Отзыв официального оппонента на диссертацию Аборнева Александра Викторовича на тему «Нелинейные подстановки, линейно представимые над кольцами Галуа, и их приложения в задачах защиты информации», представленной на соискание учёной степени кандидата физико-математических наук по специальности 01.01.06 – математическая логика, алгебра и теория чисел

Рассматриваемая в диссертации задача имеет криптографическое происхождение и относится к способам построения подстановок на декартовых степенях X^m конечных множеств X. Автор следует оригинальному приёму, в основу которого закладывается некое конструктивно задаваемое семейство отображений $X^m \to X^m$ с последующей проверкой их на биективность.

Конкретно в качестве X в диссертаци рассматриваются множества, наделённые структурой конечного поля $GF(p^r)$ для различных простого p и целого $r \geqslant 1$, причём на X^2 дополнительно задаётся структура кольца Галуа $GR(p^{2r}, p^2)$. Семейство отображений $X^m \to X^m$ строится посредством суперпозиций линейных (над кольцом X^2) отображений модуля $(X^2)^m \to (X^2)^m$ и операции взятия старшего разряда элементов кольца Галуа. Последняя операция, использующая знак переноса при сложениях, обеспечивает в последующем важную для криптографических приложений нелинейность подстановок $X^m \to X^m$.

Следует сказать, что собственно теоретическим исследованиям автора предшествовало значительное число проведённых им компьютерных экспериментов по поиску подстановок среди конкретных семейств отображений, причём (как следует из общих соображений) в условиях очень малых надежд на успех. Наградой явились постановки интересных теоретических задач, причём, что важно, частью поддающихся нетривиальному решению.

Основные результаты диссертации сформулированы в нескольких теоремах.

В теореме 1.16 (стр. 38) для пары специальных квадратичных форм над полем $GF(2)$ от m переменных, у которых нелинейные части являются элементарными симметрическими многочленами, приводятся критерии, при которых они дополняются $(m-2)$-я линейными функциями до алгебраически независимой системы. Для криптографических прило-

жений важней, конечно, чтобы все координатные функции подстановки $GF(2)^m \to GF(2)^m$, как и их ненулевые линейные комбинации, были нелинейными. Теоретическая же сложность подобных задач характеризуется уже тем, что даже для сильно разреженных матриц, например с числом единиц в строках и столбцах по 3, не известно способов определения их невырожденности с трудоёмкостью меньшей $O(m^2)$.

В теоремах 1.17 (стр. 51) и 1.18 (стр. 52) приводятся два семейства многочленов степени $m \geqslant 3$ над кольцом $\mathbb{Z}_4$, для которых сопровождающие матрицы соответствующих рекуррентных последовательностей позволяют строить технически легко реализуемые нелинейные подстановки на множестве $GF(2)^m$.

Приведённые три теоремы первой главы потребовали очень сложных рассуждений большого объёма. Доказательста проведены достаточно подробно и с надлежащей тщательностью.

Теоремой 2.9 (стр. 92) утверждается, что для подстановки $\pi : GF(2)^m \to GF(2)^m$, реализуемой одним тактом линейного регистра сдвига с квадратичной функцией обратной связи, множество подстановок $\left\{\prod_{i=1}^{m+1}(T_{x_i}\pi) | \, x_i \in GF(2)^m,\ i = 1, \ldots, m+1\right\}$ является дважды транзитивным на $GF(2)^m$. Здесь: $T_x(v) = x + v$, $x, v \in GF(2)^m$. Дважды транзитивность на короткой длине выступает важным криптографическим свойством. Комментарии и эксперименты, связанные с этой теоремой выявили достаточно неожиданное обстоятельство. Рассматриваемые подстановки строятся по матрицам A размера $m \times m$ над кольцом $\mathbb{Z}_4$. Оказывается, что биективность подстановок $\pi_A : GF(2)^m \to GF(2)^m$, которые строятся по основной рассматриваемой в диссертации конструкции, и требование большого периода рекуррентных последовательностей с сопровождающими матрицами A находятся в антогонизме друг с другом. Если по основной конструкции π_A является подстановкой, то период соответствующей рекуррентной последовательности короткий, не больше (по экспериментам) $4m$.

В теоремах 2.13 (стр. 104) и 2.16 (стр. 108) рассматриваются подстановки $\eta_W : R^m \to R^m$, $R = GR(p^{2r}, p^2)$, которые строятся по специальным матрицам W размера $m \times 2m$ над кольцом R, $\eta_W(x) = \gamma(xW) + p\gamma(xW)$, $x \in R^m$. Здесь $\gamma : R^m \to GF(p^r)^m$ – выделение старшего разряда у всех компонент элемента модуля R^m. В теоремах 2.13 и 2.16 формулируются условия, соответственно для $p > 2$ и $p = 2$, при

которых множества подстановок $\left\{\prod_{i=1}^{4}(L_{x_i}\eta_W)|\, x_i \in R^m,\, i=1,\ldots,4\right\}$ является дважды транзитивными на R^m. Здесь $L_x(v)=x+v$, $x,v\in R^m$, а сложение (в кольце R) осуществляется покомпонентно. При меньшей чем 4 длине произведения, как доказывается в диссертации на стр. 102 – 106, дважды транзитивность не достигается.

Приведённые теоремы, представляющие основное содержание диссертации, снабжены чёткими и подробными доказательствами. Эти теоремы отличаются лаконичными формулировками и большими (порядка десяти страниц) доказательствами, содержащими достаточно глубокие рассуждения.

К сожалению этого нельзя сказать для всех остальных второстепенных утверждений диссертации. Не все из них представлены с надлежащей аккуратностью, имеются пробелы в доказательствах, пусть и легко устранимые квалифицированным читателем. Напротив, некоторые доказательства приведены излишне подробно, без необходимой на то надобности. Это относится к предложению 1.6 (стр. 20), к предложению 1.9 (стр. 27), к теореме 1.10 (стр. 29), к теореме 1.15 (стр. 37), к теореме 1.19 (стр. 56), к предложению 2.15 (стр. 108).

Из других замечаний отметим наличие в диссертации вероятностных выражений без задания исходных распределений и вероятностных пространств (стр. 76, 78, 96). На стр. 86, 97 вместо вероятностей следует использовать преобладания над $1/2$ этих вероятностей.

На стр. 78 под степенью отображения понимается максимальная степень координатных функций, тогда как в криптографии под степенью отображения (в соответствии с общим принципом "минимакса") понимается минимум и даже не отдельных степеней координатных функций, но и их ненулевых линейных комбинаций.

В § 1.2 в некоторых формулах одновременно встречается обозначение $\overrightarrow{x}$ для двух различных конечных последовательностей: для вектора арифметического векторного пространства K^m и для упорядоченного набора его координат в базисе произвольного вида. Такое допустимо только для стандартного базиса, когда эти две последовательности совпадают.

Имеются замечания терминологического характера к стр. 14, 19, 24, 51, 54, 70, 80, 84.

Встретившиеся опечатки на стр. 7,15, 20, 21, 35, 74, 79, 82, 86, 88, 95, 100 не являются помехой для правильного понимания.

Подводя итог, отметим, что основные результаты диссертации получены лично автором, математически грамотно им обоснованы, они несомненно найдут применение в области теоретической криптографии в разделах синтеза перспективных шифрпреобразований, и, возможно, будут внедрены в действующую аппаратуру по защите информации. Имеющиеся недостатки, неизбежные в работах такого объёма, не должны влиять на положительную оценку настоящей диссертационной работы.

Автореферат отвечает содержанию диссертации.

Диссертация соответствует критериям, установленным «Положением о присуждении учёных степеней в Московском государственном университете имени М.В.Ломоносова», утверждённым Ректором МГУ 27 октября 2016 г. Автор заслуживает присуждения ему учёной степени кандидата физико-математических наук по специальности 01.01.06 – «Математическая логика, алгебра и теория чисел».

Ведущий научный сотрудник отдела дискретной математики
ФГБУН Математический институт им. В.А. Стеклова РАН
(119991, г. Москва, ул. Губкина, д.8, тел: +7 (495) 984-81-41,
электронная почта: steklov@mi.ras.ru)

доктор физико-математических наук Малышев 09.02.2018 Ф.М. Малышев

(телефон: 8 (499)941-01-84, e-mail: malyshevfm@mi.ras.ru)

Подпись ведущего научного сотрудника Ф.М. Малышева и сведения заверяю.

ГА Ясков
Ученый секретарь МИАН