. Если распределение шифртекста для всех 100 ключей является равномерным, то $U_{0,01}$ в среднем равно единице, и непосредственным вычислением показано, что, если $U_{0,01} > 4$, то с вероятностью более 99,9% распределение шифртекста — не равномерное.

Рассмотрим 32-раундовый шифр MARS, состоящий из 8 раундов четырёх типов: *forward core*, *backward core*, *forward mixing* и *backward mixing* раунды. При его анализе рассматриваются следующие варианты: раунды одного типа или одинаковое число раундов каждого типа. В табл. 4 показаны результаты экспериментов, откуда видно, что $U_{0,01}$ значительно больше 4, поэтому на основании приведённых выкладок можно сделать вывод о том, что распределение шифртекста не является равномерным с вероятностью более 99,9%.

Статистический анализ защищённости информации шифрами FROG и LOKI97 проведён по той же схеме. При использовании шифра FROG наибольшие отклонения от равномерного распределения достигаются при $u = 2$ и $v = 2$ (см. табл. 5), а при использовании шифра LOKI97 параметры u и v равны соответственно 1 и 2 для всех раундов кроме восьмого, а для него — $u = 0$ и $v = 3$ (см. табл. 6). Для этих двух шифров величина $U_{0,01}$ также

Таблица 4: Результаты статистического анализа шифра MARS

r	N	$U_{0,01}$	K	s	r	N	$U_{0,01}$	K	s
Forward mixing $u=3, v=2$					Backward mixing $u=3, v=1$				
2	$\mathbf{2^6}$	100	2^6	8	2	$\mathbf{2^6}$	100	2^6	8
4	$\mathbf{2^6}$	100	2^6	8	4	$\mathbf{2^6}$	100	2^6	8
6	$\mathbf{2^{14}}$	67	2^{14}	24	6	$\mathbf{2^8}$	99	2^6	8
8	$\mathbf{2^{18}}$	43	2^{18}	32	8	$\mathbf{2^{14}}$	25	2^{18}	24
Forward core $u=3, v=3$					Backward core $u=3, v=0$				
1	$\mathbf{2^6}$	100	2^6	8	1	$\mathbf{2^6}$	100	2^6	8
3	$\mathbf{2^6}$	100	2^6	8	3	$\mathbf{2^6}$	100	2^6	8
5	$\mathbf{2^{20}}$	17	2^{18}	32	5	$\mathbf{2^6}$	100	2^6	8
Всех раундов поровну $u=3, v=0$									
1+1+1+1	$\mathbf{2^6}$	100	2^6	8	2+2+2+2	$\mathbf{2^{18}}$	29	2^{18}	32

значительно превосходила 4. Результаты анализа защищённости при использовании остальных 12 участников конкурса AES приведены в табл. 7.

Таблица 5: Результаты статистического анализа шифра FROG

r	N	$U_{0,01}$	K	s	r	N	$U_{0,01}$	K	s
1	$\mathbf{2^9}$	100	2^8	16	3	$\mathbf{2^{22}}$	20	2^{18}	32
2	$\mathbf{2^{13}}$	22	2^{10}	16	4	$\mathbf{2^{32}}$	17	2^{20}	32

Таблица 6: Результаты статистического анализа шифра LOKI97

r	N	$U_{0,01}$	K	s	r	N	$U_{0,01}$	K	s
1	$\mathbf{2^3}$	100	2^3	6	5	$\mathbf{2^{18}}$	52	2^{16}	32
2	$\mathbf{2^5}$	100	2^3	6	6	$\mathbf{2^{19}}$	66	2^{16}	32
3	$\mathbf{2^8}$	100	2^6	8	7	$\mathbf{2^{27}}$	31	2^{18}	32
4	$\mathbf{2^{12}}$	100	2^{10}	16	8	$\mathbf{2^{31}}$	22	2^{20}	32

С увеличением числа раундов шифра улучшаются его статистические свойства, и повышается уровень защищённости информации при его использовании. Следовательно, растёт размер выборки, которая требуется тесту "стопка книг" для определения отклонений от равномерного распределения у последовательностей псевдослучайных чисел, генерируемых шифром. Значит, при некотором числе раундов размер выборки становится настолько большим, что обработать её экспериментально невозможно. Определить размер выборки, требуемой тесту "стопка книг" для определения отклонений от равномерного распределения при большем числе раундов, можно при помощи метода *наименьших квадратов*, который решает следующую задачу.

Даны точки $(r_1, r_2, \ldots, r_{R^*})$ и соответствующие им значения $(f_1, f_2, \ldots, f_{R^*})$. Требуется построить полиномиальную функцию вида

$$f(r) = b_0 + b_1 r + b_2 r^2 + \ldots + b_m r^m,$$

Таблица 7: Результаты статистического анализа шифров-кандидатов AES

Шифр	r	R	N	$U_{0,01}$	K	s	u	v
E2	3	12	$\mathbf{2^{20}}$	100	2^{18}	32	1	0
DFC	3	8	$\mathbf{2^{20}}$	100	2^{18}	32	0	1
CAST-256	2	12	$\mathbf{2^{18}}$	68	2^{18}	32	0	1
RIJNDAEL	2	10,12,14	$\mathbf{2^{18}}$	40	2^{18}	32	2	2
CRYPTON	3	12	$\mathbf{2^{5}}$	100	2^{5}	8	0	1
SERPENT	3	32	$\mathbf{2^{31}}$	31	2^{20}	32	0	3
SAFER+	2	8,12,16	$\mathbf{2^{30}}$	77	2^{20}	32	1	2
DEAL	2	6,8,8	$\mathbf{2^{6}}$	100	2^{5}	8	2	2
MAGENTA	2	6,6,8	$\mathbf{2^{6}}$	100	2^{5}	8	0	1
HPC	1	8	$\mathbf{2^{10}}$	100	2^{10}	16	2	2
RC6	4	20	$\mathbf{2^{27}}$	47	2^{20}	32	0	2
TWOFISH	3	16	$\mathbf{2^{20}}$	52	2^{18}	32	2	0

где коэффициенты b_r минимизируют среднеквадратичное отклонение функции f от этих точек. Рассмотрим, как вычисляются коэффициенты для случая многочлена второй степени, который понадобится в дальнейшем. Пусть искомая функция имеет вид

$$f(r) = b_0 + b_1 r + b_2 r^2.$$

При вычислении неизвестных коэффициентов b_0, b_1 и b_2 методом наименьших квадратов решается система так называемых *нормальных уравнений*:

$$\begin{cases} \sum\limits_{i=0}^{R^*} f_i = b_0(R^*+1) + b_1 \sum\limits_{i=0}^{R^*} r_i + b_2 \sum\limits_{i=0}^{R^*} r_i^2, \\ \sum\limits_{i=0}^{R^*} f_i r_i = b_0 \sum\limits_{i=0}^{R^*} r_i + b_1 \sum\limits_{i=0}^{R^*} r_i^2 + b_2 \sum\limits_{i=0}^{R^*} r_i^3, \\ \sum\limits_{i=0}^{R^*} f_i r_i^2 = b_0 \sum\limits_{i=0}^{R^*} r_i^2 + b_1 \sum\limits_{i=0}^{R^*} r_i^3 + b_2 \sum\limits_{i=0}^{R^*} r_i^4. \end{cases}$$

Система линейна относительно искомых коэффициентов, поэтому может быть решена методом Гаусса.

Для шифров LOKI97 и FROG зависимость величины $log_2 N$ от числа раундов, приведённая в табл. 6, почти линейная, поэтому её разумно приблизить квадратичной функцией

$$log_2 \tilde{N}(r) = b_2 r^2 + b_1 r + b_0$$

и с помощью метода наименьших квадратов найти коэффициенты b_0, b_1 и b_2. Для шифра FROG указанная зависимость имеет вид

$$log_2 \tilde{N}(r) = 0{,}5r^2 + 5{,}7r + 0{,}8,$$

а для шифра LOKI97 — $log_2\tilde{N}(r) = 0{,}2r^2 + 2{,}5r - 0{,}3$.

В табл. 8 и 9 показаны численные значения полученных функций.

Таблица 8: Прогноз для шифра FROG

	Эксперименты					Прогноз			
r_i	0	1	2	3	4	5	6	7	8
N_i	2^0	2^9	2^{13}	2^{22}	2^{32}	2^{42}	2^{53}	2^{65}	2^{78}

Таблица 9: Прогноз для шифра LOKI97

	Эксперименты									Прогноз			
r_i	0	1	2	3	4	5	6	7	8	10	12	14	16
N_i	2^0	2^3	2^5	2^8	2^{12}	2^{18}	2^{19}	2^{27}	2^{31}	2^{43}	2^{56}	2^{70}	2^{86}

В **§3.5** описан программный комплекс для статистического оценивания защищённости информации при использовании итеративных блочных шифров "СКАБШ-2012", включающий программу, моделирующую атаки на MARS и CAST-256; тест "стопка книг" и его применение к анализу защищённости информации блочными шифрами; метод наименьших квадратов; расчёт сложности разностной атаки в зависимости от параметров шифра. Исходный код программного комплекса приведён в приложении. В **заключении** сформулированы результаты диссертационной работы.

1. Формализованы основные понятия разностного метода анализа итеративных блочных шифров, и систематизированы связи между ними.
2. Теоретически определено влияние (найдена зависимость) веса Хэмминга разности двух величин на вероятность её сохранения после арифметических операций по модулю 2^s.
3. Методом разностного анализа проведена оценка защищённости информации при использовании блочных шифров MARS и CAST-256. Предложены разностные характеристики, позволившие разработать атаки на эти шифры, являющиеся эффективнее существующих.
4. Теоретически и экспериментально обоснована эффективность статистического теста "стопка книг" для одного класса альтернативных гипотез и одного класса генераторов псевдослучайных чисел.
5. Статистически исследована защищённость информации, обеспечиваемая итеративными блочными шифрами кандидатами конкурса AES. Определены зависимости их статистических свойств от числа раундов. Для каждого шифра найдено минимальное число раундов, при котором он обладает удовлетворительными статистическими свойствами.

6. Разработан программный комплекс "СКАБШ-2012", предназначенный для статистического оценивания защищённости информации при использовании итеративных блочных шифров, включающий в себя следующие основные части: моделирование атак на шифры MARS и CAST-256, расчёт характеристик S-блоков шифра MARS, реализацию статистического теста "стопка книг" и его применение к статистическому анализу итеративных блочных шифров.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

В журналах, рекомендованных ВАК:

[1] *Пестунов А. И.* О вероятности протяжки однобитовой разности через сложение и вычитание по модулю // Прикладная дискретная математика. — 2012. — № 4. — С. 53–60.

[2] *Пестунов А. И.* Дифференциальный криптоанализ блочного шифра CAST-256 // Безопасность информационных технологий. — 2009. — № 4. — С. 57–62.

[3] *Пестунов А. И.* Дифференциальный криптоанализ блочного шифра MARS // Прикладная дискретная математика. — 2009. — № 4 (6). — С. 56–63.

[4] *Пестунов А. И.* Статистический анализ современных блочных шифров // Вычислительные технологии. — 2007. — Т. 12, № 2. — С. 122–129.

[5] *Пестунов А. И.* Блочные шифры и их криптоанализ // Вычислительные технологии. — 2007. — Т. 12, спец. вып. № 4. — С. 42–49.

[6] *Пестунов А. И.* Теоретические исследования статистического теста "Стопка книг" // Вычислительные технологии. — 2006. — Т. 11, № 6. — С. 96–103.

[7] *Рябко Б. Я., Пестунов А. И.* "Стопка книг" как новый статистический тест для случайных чисел // Проблемы передачи информации. — 2004. — Т. 40, № 1. — С. 73–78.

В трудах международных конференций:

[8] *Pestunov A.* Differential cryptanalysis of 24-round CAST-256 // Proc. IEEE Region 8 International Conf. on Computational Technologies in Electrical and Electronic Engineering (Sibircon-2008). — Novosibirsk. — 2008. — P. 46–49.

[9] *Pestunov A.* Differential Cryptanalysis of Reduced-Round MARS // Proc. XI International Symposium on Problems of Redundancy in Information and Control Systems. — Saint Petersburg. — 2007. — P. 197–201.

[10] *Пестунов А. И.* Асимптотические свойства статистического теста "Стопка книг" // Тр. междунар. конф. "Вычислительные и информационные технологии в науке, технике и образовании". — Павлодар. — 2006. — Т. 2. — С. 110–117.

[11] *Пестунов А. И.* Статистический анализ блочного шифра MARS // Тр. междунар. конф. "Вычисл. и информационные технологии в науке, технике и образовании". — Павлодар. — 2006. — Т. 2. — С. 118–123.

В тезисах конференций:

[12] *Пестунов А. И.* Оценки сложности дифференциальной атаки при различных параметрах блочного шифра // Тез. докл. IX сибирской науч. школы-семинара с междунар. участием "Компьютерная безопасность и криптография" (Sibecrypt-10). — Тюмень: ТюмГУ. — 2010. — С. 25–27.

[13] *Пестунов А. И.* Новые статистические атаки на блочные и потоковые шифры // Тез. докл. междунар. школы-конф. по приоритетным направлениям развития науки и техники с участием молодых ученых, аспирантов и студентов. — Москва: РГУИТП. — 2006. — С. 58–60.

[14] *Пестунов А. И.* Градиентная статистическая атака на блочный шифр FEAL // Тез. докл. VII всеросс. конф. молодых ученых по матем. моделированию и информ. технологиям. — Красноярск: ИВМ СО РАН. — 2006. — С. 91–92.

СВИДЕТЕЛЬСТВО О РЕГИСТРАЦИИ ПРОГРАММЫ ДЛЯ ЭВМ

[15] *Пестунов А. И.* Программный комплекс для статистического оценивания защищённости информации при использовании итеративных блочных шифров "СКАБШ-2012" // Свид. о гос. регистрации программы для ЭВМ. — Федеральная служба по интеллектуальной собственности, патентам и товарным знакам. — 12.02.2013.

Подписано в печать 17.05.2013 г.
Формат 60x84 1/16. Гарнитура Times.
Тираж 100 экз. Усл. печ. л. 1,25.

Новосибирский государственный университет
экономики и управления "НИНХ"
630099, г. Новосибирск, ул. Каменская, 56