Московский государственный университет имени М.В.Ломоносова

На правах рукописи

Алексеев Евгений Константинович

АППРОКСИМАЦИЯ ДИСКРЕТНЫХ ФУНКЦИЙ АЛГЕБРАИЧЕСКИ ВЫРОЖДЕННЫМИ ФУНКЦИЯМИ В АНАЛИЗЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Специальность **05.13.19.** — методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2011

Работа выполнена на
кафедре Математической Кибернетики
Факультета Вычислительной математики и кибернетики
Московского государственного университета имени М.В.Ломоносова

Научный руководитель: *кандидат физико-математических наук,*
старший научный сотрудник
Логачев Олег Алексеевич;

Официальные оппоненты:
доктор технических наук,
доцент Никонов Владимир Глебович;

кандидат физико-математических наук
доцент Таранников Юрий Валерьевич.

Ведущая организация: *Национальный исследовательский*
ядерный университет «МИФИ».

Защита диссертации состоится 23 ноября 2011 года в 16^{45} на заседании диссертационного совета *Д 501.002.16* при Московском государственном университете им. М.В. Ломоносова по адресу: РФ, 119991, Москва, ГСП-1, Ленинские горы, д. 1, МГУ, Главное здание, механико-математический факультет, аудитория 14-08.

С диссертацией можно ознакомиться в библиотеке Механико-математического факультета МГУ имени М.В. Ломоносова (Главное здание, 14 этаж).

Автореферат разослан 21 октября 2011 г.

Ученый секретарь диссертационного совета
Д.501.002.16 при МГУ,
доктор физико-математических наук,
профессор

А.А. Корнев

Общая характеристика работы

Актуальность темы. Стремительное развитие информационных технологий оказывает существенное влияние на все стороны жизни государства и общества. Эпоха массовых коммуникаций, технологии Интернет, информатизация управления технологическими процессами в различных сферах деятельности человека привели к резкому возрастанию потребности в обеспечении безопасности информационных систем от несанкционированного доступа и деструктивных воздействий. Как следствие, актуальны задачи построения надежных телекоммуникационных систем и разработки методов оценки уровня их защищенности.

Одну из ведущих ролей при синтезе и анализе уровня защищенности информационных и телекоммуникационных систем играют математические модели и методы. В комплексе мер по обеспечению информационной безопасности подобных систем важное место занимают криптографические методы, включающие использование потоковых шифров. Настоящая работа посвящена исследованию математических моделей обеспечения информационной безопасности, использующих криптографические булевы функции.

Булевы функции и отображения являются одними из основных структурных элементов в большинстве современных криптографических конструкций (потоковые шифры, блоковые шифры, хэш-функции и т.п.). Традиционно, те функции (системы функций), которые применяются при синтезе криптографических объектов, называют *криптографическими функциями*.

В ходе развития средств и методов криптографического анализа выделился ряд математических свойств, которым должны удовлетворять криптографические функции (системы функций). Наличие подобных свойств у функций призвано обеспечить устойчивость построенных с их помощью криптографических схем относительно методов криптографического анализа.

Примерами таких свойств являются: максимально возможная удаленность от множества аффинных функций[1]; отсутствие корреляционных связей между значением функции и набором ее переменных фиксированной мощности[2]; отсутствие у булевой функ-

[1] Rothaus O. S. On «Bent» Functions // Journal of Combinatorial Theory (A). 1976. Vol. 20. No. 3. Pp. 300–305.

[2] Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications // IEEE Trans. on Inform. Theory. 1984. Vol. 5. Pp. 776–780.

ции низкостепенных аннигиляторов[3]; отсутствие у булевой функции (отображения) линейных структур[4]. Множества булевых функций, обладающих данными свойствами, выделяются в отдельные классы. К их числу относятся бент-функции, корреляционно-иммунные функции, алгебраически иммунные функции и алгебраически невырожденные функции. Характерной особенностью этих классов является отсутствие не только хорошего алгебраического их описания, но также отсутствие точных выражений для их мощностей и хороших оценок. Примерами результатов исследований в этой области могут служить работы Денисова[5][6] и Maitra[7] для корреляционно-иммунных функций, оценки для числа бент-функций в работах Carlet[8] и Krotov[9], асимптотические оценки числа алгебраически вырожденных функций[10]. Подобные функции, имеющие нетривиальные линейные структуры, не обладают необходимыми криптографическими свойствами. Вместе с тем, они играют важную роль в криптоанализе.

Ряд методов криптографического анализа использует аппроксимацию (относительно метрики Хэмминга) криптографических функций с помощью функций специального вида с целью перехода от исходной криптографической задачи к соответствующей математической задаче. Исторически первыми для аппроксимации были использованы аффинные функции[11], входящие в класс функций, обладающих нетривиальными линейными структурами. Например, некоторые разновидности корреляционного метода криптоанализа

[3]Courtois N., Meier W. Algebraic attacks on stream ciphers with linear feedback // Lecture Notes in Computer Science. 2003. Vol. 2656. Pp. 345–359.

[4]Evertse J. H. Linear Structures in Block Ciphers // Proceedings of Eurocrypt'87. 1987. Pp. 249–266.

[5]Денисов О. В. Асимптотическая формула для числа корреляционноиммунных порядка k булевых функций // Дискретная математика. 1991. Т. 3. С. 25–46.

[6]Денисов О. В. Локальная предельная теорема для распределения части спектра случайной двоичной функции // Дискретная математика. 2000. Т. 12. С. 82–95.

[7]Maitra S., Sarkar P. Enumeration of Correlation Immune Boolean Functions // Lect. Notes in Comp. Sci. 1999. Vol. V. 1587. Pp. 12–15.

[8]Carlet C., Klapper A. Upper bounds on the numbers of resilient functions and of bent functions // 23rd Symposium on Information Theory. 2002. Pp. 307–314.

[9]Krotov D. S., Avgustinovich S. V. On the Number of 1-Perfect Binary Codes: A Lower Bound // IEEE Trans. Inform. Theory. 2008. Vol. 54. Pp. 1760–1765.

[10]Didier F. A new bound on the block error probability after decoding over the erasure channel // IEEE Trans. on Information Theory. 2006. Vol. IT-52.

[11]Siegenthaler T. Decrypting a Class of Stream Chipher Using Ciphertext Only // IEEE Trans. on Computers. 1985. Vol. C-34(1). Pp. 81–85.

используют для аппроксимации аффинные функции[12]. При его использовании осуществляется переход от исходной криптографической задачи определения ключа (в широком смысле) к задачам математической статистики или теории кодирования. По этой причине, в частности, расстояние до функций, обладающих нетривиальными линейными структурами, рассматривается как одна из криптографических характеристик булевых функций[13], обобщающих понятие нелинейности булевой функции. Класс функций, обладающих нетривиальными линейными структурами, включает в себя такой интересный с точки зрения приложений класс функций, как алгебраически вырожденные функции[14].

В данной работе исследуются алгебраические, комбинаторные и криптографические свойства аппроксимаций криптографических функций алгебраически вырожденными булевыми функциями.

Цель диссертации. Цель диссертационной работы заключается:

1) в изучении алгебраических и комбинаторных свойств множества корреляционно-иммунных булевых функций «в целом»;

2) в изучении свойств расстояния до множества алгебраически вырожденных функций, как криптографической характеристики булевой функции, обобщающей понятие ее нелинейности;

3) в исследовании возможности построения алгоритмов, реализующих метод криптографического анализа фильтрующего генератора, на основе аппроксимации фильтрующей функции алгебраически вырожденной булевой функцией, не являющейся аффинной.

Научная новизна. Все результаты диссертации являются новыми. Основные результаты диссертационной работы состоят в следующем:

1) Получено новое алгебраическое описание структуры множества корреляционно-иммунных как минимум первого порядка

[12] Meier W., Staffelbach O. Fast correlation Attacks on certain Stream Ciphers // Journal of Cryptology. 1989. Vol. 1. Pp. 159–176.

[13] Meier W., Staffelbach O. Nonlinearity criteria for cryptographic functions // Springer Verlag. 1989. Vol. EUROCRYPT'89.

[14] Dawson E., Wu C. Construction of Correlation Immune Boolean Functions // Information and Communications Security. 1997. Pp. 170–180.

булевых функций от фиксированного числа переменных. Получена точная формула для числа корреляционно-иммунных функций от фиксированного числа переменных веса 4;

2) Описаны свойства минимальных корреляционно-иммунных булевых функций, получены оценки на вес и порядок их корреляционной иммунности;

3) Впервые описаны свойства такого параметра булевой функции как расстояние до множества алгебраически вырожденных функций. Получена точная верхняя оценка на значение этого параметра и описаны некоторые классы функций, для которых этот параметр достигает своего максимального значения;

4) Описаны свойства алгебраически вырожденных функций наилучшим образом аппроксимирующих данную функцию. Получено неравенство, связывающее порядок алгебраической вырожденности наилучших аппроксимаций и расстояние до множества алгебраически вырожденных функций, описаны некоторые классы функций, показывающие, что это неравенство является точным. Исследованы значения этих параметров для бент-функций. Предложены алгоритмы вычисления значений этих параметров;

5) Впервые разработаны два алгоритма (детерминированный и вероятностный) определения ключа фильтрующего генератора, которые используют аппроксимацию функции усложнения с помощью алгебраически вырожденных функций, не являющихся аффинными.

Научная и практическая ценность. Работа имеет теоретический характер. Полученные в диссертации результаты могут найти применение:

1) при синтезе и анализе систем обеспечения информационной безопасности на основе потоковых шифров, использующих фильтрующие генераторы;

2) при изучении свойств преобразований, осуществляемых кодирующими устройствами, состоящими из регистра сдвига и функции усложнения;

3) в учебном процессе для студентов-математиков, обучающихся рамках специализации «Математические и программные методы обеспечения информационной безопасности»;

4) в научных центрах, занимающихся исследованиями в области обеспечения информационной безопасности.

Методы исследования. В диссертации используются методы теории булевых функций, линейной алгебры, комбинаторного анализа, теории вероятностей и математической статистики.

Апробирование. Результаты диссертации докладывались на следующих семинарах и конференциях:

- семинаре «Дискретная математика и математическая кибернетика» кафедры математической кибернетики факультета Вычислительной математики и кибернетики Московского государственного университета им. М.В. Ломоносова;
- семинаре «Математические проблемы криптографического анализа» кафедры математической кибернетики факультета Вычислительной математики и кибернетики Московского государственного университета им. М.В. Ломоносова;
- семинаре «Булевы функции в криптологии» кафедры дискретной математики Механико-математического факультета Московского государственного университета им. М.В. Ломоносова;
- семинаре по криптографии ИПИБ МГУ им. М. В. Ломоносова;
- IV международной научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2008), 2008 год;
- VI международной научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2010), 2010 год;
- VII международной научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2011), 2011 год;

- VIII международной конференции «Дискретные модели в теории управляющих систем», 2009 год;
- научной конференции «Тихоновские чтения», 2010 год;
- VI молодежной научной школе по дискретной математике и ее приложениям, 2007 год;
- IX международном семинаре «Дискретная математика и ее приложения», 2007 год.

Публикации по теме диссертации. Основное содержание диссертации опубликовано в 8 работах [1, 2, 3, 4, 5, 6, 7, 8]; в том числе, в работах [1] и [2] в журналах, входящих в перечень ВАК ведущих рецензируемых научных журналов и изданий.

Структура и объем работы. Диссертация состоит из введения, четырех глав, заключения, приложения и списка литературы, включающего 34 наименования. Объем работы 106 страниц.

Содержание работы

Во Введении обосновывается актуальность диссертационной работы, формулируются цели и аргументируется научная новизна исследований, показывается практическая значимость полученных результатов, представляются выносимые на защиту научные положения.

В первой главе диссертации приводятся основные понятия и ранее известные результаты, которые используются далее в работе или представляются важными для понимания следующих глав.

Во второй главе исследуются комбинаторные и алгебраические свойства множества корреляционно-иммунных булевых функций «в целом». Булева функция называется корреляционно-иммунной порядка k, если ее выход статистически не зависит в естественной теоретико-вероятностной модели от любой линейной комбинации k и менее входов. $CI(n)$ — множество всех корреляционно-иммунных булевых функций как минимум первого порядка от n переменных.

В разделе 2.1 рассматриваются свойства четных ($f(x) = f(x \oplus 1^n)$) булевых функций.

В разделе 2.2 получено описание множества $CI(n)$, как объединения смежных классов по подпространствам пространства четных

функций специального вида (Теорема 2.6). Следствием этого описания является доказанная в разделе 2.3 конструктивная нижняя оценка для мощности множества $CI(n)$ (Теорема 2.8).

В разделе 2.4 доказаны два критерия принадлежности булевой функции множеству $CI(n)$. Один из этих критериев (Теорема 2.9) может быть полезен при исследовании свойств множества корреляционно-иммунных булевых функций при расчетах на ЭВМ. Критерий, доказанный в теореме 2.10, характеризует метрические свойства носителей корреляционно-иммунных булевых функций как минимум первого порядка.

В разделе 2.5 вводится понятие минимальной корреляционно-иммунной булевой функции. Функция $f \in CI(n)$ называется минимальной, если не существует такой булевой функции g от n переменных, что $f \cdot g = g$ и $g \in CI(n)$. Введение этого определения продиктовано следующим свойством корреляционно-иммунных булевых функций: если $f \in CI(n)$ и g такова, что $f \cdot g = g$ и $g \in CI(n)$, то $f \oplus g \in CI(n)$. Это означает, что корреляционно-иммунные функции, которые не являются минимальными, «раскладываются» на сумму ортогональных (таких g и h, что $g \cdot h = \overline{0}$) корреляционно-иммунных функций. С помощью введенного понятия исследуются свойства множества корреляционно-иммунных функций «в целом». Получено исчерпывающее описание множества минимальных функций веса 2, 4 и 6 (примеры 2.1, 2.2 и 2.3). Получены верхние оценки для веса (предложение 2.10) и порядка корреляционной иммунности (предложение 2.12) минимальных функций: $wt(f) \leq 2^{n-1}$ и $cor(f) \leq 2$.

В следующем разделе вводится понятие минимальной корреляционно-иммунной булевой функции в классе функций, носители которых представляют собой смежные классы по некоторым подпространствам (определение 2.3). Заметим, что эти функции являются алгебраически вырожденными. Для минимальных функций такого вида также получены верхние оценки для веса и порядка корреляционной иммунности: $wt(f) \leq n + 1$ и $cor(f) \leq 2$ (соответственно предложение 2.14 и предложение 2.15). Теорема 2.12 описывает множества минимальных в классе $LCI(n)$ функций, порядок корреляционной иммунности которых равен 2. Благодаря этому описанию удалось привести пример минимальной корреляционно-иммунной булевой функции с порядком корреляционной иммунности равным 2 (пример 2.6). Таким образом, оценка $cor(f) \leq 2$ для минимальных корреляционно-иммунных функций является точной.

Результатом исследований, представленных в данном разделе, является также некоторое улучшение оценки для веса минимальной корреляционно-иммунной функции: при $n > 3$ для любой минимальной корреляционно-иммунной булевой функции справедливо неравенство $wt(f) < 2^{n-1}$ (следствие 2.14).

Результатом раздела 2.7 является точная формула для мощности множества корреляционно-иммунных булевых функций от n переменных веса 4 и $2^n - 4$ (следствие 2.15).

В заключительном разделе второй главы рассматриваются свойства подпространств булевых функций, состоящих из корреляционно-иммунных функций.

В третьей главе анализируются свойства аппроксимации булевых функций с помощью алгебраически вырожденных функций. В работе Meier, Staffelbach[15] в качестве мер нелинейности анализируются расстояния до аффинных функций и до функций, имеющих нетривиальные линейные структуры: $nl(f)$ — расстояние до множества аффинных функций; $\delta(f)$ — расстояние до множества функций, имеющих нетривиальные линейные структуры. В разделе 3.1 третьей главы представлено понятие невырожденности булевой функции $\rho(f)$ — расстояние до алгебраически вырожденных функций. Показывается (следствие 3.1) связь вновь введенного понятия с автокорреляционными коэффициентами булевой функции: $\rho(f) = 2^{n-2} - \frac{1}{4} \max_{u \in V_n^*} \triangle_f(u)$. В предложении 3.3 доказывается, что значение параметра $\rho(f)$ для любой булевой функции не превосходит 2^{n-2}. Описываются некоторые классы функций, для которых параметр $\rho(f)$ достигает своего максимального значения 2^{n-2} (теорема 3.3). В предложении 3.1 доказывается важное утверждение о связи порядка алгебраической вырожденности ($AD(f)$) булевой функции с пространством тех векторов, сдвиги на которые не меняют функцию ($J(f) = \{u \in V_n | f(x \oplus u) = f(x)$ для всех векторов $x\}$): $AD(f) = dim\, J(f)$.

В разделе 3.2 анализируется порядок алгебраической вырожденности тех функций, которые находятся на расстоянии $\rho(f)$ от аппроксимируемой функции f, а именно - тех алгебраически вырожденных функций, которые наилучшим образом аппроксимируют данную.

[15] Meier W., Staffelbach O. Nonlinearity criteria for cryptographic functions // Springer Verlag. 1989. Vol. EUROCRYPT'89.

Анализируются свойства следующих функционалов:

$$\pi_\rho(f) = \max_{g \in \mathcal{F}_n, dist(f,g)=\rho(f)} AD(g),$$

$$\pi_\delta(f) = \max_{g \in \mathcal{F}_n, dist(f,g)=\delta(f)} dim\,\{u \in V_n | f^u \oplus f \in \{\overline{0}, \overline{1}\}\}.$$

Доказывается предложение 3.4 (если $\rho(f) = \delta(f)$, то $\pi_\delta(f) = \pi_\rho(f)$ либо $\pi_\delta(f) = \pi_\rho(f) + 1$; если $\rho(f) > \delta(f)$, то $\pi_\delta(f) = 1$), из которого можно сделать следующий вывод. Если рассматривать параметры ρ и δ в совокупности со связанными с ними функционалами π_ρ и π_δ, то более содержательной парой представляется именно пара ρ, π_ρ. Как следствие далее в главе 3 основное внимание уделяется именно этой паре параметров.

В разделе 3.2 доказывается основное неравенство, которое связывает параметры ρ и π_ρ: $\log_2 \rho(f) + \pi_\rho(f) \leq n$ (теорема 3.4). Полученное неравенство сравнивается с неравенством Зигенталера ($cor(f) + deg\, f \leq n$). С точки зрения стойкости криптографических примитивов параметры $cor(f)$ и $deg\, f$ надо максимизировать, поэтому неравенство Зигенталера препятствует их одновременной оптимизации. Параметры же ρ и π_ρ, участвующие в неравенстве теоремы 3.4, нужно максимизировать и минимизировать, соответственно. По этой причине неравенство $\log_2 \rho(f) + \pi_\rho(f) \leq n$ способствует оптимизации их значений.

Далее доказываются две леммы (3.1,3.2), которые описывают некоторые классы функций, для которых в доказанном выше неравенстве достигается равенство. В конце раздела представлен пример функции от восьми переменных, для которой $\log_2 \rho(f) + \pi_\rho(f) = 8$.

В разделе 3.3 данной главы доказываются теоремы, связывающие параметры ρ и π_ρ с такими криптографическими параметрами булевых функций как вес, алгебраическая степень и порядок корреляционной иммунности.

Раздел 3.4 третьей главы посвящен исследованию тех алгебраически вырожденных функций, которые расположены от данной функции f на расстоянии $\rho(f)$. Доказывается теорема 3.9 о представлении некоторого подмножества таких функций через функцию f и ее сдвиги. Следствием доказанной теоремы является метод вычисления значения параметра π_ρ.

В разделе 3.5 исследуются свойства введенных ранее понятий для бент-функций. Доказываются утверждения о виде наилучших

алгебраически вырожденных аппроксимаций для бент-функций (лемма 3.3). С помощью лемм, доказанных в предыдущем разделе, строится пример бент-функции, для которой значение параметра π_ρ максимально и равно 2.

В четвертой главе исследуется возможность построения алгоритмов определения ключа фильтрующего генератора с использованием аппроксимации функции усложнения алгебраически вырожденными булевыми функциями.

В разделе 4.1 описывается криптографическая задача восстановления ключа фильтрующего генератора и эта задача сводится к задаче решения системы булевых уравнений.

В разделе 4.2 приводятся утверждения, которые необходимы для дальнейшего описания алгоритма. Описываются условия, которые обеспечивают возможность построения атаки. Делаются некоторые естественные предположения криптографического характера.

В разделе 4.3 описывается алгоритм $\mathcal{K}$ определения ключа фильтрующего генератора, который основан на аппроксимации функции усложнения с помощью алгебраически вырожденных булевых функций. В условиях предположений, сделанных в предыдущем разделе, доказывается теорема 4.1 о том, что описанный алгоритм всегда останавливается и возвращает истинное значение ключа.

Раздел 4.4 посвящен оценке трудоемкости алгоритма $\mathcal{K}$. В теореме 4.2 доказывается верхняя оценка для трудоемкости $S_{\mathcal{K}}$ алгоритма $\mathcal{K}$:

$$S_{\mathcal{K}} \leq 2^k + 2^{n-k} + 2^{n-d} + 2^{n-m} \cdot dist(f, g).$$

В данном случае g — алгебраически вырожденная булева функция, с помощью которой аппроксимируется функция усложнения f. Параметр m определяется лишь конструкцией фильтрующего генератора. Параметр k равен порядку алгебраической вырожденности функции g. Параметр d зависит от того, сколько битов выходной последовательности фильтрующего генератора известно.

В следующем разделе описывается вероятностный алгоритм $\mathcal{K}_{Pr}$, который также направлен на определение ключа фильтрующего генератора, и оценивается его трудоемкость.

Раздел 4.6 посвящен оценке параметров, входящих в верхнюю оценку алгоритма $\mathcal{K}$. Описываются некоторые классы фильтрующих функций, для которых можно достаточно эффективно строить аппроксимирующие функции.

Раздел 4.7 содержит два примера, которые иллюстрируют тот факт, что с помощью описанных ранее алгоритмов можно определять ключ фильтрующего генератора с трудоемкостью, которая существенно ниже трудоемкости полного перебора.

В заключении сформулированы основные результаты диссертации.

Приложение содержит исчерпывающий список минимальных корреляционно-иммунных булевых функций от 5 переменных веса 8 (всего 160 функций).

Благодарности. Автор выражает глубокую благодарность своему научному руководителю кандидату физико-математических наук Логачеву Олегу Алексеевичу за постановку задачи, всестороннюю помощь и внимание к работе над диссертацией. Также автор выражает благодарность Селезневой Светлане Николаевне, Ященко Валерию Владимировичу и всем сотрудникам кафедры математической кибернетики факультета ВМК МГУ имени Ломоносова за доброжелательное отношение и творческую атмосферу.

Список литературы

[1] *Е.К. Алексеев.* **О некоторых алгебраических и комбинаторных свойствах корреляционно-иммунных булевых функций.** // Дискретная математика. 2010. Т. 22. С. 110–126.

[2] *Е.К. Алексеев.* **О некоторых мерах нелинейности булевых функций.** // Прикладная дискретная математика. 2011. Т. 2. С. 5–16.

[3] *Е.К. Алексеев.* **О некоторых алгебраических и комбинаторных свойствах множества корреляционно-иммунных функций в целом.** // Материалы IX Международного семинара "Дискретная математика и ее приложения". 2007. С. 477.

[4] *Е.К. Алексеев.* **О некоторых криптографических свойствах множества четных функций.** // Материалы VI молодежной научной школы по дискретной математике и ее приложениям (Москва, 16-21 апреля, 2007). 2007.

[5] *Е.К. Алексеев.* **О некоторых свойствах линейных кодов, образующих носители корреляционно-иммунных буле-**

вых функций. // Материалы IV международной конференции по проблемам безопастности и противодействия терроризму (МГУ, 30-31 октября 2008 г.). 2008. С. 93–101.

[6] *Е.К. Алексеев.* **Об атаке на фильтрующий генератор с функцией усложнения, близкой к алгебраически вырожденной.** // Материалы VI международной конференции по проблемам безопастности и противодействия терроризму (МГУ, 11-12 ноября 2010 г.). 2010. С. 114–123.

[7] *Е.К. Алексеев.* **Об атаке на фильтрующий генератор с функцией усложнения близкой к алгебраически вырожденной.** // Сборник статей молодых ученых факультета ВМК МГУ. 2011. Т. 8. С. 20–34.

[8] *Е.К. Алексеев.* **Об атаке на фильтрующий генератор с функцией усложнения близкой к алгебраически вырожденной.** // Сборник статей научной конференции «Тихоновские чтения» (25-29 октября 2010 года). 2011. С. 13–14.