МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ИМЕНИ М.В. ЛОМОНОСОВА

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи

УДК 511.2, 511:51

Назаров Вадим Владиславович

Об использовании свойства коммутирования символа степенного вычета в схемах открытого распределения ключа

01.01.06 — математическая логика, алгебра и теория чисел

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата физико-математических наук

Москва, 2007

Работа выполнена на кафедре теории чисел Механико-математического факультета Московского государственного университета имени М.В. Ломоносова.

Научный руководитель: кандидат физико-математических наук, доцент М.А. Черепнёв

Официальные оппоненты: доктор физико-математических наук, профессор С.А. Степанов, кандидат физико-математических наук, доцент А.В. Устинов

Ведущая организация: Московский физико-технический институт (государственный университет)

Защита диссертации состоится 2 марта 2007 г. в 16 ч. 15 мин. на заседании диссертационного совета Д.501.001.84 в Московском государственном университете им. М.В. Ломоносова по адресу: 119992, ГСП-2, Москва, Ленинские горы, МГУ, Механико-математический факультет, ауд. 14-08.

С диссертацией можно ознакомиться в библиотеке Механико-математического факультета МГУ (главное здание МГУ, 14 этаж).

Автореферат разослан 2 февраля 2007 г.

Ученый секретарь
диссертационного совета
Д.501.001.84 в МГУ
профессор В.Н. Чубариков

Общая характеристика работы

Актуальность темы. В 1976 Диффи и Хеллман[1] предложили первую схему открытого распределения ключа, использующую возведение в степень по модулю большого простого числа. Стойкость схемы основана на вере в то, что задача Диффи-Хеллмана является вычислительно сложной, возможно, столь же сложной, как и задача дискретного логарифмирования. Схема Диффи-Хеллмана обобщается на любую полугруппу с эффективно вычислимой операцией, в которой задача дискретного логарифмирования вычислительно сложна. В частности, были рассмотрены кольца матриц над конечными полями[2], группа единиц кольца $\mathbb{Z}/n\mathbb{Z}$, где n – произведение двух различных простых[3], группа точек эллиптической кривой[4], группа классов мнимого квадратичного поля[5]. Шэйдлер[6] построил модификацию схемы Диффи-Хеллмана, использующую структуру полугруппы на идеалах вещественного квадратичного поля. Схемы типа Диффи-Хеллмана в различных группах являются на данный момент наиболее широко используемыми на практике схемами открытого распределения ключа.

В 1995 году В.М. Сидельниковым[7] была предложена новая схема открытого распределения ключа на основе некоммутативной ассоциативной группы $\mathbb{G}$. Пусть $\mathbb{G}_1, \mathbb{G}_2 \subset \mathbb{G}$ – коммутативные подгруппы; c – элемент $\mathbb{G}$, не лежащий в $\mathbb{G}_1, \mathbb{G}_2$.

<u>схема C</u>

A	**B**
Шаг 1. Выбирает $a_i \in \mathbb{G}_i$, $i = 1, 2$; вычисляет $d_A = a_1 * c * a_2$; отправляет d_A абоненту **B**	Шаг 1. Выбирает $b_i \in \mathbb{G}_i$, $i = 1, 2$; вычисляет $d_B = b_1 * c * b_2$; отправляет d_B абоненту **A**

[1] Diffie W., Hellman M.E., *New directions in criptography.* IEEE Transactions on Information Theory, 22 (1976), pp. 644-654

[2] Odoni R.W.K., Varadharajan V., Saunders P.W., *Public-key distribution in matrix rings.* Electr. Letters, 20 (1984), pp. 386-387

[3] McCurley K.S., *A key distribution scheme based on factoring.* Journ. Cryptology, 1 (1988), pp. 95-105

[4] Koblits N. *Elliptic curve cryptosystems.* Math. Comp, 48 (1987), pp. 203-209

[5] Buchmann J.A., Williams H.C. *A key-exchange system based on imaginary quadratic fields.* Journ. Cryptology, 1 (1988), pp. 107-118

[6] Jacobson M.J., Jr., Scheidler R., Williams H.C. *The efficiency and security of a Real Quadratic Field Based Key Exchange Protocol.* Public-Key Cryptography and Computational Number Theory (Warsaw, Poland), de Gruyter, 2001, pp. 89-112; Scheidler R., Buchmann J.A., Williams H.C. *A key-exchange protocol using real quadratic fields.* Journ. Cryptology, 7 (1994), pp. 171-199

[7] Сидельников В.М., Черепнёв М.А., Ященко В.В. *Системы открытого распределения ключа на основе некоммутативных полугрупп.* Доклады РАН, 332 (1993), Вып. 5, стр. 566-567.

Шаг 2. Получает d_B и вычисляет $\mathbb{K} = \mathbb{K}_A = a_1 * d_B * a_2$

Шаг 2. Получает d_A и вычисляет $\mathbb{K} = \mathbb{K}_B = b_1 * d_A * b_2$

Кроме общей схемы рассматривались два её частных случая, определяемые специальным выбором параметров: схема C1, в которой $c \notin \mathbb{G}_1 = \mathbb{G}_2$, и схема C2, в которой $c = 1$. В качестве группы была рассмотрена группа $\mathrm{GL}_n(\mathbb{F}_p)$, но при таком выборе схема оказалась нестойкой. Позднее В.М. Сидельниковым был изучен[8] усовершенствованный вариант схемы на основе "экспоненциального" представления группы $\mathrm{GL}_n(\mathbb{F}_p)$.

М.А. Черепнёв предложил[9] использовать некоммутативную операцию в полугруппе или в множестве, не имющем алгебраической структуры. Искомая операция была построена с использованием умножения в кольце целых чисел и символа Лежандра.

$$x * y = x \cdot y \cdot \left(\frac{\eta(x)}{\mu(y)}\right), \tag{1}$$

где η и μ – мультипликативные функции из $\mathbb{Z}$ в $\mathbb{Z}$ такие, что $\eta(-1) = \mu(-1) = 1$ О.Н. Василенко заметил, что по аналогии можно рассматривать и некоммутативную операцию в кольце целых чисел простого кругового поля на основе умножения в кольце и символа p-степенного вычета:

$$x * y = x \cdot y \cdot \left(\frac{\eta(x)}{\mu(y)}\right)_p, \tag{2}$$

где η и μ – мультипликативные функции из $\mathbb{Z}[\zeta_p]$ в $\mathbb{Z}[\zeta_p]$ такие, что $\eta(\zeta_p) = \mu(\zeta_p) = 1$.

При исследовании схем данного типа возникают три основные задачи, а именно: построение эффективно вычислимой ассоциативной некоммутативной операции, построение или описание коммутирующих подмножеств, анализ стойкости схемы.

Для описания коммутирующих подмножеств при использовании операций на основе символа степенного вычета возникает необходимость описать максимальные подмножества $\mathbb{Z}[\zeta_p]$, для любых элементов которых $(x, y)_\lambda = 1$. Эта задача в некотором смысле является усилением

[8] Сидельников В.М. *Системы распределения ключей на основе экспоненциального представления линейной группы* $\mathrm{GL}_n(\mathbb{F}_p)$. www.cryptography.ru

[9] Черепнёв М.А. *Схемы открытого распределения ключа на основе некоммутативной группы.* Дискретная математика Т.15 (2003), Вып. 2., 47-51

задачи нахождения кондуктора[10] элемента $x \in \mathbb{Z}[\zeta_p]$ ($x \equiv 1 \pmod{\lambda}$), то есть нахождения числа $u \in \mathbb{N}$, такого что $(x\,,\,y)_\lambda = 1$ для всех $y \equiv 1 \pmod{\lambda^u}$.

При решении задач эффективного вычисления и анализа стойкости для операций на основе символа степенного вычета необходимо уметь оценивать сложность вычисления символов степенного и норменного вычетов в простых круговых полях для аргументов общего и специального вида. Для вычисления символа степенного вычета от аргументов произвольного вида были предложены два алгоритма – один из них вероятностный,[11] а второй детерминированный.[12] Оба алгоритма имеют полиномиальную сложность, если в качестве параметра рассматривать длину записи входа. Однако, если взять в качестве растущего параметра степень расширения поля, то сложность этих алгоритмов растёт как минимум экспоненциально. Более того, если p и q – большие простые числа, такие, что p делит $q-1$; $a \in \mathbb{Z}$; $\mathcal{Q}$ – один из простых идеалов $\mathbb{Z}[\zeta_p]$, лежащих над q, то сложность вычисления символа p-степенного вычета $\left(\frac{a}{\mathcal{Q}}\right)_p$ эквивалентена[13] сложности вычисления индексов в подгруппе порядка p группы $(\mathbb{Z}/(q-1)\mathbb{Z})^*$.

Аналогичную (полиномиальную от длины входа и экспоненциальную от степени расширения поля) сложность имеют и известные алгоритмы вычисления символа норменного вычета: основанный на K-теории[14] и использующий закон взаимности Артина-Хассе. [9]

Для операций на основе символа степенного вычета М.А. Черепнёв придумал алгоритм построения коммутирующих элементов "экспериментальным путём" и привёл пример элементов, для которых вычисление символа степенного вычета сводится к вычислению символа Якоби. [9]

В диссертации изучается свойство коммутирования символа степенного вычета и свойства символа норменного вычета в простых круговых полях, а также возможности использования указанных символов в схемах открытого распределения ключа на основе некоммутативной операции.

Цель работы. Целью работы является описание коммутирующих

---

[10] Sharify R.T. *Minimal conductors of Kummer extensions by roots of unity elements.* Journ. Ramanujan Math. Soc. 16 (2001), № 2, pp. 101–117 и ссылки из указанной работы

[11] Horowits J. *Applications of Cayley graphs, bilinearity and higher-order residues to cryptology.* Staford Univercity, PhD. Thesis, 2004

[12] Squirell D. *Computing power residue symbol.* Reed College, Undergraduate Thesis, 1997

[13] Adelman L.M., Pomerance C., Rumely R.S. *On distinguishing prime numbers from composite numbers.* Annals of Mathematics, 117 (1983), pp. 173-206

[14] Daberkow M., *On computations in Kummer extensions.* Journ. Symbolic Computations 31 (2001), pp. 113-131

множеств и анализ стойкости схемы при использовании операций на основе символа степенного вычета, а также исследование возможности применения в схеме операций на основе символа норменного вычета.

Методы исследования. Работа опирается на исследования в теории алгебраических чисел и алгоритмической алгебраической теории чисел. Для исследования свойств символов степенного и норменного вычета применяются методы алгебраической теории чисел, для оценки сложностей предложенных алгоритмов и стойкости схем - методы теории сложности вычислений.

Научная новизна. Полученные результаты работы являются новыми и получены автором самостоятельно. Основными из них являются следующие:

Доказана теорема о критерии вскрытия схемы открытого распределения ключа на основе некоммутативной операции, построенной с использованием некоторой двуместной мультипликативной функции. С помощью теоремы впервые показано принципиальное различие между стойкостями схем $C1$ и $C2$.

Доказана нестойкость схемы при использовании класса операций на основе логарифмических функций, подобных предложенной ранее.[15]

Доказана теорема о структуре максимальных коммутирующих подмножеств символа степенного вычета в кольцах целых чисел простых круговых полей, позволяющая, в частности, эффективно их строить. Также вычислена их мощность.

Получены формулы для полиномиального вычисления символа норменного вычета от аргументов специального вида в кольцах целых чисел простых круговых полей, выражающие символ норменного вычета через классические частные Ферма.

Построен новый алгоритм вычисления символа норменного вычета от аргументов общего вида, построенный на основе разложения по мультипликативному базису элементов мультипликативной группы некоторого фактор-кольца кольца целых чисел простого кругового поля и дана оценка сложности его работы.

Получены условия, необходимые для стойкости схемы при использовании операций с символами степенного и норменного вычетов. Показано, что эти условия будут выполнены, если вычисления в схеме осу-

[15] Черепнёв М.А. *Схемы открытого распределения ключа на основе некоммутативной операции.* Тезисы докладов XIII Международной конференции "Проблемы теоретической кибернетики". Казань 27-31 мая 2002 г. стр. 190

ществляются за время, зависящее полиномиально от логарифма степени расширения поля. В случае символа норменного вычета построен условный полиномиальный от логарифма степени расширения поля алгоритм вычислений по протоколу схемы, основанный на полученных формулах для символа норменного вычета.

Теоретическая и практическая ценность. В диссертации доказываются теоремы и выводятся формулы, которые могут найти применение в алгебраической теории чисел. Построенные алгоритмы с оценками сложности могут использоваться в вычислительной теории чисел. Доказанные свойства схем распределения ключа могут быть полезны специалистам по математическим методам защиты информации.

Апробация работы. Результаты настоящей диссертации неоднократно докладывались на научно-исследовательском семинаре по теории чисел под руководством Ю.В. Нестеренко и Н.Г. Мощевитина (механико-математический факультет МГУ) и на семинаре "Теоретико-числовые вопросы криптографии" под руководством М.А. Черепнева и Ю.В. Нестеренко (там же) в 2002-06 гг. Кроме того, часть результатов диссертации была доложена на конференции "Математика и безопасность информационных технологий" (МГУ, октябрь 2003 г).

Публикации. Результаты диссертации опубликованы в работах [1-4], список которых приводится в конце автореферата.

Структура и объём работы. Диссертация изложена на 91 странице. Она состоит из введения, четырёх глав и списка литературы, включающего 33 наименования.

Содержание работы

В главе 2 предложен метод построения некоммутативной ассоциативной операции на основе коммутативной полугруппы $\mathbb{G}$ и мультипликативной функции. С помощью предложенного метода получается в том числе и операция (2). Пусть функция $F : \mathbb{G} \times \mathbb{G} \longrightarrow \mathbb{G}$ мультипликативна по обоим аргументам на своей области определения. Пусть также для всех $g_1, g_2, g_3 \in \mathbb{G}$, таких, что F определена на парах (g_1, g_2), (g_2, g_3), $(F(g_1, g_2), g_3)$, $(g_1, F(g_2, g_3))$, выполнены равенства

$$F(F(g_1, g_2), g_3) = 1\,; F(g_1, F(g_2, g_3)) = 1\,.$$

Тогда операция $*$, заданная соотношением

$$g_1 * g_2 = g_1 \cdot g_2 \cdot F(g_1, g_2)\,, \tag{3}$$

будет ассоциативной, а в случае, если F не симметрична, то и некоммутативной. Поэтому множество $\mathbb{G}$ с операцией типа (3) может применяться в схеме C.

В работе показано, что в полугруппе $(\mathbb{G}, \cdot)$ элементы d_A и d_B делятся на c, элемент $(d_A/c) * c$ делится на d_A, а элемент $(d_B/c) * c$ делится на d_B. Кроме того доказано, что параметры схемы C связаны соотношениями:

Лемма 1.
(1) Пусть существует $\tau_1 \in \mathbb{G}$ *такой, что* $\tau_1 \cdot F(b_1, a_2) = F(a_2, b_1)$ *; тогда*

$$\frac{d_A}{c} * d_B = \mathbb{K} \cdot \tau_1 \cdot \frac{\frac{d_A}{c} * c}{d_A} \tag{4}$$

(2) Пусть существует $\tau_2 \in \mathbb{G}$ *такой, что* $\tau_2 \cdot F(a_1, b_2) = F(b_2, a_1)$ *; тогда*

$$\frac{d_B}{c} * d_A = \mathbb{K} \cdot \tau_2 \cdot \frac{\frac{d_B}{c} * c}{d_B}\,. \tag{5}$$

Из полученных формул следует основная теорема главы 2:

Теорема 1. *Пусть для* $i \in \{1, 2\}$ *существует* $\tau_i \in \mathbb{G}$ *с указанными в лемме свойствами. Тогда задача нахождения общего секретного ключа* $\mathbb{K}$ *по открытой информации в схеме* C *с использованием операции (3) эквивалента задаче находждения элемента* τ_i *по открытой информации.*

При рассмотрении схемы C1 очевидно получаем, что $\tau_i = 1$, поэтому схема нестойка.

В главе 3 изучаются схемы на основе функций из $\mathbb{Z}[\zeta_p]$ в $\mathbb{Z}$, обладающих логарифмическим свойством по модулю p. В работе[15] М.А. Черепнёв привёл пример операции на основе символа степенного вычета, которая является частным случаем операции (3). Пусть $a \in \mathbb{Z}$, взаимно прост с p ,

$$\Phi_p(a) = \frac{a^{p-1} - 1}{p} \pmod p$$

частное Ферма по модулю p. Пусть $\mathcal{J}$ – фиксированный идеал $\mathbb{Z}[\zeta_p]$, тогда

$$x * y = x \cdot y \cdot \left(\frac{\mathrm{N}(x)}{\mathcal{J}}\right)_p^{\Phi_p(\mathrm{N}(y))} \tag{6}$$

является некоммутативной ассоциативной операцией, определённой на элементах, чьи главные идеалы взаимно просты с $\mathcal{J}$ и (λ).

В диссертации показано, что операция (6) является частным случаем операции

$$x * y = x \cdot y \cdot \zeta_p^{f_1(x)\cdot f_2(y)} \tag{7}$$

где функции $f_i : \mathbb{Z}[\zeta_p] \longrightarrow \mathbb{Z}$ обладают свойствами
$f_i(xy) \equiv f_i(x) + f_i(y) \pmod p$; $f_i(\zeta_p) \equiv 0 \pmod p$ для $i = 1, 2$.

Обозначим через $\mathbb{E}$ – подмножество $\mathbb{Z}[\zeta_p]$, на котором определена операция (7) и рассмотрим следующие подмножества $\mathbb{E}$:

$\mathbb{H}_{0,0} = \{x \in \mathbb{E} \,|\, f_1(x) \equiv f_2(x) \equiv 0 \pmod p\}$,
$\mathbb{H}_0 = \{x \in \mathbb{E} \,|\, f_1(x) \equiv 0;\ f_1(x) \not\equiv 0 \pmod p\}$,
$\mathbb{H}_p = \{x \in \mathbb{E} \,|\, f_1(x) \not\equiv 0;\ f_2(x) \equiv 0 \pmod p\}$,
$\mathbb{H}_i = \{x \in \mathbb{E} \,|\, f_1(x) \cdot f_2(x)^{-1} \equiv i \pmod p\};\ i = 1 \ldots p-1$.

В работе доказана следующая теорема о коммутирующих множествах:

Теорема 2. *Для любого коммутирущего множества $\mathbb{M}$ относительно операции (7) существует i: $0 \le i \le p$, такое что $\mathbb{M}$ является подмножеством, собственным или несобственным, множества $\mathbb{H}_{0,0} \cup \mathbb{H}_i$.*

На основе этой теоремы, а также соотношений из леммы 1, в работе построен эффективный алгоритм нахождения общего секретного ключа по открытой информации. Из его существования следует

Теорема 3. *При использовании операции типа (7) схема* C *является нестойкой.*

В главе 4 изучается схема C, использующая операцию (2) в случае, когда функции μ и η совпадают. В первом разделе главы изучаются коммутирующие множества относительно данной операции, а во втором – строится алгоритм атаки на схему, из которого выводятся условия, необходимые для её стойкости.

При изучении свойства коммутирования элементов основополагающим является следствие из степенного закона взаимности:[16] элементы x и y коммутируют тогда и только тогда, когда $(\eta(x)\,,\, \eta(y))_\lambda = 1$.

[16] Artin E., Tate J. *Class field theory* Notes of a Seminar at Princeton, 1951/52. Harvard University, Mathematics Department, 1961.

Обозначим через $\mathcal{Z}$ подмножество $\mathbb{Z}[\zeta_p]$, состоящее из элементов, взаимно простых с λ. Так как идеал (λ) – простой, то $\mathcal{Z}$ является полугруппой относительно умножения.

Определение 1. *Максимальным тривиальным подмножеством символа норменного вычета назовём подмножество $\mathcal{M} \subseteq \mathcal{Z}$, удовлетворяющее двум условиям:*

(1) для любых $x, y \in \mathcal{M}$ выполнено $(x\,,\,y)_\lambda = 1$;

(2) если $z \in \mathcal{Z}$ таков, что для любого $x \in \mathcal{M}$ выполнено $(z\,,\,x)_\lambda = 1$, то $z \in \mathcal{M}$.

Замечание. В силу мультипликативности символа норменного вычета по обоим аргументам, любое максимальное тривиальное подмножество будет полугруппой по умножению. Поэтому будем говорить о *максимальных тривиальных полугруппах* символа норменного вычета.

В диссертации доказано, что на $\mathcal{Z}$ символ норменного вычета имеет аддитивный период, равный λ^p:

Теорема 4. *Пусть $x,\, y,\, z \in \mathcal{Z}$; $x \equiv z \pmod{\lambda^p}$, тогда*

$$(x\,,\,y)_\lambda = (z\,,\,y)_\lambda\,;\ (y\,,\,x)_\lambda = (y\,,\,z)_\lambda\,.$$

Принимая во внимание теорему 4, при изучении свойств символа норменного вычета можно рассматривать не сами аргументы символа, а содержащие их классы фактор кольца $\mathbb{Z}[\zeta_p]/(\lambda^p)$. Так как символ норменного вычета мультипликативен по обоим аргументам, то при описании его максимальных тривиальных полугрупп можно использовать мультипликативную структуру группы $(\mathbb{Z}[\zeta_p]/(\lambda^p))^*$. Пусть $\omega_i := 1 - \lambda^i$ для натуральных i. В книге [16] показано, что любой элемент мультипликативной группы $\mathbb{Q}_p^*(\zeta_p)$ поля $\mathbb{Q}_p(\zeta_p)$ единственным образом представляется в виде произведения

$$\lambda^{\gamma_\lambda} g \prod_{i=1}^{\infty} {\omega_i}^{\gamma_i}\,,$$

где g – произвольный корень из 1 степени $p-1$, лежащий в $\mathbb{Q}_p(\zeta_p)$, γ_λ целое, γ_i целые неотрицательные. Для группы $(\mathbb{Z}[\zeta_p]/(\lambda^p))^*$ в диссертации доказана

Теорема 5. *Любой $x \in \mathbb{Z}[\zeta_p]$, взаимно простой с (λ), единственным образом представим в виде*

$$x \equiv {g_0}^{p\gamma_0} \cdot {\omega_1}^{\gamma_1} \cdot \ldots \cdot {\omega_{p-1}}^{\gamma_{p-1}} \pmod{(\lambda^p)}\,, \tag{8}$$

где $g_0 \in \mathbb{Z}$ *– произвольный фиксированный первообразный корень по модулю* p^2, $0 \le \gamma_0 \le p-2$, $0 \le \gamma_i \le p-1$ *для* $i = 1, \ldots, p-1$.

Из теорем 4 и 5 выводится основной результат о структуре максимальных тривиальных полугрупп:

Теорема 6. *Любая максимальная тривиальная полугруппа символа норменного вычета имеет вид:*

$$\mathcal{M} = \{x \in \mathcal{Z} \,|\, x = {g_0}^{p \cdot \nu_0} \cdot {\xi_1}^{\nu_1} \cdot \ldots \cdot {\xi_{\frac{p-1}{2}}}^{\nu_{\frac{p-1}{2}}} + \nu_p \cdot \lambda^p\}, \qquad (9)$$

где g_0 *– первообразный корень по модулю* p^2; $\xi_1, \ldots, \xi_{\frac{p-1}{2}}$ *– мультипликативно независимые в* $(\mathbb{Z}[\zeta_p]/(\lambda^p))^*$ *элементы порядка* p, *такие что* $(\xi_i\,,\,\xi_j)_\lambda = 1$; $\nu_0 = 0, \ldots, p-2$; $\nu_i = 0, \ldots, p-1$ *для* $i = 1, \ldots, \frac{p-1}{2}$; $\nu_p \in \mathbb{Z}[\zeta_p]$.
Обратно, пусть $\xi_1, \ldots, \xi_{\frac{p-1}{2}}$ *произвольные мультипликативно независимые в* $(\mathbb{Z}[\zeta_p]/(\lambda^p))^*$ *элементы порядка* p, *такие что* $(\xi_i\,,\,\xi_j)_\lambda = 1$; $g_0 \in \mathbb{Z}$ *произвольный первообразный корень по модулю* p^2, *тогда множество вида*

$$\mathcal{M} = \{{g_0}^{p\,\nu_0} \cdot {\xi_1}^{\nu_1} \cdot \ldots \cdot {\xi_{\frac{p-1}{2}}}^{\nu_{\frac{p-1}{2}}} + \nu_p \cdot \lambda^p\},$$

где $\nu_0 = 0, \ldots, p-2$; $\nu_i = 0, \ldots, p-1$ *для* $i = 1, \ldots, \frac{p-1}{2}$; $\nu_p \in \mathbb{Z}[\zeta_p]$ *будет являться максимальной тривиальной полугруппой символа норменного вычета.*

Определение 2. *Элементы* $\xi_1, \ldots, \xi_{\frac{p-1}{2}}$ *из (9) назовём основными образующими максимальной тривиальной полугруппы.*

Замечание. Для каждой максимальной тривиальной полугруппы набор основных образующих не уникален. Максимальные тривиальные полугруппы могут быть построены за время, полиномиальное от p.

Каждое из коммутирующих подмножеств, используемых в схеме, будет являться подмножеством полного прообраза какой-либо максимальной тривиальной полугруппы: $\mathbb{G}_1 \subseteq \eta^{-1}(\mathcal{M}_1)$, $\mathbb{G}_2 \subseteq \eta^{-1}(\mathcal{M}_2)$ где $\mathcal{M}_1$ и $\mathcal{M}_2$ имеют вид (9). В предположении, что для $\mathcal{M}_1$ и $\mathcal{M}_2$ известны какие-либо наборы основных образующих, построена атака, позволяющая находить по открытой информации общий секретный ключ $\mathbb{K}$. Для реализации алгоритма атаки необходимо осуществить $O(p^3)$ арифметических операций в $\mathbb{Z}/p\mathbb{Z}$, $O(p^2)$ вычислений символа норменного вычета

и $O(1)$ вычислений символа степенного вычета. Сложность работы этого алгоритма, обозначаим через $T_A(p)$.

Обозначим через $T(p)$ сложность вычисления по протоколу схемы, через $T_I(p)$ – сложность нахождения основных образующих максимальных тривиальных полугрупп $\mathcal{M}_1$ и $\mathcal{M}_2$ по открытому описанию коммутирующих подмножеств $\mathbb{G}_1, \mathbb{G}_2$, используемых в схеме. Тогда общая сложность предложенной атаки на схему равна $T_I(p) + T_A(p)$ – сначала находятся основные образующие по открытой информации, а потом реализуется алгоритм атаки. Поэтому для обеспечения стойкости схемы необходимо, хотя, возможно, и не достаточно, чтобы функция $T(p)$ имела бы полиномиально меньший порядок роста, чем $T_A(p) + T_I(p)$ (под полиномиально меньшим порядком роста имеем ввиду то, что функция $U(p)$ является полиномом от некоторого параметра, а $V(p)$ растёт по крайней мере субэкспоненциально от того же параметра, и обозначаем такое отношение: $U(p) \ll V(p)$). В результате, для стойкости схемы необходимо выполнить хотя бы одно из двух условий:

Условие 1. *Коммутирующие подмножества* $\mathbb{G}_1$ *и* $\mathbb{G}_2$ *заданы так, что* $T(p) \ll T_I(p)$.

Условие 2. *Легальные абоненты используют при вычислениях только те элементы, для которых* $T(p) \ll T_A(p)$.

Отметим, что при известных основных образующих и при использовании для вычислений символов степенного и норменного вычета стандартных алгоритмов (от произвольных аргументов) ни одно из этих условий не выполнено. Главным членом как в $T(p)$, так и в $T_I(p) + T_A(p)$ будет сложность алгоритма вычисления символа p-степенного вычета.

С другой стороны, оба эти условия выполнены, если вычисления по протоколу схемы осуществимы за время, полиномиальное от $\log p$. Действительно, во-первых, число основных образующих каждой из максимальных тривиальных полугрупп равно $\frac{p-1}{2}$, поэтому $T_I(p)$ растёт не медленнее, чем p, и следовательно выполнено условие 1. Во-вторых, $T_A(p)$ растёт не медленнее, чем $O(p^3)$, поэтому выполнено условие 2.

Как уже было отмечено выше, известные алгоритмы вычисления символа норменного вычета $(x\,,\,y)_\lambda$ от произвольных аргументов x, y имеют сложность, растущую, как полином от длины записи x и y, и быстрее, чем полином от $\log p$. Однако, ни в статье М. Даберкова [9], ни в статье М.А. Черепнёва [14] не даны точные оценки сложности предложенных алгоритмов в зависимости от степени расширения поля.

В третьем разделе четвёртой главы диссертации построен альтернативный алгоритм вычисления символа норменного вычета в кольце целых чисел $\mathbb{Z}[\zeta_p]$ простого кругового поля для элементов из $\mathcal{Z}$. Алгоритм работает за $O(p^3)$ проверок сравнимости с 0 по модулю натурального числа, не превосходящего p в $\mathbb{Z}$ и за $O(p^3)$ арифметических операций в $\mathbb{Z}/p\mathbb{Z}$. Вычисление символа норменного вычета сводится к вычислению семейства функций из $\mathbb{Z}[\zeta_p]$ в $\mathbb{Z}$, обладающих логарифмическим свойством по модулю p. Пусть идеал (x) взаимно прост с (λ). Тогда разложение (8) для x^{p-1} имеет вид:

$$x^{p-1} \equiv {\omega_1}^{-\gamma_1 \pmod p} \cdot \ldots \cdot {\omega_{p-1}}^{-\gamma_{p-1} \pmod p} \pmod{(\lambda^p)} \qquad (10)$$

Рассмотрим для $i = 1, ..., p-1$ функции $e_i(x) = -\gamma_i \pmod p$ (оператор $\pmod p$ означает взятие наименьшего положительного вычета по модулю p):

$$e_i : \mathcal{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}\,.$$

В силу свойств показателей и того, что порядок ω_i в $(\mathbb{Z}[\zeta_p]/(\lambda^p))^*$ равен p, $e_i(x)$ обладают логарифмическим свойством по модулю p. Кроме того, для всех $i \neq 1$ $e_i(\zeta_p) = 0$. В диссертации показано, что функции $e_i(x)$ для различных i связаны соотношениями:

Теорема 7. *Пусть* $X_0 = x_0^{-1} \pmod p$, $x' = 1 + x_1 X_0 \lambda + \ldots + x_{p-2} X_0 \lambda^{p-2}$, *тогда для* $k = 1, \ldots, p-1$ *выполнено*

$$1 + e_k(x)\lambda^k \equiv x' {x_0}^{(p-1)^2} {\omega_1}^{e_1(x)} \ldots {\omega_{k-1}}^{e_{k-1}(x)} \pmod{(\lambda^{k+1})}\,. \qquad (11)$$

На основе этой теоремы построен алгоритм, вычисляющий по $x \in \mathcal{Z}$ набор значений $\mathcal{E}(x) = (e_1(x), \ldots, e_{p-1}(x))$ за $O(p^3)$ операций в $\mathbb{Z}/p\mathbb{Z}$ и за $O(p)$ операций нахождения остатка от деления на p в $\mathbb{Z}$.

В главе 5 изучаются свойства символа норменного вычета и возможность применения этого символа для построения некоммутативной операции в $\mathbb{Z}[\zeta_p]$.

По аналогии с операцией (2) в качестве примера операции (3) можно взять следующую операцию в $\mathcal{Z}$:

$$x * y = x \cdot y \cdot (\mu(x)\,,\, \eta(y))_\lambda\,, \qquad (12)$$

где μ, η – мультипликативные функции, такие что $\mu(\zeta_p) = \eta(\zeta_p) = 1$. Так как символ норменного вычета имеет на $\mathcal{Z}$ аддитивный период λ^p, то для обеспечения ассоциативности операции (12) достаточно взять

функции μ и η с указанными выше свойствами, но действующие не из $\mathbb{Z}[\zeta_p]$ в $\mathbb{Z}[\zeta_p]$, а из $\mathbb{Z}[\zeta_p]$ в $(\mathbb{Z}[\zeta_p]/(\lambda^p))^*$. В частности, можно использовать функции $\mu_{i,j}(x) = \omega_j^{e_i(x)} \pmod{(\lambda^p)}$ для $i = 2, \ldots, p-1$, $j = 1, \ldots, p-1$, где ω_j и $e_i(x)$ определены выше. Опять рассматриваем операцию в случае, когда функции μ и η совпадают:

$$x * y = x \cdot y \cdot (\eta(x)\,,\, \eta(y))_\lambda\ . \tag{13}$$

В диссертации доказаны критерии коммутирования относительно операции (13) и стойкости схемы C при использовании этой операции:

Теорема 8. (критерий коммутирования)
$x * y = y * x$ тогда и только тогда, когда

$$(\eta(x)\,,\, \eta(y))_\lambda = 1$$

Теорема 9. (критерий стойкости)
Задача нахождения общего секретного ключа $\mathbb{K}$ по открытой информации эквивалентна задачам нахождения по открытой информации символов норменного вычета

$$\tau_1{}' = (\eta(a_2)\,,\, \eta(b_1))_\lambda \ \text{ и } \ \tau_2{}' = (\eta(b_2)\,,\, \eta(a_1))_\lambda$$

Критерии коммутирования и стойкости совпадают с соответствующими критериями при использовании операции (2) с совпадающими функциями μ и η. Значит, совпадает структура коммутирующих множеств, а следовательно алгоритм нахождения общего секретного ключа по открытой информации из главы 4 диссертации применим и в данном случае. Поэтому если, как и ранее, будем обозначать через $T_A(p)$ сложность алгоритма атаки, через $T_I(p)$ сложность получения набора основных образующих максимальных тривиальных полугрупп $\mathcal{M}_i$ по открытому описанию коммутирующих множеств $\mathbb{G}_i$, а через $T(p)$ сложность вычислений по протоколу схемы C, то для достижения стойкости схемы необходимо, хотя, возможно, не достаточно, выполнить одно из условий 1 или 2. Для быстрых вычислений может быть использована доказанная в диссертации теорема, связывающая символ норменного вычета с классическими частными Ферма по модулю p:

Теорема 10. *Пусть $a, b, c, d, \alpha \in \mathbb{Z}$; p не делит ac; $\alpha \geq 1$; $\Delta = ad - bc$. Тогда*
1) Если $\alpha \geq 2$, то $(a + b\lambda^\alpha\,,\, c + d\lambda^\alpha)_\lambda = 1$.
2) Если $\alpha = 1$, то
если $bd \not\equiv 0, \Delta \not\equiv 0$, то $(a + b\lambda\,,\, c + d\lambda)_\lambda = \zeta_p^{\Phi_p(b)\frac{b}{a} - \Phi_p(d)\frac{d}{c} + \Phi_p(\Delta)\frac{\Delta}{ac}}$.

если $bd \not\equiv 0, \Delta \equiv 0$, *то* $(a+b\lambda\,,\, c+d\lambda)_\lambda = \zeta_p^{\Phi_p(a)\frac{b}{a} - \Phi_p(c)\frac{d}{c}}$.
если $b \equiv 0, d \not\equiv 0$, *то* $(a+b\lambda\,,\, c+d\lambda)_\lambda = \zeta_p^{\Phi_p(a)\frac{d}{c}}$.
если $b \not\equiv 0, d \equiv 0$, *то* $(a+b\lambda\,,\, c+d\lambda)_\lambda = \zeta_p^{-\Phi_p(c)\frac{b}{a}}$.
если $b \equiv d \equiv 0$, *то* $(a+b\lambda\,,\, c+d\lambda)_\lambda = 1$.
Все сравнения и все частные в показателях рассматриваются по модулю p.

Замечание. Техника, используемая в доказательстве теоремы, позволяет получить формулы и для символа норменного вычета от элементов другого вида (тоже специального).

Используя полученные формулы, можно вычислять символ норменного вычета вида $(a+b\lambda^\alpha\,,\, c+d\lambda^\alpha)_\lambda$ за время, полиномальное от $\log p$. В диссертации доказана следующая теорема о сложности вычислений по протоколу схемы:

Теорема 11. *Пусть функция* η *и множества* $\mathbb{G}_1, \mathbb{G}_2$ *таковы, что в каждом* $\mathbb{G}_i$ *есть подмножество* $\mathbb{G}_i{}'$, *элементы которого удовлетворяют свойствам:*

(1) Элементы $\mathbb{G}_i{}'$ *записываются целочисленной линейной комбинацией элементов* $1, \zeta, \ldots, \zeta^{p-1}$, *содержащей полиномиальное от* $\log p$ *число ненулевых коэффициентов;*

(2) Выбор случайного элемента из $\mathbb{G}_i{}'$ *по открытому описанию* $\mathbb{G}_i$ *осуществляется за время, полиномиальное от* $\log p$;

(3) Входом для функции η *является линейная комбинация элементов* $1, \zeta, \ldots, \zeta^{p-1}$. *Она возвращает значения в виде разложения по* λ*-базису. В случае, если поданная на вход комбинация имеет полиномиальное от* $\log p$ *число ненулевых коэффициентов, значение вычисляется за время, полиномиальное от* $\log p$;

(4) Значением $\eta(g_i)$ *для любого* $g_i \in \mathbb{G}_i{}'$ *будет элемент вида* $u+v\lambda$, *где* $u, v \in \mathbb{Z}$, *причём* $(u, p) = 1$.

Тогда $T(p)$ *растёт, как полином от* $\log p$. *При* $p \equiv 3 \pmod 4$ *вычисления по протоколу схемы реализуются с помощью детерминированного алгоритма, а при* $p \equiv 1 \pmod 4$ *– с помощью вероятностного алгоритма.*

При доказательстве теоремы используется разработанная автором диссертации техника проведения арифметических операций над "короткими" элементами круговых полей, за время, полиномиальное от $\log p$.

Если удастся построить множества $\mathbb{G}_i$ и функцию η, удовлетворяющие условиям теоремы 11, то полученная схема будет стойкой относительно предложенного в диссертации алгоритма атаки. Однако пока построить примеры таких множеств и такой функции не удалось.

Автор глубоко благодарен своему научному руководителю кандидату физико-математических наук, доценту Михаилу Алексеевичу Черепнёву за привитый интерес к области исследования, полезные советы и постоянное внимание к работе.

Работы автора по теме диссертации

[1] В.В. Назаров. *Об использовании символа степенного вычета в схемах открытого распределения ключа.* Вестник Московского Университета, сер.1, Математика, Механика. №3 (2005), стр. 9 - 13.

[2] В.В. Назаров. *Схемы открытого распределения ключа на основе некоммутативной операции.* Дискретная математика Т.18 (2006), Вып. 4, стр. 149 - 156

[3] В.В. Назаров. *О некоторых вычислительных свойствах символа норменного вычета в простых круговых полях.* Депонировано в ВИНИТИ 31.10.2006, № 1289-В2006, 24 стр

[4] В.В. Назаров. *Схемы открытого распределения ключа на основе некоммутативной операции. Использование в схемах данного типа символа степенного вычета.* Математика и безопасность информационных технологий. Материалы конференции в МГУ 23-24 октября 2003 г. М.; изд-во МЦНМО, 2004, стр. 179 - 182