ФГБОУ ВО МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ им. М. В. ЛОМОНОСОВА

На правах рукописи

Грибов Алексей Викторович

Алгебраические неассоциативные структуры и их приложения в криптографии

Специальность 01.01.06 — математическая логика, алгебра и теория чисел

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
кандидата физико-математических наук

Москва – 2015

Работа выполнена на кафедре высшей алгебры
Механико-математического факультета ФГБОУ ВО “Московский государственный университет имени М. В. Ломоносова”.

Научный руководитель: **Михалёв Александр Васильевич**
доктор физико-математических наук,
профессор

Официальные оппоненты: **Кожухов Игорь Борисович**,
доктор физико-математических наук,
профессор кафедры высшей математики
ФГБОУ ВПО “Национальный исследовательский университет “МИЭТ”;

Голубков Артем Юрьевич,
кандидат физико-математических наук,
доцент факультета прикладной математики и информатики
ФГБОУ ВПО “Московский государственный технический университет им. Н.Э.Баумана”.

Ведущая организация: ФГБОУ ВПО “Тульский государственный педагогический университет имени Л.Н.Толстого”.

Защита диссертации состоится 25 сентября 2015 г. в 16 ч. 45 мин. на заседании диссертационного совета Д 501.001.84 на базе ФГБОУ ВО “Московский государственный университет имени М.В. Ломоносова”, по адресу: 119991, Москва, ГСП-1, Ленинские горы, д. 1, ФГБОУ ВО “Московский государственный университет имени М.В. Ломоносова”, Механико-математический факультет, аудитория 14-08.

С диссертацией можно ознакомиться в Фундаментальной библиотеке ФГБОУ ВО “Московский государственный университет имени М.В. Ломоносова” по адресу: Москва, Ломоносовский проспект, д. 27, сектор А, http://mech.math.msu.su/$\sim$snark/index.cgi, http://istina.msu.ru/dissertations/9607776.

Автореферат разослан 25 августа 2015 г.

Учёный секретарь
диссертационного совета
Д 501.001.84 на базе
ФГБОУ ВО МГУ имени М.В. Ломоносова
доктор физико-математических наук,
профессор Александр Олегович Иванов

Общая характеристика работы

Актуальность темы.

Диссертация относится к структурной теории неассоциативных структур, а именно к теории радикалов луп, луп обратимых элементов альтернативных луповых колец и Ω-луп. Приложения развитой техники использованы для построения криптографических схем.

При рассмотрении алгебраических систем одной из основных задач является построение структурной теории, которая сводит изучение к более простым системам. Одной из конструкций, осуществляющих такое сведение, является радикал. С тех пор, как в 1950-х гг. А.Г. Курош[1] и С. Амицур[2] ввели аксиоматическое понятие радикала для колец и алгебр, теория радикалов распространилась и на другие алгебраические структуры. Понятие радикала в теории групп окончательно сформировалось к началу шестидесятых годов в определении, предложенном А.Г. Курошем[3]. В это же время А.Г. Курош обратил внимание на аналогию между разрешимыми нормальными подгруппами и нильпотентными идеалами, позволившую К.К. Щукину[4] построить теорию первичного радикала групп.

Описание первичного радикала группы как множества строго энгелевых элементов крайне близка к первичному радикалу в теории ассоциативных колец и алгебр. В связи с этим возник естественный вопрос о соотношении между первичным радикалом кольца с единицей и первичным радикалом подгрупп группы его обратимых элементов. Положительный ответ на него был получен А.В. Михалёвым и И.З. Голубчиком в их теореме о первичном радикале линейной группы над ассоциативным кольцом. В дальнейшем структурная теория первичного радикала алгебраических систем активно развивалась в работах[5] [6].

В теории квазигрупп некоторые понятия, например, нормальность, производная и центр, хорошо сочетаются с обычными теоретико-групповыми определениями. Р. Брак[7] показал, что обычные теоретико-групповые определения полностью корректны для луп Муфанг. Наиболее полно теория

[1] А.Г. Курош, *Радикалы колец и алгебр*. Матем. сборн. **33**, N.1, (1953), 13–26.

[2] S.A. Amitsur, *A general theory of radicals II. Radicals in rings and bicategories*. SAmer. J. Math. **76**, N.1, (1954), 125–197.

[3] А.Г. Курош, *Радикалы в теории групп*. ДАН СССР. **141**, N.4, (1961), 789–791.

[4] К.К. Щукин, *RI*-разрешимый радикал групп*. Матем. сборн. **52**, N.4, (1960), 1021–1031.

[5] А.В. Михалев, И.Н. Балаба, С.А. Пихтильков *Первичный радикал Ω-групп*. Фунд.приклад. матем. **12**, N.2, (2006), 159–174.

[6] А.Ю. Голубков, *Первичный радикал групп над ассоциативными кольцами*. дис.к.ф.-м.н. (2000)

[7] R. Bruck, *A survey of binary systems*. Berlin: Springer-Verlag, (1958).

квазигрупп изложена в работе В.Д. Белоусова[8], различные классы и свойства квазигрупп рассмотрены в работах М.М. Глухова[9] ,Г.Б. Белявской[10] и А.Х. Табарова[11].

Теория коммутаторов и нового, с точки зрения теории групп, понятия ассоциатора в значительной степени отличается от теоретико-группового случая. Теория коммутаторов в лупах развивается в работе Дж. Смита[12]. В работе Р. Маккензи и Дж. Сноу[13] теория коммутаторов в лупах рассмотрена с точки зрения коммутаторов конгруэнций лупы как универсальной алгебры. Именно с этой точки зрения П. Войтеховский и Д. Становский[14] смогли вычислить взаимный коммутант нормальных подлуп.

Квазигруппы и латинские квадраты имеют богатую историю применений в криптографии. Достаточно полные обзоры использования квазигрупп в криптографии приведены в работе М.М. Глухова[15], где применение квазигрупп рассмотрено для построения схем шифрования и однонаправленных функций, а также в работе В.А. Щербакова[16]. Основные результаты в этих работах получены для симметрической криптографии. Одной из первых работ, где использовались квазигруппы для криптографии с открытым ключом является работа С. Косельны и Г. Мюллена[17].

С алгебраической точки зрения классические задачи в криптографии рассматривались в конечнопорожденных и коммутативных группах[18] [19] [20]. Достаточно полно эти вопросы описаны в пособиях[21] [22]. Следующим

[8]В.Д.Белоусов *Основы теории квазигрупп и луп*. Москва: Наука, 1967.

[9]М.М. Глухов, *T-разбиения квазигрупп и групп*. Дискрет.матем. **4**, N.3, (1992), 47–56.

[10]Г.Б. Белявская, *Ассоциаторы, коммутаторы и линейность квазигрупп*. Дискрет.матем. **4**, N.7, (1995), 116–125.

[11]А.Х. Табаров, *Тождества и линейность квазигрупп*. дис. д.ф.-м.н., 2009.

[12]J. Smith, *On the nilpotence class of commutative Moufang loops*. Math. Proc. Cambridge Philos. Soc. **84**, N.3, (1978), 387–404.

[13]R. McKenzie, J. Snow, *Congruence modular varieties commutator theory and its uses*. Structural theory of automata, semigroups and universal algebras **207**, (2005), 273–329.

[14]D. Stanovsky,P. Vojtechovsky, *Commutator theory for loops*. Journal of Algebra **399**,(2014), 290–322.

[15]М.М. Глухов, *О применениях квазигрупп в криптографии*. Прикладная дискретная математика, **2**, N.2, (2008), 28–32.

[16]V.A. Shcherbacov, *Quasigroups in cryptology*. Comput. Sci. J. Moldova **17**, N.2, (2009), 193–228.

[17]C. Koscielny and G. L. Mullen, *A quasigroup-based public-key cryptosystem,*. Int. J. Appl. Math. Comp. Sci., **9**, N.4, (1999), 955–963.

[18]W. Diffie, M.E. Hellman, *New directions in cryptography,*. IEEE Transactions on Information Theory, **22**, (1976), 644–654.

[19]R.L. Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public key cryptosystems,*. Communications of the ACM, **21**, (1978), 120–126.

[20]T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms,*. IEEE Transactions on Information Theory, **31**, (1985), 469–472.

[21]М.М.Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин, *Введение в теоретико-числовые методы криптографии*. Санкт-Петербург: Лань, 2011.

[22]А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В.Черемушкин *Основы криптографии* . Москва:

шагом в развитии можно считать рассмотрение некоммутативных алгебраических структур и изучение в них вычислительно сложных задач. Одной из первых работ в некоммутативной криптографии является статья Н. Вагнера и М. Магийярика[23], где приведена схема, основанная на неразрешимости слова в конечно представленных группах (для данного представления группы G и элемента $g \in G$ определить, выполняется ли условие $g = 1$.). Достаточно полное описание и изучение аспектов некоммутативной криптографии в группах приведено в монографии В. Шпильрайна, А. Мясникова, А. Ушакова [24]. В работах А.В. Михалева, В.Т. Маркова, А.А. Нечаева и др.[25] [26] исследованы некоторые возможности использования неассоциативных структур в криптографии с открытым ключом. В частности, была построена криптосистема над квазигрупповым кольцом, развивающая подход С.К. Россошека[27]. Также можно выделить работу В.А. Романькова[28], посвященную алгебраическому анализу существующих подходов в некоммутативной и неассоциативной криптографии.

Гомоморфное шифрование позволяет производить определённые математические действия с зашифрованным текстом и получать зашифрованный результат, который соответствует результату операций, выполняемых с открытым текстом. В 2009 году К. Джантри[29]. предложил модель, основанную на алгебраических решетках, полногомоморфной алгебраической системы, то есть гомоморфной для операций умножения и сложения (и других операций) одновременно.

Цель работы

Целью диссертационной работы является исследование: строения первичного радикала ряда неассоциативных структур: луп; Ω-луп; луповых колец; связей первичного радикала луп обратимых элементов с первичным радикалом неассоциативных колец; криптографических схем над раз-

---

Гелиос АРВ, 2011.

[23] M. R. Magyarik and N. R. Wagner, *A Public Key Cryptosystem Based on the Word Problem,*.Lecture Notes in Computer Science, **196**, (1985), 19–36.

[24] A. Myasnikov, V. Shpilrain, A. Ushakov, *Group-based Cryptography,*.Birkhauser Basel, Berlin, (2008).

[25] А.В. Грибов, П.А. Золотых, А.В. Михалёв, *Построение алгебраической криптосистемы над квазигрупповым кольцом,*.Математические вопросы криптографии, **4**, N.4 (2010), 23–33.

[26] С.Ю. Катышев, В.Т. Марков и А.А. Нечаев, *Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей,*.Дискрет. матем., **26**, N.3 (2014), 45–64.

[27] С.К. Росошек, *Криптосистемы групповых колец.* Вестник Томского госуниверситета, **6**, (2003), 57–62.

[28] В.А. Романьков, *Криптографический анализ некоторых схем шифрования, использующий автоморфизмы.* Мат.методы криптографии, **3**, N.21 (2013), 35–51.

[29] C. Gentry, *A fully homomorphic encryption scheme,*.Stanford University PhD thesis, (2009).

личными неассоциативными структурами; новых примеров гомоморфной криптографии.

Научная новизна

Результаты диссертации являются новыми и получены автором самостоятельно. Основные результаты диссертации состоят в следующем:

1. Развита теория первичного радикала лупы, исследованы его свойства, доказано его совпадение с множеством строго энгелевых элементов лупы.

2. Получено описание Ω-первичного радикала Ω-лупы, как множества Ω-строго энгелевых элементов.

3. Установлены связи первичного радикала лупы обратимых элементов альтернативного кольца и первичного радикала кольца.

4. Построены криптографические схемы над различными неассоциативными структурами:

   – аналог схемы шифрования Эль-Гамаля над ППС-квазигруппой;

   – схема выработки общего секретного ключа над лупами Пейджа;

   – схема шифрования с открытым ключом на основе покрытий лупы Муфанг.

5. Рассмотрена схема шифрования с открытым ключом над луповым кольцом, проанализированы свойства данной схемы, доказана гомоморфность данной схемы относительно одной из операций.

Основные методы исследования

В работе применяются методы и результаты теории ассоциативных и неассоциативных колец, теории квазигрупп, теории луповых колец и криптографии с открытым ключом.

Теоретическая и практическая ценность.

Работа имеет как теоретический, так и прикладной характер. Полученные в ней результаты могут быть использованы в различных задачах теории луп. Построенные криптографические схемы могут быть использованы при построении различных систем безопасности.

Апробация диссертации.

Результаты диссертации докладывались на следующих конференциях:

- на семинаре “Algebra and Cryptography”, Нью-Йорк, США, 2013 г.;
- на конференции “New directions in cryptography”, Москва, 12 июня 2014.
- на конференции “Non-associative algebra and Lie theory”, Оахака, Мексика, 26-30 января 2015.
- на конференции “Индо - Российская конференция по алгебре, теории чисел, дискретной математике и их приложений”, Москва, 15-17 октября 2014.

а также на следующих семинарах кафедры высшей алгебры механико-математического факультета МГУ:

- на научно-исследовательском семинаре кафедры высшей алгебры, 2009–2015 гг., неоднократно;
- на семинаре “Теория колец”, 2009–2015 гг., неоднократно;

Публикации

Основные результаты диссертации опубликованы в работах, список которых приведен в конце автореферата [1] – [5]. Работы [1], [2] – из перечня ВАК.

Структура диссертации Диссертационная работа состоит из четырех глав. Текст диссертации изложен на 93 листах. Список литературы содержит 72 наименования.

Основное содержание работы

Во **введении** даётся краткий исторический обзор и формулируются основные результаты диссертации.

В **главе 1** в **разделе 1.1** определяются основные понятия, терминология, принятая при изложении, и вспомогательные утверждения.

В **разделе 1.2** излагается понятие коммутанта нормальных подлуп и приводятся порождающие множества этого коммутатнта. Пусть $(L, \cdot)$ – лупа, тогда можно дополнительно рассматривать операции $\backslash, /$ такие, что $x \setminus (x/y) = y; \quad x \cdot (x \setminus y) = y; \quad (y \cdot x)/x = y; \quad (y/x) \cdot x = y$. Для каждого $x \in L$ определим биективные отображения $L_x, R_x, M_x : G \to G$:

$$L_x(y) = xy, R_x(y) = yx, M_x(y) = y \setminus x, y \in G.$$

Далее определим биективные отображения

$$L_{x,y} = L_{xy}^{-1} L_x L_y, \quad R_{x,y} = R_{xy}^{-1} R_x R_y, \quad M_{x,y} = M_{y \setminus x}^{-1} M_x M_y.$$

Следующее утверждение описывает взаимный коммутант нормальных подлуп.

Следствие 1.49. *Пусть L – лупа, A, B – нормальные подлупы лупы L, тогда*

$$[A,B]_L = Ng([a,b]_L, [b,a,x]_L, w_{u_1,u_2}(a)/w_{v_1,v_2}(a) :$$
$$w \in \{L,R,M\}, a \in A, b \in B, u_i/v_i \in B, x \in L),$$

Причем,

1) если L – IP-лупа, то

$$[A,B]_L = Ng([a,b]_L, L_{u_1,u_2}(a)/L_{v_1,v_2}(a) : a \in A, b \in B, u_i/v_i \in B);$$

2) если L – коммутативная лупа, то

$$[A,B]_L = Ng(w_{u_1,u_2}(a)/w_{v_1,v_2}(a) : w \in \{L,M\}, a \in A, u_i/v_i \in B);$$

3) если L – группа, то

$$[A,B]_L =< [a,b]_L : a \in A, b \in B > .$$

где $Ng(X)$ – наименьшая нормальная подлупа, содержащая множество X.

В **разделе 1.3** вводится понятие первичного радикала лупы и строго энгелева элемента.

Определение 1.54. *Лупа $(L,\cdot)$ называется первичной, если для любых ее двух нормальных подлуп A, B из равенства $[A,B]_L = E$ следует, что либо $A = E$, либо $B = E$, где E – единичная подлупа лупы L.*

Определение 1.59. *Пусть $(L,\cdot)$ – лупа. Элемент $a \in L$ называется строго энгелевым, если в любой последовательности $a_0, a_1, \ldots$ элементов лупы L, удовлетворяющей условию $a_0 = a, a_{i+1} \in [Ng(a_i), Ng(a_i)]_L$, начиная с некоторого номера все элементы равны 1.*

Основным результатом этого раздела является:

Теорема 1.61. *Первичный радикал $rad(L)$ лупы $(L,\cdot)$ совпадает с множеством всех строго энгелевых элементов лупы.*

В **разделе 1.4** получено описание первичного радикала Ω-лупы. Лупа $(L,+)$ (не обязательно, коммутативная или ассоциативная) называется лупой с операторами или Ω-лупой, если в L задана помимо сложения

еще система n-арных алгебраических операций Ω, причем для всех $\omega \in \Omega$ должно выполняться условие $00\ldots0\omega = 0$. Идеал P в Ω-лупе L называется Ω-первичным, если для любой операции $\omega \in \Omega$ и любых идеалов $I_1, \ldots, I_n \subseteq L$ из включения $(I_1, \ldots, I_n)\omega \subseteq P$ следует, что $I_j \subseteq P$ для некоторого $j = 1, 2, \ldots, n$. Пересечение всех Ω-первичных идеалов Ω-лупы L называется первичным радикалом Ω-$rad(L)$ лупы L. Обозначим через $\{a\}^L$ идеал Ω-лупы L, порождённый элементом $a \in L$. Подмножество M Ω-лупы L называется Ω-m-системой, если для любой операции $\omega \in \Omega$ и любых элементов $a_1, \ldots, a_n \in M$ существуют $a_i' \in \{a_i\}^L$, такие что $a_1' \ldots a_n'\omega \in M$. Теперь каждому элементу $a \in L$ поставим в соответствие подмножество $M_a \subseteq L$, которое получается следующим образом: $M_a = \cup_i A_i$, где

$$A_0 = a, A_i = \cup_{\lambda\in\Lambda} A_{i,\lambda}, A_{i,\lambda} = \{a_{i,j_1\ldots j_n} = a'_{i-1,j_1} \ldots a'_{i-1,j_n}\omega_\lambda\},$$

где ω_λ – n-арная операция, $a'_{i,j_k} \in \{a_{i,j_k}\}^L$, $a_{i,j_1}, \ldots, a_{i,j_n}$ – всевозможные наборы по n элементов из A_i.

Основной результат:

Теорема 1.72. *Пусть $a \in L$, где L – Ω-лупа, тогда эквивалентны следующие условия:*

1) $a \in \Omega$-$rad(L)$;

2) любая Ω-m-система, содержащая элемент a, содержит 0;

3) любая Ω-m-система M_a, соответствующая элементу a, содержит 0,

В начале **главы 2** излагается описание первичного радикала неассоциативных s-колец и показываются некоторые его свойства (в частности, его совпадение с множеством строго нильпотентных элементов s-кольца).

В **разделе 2.1** приводятся классические результаты для альтернативных колец. Отметим теорему, описывающую лупу обратимых элементов альтернативного кольца.

Теорема 2.13. *Пусть R – альтернативное кольцо с единицей, тогда множество обратимых элементов $U(R)$ является лупой Муфанг.*

Также рассмотрены различные свойства первичных альтернативных колец.

В **разделе 2.2** приведены различные свойства альтернативных луповых колец. Получено необходимое и достаточное условие того, что луповое кольцо является альтернативным.

Определение 2.20. *Лупа L для которой луповое кольцо KL, где K – коммутативное и ассоциативное кольцо с единицей и $charK \neq 2$,*

является альтернативным неассоциативным кольцом называется RA-лупой.

Будем называть упорядоченную тройку элементов лупы (a, b, c) неассоциативной, если равенство ассоциативности не выполняется для этих элементов (т.е. $a(bc) \neq (ab)c$). Соответственно, упорядоченная тройка (a, b, c) ассоциативна, если $a(bc) = (ab)c$.

Теорема 2.21. *Лупа L является RA-лупой тогда и только тогда, когда выполняются следующие условия:*

1. *если какие-либо элементы лупы ассоциативны в нектором порядке, то они ассоциативны в любом другом порядке;*

2. *если элементы $a, b, c \in L$ неассоциативны, то $a \cdot bc = ac \cdot b = c \cdot ab$;*

В **разделе 2.3** исследовано строение первичного радикала лупы обратимых элементов альтернативного кольца. Основной результат:

Теорема 2.38. *Если R – альтернативное кольцо с единицей, то для любой подлупы L лупы $U(R)$ выполняется включение $L \cap Z(R, rad\ R) \subseteq radL$.*

В **разделе 2.4** получено описание первичного радикала лупы обратимых элементов альтернативного кольца $GLL(2, R)$ (неассоциативный аналог теоремы А.В. Михалева и И.З. Голубчика). Основным результатом этого раздела является:

Теорема 2.40. *Пусть K – коммутативное и ассоциативное кольцо с единицей, $\mathcal{Z}(K)$ – кольцо матриц Цорна и $GLL(2, K)$ – лупа обратимых матриц из $\mathcal{Z}(K)$, тогда $rad\ GLL(2, K) = Z(\mathcal{Z}(K), rad\ \mathcal{Z}(K))$.*

В **главе 3** описаны некоторые криптографические схемы с открытым ключом. Расширены на лупы некоторые известные алгоритмы для криптографии, основанной на группах.

В **разделе 3.1** построена схема шифрования с открытым ключом над луповым кольцом.

Пусть K – кольцо с единицей (необязательно ассоциативное), Q – квазигруппа, KQ – луповое кольцо.

Участник A :

1. Конструирует автоморфизмы $\sigma \in AutK, \eta \in AutQ$, такие что $|\sigma| \geq t_3, |\eta| \geq t_5$, причем выполняются следующие условия на централизаторы $|C(\sigma) \setminus \langle\sigma\rangle| \geq t_4$ и $|C(\eta) \setminus \langle\eta\rangle| \geq t_6$, где t_3, t_4, t_5, t_6 - параметры безопастности.

2. Случайно выбирает автоморфизмы $\tau \in C(\sigma) \setminus \langle\sigma\rangle$ и $\omega \in C(\eta) \setminus \langle\eta\rangle$.

3. По τ и ω строит секретный автоморфизм $\varphi \in AutKQ$ так: для любого $h \in KQ$ вида $h = a_{q_1}q_1 + \cdots + a_{q_n}q_n$, пусть $\varphi(h) = \tau(a_{q_1})\omega(q_1) + \cdots + \tau(a_{q_n})\omega(q_n)$.

4. Выбирает элементы $a \in KQ, x \in KQ$ и вычисляет $\varphi(x)$ и $\varphi(a)$.

Открытым ключом участника A является:

$$\Big(\sigma, \eta, x, \varphi(x), a, \varphi(a)\Big).$$

Участник B:

1. Выбирает натуральные числа (i, j, k, l) и с помощью пар автоморфизмов (σ^i, η^j),(σ^k, η^l) строит сеансовые автоморфизмы $\psi, \chi \in AutKQ$.

2. Вычисляет $(\chi(a) \cdot \psi(x)$, $\chi(\varphi(a)) \cdot \psi(\varphi(x))$ и левый аннулятор $Ann\big(\chi(\varphi(a)) \cdot \psi(\varphi(x))\big)$.

3. Записывает исходный текст, который надо передать, в виде $m \in KL$ и вычисляет $m \cdot \Big[\chi(\varphi(a)) \cdot \psi(\varphi(x))\Big]$.

4. Отправляет для A криптограмму

$$\Big(\chi(a) \cdot \psi(x),\, m \cdot \Big[\chi\big(\varphi(a)\big) \cdot \psi\big(\varphi(x)\big)\Big]\Big)$$

Получив криптограмму, участник A расшифровывает её:

1. Используя секретный автоморфизм φ, вычисляет $\varphi\big(\chi(a) \cdot \psi(x)\big)$.

2. Расшифровывает посланный текст пользуясь тем, что χ, ψ и φ коммутируют, поскольку сеансовые автоморфизмы ψ, χ построены на степенях выбранных автоморфизмов σ, η, а секретный автоморфизм φ построен с помощью элементов из централизаторов для σ, η.

В **разделе 3.2** доказана гомоморфность данной схемы по отношению к одной из операций. В **разделе 3.3** приведен аналог схемы шифрования Эль-Гамаля над ППС-квазигруппой и доказана ее гомоморфность для медиальных квазигрупп. В **разделе 3.4** построена MQ-криптосхема над альтернативным кольцом. В **разделе 3.5** исследуются криптографичесие примитивы над лупами. В частности, схема выработки общего секретного

ключа над лупами Пейджа и схема шифрования с открытым ключом на основе покрытий лупы Муфанг.

В **приложении** приведена программа на языке компьютерной системы GAP для анализа параметров безопасности криптосхемы на луповом кольце.

Благодарности

Автор выражает глубокую благодарность своему научному руководителю д.ф.-м.н., профессору Александру Васильевичу Михалёву за выбор темы исследования, постановки задач и внимание к работе. Автор благодарен к.ф.-м.н., доценту Виктору Тимофеевичу Маркову за многочисленные советы и обсуждения работы. Автор приносит благодарность профессору Михаилу Михайловичу Глухову за ценные советы. Автор благодарен всему коллективу кафедры высшей алгебры за внимание к работе.

Работы автора по теме диссертации

[1] А. В. Грибов, П. А. Золотых, А. В. Михалёв, *Построение алгебраической криптосистемы над квазигрупповым кольцом*. Математические вопросы криптографии **1**, N.4 (2010), 23–33. *А. В. Грибову принадлежат разделы 3 и 5.*

[2] А. В. Грибов, П. А. Золотых, В. Т. Марков, А. В. Михалёв, С. С. Скаженик. *Квазигруппы и кольца в кодировании и построении криптосхем*. Прикладная дискретная математика **4**, (2012), 31–52. *А. В. Грибову принадлежат разделы 1 и 3.*

[3] А. В. Грибов, А. В. Михалёв, *Первичный радикал для луп и Ω-луп: I*. Фундамент. и прикл. мат. **19**, N. 2, (2014), 25–42.

А. В. Грибову принадлежат доказательсва основных результататов работы. А. В. Михалёву принадлежит постановка задач и общая редакция работы.

[4] А. В. Грибов, *Гомоморфность некоторых криптографических систем на основе неассоциативных структур*. Фундамент. и прикл. мат. **20**, N. 1, (2015), 131–139.

[5] А. В. Грибов, *Первичный радикал для альтернативных колец и луп*. Фундамент. и прикл. мат. **20**, N. 1, (2015), 141–162.