МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«НОВОСИБИРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» (НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ, НГУ)

Кафедра компьютерных систем

Спицына Екатерина Олеговна

Применение полиномиальных отображений для создания криптографических примитивов

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ
по направлению высшего профессионального образования

230100.68 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Тема диссертации утверждена распоряжением по НГУ № 4 от «11» января 2012г.

Руководитель

Кренделев С. Ф.
к. ф.-м. н., доцент КафМА ММФ НГУ

Новосибирск, 2013г.

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«НОВОСИБИРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» (НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ, НГУ)

Кафедра компьютерных систем

УТВЕРЖДАЮ

Зав. Кафедрой Пищик Б. Н.

…….
(подпись, дата)

ЗАДАНИЕ
на магистерскую диссертацию

студент Спицына Екатерина Олеговна

факультета ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Направление подготовки 230100.68 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Магистерская программа «Безопасность и защита информации»

Тема «Применение полиномиальных отображений для создания криптографических примитивов»

Цели работы: разработать алгоритм построения взаимно однозначных полиномиальных отображений над кольцами, предложить и программно реализовать систему шифрования с открытым ключом, основанную на полиномиальных отображениях над кольцами, исследовать ее криптостойкость и области применения.

Руководитель

Кренделев С. Ф.
к. ф.-м. н., доцент КафМА ММФ НГУ

……..
(подпись, дата)

Содержание

ВВЕДЕНИЕ

Проблема сокрытия секретных данных при их хранении или передаче стояла перед человечеством с древнейших времен: одними из первых известных нам ее решений были шифр Цезаря и скитала, являющиеся шифрами подстановки. Также примеры применения криптографии можно встретить в древнем Египте, Индии Месопотамии; всего история криптографии насчитывает около 4 тысяч лет.

Со времени первых упоминаний о криптографии было разработано множество криптосистем, и область их применения значительно расширилась. В настоящее время шифрованию подвергаются уже не только тексты документов, но и голосовые данные и изображения; шифры используется в банковских операциях, сотовой связи, цифровом телевидении и многих других областях. На вновь создающиеся криптосистемы накладывается ряд общепринятых требований, касающихся возможности их аппаратной реализации, быстродействия и надежности. В связи с ростом мощности процессоров последний пункт получает особенно высокое значение: дешифрование путем перебора всех возможных ключей системы зачастую может быть легко осуществлено на современных ЭВМ. Именно поэтому при разработке системы, описываемой в данной работе, в первую очередь уделялось внимание вопросам криптостойкости. Предлагаемая криптосистема основывается на широко известном асимметричном алгоритме шифрования RSA, предложенном в 1977 году Рональдом Райвестом (Ronald Linn Rivest), Ади Шамиром (Adi Shamir) и Леонардом Адлеманом (Leonard Adleman) [10], превосходя его в надежности и скорости. Была разработана библиотека, осуществляющая операции шифрования и дешифрования в соответствии с полученным алгоритмом.

Поскольку в основе предлагаемой системы лежат взаимно однозначные полиномиальные отображения над кольцами, первая часть работы посвящена поиску таких отображений. С целью выявления алгоритма построения были проведены эксперименты, которые позволили получить способ построения взаимно однозначных многочленов, наиболее подходящих под условия поставленной задачи.

1 Содержательная постановка задачи

Методы шифрования информации – это обратимое преобразования открытого (исходного) текста на основе секретного алгоритма и/или ключа в шифрованный текст (шифротекст). Первые криптосистемы были симметричными, то есть операции шифрования и дешифрования в них осуществлялись с применением одного и того же ключа, который должен был быть известен обеим сторонам. Среди таких систем выделяют две группы: потоковые шифры, обрабатывающие отдельно каждый бит исходного текста (RC4, WAKE), и блочные шифры, преобразующие блоки исходного текста на протяжении определенного числа раундов (DES, AES, Blowfish, RC2, IDEA). Несмотря на свои достоинства – простоту реализации, сравнительно большую скорость и меньшую требуемую длину ключа, использование симметричного шифра предполагает наличие секретного канала связи для надежной передачи ключа между абонентами, а также ставит перед разработчиком задачу проверки подлинности. Эти недостатки значительно сокращают область применения симметричных систем.

Системы шифрования с открытым ключом, появившиеся в конце 70-х годов прошлого века, используют открытый (публичный) ключ для шифрования сообщения и секретный (приватный) для дешифрования. Таким образом, при их использовании требуется лишь незащищенный канал связи для распространения публичного ключа; приватный ключ известен только адресату и не требует передачи. Схема работы асимметричной системы шифрования представлена на рисунке 1: (e,d) – пара публичного и приватного ключей, $E_e(m), D_d(c)$ – функции шифратора и дешифратора, m – исходное сообщение, c – шифротекст. Большинство таких алгоритмов основано на вычислительно однонаправленных задачах: задаче дискретного логарифмирования в различных алгебраических структурах (система Эль-Гамаля, ГОСТ Р. 34.10-2001) и факторизации (RSA). Асимметричные системы уступают системам с секретным ключом в скорости и длине ключей, поэтому распространение получили гибридные системы, сочетающие преимущества обоих подходов: для шифрования данных применяется симметричный шифр, а секретный ключ шифруется с использованием асимметричного алгоритма (протоколы TLS и PGP). Современные исследования в области традиционной криптографии направлены на создание и анализ надежности алгоритмов шифрования и протоколов.

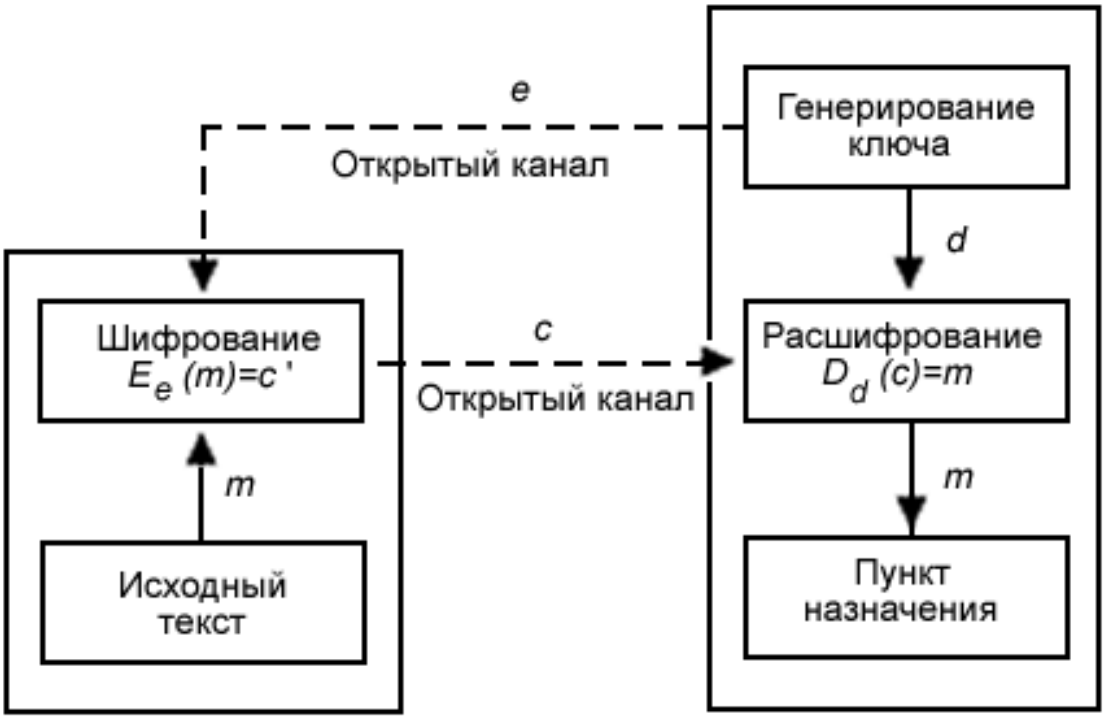

Рисунок 1. Система шифрования с секретным ключом

Взаимно однозначные полиномиальные отображения применяются во многих известных методах шифрования. Наиболее распространены полиномиальные отображения над конечными полями: в качестве примера таких методов можно рассмотреть асимметричные системы Эль-Гамаля, HFE (hidden field equations) [9] или TRMC (tractable rational map cryptosystem) [11]. В отличие от них криптосистема RSA, имеющая широкое применение в большом числе криптографических приложений для защиты программного обеспечения и в схемах цифровой подписи, использует взаимно однозначные полиномиальные отображения над кольцами для генерации пары ключей. Такие отображения представляют наибольший интерес для анализа ввиду отсутствия общей теории их получения. Данное обстоятельство послужило причиной выбора алгоритма RSA в качестве основы для построения новой системы, расширяющей класс используемых отображений и улучшающей основные его показатели.

2 Математическая постановка задачи

Алгоритм генерации пары ключей RSA состоит из следующих этапов:

1. Выбираются два случайных простых числа p, q.
2. Вычисляется модуль $n = p * q$, служащий основанием кольца вычетов Z_n.
3. Выбирается открытая экспонента e, обратимая в кольце $Z_{\varphi(n)}$. Это означает, что $НОД(e, \varphi(n)) = 1$, где $\varphi(n)$ – функция Эйлера.
4. Вычисляется секретная экспонента d, мультипликативно обратная к экспоненте e в кольце $Z_{\varphi(n)}$.

Таким образом, пара (e, n) выступает в роли публичного ключа, $\Phi(x) = x^e (\mathrm{mod}\, n)$ – функция шифратора. Приватным ключом является пара (d, n), а $S(y) = y^d (\mathrm{mod}\, n)$ – функция дешифратора.

При фиксированном n мощность множества допустимых для RSA отображений равняется количеству обратимых элементов в кольце $Z_{\varphi(n)}$, а именно $\varphi(\varphi(n))$. Это число много меньше $n!$ – количества всех перестановок над кольцом Z_n. Возникает вопрос о том, как получить оставшиеся полиномиальные взаимно однозначные отображения, и как их использование для построения пары ключей отразится на криптостойкости и быстродействии полученной системы.

3 Построение взаимно однозначных отображений над кольцами

Пусть Z_p – поле, p – простое. Все взаимно однозначные отображения над полем являются полиномиальными, так как они могут быть получены в результате применения интерполяции Лагранжа. Множество взаимно однозначных полиномов степени меньше p над полем Z_p образует группу относительно операции композиции. Указанная группа изоморфна симметрической группе S_p – группе всех перестановок на множестве из p элементов. Согласно теореме о перестановочных многочленах, группа S_p порождается многочленами $cx, x+1, x^{p-2}$ [6]. Следовательно, взаимно однозначные полиномиальные отображения над полями – это всевозможные суперпозиции отображений вида:

$$P(x) = (ax+b)^e + d, \tag{3.1}$$

где $a \in Z_p$, $a \neq 0$, b, d – произвольные элементы из Z_p, e – обратимый элемент в кольце Z_{p-1}.

Если p не является простым, то общая теория чисел не дает ответа на вопрос, как построить необходимые взаимно однозначные отображения. Применение интерполяционной формулы Лагранжа невозможно, так как при использовании интерполяции стандартными методами матрица Вандермонда оказывается вырожденной, следовательно, невозможно задать значения многочлена в точках произвольным образом. В ходе исследований были рассмотрены два варианта построения отображений.

3.1 Вариант первый: представление в виде суперпозиции

Пусть n – составное натуральное число, тогда Z_n – кольцо. В первоначальных исследованиях предлагалось обобщить описанное выше правило построения отображений над полями и использовать отображения вида (3.1) для получения полиномиальных взаимно однозначных отображений над кольцами. Таким образом, требуемые отображения над кольцом Z_n можно получить, применяя операцию суперпозиции к элементарным отображениям $x^e, ax, x+d$, то есть рассматривались всевозможные отображение вида:

$$P(x) = (...(a_2(a_1x + d_1)^{e_1} + d_2)^{e_2} + d_3)...) + d_r, \quad (3.2)$$

$a_1...a_r, d_1...d_r \in Z_n$, $a_1...a_r \neq 0$, $e_1...e_{r-1}$ обратимы в $Z_{\varphi(n)}$. После раскрытия скобок и приведения подобных этот полином может использоваться для построения открытого и секретного ключей криптосистемы или же выступать в качестве самостоятельного открытого ключа. Серьезный недостаток такого подхода, однако, состоит в том, что если в выражении для многочлена $P(x)$ показатели $e_1...e_{r-1}$ малы по сравнению с n, то все элементарные отображения, входящие в состав $P(x)$, находятся за полиномиальное время, и шифр вскрывается. С ростом показателей $e_1...e_{r-1}$ происходит увеличение количества слагаемых в выражении (3.2), и, как следствие, увеличение размера ключа. Кроме того, высокая степень ключа приводит к значительному увеличению временных затрат на операции шифрования и дешифрования.

3.2 Вариант второй: сведение к полиномам над полями

Второй подход к проблеме построения отображений состоит в сведении задачи поиска полиномиальных взаимно однозначных отображений над кольцами к задаче поиска полиномиальных взаимно однозначных отображений над полями. Действительно, пусть Z_n – кольцо вычетов по модулю n, где n – произвольное натуральное число. Предположим, что $P(x)$ – искомый полином, то есть полином, который отображает множество Z_n в себя взаимно однозначно. Данное условие на отображение $P(x)$ означает, что уравнение $P(x) = a$ всегда имеет решение, причем оно единственно для всякого $a \in Z_n$.

Произведем факторизацию числа n:

$$n = p_1^{k_1} p_2^{k_2} ... p_s^{k_s}, \quad (3.3)$$

где $p_1, p_2...p_s$ – простые числа, $k_1, k_2...k_s \in N$. Согласно элементарной теории чисел, разрешимость уравнения $P(x) = a(\mathrm{mod}\, n)$ эквивалентна разрешимости системы уравнений $P(x) = a(\mathrm{mod}\, p_i^{k_i})$, $i = 1...s$ [2]. Этот набор уравнений сводится к разрешимости системы уравнений $P(x) = a(\mathrm{mod}\, p_i)$, $i = 1...s$. Поэтому без ограничения общности можно считать, что $k_1 = k_2 = ... = k_s = 1$. Отсюда следует, что при построении отображений над

кольцами можно воспользоваться отображениями над полями, которые являются более детально изученными. Разработанный алгоритм состоит из следующих этапов:

1 Генерируются взаимно однозначные полиномиальные отображения $f_1(x)...f_s(x)$ над полями $Z_{p_1}...Z_{p_s}$ соответственно. Для этого для каждого $i=1...s$ фиксируется набор элементарных отображений $q_1^i(x)...q_{m_i}^i(x)$ вида (3.1) и вычисляется их суперпозиция: $f_i(x)=q_1^i(q_2^i(..q_{m_i}^i(x)..))(\mathrm{mod}\, Z_{p_i})$.

2 Затем полиномы $f_1(x)...f_s(x)$ собираются в полином над кольцом Z_n с применением Китайской теоремы об остатках. Пусть $f_i(x)=a_i^0+a_i^1x+a_i^2x^2+...$, $i=1...s$. Тогда результирующий многочлен $h(x)$ над кольцом Z_n будет иметь вид:

$$h(x)=c^0+c^1x+c^2x^2+..., \tag{3.4}$$

где $c^j=a_i^j(\mathrm{mod}\, p_i)$, $i=1...s$, $j=0,1,2....$

В алгоритме RSA данная схема имеет вырожденный вид: если положить, что $n=p_1p_2$, где p_1, p_2 – простые, то выбирается элемент e, обратимый одновременно в кольцах Z_{p_1-1} и Z_{p_2-1}. Тогда $P(x)=x^e$ – взаимно однозначное отображение в полях Z_{p_1-1} и Z_{p_2-1}, а следовательно и в Z_n.

3.3 Пример

Проиллюстрируем шаги, описанные в пункте (3.2), в случае кольца вычетов небольшой размерности. Пусть вычисления ведутся в Z_{2737}, разложив модуль на простые сомножители, получим: $2737=7*17*23$, таким образом $p_1=7, p_2=17, p_3=23$.

1 Для каждого p_i определяется взаимно однозначный над кольцом Z_{p_i} полином.

- Для p_1: $q_1^1(x)=x+1, q_2^1(x)=5x, q_3^1(x)=x+6$. Вычисляя суперпозицию, $f_{p_1}(x)=f_1(f_2(f_3(x)))=5x+31=5x+3(\mathrm{mod}\, 7)$.

- Для p_2: $q_1^2(x) = x + 10, q_2^2(x) = 2x^5, q_3^2(x) = 7x$. Вычисляя суперпозицию, $f_{p_2}(x) = f_1(f_2(f_3(x))) = 5x^5 + 10 (\mathrm{mod} 17)$.

- Для p_3: $q_1^3(x) = 2x + 3, q_2^3(x) = 12x, q_3^3(x) = x^7$. Вычисляя суперпозицию, $f_{p_3}(x) = f_1(f_3(f_2(x))) = 9x^7 + 3 (\mathrm{mod}\, 23)$.

2 Пусть искомый полином $h(x)$ имеет вид $h(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 + a_7x^7$. Для того, чтобы вычислить значение коэффициента a_0, необходимо найти решение системы уравнений:

$$\begin{aligned} a_0 &= 3 (\mathrm{mod}\, 7) \\ a_0 &= 10 (\mathrm{mod} 17) \\ a_0 &= 3 (\mathrm{mod}\, 23). \end{aligned} \qquad (3.5)$$

Поскольку числа $7, 17, 23$ являются взаимно простыми, данная система может быть решена с использованием Китайской теоремы об остатках.

В соответствии с алгоритмом Гаусса, основанном на данной теореме, следует положить:

$$a_0 = M_1y_1 + M_2y_2 + M_3y_3 (\mathrm{mod}\, n), \qquad (3.6)$$

где на переменный y_1, y_2, y_3 накладывается ряд ограничений:

$$\begin{aligned} M_1y_1 &= 3 (\mathrm{mod}\, 7) \\ M_2y_2 &= 10 (\mathrm{mod} 17) \\ M_3y_3 &= 3 (\mathrm{mod}\, 23), \end{aligned} \qquad (3.7)$$

и коэффициенты имеют значения $M_1 = 17 * 23 = 391, M_2 = 7 * 23 = 161, M_3 = 7 * 17 = 119$.

Решая систему (3.7) с применением расширенного алгоритма Евклида, получаем значения $y_1 = 4, y_2 = 14, y_3 = 18$, следовательно, $a_0 = 4M_1 + 14M_2 + 18M_3 = 1564 + 2254 + 2142 = 486 (\mathrm{mod}\, 2737)$.

Повторяя данный алгоритм для остальных коэффициентов a_i, $i = 1..6$, вычисляем значение искомого полинома $h(x) = 929x^7 + 1110x^5 + 775x + 486$.

3.4 Выводы

Отображения, полученные в результате работы алгоритма (3.4), являются взаимно однозначными полиномиальными отображениями над кольцом по построению. Предложенный алгоритм может быть реализован программно и распараллелен с целью увеличения скорости работы.

Вычислительные эксперименты показали, что длины циклов отображения $h(x)$ превосходят длины циклов исходных отображений $f_1(x)...f_s(x)$, что делает отображения типа $h(x)$ наиболее подходящими для последующего использования в криптографическом примитиве ввиду устойчивости таких отображений к так называемым циклическим атакам.

4 Система шифрования с открытым ключом

Полином, полученный с использованием формулы (3.4), задает взаимно однозначное отображение из кольца в себя, следовательно, может быть использован в качестве открытого ключа криптографического примитива. Однако при работе с числами по модулю, к примеру, 2737, такой примитив позволит зашифровать $\log_2 2737 \approx 11.5$ бит информации. Для того чтобы иметь возможность зашифровать блок данных из хотя бы 256 бит (то есть 23 числа из кольца вычетов Z_{2737}), конструкцию открытого ключа необходимо усложнить.

4.1 Генерация ключевой пары

Рассмотрим векторное пространство Z_n^k над кольцом Z_n. В основе открытого ключа будет лежать диагональное отображение, заданное взаимно однозначными полиномами над кольцом Z_n (3.4). Для повышения криптостойкости перед применением данного диагонального отображения необходимо сделать замену переменных в открытом тексте, то есть подействовать на него некоторым обратимым аффинным отображением. Очевидно, что даже в таком линейном случае замена переменных сильно увеличит размер результирующего открытого ключа за счет появления дополнительных слагаемых в качестве аргументов диагонального отображения. Поэтому на матрицу аффинного отображения накладывается условие: в каждой строке она должна иметь не более 3 ненулевых компонентов.

После применения диагонального отображения компоненты полученного вектора следует еще раз перемешать при помощи преобразования, обратное к которому может быть легко вычислено. С этой целью были выбраны преобразования Кремоны, частным случаем которых является преобразование Фейстеля.

Таким образом, был выделены следующие этапы генерации ключевой пары:

1 Применяя способ получения отображений, описанный в пункте 3.2, строим взаимно однозначные полиномы $F_1(x)...F_k(x)$ над кольцом Z_n.

2 Полагаем, что полученные полиномы задают отображение $G(x)$ диагональным отображением из Z_n^k в себя: $G: Z_n^k \to Z_n^k$; $y = G(x_1...x_k) = (F_1(x_1)...F_k(x_k))$.

3 Генерируем обратимое аффинное отображение $Ax+b$ такое, что в каждой строке матрицы A содержится не более 3 ненулевых элементов.

4 Строим преобразование Кремоны $B: Z_n^k \to Z_n^k$, $y = B(x_1..x_k)$, которое имеет вид:

$$\begin{aligned} &y_j = x_j, (j \neq i) \\ &y_i = x_i + Q_i(x_1,...,x_{i-1},x_{i+1},...,x_k), \end{aligned} \tag{4.1}$$

где $Q_i(x_1,...,x_{i-1},x_{i+1},...,x_k)$ – произвольный полином от $k-1$ переменной, $i = 1..k$.

Обратное к нему отображение известно и имеет вид:

$$\begin{aligned} &x_j = y_j, (j \neq i) \\ &x_i = y_i - Q_i(y_1,...,y_{i-1},y_{i+1},...,y_k). \end{aligned} \tag{4.2}$$

5 Таким образом, будет задано отображение $H(x) = B \circ G \circ (Ax+b)$. По построению оно взаимно однозначно над Z_n^k и будет играть роль открытого ключа предложенной криптосистемы. В свою очередь преобразование Кремоны Bx, диагональное отображение $G(x)$ и аффинное отображение $Ax+b$ – секретный ключ данной системы шифрования.

4.2 Шифрование и дешифрование

Предположим, сторона B хочет отправить стороне A сообщение $m \in Z_n^k$. Алгоритм шифрования состоит из следующих шагов:

1 Взять открытый ключ (H, n, k) стороны A.

2 Зашифровать исходное сообщение m при помощи открытого ключа: $c = H(m) (\mathrm{mod}\, n)$.

3 Передать секретное сообщение c по коммуникационному каналу.

При дешифровании сообщения c на стороне A выполняются следующие действия:

1 Принять сообщение c от стороны B.

2 Положить $M_1 = cB^{-1} (\mathrm{mod}\, n)$, где B^{-1} имеет вид (4.2).

3 Вычислить $M_2 = G^{-1}(M_1)(\mathrm{mod}\, n)$, где значение $G^{-1}(M_1)$ берется из таблицы прообразов функции $G(x)$, находящейся на стороне A.

4 Вычислить $M_3 = (M_2 A^{-1} - b)(\mathrm{mod}\, n)$, где A^{-1} – матрица, обратная матрице A над кольцом вычетов Z_n.

5 Положить исходное сообщение $m = M_3$.

4.3 Пример

Для иллюстрации описанного алгоритма рассмотрим пример генерации ключевой пары в случае линейного пространства Z_{2737}^2. Элементы из этого пространства – векторы длины 2 – будем обозначать парой (x, y).

1 Необходимо построить взаимно однозначные полиномиальные отображения $F_1(x), F_2(x)$ над кольцом Z_{2737} по алгоритму (3.2). Пусть $F_1(x) = 929x^7 + 1110x^5 + 775x + 486$ (пример из пункта 3.3), аналогично получим отображение $F_2(x) = 301x^5 + 629x + 1457$.

2 Полиномы $F_1(x), F_2(x)$ задают диагональное отображение

$$G(x, y) = \begin{cases} F_1(x) \\ F_2(y) \end{cases} = \begin{cases} 929x^7 + 1110x^5 + 775x + 486 \\ 301y^5 + 629y + 1457. \end{cases}$$

3 Фиксируем аффинное отображение с ограничением на матрицу, $A\begin{pmatrix} x \\ y \end{pmatrix} + b = \begin{pmatrix} 12 & 3 \\ 0 & 101 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{cases} 12x + 3y \\ 101y + 1 \end{cases}$. Матрица A обратима по той причине, что ее определитель равен $12 * 101 = 1212$ и обратим в кольце Z_{2737}, так как $НОД(1212, 2737) = 1$; следовательно, матрица не вырождена.

4 Введем преобразование Кремоны $B\begin{pmatrix} x \\ y \end{pmatrix} = \begin{cases} 7x + 3y^2 + 2 \\ 2y \end{cases}$.

5 На последнем этапе формируется отображение $H(x, y) = B \circ G \circ (A + b)(x, y)$, являющееся криптографическим. Для наглядности введем обозначение $H(x, y) = (u, v)$.

Тогда:

$$u = 7[929(12x+3y)^7 + 1110(12x+3y)^5 + 775(12x+3y) + 486] + 3[301(101y+1)^5 + 629(101y+1) + 1457]^2 + 2;$$

$$v = 2[301(101y+1)^5 + 629(101y+1) + 1457].$$

Раскрывая скобки и приводя подобные с учетом вычислений в кольце вычетов Z_{2737}, получаем:

$$u = 1491x^7 + 1925x^6y + 2128x^5y^2 + 2366x^5 + 1799x^4y^3 + 1589x^4y + 1134x^3y^4 + 2163x^3y^2 + 2086x^2y^5 + 1225x^2y^3 + 630xy^6 + 2548xy^4 + 2149x + 1435y^{10} + 2310y^9 + 672y^8 + 1792y^7 + 994y^6 + 1134y^5 + 1064y^4 + 1638y^3 + 370y^2 + 1617y + 1409;$$

$$v = 469y^5 + 511y^4 + 525y^3 + 2688y^2 + 1359y + 2037.$$

В данном примере открытым ключом стороны A будет являться набор $(H, 2737, 2)$, а секретный ключ – набор $(B, G, A+b, 2737, 2)$.

4.4 Анализ криптостойкости и применения криптосистемы

Система шифрования с публичным ключом, сгенерированным предложенным образом, не обладает присущим RSA свойством гомоморфизма, который делает алгоритм уязвимым к атакам на основе подобранного шифротекста. При данной атаке злоумышленник владеет информацией о том, какие открытые тексты соответствуют выбранным им шифротекстам. При этом шифротексты могут быть как выбраны заранее (неадаптивная атака), так и выбираться в зависимости от уже известных пар открытых и зашифрованных сообщений (адаптивная атака).

Вычислительные эксперименты показали, что длина циклов такого криптографического отображения, как правило, увеличивается по сравнению с циклами исходных отображений над полями. Это свойство позволяет повысить стойкость криптосистемы к так называемым циклическим атакам. Циклические атаки состоят в последовательном применении криптографического отображения к перехваченному сообщению. В силу взаимной однозначности отображения и конечности кольца вычетов, последовательность замкнется (образуется цикл), и последним ее элементом и будет исходное открытое отображение.

В отличие от методов типа HFE (Hidden Field Equations), в случае предложенной системы дешифрование не позволяет использовать методы базисов Гребнера, поскольку этот метод приспособлен к полиномам над полями, а в данном алгоритме используются полиномы над кольцами.

Сложность взлома данной системы обуславливается не только задачей факторизации, как в случае RSA, но и задачей представления многочленов в виде суперпозиции. Кроме того задача, которую необходимо решить взломщику для восстановления матрицы A аффинного отображения, сводится к проблеме 3-SAT разрешимости, являющейся NP полной.

Процесс вычисления полиномов легче спрятать в программе, поскольку значение многочлена в точке можно находить несколькими разными способами. Благодаря этому данный криптографический примитив предлагается использовать в подходе White Box Cryptography, который позволяет реализовать криптографические примитивы в программном обеспечении так, чтобы они сохранили свою секретность, несмотря на присутствие в системе злоумышленника, имеющего доступ к ключам и секретной информации.

Скорость работы шифратора и дешифратора описанной системы превышает скорость аналогичных операций RSA, поскольку криптографическое отображение RSA имеет степень, значительно превосходящую степень криптографического отображения в данном случае. Известно, что возведение в степень является наиболее дорогостоящей операцией с вычислительной точки зрения.

4.5 Программная реализация

Для демонстрации практической реализуемости предлагаемой системы была разработана библиотека на языке Java, позволяющая генерировать публичные и приватные ключи системы, и использовать их для шифрования и дешифрования в случае колец небольших размерностей.

Взаимно однозначные отображения над кольцом генерируются с использованием Китайской теоремы об остатках, применяя при этом алгоритма Гаусса.

В соответствии с критерием обратимости матриц над кольцом целых чисел, обратимую матрицу можно получить в результате произведения элементарных матриц [5]. Элементарная матрица – это либо диагональная матрица, все диагональные элементы которой кроме одного равны 1; либо матрица с единицами на диагонали, все недиагональные элементы которой равны 0 кроме одного, равному произвольному многочлену. Элементарные матрицы первого вида были использованы для получения обратимой матрицы над кольцом. Обращение матрицы осуществлялось методом Гаусса-Жордана, в соответствии с которым необходимо дописать единичную матрицу того же порядка к исходной и осуществлять над получившейся блочной матрицей элементарные

преобразования до тех пор, пока исходная матрица не станет единичной. При этом единичная матрица будет преобразована в искомую обратную матрицу.

Заключение

Целью данной работы было исследование возможностей построения полиномиальных взаимно однозначных отображений над кольцами и анализ перспектив их использования для создания криптосистемы с открытым ключом. Поставленные цели были достигнуты: в работе представлен алгоритм получения требуемых отображений; кроме того, описана криптографическая система, использующая полученные отображения в качестве функций шифратора и дешифратора. Данная система превосходит по скорости алгоритм шифрования RSA и является более устойчивой к ряду атак. Приведен пример работы предложенной системы и произведен анализ криптостойкости и возможностей ее применения.

Данная работа была представлена на XX Международной студенческой конференции-школе-семинаре «Новые информационные технологии» и была награждена дипломом за лучшую работу [7]. Совместно с работой о разработке white-box криптографической системы она получила диплом первой степени на международной студенческой конференции «Студент и научно-технический прогресс» в 2013 году с последующей публикацией тезисов [1]. Также совместная работа стала призером на конкурсе докладов конференции «РусКрипто 2013», и материалы были приняты к публикации.

Список литературы

1. Арыков Н. Е., Спицына Е. О. Разработка алгоритма шифрования с открытым ключом и его применение для построения безопасного хранилища данных / Материалы 51-й международной научной студенческой конференции «Студент и научно-технический прогресс», 2013.
2. Виноградов И. М. Основы теории чисел / Москва: Мир, 1965. – 172 с.
3. Гашков С. Б., Применко Э. А., Черепнев М. А. Криптографические методы защиты информации / Москва: Академия, 2010.
4. Кренделев С. Ф., Спицына Е. О. Число 667. Проверка RSA на устойчивость. Вариант криптографии с открытым ключом / Системы высокой доступности. - 2011. - Т. 7. - №. 2. – С. 34-38.
5. Милованов М. В., Толкачев М. М. Алгебра и аналитическая геометрия в 2-х частях / Минск: Высшая школа, 1987. – С. 60-61.
6. Лидл Р., Нидеррайтер Г. Конечные поля, в 2-х томах / Москва: Мир, 1988. – 820 с.
7. Спицына Е.О. Варианты построения системы шифрования с открытым ключом / Тезисы докладов XX международной студенческой конференции-школы-семинара «Новые информационные технологии», 2012.
8. Koblitz N. Algebraic aspects of cryptography / Springer, 2004.
9. Patarin J. Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new Families of Asymmetric Algorithms [Электронный ресурс]. URL: http://cryptosystem.net/hfe.pdf.
10. Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public key cryptosystems / Commun. of the ACM, 21:120-126, 1978.
11. Wang L., Chang F. Revision of tractable rational map cryptosystem [Электронный ресурс]. URL: http://eprint.iarc.org/2004/046.pdf.