Министерство образования и науки РФ

Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Казанский (Приволжский) федеральный университет»

ИНСТИТУТ МАТЕМАТИКИ И МЕХАНИКИ
им. Н.И.Лобачевского

КАФЕДРА АЛГЕБРЫ И МАТЕМАТИЧЕСКОЙ ЛОГИКИ
Специальность: 010100 - математика
Специализация: 01.01.06 – математическая логика, алгебра и теория чисел

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
(Магистерская диссертация)

Криптосистема NICE и некоторые ее модификации

Работа завершена:
“___”_____ 2014 г. _____ (Фу Сяомин)

Работа допущена к защите:
Научный руководитель
доктор физ.-мат. наук,
Профессор кафедры алгебры
и математической логики КФУ

“___”_____ 2014 г. _____ (Тронин С. Н.)

Заведующий кафедрой
Доктор физ.-мат. наук,
Профессор
“___”_____ 2014 г. _____ (Арсланов М.М.)

Казань-2014

ОГЛАВЛЕНИЕ

Введение 4
Глава 1. Криптография с открытым ключом 6
§ 1. Односторонние функции 6
§ 2. Шифрование по RSA 10
§ 3. Цифровые подписи 13
§ 4. Подпись RSA 15
§ 5. Хэш-функции 15
§ 6. Шифрование по Эль-Гамалю 19
§ 7. Подпись Эль-Гамаля 21
§ 8. Подпись DSA 22
§ 9. Подпись Шнорра 24
§ 10. Протокол обмена ключами Диффи-Хеллмана 26
Глава 2. Группа классов идеалов 29
§ 1.Необходимые алгебраические понятия 29
§ 2. Алебраические числа и дедекиндовы кольца 40
§ 3. Группа классов идеалов: определения и основные свойства 43
§ 4. Квадратичные поля и их группы классов 45
§ 5. Гомоморфизмы между группами классов идеалов 50
§ 6. Действительные и мнимые квадратичные поля 51
Глава 3. Криптосистема NICE для мнимых квадратичных полей 56
§ 1. Идейная основа криптосистемы NICE 56
§ 2. Алгоритм умножения элементов в группе классов идеалов 57
§ 3. Алгоритм вычисления гомоморфизма π 58
§ 4. Протокол шифрования 60
Глава 4. Криптосистема NICE
для действительных квадратичных полей 62

§ 1. Модификация криптосистемы NICE 62
§ 2. Арифметика идеалов 67
§ 3. Особенности криптосистемы NICE для действительных квадратичных полей 68
ЛИТЕРАТУРА 74

Введение

В современной криптографии с открытым ключом широко используются различные алгебраические методы. В 1900-х годах началось применение алгебраической теории чисел. В частности, стали использоваться некоторые свойства идеалов в кольцах целых алгебраических чисел. Известно,что группы классов идеалов колец целых алгебраических чисел во многих случаях являются трудновычислимыми. Именно это и позволило использовать их в криптографии с открытым ключом в криптосистеме NICE. Слово NICE является аббревиатурой для New Ideal Coset Encryption.

Криптосистема NICE была введена в статье [11] в 1999 году. В последствии эта криптоистема изучалась и усовериненствовалась в ряде других статей и диссертаций, например, в [16], [17], [13].

Целью нашей работы является подробное изложение криптосистемы NICE для мнимых квадратичных полей, и ее модификации REAL-NICE для действительных квадратичных полей.

Опишем содержания работы.

В главе 1 дан обзор главных идей и алгоритмов криптографии с открытым ключом. Использованы книги [4], [9], [10].

В главе 2 приводится сводка необходимых для понимания дальнейшего сведений из алгебры и алгебраической теории чисел. В параграфе 1 содержится минимум информации о коммутативных кольцах и их идеалах. В парагрифе 2 напоминаются основные факты об алгебраических числах. В частности, определяются поля алгебраических чисел, и формулируются теоремы о том,что такие кольца являются дедекиндовыми, что факторкольца по максимальным идеалам являются конечными полями, и что каждый идеал в таких кольцах порождается двумя элементами. В следующем

параграфе описываются дробные идеалы в кольцах целых алгебраических чисел.

Группа классов идеалов кольца определяется как факторгруппа группы обратимых дробных идеалов по подгруппе главных дробных идеалов. Именно такие группы используются в криптосистеме NICE.

Отметим, что для написания этой главы, помимо учебников [2], [1], [3], [6], [7] и монографии [8], использовался обзор М.М.Глухова [5] в журнале “Математические вопросы криптографии”, 2010 год, а такие материалы статей [11] и [13].

В главе 3 дается подробное описание криптосистемы NICE для мнимых квадратичных полей. Мы следуем работе [11] и диссертации [16].

В главе 4 описывается модификация NICE для действительных квадратичных полей. Мы следуем работе [13], которая опирается на диссертацию [17]. Глава начинается с описания NICE, которое несколько отличается от того, что изложено в главе 3. Это необходимо для сравнения случаев мнимых и действительных квадратичных полей. Основное отличие состоит в том, что в случае мнимых полей алгоритмы шифрования и дешифрования являются детерминистскими, а в случае действительных полей вероятностными. Это связано с особенностями строения групп классов идеалов для порядков в действительных квадратичных полях.

Исследование криптосистемы NICE и ее модификаций — это новое перспективное направление в современной криптографии, использующее глубокие теоремы из алгебраической теории чисел. Окончательные результаты, пригодные для практического использования, пока не получены, но, судя по всему, активная работа в этом направлении продолжается.

Глава 1. Криптография с открытым ключом.

§ 1. Односторонние функции

Понятие односторонней функции является центральным в криптографии с открытыми ключами.

Пусть дана функция

$$f : X \longrightarrow Y, \tag{1}$$

Определенная на большом конечном множестве X, принимающая значения в большом конечном множестве Y, для которой существует обратная функция

$$x = f^{-1}(y), \tag{2}$$

Эта функция называется *односторонней*, если вычисление по формуле (1) — простая задача, требующая немного времени, а вычисление по формуле (2) — задача сложная, требующая привлечения массы вычислительных ресурсов, например, $10^6 - 10^{10}$ лет работы современного суперкомпьютера.

Более точное математическое определение можно найти, например, в [4, с.30].

В настоящее время не известно ни одной конкретной функции, для которой было бы строго доказано, что она является односторонней. Однако имеется несколько функций, для которых свойство односторонности предполагается. Эти функции широко применяются в криптографии.

В качестве примера предположительно односторонней функции рассмотрим следующую функцию:

$$y = a^x \pmod p, \tag{3}$$

где p некоторое простое число, $x \in \{0, 1, \ldots, p-2\}$, a — целое число из множества $\{1, 2, \ldots, p-1\}$, которое является первообразным корнем по

модулю p. В этом случае существует обратная функция из $\{1, \ldots, p-1\}$ в $\{0, \ldots, p-2\}$, которая обозначается так:

$$x = \log_a y \pmod p \tag{4}$$

Эта функция называется *дискретным логарифмом.*

Для того чтобы обеспечить трудность вычисления по (4) при использовании лучших современных компьютеров, в настоящее время используются числа размером более 512 бит.

На практике часто применяются другие функции, похожие на односторонние функции, например, так называемые хеш-функции, оперирующие с существенно более короткими числами порядка 60-120 бит.

Покажем, что вычисление по (3) может быть выполнено достаточно быстро. Начнем с примера вычисления числа $a^{16} \pmod p$. Мы можем записать

$$a^{16} \pmod p = \left(\left(\left(a^2\right)^2\right)^2\right)^2 \pmod p$$

т.е. значение данной функции вычисляется всего за 4 операции умножения вместо 15 при "наивном" варианте $a \cdot a \cdot \ldots \cdot a$. На этом основан общий алгоритм.

Для описания алгоритма введем величину $t = \lfloor log_2 \rfloor$ — целую часть $log_2 x$. Вычисляем числа ряда

$$a,\ \ a^2,\ \ a^4,\ \ a^8, \ldots, a^{2t} \pmod p. \tag{5}$$

В ряде (5) каждое число получается путем умножения предыдущего числа на себя по модулю p. Напишем показатель степени x в двоичной системе счисления:

$$x = (x_t x_{t-1} \ldots x_1 x_0)_2.$$

Тогда число $y = a^x \pmod p$ может быть вычислено как

$$y = \prod_{i=0}^{t} a^{x^i \cdot 2^i} \pmod p \tag{6}$$

(все вычисления проводятся по модулю p).

Ещё одним новым понятиям является понятие *функции с секретом.* Иногда ещё употребляется термин *функция с ловушкой. Функции с секретом* K называется функция $F_K : X \to Y$, зависящая от параметра K и обладающая тремя свойствами:

а) существует полиномиальный алгоритм вычисления значения $F_K(x)$ для любых K и x;

б) не существует полиномиального алгоритма инвертирования F_K при неизвестном K;

в) существует полиномиальный алгоритм инвертирования F_K при неизвестном K.

Про существование функций с секретом можно сказать то же самое, что сказано про одностроние функции. Для практических целей криптографии было построено несколько функций, которые могут оказаться функциями с секретом. Для них свойство б) пока строго не доказано, но считается, что задача инвертирования эквивалентна некоторой давно изучаемой трудной математической задаче. Наиболее известной и популярной из них является теоретико-числовая функция, на которой построен шифр RSA.

Примение функций с секретом в криптографии позволяет:

1) организавать обмен шифрованными сообщениями с использованием только открытых каналов связи, т.е отказаться от секретных каналов связи для предварительного обмена ключами;

2) включить в задачу вскрытия шифра трудную математическую задачу и тем самым повысить обоснованность стойкости шифра;

3) решать новые криптографические задачи, отличные от шифрования(электро цифровая подпись и др).

Опишем, например, как можно реализовать п.1) Пользователь A, который хочет получать шифрованные сообщения, должен выбрать какую-нибудь функцию F_K с секретом K. Он сообщает всем заинтересованным (например, публикует) описание функции F_K в качестве своего алгоритма шифрования. Но при этом значение секрета K он никому не сообщает и держит в секрете. Если теперь пользователь B чочет послать пользователю A зашищаемую информацию $x \in X$, то он вычисляет $y = F_K(x)$ и посылает y по открытому каналу пользователю A. Поскольку A для своего секретом K умеет инвертировать F_K, то он вычисляет x по полученному y.Никто другой не знает K и поэтому в силу свойства б) функции с секретом не сможет за полиномиальное время по известному шифрованному сообщению $F_K(x)$ вычислить защищаемую информацию x.

Описанную систему называют *криптосистемой с открытым ключом,* поскольку алгоритм штфрования F_K является общедоступным или открытым. В последнее время такие криптосистемы ещё называют *асимметричными,* поскольку в них есть асимметрия в алгоритмах: алгоритмы шифрования и дешифрования различны. В отличие от таких систем традиционные шифры называется *симметричными:* в них ключ для шифрования и дешифрования один и тот же. Для асимметричных систем алгоритм шифрования общеизвестен, но восстановить по нему алгоритм дешифрования за полиномиальное время невозможно.

Описанную выше идею Диффи и Хеллман предложили использовать также для электронной цифровой подписи сообщений, которую невозможно подделать за полиномиальное время. Пусть пользователю A необходимо

подписать сообщение x. Он, зная секрет K, находит такое y, что $F_K(y) = x$, и вместе с сообщение x посылает y пользователю B в качестве своей цифровой подписи. Пользователь B хранит y в качестве доказательства того, что A подписал сообщение x.

Сообщение, подписанное цифровой подписью, можно представлять себе как пару (x, y), где x — сообщение, y — решение уравнения $F_K(y) = x$, $F_K : X \to Y$ — функция с секретом, известная всем взаимодействующим абоненам. Из определения функции F_K очевидны следующие полезные свойства цифровой подписи:

1) подписать сообщение x, т.е решить уравнение $F_K(y) = x$, может только абонент — обладатель данного секрета K; другими словами, подделать подписать невозможно;

2) проверить подлинность подписи может любой абонент, знающий открытый ключ, т.е саму функцию F_K;

3) при возникновении споров отказаться от подписи невозможно в силу её неподделываемости;

4) подписанные сообщение (x, y) можно, не описаясь ущерба, пересылать по любым каналам связи.

§ 2. Шифрование по RSA

Алгоритм RSA — первый из алгоритмов шифрования с открытым ключом, достойно выдержал испытание временем. Криптостойкость алгоритма RSA базируется на сложности проблемы факторизации, хотя и не в полной мере.

Предположим, Алиса считает нужным разрешить всем желающим отправлять ей секретные сообщения, расшифровать которые способна только она. Тогда Алиса подбирает два больших простых числа p и q. Держа их в секрете, Алиса публикует их произведение $N = p \cdot q$, которое называют модулем алгоритма. Кроме того, Алиса выбирает шифрующую экспоненту E удовлетворяющую условию НОД$(E, (p-1)(q-1)) = 1$.

Как правило, берут равным $3, 17$ или 65537. Пара, доступная всем желающим, — это (N, E).

Для выбора секретного ключа Алиса применяет расширенный алгоритм Евклида к паре чисел E и $(p-1)(q-1)$, получая при этом расшифровывающую экспоненту d. Найденная экспонента удовлетворяет соотношению

$$E \cdot d = 1 \pmod{(p-1)(q-1)}.$$

Секретным ключом является тройка (d, p, q). Фактически, можно было бы выбросить простые делители p и q из ключа и помнить лишь о d и всем числе N. Но это снизит скорость алгоритма.

Допустим, что Боб намерен зашифровать сообщение, адресованное Алисе. Он сверяется с открытым ключом и представляет сообщение в виде число m строго меньшего модуля N алгоритма. Шифротекст C получается из m по следующему правилу:

$$C = m^M \pmod{N}.$$

Алиса, получив шифрограмму, расшифровывает ее, возводя число C в степень d:

$$m = C^d \pmod{N}.$$

Равенство имеет место в связи с тем, что порядок группы $(\mathbb{Z}/N\mathbb{Z})^*$ равен $\varphi(N) = (p-1)(q-1)$. Поэтому, по теореме Лагранжа,

$$x^{(p-1)(q-1)} = 1 \pmod{N}$$

для любого числа $x \in (\mathbb{Z}/N\mathbb{Z})$. Поскольку E и d взаимно обратны по модулю $(p-1)(q-1)$, при некотором целом числе s получается равенство

$$Ed = 1 + s(p-1)(q-1).$$

Следовательно,

$$C^d = (m^E)^d = m^{Ed} = m^{1+s(p-1)(q-1)} = m \cdot m^{1+s(p-1)(q-1)} = m \pmod N$$

Рассмотрим пример. Пусть $p = 7$ и $q = 11$. Тогда $N = 77$, а $(p-1)(q-1) = 6 \cdot 10 = 60$. В качестве открытой шифрующей экспоненты возьмем число $= 37$, поскольку НОД $(37, 60) = 1$. Применяя расширенный алгоритм Евклида, найдем $d = 13$, т. к. $37 - 13 = 481 = 1 \pmod{60}$. Предположим, нужно зашифровать сообщение, численное представление которого имеет вид: $m = 2$. Тогда вычисляем

$$C = m^E \pmod N = 2^{37} \pmod{77} = 51.$$

Процесс расшифровывания происходит аналогично:

$$m = C^d \pmod N = 51^{13} \pmod{77} = 2.$$

При первом знакомстве с алгоритмом RSA можно увидеть, что его криптостойкость обеспечивается сложностью вычисления расшифровываюшей экспоненты dпо открытому ключу, т. е. по известным числу N (модулю системы) и шифрующей экспоненте. Очевидно, что задача RSA не сложнее проблемы факторизации. Поэтому, если разложим на множители числоN т.е. найдем p и q, то сможем вычислить d. Следовательно, если проблема факторизации модуля системы окажется легкой, RSA будет взломана. Самые большие числа, которые к настоящему времени удается разложить на множители за разумное время, имеют 500 двоичных знаков. В связи

с этим, для обеспечения стойкости систем среднего срока действия, рекомендуют брать модули шифрования порядка 1024 битов. Для систем большого срока действия следует выбирать модули, состоящие из 2048 битов.

§ 3. Цифровые подписи

Подписи — важнейший момент в криптографии с открытым ключом. Они были предложены Диффи и Хеллманом все в статье 1976 года, но первая практическая разработка подписи принадлежит Ривесту, Шамиру и Адлеману. Движущая пружина подписей в криптографии с открытым ключом изображена на следующей схеме: СООБЩЕНИЕ + секретный ключ Алисы = ПОДПИСЬ, СООБЩЕНИЕ + ПОДПИСЬ + ОТКРЫТЫЙ КЛЮЧ АЛИСЫ = ДА/НЕТ. Эта схема называется схемой подписи с приложением, так как подпись добавляется в конец сообщения перед его передачей. Полученное сообщение подается на вход процедуры проверки подписи. Другой вариант — схема подписи с восстановлением сообщения когда сообщение восстанавливается на выходе процедуры проверки подписи: СООБЩЕНИЕ + секретный ключ Алисы = ПОДПИСЬ, ПОДПИСЬ + ОТКРЫТЫЙ КЛЮЧ АЛИСЫ = ДА/НЕТ + СООБЩЕНИЕ.

Важным моментом здесь является то, что только Алиса может подписать свое сообщение, поскольку только она имеет доступ к своему секретному ключу. С другой стороны, ее подпись может быть проверена любым желающим, поскольку для этого нужен лишь открытый ключ Алисы.

Главная проблема состоит в том, каким открытым ключам можно доверять. Как удостовериться, что тот или иной открытый ключ принадлежит конкретному лицу? Вы можете считать, что данный ключ использует Алиса, в то время как он имеет отношение к Еве. Поэтому Ева может подписывать чеки или нечто подобное, а Вы будете считать, что все это исходит от Алисы. Более формально, схема цифровой подписи состоит из таких двух преобразований:

- секретное преобразование подписи s,

- открытое преобразование проверки V. Далее будем предполагать, что используется схема подписи с восстановлением сообщения, поскольку схема подписи с приложением несильно от нее отличается.

Алиса, посылая сообщение вычисляет $S = sM$ и передает результат , где S — цифровая подпись на сообщении M. Заметим, что мы сейчас не заботимся о секретности сообщения, т. к. для нас сейчас важно лишь то, кто его отправил. Если существенна и конфиденциальность сообщения, то подпись S можно зашифровать, используя, например, открытый ключ адресата. Получатель подписи S применяет открытое преобразование проверки V к S и получает на выходе процедуры сообщение M и некоторый бит v, который отвечает за результат проверки подписи. Если результат проверки положителен, то адресат получает уверенность в следующем:

- в целостности сообщения,т. е. в том, что оно не было изменено при передаче;

- в его оригинальности, т. е. в том, что сообщение было послано именно Алисой;

- в отсутствии ренегатства: Алиса не сможет утверждать, что не посылала сообщения.

Алгоритм шифрования RSA представляет особый интерес, поскольку его можно непосредственно использовать в качестве алгоритма подписи с восстановлением сообщения.

§ 4. Подпись RSA

Секретный ключ знает подписывающий (Алиса).

Подписание

$$S = m^d \pmod{N}.$$

Алиса отправляет Бобу сообщение m и подпись S.

Проверка подписи

$$m \equiv S^E \pmod{N}.$$

Далеко не все сообщения имеют малую длину, позволяющую применить этот метод. Нам необходимы хэш-функции со специальными свойствами, о которых мы сейчас будем говорить.

§ 5. Хэш-функции

Криптографическая хэш-функция h — это функция, определенная на битовых строках произвольной длины со значениями в строках битов

фиксированной длины. Ее значение часто называют хэги- кодом или хэш-значением, В информатике тоже используются своего рода хэш-функции, но важное отличие криптографических хэш- функций от стандартных состоит в том, что первые должны быть односторонними. Другими словами, должно быть невозможно в вычислительном отношении по элементу y из множества значений хэш-функции подобрать такой x из области определения, при котором $h(x) = y$. Другая характеризация односторонних хэш-функций — сказать о них, что они защищены от восстановления прообразов. Применение криптографических хэш-функций позволяет создать схему подписи RSA без восстановления сообщения, что намного эффективней для длинных сообщений.

Предположим, нам дано длинное сообщение M для подписывания. Сначала вычисляется $h(M)$ и потом применяется преобразование подписи RSA к хэш-значению $h(M)$ т.е. подпись получается как

$$S = h(M)^d \pmod N. \tag{7}$$

Наконец, подпись и само сообщение передаются вместе в виде пары (M, S). Проверка подписи (M, S) начинается с “шифрования” S с помощью шифрующей экспоненты RSA для получения H':

$$H' = S^E \pmod N \tag{8}$$

Затем осуществляется к проверке равенства $H' = h(M)$. Если оно верно, то подпись законна.

В противном случае - незаконна.

Почему нам нужна хэш-функция со свойством односторонности? Ответ заключается в том, что свойство односторонности препятствует

криптоаналитику фабриковать сообшение с данной подписью. Предположим, например, что мы используем только что описанную схему подписи RSA с приложением, но хэш-функцию берем не одностороннюю. Тогда возможна следуюшая атака.

- Ева вычисляет $H' = R^E \pmod N$ с некоторым выбранным наугад целом числом R.

- Кроме того, она находит прообраз значения при отображении h (что h сейчас стандартная хэш-функция и вычисление прообраза вполне возможно), т.е. Ева определяет $M = h^{-1}(H')$. Теперь Ева обладает Вашей подписью (M, R) сообшения M. Такая подделка называется экзистенциальной. В ней нападающий не имеет контроля над содержанием сообщения, на которое он поставил Вашу подпись.

На практике требуется нечто большее, чем свойство односторонности. Хэш-функцию h называют защищенной от повторений если вычислительно невозможно найти два таких различных значения и x' при которых $h(x) = h(x')$. Это требование помогает избежать следующих атак со стороны подписывающего лица.

- Отправитель выбирает два сообщения M и M', удовлетворяющие соотношению $h(M) = h(M')$.

- Он подписывает M и получает подпись (M, S).

- Потом он отказывается от своего сообщения, утверждая, что посылал сообщение M'. Например, можно предположить, что — электронный чек на сумму в 1000 евро, в то время как M' — чек на сумму в 10 евро. Ясно, что получится неприятность.

Защищенные от повторений хэш- функции строятся сложнее, чем односторонние. Чтобы найти повторы в значениях хэш-функции f, нам необходимо запоминать результаты вычисления $f(x_1)$, $f(x_2)$, $f(x_3)$ и

т. д., пока не встретится повторение. Если значения этой функции имеют длину nбитов, то ожидаемое совпадение появится через $O(2^{n/2})$ итераций. Эту оценку стоит сравнить с числом шагов, необходимых для вычисления прообраза, которое имеет порядок $O(2^n)$ для корректно заданной Следовательно, для достижения необходимого уровня стойкости устойчивая от повторений функция, определенная на80 - битовых строках должна принимать значения в 160 - битовых строках.

Криптографическая хэш-функция должна обладать также свойством защищенности от вторых прообразов т. е. по данному должно быть практически невозможно отыскать такой $M' \neq M$, для которого $h(M) = h(M')$. Это требование обеспечивает стойкость против следующих атак:

- нападающий получает Вашу подпись (M, S) на сообщении M
- находит другое сообщение M' для которого $h(M) = h(M')$
- ставит Вашу подпись (M', S) на своем сообщении M'.

Таким образом, криптографические хэш-функции должны обладать следующими тремя свойствами:

1) защищенностью от восстановления прообразов: должно быть невозможно в вычислительном отношении найти сообщение с данным значением хэш-функции;

2) защищенностью от повторений: вычислительно невозможно найти два сообщения с одним и тем же значением хэш- функции;

3) защищенностью от вторых прообразов: по данному сообщению нереально найти другое сообщение с тем же значением хэш-функции.

Хэш-функции можно также рассматривать как специальный тип кодов обнаружения вмешательства, MDC (от англ. manipulation detection code). Например, хэш-функцию можно использовать для защиты целостности больших файлов так, как это делается в некоторых программах защиты от

вирусов. Вычисляется значение хэш-функции от содержания файла и либо хранится в каком-то безопасном месте (например, на дискете, спрятанной в сейф), или помещается в файл с подобными данными, который затем снабжается цифровой подпись, препятствующей дальнейшему вмешательству.

Основной принцип проектирования хэш-функции заключается в том, что ее значения должны производить лавинный эффект. Другими словами, небольшое изменение в аргументе хэш-функции должно очень сильно повлиять на ее значение. Это обеспечивает дополнительную стойкость, например, чтобы подпись на чеке в 30 фунтов нельзя было переделать в подпись на чеке в 30000 фунтов, и наоборот. Чтобы значения хэш-функции, применяемой в системах с низким уровнем стойкости, были свободны от повторений, их длина должна быть приблизительно равна 128битам, но предпочтительнее значения в 160битов.

§ 6. Шифрование по Эль-Гамалю

Пусть G — некоторая коммутативная группа. Например, это может быть $\mathbb{F}_q^* = \{1, \ldots, p-1\}$ — группа ненулевых элементов конечного поля. Берется элемент $g \in G$, такой, что порядок g — большое простое число r. Берется число x — секретный ключ, $x \in [1, r-1]$. Открытый ключ:

$$y = g^x.$$

Шифруется сообщение M, которое кодируется элементом G.

Протокол шифрования.

1. Случайным образом выбирается эфемерный (разовый) ключ $k \in [1, r-1]$.
2. Вычисляется $C_1 = g^k$.
3. Вычисляется $C_2 = M \cdot y^k$.
4. Зашифрованное сообщение — это пара (C_1, C_2).

Расшифрование.

$M = C_2 \cdot C_1^{-x} = M(g^x)^k \cdot (g^k)^{-x}$.

Заметим,что при каждом шифровании применяется свой кратковременный ключ. Поэтому, шифруя одно сообщение дважды, мы получаем разные шифротексты.

§ 7. Подпись Эль-Гамаля

Исходные данные таковы: p — большое простое число, g — порождающий элемент группы $\mathbb{F}_p^*$, x — секретный ключ Алисы, $1 < x < p-1$. Имеется также открытая хэш-функция h, $0 \le h(m) \le p-2$.

Напомним, что можно считать, что $\mathbb{F}_p^* = \{1, 2, \ldots, p-1\}$, а g — это такое число, что $g^{p-1} \equiv 1 \pmod p$, но $g^u \not\equiv 1 \pmod p$ для всех u, $0 < u < p-1$.

Вычисляется открытый ключ: $y = g^x \pmod p$. Он известен и Алисе, и Бобу.

Алиса подписывает сообщение m следующим образом.

1) Сначала генерируется случайное число k, $0 < k < p-1$. Это — так называемый сеансовый ключ, или эфемерный ключ, или ключ подписания. В отличие от случая шифрования по Эдь-Гпамалю, здесь требуется, чтобы НОД$(k, p-1) = 1$.

2) Вычисляется первая часть подписи: $s_1 = g^k \pmod p$.

3) Вторая часть подписи s_2 ищется как решение уравнения:

$$h(m) \equiv xs_1 + ks_2 \pmod{(p-1)}.$$

Так как НОД$(k, p-1) = 1$, то в кольце вычетов по модулю $p-1$ элемент k обратим, и сравнение разрешимо. На практике это означает, что существует число r, $1 \le r < p-1$, такое, что $kr = 1 + (p-1)t$ для некоторого t. Это число r и есть k^{-1} в кольце вычетов по модулю $p-1$. Таким образом,

$$s_2 = (h(m) - xs_1)k^{-1} \pmod{(p-1)} = (h(m) - xs_1)r \pmod{(p-1)}.$$

4) Подпись сообщения m — пара чисел s_1, s_2. Таким образом, Алиса отправляет Бобу три числа: m, s_1, s_2.

Боб не знает ни x, ни k, но знает p, g, y, h.

Проверка подписи состоит в проверке сравнения:

$$g^{h(m)} \equiv y^{s_1} s_1^{s_2} \pmod p.$$

Если сравнение выполняется, то подпись принимается, если нет, то отвергается.

Криптостойкость этой подписи основана на трудности решения *задачи о дискретном логарифме*: по известным p, g, y, если число p достаточно велико, вычислительно очень трудно найти решение сравнения:

$$y \equiv g^x \pmod p.$$

§ 8. Подпись DSA

DSA — алгоритм с использованием открытого ключа для создания электронной подписи, но не дляшифрования (в отличие от RSA и схемы Эль-Гамаля). Подпись создается секретно, но может быть публично проверена. Это означает, что только один субъект может создать подпись сообщения, но любой может проверить её корректность. Алгоритм основан на вычислительной сложности взятия логарифмов в конечных полях.

Для построения системы цифровой подписи нужно выполнить следующие шаги:

1. Выбор криптографической хеш-функции $H(x)$.

2. Выбор большого простого числа q, размерность которого N в битах совпадает с размерностью в битах значений хэш-функци $H(x)$.

3. Выбор простого числа p, такого, что $p-1$ делится на q. Битовая длина p обозначается $L\,(2^{L-1} < p < 2^L)$.

4. Выбор числа g такого, что его мультипликативный порядок по модулю p равен q. Для его вычисления можно воспользоваться формулой $g = h^{(p-1)/q} \pmod p$, гд h — некоторое произвольное число $h \in (1, p-1)$ такое, что $g \neq 1$.

Открытый и секретный ключи

1.Секретный ключ представляет собой число $x \in (0, q)$

2. Открытый ключ вычисляется по формуле $y = g^x \pmod p$. Открытыми параметрами являются числа (p, q, g, y). Закрытый параметр только один — число x. При этом числа (p, q, g) могут быть общими для группы пользователей, а числа x и y являются соответственно закрытым и открытым ключами конкретного пользователя. При подписании сообщения используются секретные числа x и k, причем число k должно выбираться случайным образом (на практике псевдослучайным) при подписывании каждого следующего сообщения. Поскольку (p, q, g) могут быть использованы для нескольких пользователей, на практике часто делят пользователей по некоторым критериям на группы с одинаковыми (p, q, g). Поэтому эти параметры называют доменными параметрами .

Подпись сообщения выполняется по следующему алгоритму:

1 Выбор случайного числа $k \in (0, q)$

2 Вычисление $r = (g^k \pmod p) \pmod q$

3 Вычисление $s = k^{-1}(H(m) + x \cdot r) \pmod q$

4 Выбор другого k, если оказалось, что $r = 0$ или $s = 0$

Подписью является пара чисел (r, s), общая длина подписи $2 * N$.

Проверка подписи выполняется по алгоритму:

1 Вычисление $\omega = s^{-1} \pmod q$

2 Вычисление $u_1 = H(m) \cdot \omega \pmod q$

3 Вычисление $u_2 = r \cdot \omega q$

4 Вычисление $\upsilon((g^{u_1} \cdot yu_2) \pmod p) \pmod q$

§ 9. Цифровая подпись Шнорра

Множество вариантов схем подписей основывается на дискретных логарифмах. С практической точки зрения интересен алгоритм, носящий название подписи Шнорра. Расскажем об этом алгоритме в его оригинальном виде, оставив читателю разбираться самостоятельно с его обобщением на эллиптические кривые.

Пусть A — открытая конечная абелева группа, порожденная элементом G простого порядка Q. Ключевая пара в алгоритме подписи Шнорра совпадает с такой же парой в DSA а именно, секретным ключом служит целое число из интервала $(0, Q)$, а открытый ключ определяется формулой $Y = G^x$. Чтобы подписать сообщение, в алгоритме Шнорра поступают следующим образом:

- Выбирают эфемерный ключ из промежутка $(0, Q)$.

- Вычисляют соответствующий открытый ключ $R = G^k$.

- Находят $E = h(M\|R)$. Значение хэш-функции зависит как от сообщения, так и от эфемерного открытого ключа.

- Вычисляют $S = k + x \cdot E \pmod Q$.

Полученная таким образом пара (E, S) является искомой подписью.

Проверка подписи: вычисляют $R = G^S Y^{-E}$ и $h(M\|R)$.

Подпись корректна, если верно равенство $= h(M\|R)$.

Для примера выберем следующие параметры домена: $Q = 101$, $= 607$ и $G = 601$. Чтобы зафиксировать ключевую пару, положим $= 3$ и

$$Y = G^x \pmod p = 391.$$

Затем генерируем эфемерный ключ $k = 65$ и вычисляем

$$R = G^k \pmod p = 223.$$

Теперь находим хэш-значение $= h(M\|R) \pmod Q$. Допустим, что при этом получилось $= 93$. Тогда вторая компонента подписи выглядит как

$$S = k + x \cdot E \pmod Q = 65 + 3 \cdot 93 \pmod{101} = 41$$

.

Можно доказать криптостойкость алгоритма подписи Шнорра в предположени о трудноразрешимости задачи дискретного логарифмирования, в то время как никакого доказательства криптостойкости DSA пока не найдено.

Алгоритм подписи Шнорра был предложен к эксплуатации в процедурах запрос-ответ идентификации кредитных карточек, поскольку <отвечающая> часть подписи (значение S) легко проверяется, так как для этого нужно всего лишь одно умножение и одно сложение в конечном поле. Независимо от того, в какой группе мы работаем, эта заключительная стадия требует только арифметики по модулю относительно небольшого простого числа.

Рассмотрим пример. Допустим, Вы хотите с помощью смарт-карты подтвердить свою подлинность при проходе в какое-то закрытое помещение или при обращении к торговому автомату. Считыватель карты обладает копией Вашего открытого ключа Y, в то время как в карточке записан Ваш секретный ключ гг. Пока Вы носите карточку в кармане, она генерирует некие обращения, которые фактически являются эфемерным

открытым ключом вида $R = G^k$. Когда Вы помещаете смарт-карту в считывающее устройство, она передает тому одно из этих заранее вычисленных обращений. Считыватель выдает запрашивающее сообщение E. После чего Вашей карточке остается лишь найти

$$S = k + xE \pmod{Q}$$

и передать результат считывателю, который проверит <подпись> вычислением $G^S = RY^E$. Все требуемые вычисления при этом крайне просты для реализации.

Более подробно, если обозначить через K смарт-карту, а через A — читающий ее автомат, то

$$K \to A : R = G^K,$$

$$A \to K : R = E,$$

$$K \to A : S = k + xE \pmod{Q}.$$

Таким образом, этот протокол состоит из трех фаз: обращение $\to$ запрос $\to$ ответ, которые присущи всем идентифицирующим протоколам.

§ 10. Протокол обмена ключами Диффи-Хеллмана

Напомним, что основное препятствие к быстрому шифрованию большого количества данных с использованием блочного или поточного шифра, — это сложная проблема распределения ключей. Мы уже познакомились с некоторыми методами ее решения: с помощью протоколов, базирущихся на симметричном шифровании или с использованием алгоритма с открытым ключом для генерирования и передачи сеансового ключа заинтересованным

партнерам. Однако все эти методы не лишены недостатков. Например, протоколы с симметричным ключом слишком сложны для анализа и требуют постоянно работающих долговременных ключей для обмена закрытой информацией между пользователями и центром доверия.

Диффи и Хеллман предложили решать эти задачи с помощью фнкции

$$F(x) = \alpha^x \pmod p$$

где p — большое простое число, x — произвольное натуральное число, α — некоторый примивный элемент поля $GF(p)$. Общепризнанно, что инвертирование функции $\alpha^x \pmod p$, т.е дискретное логарифмирование, является трудой математической задачей.

Сама процедура или, как принято говорить, *протокол выработки общего ключа* описывается следующим образом.

Абоненты A и B независимо друг от друга случайно выбирают по одному натуральному числу — скажем x_A и x_B. Эти элемент:$y_A = \alpha^{x_A} \pmod p$ $\quad y_B = \alpha^{x_B} \pmod p$ (Числа p и α считаются общедоступными.) Потом они обмениваются этими элементами по каналу связи. Теперь абонент A, получив y_B и зная свой секретный элемент x_A, вычисляет новый элемен:

$$y_B^{x_A} \pmod p = \alpha^{x_B x_A} \pmod p$$

Аналогично поступает абонент B:

$$y_A^{x_B} \pmod p = \alpha^{x_A x_B} \pmod p$$

Тем самым у A и B появился общий элемент поля, равный $\alpha^{x_A x_B}$. Этот элемени и объявляется общим ключом A и B.

Из описания протокола видно, что противник знает p, α,α^{x_A} α^{x_B} не знает x_A и x_B и хочет знать $\alpha^{x_A x_B}$. В настоящее время не аогоритмов

действий противника, более эффективных, чем дискретное логарифмирование, а это — трудная математическая задача.

Глава 2. Группа классов идеалов

§ 1. Необходимые алгебраические понятия

Кольцом A называется множество с двумя бинарными операциями (сложение и умножение), которое удовлетворяет следующим аксиомам:

1. По сложению A является абелевой группой (стало быть, в A есть 0, а у каждого элемента $x \in A$ есть противоположный $-x$).

2. Умножение ассоциативно: $(xy)z = x(yz)$ и дистрибутивно относительно сложения:

$$x(y+z) = xy + xz, \qquad (y+z)x = yx + zx.$$

Кольцо является коммутативном кольцом, если:

3. $xy = yx$ для всех $x, y \in A$.

Кроме того, кольцо имеет единичный элемент 1:

4. Существует такой элемент $1 \in A$, что $x1 = 1x = x$ для всех $x \in A$.

Кольцо называется *коммутативном кольцом с единицей*, если кольцо удавлетворяет приведенным выше аксиомам 1 - 4.

Примеры таких колец: кольцо целых чисел $\mathbb{Z}$, кольцо многочленов $R[x_1, \ldots, x_n]$, где R — некоторое коммутативное кольцо. Факторкольцо коммутативного кольца — также коммутативное кольцо.

Гомоморфизмом коммутативных колец называется всякое отображение f кольца A в кольцо B со следующими свойствами:

1. $f(x+y) = f(x) + f(y)$ (так что f-гомоморфизм абелевых групп; поэтому

$f(x-y) = f(x) - f(y), f(-x) = -f(x), f(0) = 0$);

2. $f(xy) = f(x)f(y)$;

3. $f(1) = 1$.

Иными словами, гомоморфизм сохраняет сложение, умножение и единичный элемент.

В дальнейшем все рассматриваемые кольца предполагаются коммутативными.

Подмножество S кольца A называется *подкольцом в* A, если S является аддитивной подгруппой, замкнуто относительно умножения и содержит единичный элемент A. В этом случае тождественное отображение S в A является гомоморфизмом колец.

Идеалом $\mathfrak{a}$ в кольце A называется всякая аддитивная подгруппа со свойством $A\mathfrak{a} \subseteq \mathfrak{a}$, т.е из включений $x \in A$ и $y \in \mathfrak{a}$ следует, что $xy \in \mathfrak{a}$. Умножение в A индуцирует однозначно определенное умножение в факторгруппе $A/\mathfrak{a}$, что превращает эту группу в кольцо, называемое факторкольцо (или кольцо классов вычетов) $A/\mathfrak{a}$.

В любом кольце имеются два идеала, называемых тривиальными: нулевой идеал $\{0\}$, и само кольцо.

Все кратные ax некоторого элемента $x \in A$ образуют идеал, который обозначается (x) или Ax и называется *главны.* Если в кольце каждый идеал является главным, то такое кольцо называется *кольцом главных идеалов.* Говорят, что элемент x порождает идеал (x), или является его образующим.

Теорема 2.1.1. *Каждый идеал кольца $\mathbb{Z}$, и каждый идеал кольца многочленов $K[x]$ (где K — поле) является главным.*

Элемент 1 порождает тривиальный идеал (1), совпадающий с кольцом A.

По любому множеству элементов $\{x_i | i \in I\}$ можно построить идеал $\mathfrak{a}$, состоящий из всех конечных линейных комбинаций вида:

$$\sum_{i \in I} a_i x_i, \qquad a_i \in A.$$

Конечность суммы означает, что $a_i = 0$ для всех индексов, кроме конечного числа. Говорят, что такой идеал порожден множеством $\{x_i | i \in I\}$ (или что это множество является множеством образующих данного идеала).

Если $I = \{1, 2, \ldots, n\}$, то такой идеал обозначается через $(x_1, \ldots, x_n)$. Иногда встречается запись $Ax_1 + \cdots + Ax_n$. Действительно,

$$(x_1, \ldots, x_n) = (x_1) + \cdots + (x_n).$$

Если в идеале $\mathfrak{a}$ можно найти такое конечное множество элементов $x_1, \ldots, x_n$, что $\mathfrak{a} = (x_1, \ldots, x_n)$, то говорят, что идеал $\mathfrak{a}$ конечно порожден (или является конечно порожденным).

Полем называется кольцо A, в котором $1 \neq 0$ и всякий ненулевой элемент обладает обратным по умножению. То есть для каждого $a \neq 0$ найдется такой (однозначно определенный) b, что $ab = ba = 1$. Такой элемент b обозначается через a^{-1} или через $1/a$.

Примеры полей: поле рациональных чисел $\mathbb{Q}$, поле действительных чисел $\mathbb{R}$, поле комплексных чисел $\mathbb{C}$.

Конечные поля: поля вида $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-1\}$, где p — простое число.

Делителем нуля в кольце A называется всякий элемент $x \neq 0$, для которого существует $y \neq 0$ в A, такой, что $xy = 0$. Кольцо, в котором нет ненулевых делителей нуля(и $1 \neq 0$), называется *областью целостности, или просто областью.*

Идеал $\mathfrak{b}$ в кольце A называется *простым,* если $\mathfrak{b} \neq (1)$ и из включения $xy \in \mathfrak{b}$ следует, что либо $x \in \mathfrak{b}$, либо $y \in \mathfrak{b}$.

Идеал $\mathfrak{m}$ в A называется *максимальным,* если $\mathfrak{m} \neq (1)$, не существует идеала $\mathfrak{a}$, удовлетворяющего условию $\mathfrak{m} \subset \mathfrak{a} \subset (1)$.

Иными словами:

$\mathfrak{p}$ — простой идеал $\Leftrightarrow$ $A/\mathfrak{p}$ — область целостности;

$\mathfrak{m}$ — максимальный идеал $\Leftrightarrow$ $A/\mathfrak{m}$ — поле.

В кольце целых чисел все простые идеалы являются максимальными и имеют вид $(p) = p\mathbb{Z}$, где p — простое число.

В кольце многочленов $K[x]$ все простые идеалы являются максимальными и имеют вид $(f(x)) = f(x)K[x]$, где $f(x)$ — неприводимый многочлен.

Пусть $\mathfrak{a}$, $\mathfrak{b}$ — идеалы в кольце A. Осноные операции над идеалами таковы:

1) Суммой $\mathfrak{a} + \mathfrak{b}$ называется множество всех сумм $x + y$, где $x \in \mathfrak{a}$, $y \in \mathfrak{b}$. Это — наименьший идеал, содержащий $\mathfrak{a}$ и $\mathfrak{b}$.

2) Пересечение идеалов: $\mathfrak{a} \cap \mathfrak{b}$.

3) Произведение идеалов: $\mathfrak{a}\mathfrak{b} = \{\sum\limits_{i=1}^{n} a_i b_i \,|\, a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, n \geq 0\}$. То есть, произведением двух идеалов $\mathfrak{a}$, $\mathfrak{b}$ в кольце A называется идеал, порождённый всевозможными произведениями xy, где $x \in \mathfrak{a}$, $y \in \mathfrak{b}$. Иначе говоря, это множество всех конечных сумм $\sum x_i y_i$, где все $x_i \in \mathfrak{a}$ и все $y_i \in \mathfrak{b}$. Аналогично определяется произведение любого конечного семейства идеалов. В частности, определены степени $\mathfrak{a}^n$ $(n > 0)$ любого идеал $\mathfrak{a}$. По определению, $\mathfrak{a}^0 = (1)$. Идеал $\mathfrak{a}^n$ $(n > 0)$ порожден всевозможными произведениями $x_1 x_2 \cdots x_n$, где $x_i \in \mathfrak{a}$ для всех i.

4) Частное идеалов: $\mathfrak{a} : \mathfrak{b} = \{c |\, c\mathfrak{b} \subseteq \mathfrak{a}\}$.

Идеалы $\mathfrak{a}_1$ и $\mathfrak{a}_2$ называются *взаимно простыми*, если $\mathfrak{a}_1 + \mathfrak{a}_2 = A$. В этом случае $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{a}_2$. Если $A = \mathbb{Z}$, $\mathfrak{a} = (m)$, $\mathfrak{b} = (n)$, то идеал $\mathfrak{a} + \mathfrak{b}$ порожден наибольшим общим делителем m и n; $\mathfrak{a} \cap \mathfrak{b}$ порожден их наименьшим общим кратным, а $\mathfrak{a}\mathfrak{b} = (mn)$. В этом случае, таким образом $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b} \Leftrightarrow m, n$ взаимно просты.

$A = k[x_1, \cdots, x_n]$, $\mathfrak{a} = (x_1, \cdots, x_n)$ — идеал, опрожденный элементами $x_1, \cdots, x_n$. Тогда $\mathfrak{a}^m$ — множество всех многочленов, не содержащих

членов степени $< m$.

Все три определенные выше операции(сумма,пересечение,произведение) коммутативны и ассоциативны. Справедлив также дистрибутивный закон:

$$\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$$

В кольце $\mathbb{Z}$ операции $\cap$, $+$ дистрибутивны друг относительно друга. В общем случае это неверно; самое сильное, что можно доказать, — модулярный закон:

$$\mathfrak{a} \cap (\mathfrak{b}+\mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{b} \cap \mathfrak{c}$$

если $\mathfrak{a} \supseteq \mathfrak{b}$ или $\mathfrak{a} \supseteq \mathfrak{c}$.

В кольце $\mathbb{Z}$ имеет $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}\mathfrak{b}$, но в общем случае вено лишь включение $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}$, потому что

$$(\mathfrak{a}+\mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}(\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{b}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}$$

Очевидно, $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$, поэтому

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$$

если $\mathfrak{a}+\mathfrak{b} = (1)$

Если $\mathfrak{a}+\mathfrak{b} = (1)$, идеал $\mathfrak{a}, \mathfrak{b}$ имеет $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$. Очевидно, взаимно простых идеалов $\mathfrak{a}$,$\mathfrak{b}$ равносильна существованию таких элементов $x \in \mathfrak{a}$,$y \in \mathfrak{b}$, что $x + y = 1$.

Пусть $A_1, \cdots, A_n$- некоторые кольца. Их прямым произведением

$$A = \prod_{i=1}^{n} A_i$$

называется *множество всех последовательностей* $x = (x_1, \cdots, x_n)$, $x_i \in A_i$, где $(1 \leq i \leq n)$, с покомпонентным сложением и умножением. Проекции $p_i : A \to A_i$, $p_i(x) = x_i$ являются гомоморфизмами колец.

Пусть A - некоторое кольцо, $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ - его идеалы. Определим гомоморфизм

$$\varphi : A \to \prod_{i=1}^{n} (A/\mathfrak{a}_i),$$

формулой

$$\varphi(x) = (x + \mathfrak{a}_1, \cdots, x + \mathfrak{a}_n).$$

Теорема 2.1.2. ("Китайская теорема об остатках") *Пусть* $\mathfrak{a}_i$, $1 \leq i \leq n$ *— множество различных идеалов, каждые два из которых являются взаимно простыми. Тогда естественный гомоморфизм*

$$A \longrightarrow A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n,$$

сопоставляющий элементу a *элемент* $(a + \mathfrak{a}_1, \ldots, a + \mathfrak{a}_n)$, *является сюръективным, и его ядро равно*

$$\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \ldots \mathfrak{a}_n.$$

Это означает, что имеется изоморфизм коммутативных колец:

$$A/\mathfrak{a}_1 \ldots \mathfrak{a}_n \cong A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n.$$

Свойство целых чисел: каждое целое число n можно единственным способом представить в виде произведения простых чисел:

$$n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}.$$

Свойство многочленов над полем: каждый многочлен $f(x)$ можно единственным способом представить в виде произведения неприводимых многочленов:

$$f(x) = p_1(x)^{k_1} p_2(x)^{k_2} \ldots p_m(x)^{k_m}.$$

Единственность здесь означает единственность с точностью до ненулевого множителя — элемента поля.

На языке идеалов это означает, что:

Теорема 2.1.3. *В кольце целых чисел и в кольце многочленов над полем каждый идеал можно единственным способом представить в виде произведения максимальных идеалов.*

Пусть A — коммутативное кольцо без делителей нуля. Пусть $S \subset A$ — мультипликативное подмножество. Это означает, что $0 \notin S$, $1 \in S$, и из $s_1, s_2 \in S$ следует $s_1 s_2 \in S$.

Способ, которым строится поле рациональных чисел $\mathbb{Q}$, исходя из кольца целых чисел $\mathbb{Z}$, без труда обобщатся на любые области целостности A и доставляет поле частных кольца A. Эта конструкция состоит в том, что берется множество всех упорядоченных пар вида (a, s), где $a, s \in A$ и $s \neq 0$, и на нем вводится отношение эквивалетности

$$(a, s) \equiv (b, t) \Longleftrightarrow at - bs = 0.$$

При проверке транзитивности этого отношения приходится делать сокращения, т.е пользоваться отсутствием ненулевых делителей нуля в A; поэтому нужно считать, что A - область целостности. Однако можно обобщить конструкцию и избавиться от этого органичения.

Пусть A - любое кольцо. Мультипликавно замкнутым подмножеством в A называется всякое подмножество $S \subset A$, содержащее 1 и замкнутое относительно умножения. Иными словами, S -подполугруппа мультипликативной полугруппа в A. Определим отношение $\equiv$ на $A \times S$ следующим способом:

$(a, s) \equiv (b, t) \Longleftrightarrow (at - bs)u = 0$ для некоторого $u \in S$

Очевидно, оно рефлексивно и симметрично. Для проверки транзитивности предположим, что $(a, s) \equiv (b, t)$ и $(b, t) \equiv (c, u)$. Тогда в S существуют такие элементы υ, ω, что $(at - bs)\upsilon = 0$, $(bu - ct)\omega = 0$. Исключив b из этих уравнений,найдем $(au - cs)t\upsilon\omega = 0$. Так как S, замкнуто относительно умножения, имеем $t\upsilon\omega \in S$, и, следовательно, $(a, s) \equiv (c, u)$. Стало

быть, мы определили отношение эквивалентности. Обозначим через a/s класс эквивалентности пары (a, s), и пусть $S^{-1}A$-множество всех классов эквивалентности. Введем на $S^{-1}A$ структуру кольца,определив сложение и умножение << дробей >> a/s формулами элементарной алгебры

$$(a/s) + (b/t) = (at + bs)/(st),$$

$$(a/s)(b/t) = (ab/st).$$

Эти определения не зависит от выбора представителей (a, s), (b, t) и что $S^{-1}A$ удовлетворяет аксиомам коммутативного кольца с единицей.

Формула $f(x) = x/1$ определяет гомоморфизм колец $f : A \to S^{-1}A$ Вообще говоря, что он не инъективен.

Если A - обрасть целостности и $S = A - \{0\}$, то $S^{-1}A$- поле частных кольца A.

Свойство P кольца A (или A-модуля M) называется *локальным* , если справедливо следующее утверждение:

A или (M) обладает свойством $P \Leftrightarrow A_{\mathfrak{p}}$ (или $M_{\mathfrak{p}} = 0$) обладает свойством P для всех простых идеалов $\mathfrak{p}$ кольца A.

Следующие предложения доставляют примеры локальных свойств:

Пусть M -некоторый A-модуля. Следующие утверждения равносильн:

1. $M = 0$;

2. $M_{\mathfrak{p}} = 0$ для всех простых идеалов $\mathfrak{p}$ кольца A;

3. $M_{\mathfrak{m}} = 0$ для всех максимальных идеалов $\mathfrak{m}$ кольца A.

Кольцо $S^{-1}A$ называтся кольцом частных A относительно S. Можно считать, что $A \subseteq S^{-1}A$: элементы $a \in A$ отождествляем с элементами $a/1 \in S^{-1}A$.

Для всякого простого идеала $\mathfrak{p}$ кольца A простые идеалы локального кольца $A_{\mathfrak{p}}$ находятся во взаимно однозначном соответствии с простыми идеалами A, содержащимися в $\mathfrak{p}$.

Переход от A к $A_{\mathfrak{p}}$ вырезает все простые идеалы, кроме тех, которые содержатся в $\mathfrak{p}$. С другой стороны, переход от A к $A_{\mathfrak{p}}$ вырезает все простые идеалы, кроме тех, которые содержат $\mathfrak{p}$. Пусть теперь $\mathfrak{p} \supseteq \mathfrak{q}$ — пара простых идеалов. Тогда локализуя по $\mathfrak{p}$ и факторизуя по $\mathfrak{q}$. Мы можем сосредоточить внимание лишь на идеалах, промежуточных между $\mathfrak{p}$ и $\mathfrak{q}$. В частности $\mathfrak{p} = \mathfrak{q}$, мы придем к полю, которое называеся *полем вычетов идеала* $\mathfrak{q}$. Оно совпадает с полем частных области целостности $A/\mathfrak{p}$ и с полем вычетов локального кольца $A_{\mathfrak{p}}$.

Примеры мультипликативных подмножеств: если $\mathfrak{p}$ — простой идеал кольца A, то $S = A \setminus \mathfrak{p}$ будет мультипликативным подмножеством.

В этом случае кольцо $S^{-1}A$ обозначается через $A_{\mathfrak{p}}$. Это — локальное кольцо с единственным максимальным идеалом $\mathfrak{p}A_{\mathfrak{p}}$.

Если $S = A \setminus \{0\}$, то кольцо частных будет полем. Оно называется полем частных кольца A.

Пусть $A \subseteq B$ — коммутативные кольца. Рассмотрим множество $C = \{b \in B|$ сущестует многочлен $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ с коэффициентами их A, такой, что $f(b) = 0\}$.

Теорема 2.1.4. *Множество C является коммутативным ассоциативным кольцом с единицей — подкольцом кольца B, $A \subseteq C \subseteq B$.*

Кольцо C называется *целым замыканием* подкольца A в кольце B.

Кольцо называется *целозамкнутым*, если оно совпадает со своим целым замыканием.

Пусть $\sum$-множество,частично упорядоченное отношением $\leq$,иными словами, это отношение рефлексивно и транзитивно, а из $x \leq y$ и $y \leq x$ вместе следует, что $x = y$.

Следующие свойства $\sum$ равносильны:

1. Любая возрастающая последовательность $x_1 \leq x_2 \leq \cdots$ в $\sum$ стационарна, иными словами, существует такое n,что $x_n = x_{n-1} = \cdots$

2. Любое непустое подмножество в $\sum$ содержит максимальный элемент.

Пусть $\sum$ множество всех подмодулей модуля M, упорядоченное отношение $\supset q$. Тогда свойство 1 называется *условием обрыва возрастающих цепочек* , а 2 условием *максимальности* . Модуль M, удовлетворяющий этим двум равносильным условиям, называется *нетеровым.*

Если же $\sum$ упорядочено отношение $\supset$, то 1 называется условием *обрыва убывающих цепочек* , а 2 -*условием минимальности* . Модуль M,удовлетволяющий этим двум условиям, называется *артиновым.*

Примеры 1) Любая конечная абелава группа (как Z-модуль) удовлетворяет одновременно условиям обрыва возрастающих цепочек и обрыва убывающих цепоче.

2)Кольцо Z как Z-модуль удовлетворяет условию обрыва возрастающих цепочек, но не удовлетволяет обрыва убывающих цепочек. Действительно, пусть $a \in Z$ и $a \neq 0, 1$ тогда $(a) \supset (a^2) \supset \cdots \supset (a^n) \supset \cdots$.

3) Кольцо $k[x]$(k-поле, x-переменая) удовлетворяет условием рыва возрастающих цепочек, но не удовлетворяет условием .

4) Кольцо многочленов $k[x_1, x_2, \ldots]$ от бесконечного множества переменных не удовлетворяет ни одному из двух уловий для идеалов: последовательность $(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \cdots$ строго возрастает, а $(x_1) \supset (x_1^2) \supset (x_1^3) \cdots$ строго убывает.

Теорема 2.1.5. *Эквивалентны два варианта определения нетерова кольца:*

1) Каждый идеал кольца обладает конечным множеством образующих;

2) Каждая возрастающая цепь идеалов

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_n \subseteq \mathfrak{a}_{n+1} \subseteq \cdots$$

стабилизируется, то есть начина с некоторого m должны выполняься равенства:

$$\mathfrak{a}_m = \mathfrak{a}_{m+1} = \mathfrak{a}_{m+2} = \cdots$$

Кольцо, удовлетворяющее этим свойством, называется нтеровым.

Примеры:

1) Всякое поле одновременно артиново и нётерово, кольцо $Z/(n)$-тоже $n \neq 0$.

2) Любое кольцо главных идеалов нётерово.

Кольцами главных идеалов является $\mathbb{Z}$ и $K[x]$, где K — поле.

Теорема 2.1.6. (Теорема Гильберта о базисе) *Если R — нетерово кольцо, то кольцо многочленов $R[x]$ также является нетеровым кольцом.*

Если кольцо A нётерово, то кольцо $A[x_1, \cdots, x_n]$ тоже нётерово.

Пусть B - конечно порождённая A -алгебра. Если кольцо A нётерово, то же верно для B.

Пусть k - некоторое поле, E-конечно порожденная k - алгебра. Если E - тоже поле, то оно является конечным алгебраическим расширением k.

Факторкольцо нетерова кольца является нетеровым кольцом.

Целое замыкание нетерова кольца без делителей нуля есть ??????

§ 2. Алгебраические числа и дедекиндовы кольца

Алгебраическим числом называется комплексное число $\alpha \in \mathbb{C}$, $\mathbb{C}$ — комплексное число, являющееся корнем некоторого многочлене $a_0x^n + a_1x^{n-1} + \cdots + a_n$, где $a_0, a_1, \ldots, a_n \in \mathbb{Z}$, и $a_0 \neq 0$.

При этом унитарный многочлен наименьшей степини с корнем α называется *минимальным многочленом* числа и обозначается через $m_\alpha(x)$. Степень этого многочлена называется *степенью числа* α, а также *степенью расширения* $\mathbb{Q}(\alpha)$ поля $\mathbb{Q}$ с помощью числа α и обозначается через $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Многочлен $m_\alpha(x)$ неприводим над $\mathbb{Q}$ и имеет в поле комплексных чисел $\mathbb{C}$ ровно n различных корней $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_n$. Все они называется числам *сопряженным* с α.

Целым алгебраическим числом называется комплексное число ω, являющееся корнем некоторого многочлена $x^n + b_1x^{n-1} + \cdots + b_n$, где $b_1, b_2 \cdots, b_n \in \mathbb{Z}$.

Очевидно, что всякое целое алгебраическое число будет алгебраическим числом. Обратное утверждение неверно.

Рациональное число $r \in \mathbb{Q}$ будем целым алгебраическим числом тогда и только тогда, когда $r \in \mathbb{Z}$.

Пусть $\mathbb{K} = \mathbb{Q}(\alpha) = \{c_0\alpha^r + c_1\alpha^{r-1} + \cdots + c_r; c_i \in \mathbb{Q}\}$. При изучении поля $\mathbb{K}$ существенно используются его изоморфизмы над $\mathbb{Q}$ в поле комплексных чисел $\mathbb{C}$. Любой такое изоморфизм определяется образом элемента α. Образом α — это корни $m_\alpha(x)$, т.е $\alpha_1, \alpha_2, \cdots, \alpha_n$. Изоморфизм,отображающий α в α_i, обозначим через $\sigma_i, i = 1, \cdots, n$. Числа $N(\mu) = \sigma_1(\mu) \cdots \sigma_n(\mu)$, $Tr(\mu) = \sigma_1(\mu) + \cdots + \sigma_n(\mu)$ называются соответственно *нормой и следом* числа μ. Фукция $N(x)$ и $Tr(x)$ обладают следующими свойствами.

Для любых $\mu, \nu \in \mathbb{K}$:

$$N(\mu), Tr(\mu) \in \mathbb{Q}, \qquad N(\mu\nu) = N(\mu)N(\nu), \qquad Tr(\mu+\nu) = Tr(\mu) + Tr(\nu)$$

Подмножество $V \subset \mathbb{C}$ комплексных чисел называется $\mathbb{Q}$-*модулем*, если

1) из того, что $\gamma_1, \gamma_2 \in V$, следует, что $\gamma_1 \pm \gamma_2 \in V$;

2) из того, что $\gamma_{\in} V$, $r \in \mathbb{Q}$, следует, что $r\gamma \in V$;

3) существуют такие элементы $\gamma_1, \gamma_2, \ldots, \gamma_l \in V$, что каждый элемент $\gamma_{\in} V$, представляется в виде $\sum\limits_{i=1}^{l} r_i\gamma_i$, где $r_i \in \mathbb{Q}$.

Подмножество $V \subset \mathbb{C}$ есть $\mathbb{Q}$-модуль, если оно является конечномерным векторным пространством над $\mathbb{Q}$.

Если $\gamma_1, \gamma_2, \ldots, \gamma_l \in \mathbb{C}$, то множество всех выражений $\sum\limits_{i=1}^{l} r_i\gamma_i$, где $r_i \in \mathbb{Q}$, $r_1, r_2, \ldots, r_l \in \mathbb{Q}$, как нетрудно убедиться, образует $\mathbb{Q}$-модуль. Обозначим этот $\mathbb{Q}$-модуль через $[\gamma_1, \gamma_2, \ldots, \gamma_l]$.

Пусть $V = [\gamma_1, \gamma_2, \ldots, \gamma_l]$, и предположим, что $\alpha \in \mathbb{C}$ обладает тем свойством, что $\alpha\gamma \in V$ для всех $\gamma \in V$. Тогда α будет алебраическим числом.

Множество алгебраических чисел образует поле.

Подмножество $W \subset \mathbb{C}$ комплексных чисел называется$\mathbb{Z}$-*модулем*, если

1) из того, что $\gamma_1, \gamma_2 \in W$, следует, что $\gamma_1 \pm \gamma_2 \in W$;

2) существуют такие элементы $\gamma_1, \gamma_2, \ldots, \gamma_l \in V$,что каждый элемент $\gamma_{\in} W$, имеет вид $\sum\limits_{i=1}^{l} b_i\gamma_i$, где $b_i \in \mathbb{Q}$.

Пусть W-некоторый $\mathbb{Z}$-модуль, и предположим,что элемент $\omega \in \mathbb{C}$ таков, что $\omega\gamma \in W$ для всех $\gamma \in W$. Тогда ω будет целым алгебраическим числом.

Множество целых алгебраических чисел образует кольцо.

Подполе F поля комплексных чисел называется *полем алгебраических чисел*, если степень расширения $[F : \mathbb{Q}]$ конечно. Если F — такое поле, то

подмножество в нем, состоящее из целых алгебраичеких чисел, образует кольцо $\mathcal{O}$, называемое кольцом целых алгебраических чисел в F.

Пусть Ω-множество всех целых алгебраических чисел. Тогда Ω-кольцо. Так как $\mathcal{O} = \Omega \cap F$, то $\mathcal{O}$-тоже кольцо. Будем говорить, что $\mathcal{O}$ есть кольцо целых чисел в F.

Оказывается, что в общем случае $\mathcal{O}$ не является областью с однозначным разложением на множители. Однако $\mathcal{O}$ обладает почти столь же хорошим свойством. А именно, каждый ненулевой идеал может быть однозначно представлен в виде произведения простых идеалов. Область целостности с таким свойством называется *дедекиндовым кольцом.* Тогда $\mathcal{O}$ — дедекиндовым кольцо.

Теорема 2.2.1. *$\mathcal{O}$ — дедекиндово кольцо. Таким образом, каждый идеал $\mathcal{O}$ можно единственным способом записать в виде $\mathfrak{A} = \mathfrak{M}_1^{k_1}\mathfrak{M}_2^{k_2}\cdots\mathfrak{M}_s^{k_s}$, где $\mathfrak{M}_i$ — максимальные идеалы.*

Теорема 2.2.2. *Каждый идеал кольца $\mathcal{O}$ порожден двумя элементах $a_1, a_2 \in \mathfrak{A}$, $\mathfrak{A} = (a_1, a_2) = \{a_1'a_1 + a_2'a_2 | a_1', a_2' \in \mathcal{O}\}$*

Теорема 2.2.3. *Если $\mathfrak{M}$ — максимальный идеал в $\mathcal{O}$, то поле $\mathcal{O}/\mathfrak{M}$ конечное.*

§ 3. Группа классов идеалов: определения и основные свойства

Пусть A — коммутативное кольцо без делители нуля, K — поле частных $K = \{\frac{a}{b} | a \in A, b \in A, b \neq 0\}$, где $A \subset K$

Дробный идеал A — это множество $I \subseteq K$, такое, что:

1) I — группа по сложению;

2) I есть A-модуль, то есть $\forall x \in I, \forall a \in A : ax \in I$;

3) $\exists c \in A : cI = \{cx | x \in I\} \subseteq A$.

Положим $I^{-1} = \{y \in K | yI \subseteq A\}$.

Пусть $a_1, a_2 \in A, a_2 \neq 0$. Множество $(\frac{a_1}{a_2}) = \{\frac{a_1}{a_2} a | a \in A\}$ называтся *главным дробным идеалым.* И $(\frac{a_1}{a_2})^{-1} = (\frac{a_2}{a_1})$.

Для любого дробного идеала M множество элементов $x \in K$ со свойством $xM \subseteq A$ обозначается символом $(A : M)$.

Любой конечно порождённый A -подмодуль M поля K является *дробным идеалом.* Действительно, пусть M порожден элементами $x_1, \cdots, x_n \in K$. Тогда можно положить $x_i = y_i z^{-1}(\ 1 \leq i \leq n)$, где y_i и z лежат в A и, очевидно $zM \subseteq M$. Наоборот, если кольцо A нётерово, любой дробный идеал конечно порожден, потому что его можно представить в виде $x^{-1}\mathfrak{a}$, где $\mathfrak{a}$-некоторый целый идеал.

A-подмодуль M поля K является *обратимым идеалом*, если сущестует такой подмодуль N поля K, что $MN = A$. В этом случае N определяется однозначно и совпадает с $(A : M)$, потому что

$$N \subseteq (A : M) = (A : M)MN \subseteq AN = N.$$

Отсюда следует, что M конечно порожден и, следовательно, является it дробным идеалом. Действительно, поскольку $M(A : M) = A$, существуют такие элементы $x_i \in M$ и $y_i \in (A : M)(\ 1 \leq i \leq n)$,что $\sum x_i y_i = 1$, так

что для всякого $x \in M$ имеем $\sum(y_i x)x_i$. Но все $y_i x$ принадлежает A, так что M порожден элементами $x_1, \ldots, x_n$.

Теорема 2.3.1. (Свойства дробных идеалов)

1) *I_1, I_2-дробные идеалы , то $I_1 I_2 = \{\sum\limits_{i \geq 1} x_{i1} x_{i2} | x_{i1 \in I_1}, x_{i2} \in I_2\}$ —тоже дробный идеал*

2) $(I_1 I_2) I_3 = I_1 (I_2 I_3)$

3) $I_1 I_2 = I_2 I_1$

Пусть A — дробный идеал, тогда $AI = IA = I$, то есть A играет роль единицы при умножении дробных идеалов.

Теорема 2.3.2. *Кольцо A является дедекиндовым когда и только тогда, когда любой дробный идеал I удовлетворяет свойству: $II^{-1} = A$.*

Это эквивалентно тому что, множество FI_K всех дробных идеалов A образует группу по умножениею идеалов.

Теорема 2.3.3. *A — дедекиндово тогда и только тогда, когда FI_K-группа.*

В группе FI_K есть подгруппа PI_K, состоящая из главных дробных идеалов I.

В частности целые идеалы является частным случаем дробных.

§ 4. Квадратичные поля и их группы классов

Пусть F —поле алгебраических чисел. Если $[F:\mathbb{Q}]=2$, то F называется *квадратичным расширением поля* $\mathbb{Q}$. Это означает, что F как векторные пространство над $\mathbb{Q}$ имеет базис из двух элементов w_1, w_2.

Например $w_1, w_2 \in F$, тогда

$$F = \{\lambda_1 w_1 + \lambda_2 w_2; \lambda_1, \lambda_2 \in \mathbb{Q}\}$$

Можно выбрать базис так, чтобы $w_1 = 1,\ w_2 = w \in F,\ w \notin \mathbb{Q}$

$$F = \{\lambda_1 + \lambda_2 w; \lambda_1, \lambda_2 \in \mathbb{Q}\}.$$

Любое квадратичное расширение поля $\mathbb{Q}$ можно представить в виде $\mathbb{Q}(\sqrt{D})$, где D-свободное от квадратов и отличное от 1 и 0 целое число. Любое число $\alpha \in \mathbb{Q}(\sqrt{D})$ однозначно представляется в виде

$$\alpha = a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D}).$$

Это расширение поля $\mathbb{Q}$ называется *мнимым*, если $D < 0$, и *реальным*, или *вещественным* , если $D > 0$.

Пусть $\Delta \in \mathbb{Z}, \Delta \neq a^2$ тогда

$$\Delta \equiv 0, 1 \pmod 4$$

Δ называется *(квадратичным) дискриминантом.* Δ называется *фундаментальн дискриминантом,* если

$$\Delta \equiv 1 \pmod 4 \qquad \text{и} \qquad \Delta \neq a^2 b,$$

или

$$\Delta \equiv 0 \pmod 4, \qquad \text{и} \qquad \Delta/4 \equiv 2, 3 \pmod 4 \qquad \text{и} \qquad \Delta \neq a^2 b$$

Каждый дискриминант Δ можно представить в виде $\Delta = \Delta_1 f^2$, где Δ_1 —фундаментальный дискриминант, и $f \in \mathbb{Z}$

Рассматриваем $\Delta < 0$. Положим $\sqrt{\Delta_f} = i\sqrt{|\Delta_f|}$

Рассмотрим кольцо

$$\mathcal{O}_{\Delta_f} = \mathbb{Z} + \frac{\Delta_f + \sqrt{\Delta_f}}{2}\mathbb{Z}$$

$$= \{a + \frac{\Delta_f + \sqrt{\Delta_f}}{2} b | a, b \in \mathbb{Z}\}$$

Оно называется *квадратичным порядком с дискриминантом* Δ_f. Если Δ_f — не фундаментальный дискриминант, то

$$\mathcal{O}_{\Delta_f} \subset \mathcal{O}_{\Delta_1}$$

и $[\mathcal{O}_{\Delta_1} : \mathcal{O}_{\Delta_f}] = f$, как абелевы группы.

Более того,

$$\mathcal{O}_{\Delta_f} = \mathbb{Z} + f\mathcal{O}_{\Delta_1}$$

Порядок $\mathcal{O}_{\Delta_f}$ называется *немаксимальным порядком с кондуктором f,* а порядок $\mathcal{O}_{\Delta_1}$ называется *максимальным порядком* .

Каждый элемент $\alpha \in \mathcal{O}_{\Delta_f}$ представляется в виде :

$$\alpha = a + \frac{\Delta_f + \sqrt{\Delta_f}}{2} b =$$

$$= \frac{2a + \Delta_f b}{2} + \frac{\sqrt{\Delta_f} b}{2} =$$

$$= \frac{(2a + \sqrt{\Delta_f} b) + b\sqrt{\Delta_f}}{2} =$$

$$= (x + y\sqrt{\Delta_f})/2$$

где $x, y \in \mathbb{Z}, \qquad y = b, \qquad x = 2a + \Delta_f b.$

Для $\alpha = (x + y\sqrt{\Delta_f})/2$, положим $\alpha' = (x - y\sqrt{\Delta_f})/2$. $\alpha' = \bar{\alpha}$ — комплексно сопряженное число.

Норма α:

$$N(\alpha) = \alpha\alpha' = (x^2 - y^2\Delta_f)/4$$

Каждый идеал $\mathfrak{A} \subset \mathcal{O}_{\Delta_f}$ можно представить в виде

$$\mathfrak{A} = m(a\mathbb{Z} + \frac{b + \sqrt{\Delta_f}}{2}\mathbb{Z})$$

где $m \in \mathbb{Z}, a \in \mathbb{Z}, a > 0, b \in \mathbb{Z}$ и $b^2 \equiv \Delta_f \pmod{4a}$

При выборе a, b такими, что $-a < b \leq a$ параметры a, b, m определены однозначно. Числа (m, a, b) называется *стандартным представлением* $\mathfrak{A}$.

Норма идеала :

$$N(\mathfrak{A}) = am$$

Идеал $\mathfrak{A}$ называется *примитивным* , если $m = 1$. В этом случае идеал $\mathfrak{A}$ задаётся параметрами (a, b).

Идеал $\mathfrak{A} \subset \mathcal{O}_{\Delta_f}$ называется *взаимно-простым с* f, если

$$gcd(N(\mathfrak{A}), f) = 1$$

Идеал $\mathfrak{A}$ и $\mathfrak{B}$ эквиваленты, если существует $\alpha \in \mathcal{O}_{\Delta_f}$ такой, что

$$\mathfrak{A} = \alpha\mathfrak{B}$$

Эквивалентность обозначается через $\mathfrak{A} \sim \mathfrak{B}$.

Если $\gamma \in \mathcal{O}_{\Delta_f}$, то идеал $(\gamma) = \gamma\mathcal{O}_{\Delta_f}$ называется *главным идеалом.*

Идеал $\mathcal{O}_{\Delta_f}$, взаимно простые с f, образуют по умножению абелеву группу $\mathfrak{I}_{\Delta_f}(f)$

Главные идеалы, взаимно простые с f, образуют по умножению группу

$$\mathfrak{P}_{\Delta_f}(f) \subset \mathfrak{I}_{\Delta_f}(f)$$

Группа классов $\mathcal{O}_{\Delta_f}$

$$Cl(\Delta_f) = \mathfrak{I}_{\Delta_f}(f)/\mathfrak{P}_{\Delta_f}(f)$$

$$h(\Delta_f) = |Cl(\Delta_f)|.$$

Пусть $\mathfrak{A} = (a, b)$ — примитивный идеал из $\mathfrak{I}_{\Delta_f}(f)$. Он называется *редуцированным* , если

$$|b| \leq a \leq c = (b^2 - \Delta_f)/4a, \qquad \text{и} \qquad b \geq 0 \qquad \text{при} \qquad a = c \qquad \text{или} \qquad a = |b|.$$

В каждом классе эквивалентных по отношению $\sim$ идеалов иммется единственный редуцированный идеал.

Пусть $Red_{\Delta_f}(\mathfrak{A})$ есть редуцированный идеал, эквивалентный $\mathfrak{A}$. Множество редуцированных идеалов можно отождествить с $Cl_{\Delta_f}(f)$.

Для каждого редуцированного идеала $\mathfrak{A} \in \mathfrak{I}_{\Delta_f}(f)$. выполнено неравенство

$$N(\mathfrak{A}) < \sqrt{|\Delta_f|/3}$$

Обратно, если $\mathfrak{A} \in \mathfrak{I}_{\Delta_f}(f)$ таков, что

$$N(\mathfrak{A}) < \sqrt{|\Delta_f|/4}.$$

то $\mathfrak{A}$ —редуцированный идеал.

При этом сопряженным с ним числом будет $\alpha' = a - b\sqrt{D}$. Если $b \neq 0$, то число α имеет минимальный многочлен $m_\alpha(x) = x^2 - 2ax + a^2 - b^2D$, и потому

$$N(\alpha) = a^2 - b^2D, \qquad Tr(\alpha) = 2a.$$

Будем обозначать через $\mathbb{Q}_0(\sqrt{D})$ или через $\mathbb{Q}(\sqrt{D})$кольцо целых чисел в поле $\mathbb{Q}(\sqrt{D})$. Следовательно,

$$\alpha \in \mathbb{Q}_0[\sqrt{D}] \Leftrightarrow a^2 - b^2D, 2a \in \mathbb{Z}$$

Отсюда получается описание всех целых чисел поля $\mathbb{Q}(\sqrt{D})$:

1) $\mathbb{Q}_0(\sqrt{D}) = a + b\sqrt{D}; a, b \in \mathbb{Z}$, если $D \neq 1 \pmod 4$

2) $\mathbb{Q}_0(\sqrt{D}) = \{\frac{a+b\sqrt{D}}{2};\ a, b \in \mathbb{Z}, a \equiv \pmod 2\}$, если $D \equiv 1 \pmod 4$.

Система чисел $(1, w)$, где $w = \frac{d+\sqrt{d}}{2}$, является $\mathbb{Z}$ - *базисом поля* $\mathbb{Q}(\sqrt{D})$ в любом указанных случаев.

Дискриминант d поля $\mathbb{Q}(\sqrt{D})$ в указанных двух случаях равен соответственно $4D$ и D, а в качестве $\mathbb{Z}$ - базисов могут быть взяты соответственно системы $(1, \sqrt{D})$ и $(1, \frac{1+\sqrt{D}}{2})$

Множество простых идеалов кольца $\mathbb{Q}_0(\sqrt{D})$, содержащих нечетное простое число p, исчерпывается:

I a) при $(\frac{d}{p}) = 1$ идеалами $P_i = [p, b_i + w]$, $i = 1, 2$, где $(\frac{d}{p}) = 1$ — символ Лежандра, а b_1, b_2 p -различные решения сравнения по модулю p

$$(2x + d)^2 \equiv d \pmod p;$$

I b) при $(\frac{d}{p}) = -1$ одним идеалом (p);

I c) при $(\frac{d}{p}) = 0$ одним идеалом $P = [p, w]$;

В случае $p = 2$ множество простых идеалов $\mathbb{Q}_0(\sqrt{D})$, содержащих число 2, исчерпывается:

II a) при $d \equiv 1 \pmod 8$ идеалами $P_1 = [2, w]$,$P_2 = [2, 1 + w]$;

II b) при $d \neq 0 \pmod 8$, $d \equiv 1 \pmod 4$ одним идеалами (2);

II c) при $d \equiv -1 \pmod 4$ одним идеалами $P = [2, 1 + w]$;

II d) при $d \equiv 2 \pmod 4$ одним идеалом $P = [2, w]$.

§ 5. Гомоморфизмы между группами классов идеалов

Опишем, как устроен гомоморфизм из $Cl(\Delta_q)$ в $Cl(\Delta_1)$.

Пусть $\Delta_f = f^2\Delta_1 < 0$ — квадратичный дискриминант.

Пусть $\mathfrak{a} \in \mathfrak{I}_{\Delta_f}(f)$, так как $\mathcal{O}_{\Delta_f} \subset \mathcal{O}_{\Delta_1}$, то можно образовать идеал

$$\mathfrak{A} = \mathfrak{a}\mathcal{O}_{\Delta_1} = \{\sum_{i\geq 0} a_i b_i | a_i \in \mathfrak{a}, b_i \in \mathcal{O}_{\Delta_1}\}$$

Ясно, что $\mathfrak{A} \in \mathfrak{I}_{\Delta_f}(f)$, и $N(\mathfrak{a}) = N(\mathfrak{A})$

Обратно, если $\mathfrak{A} \in \mathfrak{I}_{\Delta_f}(f)$, то $\mathfrak{a} = \mathfrak{A} \bigcap \mathcal{O}_{\Delta_f} \in \mathfrak{I}_{\Delta_f}(f)$ и $N(\mathfrak{A}) = N(\mathfrak{a})$.

Соответствие $\phi : \mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_{\Delta_1}$ индуцирует изоморфизм

$$\mathfrak{I}_{\Delta_f}(f) \xrightarrow{\sim} \mathfrak{I}_{\Delta_1}(f) \qquad \phi^{-1}(\mathfrak{A}) = \mathfrak{A} \bigcap \mathcal{O}_{\Delta_f}$$

Пусть $f = q$ — простое число, и $\sqrt{|\Delta_f|/3} < q$

Тогда редуцированные идеалы из $Cl(\Delta_1)$ являются *взаимно простыми с кондукторым* q.Поэтому можно определить следующее отображение :

$$\varphi_q : Cl(\Delta_q) \to Cl(\Delta_1)$$

$$\mathfrak{a} \mapsto Red_{\Delta_1}(\mathfrak{a}\mathcal{O}_{\Delta_1})$$

Здесь предполагается, что элементы группы классов идеалов отожествляются с соответствующеми редуцированными идеалами.

Практический способ вычисления отображения φ_q

Алгоритм GoToMaxOrder

Исходные данные: Редуцированный идеал $a = (a, b) \in Cl(\Delta_q)$.

Фундаментальный дискриминант Δ_1, дискриминант Δ_q кондуктор q.

Вычисляется редуцированный идеал

$$\mathfrak{A} = \varphi_q(a) = (A, B).$$

1. $b_{\mathcal{O}} = \Delta_q \pmod 2$

2. Решаем уравнение

$$1 = \mu q + \lambda a$$

относительнно $\mu, \lambda \in \mathbb{Z}$ используя расширенный алгоритм Евклида.

3. $B = b\mu + ab_{\mathcal{O}} \pmod{2a}$.

4. $(A, B) = Red_{\Delta_1}(A, B)$.

Алгоритм вычисления $Red_{\Delta_1}(A, B)$ можно найти в статье [12].

§ 6. Действительные и мнимые квадратичные поля

Пусть K — поле алгебраических чисел, $\mu_1, \mu_2, \ldots, \mu_m \in K$. Модуль в K — это множество всех выражений

$$c_1\mu_1 + c_2\mu_2 + \cdots + c_m\mu_m$$

где $c_1, c_2, \ldots, c_m \in \mathbb{Z}$.

Полный модуль в K — это модуль, обладающий базисом из $n = [K : \mathbb{Q}]$ элементов, т.е можно считать, что $m = n$ и $\mu_1, \mu_2, \ldots, \mu_m$ — базис. Если полный модуль является кольцом, то он называется *порядком поля* K.

Теорема 2.6.1. *Если рассматривать R как абелеву группу, то в R есть базис из $n = [K : \mathbb{Q}]$ элементов.*

Лемма 2.6.1. *Порядок в поле целых алгебраических чисел — это полный модуль M, содержащий единицу , $1 \in M$ и являющий кольцо.*

Каждый порядок содержится в R. R является *максимальным порядком.*

$K = \mathbb{Q}(\sqrt{D})$ — квадратичное поле. $[F : \mathbb{Q}] = 2$. Базис над $\mathbb{Q}$ состоит из 1 и $\sqrt{D}$. $\alpha \in K : \alpha = a + b\sqrt{D}$, где $a, b \in \mathbb{Q}$.

K называется *мнимым квадратичным полем* , если $D < 0$, и *действительным квадратичгым полем,* если $D > 0$. Положем $\Delta_1 = 4D$ при $D \equiv 2$ или $,3 \pmod 4$ $\Delta_1 = D$ если $D \equiv 1 \pmod 4$ так что $\Delta_1 \equiv 0$ или $1 \pmod 4$

Δ_1 называется *фундаментальным дискриминантым* . Пусть $f \in \mathbb{N}$. Положим $\Delta_f = f^2\Delta_1$. Квадратичный порядок с кондуктором f в K есть $\mathbb{Z}$ — подмодуль $\mathcal{O}_{\Delta_f} \subset K$ иммеющий ранг 2, и поряжденный 1 и $f(\Delta_1 + \sqrt{\Delta_1})/2$. В этом случае $\mathcal{O}_{\Delta_f}$ будет подкольцом K, т.е порядком в обычном смысле.

Дискриминант $\mathcal{O}_{\Delta_f}$ есть число Δ_f. Порядок называется *мнимым* , если $\Delta_1 < 0$ и *действитем*, если $\Delta_1 > 0$.

Максимальный порядок (кольцо целых алгебраических чисел) есть $R = \mathcal{O}_{\Delta_1}$

Теорема 2.6.2. $\mathcal{O}_{\Delta_f} \subset \mathcal{O}_{\Delta_1}$, $|\mathcal{O}_{\Delta_1} : \mathcal{O}_{\Delta_f}| = f$

Теорема 2.6.3. *Поле частных $\mathcal{O}_{\Delta_f}$ есть K такое, что*

$$\mathbb{Q} \subset \mathcal{O}_{\Delta_f} \subset \mathcal{O}_{\Delta_1} = R \subset K$$

Можно говорить о дробных идеалах в $\mathcal{O}_{\Delta_f}$. Дробный идеал $\mathfrak{a} \subset \mathcal{O}_{\Delta_f}$ называется *обратимым* , если существует другой дробный идеал $\mathfrak{b}$ такой, что $\mathfrak{ab} = \mathcal{O}_{\Delta_f}$

Обозначим через $\mathcal{I}(\mathcal{O}_{\Delta_f})$ множество всех обратимых дробных идеалов $\mathcal{O}_{\Delta_f}$. Это группа по умножению идеалов. Если $\mathcal{O}_{\Delta_f}$ дедекиндово, тогда $\mathcal{I}(\mathcal{O}_{\Delta_f}) = FI_K$, $\mathcal{P}(\mathcal{O}_{\Delta_f}) \subset \mathcal{I}(\mathcal{O}_{\Delta_f})$ — подгруппа всех главных дробных идеалов.

$Cl(\mathcal{O}_{\Delta_f}) = \mathcal{I}(\mathcal{O}_{\Delta_f})/\mathcal{P}(\mathcal{O}_{\Delta_f})$ — группа классов идеалов порядка $\mathcal{O}_{\Delta_f}$. Это конечная абелева группа. Её порядок $|Cl(\mathcal{O}_{\Delta_f})| = h_{\Delta_f}$ называется

числом классов порядка $\mathcal{O}_{\Delta_f}$. Если $\mathfrak{a}$ — обратимый идеал $\mathcal{O}_{\Delta_f}$, то через $[\mathfrak{a}]$ обозначается образ $\mathfrak{a}$ в $Cl(\mathcal{O}_{\Delta_f})$ относительно гомоморфизм

$$\mathcal{I}(\mathcal{O}_{\Delta_f}) \to Cl(\mathcal{O}_{\Delta_f}) = \mathcal{I}(\mathcal{O}_{\Delta_f})/\mathcal{P}_(\mathcal{O}_{\Delta_f}).$$

Пусть $\alpha = a + b\sqrt{D} \in K$, где $a, b \in \mathbb{Q}$. $\bar{\alpha} = a - b\sqrt{D}$. Норм α, $N(\alpha) = \alpha\bar{\alpha} = a^2 - b^2 D \in \mathbb{Q}$ $\alpha \in \mathcal{O}_{\Delta_1}$ тогда $N(\alpha) \in \mathbb{Z}$.

Пусть $\mathfrak{a}$ — идеал $\mathcal{O}_{\Delta_f}$. Норм $\mathfrak{a}$ $N(\mathfrak{a}) = N_{\Delta_f}(\mathfrak{a}) = |\mathcal{O}_{\Delta_f} : \mathfrak{a}|$ индекс подгруппы $\mathfrak{a}$ в группе $\mathcal{O}_{\Delta_f}$. Если $\bar{\mathfrak{a}} = \{\bar{\alpha} | \alpha \in \mathfrak{a}\}$, то это идеал, и $\mathfrak{a}\bar{\mathfrak{a}} = (N(\mathfrak{a}))$ — главный идеал. Если $\mathfrak{a}$ — главный идеал, $\mathfrak{a} = (\alpha)$, $\alpha \in \mathcal{O}_{\Delta_f}$, то $N(\mathfrak{a}) = |N(\alpha)|$.

Целый идеал $\mathfrak{a} \subset \mathcal{O}_{\Delta_f}$ называется *примитивным*, если из того, что в $\mathcal{O}_{\Delta_f}$ любой элемент идеал $\mathfrak{a}$ делиться на положительное число d, следут, что $d = 1$.

Идеал $\mathfrak{a} \subset \mathcal{O}_{\Delta_f}$ называется *редуцированным* , если он

1) примитивен;

2) не существует никакого $0 \neq \alpha \in \mathfrak{a}$ такого, что $|\alpha| < N(\mathfrak{a})$ и $|\bar{\alpha}| < N(\mathfrak{a})$.

Теорема 2.6.4. *Пусть* $\mathcal{O}_{\Delta_f}$ *— порядок в квадратичном числовым поле* $K = \mathbb{Q}(\sqrt{D})$. *Тогда выполнены следующие утверждения*

1) Каждый класс идеалов $Cl(\mathcal{O}_{\Delta_f})$ *содержит редуцированный идеал.*

2) Если поле K *мнимое, то каждый класс идеалов* $Cl(\mathcal{O}_{\Delta_f})$ *содержит единственный редуцированный идеал. Пусть* $r_{\mathbf{C}}$ *количество редуцированных идеалов в классе идеалов* $\mathbf{C} \in Cl(\mathcal{O}_{\Delta_f})$. *Выполнены неравенство*

$$R_{\Delta_f}/\log(f^2 D) \leq r_{\mathbf{C}} < 2R_{\Delta_f}/\log(2) + 1,$$

где $R_{\Delta_f} = \log(\varepsilon_{\Delta_f})$, ε_{Δ_f} *— образующий бесконечный циклической группы* $\mathcal{O}^*_{\Delta_f}$ *обратимых элементов* $\mathcal{O}_{\Delta_f}$ *причем* $\varepsilon_{\Delta_f} > 1$. *Число* R_{Δ_f} *называется регулятором порядка* $\mathcal{O}_{\Delta_f}$.

3) Если $\mathfrak{a}$ — примитивный $\mathcal{O}_{\Delta_f}$ — идеал, такой, что $N(\mathfrak{a}) < \sqrt{|\Delta_f|}/2$, то $\mathfrak{a}$ является редуцированным идеал.

4)Пусть $\mathfrak{a}$ — редуцированный идеал. Тогда, если K — действительное поле, то $N(\mathfrak{a}) < \sqrt{\Delta_f}$. Если K — мнимое поле, то $N(\mathfrak{a}) < \sqrt{|\Delta_f|/3}$.

Пусть $\mathfrak{a}$ — идеал $\mathcal{O}_{\Delta_f}$. Обозначим через $\rho_{\Delta_f}(\mathfrak{a})$, любой редуцированный $\mathcal{O}_{\Delta_f}$ — идеал из класса $\mathfrak{a}$.

Если K — мнимое поле, то $\rho_{\Delta_f}(\mathfrak{a})$ определяется однозначно. Если же K — действительное поле, то $\rho_{\Delta_f}(\mathfrak{a})$ можно выбрать многими способами.

Пусть d — целое число. Целый идеал $\mathfrak{a} \subset \mathcal{O}_{\Delta_f}$ называется *взаимно простым с* d, если число $N(\mathfrak{a})$ является взаимно простым с d, т.е $gcd(N(\mathfrak{a}), d) = 1$.

Если $d = f$, то каждый идеал, взаимно простой с f, является *обратимым* . Отображение $\mathfrak{a} \mapsto N(\mathfrak{a})$ является *мультипликативным* на множестве всех идеалов $\mathcal{O}_{\Delta_f}$, взаимно простых с f, т.е если $N(\mathfrak{a})$ и $\mathfrak{b}$ взаимно просты с f, то $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.

Обозначим через $\mathcal{I}(\mathcal{O}_{\Delta_f}, f)$ подгруппу группы $\mathcal{I}(\mathcal{O}_{\Delta_f})$, порождённую всеми идеалами $\mathcal{O}_{\Delta_f}$, взаимно простым с f. Пусть $\mathcal{P}(\mathcal{O}_{\Delta_f}, f)$ — подгруппа $\mathcal{I}(\mathcal{O}_{\Delta_f}, f)$, порождённая всеми главными идеалами $(\mathfrak{a})$, где $\alpha \in \mathcal{O}_{\Delta_f}$ и $N(\alpha)$ взаимно просто с f.

Положим

$$Cl(\mathcal{O}_{\Delta_f}, f) = \mathcal{I}(\mathcal{O}_{\Delta_f}, f)/\mathcal{P}(\mathcal{O}_{\Delta_f}, f)$$

Теорема 2.6.5. $Cl(\mathcal{O}_{\Delta_f}, f) \cong Cl(\mathcal{O}_{\Delta_f})$

Для криптосистемы NICE важно установить соотношение между идеалами $\mathcal{O}_{\Delta_f}$, взаимно простыми с f, и идеалами $\mathcal{O}_{\Delta_1}$, взаимно простыми с f.

Теорема 2.6.6. *Существует изоморфизм*

$$\mathcal{I}(\mathcal{O}_{\Delta_1}, f) \longrightarrow \mathcal{I}(\mathcal{O}_{\Delta_f}, f) \qquad \phi(\mathfrak{A}) = \mathfrak{A} \cap \mathcal{O}_{\Delta_f} \qquad \phi^{-1}(\mathfrak{a}) = \mathfrak{a}\mathcal{O}_{\Delta_1} \tag{1}$$

Если f и Δ_1 известны, то ϕ и ϕ^{-1} вычисляюся эффективно. Если же f неизвестно, то ϕ^{-1} будет играть роль односторонней функции с ловушкой f, причём f должно быть простым числом.

Лемма 2.6.2. *1) Отбражения ϕ и ϕ^{-1} сохраняют нормы идеалов, и переводят примитивные идеалы в примитивные идеалы.*

2) Отображение ϕ^{-1} переводит главные идеалы снова в главные идеалы, но ϕ таким свойством не обладает.

Из этой леммы следует, что ϕ^{-1} индуцирует сюръективный гомоморфизм группы:

$$\hat{\Phi} : Cl(\mathcal{O}_{\Delta_f}, f) \longrightarrow Cl(\mathcal{O}_{\Delta_1}, f), \qquad \hat{\Phi}([\mathfrak{a}]) = [\phi^{-1}(\mathfrak{a})] = [\mathfrak{a}\mathcal{O}_{\Delta_1}] \tag{2}$$

$Ker(\hat{\Phi}) = \{[\mathfrak{a}] \in Cl(\mathcal{O}_{\Delta_f}, f) | \phi^{-1}(\mathfrak{a})$ есть главный идеал $\mathcal{O}_{\Delta_1}\}$. Эта группа играет очень важную роль в криптосистеме NICE для мнимых полей

$$|Ker(\hat{\Phi})| = h_{\Delta_f}/h_{\Delta_1}$$

Для криптографии интересен случай, когда кондуктор $f = q$ — простое число. Часто рассматривается случай $\Delta_1 = -3$ или $\Delta_1 = -4$, причём K должно содержать нетривиальные корни из единицы.

В этом случае

$$|Ker(\hat{\Phi})| = \frac{h_{\Delta_q}}{h_{\Delta_1}} = \begin{cases} q - (\Delta_1/q) & \text{при } \Delta_1 < -4 \\ q - (\Delta_1/q)R_{\Delta_1}/R_{\Delta_q} & \text{если } \Delta_1 > 0 \end{cases} \tag{3}$$

Глава 3. Криптосистема NICE для мнимых квадратичных полей

§ 1. Идейная основа криптосистемы NICE

Данны две конечные абелевы группы G и H, и сюръективный гомоморфизм $\pi : G \to H$

Открытые(известные) данные:

1) Способ задания для компьютера элементов G;

2) Алгоритм вычисления групповой операции умножения элементов в G;

3) Некоторый элемент $p \in Ker(\pi)$;

4) Способ задания для компьютера элементов H;

5) Алгоритм вычисления умножения элементов в H;

6) Алгоритм вычисления $\pi(x)$.

Кроме того задано пространство сообщение Msg: оно содержится в G, $Msg \subset G$ и $\pi|_{Msg} : Msg \to H$, есть биекция, то есть для каждого $M \in H$ существует единственный $m \in Msg$, такой, что $\pi(m) = M$.

Шифрование

Дано сообщение $m \in Msg$

1) Случайным образом выбирается натуральные число e;

2) Вычисляется $p^e \in Ker(\pi)$;

3) Шифртекст: $c = m * p^e \in G$, здесь $*$ обозначит группую операцию в G.

Дешифрование

1) $M = \pi(m * p^e) = \pi(m) \cdot \pi(m) = \pi(m)$, так как $\pi(m) = 1$;

2) Для M определяется $m \in Msg$ по известному соотвествию $\pi|_{Msg} : Msg \to H$

Таким образом, секретным ключом является число e, которое каждый раз выбирается по-новому, и способ нахождения по $M \in H$, элемента $(\pi|_{Msg})^{-1}(M) = m$.То есть тот, кто рашифровывает , должен знать, как по любому $M \in H$, найти $m \in Msg$ такой, что $\pi(m) = M$. И это должно быть секретом. Можно сказать, что функция $\pi|_{Msg}: Msg \to H$ является односторонной для тех, кто не знает секрета.

§ 2. Алгоритм умножения элементов в группе классов идеалов

Алгоритм умножения элементов в $Cl(\Delta_q)$, Δ_q—дискриминант.

Любой элемент $H = Cl(\Delta_q)$ задается парой чисел (a, b) таких, что

$$0 < a \leq \sqrt{|\Delta_q|/3}, \qquad -a < b \leq a, \qquad b^2 \equiv \Delta_q \pmod{4a}$$

(a, b)—это образующие дробного идеала, который является представителем смежного класса группы FI_k по подгруппе PI_k.

Исходные данные :

$(a_1, b_1), (a_2, b_2) \in Cl(\Delta_q)$ и дискриминант Δ_q

Шаг 1. Уравнение

$$d = ua_1 + va_2 + w(b_1 + b_2)/2$$

решается относительно $d, u, v, w \in \mathbb{Z}$ с использованием расширенного алгоритма Евклида.

Шаг 2. Положим

$$a = a_1 a_2 / d^2.$$

Шаг 3. Положим

$$b = b_2 + (va_2(b_1 - b_2) + w(\Delta_q - {b_2}^2)/2)/2 \pmod{2a}$$

Шаг 4. Положим

$$(\Delta_q - b^2)/4a.$$

Шаг 5. До тех пор, пока выполняется неравенство

$$-a < b \leq a < c$$

или неравенство

$$0 \leq b \leq a = c$$

выполнить действия:

1. Найти $\lambda\mu \in \mathbb{Z}$ такие, что

$$-a \leq \mu = b + 2\lambda a < a$$

используя деление, и взятие остатка.

2. Пусть

$$a = c - \lambda\frac{b+\mu}{2};$$

$$b = -\mu;$$

$$c = a.$$

Шаг 6. Если $a = c$ и одновременно $b < 0$, то положим $b = -b$

Выход: $(a, b) = (a_1, b_1) * (a_2, b_2)$

§ 3. Алгоритм вычисления гомоморфизма π

Вычисление $\pi : G \to H$, где $G = Cl(\Delta_1), H = Cl(\Delta_q)$

Исходнные данные:

Алгоритм:

Шаг 1. $b_{\mathcal{O}} = \Delta_q \pmod 2$

Шаг 2. Решаем уравнение

$$1 = uq + va$$

где $u, v \in \mathbb{Z}$ используя расширенный алгоритм Евклидаю

Шаг 3. $B = bu + ab_{\mathcal{O}}v \pmod{2a}$

Шаг 4.$C = (\Delta_1 - B^2)/4A$

Шаг 5.До тех пор, пока выполняются неравенство

$$-A < B \leq A < C$$

или неравенство

$$0 \leq B \leq A = C$$

выполнить действия :

1. Найти такие,что $\lambda\mu \in \mathbb{Z}$

$$-A \leq \mu = B + 2\lambda A < A$$

2. Пусть

$$A = C - \lambda\frac{B+\mu}{2};$$

$$B = -\mu;$$

$$C = A.$$

Шаг 6. Если $A = C$ и одновременно $B < 0$, то полагаем $B = -B$

На выходе получаем

$$(A, B) = \pi((a, b))$$

§ 4. Протокол шифрование

Сначала производится формирование ключа.

Для этого мы выбираем элемент $(m, b_p) \in Ker(\pi)$. Это элемент является общедоступным. Сообщение (m, b_m) —это элемент $Cl(\Delta_q)$, причём $m < [\sqrt{|\Delta_1|/4}]$.

Шифрование происходит в группе $Cl(\Delta_q)$ с помощью вычисления

$$(c, b_c) = ((m, b_m) * (p, b_p)^r)$$

где r—случайно выбранные число , и $r < 2^l$, где $l = log(q - (\frac{\Delta_1}{q}))$.

Тогда , зная секретную информацию , а иммено ,зная кондуктор , можно определить максимальный порядок и образ сообщения $\pi((m, b_m))$ в максимальным порядке . После этого можно найти (c, b_c) такой , что $\pi((c, b_c)) = \pi((m, b_m))$.

При расшиврование мы находим (m, b_m) , выбирая однозначно определяемый прообраз элемента $(d, b_d) = \pi((c, b_c))$. Для этого прообраза (m, b_m) известно ,что $d = m$.

Протокол шифрования $NICE$

1. Формирование ключа .

Выбераем два случайных простых числа $p, q > 4$ таких , что $p \equiv 3 \pmod 4$ и $\sqrt{p/4} < q$.

Пусть $\Delta_1 = -p$, и $\Delta_q = \Delta_1 q^2$.

Пусть k и l —длины записи чисел $[\sqrt{|\Delta_1|/4}]$ и $q - (\frac{\Delta_1}{q})$ (соовественно) в виде битовых строк (записи в двоичной системе счисления)

Выберем $(p, b_p) \in Cl(\Delta_q)$ так , чтобы

$$\pi((p, b_p)) = (1, 0)(1)$$

Тогда (p, b_p) , Δ_q , k , l —системные параметры , и q—секретный ключ .

2. Шифрование

Пусть $(m, b_m) \in Cl(\Delta_q)$—сообщение , причём $log_2 m < k$.

Выберем случайным образом $l - 1$ бит (нули или единицы)

$$(c, b_c) = ((m, b_m) * (p, b_p)^r)(2)$$

Тогда (c, b_c) есть шифротекст .

3. Рашифрование

Используя секретный ключ q , вычисляем $(d, b_d) = \pi((c, b_c))$.

Расшифровываемые сообщение находится как единственным способом выбранный прообраз (m, b_m) элемент (d, b_d).

Глава 4. Криптосистема NICE для действительных квадратичных полей

§ 1. Модификация криптосистемы NICE

Криптосистема NICE использует взаимосвязь между идеалами в максимальном и немаксимальном порядке простого кондуктора q, описанную в формулах (1) и (2) из параграфа 6 главы 2..

Образ идеалов из $\mathcal{O}_{\Delta_q}$ относительно ϕ^{-1} (Формула (1)) являются эффективно вычислимыми, если число q известно. В то же время, если "ловушка" q неизвестна (т.е только число $\mathcal{O}_{\Delta_q}$), задача становится трудной, и можно показать, что она эквивалентна задаче о разложении $\mathcal{O}_{\Delta_q}$ на множители за случайные полиномиалное время.

Описание алгоритма NICE

Секретный ключ: Два больших простых числа p и q, приблизительно одного размера, причём $p \equiv 3 \pmod 4$.

Открытый ключ: $(\mathcal{O}_{\Delta_q}, k, n, \mathfrak{p})$, где

1) $\Delta_q = q^2\Delta_1$, $\Delta_1 = -p$.

2) k и n имеют длину в битах $\lfloor\sqrt{|\Delta_1|}/4\rfloor$ и $q - (\Delta_1/q)$ соответственно.

3) $\mathfrak{p}$ есть случайно выбранный идеал из $\mathcal{O}_{\Delta_q}$, такой, что $[\mathfrak{p}] \in Ker(\hat{\Phi})$

Идеал $\mathfrak{p}$ можно найти, генерируя случайный элемент $\alpha \in \mathcal{O}_{\Delta_1}$, норма которого не делится на q, затем находя $\mathbb{Z}$ — базис главного $\mathcal{O}_{\Delta_1}$ — идеал $\mathfrak{A} = (\alpha)$, а затем вычисляя

$$\mathfrak{p} = \phi(\mathfrak{A})$$

Заметим, что идеал $\mathfrak{p}$ в общем случае не главный, но его образ $\phi^{-1}(\mathfrak{p})$ — главный идеал.

Шифрование : Шифрование сообщение — битовая строка длины $k-t$, где t — фиксированный параметр (будет объяснён ниже)

1) Сопоставым числу m примитивный $\mathcal{O}_{\Delta_q}$ — идеал $\mathfrak{m}$, взаимно простой с q, такой, что $N_{\Delta_q}(\mathfrak{m}) \leq 2^k$. Требуется, чтобы $N_{\Delta_q}(\mathfrak{m})$ однозначно определяло m.

2) Порождаем случайные $r \in 1, 2, \ldots, 2^{n-1}$.

3) Шифротекст есть редуцированный $\mathcal{O}_{\Delta_q}$ — идеал $\mathfrak{c} = \rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$.

Заметим, так так $2^{n-1} < q - (\frac{\Delta_1}{q}) < 2^n$, по выбору r на шаге 2 будем иметь

$$r < q - (\frac{\Delta_1}{q}) = |Ker(\hat{\Phi})|$$

Это оптимальное значение,так как $[\mathfrak{p}]^{q-(\frac{\Delta_1}{q})} = 1$ в $Cl(\mathcal{O}_{\Delta_q})$, т.е $\mathfrak{p}^{q-(\frac{\Delta_1}{q})}$ есть главный идеал.

Далее будем объяснено, как вычисляется идеал $\mathfrak{c}$.

Дешифрование : Чтобы расшифровать шифротекст идеал $\mathfrak{c}$, необходимо:

1) Вычислить $\mathfrak{M} = \rho_{\Delta_1}(\phi^{-1}(\mathfrak{c}))$

2) Извлечть m из $N_{\Delta_1}(\mathfrak{M})$.

Заметим, что из $[\mathfrak{p}] \in Ker(\hat{\Phi})$ и из (2) $\sigma 1$ следует, что

$$\begin{aligned}[\mathfrak{M}] = [\rho_{\Delta_1}(\phi^{-1}(\mathfrak{c}))] = [\phi^{-1}(\mathfrak{c})] = \hat{\Phi}([\mathfrak{c}])] = \hat{\Phi}[\rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)] \\ = \hat{\Phi}([\mathfrak{m}\mathfrak{p}^r]) = \hat{\Phi}([\mathfrak{m}])\hat{\Phi}([\mathfrak{p}])^r = \hat{\Phi}([\mathfrak{m}]) = [\phi^{-1}(\mathfrak{m})]\end{aligned}$$

Так как ϕ^{-1} сохраняет нормы идеалов и $2^{k-1} \leq \lfloor\sqrt{|\Delta_1|}/4\rfloor < 2^k$, то на шаге 1 алгоритма шифрования выполгено следующии :

$$N_{\Delta_1}(\phi^{-1}(\mathfrak{m}) = N_{\Delta_q}(\mathfrak{m}) \leq 2^k \leq 2\lfloor\frac{\sqrt{|\Delta_1|}}{4}\rfloor < \frac{\sqrt{|\Delta_1|}}{2}$$

Последнее неравенство следует из того, что $\lfloor\sqrt{|\Delta_1|}/4$ не является целым числом.

Таким образом, $\mathfrak{M}$ и $\phi^{-1}(\mathfrak{m})$ — редуцированные идеалы, принадлежащие к одному и тому же классу идеалов $\mathcal{O}_{\Delta_1}$ ($[\mathfrak{M}] = [\phi^{-1}(\mathfrak{m})]$ в $Cl(\mathcal{O}_{\Delta_1})$)

По тексти 2) теоремы 4 из $\sigma 1$ эти идеалы должны совпадать,

$$\mathfrak{M} = \phi^{-1}(\mathfrak{m})$$

Отсюда следует, что

$$N_{\Delta_1}(\mathfrak{M})) = N_{\Delta_1}(\phi^{-1}(\mathfrak{m})) = N_{\Delta_q}(mathfrakm)$$

Согласно шагу алгоритма шифрования 1, число однозначно определяет m

Заметим также, что

$$N_{\Delta_f}(\mathfrak{m}) = N_{\Delta_1}(\mathfrak{M}) < \sqrt{|\Delta_1|}/2 < q$$

где последнее неравенство выполняется потому что p и q, имеют одиноковый размер как битовые строкию

Идеал $\mathfrak{m}$ и $\mathfrak{M}$ — взаимно простые с q. Так как $N(\mathfrak{c}) = N(\mathfrak{m})N(\mathfrak{p})^r$, то идеал $\mathfrak{c}$ также является взаимно простым с q.

Так как расшифровывающий (Боб) знает кондуктор q порядка $\mathcal{O}_{\Delta_q}$, он может эффективно вычислить $\phi^{-1}(\mathfrak{c})$, а значит, и $\mathfrak{M}$, используя стандартную арифметику редукции. Как вычислить образ относительно ϕ^{-1}, будет объяснено делее.

Чтобы выполнить шаг 1 алгоритма шифрования, сначала надо выбрать параметр t. Шифруемый текст надо разбить на блок длины $k - t$ бит. Чтобы сопоставить блоку m редуцированный $\mathcal{O}_{\Delta_q}$ — идеал, взаимно простой с q, шифрующий (Алиса) должен выполнить следующий действия:

1) Положим $\bar{m} = m2^t$. Надо дабиться, чтобы $\bar{m}$ имело (как строка битов) длины k, причём t правых разрядов были нулевыми.

2)Найдем наименьшее простые $l > \bar{m}$, такое ,что $(\frac{\Delta_q}{e}) = 1$

3) Пусть $\mathfrak{m}$ есть идеал $\mathcal{O}_{\Delta_q}$, такое, что $N(\mathfrak{m}) = l$.

Если $l \equiv 3 \pmod 4$, что $\mathbb{Z}$ — базис $\mathfrak{m}$ можно вычислить эффективно, причём с помощью детерминистского алгоритма.

Если $l \equiv 1 \pmod 4$, то существует быстрый вероятностный метод для выполнения шага 3. Подробности ниже.

Если $l \leq \bar{m} + 2^t$, то $m \leq 2^{k-1} - 1$, откуда следует, что

$$N_{\Delta_f}(\mathfrak{m}) = l \leq \bar{m} + 2^t = (m+1)2^t \leq 2^k$$

что и требовалось.

Далее, k левых битов числа l (как строки битов) совпадают с соответствующими битами $\bar{m}$, а значит, и битами m.

Так как $N_{\Delta_1}(\mathfrak{M}) = N_{\Delta_q}(\mathfrak{m}) = l$, то m легко получается из $N_{\Delta_1}(\mathfrak{M})$ на шаге 2 дешифрования, с помощью отсечения первых k бит из стреки l. Вероятность того, что $l \leq \bar{m} + 2^t$ ограничена снизу числом $P_t = 1 - 2^{-2^t/k}$

Отсюда следует,что расшифровая на шаге 2 будет успешной с высокой вероятностью, если параметр t является достаточно большим числом.

Криптостойкость NICE детально проанализирована в статьях [14], [15], [17]. Она сводится к трудности разложения на множители числа Δ_q.

Опишем кратко, что известно о криптостойкости NICE.

Шифрование по NICE можно рассматривать как способ замаскировать сообщение, представленное идеалом $\mathfrak{m}$ с помощью умножения на случайно выбранный идеал $\mathfrak{a} = \mathfrak{p}^r$, где $[\mathfrak{a}] \in Ker(\hat{\Phi})$, то есть его сокрытия в $\mathfrak{m}Ker(\hat{\Phi})$.

Размер каждого такого множества равен $\|Ker(\hat{\Phi})\| = q - (\frac{\Delta_1}{q})$.При этом q надо выбрать достаточно большим, чтобы сделать поиск относительно $Ker(\hat{\Phi})$ максимально трудны.

Для того, чтобы гарантировать достаточно большое количество различних элементов вида $\mathfrak{m}Ker(\hat{\Phi})$ (или равносильн, достаточно большого количество различных степеней p^2), необходимо быть уверенным в том, что подгруппа в $Ker(\hat{\Phi})$, прожденной классом $[\mathfrak{p}]$.

Порядок этой подгруппы — делитель $q - (\frac{\Delta_1}{q})$, и это число должно выбрано простым или почти простым.

Допустим, что $q - (\frac{\Delta_1}{q}) = Ld$, где L — большое простое, а d — очень мало.

Тогда число образуюших циклической подгруппы группы $Ker(\hat{\Phi})$, порядка L равно $\varphi(L) = L - 1$.

Поэтому вероятность, того, что случайно выбранный идеал $\mathfrak{p} \in Ker(\hat{\Phi})$ порождает эту подгруппу, равна $(L-1)/Ld \approx 1/d$, и эта вероятность тем выше, чем меньше d. Ожидается, что d будет испытывать идеал $\mathfrak{p}$ для того, чтобы получить желаемый ключ.

Для любого такого испытания, проверка того, что

$$\rho_{\Delta_q}(\mathfrak{p}^d) \neq \mathcal{O}_{\Delta_q}$$

гарантирует, что $\mathfrak{p}$ порождает подгруппу $Ker(\hat{\Phi})$ порядка L.

Алгоритм, который вычисляет образы примитивных $\mathcal{O}_{\Delta_q}$, при неизвестном q, должен был бы расшифровывать любое сообщение.

Однако, по теореме 1 из статьи [15], такой алгоритм мог бы быть использован в качестве оракула для разложения Δ_q на множители за случайное полиномальное время.

Следовательно, криптостойность NICE эквивалентна сложности разложения на множители целого числа вида q^2p, где p,q должны быть выбраны достаточно большими, чтобы обезопасить от разложения Δ_q с помощью эллиптической кривой методом решета числового поля.

Размеры параметров p и q, рекомендованные NIST

symmetric key size	80	112	128	192	256
Size of Δ_q	1024	2048	3072	8192	15360
Size of p and q	341	682	1042	2731	5120

§ 2. Арифметика идеалов

Пусть $K = \mathbb{Q}(\sqrt{D})$, и $\mathcal{O}_{\Delta_f}$ — порядок в K с кондуктором f.

Пусть $\sigma = 1$, если $D \equiv 2, 3 \pmod 4$ и $\sigma = 2$ если $D \equiv 1 \pmod 4$

Отсюда $\Delta_1 = (2/\sigma)^2 D \equiv \sigma - 1 \pmod 4$. В этих обозначениях каждый целый $\mathcal{O}_{\Delta_f}$

В этих обозначениях каждый целый $\mathcal{O}_{\Delta_f}$ — идеал $\mathfrak{a}$, есть $\mathbb{Z}$ — модуль вида:

$$\mathfrak{a} = S\left\{\frac{Q}{\sigma}\mathbb{Z} + \frac{p + f\sqrt{D}}{\sigma}\mathbb{Z}\right\}$$

где $S, Q \in \mathbb{N}$, $P \in \mathbb{Z}$,σ делит Q, σQ делит $f^2D - P^2$, и $gcd(Q, 2P, (f^2D - P^2)/Q) = \sigma$. Здесь Q и S определены однозначно, $\mathfrak{a}$ число P, однозначно по модулю Q.

При этом

$$N_{\Delta_f}(\mathfrak{a}) = S^2 Q/\sigma$$

Идеал $\mathfrak{a}$ примитивен тогда и только тогда, если $S = 1$. В этом случае можно для краткости писать, $\mathfrak{a} = (Q, P)$.

§ 3. Особенности криптосистемы NICE для действительных квадратичных полей

Криптосистему REAL-NICE можно описать следующим образом.

Секретный ключ: Два больших простых числа p и q, приблизительно одинакового размера, причём $p \equiv 1 \pmod 4$.

Открытый ключ: $(\mathcal{O}_{\Delta_q}, k, n, \mathfrak{p})$ или $(\mathcal{O}_{\Delta_q}, k, n)$, где

1) $\Delta_q = q^2\Delta_1$, $\Delta_1 = -p$.

2) k и n как битовые строки имеют длины $\lfloor\sqrt{|\Delta_1|}/4\rfloor$ и $q - (\frac{\Delta_1}{q})$ соответственно.

3) $\mathfrak{p}$ — случайно выбранный идеал из $\mathcal{O}_{\Delta_q}$, такой, что $[\mathfrak{p}] \in Ker(\hat{\Phi})$

При этом p и q надо выбрать так, чтобы R_{Δ_1} было небольными, а R_{Δ_q} было очень большим. Подробнее об этом будет сказано ниже.

Если область возможных ключей ограничена, то $\mathfrak{p}$ можно не включать в число открытых ключей.

В самом деле, другой идеал $\mathfrak{p}$ с $[\mathfrak{p}] \in Ker(\hat{\Phi})$, может порождается при каждом шифровании, что увеличивает время шифрования. Если $\mathfrak{p}$ включается в число открытых ключей, его можно построить так же, как и в первоначальной криптосистеме NICE

Далее будет описано, как по другому можно найти $\mathfrak{p}$, не зная q и Δ_1. Это можно использовать при шифровании.

Шифрование : Шифруемое сообщение — битовая строка длины $k - t - u$, где t и u — фиксированные параметры, смысл которых объясняется ниже.

1) Строка m преобразуется в строку m', которая однозначно определяется m и содержит битовый шаблон длины u.

2) Сопоставим строке m' примитивный ($\mathcal{O}_{\Delta_q}$ — идеал $\mathfrak{m}$, взаимно простой с q, такой что $N_{\Delta_q}(\mathfrak{m}) \leq 2^k$. Требуется, чтобы по числу $N_{\Delta_q}(\mathfrak{m})$ можно было однозначно определить m'.

3) Выберем случайным образом $r \in 1, 2, \ldots, 2^{n-1}$.

4) Если открытый ключ не содержит идеал $\mathfrak{p}$, порождем случайным образом идеал $\mathfrak{p}$ такой, что $[\mathfrak{p}] \in Ker(\hat{\Phi})$.

5) Шифротекст есть редуцированный $\mathcal{O}_{\Delta_q}$ — идеал $\mathfrak{c} = \rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$.

Дешифрование : Чтобы расшифровать шифротекст идеал $\mathfrak{c}$ (идеал $\mathcal{O}_{\Delta_q}$), требуется :

1) Вычислить $\mathfrak{C} = \phi^{-1}(\mathfrak{c})$.

2) Найти редуцированный идеал $\mathfrak{M} \in [\mathfrak{C}]$ такой, что $N_{\Delta_1}(\mathfrak{M})$ содержит битовый шаблон, длины u, сформированный на шаге 1 алгоритма шифрования.

3) Из $N_{\Delta_1}(\mathfrak{M})$ получить m', а из m' получить m.

Так как расшифровывающий знает q, он может эффективно вычислить $\mathfrak{C}$.

Как и в первоначальном алгоритм NICE, $[\mathfrak{M}] = [\phi^{-1}(\mathfrak{m})]$.

К сожалению, отсюда не следует, что $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$, а следует только, что это два идеала из множества редуцированных идеалов, взаимно простых с q, содержащихся в одном и том же классе $\mathcal{O}_{\Delta_q}$ — идеалов. В этом причина того, что в отличие от NICE для мнилых полей, сопоставление сообщению m.

$\mathcal{O}_{\Delta_q}$ — идеала $\mathfrak{m}$ требует двух шагов. Для того, чтобы была уверенность, что $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$, m должен быть снабжен открытым битовым шаблоком длины u, для того, чтобы получить m'.

Ниже будут приведены аргументы в пользу того, что это позволяет получить $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$ с высокой вероятностью, поэтому $N_{\Delta_1}(\mathfrak{M}) =$

$N_{\Delta_q}(\mathfrak{m})$ с этой же вероятностью будет однозначно определять m' согласно шагу 2 шифрования.

Более точно, чтобы выполнить шаги 1 и 2 шифрования, надо сначала выбрать большие параметры t и u

Шифруемый текст надо разбить на блоки длины $k-t-u$ бит. Чтобы сопоставить блоку m редуцированный $\mathcal{O}_{\Delta_q}$ — идеал $\mathfrak{m}$, взаимно простой с q, необходимо выполнить следующее :

1) Положим $m' = m + 2^{k-t}$ так, чтобы m' имело битовую длину $k-t$, причём u левых бит были такими: $100\ldots00$.

2) Положим $\bar{m}' = m'2^t$.Получится число $\bar{m}'$ длиной (как строка битов) k бит таковы :$100\ldots00$, а t правых бит (разрядов)

3) Найдем наименьшее простое число $l > \bar{m}'$, такое, что $\frac{\Delta_q}{l} = 1$

4) Пусть $\mathfrak{m}$ есть $\mathcal{O}_{\Delta_q}$ — идеал, норма которого равна l.

Идеал $\mathfrak{m}$ можно найти так же, как и в первоначальном алгоритме NICE, и при условии $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$ число m' может быть найдено по числу $N_{\Delta_1}(\mathfrak{M}) = N_{\Delta_q}(\mathfrak{m}) = l$ с высокой вероятностью, после отбрасывания из l правых k бит. После этого m получается из m' простым удалением u правых бит m'.

Выше было обосновано, что с высокой вероятностью класс $[\mathfrak{C}]$ содержит единственный идеал, норма которого содержит уже упоминавшийся битовый шаблон. Это будет идеал $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$ с нормой.

Объясним, как найти этот идеал. Для этого расшифровывающему необходимо обозреть множество редуцированных $\mathcal{O}_{\Delta_1}$ — идеалов из класса $\mathfrak{C}$, чтобы выбрать из него $\mathfrak{M}$.

Это можно выполнить, используя повторяющийся алглритм "шаги младенца взяв за исходных данные $\mathcal{O}_{\Delta_1}$ — идеал $\mathfrak{C} \in [\mathfrak{M}]$.

Так как Δ_1 выбран таким образом, что класс $\mathfrak{C}$ содержит очень мало

редуцированных идеалв, идеал $\mathfrak{M}$ можно найти эффективно.

После каждого "шага младенца"расшифровывающий (Боб) выполняет простые операции XOR (исключающее "или"$\oplus$) с левыми u битам нормы идеала, где содержится строка $100\ldots00$. При этом каждый раз проверяется, будет или нет получающаяся строка содержать только нули.

Процедура расшифрования будет работать с высокой вероятностью при двух условиях.

Во-первых, так же как в NICE для мнимых полей, параметр t надо выбрать, как описано выше в § 6 главы 2, чтобы была уверенность, что m' можно однозначно определить по идеалу $\mathfrak{M}$.

Выше уже говорилось, что успешность такого выбора возможна с вероятностью по крайней мере (самое меньшее) $P_t = 1 - 2^{-2^t/k}$

Во-вторых. число u должно быть выбрано достаточно большим, чтобы с высокой вероятностью, класс идеал $\mathfrak{C}$ в ($\mathcal{O}_{\Delta_1}$ содержал только один редуцированный ($\mathcal{O}_{\Delta_1}$ — идеал $\mathfrak{M}$ такое, что u левых битов в $N_{\Delta_1}(\mathfrak{M})$ были такими $100\ldots00$.

В [17] на странице 53 показано, что эта вероятность ограничена снизу числом $P_u = (1 - 2^{-u})^N$, где N есть верхняя граница количества редуцированных идеалов в каждом классе $Cl(\Delta_1)$. Далее будет показано, что Δ_1 можно выбрать так, что эта верхняя граница имеет вид $\kappa_1 log(\Delta_1)$ для некоторой точно вычисляемой константы κ_1.

Параметры в криптосистеме REAL-NICE должны выбираться исходя из соображений эффективности и криптостойности.

Число p и q должны удовлетворять следующим условиям

1) R_{Δ_q} должен быть достаточно большим, чтобы обеспечить достаточно большое количество редуцированных идеалов в каждом классе $\mathcal{O}_{\Delta_q}$ — идеалов.

2) R_{Δ_1} должен быть достаточно небольшим, что обеспечить достаточно небольшое количество редуцированных идеалов в каждом классе $\mathcal{O}_{\Delta_1}$ — идеал.

Эти условия достигаюся за два шага. Во-первых, утвердается, что частное $\mathcal{O}_{\Delta_q}/\mathcal{O}_{\Delta_1}$ с высокой вероятностью есть порядок изменения q. Затем будут высказаны соображения, гарантирующие, что R_{Δ_1} мал, т.е ограничен полиномом от $\log(\Delta_1)$.

Индекс единиц $\mathcal{O}_{\Delta_q}$ есть по определению индекс $[\mathcal{O}^*_{\Delta_1} : \mathcal{O}^*_{\Delta_q}]$, где $\mathcal{O}^*_{\Delta_1}$ — группа единиц (т.е обратимых элементов) кольца $\mathcal{O}_{\Delta_1}$ и $\mathcal{O}^*_{\Delta_q}$ — группа единиц $\mathcal{O}_{\Delta_q}$. Это наименьшее положительное число, такое, что $\epsilon^i_{\Delta_1} = \epsilon_{\Delta_f}$, или, что равносильно, $R_{\Delta_f} = iR_{\Delta_1}$. Согласно формуле (3) из § 6 главы 2, i делит $q - (\frac{\Delta_1}{q})$. Поэтому, если сделать i большим, то $q - (\frac{\Delta_1}{q})$ станет почти простым.

Теорема 5.8 на странице с 58 [17] утверждает, что есть $q - (\frac{\Delta_1}{q}) = Ld$, где L — большое простое число, и $d \leq \log(\Delta_1)^\kappa$ для некоторой константы $\kappa > 0$, то вероятность того, что $i < L$, ограничена сверху числом

$$\log(\Delta_1)^{2\kappa}/(\sqrt{\Delta_1} - 1)$$

Другими словами,

$$i = R_{\Delta_q}/R_{\Delta_1} \geq L$$

с гарантировано высокой вероятностью.

Чтобы проверить $i \geq L$, достаточно проверить, что i не делит d, т.е $\epsilon^d_{\Delta_1} \neq \epsilon_{\Delta_f}$.

Допустим, что R_{Δ_1} достаточно мал, так что $\epsilon_{\Delta_1} = u_1 + v_1\sqrt{\Delta_1}$ эффективно вычислимая величина.

Тогда любую степень

$$\epsilon^j_{\Delta_1} = u_j + v_j\sqrt{\Delta_1}$$

также можно эффективно вычислить, используя функцию Люка.

Далее, покажем, как выбрать Δ_1 так, чтобы регулятор R_{Δ_1} оказался маленьким.

В общем случае R_{Δ_f} для любого квадратичного порядка $\mathcal{O}_{\Delta_f}$ имеет *magnitude* $\sqrt{\Delta_f}$, и это число слишком велико.

Можно выбрать в качестве D положительное свободное от квадратов целое число вида

$$D = D(x) = a^2x^2 + 2bx + c$$

где $a, b, c, x \in \mathbb{Z}$, $a \neq 0$ и $b^2 - a^2c$ делит $4gcd(a^2, b)^2$.

Можно показать, что регулятор R_{Δ_1} имеет тот же порядок, что и $\log(\Delta_1)$.

Если a, b, c, κ выбраны так, что число $gcd(a^2, 2b, c)$ свлбодно от квадратов $D \equiv 0, 1 \pmod 4$ (поэтому $\Delta_1 = D$), то по теореме 5.4 страница 52 из [17], количество редуцированных $\mathcal{O}_{\Delta_1}$ — идеал в каждом классе из $Cl(\mathcal{O}_{\Delta_1})$ огранично сверху число $\kappa_1 \log(\Delta_1)$ для некоторой точно вычисляемой константы κ_1, которая зависит только от a и b.

Наконец, фиксированный битовый шаблон в каждом сообщении является в REAL-NICE необходиммым для противодействии атаки с выбранным шифротекстом ([14]).

Эта атака может быть обнаружена с той же вероятностью, с которой идеал — зашифрованное сообщение — может быть успешно расшифрован.

Список литературы

[1] Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. — М.: Мир, 1987. — 416 с.

[2] Атья М., Макдональд И. Введение в коммутативную алгебру. — М.: МИР, 1972. —160 с.

[3] Боревич З.И., Шафаревич И.Р. Теория чисел. — 3-е изд., доп. — М.:Наука. Гл.ред. физ.-мат.лит., 1985. — 504 с.

[4] Введение в криптографию/ Под общ. ред. В.В.Ященко. — 3-е изд., доп. — М.: МЦНМО: «ЧеРо», 2000. — 288 с.

[5] Глухов М.М. Об использовании групп классов идеалов квадратичных полей для построения криптографических систем с открытым ключом // Математические вопросы криптографии. — 2010. — Т. 1. — № 1. — С. 23–54.

[6] Зарисский О., Самюэль П. Коммутативная алгебра. Том 1. — М.: Изд-во Иностранной Литературы, 1963. — 373 с.

[7] Ленг С. Алгебра. — М.: Мир, 1968. — 564 с.

[8] Манин Ю.И., Панчишкин А.А. Введение в совеременную теорию чисел. — М.: МЦНМО, 2009. — 552 с.

[9] Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учебное пособие для вузов.— М.: Горячая линия-Телеком, 2005. — 229 с.

[10] Смарт Н. Криптография.— М.: Техносфера, 2005.—528 с.

[11] Hartmann M., Paulus S., Takagi T. NICE — New Ideal Coset Encryption // Lecture Notes in Computer Science. — 1999. — Vol. 1717. — P. 341–352.

[12] Huhnlein D., Jacobson M.,Jr., Paulus S., Takagi T. A cryptosystem based on non-maximal imaginary quadratic orders with fast decryption // EUROCRYPT'98. — Lecture Notes in Computer Science. — 1998. — Vol. 1403.— P. 294–307.

[13] Jacobson M.J., Scheidler R., Weimer D. An Adaptation of the NICE Cryptosystem in Real Quadratic Orders // AFRICACRYPT 2008. — Lecture Notes in Computer Science. — 2008. — Vol. 5023.— P. 191–208.

[14] Jaulmes E., Joux A. A NICE Cryptanalysis // EUROCRYPT 2000. — Lecture Notes in Computer Science. — 2000. — Vol. 1807. — P. 282-391.

[15] Paulus S., Takagi T. A New Public-Key Cryptosystem over a Quadratic Order with Quadratic Decryption Time // Journal of Cryptology. — 2000. — V. 13. — P. 263–272.

[16] Takagi T. New publik-key cryptosystems with fast decryption. — Dissertation (Dr.rer. nat.) — Darmstadt, 2001. — x+63 p.

[17] Weimer D. An Adaptation of the NICE Cryptosystem to Real Quadratic Orders. — Master's Thesis. — Darmstadt, 2004. — xv+110 p.