УДК 681.3.06:519.248.681

М.Н. САВЧУК

О РАБОТАХ КИЕВСКОЙ ШКОЛЫ ТЕОРЕТИЧЕСКОЙ КРИПТОГРАФИИ

Ключевые слова: *криптография, криптоанализ, вероятностная комбинаторика, вероятности на алгебраических структурах, случайные размещения, статистические критерии, оценки сложности криптоалгоритмов, асимптотический анализ.*

ВВЕДЕНИЕ

В системах защиты информации существенная роль отведена криптографическим механизмам. Президент НАН Украины академик Б.Е. Патон и академик В.М. Глушков, возглавлявший Институт кибернетики АН УССР, осознавали необходимость развития криптологических исследований еще в начале 70-х годов прошлого века.

К концу 40-х годов прошлого века в Советском Союзе главное внимание уделяли созданию сугубо технических средств шифрования. На рубеже 40-50-х годов стало ясно, что без серьезного математического обоснования надежная защита государственных тайн невозможна. Тогда для усовершенствования криптографической службы привлекли группу ведущих математиков. Организатором и научным руководителем службы был Владимир Яковлевич Козлов — выдающийся математик, впоследствии член-корреспондент РАН, академик Академии криптографии России.

По инициативе В.Я. Козлова в 1973 г. в Институте кибернетики АН УССР было создано научно-исследовательское подразделение для проведения криптологических исследований. С начала его создания этим подразделением руководил академик И.Н. Коваленко (с середины 80-х годов вместе с А.М. Фалем). Подразделение занималось решением математических задач, обусловленных запросами криптографии. Задачи формулировались ведущими специалистами криптографической службы, которые работали в Москве. Подразделение успешно работало до 1992 года.

В независимой Украине в Институте кибернетики продолжали вестись активные исследования в области криптографии. Полученные результаты, а также исследования по теории надежности были высоко оценены. В 2001 году научному коллективу, основу которого составляли специалисты Института кибернетики, присуждена Государственная премия в области науки и техники за цикл работ по безопасности и надежности информационных технологий. Кроме того, Государственные премии в области науки и техники в 2004 г. и 2009 г. присуждены научным коллективам, в состав которых вошли специалисты в области криптографии и стеганографии.

Большую поддержку криптологическим исследованиям в учреждениях НАН Украины оказывает директор Института кибернетики имени В.М. Глушкова, академик НАНУ И.В. Сергиенко. По его инициативе в 2001 г. было проведено заседание Президиума НАН Украины, посвященное проблемам защиты информации и развития криптологических исследований, на котором с докладом выступил И.Н. Коваленко.

На созданном в 2000 г. факультете информационной безопасности Физико-технического института НТУУ «КПИ» была создана кафедра математических методов защиты информации, которую возглавил ученик академика И.Н. Коваленко доктор физико-математических наук М.Н. Савчук. К преподаванию на кафедре специальных дисциплин привлечены как бывшие, так и нынешние сотрудники Института кибернетики.

На базе этой кафедры согласно постановлению Президиума НАН Украины был создан в 2001 г. регулярно действующий научный семинар «Проблемы современной криптологии». Тематика докладов, которые заслушиваются на семинаре, является весьма разносторонней и охватывает различные аспекты как синтеза, так и анализа криптографических систем защиты информации, математические задачи теоретической криптографии. Отметим некоторые из них.

– Построение алгебраических моделей симметричных криптосистем.

– Анализ криптостойкости алгоритмов шифрования.

– Исследование задач вероятностной комбинаторики и их применение в криптографии.

– Теория инвариантности и методы решения систем линейных уравнений над конечными полями, кольцами.

– Методы решения систем линейных булевых уравнений с искажениями, а также систем случайных псевдобулевих уравнений.

– Методы решения систем нелинейных булевых уравнений.

– Спектральные методы в стеганографии.

– Схемы защиты информации в динамических средах.

– Алгоритмы реализации операций в группе точек эллиптической кривой.

– Сравнительный анализ стандартов цифровой подписи Украины и России, основанных на эллиптических кривых.

– Вероятностные методы тестирования неприводимости полиномов.

– Исследование методов тестирования генераторов случайных последовательностей.

– Схемы разделения секретов.

– Методы распределения ключей.

– Создание программно-аппаратных комплексов арифметики многократной точности и их применение в криптографии.

– Алгебраические атаки на потоковые шифры.

– Критерии выбора и алгоритм генерирования долгосрочных ключей для ГОСТ 28147-89.

– Предложения по созданию новых блочных симметричных алгоритмов шифрования с целью их внедрения в Украине.

– Эффективные алгоритмы квантовых вычислений и их применение в криптографии.

– Исследование новых методов построения односторонних функций.

(Список докладов семинара «Проблемы современной криптологии», заслушанных и обсужденных с 2001 г. по 2009 г., приведен в конце статьи.)

Одним из важнейших направлений, связанных с математическими задачами криптографической защиты информации, является вероятностно-комбинаторный подход с применением методов абстрактной алгебры, теории сложности и асимптотического анализа. Использование хорошо разработанных аналитических методов, предельных теорем теории вероятностей дает возможность лучше исследовать динамику развития сложных систем как в практическом, так и в теоретическом отношении. Вероятностный подход к комбинаторным проблемам в теоретико-множественной постановке позволяет достичь большей ясности и рассматривать много различных классов задач с единой точки зрения и решать едиными методами. Среди разнообразных областей вероятностной комбинаторики выделим несколько направлений.

– Вероятности на алгебраических структурах. Теория инвариантности.

– Теория кодирования.

– Случайные размещения и их применения в криптологии.

– Случайные отражения, подстановки и графы.

– Порядковые статистики, экстремальные значения, оптимизация.

– Комбинаторные методы в теории случайных процессов.

– Статистические критерии и их применения в криптологии.

– Алгебраические и комбинаторные модели симметричных криптосистем.

– Комбинаторно-вероятностные алгоритмы и их применения в криптологии.

– Статистические и алгебраические методы в криптоанализе.

– Алгебраическо-вероятностные подходы в анализе асимметричных криптосистем.

– Классические и постквантовые модели вычислений.

По этим направлениям проводились исследования специалистами различных математических школ, в том числе специалистами киевской школы теоретической криптографии. Приведем краткий обзор некоторых работ этой школы (в основном за последние 10–20 лет).

Алгоритмы декодирования искаженных линейных кодов над полем $GF(2)$. Известно, что декодирование линейных кодов общего вида является *NP*-полной задачей. Поиск алгоритмов декодирования, которые имеют сравнительно с методом максимума правдоподобия меньшую сложность и эффективны в практическом применении, представляет значительный интерес особенно для методов защиты информации и криптоанализа. Наибольший интерес в криптоанализе представляют случаи сильно искаженных линейных кодов большой длины, когда вероятность безошибочной передачи символа близка к 1/2. Эти алгоритмы в другой интерпретации используются также для решения систем линейных уравнений с искаженной правой частью в полях Галуа. Эффективные методы решения систем линейных уравнений с искаженными правыми частями над конечными полями, кольцами, группами — это мощный аппарат в криптоанализе. Предложенный в работе [1] алгоритм значительно уменьшает объем вычислений по декодированию и решению систем линейных уравнений и является новым шагом в этой области. Основной результат работы [1] заключается в следующем.

Пусть линейный код над полем $CF(2)$ задается образующей матрицей $A = (a_{ij})$, $i = \overline{1, N}$, $j = \overline{1, n}$, с помощью которой информационное слово $\bar{x} = (x_1, x_2, \ldots, x_n)$ кодируется в кодовое слово $\bar{y} = (y_1, \ldots, y_N)$. Это кодовое слово передается по двоичному симметричному каналу с вероятностью безошибочной передачи i-го символа p_i. При определенных асимптотических при $n \to \infty$ условиях на распределение (не обязательно независимых) элементов случайной матрицы A, на вероятность безошибочной передачи p_i и число уравнений существует алгоритм декодирования, имеющий асимптотически среднюю сложность $L \le \exp\{Cn(1+\varepsilon)\log^{-1} n\}$, $C = \text{const} > 0$. Алгоритм основан на поэтапном суммировании строк подматриц, образованных после разбиения расширенной матрицы $\bar{A}$ (с добавлением к матрице A принятого слова в качестве $(n+1)$-го столбца), последующей сортировки каждой полученной таким образом матрицы, новым суммированием и повторением этой процедуры до получения ряда уравнений с одним неизвестным. Специальным образом подобранные параметры на каждом этапе алгоритма позволили снизить сложность декодирования до субэкспоненциальной.

Алгоритмы декодирования искаженных линейных кодов, основанных на сортировке и суммировании строк образующей матрицы, предложены в работах [2, 3]. Строятся алгоритмы декодирования этого линейного кода, которые по принятому слову $\bar{y} = (y_1, \ldots, y_{N_0})$ и заранее неизвестной образующей матрицы восстанавливают информационное слово $\bar{x} = (x_1, x_2, \ldots, x_n)$ и базируются на суммировании строк расширенной матрицы $\bar{A}$, сформированной добавлением к образующей матрице принятого слова, как последнего столбца.

Описанные алгоритмы применяются для декодирования серии линейных кодов M над $GF(2)$ с одной образующей матрицей для всех кодов серии и различными информационными словами, которые преобразуются в кодовые слова и передаются по двоичному симметричному каналу без памяти с вероятностью безошибочной передачи p_i^l, $l = \overline{1, M}$, $i = \overline{1, N_0}$, зависящей от номеров кода и символа.

Для данных методов проводится асимптотический анализ, отыскиваются асимптотические оценки сложности алгоритмов при независимых в совокупности элементах образующей матрицы, когда $\mathbf{P}\{a_{ij} = 1\} = 1 - \mathbf{P}\{a_{ij} = 0\} = \rho \le 1/2$, $i = \overline{1, N_0}$, $j = \overline{1, n}$, и сильных искажениях: при $N_0, n \to \infty$, $p_i \to 1/2$, $p_i^l \to 1/2$, $i = \overline{1, N_0}$, $l = \overline{1, M}$. Описанные алгоритмы особенно эффективны при разряженных образующих матрицах и недостаточной для других методов размерности кодового слова.

Приведенные алгоритмы можно применять для оценки криптографической устойчивости систем защиты информации, при их взломе с помощью криптографического анализа, а также при исследовании свойств и параметров случайных систем уравнений с искажениями над конечными алгебраическими структурами (группами, кольцами, полями Галуа) и разработки методов их решения.

Экспериментальные исследования алгоритмов декодирования. В работе [4] рассматриваются два метода декодирования описанных выше ли-

нейных кодов: метод максимального правдоподобия и метод Монте-Карло. Алгоритм максимального правдоподобия заключается в переборе всех 2^n информационных слов $X^{(k)}$, $k = \overline{1, 2^n}$, для каждого из которых находим расстояние Хемминга $\rho_k = |AX^{(k)} - \tilde{Y}|$, $k = \overline{1, 2^n}$, между кодовым $AX^{(k)}$ и принятым $\tilde{Y}$ словами. Слово, которое отвечает минимальному значению ρ_k, и является искомым. Если же минимум достигнут на нескольких векторах, то однозначное восстановление информационного слова при заданной вероятности ошибки и длине кода N невозможно.

Метод Монте-Карло декодирования кода заключается в поиске случайным образом неискаженной системы n уравнений от n переменных среди уравнений, определяющих код, в решении этой системы в случае, если определитель системы не равен нулю, и проверке полученного решения X^* на случайно выбранной (N', n)-подматрице A^* с соответствующими символами принятого слова $\tilde{Y}^*$. Если расстояние Хемминга $\rho^* = |A^* X^* - \tilde{Y}^*|$ не превышает некоторого заданного порога C, то X^* считаем декодированным информационным словом. В случаях, когда определитель равен нулю или $\rho^* > C$, переходим к поиску новой системы с n уравнениями.

В [4] приведены результаты экспериментального исследования двух указанных алгоритмов при конечных значениях параметров n, N и Δ, дано сравнение этих алгоритмов по надежности и трудоемкости, а также сравнение полученных экспериментально характеристик с асимптотическими теоретическими значениями.

Системы линейных уравнений с искаженной правой частью над кольцами. В работах А.Н. Алексейчука и С. М. Игнатенко [5–7] изучаются системы линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. Такие системы уравнений являются классическим объектом исследований в криптографии и, как правило, используются при построении корреляционных атак на симметричные криптосистемы (генераторы псевдослучайных последовательностей, блочные и потоковые шифры). В связи с развитием методов синтеза и распространением сферы применения недвоичных программно-ориентированных поточных шифров в настоящее время наблюдается повышенный интерес специалистов к системам уравнений с искаженной правой частью над конечными кольцами и полями мощности $q > 2$.

В статьях [5, 6] получены аналитические оценки надежности восстановления истинного решения системы линейных уравнений с искаженной правой частью над кольцом $Z/(2N)$ методом максимума правдоподобия, предложены модификации этого метода, которые имеют меньшую временную сложность по сравнению с классическим вариантом его применения. В работе [7] предложен метод построения новых алгоритмов решения указанных систем уравнений по произвольной конечной совокупности таких исходных алгоритмов. Приведены аналитические выражения надежности и временной сложности алгоритмов, полученные данным методом, через соответствующие характеристики исходных алгоритмов и описана процедура построения оптимальных (по критерию минимума трудоемкости при заданной нижней границе надежности) в определенном классе алгоритмов решения уравнений с искаженной правой частью над кольцом $Z/(2N)$.

Исследования булевых матриц и систем линейных уравнений над конечными полями и кольцами. В работе И.Н. Коваленко [8] доказываются теоремы инвариантности для случайного булевого определителя, изучаются задачи о ранге случайной матрицы, о распределении ранга линий случайной матрицы с учетом скорости сходимости к предельным величинам. А.А. Левитская в [8] исследует системы линейных уравнений над конечными кольцами. Ряд результатов в теории инвариантности получены в работах В.И. Масола. Обзор работ по исследованию систем случайных уравнений над конечными алгебраическими структурами до 2004 г. приведен в [12].

В работе А.Н. Алексейчука [9] с использованием метода решетчатых моментов (см. ниже) показано, что предельное (при $n \to \infty$, $s = \text{const}$) распределение числа решений системы линейных уравнений $Ax = 0$ над кольцом вычетов по модулю p^d (p — простое, d — натуральное), где A — случайная равновероятная матрица размера $(n + s) \times n$, тогда и только тогда определяется однозначно последовательностью своих моментов, когда $d \le 2$.

В статье [10] приведены результаты исследований распределения ранга $(n+s)\times n$-матрицы A с независимыми в совокупности строками над полем из q элементов. В терминах коэффициентов Фурье распределений строк этой матрицы получены верхние и (в случае, когда коэффициенты Фурье — неотрицательные числа) нижние оценки вероятностей значений ее ранга. Получена также верхняя граница расстояния по вариации между распределениями рангов матрицы A и рангов случайной равновероятной матрицы. Сформулировано условие, согласно которому это расстояние по вариации стремится к нулю при $n\to\infty$, $s=\text{const}$, и показано, что это условие в некотором естественном смысле не может быть ослаблено. Статья [10] отличается от предыдущих работ по данной тематике большей общностью постановки задачи и новым методом исследования, связанным с коэффициентами Фурье, а полученные в ней оценки в ряде случаев являются более точными по сравнению с известными оценкам Г.В. Балакина [11].

В обзоре [12] приведены также результаты по исследованию матриц и их рангов, определителей, методов решения систем линейных уравнений над конечными алгебраическими структурами

Исследование логических, нелинейных уравнений, а также уравнений над группами. В работе [8] вводятся системы случайных логических уравнений и исследуется вероятность совместимости, а также вероятность единственности решения нелинейных систем случайных уравнений. Для систем линейных уравнений в конечной абелевой группе находятся оценки среднего числа решений, распределение числа решений для примарной группы, исследуются случаи циклической группы. Результаты имеют асимптотический характер. Доказанные теоремы можно считать открытием нового направления исследований в дискретной математике. Нелинейные уравнения над конечными полями рассматривались в работах Масола В.И. и его учеников. Теоремы инвариантности для систем случайных нелинейных уравнений над произвольным конечным кольцом с левой единицей доказывались в работе [74].

Вероятностные распределения на решетке. Проблема моментов. В работах А.Н. Алексейчука [13, 14] приведены результаты исследований общей схемы независимых случайных элементов, принимающих значения в конечной решетке. Показано, что в терминах этой схемы возможно общее формулирование ряда вероятностно-комбинаторных задач (о распределении вероятностей числа непокрытых точек в обобщенной схеме размещения частиц комплектами, числа компонент связности случайного гиперграфа, числа решений системы случайных линейных уравнений над конечным кольцом с единицей и т.п.). Предложен также метод доказательства теорем о сходимости последовательностей случайных величин ξ_n, принимающих значения в множестве (0, 1, ..., n), к дискретным распределениям вероятностей. Метод основан на исследовании асимптотического поведения определенных числовых характеристик (решетчатых моментов) распределений ξ_n. Рассмотрены примеры использования этого метода в исследованиях асимптотического поведения распределений вероятностей размерности пространства решений системы независимых случайных однородных линейных уравнений над конечным полем, а также числа компонент связности неравновероятного случайного гиперграфа с независимыми гиперребрами. В статье [15] приведены результаты, которые развивают и дополняют ряд утверждений, полученных в [13, 14]. В частности, введено понятие индекса покрытия конечной однородной решетки ранга n и доказана теорема об асимптотической нормальности числа блоков в случайном равновероятном покрытии этой решетки. С помощью метода решетчатых моментов в [14] найден вид предельного при $n\to\infty$ закона распределения индекса покрытия решетки подпространства n-мерного векторного пространства над конечным полем.

Заметим, что метод решетчатых моментов разработан в процессе исследований, направленных на поиск общих достаточных условий однозначности проблемы моментов в классе q-распределений — дискретных распределений вероятностей, которые сосредоточены на множестве степеней числа $q>1$ с неотрицательными целыми показателями [16]. Примером q-распределения является предельное при $n\to\infty$ распределение вероятностей числа решений системы, которая состоит из $n+s$ случайных однородных линейных уравнений от n неизвестных, над полем из q элементов (s — целочисленная константа). Долгое время оставался открытым вопрос: определяется ли указан-

ное распределение однозначно последовательностью своих моментов? Положительный ответ на него дан в статье [16], где получены также достаточные условия однозначности проблемы моментов для распределений вероятностей, сосредоточенных на множестве векторов $(q_1^{n(1)},\ldots,q_t^{n(t)})$, $q_i>1$, $n(i)\in N_0$, $i=1,2$.

Исследование методов подсчета числа полных отображений конечных множеств. Разработанные в работах [17–19] методы оценки числа так называемых полных отображений являются значительным продвижением в решении задачи, которая на протяжении почти трех десятилетий стояла перед специалистами в области прикладной математики и криптографических методов защиты информации. Предложен новый эффективный подход [20] к оценке числа полных отображений методом ускоренного моделирования, который позволил оценить количество полных отображений для $N=205$ с относительной погрешностью 5%. Приведены также эмпирические верхние и нижние оценки их количества. Эта проблема мотивирована задачами защиты информации. При дешифровке (взломе) таких систем шифрования как, например, «Энигма» большую роль играют полные отображения (перестановки без «параллельности» — без «особых» совпадений).

Задача о распределении идентификационных кодов. Предположим, что некоторое количество пользователей выбирают для себя (независимо один от другого) адрес или код. Возникает вопрос: с какой вероятностью несколько пользователей будут иметь одинаковый адрес? Исследование этого вопроса о коллизиях проводится в работе [21]. Оценки такой вероятности имеют важное значение для правильного построения надежных процедур доступа в автоматизированных и компьютерных системах. Сейчас при бурном развитии телекоммуникаций, глобальных компьютерных сетей, систем электронных платежей вопрос о распределении кодов приобретает особую актуальность. Неулучшаемые асимптотические оценки для минимального числа пользователей, при котором вероятность коллизии не меньше заданной, получены в работе [76].

Вероятностные методы генерации неприводимых полиномов. В работе [22] проводится обобщение вероятностных тестов определения простоты целого числа для проверки полиномов над полями Галуа на неприводимость. Обобщаются тесты Ферма, Соловея–Штрассена, Миллера–Рабина, указываются области, в которых разработанные методы генерации неприводимых полиномов более эффективны, чем детерминированные методы.

ТЕОРИЯ СЛУЧАЙНЫХ РАЗМЕЩЕНИЙ

Большой класс комбинаторных задач в зависимости от приложений, характеристик, которые изучаются, традиций, математических школ и ряда других причин может формулироваться и изучаться в различных математических терминологиях, интерпретироваться с помощью различных комбинаторных конфигураций и схем. Важнейшими такими комбинаторными конфигурациями являются размещения частиц по ячейкам, выборки или урновые схемы, отображения конечных множеств и графы.

В зависимости от того, рассматриваем ли мы частицы или ячейки как упорядоченные или неупорядоченные, как различающиеся или не различающиеся между собой, исходя из ограничений на размещение, будем получать различные схемы размещения. Соответственно разным будет и количество всех возможных размещений. Например, если ячейки различаются и не упорядочены, а частицы не различаются, то число возможных размещений будет C^n_{N+n-1}, где N — число ячеек, n — число частиц. Это соответствует коммутативному несимметричному N-базису в терминах отображений, а также статистике Бозе — Эйнштейна в статистической физике. На множестве всех возможных размещений заданной комбинаторной схемы можно задавать различные вероятностные распределения и таким образом получить большое разнообразие случайных схем размещения частиц, каждая из которых, как правило, имеет ряд приложений к прикладным задачам в вычислительной технике, в математических методах защиты информации, в области физики, биологии и т.д. Выводы и результаты, полученные для схем размещений, используются для изучения ряда дискретных моделей и вероятностно-комбинаторных алгорит-

мов, применяемых при синтезе и анализе систем криптографической защиты информации, в различных методах криптоанализа и т.д.

Схема случайного размещения комплектов частиц по ячейкам. В ячейках размещается n комплектов частиц по m частиц, в каждом комплекте частицы размещаются в ячейках не более чем по одной и все C_N^m возможных размещений равновероятны, а размещения частиц в различных комплектах независимы. (Если $m=1$, то имеем классическую схему размещения.) Обозначим $\mu_r(N,m,n)$ случайную величину, равную числу ячеек, которые содержат ровно r частиц после размещения всех n комплектов; $\xi_r(N,m,n)$ — случайная величина, равная числу ячеек, которые содержат не более чем r частиц каждая после размещения n комплектов; $\nu_r(N,m,k)$ — случайная величина, равная наименьшему числу размещенных комплектов, при котором в некоторых k ячейках содержится не менее чем по r частиц.

По схемам размещения частиц комплектами в работах [8, 23] проведены исследования смешанных факториальных и вторых моментов, а также распределений случайных величин и случайных векторов, связанных с величинами $\mu_r(N,m,n)$, $\xi_r(N,m,n)$, $\nu_r(N,m,k)$. Получено нормальное приближение для многомерного гипергеометрического распределения со случайными параметрами. Доказаны теоремы о предельных гауссовских, пуассоновских распределениях, а также экспоненциальных, дважды экспоненциальных предельных распределениях для времени ожидания. В работе [25] приведен набор предельных теорем для времени ожидания до заполнения заданных подмножеств ячеек в задаче о размещении частиц комплектами. В работе [27] обобщаются асимптотические результаты для максимальной и минимальной частот в классической схеме размещения на случай схемы размещения случайного числа частиц.

В работе [8] с помощью комбинаторного анализа рядов получены точные формулы для моментов произвольного порядка максимума двух и трех независимых гауссовских случайных величин, а также для центральных моментов этих величин.

Размещения комплектов частиц на окружности. В работах [8, 23] определяется и изучается схема размещения комплектов частиц на окружности. В отличие от классической схемы размещения здесь вводятся случайные величины, связанные с характеристиками пересечения комплектов. С помощью теории рядов, производящих функций и комбинаторно-вероятностного анализа исследуется предельное поведение моментов и распределения случайных величин, доказывается сходимость распределений к гауссовским, а также к композиции пуассоновских распределений. Приведенная схема размещения используется при анализе датчиков псевдослучайных последовательностей, которые, как известно, имеют определенный период.

Слабая сходимость векторных случайных процессов в схемах размещения к гауссовским диффузионным процессам. В работах [8, 23] разработан метод доказательства слабой сходимости векторных случайных процессов, построенных по схемам размещения в пространстве функций без разрывов второго рода. Метод основан на применении общих предельных теорем теории случайных процессов. В работах [8, 23, 28] разработанным методом доказана сходимость векторных случайных процессов с двумя типами направленности времени, построенных по различным схемам размещения, к гауссовским диффузионным процессам. Получены следствия из функциональных предельных теорем, относящиеся к асимптотическому поведению совместного распределения случайных величин, что дает еще один способ доказательства многомерных гауссовских предельных теорем в схемах размещения.

Неравновероятные схемы. Разделимые статистики. Регулярная схема независимого размещения n частиц в N пронумерованных ячейках описывается следующим образом: каждая частица независимо от других с вероятностью q_k попадает в ячейку с номером k, $k=\overline{1,N}$, $\sum_{k=1}^{N} q_k = 1$; при $N\to\infty$, $c_1, c_2 = \text{const}$, $0<c_1<c_2$ выполняются неравенства $0<c_1 \le \min\limits_k Nq_k \le \max\limits_k Nq_k \le c_2 < \infty$. В статье [28] предложенным в работах [8, 23] методом доказана слабая сходимость многомерных случайных процессов, построенных в регулярной схеме по разделимым статисти-

кам в пространстве функций без разрывов 2-го рода к векторному гауссовскому диффузионному процессу. В [24] слабая сходимость рассмотрена в схеме размещения частиц комплектами со случайными уровнями (заданными на ячейках другой схемой размещения).

Вариационные ряды вероятностей. Если при реализации полиномиальной схемы рассматривать только случаи появления m попарно различных исходов (векторов $(i_1, \dots, i_m)$), то для произвольного фиксированного γ, $0 < \gamma < 1$, можно определить величину $N(\gamma)$ как наименьшее возможное число векторов такое, что сумма их вероятностей будет не менше γ. Функция $N(\gamma)$ зависит от γ, N, m и вероятностей p_i полиномиальной схемы, $i = 1, \dots, N$. Такая модель используется, например, при генерации случайных выборок без повторения, случайных размещений комплектов частиц по ячейкам, при построении случайных функций, некоторых схем коммутации, генераторов случайных чисел и т.д. В работе [26] исследованы некоторые неравновероятные варианты этой схемы.

КОМБИНАТОРНО-ВЕРОЯТНОСТНЫЕ АЛГОРИТМЫ ОПРЕДЕЛЕНИЯ СВОЙСТВ (0,1)-ПОСЛЕДОВАТЕЛЬНОСТЕЙ И БУЛЕВЫХ ФУНКЦИЙ

Исследование случайных и псевдослучайных последовательностей. Определение статистических, криптографических характеристик случайных и псевдослучайных последовательностей, а также генераторов таких последовательностей — одна из важнейших задач в построении и применении криптографических средств и методов защиты информации. В работе [29] построены статистические алгоритмы определения моментов переключения некоторого альтернирующего случайного процесса. В работе [30] рассматривается последовательность бернуллиевских случайных величин u_t, $t = \overline{1,N}$, таких, что $\mathbf{P}(u_t = 0) = \frac{1}{2}(1 + \Delta_t)$, $|\Delta_t| < 1$, $t = \overline{1,N}$, и исследуется построенная с помощью u_t последовательность булевых случайных величин $v_t = u_t \oplus u_{t - l_1(t)} \oplus \dots \oplus u_{t - l_{m_t}(t)} \oplus \varphi(t)$, $t = \overline{1,N}$, где $\varphi(t)$ — неслучайная функция от t со значениями в $\{0,1\}$, $1 \le l_1(t) < l_2(t) < \dots \dots < l_{m_t}(t) \le t - 1$.

В работе [31] предложен новый статистический критерий проверки качества случайных и псевдослучайных последовательностей. Одним из наиболее эффективных алгоритмов сжатия является метод контекстного моделирования. Этот метод сжатия информации можно применить для проверки последовательности на случайность. Суть алгоритма заключается в том, что, просматривая последовательность слева направо, можно делать определенные прогнозы относительно следующих символов. Количеством правильных прогнозов определяются вероятностные характеристики алгоритма. Теоретический и экспериментальный анализ варианта такого алгоритма приведен в [67].

Многомерные статистические критерии проверки качества случайных и псевдослучайных последовательностей, построенные на основе предельных теорем о слабой сходимости векторных случайных процессов в схемах размещения, исследуются в работе [68].

О независимости статистических тестов. В работе [32] разработана адекватная математическая модель, сформулировано и обосновано определение попарной независимости и независимости в совокупности статистических тестов, предназначенных для проверки качества генераторов случайных, псевдослучайных и отдельных последовательностей, а также блока генерации гаммы потокового шифра; приведена методика проверки независимости статистических тестов и методика формирования набора таких тестов.

В работе [33] рассматриваются вопросы генерации ключевых параметров с неравновероятным распределением.

Статистическое определение свойств булевых функций. В работе [34] предлагаются методы статистического определения специальных криптографических свойств многомерных булевых функций. С помощью таких функций может описываться функционирование узлов дискретных устройств, конечных автоматов, криптографических преобразований и т.д. Например, блочный шифратор в режиме электронной кодовой книги реализует такие многомерные булевы функции.

При программной или аппаратной реализации сложных булевых функций от многих переменных возникает проблема проверки правильности реализации, т. е. тождества булевого преобразования некоторой эталонной булевой функции. Осуществить такую проверку при большом числе переменных перебором по всем возможными входам — проблематично даже для современной вычислительной техники. В [34] предлагаются и обосновываются вероятностные тесты, устанавливающие методом Монте-Карло тождественность или неодинаковость векторнозначных булевых функций многих переменных с параметрами и заданными доверительной вероятностью α и максимальным риском β.

НОВЫЕ МЕТОДЫ В КРИПТОАНАЛИЗЕ

Криптоанализ потоковых шифраторов. Несколько лет назад появился новый метод криптоанализа, суть которого заключается в упрощении специальным образом и последующем решении системы уравнений, которая описывает функционирование шифратора (биты ключа являются неизвестными переменными системы). Этот метод назван алгебраическими атаками.

Первые существенные результаты в криптоанализе реальных шифраторов с помощью алгебраических атак были достигнуты в 2002 году. Куртуа Н. предложил «корреляционную атаку высокого порядка» на потоковый шифратор «Toyocrypt» (предложенный на конкурс шифраторов «Cryptrec»). Новая улучшенная алгебраическая атака дала новую систему уравнений для «Toyocrypt» со сложностью решения 2^{49} операций. Позднее этот подход был усовершенствован и «быстрая алгебраическая атака» дала возможность восстанавливать ключ этого шифратора за 2^{20} операций (при наличии около 300 Кб непрерывной гаммы и этапе предварительного подсчета с 2^{23} операцями). Впоследствии была исследована результативная алгебраическая атака на блочные шифраторы.

В работах [35, 36] предложено описание алгебраической атаки на потоковые шифраторы с помощью условной корреляции. Это позволило обобщить понятие нелинейности k-го порядка булевой функции, которое используется, в частности, в корреляционных атаках высокого порядка. Приведен пример фильтрующей функции, которая сильно уязвима к корреляционной атаке высокого порядка с использованием введенной «частичной нелинейности», но слабо уязвима к атаке такого же типа с использованием обычной нелинейности k-го порядка. Также разработан эффективный алгоритм (и написана соответствующая программа) проверки булевой функции $f(\bar{x})$ на наличие аппроксимаций k-й степени, которые сильно коррелируют с f в терминах условной корреляции. В случае существования хороших аппроксимаций алгоритм находит лучшую из них. Для криптоанализа применялись также методы решения систем линейных уравнений с искаженными правыми частями над конечными полями.

В работе [36] исследовались алгебраические атаки на потоковые шифраторы. Были введены понятия условной корреляции и частичной нелинейности булевых функций, а также расширены понятия алгебраического иммунитета. Это позволило унифицировать описание детерминированных и вероятностных сценариев алгебраических атак (отметим, что вероятностные сценарии исследовались впервые). Дан простой критерий уязвимости функции к вероятностному сценарию атаки в терминах условной корреляции. Конструктивно построено определенное множество функций, уязвимых к вероятностному сценарию атаки, и на их примере показано, что для некоторых функций осложнения такой сценарий атаки является наиболее эффективным.

В работе [37] экспериментально найден ключ потокового шифратора «SFINKS» с ослабленной фильтрующей функцией с помощью вероятностной алгебраической атаки. Класс таких уязвимых функций достаточно широкий и содержит много функций, стойких относительно известных неалгебраических методов криптоанализа. В работе [38] вводятся новые теоретические понятия для булевых функций: корреляция при известном значении функции и расширение булевой функции. Доказано, что алгебраическая атака на потоковые шифраторы без памяти сводится к аппроксимации усложняющих функций шифратора низкостепенными полиномами в терминах введенной корреляции. Эта корреляция может быть использована и для описания алгебраических атак на другие типы шифраторов.

В [39] получены оценки мощности классов булевых функций от n переменных с алгебраическим иммунитетом не выше k. Результаты являются полезными при исследовании алгебраических атак на потоковые шифраторы. Суть алгебраических атак на потоковые шифры состоит в понижении определенным методом степени системы уравнений, связывающих биты неизвестного ключа с известными выходными битами шифра. Вероятностные сценарии атаки предполагают еще большее понижение степени, но при этом полученные уравнения истинны уже не на всех аргументах. В работе [40] исследованы такие сценарии и введены соответствующие понятия, в терминах которых легко описывается стойкость усложняющей булевой функции потокового шифра против такого вида атак.

Развитию теории статистических методов криптоанализа поточных шифров посвящены работы [41–44], в которых предложена и подробно исследована вероятностная модель функционирования в режиме реинициализации начального состояния комбинирующих генераторов гаммы с неравномерным движением регистров сдвига. Показано, что стойкость таких генераторов относительно ряда статистических атак определяется набором условных вероятностей, для которых получены явные аналитические выражения [42, 44]. Эти выражения позволяют установить тесную связь между двумя, на первый взгляд, различными криптоаналитическими задачами: восстановлением значений комбинирующей функции генератора гаммы с неравномерным движением и восстановлением сообщений, искаженных при передаче по дискретному каналу связи с отводом [45–47]. Наличие такой связи дает возможность распространить на рассматриваемый класс генераторов гаммы известные результаты, полученные ранее для систем со случайным кодированием, в частности получить общее достаточное условие оптимальности (по критерию минимума надежности восстановления значений) комбинирующей функции генератора гаммы с неравномерным движением регистров сдвига [41, 44].

Некоторые современные методы криптоанализа поточных шифров изучались также в работе [48].

Исследования блочных шифраторов. Новые подходы к криптоанализу блочных шифров и их устойчивости относительно линейного и дифференциального анализа исследуются в работах А.Н. Алексейчука, Л.В. Ковальчук. В частности, предложено понятие «немарковского» шифра, при использовании которого более адекватно описываются некоторые типы шифров. Разработке методов обоснования практической стойкости немарковских блочных шифров относительно разностного (дифференциального) и линейного криптоанализа посвящены публикации [49–54]. В статье [49] получены аналитические верхние границы максимумов вероятностей дифференциальных и линейных характеристик шифра Фейстеля, содержащего ключевой сумматор по модулю 2^m (примером такого шифра является стандарт ГОСТ 28147–89). Выражения для верхних границ содержат новые числовые параметры узлов замены данного шифра, которые отличаются от классических параметров, традиционно используемых для оценки практической стойкости марковских блочных шифров относительно методов разностного и линейного криптоанализа. В [50, 51] получены аналитические верхние оценки вероятностей дифференциальных аппроксимаций преобразований вида $(x,k)\mapsto\varphi(x+k)$, $x, k\in\{0,1\}^m$, где φ — подстановка на множестве $\{0, 1\}^m$, а знак + означает операцию сложения целых чисел, соответствующих двоичным векторам, по модулю 2^m. Указанные оценки построены при различных вариантах задания групповых операций на области определения и области значений изучаемых преобразований. Дальнейшие уточнения этих оценок для широкого класса так называемых обобщенных марковских шифров получены Л.В. Ковальчук [53]. Наиболее точные на данный момент верхние границы параметров, характеризующих практическую устойчивость ГОСТ-подобных блочных шифров относительно методов разностного и линейного криптоанализа, опубликованы в статье [54]. Эти границы дают возможность оценить сверху максимальные значения вероятностей дифференциальных и линейных характеристик шифра ГОСТ 28147–89 (при определенных, не слишком жестких ограничениях на выбор его узлов замены) числами 2^{-56} и 2^{-42} соответственно.

Методы, развитые в [49–54], успешно применены в работе [55] к исследованию стойкости еще одного важного класса блочных шифров, построенных с использованием ключевого сумматора по модулю 2^m, — шифру «Калина», который является кандидатом на Национальный стандарт шифрования Украины, и его аналогам. В частности, полученные в [55] оценки вероятностей дифференциальных и линейных характеристик шифра «Калина» позволяют без каких-либо упрощающих предположений обосновать его практическую стойкость относительно методов разностного и линейного криптоанализа.

В статье А.Н. Алексейчука и А.С. Шевцова [56] получены новые верхние границы надежности статистических атак первого порядка на произвольные блочные шифры. Эти границы позволяют ввести обоснованные показатели стойкости блочных шифров относительно широкого класса атак (линейных, обобщенных линейных, билинейных и др.), не прибегая к традиционным эвристическим предположениям. При этом в случае линейной различающей атаки новая оценка стойкости [56] является на один-два порядка точнее ранее известной оценки [57].

Дифференциальный анализ стандарта ГОСТ 28147-89 проводился также в работе [58].

В работах С.В. Яковлева [59, 60] приведены результаты исследования важной части стандарта ГОСТ 28147–89 — так называемых S-блоков, которые представляют собой долгосрочный секретный ключ. Были сформулированы критерии отбора подстановок в S-блоках, которые гарантируют, с одной стороны, высокую надежность, а с другой — большую мощность ключевого пространства, построены алгоритмы генерации долгосрочных ключей, исследованы S-блоки на устойчивость к атакам линеаризации, корреляционного, линейного, дифференциального анализа, а также к дифференциальным атакам по питанию и по времени. Заметим, что утвержденные алгоритмы генерации долгосрочных ключей стандарта ГОСТ 28147–89 ни в России, ни в Украине не были опубликованы.

В статье [61] предложена и проанализирована новая конструкция блочных шифров — каскадная схема Фейстеля, получены оценки дифференциальных и линейных характеристик такой схемы. Яковлевым С.В. проведен сравнительный анализ дизайна шифра «Калина» и шифров AES и W. Исследовано соответствие шифра «Калина» требованиям к кандидатам на замену национального стандарта шифрования.

Криптоанализ алгоритмов шифрования, основанных на детерминированном хаосе. В последнее время делаются попытки возможного использования в криптографии новых результатов из различных научных направлений. Одним из таких направлений является теория детерминированного хаоса.

В работах [62–64] проанализированы криптосистема с открытым ключом на основе кусочно-линейного отображения, применяемого в хаотической динамике, а также модификация криптосистемы, в которой используется удаление младших разрядов изображения числа с плавающей запятой в двоичной форме (стандарт IEEE 754). На основании результатов исследования функциональности системы и свойств использованного отображения $T_k(x) = \frac{1}{\pi}\arccos(\cos(k\pi x))$ показана возможность проведения успешной и эффективной бесключевой атаки. Представлен алгоритм восстановления сообщения без знания секретных ключей, а также указаны основные недостатки, которые приводят к взлому системы.

Локально-коммутативные симметричные шифры в асимметричной криптографии и их стойкость в постквантовой модели вычислений. В работах [65, 66] предложено использовать коммутативные и локально-коммутативные симметричные шифры, стойкие к атакам на основе открытого текста, для построения односторонних функций и асимметричных криптосхем. С учетом свойств таких шифров были построены аналоги большинства известных асимметричных протоколов (Диффи–Хеллмана, Эль–Гамаля, Шнора и др.). Проанализирована стойкость таких функций в классической модели вычислений и доказана их постквантовая уязвимость сведением задачи обращения такой функции к частному случаю задачи о скрытой подгруппе, когда существует решение в рамках квантовой модели вычислений.

Исследование и разработка криптографических стандартов. В Институте кибернетики НАНУ в течение ряда лет проводились исследования по гармонизации

европейских криптографических стандартов с целью использования их в Украине в условиях украинской нормативной базы, технических и организационных возможностей. В соответствии с планами государственной стандартизации Украины в 2004-2009 гг. по договорам между Украинским научно-исследовательским институтом стандартизации, сертификации и информатики, Государственным комитетом по вопросам технического регулирования и потребительской политики Украины и Техническим комитетом по стандартизации «Информационные технологии» (ТК-20) с участием специалистов Анисимова А.В., Фаля А.М, Ткаченко В.В. и других были разработаны и гармонизированы восемь стандартов ISO/IEC с целью их принятия в Украине [69–71]. В Институте кибернетики НАНУ продолжаются работы по исследованию и гармонизации других стандартов ISO/IEC, исследовались и разрабатывались алгоритмы цифровой подписи [72]. А.И. Кочубинским и А.С. Шаталовым разработан национальный стандарт цифровой подписи на эллиптических кривых [73].

Научный семинар «Проблемы современной криптологии». Объем настоящей статьи не позволяет перечислить все работы по теоретической криптографии, которые за последние двадцать лет выполнялись даже только специалистами киевской криптографической школы. Хотелось отметить работы Анисимова А.В., Задираки В.К., Мухачева В.А., Кочубинского А.И., Кудина А.М. и многих других. В этом номере журнала опубликованы последние статьи Алексейчука А.Н., Ендовицкого П.А., Левитской А.А. по теоретической криптографии [75–77]. Определенное представление о разнообразии направлений исследований могут дать названия приведенных ниже докладов на киевском научном семинаре «Проблемы современной криптологии» за последние девять лет (к сожалению, названия некоторых докладов не удалось восстановить).

30.11.2001. ***Алексейчук А.Н., Романов О.И.*** (Киев) «Регулярные конгруенции и строение алгебраических моделей симметричных криптосистем».

13.12.2001. ***Олейников Р.В.*** (Харьков) «Анализ устойчивости и условий применения ГОСТ-28147-89»; ***Головашич С.А.*** (Харьков) «Методы построения высокостойких симметричных шифров и схем их применения».

27.12.2001. ***Алексейчук А.Н.*** (Киев) «Решеточные» моменты целочисленных неотрицательных случайных величин и их применение при решении задач вероятностной комбинаторики».

17.01.2002. ***Телиженко А.Б.*** (Киев) «Алгоритмы случайного поиска и их применение в криптографии».

31.01.2002. ***Савчук М.Н.*** (Киев) «Об алгоритмах решения систем линейных уравнений с искажениями».

14.02.2002. ***Романович К.А.*** *(*Киев) «Методы решения случайных систем псевдобулевых уравнений».

28.02.2002. ***Фаль А.М.*** (Киев) «Сравнительный обзор международных стандартов криптографии».

14.03.2002. ***Кочубинский А.И.*** (Киев) «Сравнение стандартов Украины и России на эллиптических кривых».

28.03.2002. ***Олейников Р.В.*** (Харьков) «Дифференциальный криптоанализ стандарта шифрования ГОСТ-28147-89».

11.04.2002. ***Левитская А.А.*** *(*Киев) «Теоремы инвариантности для случайных нелинейных систем булевых уравнений».

25.04.2002. ***Будько Н.Н., Василенко В.С., Короленко М.П.*** *(*Киев) «Контроль и восстановление целостности информации в автоматизированных системах».

26.09.2002. ***Коваленко И.Н.*** *(Киев)* «Воспоминания о киевской и московской математической и кибернетической школах. Взгляд на современное состояние и перспективы в некоторых направлениях».

10.10.2002. ***Ковальчук Л.В.*** (Киев) «Псевдонесводимые полиномы. Вероятностное тестирование неприводимости полиномов» Ч. I.

24.10.2002. ***Коваленко И.Н.*** (Киев) «Некоторые задачи вероятностной комбинаторики».

07.11.2002. ***Кудин А.М.*** (Киев) «Оценка стойкости криптосистем с использованием чебышевского радиуса информации».

21.11.2002. ***Булыгин С.В.*** (Киев) «Об оценке одной криптографической функции с использованием техники алгебро-геометрических кодов».

05.12.2002. ***Уфимцева В.Б.*** *(*Харьков) «Применение Q-матриц Фибоначчи в схемах обмена сети Фейстеля».

19.12.2002. ***Задирака В.К.*** (Киев) «Спектральные методы в стеганографии».

16.01.2003. ***Задирака В.К., Бородавка Н.В.*** (Киев) «О программной реализации спектрального алгоритма построения цифрового контейнера».

30.01.2003. ***Лебедев Е.А.*** (Киев) «Алгоритмы расчета основных распределений прикладной статистики».

13.02.2003. ***Бессалов А.В.*** (Киев) «Применение эллиптических кривых в криптографии. Стандарты цифровой подписи на эллиптических кривых».

13.03.2003. ***Завадская Л.А., Меллит А.С.*** (Киев) «О криптоанализе потоковых схем шифрования».

27.03.2003. ***Турбин А.Ф., Великий А.П.*** (Киев) «О преобразовании Лобанова».

10.04.2003. ***Глазунов Н.М.*** (Киев) «Алгебраические кривые и криптография».

24.04.2003. ***Меллит А. С.*** (Киев) «О реализации алгоритма Сата для расчета порядка точек эллиптической кривой»; ***Торба С.Н.*** (Киев) «Эффективное экспоненцирование точек эллиптической кривой с операцией деления точки на два».

19.10.2003. ***Алексейчук А.Н.*** (Киев) «Анализ устойчивости рандомизированных блочных шифраторов к методу разностного криптоанализа».

23.10.2003. ***Ковальчук Л.В.*** (Киев) «Вероятностное тестирование неприводимости полиномов» Ч. II.

06.11.2003. ***Масол В.И.*** (Киев) «Асимптотика распределений некоторых характеристик случайных матриц над конечным полем».

20.11.2003. ***Алексейчук А.Н.*** (Киев) «Случайные покрытия однородной конечной решетки».

04.12.2003. ***Кохановский А.И.*** (Киев) «Проблемные вопросы защиты информации в системах электронного документооборота».

15.01.2004. ***Бородавка Н.В.*** (Киев) «Стеганограммы на базе теоремы о свертке».

29.01.2004. ***Бределев Б. А.*** (Киев) «Стеганографические системы в рамках моделей пассивного и активного противника».

12.02.2004. ***Зубенко А.*** (Киев) «Схемы защиты информации в динамических средах».

26.02.2004. ***Конюшок С.Н.*** (Киев) «Построение схем распределения ключей, имеющих теоретическую стойкость, основанную на комбинаторных конфигурациях».

11.03.2004. ***Кудин А.М., Довыдьков А.А.*** (Киев) «Построение комплексных систем защиты для распределенных автоматизированных систем с архитектурой, которая динамично меняется».

25.03.2004. ***Савчук М.Н.*** (Киев) «О криптографических свойствах булевых функций».

22.04.2004. ***Довыдьков А.А.*** (Киев) «Подходы к моделированию политик безопасности компьютерных систем».

30.09.2004. ***Коваленко И.Н.*** (Киев) «Опыт работы в области прикладной теории вероятностей и математической статистики».

14.10.2004. ***Алексейчук А.Н.*** (Киев) «Статистический метод криптоанализа генераторов гаммы, построенных на линейных регистрах с неравномерным движением».

28.10.2004. ***Ковальчук Л.В.*** (Киев) «Применение метода Полларда для нахождения коллизий хэш-функций».

11.11.2004. ***Бессалов А.В.*** (Киев) «Метод деления точек на 2 в применении к криптографии на эллиптических кривых».

25.11.2004. ***Ковальчук Л.В***. (Киев), ***Бездетный В.Т.*** (Киев) «Методика проверки "независимости" тестов для тестирования генераторов псевдослучайных последовательностей».

23.12.2004. ***Волошин А.Л.*** (Киев) «Линейная схема распределения секрета над кольцом вычетов по примарному модулю».

20.01.2005. ***Алексейчук А.Н.*** (Киев) «Универсальные алгебры и схемы распределения секретов».

03.02.2005. ***Устименко В.А.*** (Киев) «Прогулки на графах и криптография».

17.02.2005. ***Задирака В.К.*** (Киев), ***Кудин А.М.*** (Киев) «Программно-аппаратный комплекс арифметики многократной точности».

03.03.2005. ***Алексейчук А.Н.*** (Киев), ***Игнатенко С.М.*** (Киев) «Системы линейных уравнений с искаженными правыми частями над кольцом остатков по модулю 2^n».

17.03.2005. ***Кинах И.Я.*** (Тернополь) «Модель параллельной реализации общего сита числового поля»; ***Карпинский Б.З.*** (Тернополь) «Высокопроизводительные поточные шифры повышенной устойчивости к атакам».

31.03.2005. ***Пометун С.А.*** (Киев) «Алгебраические атаки на поточные шифры»; ***Кудин А.М.*** (Киев) «Об одном подходе к аппаратной реализации алгоритмов многословной арифметики» Ч. I.

14.04.2005. ***Кудин А.М.*** (Киев) «Об одном подходе к аппаратной реализации алгоритмов многословной арифметики» Ч. 2.

29.09.2005. ***Коваленко И.Н.*** (Киев) «О работе Международной конференции «Современные проблемы и новые направления в теории вероятностей» и секции «Вероятностные и статистические методы в криптографии» (в Черновцах); ***Задирака В.К.*** (Киев) «Сообщение о 32-й конференции по оптимизации вычислений, посвященной В.С. Михалевичу (в Кацивели)»; ***Анисимов А.В.*** (Киев) «О работе в области математических методов защиты информации на факультете кибернетики Киевского национального университета имени Тараса Шевченко».

13.10.2005. ***Алексейчук А.Н., Ковальчук Л.В.*** (Киев) «Верхние границы максимальных значений вероятностей дифференциальных и линейных характеристик шифратора Фейстелевского типа, содержащего сумматор по модулю 2^n».

27.10.2005. ***Гомонай Е.В., Фесенко А.В.*** (Киев) «Эффективные алгоритмы квантовых вычислений и их применение в криптографии».

10.11.2005. ***Завадский И.А.*** (Киев) «Поисковый алгоритм Гровера».

24.11.2005. ***Поляков А.А.*** (Харьков) «Генерирование системных параметров эллиптических кривых».

08.12.2005. ***Фесенко А.В.*** (Киев) «Квантовый алгоритм Шора факторизации целых чисел».

22.12.2005. ***Балагура Д.С.*** (Киев) «Анализ, сравнение и улучшение криптографических протоколов установки ключей для использования в ИВК».

02.03.2006. ***Яковлев С.В.*** (Киев) «Критерии отбора и алгоритм генерирования долгосрочных ключей ГОСТ 28147-89».

16.03.2006. ***Бределев Б.А.*** (Киев) «Стеганографический алгоритм, устойчивый к ряду статистических атак».

30.03.2006. ***Белецкий А.Я.*** (Киев) «Семейство симметричных блоковых криптографических алгоритмов защиты информации».

13.04.2006. ***Пометун С.А.*** (Киев) «Построение алгебраических атак с использованием условной корреляции».

27.04.2006. ***Белецкий А.Я.*** (Киев) «Обобщенные коды Грея и их использование в схемах защиты информации».

11.05.2006. ***Антонов А.В.*** (Харьков) «Криптографические функции с секретом на основе информационной меры сложности обращения хаотических отображений».

02.11.2006. ***Ковальчук Л.В.*** (Киев) «Обобщенные марковские шифры: оценка стойкости к дифференциальному криптоанализу».

16.11.2006. ***Алексейчук А.Н., Проскуровский Р.В.*** (Киев) «Статистическая атака на комбинированные генераторы гаммы с неравномерным движением в режиме реинициализации начального состояния».

30.11.2006. ***Белецкий А.Я.*** (Киев) «RSB технология построения симметричных блоковых криптографических алгоритмов».

14.12.2006. ***Федюкович В.Е.*** (Киев) «Частичное совпадение множеств без разглашения».

15.02.2007. ***Федюкович В.Е.*** (Киев) «Методика демонстрации частичного совпадения множеств».

01.03.2007. ***Фаль А.М.*** (Киев) «Обзор международных стандартов по безопасности информационных технологий».

15.03.2007. ***Горбенко И.Д., Долгов В.И., Олейников Р.В.*** (Харьков) «Принципы построения и спецификации блокового шифратора «Калина», представленного на конкурс».

29.03.2007. ***Кошкина Н.В.*** (Киев) «Методы синхронизации цифровых водяных знаков».

12.04.2007. ***Кузнецов Н.Ю.*** (Киев) «Использование ускоренного моделирования для определения количества «хороших» перестановок».

26.04.2007. ***Фесенко А.В.*** (Киев) «Криптоанализ систем шифрования, построенных на основе динамического хаоса».

11.10.2007. ***Пометун С.А.*** (Киев) «Обобщенная корреляция и нелинейность высокого порядка в алгебраических атаках на потоковые шифраторы».

25.10.2007. ***Задирака В.К., Кудин А.М., Людвиченко В.А.*** (Киев) «Компьютерные технологии криптографической защиты информации на специальных носителях».

08.11.2007. ***Ковальчук Л.В.*** (Киев) «Методы анализа и синтеза существующих и перспективных байт-ориентированных потоковых криптосистем для защиты государственных информационных ресурсов».

22.11.2007. ***Поперешняк С.В.*** (Киев) «Распределение рангов слабо- и сильнозаполненных случайных матриц в поле $GF(2)$»; ***Слободян Н.В.*** (Киев) «Аппроксимация распределения числа ложных решений системы нелинейных случайных уравнений в поле $GF(2)$ распределением Пуассона».

06.12.2007. ***Борисенко А.А.*** (Сумы) «Анализ криптографической стойкости источников дискретной информации».

20.12.2007. ***Ковалёв А.М., Козловский В.А., Савченко А.Я., Щербак В.Ф.*** (Донецк, Киев) «Новые методы и алгоритмы преобразования информации на основе автоматоподобных и хаотических динамических систем для цифровой обработки, кодирования, сохранения и эффективной защиты информации».

14.02.2008. ***Устименко В.А.*** (Киев, Донецк) «Экстремальная теория графов и ее криптографические приложения».

28.02.2008. ***Алексейчук А.Н., Ковальчук Л.В., Шевцов А.С.*** (Киев) «Обобщенные Марковские шифры «Калина» и «Мухомор»: оценка практической стойкости к дифференциальному и линейному криптоанализу».

13.03.2008. ***Слободян С.А.*** (Ивано-Франковск) «Теоремы о нормальном предельном распределении числа ложных решений системы нелинейных случайных уравнений в поле $GF(2)$».

27.03.2008. ***Завадская Л.А.*** (Киев) «О криптоанализе потокового шифра *RC*-4».

10.04.2008. ***Фесенко А.В.*** (Киев) «Атаки компромиса на потоковые криптосистемы»; ***Яковлев С.В.*** (Киев) «Атаки по побочным каналам на потоковые шифраторы».

24.04.2008. ***Шарапов В.Г., Федюкович В.Е.*** (Киев) «Интерактивный протокол демонстрации кратного вхождения строки».

25.09.2008. ***Пометун С.А.*** (Киев) «Алгоритмы вероятностных алгебраических атак на потоковые шифры».

09.10.2008. ***Савчук М.Н., Фесенко А.В.*** (Киев) «Исследование односторонних функций, построенных на симметричных шифрах».

23.10.2008. ***Черняхович К., Яремчук Ю.*** (Винница) «Методы цифровой подписи на эллиптических кривых с ускоренной процедурой проверки цифровой подписи».

06.10.2008. ***Алексейчук А.Н.*** (Киев) «Теоретические основы синтеза и обоснования стойкости рандомизированных симметричных систем шифрования и протоколов передачи и распределения ключей».

20.11.2008. ***Яковлев С.В.*** (Киев) «Построение коллизий для хеш-функции стандарта ГОСТ Р 34.311-95».

04.12.2008. ***Федюкович В.Е.*** (Киев) «Протоколы доказательства и аргумента: элементарное введение и примеры решаемых задач».

18.12.2008. ***Мороховец М.К.*** (Киев) «Диагностические эксперименты с конечными автоматами».

12.03.2009. ***Пометун С.А.*** (Киев) «Алгоритмы решения систем нелинейных уравнений со слабоискаженными правыми частями».

26.03.2009. ***Федюкович В.Е.*** (Киев) «Алгебраические операции над шифротекстом системы Paillier'a и протокол доказательства знания открытого текста (по материалам работ Paillier (Eurocrypt 1999), Paillier-Pointcheval (Asiacrypt 1999), Damgard-Jurik (PKC 2001))».

09.04.2009. ***Ендовицкий П.А.*** (Киев) «О методе голосования в решении систем уравнений».

23.04.2009. ***Никитенко Л.Л.*** (Киев) «Исследование критерия стойкости стеганосистем при пассивных атаках».

15.10.2009. ***Кудин А.М.*** (Киев) «Криптографические преобразования нешенноновских источников информации».

29.10.2009. ***Ромашова Л.А.*** (Киев) «О вероятности существования решений системы нелинейных случайных уравнений над полем $GF(3)$ в заданном множестве».

26.11.2009. ***Глинчук Л.Я.*** (Луцк) «Криптосистема Штерна-Броко и ее применение».

10.12.2009. ***Яковлев С.В.*** (Киев) «Каскадные схемы Фейстеля и оценка их стойкости».

24.12.2009. ***Ендовицкий П.А.*** (Киев) «Уточнение асимптотической аппроксимации размера группы в парадоксе дней рождений».

СПИСОК ЛИТЕРАТУРЫ

1. Коваленко И.Н. Об алгоритме субэкспоненциальной сложности декодирования сильно искаженных линейных кодов // Доп. АН УРСР. Сер. А. — 1988. — № 10. — С. 16–17.
2. Kovalenko I.N., Savchuk M.N. Some methods of decoding corrupted linear codes // Регистрация, хранение и обработка данных. — 1999. — **1**, № 2. — С. 62–68.
3. Kovalenko I.N., Savchuk M.N. On a statistical algorithm to decode heavily corrupted linear codes // Applied Probability and Stochastic Processes. — Berkeley: Kluwer Acad. Publ., 1999. — P. 73–82.
4. Ефремов К., Савчук М. Оценки сложности и надежности алгоритмов декодирования сильно искаженных линейных кодов // IX Междунар. науч.-практ. конф. «Безопасность информации в информационно-телекоммуникационных системах» (Київ, 17-19 мая 2006 г.): Тез. докл. — Киев, 2006. — С. 24.
5. Алексейчук А.Н. Системы линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N // Захист інформації. — 2001. — № 4. — С. 12–19.
6. Алексейчук А.Н., Игнатенко С.М. Оценки эффективности универсальных методов восстановления искаженных линейных рекуррент над кольцом вычетов по модулю 2^N // Збірн. наук. праць ІПМЕ НАН України. — К., 2003. — Вип. 20. — С. 40–48.
7. Алексейчук А.Н., Игнатенко С.М. Метод оптимизации алгоритмов решения систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N // Реєстрація, зберігання і обробка даних. — 2005. — **7**, № 1. — С. 21–29.
8. Коваленко И.Н., Левитская А.А., Савчук М.Н. Избранные главы вероятностной комбинаторики. — Киев: Наук. думка, 1986. — 224 с.
9. Алексейчук А.Н. Условия однозначности проблемы моментов в классе q-распределений // Дискрет. математика. — 1999. — **11**, вып. 4. — С. 48–57.
10. Алексейчук А.Н. Неасимптотические границы распределения вероятностей ранга случайной матрицы над конечным полем // Там же. — 2007. — **19**, вып. 2. — С. 85–93.
11. Балакин Г.В. Системы случайных уравнений над конечным полем // Тр. по дискрет. математике. — 1998. — **2.** — С. 21–37.
12. Левитская А.А. Системы случайных уравнений над конечными алгебраическими структурами // Кибернетика и системный анализ. — 2005. — № 1. — С. 82–116.
13. Алексейчук А.Н. Вероятностная схема независимых случайных элементов, распределенных на конечной решетке. I. Точные распределения функционалов объединения случайных элементов // Там же. — 2004. — № 5. — С. 1–15.
14. Алексейчук А.Н. Вероятностная схема независимых случайных элементов, распределенных на конечной решетке. II. Метод решеточных моментов // Там же. — 2004. — № 6. — С. 44–65.
15. Alekseychuk A.N. Random covers of finite homogeneous lattices // Theory of Stoh. Processes. — 2006. — **12(28)**, N 1, 2. — P. 12–19.
16. Алексейчук А.Н. Об однозначности проблемы моментов в классе q-распределений // Дискрет. математика. — 1998. — **10**, вып. 1. — С. 95–110.
17. Коваленко И.Н. Об одной верхней оценке числа полных отображений // Кибернетика и системный анализ. — 1996. — № 1. — С. 81–85.
18. Коваленко І.М., Купер К. Верхня границя для числа повних відображень // Теорія ймовірностей і мат. статистика. — 1995. — **53.** — С. 69–75.
19. Cooper C., Gilchrist R., Kovalenko I.N., Novacovic D. Deriving the number of good permutations with applications to cryptography // Кибернетика и системный анализ. — 1999. — № 5. — P. 10–16.
20. Кузнецов Н.Ю. Применение ускоренного моделирования к нахождению количества «хороших» перестановок // Там же. — 2007. — № 6. — С. 80–89.
21. Гилкрист Р., Коваленко И.Н. Об оценке вероятности отсутствия коллизий некоторых случайных отображений // Там же. — 2000. — № 1. — С. 132–138.
22. Ковальчук Л.В. Псевдонеприводимые полиномы. Вероятностное тестирование неприводимости // Там же. — 2004. — № 4 — С. 168–176.
23. Савчук М.Н. Некоторые предельные теоремы в схеме равновероятного размещения частиц комплектами // Теория вероятностей и мат. статистика. — 1983. — Вып. 28. — С. 122–130.
24. Savchuk M. Some limiting theorems in ball batch allocation scheme with random levels defined by an another allocation scheme // Probabilistic Methods in Discrete Mathematics. — M.: Теория вероятностей и ее применения, 1993. — С. 428–436.
25. Савчук М.Н. Предельное поведение случайного времени ожидания до заполнения заданного подмножества ячеек в схеме равновероятного размещения частиц комплектами // Модели и методы исследования операций, теории риска и надежности — К.: Ин-т кибернетики НАНУ, 1992. — С. 3–10.
26. Савчук М.Н. Асимптотический анализ вариационного ряда вероятностей серий различных исходов в полиномиальной схеме // Доп. НАН України. — 1999. — № 3. — С. 101–105.
27. Савчук М.Н. О предельных распределениях максимальной и минимальной частот в схеме размещения случайного числа частиц по ячейкам // Математические методы моделирования и системного анализа в условиях неполной информации. — К.: Ин-т кибернетики АН УССР, 1991. — С. 9–12.
28. Савчук М.Н. Сходимость многомерных случайных процессов, связанных с разделимыми статистиками в схемах размещения, к гауссовским диффузионным процессам // Анализ стохастических систем методами исследования операций и теорем надежности. — К.: Ин-т кибернетики АН УССР, 1987. — С. 43–47.

29. Савчук М.Н., Синявский В.Ф. Об алгоритме определения моментов изменения параметров бернуллиевской последовательности // Проблемы управления и информатики. — 1999. — № 1. — С. 84–89.
30. Савчук М.Н. Анализ одного метода улучшения характеристик случайной двоичной последовательности // Кибернетика и вычисл. техника. — 1998. — Вып. 118. — С. 57–61.
31. Шарапов В. Алгоритм тестирования случайных и псевдослучайных последоватнльностей с использованием контекстного моделирования // Сб. тез. докл. X Юбилейной междунар. науч.-практ. конф. «Безопасность информации в информационно-телекоммуникационных системах», трав. 2007 р., Київ. — К.: ЧП «ЕКМО», НИЦ «Тезіс» НТУУ «КПІ», 2007. — С. 30–31.
32. Ковальчук Л., Бездітний В. Перевірка незалежності статистичних тестів, призначених для оцінки криптографічних якостей ГПВ // Захист інформації. — 2006. — № 2 (29) — С. 18–23.
33. Ковальчук Л., Мельник С., Бездетный В. Вероятностные характеристики генерации ключей с неравномерным распределением // Радіотехніка (Харьків). — 2005. — **141**. — С. 181–188.
34. Савчук М.Н. Использование метода Монте–Карло для идентификации булевых функций большого числа переменных // Кибернетика и вычисл. техника. — 1998. — Вып. 117. — С. 3–7.
35. Пометун С.А. Исследование алгебраических атак на потоковые и блоковые шифраторы. // Сб. тез. докл. X Юбилейной междунар. науч.-практ. конф. «Безопасность информации в информационно-телекоммуникационных системах», трав. 2007 р., Київ. — К.: ЧП «ЕКМО», НИЦ «Тезіс» НТУУ «КПІ», 2007. — С. 28–29.
36. Пометун С.А. Обобщенные корреляция и нелинейность высокого порядка булевых функций для описания вероятностных алгебраических атак // Третья междунар. науч. конф. по пробл. безопасности и противодействия терроризму, МаБИТ, окт. 2007 — М., 2007. — С. 153–163.
37. Пометун С.А. Імовірнісний алгебраїчний криптоаналіз шифратора «SFINKS» з певним класом фільтруючих функцій // Правове, нормат. та метрол. забезпечення системи захисту інформації в Україні. — 2008. — № 1 (16). — С. 73–78.
38. Пометун С.А. Алгебраїчні атаки на потокові шифратори як узагальнення кореляційних атак // Системні дослідження та інформ. технології. — 2008. — № 2. — С. 29–40.
39. Пометун С.А. Про кількість булевих функцій із заданим алгебраїчним імунітетом // Прикл. радиоэлектроника. — 2008. — № 3. — С. 322–325.
40. Пометун С.А. Исследование вероятностных сценариев алгебраических атак на потоковые шифры // Проблемы управления и информатики. — 2009. — № 1. — С. 143–156.
41. Алексейчук А.Н., Проскуровский Р.В. Нижняя граница вероятности различения внутренних состояний комбинирующего генератора гаммы с неравномерным движением // Правове, нормат. та метрол. забезпечення системи захисту інформації в Україні. — Вип. 2 (13). — Київ, 2006. — С. 159–169.
42. Алексейчук А.Н., Проскуровский Р.В., Скрыпник Л.В. Статистическая атака на комбинирующий генератор гаммы с неравномерным движением в режиме реинициализации начального состояния // Математика и безопасность информационных технологий: Материалы конф. в МГУ 25–27 окт. 2006 г. — М.: МЦНМО, 2007. — С. 264–269.
43. Олексійчук А.М., Проскуровський Р.В. Оцінка середньої ймовірності помилки байєсівського критерію для перевірки гіпотез в задачі криптоаналізу комбінувального генератора гами з нерівномірним рухом // Теорія ймовірностей та мат. статистика. — 2008. — Вип. 78. — С. 152–159.
44. Алексейчук А.Н. Оптимальные уравновешенные отображения в конструкциях генераторов гаммы с неравномерным движением регистров сдвига и протоколов передачи ключей по каналу связи с отводом // Реєстрація, зберігання і обробка даних. — 2008. — **10**, № 4 — С. 47–56.
45. Иванов В.А. О методе случайного кодирования // Дискрет. математика. — 1999. — **11**, вып. 3. — С. 99–108.
46. Алексейчук А.Н. Случайное кодирование в канале связи с аддитивным шумом, распределенным на конечной абелевой группе // Захист інформації. — 2002.— № 3. — С. 7–16.
47. Алексейчук А.Н. Оптимальное случайное кодирование равновероятных сообщений в q-ичном симметричном канале // Там же. — № 4. — С. 49–58.
48. Завадская Л., Меллит А., Фаль А. О методах криптоанализа поточных шифров // Шоста Міжнар. наук.-практ. конф. «Безпека інформації в інформаційно-телекомунікаційних системах» (Київ–2003): Тези доп. — Київ, 2003. — С. 55.
49. Alekseychuk A.N., Kovalchuk L.V. Upper bounds of maximum values of average differential and linear characteristic probabilities of Feistel cipher with adder modulo 2^m // Theory of Stoh. Processes. — 2006. — **12 (28)**, N 1, 2. — P. 20–32.
50. Ковальчук Л.В. Верхние оценки средних вероятностей дифференциальных аппроксимаций булевых отображений // Материалы междунар. науч. конф. по безопасности и противодействию терроризму. Интеллект. Центр МГУ, 2–3 нояб. 2005 г. — М.: МЦНМО, 2006. — С. 163 — 167.
51. Скрыпник Л.В., Ковальчук Л.В. Верхние границы средних вероятностей дифференциалов булевых отображений // Захист інформації. — 2006. — № 3. — С. 7–12.
52. Алексейчук А.Н. Верхние границы параметров, характеризующих стойкость немарковских блочных шифров относительно методов разностного и линейного криптоанализа // Там же. — 2006. — № 3. — С. 20–28.
53. Ковальчук Л.В. Обобщенные марковские шифры: построение оценки практической стойкости относительно дифференциального криптоанализа // Математика и безопасность информационных технологий: Материалы конф. в МГУ 25–27 окт. 2006 г. — М.: МЦНМО, 2007. — С. 595–599.

54. Олексійчук А.М., Ковальчук Л.В., Пальченко С.В. Криптографічні параметри вузлів заміни, що характеризують стійкість ГОСТ-подібних блокових шифрів відносно методів лінійного та різницевого криптоаналізу // Захист інформації. — 2007. — № 2. — С. 12–23.
55. Алексейчук А.Н., Ковальчук Л.В., Скрынник Е.В., Шевцов А.С. Оценки практической стойкости блочного шифра «Калина» относительно методов разностного, линейного криптоанализа и алгебраических атак, основанных на гомоморфизмах // Прикл. радиоэлектроника. — 2008. — **7**, № 3. — С. 203–209.
56. Алексейчук А.Н., Шевцов А.С. Показатели и оценки стойкости блочных шифров относительно статистических атак первого порядка // Реєстрація, зберігання і обробка даних. — 2006. — **8**, вип. 4. — С. 53–63.
57. Vaudenay S. Decorrelation: a theory for block cipher security // J. Cryptology. — 2003. — **16**, N 4. — P. 249–286.
58. Ковальчук Л., Пальченко С. Верхние оценки вероятностей обобщенных дифференциалов раундовых преобразований ГОСТ-подобных шифров // XII Междунар. науч.-практ. конф. «Безопасность информации в информационно-телекоммуникационных системах», 19–22 мая 2009 г., тез. докл. — К.: ЧП «ЕКМО», НИЦ «Тезис» НТУУ «КПИ», 2009. — С. 22–23.
59. Яковлєв С.В. Дослідження критеріїв якості та розробка алгоритму генерації довгострокових ключових елементів шифратора ГОСТ 28147–89 // IV Всеукр. наук.-практ. конф. студентів, аспірантів та молодих вчених «Технології безпеки інформації» (Київ, 14 квіт. 2006 р.): Збірка тез доп. учасників. — Київ, 2006. — С. 34.
60. Яковлєв С.В. Збалансовані критерії якості довгострокових ключових елементів алгоритму шифрування ГОСТ 28147–89 // Інформ. технології та комп'ютер. інженерія. — 2009. — № 1. — С. 51–58
61. Яковлєв С.В. Каскадна схема Фейстеля та її стійкість до диференціального та лінійного аналізу // Правове, нормат. та метрол. забезпечення системи захисту інформації в Україні. — Київ, 2009. — Вип. 1 (18). — С. 103–108.
62. Фесенко А.В. Анализ криптосистемы с открытым ключом на основе кусочно-линейного изображения // Сб. тез. докл. X Юбилейной междунар. науч.-практ. конф. «Безопасность информации в информационно-телекоммуникационных системах», трав. 2007 р., Київ. — К.: НИЦ «Тезіс» НТУУ «КПІ», 2007. — С. 32–33.
63. Фесенко А.В. Построение бесключевой атаки на криптосистему на основе кусочно-линейного отображения // Пробл. упр. и информатики. — 2008. — № 5. — С. 149–156.
64. Фесенко А.В. Построение бесключевой атаки на криптосистему на основе кусочно-линейного отображения // Там же. — 2009. — № 1. — С. 130–142.
65. Савчук М.М., Фесенко А.В. Дослідження можливості використання симетричних шифрів для побудови постквантових криптографічних протоколів // Зб. матеріалів Шостої міжнар. конф. «ІНТЕРНЕТ–ОСВІТА–НАУКА–2008». — Вінниця: УНІВЕРСУМ–Вінниця, 2008. — Т. 2. — С. 411–412.
66. Савчук М.М., Фесенко А.В. Симетричні комутативні та локально-комутативні шифри для побудови класичних та постквантових протоколів // Інформ. технології та комп'ютер. інженерія. — 2008. — № 2 (12). — С. 43–51.
67. Савчук М.Н., Шарапов В.Г. Анализ одного метода тестирования случайных последовательностей, основанного на контекстном моделировании // Правове, нормат. та метрол. забезпечення системи захисту інформації в Україні. — 2008. — Вип. 1 (16). — С. 82–89.
68. Савчук М.Н., Шарапов В.Г. Многомерный статистический тест для двоичных последовательностей // Там же. — 2009. — Вып. 1 (18). — С. 65–72.
69. ДСТУ ISO/IEC 18014–1:2006. Інформаційні технології. Методи захисту. Послуги штемпелювання часу. Ч. 1. Основні положення (ДСТУ ISO/IEC 18014–2:2002.IDT) / А. Анісімов, Т. Аванесов, В. Ткаченко, О. Фаль (переклад та наук.-техн. редагування). — Київ: Держспоживстандарт України, 2008. — 25 с.
70. ДСТУ ISO/IEC 18014–2:2006. Інформаційні технології. Методи захисту. Послуги штемпелювання часу. Ч. 2. Механізми, що виробляють незалежні токени (ДСТУ ISO/IEC 18014–2:2002.IDT) / А. Анісімов, Т. Аванесов, В. Ткаченко, О. Фаль. — Київ: Держспоживстандарт України, 2008. — 26 с.
71. ДСТУ ISO/IEC 18014–3:2006. Інформаційні технології. Методи захисту. Послуги штемпелювання часу. Ч. 3. Механізми, що виробляють зв'язані токени (ДСТУ ISO/IEC 18014–3:2002.IDT). А. Анісімов, Т. Аванесов, В. Ткаченко, О. Фаль. — Київ: Держспоживстандарт України, 2008. — 32 с.
72. Костин А.А., Молдовян Н.А., Фаль А.М. О реализации протоколов слепой подписи и коллективной подписи на основе стандартов цифровой подписи // Материалы VI Санкт-Петербург. межрег. конф. «Информационная безопасность России (ИБРР–2009), Санкт-Петербург, 28–30 окт. — СПб.: СПОИСУ, 2009. — С. 111.
73. Національний стандарт України. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. ДСТУ 4145–2002. — Київ: Держав. комітет України з питань техн. регулювання та спожив. політики, 2003. — 36 с.
74. Левитская А.А. Теоремы инвариантности для одного класса систем случайных уравнений над произвольным конечным кольцом с левой единицей // Кибернетика и системный анализ. — 2008. — № 6. — С. 106–115.
75. Алексейчук А.Н., Шевцов А.С. Верхние оценки несбалансированности билинейных аппроксимаций раундовых функций блочных шифров // Там же. — 2010. — № 3. — С. 42–51.
76. Ендовицкий П.А. Уточнение асимптотической аппроксимации размера группы в парадоксе дней рождений // Там же. — С. 185–188.
77. Левитская А.А. Решение проблемы инвариантности вероятностных характеристик заведомо совместных систем случайных нелинейных уравнений над конечным коммутативным кольцом с единицей // Там же. — С. 28–41.

Поступила 17.02.2010