МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра компьютерной алгебры и теории чисел

Эллиптические кривые и их криптографические приложения

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 421 группы

направления **02.03.01 - математика и компьютерные науки**

механико-математического факультета

Бабушкина Александра Юрьевича

Научный руководитель
доцент, к.ф.-м.н., доцент _____ В. В. Кривобок
подпись, дата

Зав. кафедрой
зав. каф., к.ф.-м.н., доцент _____ А. М. Водолазов
подпись, дата

Саратов 2019

Введение. В последнее время одна из областей теории чисел и алгебраической геометрии - эллиптические кривые (точнее, теория эллиптических кривых над конечными полями) - нашла применение в криптографии. Во многих отношениях эллиптические кривые - естественный аналог мультипликативных групп, но более удобный, так как существует большая свобода в выборе эллиптической кривой, чем в выборе конечного поля. Целью этой работы является рассмотрения криптосистем на эллиптических кривых над расширенными полями. Бакалаврская работа состоит из введения, трех разделов, заключения и списка литературы. Первая раздел - вводные сведения, основные обозначения, термины и понятия из теории эллиптических кривых. Есть глава посвященная конечным полям. Второй раздел - изучение эллиптических кривых. В третьем разделе исследуются разработанные алгоритмы криптосистем на эллиптических кривых.
Основное содержание работы. В первом разделе выпускной работы вводится понятие конечного поля, доказывается существование мультипликативных образующих конечных полей.

Пусть F_q обозначает поле, которое состоит из конечного числа q элементов. Очевидно, что конечное поле не может иметь характеристику 0, так что характеристика F_q - простое число p. Тогда F_q содержит в себе простое поле $F_p = Z/pZ$ и, следовательно, является векторным пространством (разумеется, конечномерным) над F_p. Пусть f обозначает его размерность как F_p-векторного пространства. Выбор базиса позволяет установить взаимно однозначное соответствие между элементами этого f-мерного векторного пространства и множеством всех f-выборок элементов из F_p. Поэтому в F_q должно быть p^f элементов. Тогда, q - степень характеристики p. Далее увидим, что для каждой степени $q = p^f$ простого числа p существует единственное (с точностью до изоморфизма) поле из q элементов. Но сначала покажем мультипликативный порядок элементов в множестве F_q^* ненулевых элементов конечного поля. Под «порядком» ненулевого элемента имеем ввиду наименьшую положительную его степень, равную 1.

Существование мультипликативных образующих конечных полей. В F_q имеется $q-1$ ненулевых элементов. Согласно определению поля они образуют абелеву группу по умножению. Это значит, что произведение двух не равных нулю элементов - не нуль. Число элементов в группе делится на порядок любого элемента - это факт, общий для всех конечных групп.

Предложение 1.1. *Порядок любого $a \in {F_q}^*$ делит $q-1$.*

Предложение 1.2. *Каждое конечное поле имеет образующий элемент. Если g - образующий элемент ${F_q}^*$, то g^j - также образующий, тогда и только тогда, когда НОД$(j, q-1) = 1$. В частности, всего в F_q имеется $\varphi(q-1)$ различных образующих элементов.*

Следствие. *Для каждого простого p существует такое целое число g, что его степени пробегают все не равные нулю классы вычетов по модулю p.*

Предложение 1.3. *Существует такая последовательность простых чисел p, что случайно выбранный в $F_p{}^*$ элемент g оказывается образующим с вероятностью, стремящейся к нулю с ростом p.*

Предложение 1.4. *Если F_q есть поле с $q = p^f$ элементами, то каждый его элемент удовлетворяет уравнению $X^q - X = 0$ и F_q - это в точности множество корней этого уравнения. Обратно, для любой степени простого $q = p^f$ поле разложения над F_p многочлена $X_q - X$ есть поле из q элементов.*

Лемма. *Для любых элементов a, b поля характеристики p выполняется соотношение $(a + b)^p = a^p + b^p$.*

Предложение 1.5. *Пусть F_q - конечное поле из $q = p^f$ элементов и пусть σ - отображение F_q, при котором элементу a сопоставляется $a_p : \sigma(a) = a_p$. Тогда σ есть автоморфизм поля F_q(т.е. взаимно однозначное отображение поля в себя, сохраняющее сложение и умножение). Элементы F_q, не изменяющиеся при действии σ - это в точности элементы простого поля F_p; f-я степень σ есть тождественное отображение, и меньшие степени σ этим свойством не обладают.*

Предложение 1.6. *Если α - любой элемент F_q, то все сопряженные с α над F_p элементы (т.е. элементы F_q, являющиеся вместе с α корнями нормированного неприводимого многочлена с коэффициентами из F_p) имеют вид $\sigma^j(\alpha) = \alpha^{p^j}$.*

Предложение 1.7. *Подполя F_{p^f} - это поля F_{p^d} для $d|f$. Если элемент $\alpha \in F_{p^f}$ присоединяется к F_p, то получается одно из этих полей. Теперь нетрудно доказать формулу, которая используется при нахождении числа неприводимых многочленов данной степени.*

Предложение 1.8. *Для любого $q = p^f$ многочлен $X^q - X$ разлагается в $F_p[X]$ в произведение всех нормированных неприводимых многочленов степеней d, делящих f.*

Следствие. *Если f есть простое число, то в $F_p[X]$ существует всего $(p^f - p)/f$ неприводимых нормированных многочленов степени f.*

Заметим, что $(p^f - p)/f$ при простом f - целое число, так как малая теорема Ферма гарантирует, что $p^f \equiv p(mod f)$. Пусть n - число неприводимых нормированных многочленов степени f. Согласно предложению, многочлен $X^{p^f} - X$ степени p^f есть произведение n многочленов степени f и p неприводимых многочленов $X - a, a \in F$, степени 1. Приравнивая показатели степеней, получаем равенство $p^f = nf + p$, из которого следует искомая формула для n. Пусть теперь f - не обязательно простое число. Через n_d обозначим число неприводимых нор-

мированных многочленов степени d над F_p. Тогда имеем $n_f = (p_f - \sum dn_d)/f$, где суммирование распространяется на все делители d числа $f, d < f$. Распространим теперь временные оценки, касающиеся арифметики по модулю p, на конечные поля общего вида.

Предложение 1.9. *Пусть F_q, где $q = p^f$, есть конечное поле и $F(X)$ - неприводимый многочлен степени f над F_p. Тогда два элемента из F_q можно поделить или перемножить за $O(log^3 q)$ двоичных операций. Если k - целое неотрицательное число, то элемент поля F_q можно возвести в степень k за $O((logk)(log^3 q))$ двоичных операций.*

Второй раздел посвящен эллиптическим кривым. Предполагаем, что K - поле либо поле R вещественных чисел, либо поле Q рациональных чисел, либо поле C комплексных чисел, либо поле F_q из $q = p^r$ элементов.

Замечания. *Имеется общая форма уравнения эллиптической кривой, которая применима при любом поле: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$; в случае, когда $charK \neq 2$, ее можно привести к виду $y^2 = x^3 + ax^2 + bx + c$ (или к виду $y^2 = x^3 + bx + c$, если $K > 3$). В случае, когда поле K имеет характеристику 2, это уравнение преобразуется либо к виду $y^2 + cy = x^3 + ax + b$, либо к виду $y^2 + xy = x^3 + ax^2 + b$.*

Перед обсуждением конкретных примеров эллиптических кривых над разными полями отметим чрезвычайно важное свойство множества точек эллиптической кривой: они образуют абелеву группу. Чтобы объяснить наглядно, как это получается, временно будем полагать, что $K = R$, т.е. что эллиптическая кривая - обычная плоская кривая (с добавлением еще одной точки O «в бесконечности»).

Определение. *Пусть E - эллиптическая кривая над вещественными числами, и пусть P и Q - две точки на E. Определим точки $-P$ и $P + Q$ по следующим правилам.*

1. Если P - точка в бесконечности O, то $-P = O$ и $P + Q = Q$, т.е. O - тождественный элемент по сложению («нулевой элемент») группы точек. В следующих пунктах предполагается, что ни P, ни Q не являются точками в бесконечности.

2. Точки $P = (x, y)$ и $-P$ имеют одинаковые x-координаты, а их y-координаты различаются только знаком, т.е. $-(x, y) = (x, -y)$. Из (1) сразу следует, что $(x, -y)$ - также точка на E.

3. Если P и Q имеют различные x-координаты, то прямая $I = PQ$ имеет с E еще в точности одну точку пересечения R (за исключением двух случаев: когда она оказывается касательной в P, и тогда полагаем $R = P$, или касательной в Q, и тогда полагаем $R = Q$). Определяем теперь $P + Q$ как точку

$-R$, т.е. как отражение от оси x третьей точки пересечения. Геометрическое построение, дающее $P+Q$.

4. Если $Q=-P$ (т.е. x-координата Q та же, что и у P, а y-координата отличается лишь знаком), то полагаем $P+Q=O$ (точке в бесконечности; это является следствием правила 1).

5. Остается возможность $P=Q$. Тогда считаем, что I - касательная к кривой в точке P. Пусть R - единственная другая точка пересечения I с E. Полагаем $P+Q=-R$ (в качестве R берем P, если касательная прямая в P имеет «двойное касание», т.е. если P есть точка перегиба кривой).

Задача дискретного логарифмирования, как и задача разложения на множители, используется во многих алгоритмах криптографии с открытым ключом. Предложенная в 1976 году У. Диффи (W. Diffe) и М. Хеллманом (M. Heilman) для установления сеансового ключа, эта задача послужила основой для создания протоколов шифрования и цифровой подписи, доказательств с нулевым разглашением и других криптографических протоколов. Заметим, что в криптографии эта задача возникла еще в 1950-х годах, когда вместо роторных машин стали использоваться регистры сдвига, и нужно было обозначить место конкретного элемента в данной последовательности сдвигов. Безопасность соответствующих криптосистем основана на том, что, зная числа a, x, p вычислить $ax(modp)$ легко (например, алгоритмом Парного возведения в степень), а решить задачу дискретного логарифмирования трудно. Рассмотрим некоторые методы решения этой задачи.

ρ-Метод Полларда. ρ-метод Полларда может использоваться для решения задачи дискретного логарифмирования. При этом случайное отображение f должно обладать не только сжимающими свойствами, но и вычислимостью логарифма (логарифм числа $f(c)$ можно выразить через неизвестный логарифм x и $log_a f(c)$). Для дискретного логарифмирования в качестве случайного отображения f чаще всего используются «ветвящиеся» отображения, например

$$f(c)=\begin{cases} ac & \text{для } c<p/2, \\ bc & \text{для } c>p/2. \end{cases}$$

При $c<p/2$ имеем $log_a f(c)=log_a c+1$, при $c>p/2-log_a f(c)=log_a c+x$.

Алгоритм. Дискретное логарифмирование ρ-методом Полларда. Вход. Простое число p, число a порядка r по модулю p, целое число $b, 1<b<p$; отображение f обладающее сжимающими свойствами и сохраняющее вычислимость логарифма. Выход. Показатель x, для которого $a^x \equiv b(modp)$, если такой показатель существует.

1. Выбрать произвольные целые числа u, v и положить $c \leftarrow a^u b^v (mod p)$, $d \leftarrow c$.

2. Выполнять $c \leftarrow f(c)(mod p)$, $d \leftarrow f(f(d))(mod p)$, вычисляя при этом логарифмы для c и d как линейные функции от x по модулю r, до получения равенства $c \equiv d(mod p)$.

3. Приравняв логарифмы для c и d, вычислить логарифм x решением сравнения по модулю r. Результат: x или «Решений нет».

Пример 1. *Решим задачу дискретного логарифмирования* $10^x = 64(mod 107)$, *используя* ρ*-метод Полларда. Порядок числа* 10 *по модулю* 107 *равен* 53. *Выберем отображение* $f(c) = 10c(mod 107)$ *при* $c < 53$, $f(c) \equiv 64c(mod 107)$ *при* $c > 53$. *Пусть* $u = 2$, $v = 2$.

Метод Гельфонда и Сильвера-Полига-Хеллмана

Теорема 2.1. *Пусть целые числа* a *и* b *таковы, что* $1 < a, b < p$, *где число простое, порядок числа* a *по модулю* p *равен* r *и* $a^x = b(mod p)$. *Тогда число* x *можно найти, выполнив не более чем* $2(\sqrt{r} + log_2 r) - 1$ *операций умножения по модулю* p.

Пример 2. *Решим задачу дискретного логарифмирования* $7^x \equiv 167(mod 587)$ *методом Гельфонда. Порядок числа* 7 *по модулю* 587 *равен* $r = 293$.

Теорема 2.2. *Пусть целые числа* a *и* b *таковы, что* $1 < a, b < p$, *где число* p *простое, порядок числа* a *по модулю* p *равен* r *и* $a^x = b(mod p)$. *Пусть, кроме того, число* $r = r_1 r_2$. *Тогда число* x *можно найти, выполнив не более чем* $2(\sqrt{r_1} + \sqrt{r_2}) + 6log_2 r_1 r_2 + 2log_2 r_1 - 1$ *операций умножения по модулю* p.

Метод базы разложения. Алгоритм Диксона можно использовать для решения задачи дискретного логарифмирования. В основе этого метода лежит следующее свойство поля F_p и кольца Z целых чисел. Если для некоторых целых чисел a, bc выполняется равенство $ab = c$ в кольце Z, то выполняется и сравнение $ab \equiv c(mod p)$ по модулю любого простого числа p. Кроме того, из равенства $a^x = b$ и сравнения $a^y \equiv b(mod p)$ следует $x \equiv y(mod r)$, где r - порядок числа a по модулю p.

В третьем разделе рассмотрена криптография на эллиптических кривых. Для эллиптических кривых аналогом умножения двух элементов группы ${F_q}^*$ служит сложение двух точек эллиптической кривой E, определенной над F_q. Таким образом, аналог возведения в степень k элемента из F_q - это умножение точки $P \in E$ на целое число k. Возведение в k-ю степень в ${F_q}^*$, методом повторного возведения в квадрат можно осуществить за $O(logk log^3 q)$ двоичных операций.

Аналогично, покажем, что кратное $kP \in E$ можно найти за $O(logklogq)$ двоичных операций методом повторного удвоения.

Пример 3. *Чтобы найти* $100P$, *записываем* $100P = 2(2(P+2(2(2(P+2P)))))$ *и приходим к цели, производя* 6 *удвоений и* 2 *сложения точек на кривой.*

Предложение 3.1. *Пусть эллиптическая кривая* E *определена уравнением Вейерштрасса над конечным полем* F_q. *Если задана точка* P *на* E, *то координаты* kP *можно вычислить за* $O(logklog^3q)$ *двоичных операций.*

Замечание 3.1. *Если известно число* N *точек на эллиптической кривой* E *и если* $k > N$, *то в силу равенства* $NP = O$ *можем заменить* k *его наименьшим неотрицательным вычетом по модулю* N; *в этом случае временная оценка заменяется на* $O(log^4q)$. *Рене Шуф (R. Schoof) предложил алгоритм, вычисляющий* N *за* $O(log^8q)$ *двоичных операций.*

Кодировать наши открытые тексты точками некоторой заданной эллиптической кривой E, определенной над конечным полем F_q и осуществить это простым, и систематическим способом так, чтобы открытый текст m (который можно рассматривать как целое число из некоторого интервала) можно было легко прочитать, зная координаты соответствующей точки P_m. Заметим, что это «кодирование» - не то же самое, что засекречивание. Позднее будем рассматривать способы шифрования точек P_m открытого текста. Однако законный пользователь системы должен быть в состоянии восстановить m после дешифрования точки шифртекста. Следует сделать два замечания. Во-первых, не известно детерминистического полиномиального (по log_q) алгоритма для выписывания большого числа точек произвольной эллиптической кривой E над F_q. Однако, как увидим далее, существуют вероятностные алгоритмы с малой вероятностью неудачи. Во-вторых, порождать случайные точки на E недостаточно: чтобы закодировать большое число возможных сообщений m, необходим какой-то систематический способ порождения точек, которые были бы связаны с m определенным образом, например, чтобы x-координата имела с m простую связь.

Определение. *Пусть* E *- эллиптическая кривая над* F_q *и* B *- точка на* E. *Задачей дискретного логарифмирования на* E *(с основанием* B*) называется задача нахождения для данной точки* $P \in E$ *такого целого числа* $x \in Z$*(если оно существует), что* $xB = P$.

Вполне возможно, что задача дискретного логарифмирования на эллиптической кривой окажется более трудной для решения, чем задача дискретного логарифмирования в конечных полях. Наиболее сильные методы, разработанные для конечных полей, по-видимому, не работают в случае эллиптических кривых. Это обстоятельство по-особенному отчетливо проявляется в случае полей

характеристики 2. Специальные методы решения задачи дискретного логарифмирования в F_{2r}^* позволяют сравнительно легко вычислять дискретные логарифмы и, следовательно, вскрывать криптосистемы, если r не выбрано очень большим. Аналогичные системы, использующие эллиптические кривые над F_{2r}, судя по всему, являются надежными при значительно меньших значениях r. Так как имеются практические причины (связанные с устройством ЭВМ и программированием) предпочтительности арифметических операций над полями F_{2r}, криптосистемы с открытым ключом, рассматриваемые ниже, могут оказаться более удобными для практического применения, чем системы, основанные на задаче дискретного логарифмирования в $F_q{}^*$. До 1990 г. единственными известными алгоритмами дискретного логарифмирования на эллиптических кривых были те, которые работают в любой группе и не используют особенности ее строения. Эти алгоритмы с экспоненциальным временем работы применимы к случаям, когда порядок группы делится на большое простое число. Однако впоследствии Менезес (Menezes), Окамото (Okamoto) и Вэнстон (Vanstone) предложили новый подход к задаче дискретного логарифмирования на эллиптической кривой E, определенной над F_q. А именно, они использовали спаривание Вейля для вложения группы E в мультипликативную группу некоторого расширения F_{q^k} поля F_q. Это вложение сводит задачу дискретного логарифмирования на E к соответствующей задаче для $F_{q^k}^*$.

Теперь опишем аналоги систем с открытым ключом, основанные на задаче дискретного логарифмирования на эллиптической кривой, определенной над конечным полем F_q. Аналог ключевого обмена Диффи-Хеллмана. Предположим, что Алиса и Боб хотят договориться о ключе, которым будут впоследствии пользоваться в некоторой классической криптосистеме. Прежде всего открыто выбирают какое-либо конечное поле F_q и какую-либо эллиптическую кривую E над ним. Ключ строится по случайной точке P на этой эллиптической кривой. Если есть случайная точка P, то, например, ее x-координата дает случайный элемент F_q, который можно затем преобразовать в r-разрядное целое число в p-ичной системе счисления (где $q = p^r$), а это число может служить ключом в их классической криптосистеме. (Здесь пользуемся словом «случайный» в неточном смысле; хотим сказать, что выбор из некоторого большого множества допустимых ключей произволен и непредсказуем). Нужно выбрать точку P так, чтобы все сообщения друг другу были открытыми и все же никто, кроме них двоих, ничего бы не знал о P. Алиса и Боб первым делом открыто выбирают точку $B \in E$ в качестве «основания»; B играет ту же роль, что образующий g в системе Диффи-Хеллмана для конечных полей. Однако, не требуем, чтобы B была образующим элементом в группе точек кривой E. Эта группа может и не быть

циклической. Даже если она циклическая, не нужно тратить время на проверку того, что B - образующий элемент (или даже на нахождение общего числа N точек, которое не понадобится в последующем). Хотелось бы, чтобы порожденная B подгруппа была большой, предпочтительно того же порядка величины, что и сама E. Пока что предположим, что B - взятая открыто точка на E весьма большого порядка (равного либо N, либо большому делителю N).

Пример 4. *Точка $B = (0, 0)$ является точкой бесконечного порядка на эллиптической кривой $E : y^2 + y = x^3 - x$ и фактически порождает всю группу рациональных точек на E.*

Пример 5. *Точка $B = (0, 0)$ является точкой бесконечного порядка на E : $y^2 + y = x^3 + x^2$ и порождает всю группу рациональных точек.*

Далее, выбираем большое простое число p (или, если наша эллиптическая кривая определена над расширением K поля Q, выбираем некоторый простой идеал в K) в рассматриваем редукцию E и B по модулю p. Точнее, для всех p, за исключением нескольких малых простых чисел, коэффициенты в уравнении для E имеют взаимно простые с p знаменатели и, следовательно, могут рассматриваться как коэффициенты в уравнении по модулю p. Если сделать замену переменных, приведя полученное уравнение над F_p к виду $y^2 = x^3 + ax + b$, то кубический многочлен в правой части не будет иметь кратных корней (за исключением нескольких малых простых p) и дает поэтому эллиптическую кривую над F_p (которую будем обозначать $E(modp)$). Координаты точки B, будучи также приведенными по модулю p, дают точку на эллиптической кривой $E(modp)$, которую будем обозначать $B(modp)$. При использовании этого второго способа, раз и навсегда фиксируем E и B и за счет этого получаем много различных возможностей посредством изменения простого p.
С какой вероятностью «случайная» точка B на «случайной» эллиптической кривой оказывается порождающим элементом? Или, в случае второго метода выбора (E, B), какова вероятность того, что (для случайного p) точка B при редукции по модулю p дает образующий элемент кривой $E(modp)$? Этот вопрос близок к следующему вопросу о мультипликативных группах конечных полей: пусть целое b фиксировано, а простое p случайно; какова вероятность того, что b - образующий в F_p^*? Вопрос изучался как для конечных полей, так и для эллиптических кривых. Как упоминалось выше, описанные криптосистемы могут быть надежными, даже если точка B не является порождающим элементом. Фактически нужно, чтобы в циклической группе, порождаемой B, задача дискретного логарифмирования не была эффективно разрешима. Это будет так

(т.е. все известные методы решения задачи дискретного логарифмирования в произвольной абелевой группе оказываются слишком медленными), если порядок B делится на очень большое простое число, скажем, имеющее порядок величины, близкий к N. Один из способов гарантировать, что наш выбор B является надлежащим (а фактически, что B порождает эллиптическую кривую) - это взять такую эллиптическую кривую и такое конечное поле, чтобы число точек N было простым числом. Тогда всякая точка $B \neq O$ будет порождающим элементом. Если использовать первый из описанных выше методов, то при фиксированном F_p можно продолжать выбор пар (E, B), пока не найдется такая, для которой число точек на E есть простое число (что можно определить одним из тестов на простоту). Если применять второй метод, то для фиксированной глобальной эллиптической кривой E над Q можно продолжать выбирать простые p, пока не найдем кривую $E(modp)$, число точек на которой - простое. Как долго придется ждать? Этот вопрос аналогичен следующему вопросу о группах F_p^*: является ли $(p-1)/2$ простым числом, т.е. верно ли, что любой элемент, отличный от ± 1, - либо порождающий, либо квадрат порождающего элемента? Ни для эллиптических кривых, ни для конечных полей вопрос пока не получил явного ответа, однако в обоих случаях предполагается, что вероятность выбора p с требующимся свойством есть $O(1/logp)$.

Замечание 3.2. *Для того чтобы E $(modp)$ имела простой порядок N при большом p, надо выбирать E так, чтобы она имела тривиальное кручение, т.е. чтобы на ней не было точек конечного порядка, кроме O. В противном случае N будет делиться на порядок периодической подгруппы.*

Заключение. В заключении стоит сказать, что сегодня все стандарты асимметричной криптографии базируются на арифметике абелевой группы точек эллиптической кривой над конечным полем. Эллиптическая криптография, кроме традиционных криптосистем, основанных на проблеме дискретного логарифмирования на эллиптической кривой, стала основой для построения криптосистем с новыми свойствами. В частности, были предложены криптосистемы на гиперэллиптических кривых, и криптосистемы, основанные на спариваниях точек эллиптических кривых. Гиперэллиптические кривые - это кривые более высокого рода, которые являются обобщением понятия эллиптической кривой. При этом, если билинейная криптография ведет в сторону сверх-больших полей (до десятков килобит), то гиперэллиптические кривые дают реальную перспективу использовать малые поля (десятки бит). Целью данной работы являлось изучение криптосистем на эллиптических кривых над расширенными полями. Исследована функциональная полнота для данного класса эллиптических кривых и показано, что он позволяет строить все основные криптографические алго-

ритмы и протоколы; предложены протоколы шифрования с открытым ключом, приведены примеры возможного использования разработанных криптографических алгоритмов и протоколов в информационных системах для управления ключами.