ТРУДЫ

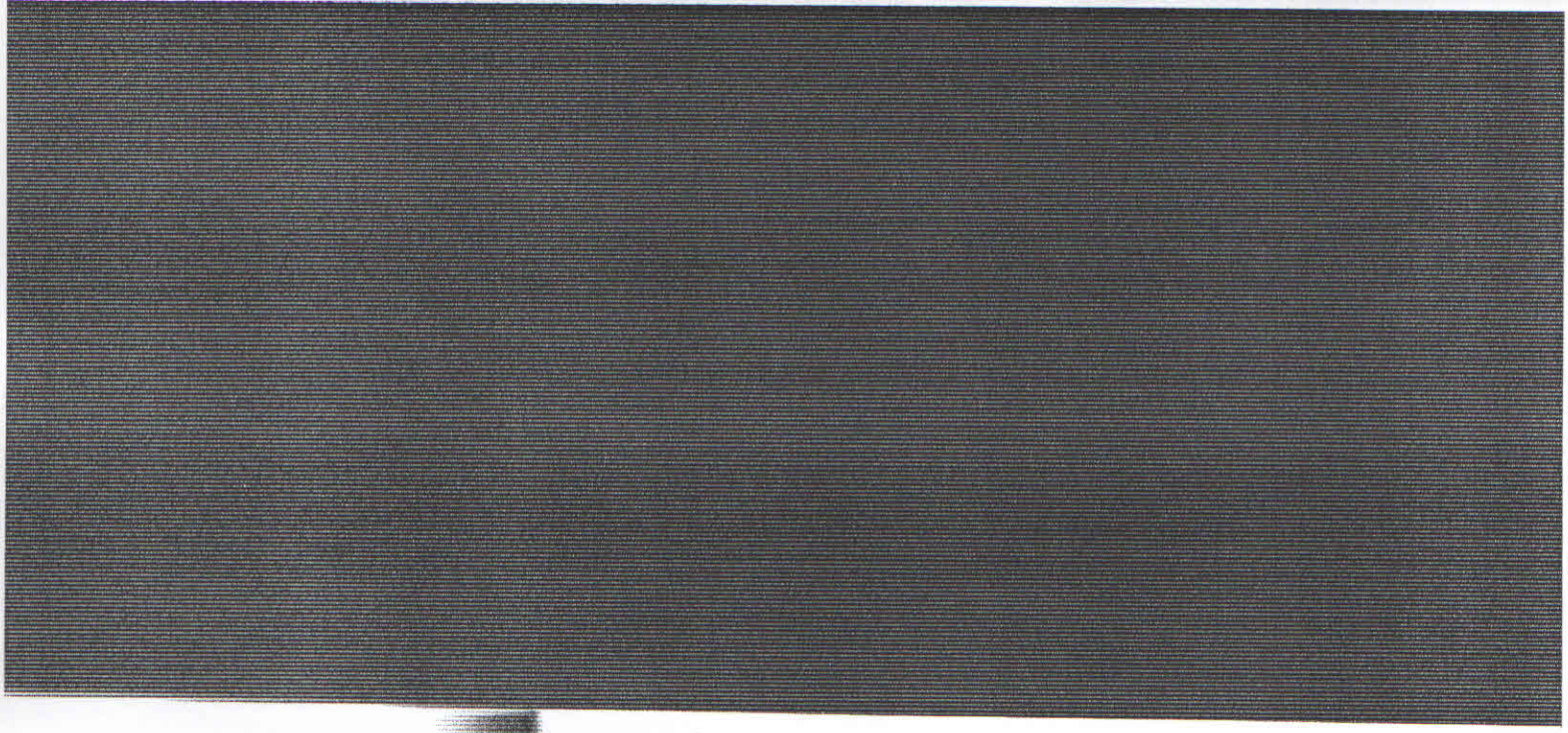
XI Международной Азиатской
школы-семинара
«ПРОБЛЕМЫ ОПТИМИЗАЦИИ
СЛОЖНЫХ СИСТЕМ»

27 июля - 7 августа 2015 г.

Часть II

Кыргызская Республика
оз. Иссык-Куль
отель "Три короны"

г. Чолпон-Ата



inal control theory. M.Dekker, 1996. 399 p.
ки в задачах управления. М.: Физматлит,

точные условия оптимальности в иерар-
томатика и телемеханика, 2013, № 3. С.

Оптимизация квазилинейных динамиче-
труктурой// Автоматика и телемеханика,

нина О.В. Оптимизация линейных систем
ика и телемеханика, 2011, № 6. С.64-78.
ерационный метод решения задач опти-
киберн., 1983. Т.2. С.160-168.
йственных задачах оптимального управ-
10. С.9-18.
ленном решении линейно-квадратичной
ным методом// Автоматика и телемеха-

точные условия оптимальности в иерар-
втоматика и телемеханика, 2013. № 12.

жение и приближенно-оптимальный син-
ектории// Автоматика и телемеханика,

ва И.С., Насатуева С.Н. Итерационные
ия управления// Программные системы:
2014. Т5, № 2 (20). С.47-61.

Содержание

5) Конструируется конкретный вариант системы разграничения доступа в виде набора моделей безопасности, выбранных для применения в соответствии с требованиями данной предметной области разграничения доступа.

6) Выполнение многокритериальной политики безопасности системы разграничения доступа достигается одновременным выполнением политик безопасности, соответствующих категориям безопасности выбранных моделей.

Это дает:

- однозначную идентификацию субъектов и объектов предметной области разграничения доступа по признакам принадлежности к ряду категорий, и, как следствие, устранение избыточности прав доступа;
- возможность учета иерархической организации пространства субъектов и объектов;
- повышенную скорость вычисления значений атрибутов безопасности.

Перечисленные характеристики многокритериальной модели разграничения доступа позволяют учитывать следующие требования, предъявляемые к моделям разграничения доступа, применяемым в облачных вычислениях:

- настраиваемость политик безопасности с учетом комплекса требований по защите конфиденциальности;
- легкость администрирования;
- возможность эффективного управления группами привилегий доступа в средах с большим числом пользователей и ресурсов.

Заключение

Предложен принцип многокритериального разграничения доступа, положенный в основу модели безопасности, которая может использоваться в среде облачных вычислений для защиты данных различного уровня и категорий пользования при наличии пользователей различных категорий.

Литература

1 Гайдамакин Н.А. Теоретические основы компьютерной безопасности: учебное пособие. – Екатеринбург: издательство Уральского университета, 2008. – 212 с.

2 Бияшев Р.Г., Горковенко Е.В. Обеспечение многоуровневой защиты в информационных и вычислительных системах // Материалы международной конференции «Развитие информационных технологий в высшей школе», КазНУ им. аль-Фараби: – Алматы, Қазақ университеті, 2003, С. 247-253

3 Sandhu R.S. Lattice Based Access Control Models // IEEE Computer. – 1993. – Volume 26, № 11. – P. 9-19.

4 Ивонин П.В. Безопасность облака в деталях // Безопасность информационных технологий 2013 – № 2, – С. 37-40.

5 Reeja S.L. Role based access control mechanism in cloud computing using co–operative secondary authorization recycling method. International Journal of Emerging Technology and Advanced Engineering. Volume 2, Issue 10, October 2012, – P. 444-448.

6 Заборовский В.С., Лукашин А.А. Система контроля доступа в среде облачных вычислений. Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление. 4(152)/2012, – С. 7-11.

7 Технологии виртуализации в коммерческих центрах обработки данных. Как обеспечить оптимальную защиту данных? «Код безопасности». ГК «Информзащита». URL: http: //www.securitycode.ru/ upload/ iblock/ 7c3/ Buklet_COD.pdf.

8 Калимолдаев М.Н., Бияшев Р.Г., Рог О.А. Формальное представление функциональной модели многокритериальной системы разграничения и контроля доступа к информационным ресурсам \\ «Проблемы информатики» № 1(22), 2014, С. 43-55.

9 Бияшев Р.Г., Калимолдаев М.Н., Рог О.А. Полиморфная типизация сущностей и задача конструирования механизма многокритериального разграничения доступа. \\«Известия НАН РК. Серия физико-математическая» №5, 2014. – С. 33-41.

10 Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2011. – 320 с.

11 Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Издательство агентства «Яхтсмен», 1996. – 192 с.

РАЗРАБОТКА МОДУЛЯРНЫХ СИММЕТРИЧНЫХ И АСИММЕТРИЧНЫХ КРИПТОСИСТЕМ

Бияшев Р.Г., Нысанбаева С.Е., Бегимбаева Е.Е., Магзом М.М.

Институт информационных и вычислительных технологий
Министерство образования и науки, Алматы, Республика Казахстан
E-mail: brg@ipic.kz, snyssanbayeva@gmail.com,
enlikb89@gmail.com, magzomxzn@gmail.com

Описываются модели модификаций нетрадиционных систем шифрования и цифровой подписи. Нетрадиционными, непозиционными или модулярными называют криптосистемы, разработанные на базе непозиционных полиномиальных систем счисления (НПСС). Создание модели системы блочного шифрования включает разработку модифицированного непозиционного блочного алгоритма шифрования с использованием аналога системы Фейстеля и режима применения этого модифицированного алгоритма. Модель цифровой подписи строится на основе схемы цифровой подписи Digital Signature Algorithm (DSA) и НПСС. Применение НПСС позволяет создавать эффективные криптографические системы повышенной надежности, с помощью которых обеспечивается конфиденциальность, аутентификация и целостность хранимой и передаваемой информации. Синонимы НПСС – классические системы счисления в остаточных классах (СОК), полиномиальные системы счисления в остаточных классах, модулярная арифметика.

1. Формирование непозиционных полиномиальных систем счисления

Основой для создания предлагаемых моделей криптосистем являются нетрадиционные системы шифрования и цифровой подписи. Эти системы разработаны на базе алгебраического подхода с использованием непозиционных полиномиальных систем счисления. Классическая СОК (модулярная арифметика) базируется на китайской теореме об остатках, которая гласит, что любое число может быть представлено своими остатками (вычетами) от деления на систему оснований, которую образуют попарно простые числа [1,2]. Тогда в СОК целое положительное число A представляется в виде последовательности остатков или вычетов

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n) \qquad (1)$$

от его деления на заданные положительные целые числа $p_1, p_2, \ldots, p_n$, которые называют основаниями системы. Цифры α_i образуются следующим образом:

$$\alpha_i = A - [A / p_i] p_i \,, \; i = \overline{1,n} \,, \qquad (2)$$

где $[A/p_i]$ обозначает целую часть от деления A на p_i. Из (2) следует, что цифра i-го разряда α_i числа A есть наименьший положительный остаток от деления A на p_i и $\alpha_i < p_i$. В этом случае образование цифры каждого разряда производится независимо друг от друга. В соответствии с китайской теоремой об остатках представление числа A в виде (1) будет единственным, если числа p_i попарно просты между собой. Объем диапазона представимых чисел в этом случае равен $P = p_1 p_2 \cdots p_n$. Здесь, аналогично позиционной системе счисления, диапазон представимых чисел растет как произведение оснований, а разрядность чисел растет как сумма разрядностей тех же оснований.

В НПСС (полиномиальных СОК) основаниями служат неприводимые многочлены над полем $GF(2)$ [3,4]. Использование НПСС позволяет уменьшить длину ключей, повысить стойкость и эффективность непозиционных криптоалгоритмов [4,5]. Повышение эффективности обеспечивается за счет правил НПСС, в которой все арифметические операции могут выполняться параллельно по модулям оснований НПСС. В разработанных нетрадиционных криптоалгоритмах шифрование и формирование цифровой подписи осуществляется для электронного сообщения заданной длины. В непозиционных криптосистемах в качестве критерия криптостойкости используется криптостойкость самих алгоритмов шифрования и формирования цифровой подписи, которая характеризуется полным секретным ключом. Криптостойкость в этом случае определяется не только длиной ключевой последовательности, но и выбранными системами полиномиальных оснований. С ростом порядка неприводимых многочленов с двоичными коэффициентами их количество стремительно растет. В связи с этим возможен широкий выбор полиномиальных оснований. Криптостойкость предложенного алгоритма шифрования с использованием НПСС существенно возрастает с увеличением длины электронного сообщения.

В [3] разработаны арифметика непозиционных систем счисления с полиномиальными основаниями и ее приложения к задачам повышения достоверности. Показано, что алгебра полиномов над некоторым полем по модулю неприводимого над этим полем многочлена является полем и представление полинома в непозиционном виде является единственным (аналог китайской теоремы об остатках для многочленов). Определены также правила выполнения арифметических операций в НПСС и восстановления многочлена по его остаткам.

При формировании НПСС для электронного сообщения M заданной длины N бит выбираются полиномиальные основания с двоичными коэффициентами

$$p_1(x), p_2(x), \ldots, p_S(x), \tag{3}$$

где $p_i(x)$. - неприводимые многочлены с двоичными коэффициентами степени m_i соответственно, $i = \overline{1,S}$. Эти основания называются рабочими. Основной рабочий диапазон НПСС представляется многочленом $P(x) = p_1(x)p_2(x)\cdots p_S(x)$ степени $m = m_1 + m_2 + \cdots + m_S$. Согласно китайской теореме об остатках, все выбираемые основания должны отличаться друг от друга, даже если они являются неприводимыми полиномами одной степени.

В НПСС любой многочлен $F(x)$, степень которого меньше m, имеет непозиционное представление в виде последовательности вычетов от его деления на рабочие основания $p_1(x), p_2(x), \ldots, p_S(x)$ и оно является единственным:

$$F(x) = (\alpha_1(x), \alpha_2(x), \ldots, \alpha_S(x)), \tag{4}$$

где $F(x) = \alpha_i(x) \left(mod p_i(x)\right)$, $i = \overline{1,S}$.

В построенной НПСС электронное сообщение (или его блок) заданной длины N бит записывается следующим образом. Оно интерпретируется как последовательность остатков от деления некоторого многочлена (обозначим его также $F(x)$) соответственно на рабочие основания $p_1(x), p_2(x), \ldots, p_S(x)$ степени не выше N, т.е. в виде (4). Каждое рабочее основание должно иметь степень не выше значения N. Рабочие основания выбираются из числа всех неприводимых полиномов степени от m_1 до m_S из условия выполнения уравнения [6]:

$$k_1 m_1 + k_2 m_2 + \cdots + k_S m_S = N. \tag{5}$$

В уравнении (5) $0 \le k_i \le n_i$ - число выбранных неприводимых многочленов степени m_i и неизвестные коэффициенты. Один конкретный набор этих коэффициентов является одним из решений алгебраического уравнения (5) и задает одну систему рабочих оснований, n_i - количество всех неприводимых многочленов степени m_i, $1 \le m_i \le N$, $S = k_1 + k_2 + \cdots + k_S$ - число выбранных рабочих оснований. В системе рабочих оснований учитывается также порядок расположения оснований.

Уравнение (5) определяет количество S рабочих оснований, вычеты по которым покрывают длину N заданного сообщения. Полные системы вычетов по модулям многочленов степени m_i включают в себя все полиномы степени не выше $m_i - 1$. Для записи полиномов степени $m_i - 1$ требуется m_i бит. Тогда остатки $\alpha_1(x), \alpha_2(x), \ldots, \alpha_S(x)$ формируются так, чтобы первым l_1 битам сообщения соответствовали двоичные коэффициенты остатка $\alpha_1(x)$, следующим l_2 битам - двоичные коэффициенты остатка $\alpha_2(x)$ и так далее, последним l_S двоичным разрядам - двоичные коэффициенты вычета $\alpha_S(x)$. С увеличением степени неприводимых многочленов их количество стремительно растет (таблица 1), в связи с этим значительно увеличивается и количество решений уравнения (5).

По (4) восстанавливается позиционное представление многочлена $F(x)$ [3,4]:

$$F(x) = \sum_{i=1}^{S} \alpha_i(x) B_i(x), \; B_i(x) = \frac{P_S(x)}{p_i(x)} M_i(x), \; i = \overline{1,S}. \tag{6}$$

Многочлены $M_i(x)$ выбираются такие, чтобы выполнялось сравнение в (6).

Таблица 1 - Количество n неприводимых многочленов с двоичными коэффициентами в зависимости от их степени m

m	n	m	n	m	n	m	n
1	1	8	30	15	2182	22	190557
2	1	9	56	16	4080	23	364722
3	2	10	99	17	7710	24	698870
4	3	11	186	18	14532	25	1342176
5	6	12	335	19	27594	26	2580795
6	9	13	630	20	52377	27	5070428
7	18	14	1161	21	99858	28	9774363

В НПСС возможно хэширование (сжатие) электронного сообщения от заданной длины N бит до N_k бит [3]. Эта процедура осуществляется путем введения избыточности, т.е. сообщение в НПСС расширяется на избыточные основания $p_{S+1}(x), p_{S+2}(x),\ldots, p_{S+U}(x)$. Система избыточных оснований формируется независимо от выбора рабочих оснований $p_1(x), p_2(x),\ldots, p_S(x)$. Отметим, что среди U избыточных оснований могут быть и совпадающие с некоторыми из рабочих.

Выбор избыточных оснований осуществляется по аналогии с выбором рабочих оснований. Эти основания выбираются произвольно из всех неприводимых многочленов степени, не превышающей значения N_k. Обозначим степени и число неприводимых многочленов, используемых при их выборе, как $a_1, a_2,\ldots, a_U$ и $d_1, d_2,\ldots, d_U$ соответственно. Число выбранных избыточных оснований в этом случае определяется из уравнения (аналога уравнения (5)):

$$t_1 a_1 + t_2 a_2 + \ldots + t_U a_U = N_k . \qquad (7)$$

где $0 \le t_j \le d_j$, $0 \le a_j \le N_k$, $j = \overline{1,U}$, t_j - количество выбранных избыточных оснований степени a_j, $U = t_1 + t_2 + \ldots + t_U$ – число выбранных избыточных оснований, запись вычетов по которым покрывает хэш-значение длины N_k. Решение уравнения (7) определяет одну систему избыточных оснований.

Далее вычисляются избыточные вычеты (остатки) $\alpha_{S+1}(x), \alpha_{S+2}(x),\ldots, \alpha_{S+U}(x)$ от деления восстановленного многочлена $F(x)$ на избыточные основания $p_{S+1}(x), p_{S+2}(x),\ldots, p_{S+U}(x)$. Тогда хэш-значение $h(F(x))$ длины N_k бит можно интерпретировать как последовательность этих вычетов:

$$h(F(x)) = (\alpha_{S+1}(x), \alpha_{S+2}(x),\ldots, \alpha_{S+U}(x)) \qquad (8)$$

где $h(F(x)) \equiv \alpha_{S+j}(x) mod(p_{S+j}(x))$, $j = \overline{1,U}$. Сумма длин избыточных вычетов составляет длину хэш-значения.

2. Моделирование модулярной системы шифрования

Алгоритм шифрования электронного сообщения заданной длины N бит на базе НПСС включает в себя следующие этапы. Вначале формируется НПСС (эта процедура описана выше). Затем генерируется ключевая (псевдослучайная) последовательность и производится шифрование открытого текста.

Пусть для шифрования из множества всех неприводимых многочленов степени не выше значения N выбрана система рабочих оснований (3). Сообщение длины N бит представляется в виде последовательности вычетов от деления некоторого многочлена на рабочие основания (обозначим этот многочлен также $F(x)$), т.е. в виде (4).

Затем ключ зашифрования длины N бит также интерпретируется как система вычетов $\beta_1(x), \beta_2(x),\ldots, \beta_S(x)$, но от деления некоторого другого многочлена $G(x)$ на те же рабочие основания:

$$G(x) = (\beta_1(x), \beta_2(x),\ldots, \beta_S(x)), \qquad (9)$$

где $G(x) \equiv \beta_i(x) (mod\, p_i(x))$, $i = \overline{1,S}$.

После зашифрования сообщения $F(x)$ с использованием ключа $G(x)$ получим криптограмму. Эта криптограмма рассматривается в виде некоторой функции $H(x)$:

$$H(x) = (\omega_1(x), \omega_2(x),\ldots, \omega_S(x)), \qquad (10)$$

где $H(x) \equiv \omega_i(x) (mod\, p_i(x))$, $i = \overline{1,S}$. В криптограмме (10) двоичным коэффициентам остатка $\omega_1(x)$ ставятся в соответствие первые l_1 бит криптограммы. Двоичным коэффициентам остатка $\omega_2(x)$ соответствуют следующие l_2 бит криптограммы и т.д. Двоичным коэффициентам последнего вычета $\omega_S(x)$ будут соответствовать последние l_S двоичных разрядов криптограммы.

При программной реализации этого нетрадиционного алгоритма шифрования сообщения будет использован нетрадиционный метод [7]. Применение разных методов позволяет получать различные модели шифрования.

В этой модели шифрования криптограмма (10) для электронного сообщения длины N бит получается в результате умножения многочленов (4) и (9) в соответствии со свойствами сравнений по двойному модулю $F(x)G(x) = H(x) (mod\, P(x))$.

Тогда элементы последовательности вычетов $\omega_1(x), \omega_2(x),\ldots, \omega_S(x)$ являются наименьшими остатками от деления произведений $\alpha_i(x)\beta_i(x)$ на соответственные основания $p_i(x)$:

$$\alpha_i(x)\beta_i(x) = \omega_i(x) (mod\, p_i(x)), \; i = \overline{1,S}, \qquad (11)$$

При расшифровании криптограммы $H(x)$ по известному ключу $G(x)$ для каждого значения $\beta_i(x)$ вычисляется обратный (инверсный) многочлен $\beta_i^{-1}(x)$ из условия выполнения следующего сравнения:

$$\beta_i(x)\beta_i^{-1}(x) \equiv 1 (mod\, p_i(x), \; i = \overline{1,S}. \qquad (12)$$

В результате получается многочлен $G_i^{-1}(x)=(\beta_1^{-1}(x),\beta_2^{-1}(x),...,\beta_S^{-1}(x))$, инверсный к многочлену $G(x)$. Тогда исходное открытое сообщение в соответствии с (11) и (12) восстанавливается по сравнению:

$$F(x)=G^{-1}(x)H(x)\big(mod\,P(x)\big). \qquad (13)$$

Через вычеты выражение (12) запишется в виде следующих сравнений:

$$\alpha_i(x)\equiv\beta_i^{-1}(x)\omega_i(x)(mod\,p_i(x),\ i=\overline{1,S}. \qquad (14)$$

Таким образом, в рассмотренной модели (9) - (14) алгоритма шифрования электронного сообщения заданной длины N бит в НПСС полным ключом является выбранная система полиномиальных оснований $p_1(x),p_2(x),...,p(x)$, полученный при генерации псевдослучайных последовательности секретный ключ $G(x)=(\beta_1(x),\beta_2(x),...,\beta_S(x))$ и инверсный к нему ключ $G_i^{-1}(x)=(\beta_1^{-1}(x),\beta_2^{-1}(x),...,\beta_S^{-1}(x))$. Криптостойкость алгоритма шифрования на базе НПСС определяется общим числом всех возможных и отличающихся друг от друга вариантов выбора ключевых последовательностей и систем рабочих оснований.

Разработанный нетрадиционный алгоритм шифрования является базой для решения задач криптографии. С целью его практического применения выполняются научно-исследовательские работы по разработке модифицированного алгоритма на основе сети Фейстеля для улучшения статистических характеристик непозиционной криптограммы (10)-(11), и моделей режимы работы модифицированного алгоритма нетрадиционного шифрования.

Чем больше длина полного ключа шифрования в НПСС, тем больше вариантов выбора систем рабочих оснований. В связи с этим можно использовать несколько моделей схемы Фейстеля. Модели могут отличаться как количеством подблоков, так и числом раундов (или итераций). Функции криптографического преобразования подблоков в моделях схемы также могут различаться. Блок входных данных в зависимости от его длины может быть разбит на разное четное количество подблоков. На каждом шаге итерации будет исследованы возможные варианты использования ключевых последовательностей и систем рабочих оснований.

При компьютерном моделировании разработанных модифицированных алгоритмов будет проведен анализ их статистических характеристик.

В виду того, что блочные шифры шифруют данные блоками фиксированного размера, существует потенциальная возможность утечки информации о повторяющихся частях данных шифруемых на одном и том же ключе [2,8]. Поэтому для использования алгоритмов блочных шифрования разработаны различные режимы [2,9] для обеспечения требуемых условий зашифрованных сообщений. Основное условие - результат шифрования каждого блока должен быть уникальным вне зависимости от шифруемых данных.

Рассматриваются модели одного из режимов работы шифра – режим сцепления блоков CBC (Cipher Block Chaining)[2]. В этом режиме вначале каждый блок открытого текста складывается по модулю два с предыдущим блоком криптограммы, а затем полученный результат шифруется. Таким образом, каждый блок шифротекста зависит от всех обработанных блоков открытого текста. При этом для вычисления первого зашифрованного блока используется случайный вектор инициализации.

Необходимо гарантировать уникальность векторов инициализации при каждом шифровании, чтобы два одинаковых сообщения не шифровались одинаково.

Программная реализация предложенных моделей режима CBC позволит выбрать требуемый режим работы модифицированного алгоритма на базе НПСС.

3. Моделирование модулярной системы цифровой подписи

Схема цифровой подписи (ЦП) Эль-Гамаля основана на трудности вычисления дискретных логарифмов в конечном поле [10,11]. На базе этой схемы были построены стандарты цифровой подписи DSS (Digital Signature Standard, США, 1994) и ГОСТ Р 34.10-94 (Россия, 1994 г.) [12,13]. Стандарт DSS основан на алгоритме хэширования SHA и алгоритме формирования цифровой подписи DSA (Digital Signature Algorithm). Этот алгоритм принят в 1994 году в качестве стандарта цифровой подписи США и представляет собой вариацию цифровой подписи схемы Эль-Гамаля и К. Шнорра. Длина подписи в системе DSA составляет 320 бит.

Алгоритм DSA является "классическим" примером схемы ЦП на основе использования хэш-функции и асимметричного алгоритма шифрования.

Суть схемы ЦП DSA состоит в следующем. Пусть отправитель и получатель электронного документа при вычислении цифровой подписи используют большие целые простые числа p и q: $2^{L-1}<p<2^L$, $512\le L\le 1024$, L кратно $64, 2^{159}<q<2^{160}$, q - простой делитель $(p-1)$ и $g=h^{(p-1)/q}mod\,p$, где h - любое целое число, $1<h<p-1$ такое, что $h^{\frac{p-1}{q}}(mod\,p)>1$.

Ключ b случайно выбирается из диапазона $1\le b\le q$ и держится в секрете. Вычисляется значение $\beta=g^b mod\,p$. Параметры p,q,g являются открытыми ключами и опубликовываются для всех пользователей системы информационного обмена с ЦП.

Рассмотрим формирование ЦП для сообщения M.

1. Определяется хэш-значение h от подписываемого сообщения M: $h=h(M)$.

2. Выбирается случайное целое число r, $1\le r\le q$. Это число хранится в секрете и меняется для каждой подписи.

3. Определяется значение: $\gamma=\big(g^r mod\,p\big)mod\,q$.

4. С использованием секретного ключа отправителя находится $\delta=\big(r^{-1}(h+b\gamma)\big)mod\,q$, где r^{-1} удовлетворяет условию $\big(r^{-1}r\big)mod\,q=1$.

5. Цифровой подписью для сообщения M являются пара чисел (γ,δ), которые передаются вместе с сообщением по открытым каналам связи.

Проверка ЦП. Полученные адресатом версии M,δ,γ обозначим M',δ',γ'.

1. Проверяется выполнение условий $0<\delta<q$ и $0<\gamma<q$. При невыполнении хотя бы одного из условий цифровая подпись считается недействительной.

2. Вычисляется хэш-значение $h_1=h(M')$ от полученного сообщения M'.

3. Находится значение $v=(\delta')^{-1}mod\,q$.

4. Вычисляются значения выражений: $z_1=(h_1 v)mod\,q$ и $z_2=(\gamma' v)mod\,q$.

5. Определяется значение: $u=\big(\big(g^{z_1}\beta^{z_2}\big)mod\,p\big)mod\,q$.

6. Если выполняется равенство $\gamma' = u$, то ЦП принимается, т.е. в процессе передачи не нарушена целостность сообщения: $M' = M$. При невыполнении равенства ЦП считается недействительной.

Криптостойкость схемы DSA против атак методом "грубой силы" в первую очередь зависит от размера параметров p и q. Соответственно криптостойкость против атаки методом "грубой силы" на параметр p в случае 512 и 160 бит будет равна 2^{160}. Успешная атака на параметр q возможна только в том случае, если злоумышленник может вычислять дискретные логарифмы в поле Галуа $GF(2^{512})$.

Одной из теоретически возможных атак на схему DSA является компрометация параметра r. Для каждой подписи требуется новое значение r, которое должно быть выбрано случайным образом. Если злоумышленник найдет значение r, то секретный ключ b может быть раскрыт. Другой возможный вариант - две подписи были сгенерированы на одном значении r. В этом случае злоумышленник тоже в состоянии восстановить b. Следовательно, одним из факторов, повышающих безопасность использования схем ЦП, является наличие надежного генератора случайных чисел.

В DSA длина модуля преобразования составляет порядка 1024 битов. До такой же длины увеличены длины ключей. В связи с этим увеличивается вычислительная сложность криптографических преобразований, но уменьшается скорость вычислений. Сокращение длины ключа и повышение скорости вычислений возможно при разработке модификации этой схемы ЦП на базе НПСС.

Разрабатывается модулярная система ЦП с открытым ключом, при создании которой будет использован модифицированный алгоритм DSA на базе НПСС. Вначале алгоритм DSA записывается в виде, в котором отсутствует модуль q, и все вычисления производятся только по одному модулю p. Затем разрабатывается модификация этой схемы на базе НПСС.

Процесс формирования НПСС для электронного сообщения M заданной длины N бит и вычисление хэш-значения для этого сообщения приведены в разделе 1.

Модификация схемы цирофой подписи DSA на базе НПСС осуществляется следующим образом. Пусть сформирована НПСС с рабочими основаниями $p_1(x), p_2(x),..., p_S(x)$. Для каждого из рабочих оснований выбираются соответственные порождающие элементы (полиномы) $g_1(x), g_2(x),..., g_S(x)$. Порождающие полиномы являются аналогом примитивных элементов в конечном поле по модулю простого числа. Выбирается также секретный ключ отправителя b в диапазоне $[1, 2^m]$. Вычисляется значение открытого ключа $\beta(x)$: $\beta(x) = (\beta_1(x), \beta_2(x),..., \beta_S(x))$. В модифицированном алгоритме ЦП на базе НПСС будет использована процедура вычисления хэш-значения в НПСС. Далее, выбирается случайное целое число r из диапазона $[1, 2^m]$.

Полиномы $\gamma(x)$ и $\delta(x)$ представляются в непозиционном виде как последовательности вычетов от их деления на основания НПСС:

$$\gamma(x) = (\gamma_1(x), \gamma_2(x),..., \gamma_s(x)),\ \delta(x) = (\delta_1(x), \delta_2(x),..., \delta_s(x)).$$

Цифровой подписью для сообщения M является пара многочленов $(\gamma(x), \delta(x))$.

Проверка цифровой подписи осуществляется по аналогии приведенной проверкой DSA.

Использование алгебраического подхода на базе НПСС позволит сократить длину ключа для цифровой подписи без существенного понижения ее криптостойкости.

4. Заключение

Криптостойкость разрабатываемых модифицированных систем шифрования и цифровой подписи на базе НПСС характеризуется полным секретным ключом. Этот ключ зависит не только от длины ключа (псевдослучайной последовательности), но и от выбранной системы полиномиальных оснований НПСС, а также от количества всех возможных перестановок оснований в системе.

Исследование и применение режимов шифрования направлено на устранение потенциальных уязвимостей при обработке блоков больших сообщений. В связи с этим будут рассматриваться модели применения режима работы шифра CBC. Этот режим позволяет устранять недостатки применения одного ключа при шифровании всех блоков открытого текста без существенного снижения скорости его работы, т.к. задержка при выполнении операции XOR является небольшой. Разрабатываемая модифицированная система цифровой подписи на базе алгоритма DSA и НПСС характеризуется улучшением основных характеристик ЦП. Компьютерное моделирование модифицированных криптосистем на базе НПСС позволит выработать рекомендации по их надежному использованию и генерации полных секретных ключей.

Проводимые исследования финансируются Министерством образования и науки Республики Казахстан

Литература

1. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. - М., «Советское радио», 1968. - 440 с.
2. Stallings W., Cryptography and Network Security (4th Edition), Prentice Hall, 2005.
3. Бияшев Р.Г. Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ: дисс. докт. тех. наук: 05.13.06: защищена 09.10. 1985: утв. 28.03.1986. - М., 1985. - 328 с.
4. Бияшев Р.Г., Нысанбаева С.Е. Алгоритм формирования электронной цифровой подписи с возможностью обнаружения и исправления ошибки // Кибернетика и системный анализ. – 2012 г. – Т. 48, № 4. – С. 14-23.
5. Biyashev R., Nyssanbayeva S., Kapalova N.: The Key Exchange Algorithm on Basis of Modular Arithmetic. International Conference on Electrical, Control and Automation Engineering (ECAE2013), December 1-2, 2013, Hong Kong – Monami,S. 2014. – P.501-505.
6. Моисил Гр. К. Алгебраическая теория дискретных автоматических устройств / Пер. с рум. В.М.Остиану. Под ред. В.И. Шестакова. – М.: Изд-во иностранной литературы, 1963. - 680 с.
7. Нысанбаев Р.К. Криптографический метод на основе полиномиальных оснований // Вестник Мин-ва науки и высшего образования и Нац. акад. наук Республики Казахстан – Алматы: Гылым. – 1999. – № 5. – С. 63-65.
8. N. Ferguson, B. Schneier, T. Kohno, Cryptography Engineering: Design Principles and Practical Applications, Wiley Publishing Inc, 2010.
9. Recommendation for Block Cipher Modes of Operation. NIST Special Publication 800-38A. Technology Administration U.S. Department of Commerce. 2001 Edition.

10. Диффи У., Хеллман М.Э. Защищенность и имитостойкость: Введение в криптографию // ТИИЭР – Труды института инженеров по электротехнике и радиоэлектронике. – 1979 – Том 67, № 3. – С. 71–109.

11. ElGamal T. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Transactions on Information Theory, v. IT-31, n. 4, 1985.– P. 469-472.

12. FIPS PUB 186. Digital Signature Standard (DSS).

13. Информационная технология. Криптографическая защита информации. Функция хэширования ГОСТ 4.11-94, Госстандарт РФ, М., 1994. ftp://ftp.wtc-ural.ru/pub/ru.crypt/ ГОСТ 34.11/: 10.01.2015.

МОДЕЛИРОВАНИЕ ПРОГРАММНОЙ РЕАЛИЗАЦИИ АСИММЕТРИЧНОЙ НЕПОЗИЦИОННОЙ СХЕМЫ ШИФРОВАНИЯ

Бияшев Р.Г., Нысанбаева С.Е., Капалова Н.А., Дюсенбаев Д.С.
Институт информационных и вычислительных технологий,
Республика Казахстан, г. Алматы,
E-mail:brg@ipic.kz, sultasha1@mail.ru, kapalova@ipic.kz, dimash_dds@mail.ru

Представлена система шифрования с открытым ключом, разработанная на базе шифрсистемы Эль-Гамаля и непозиционных полиномиальных систем счисления (НПСС). Проведено исследование и осуществлена программная реализация этой системы, результаты выполнения компьютерной программы проверены на конкретных примерах. Эффективность непозиционной системы шифрования увеличивается за счет возможности параллельной обработки полиномов, которые являются остатками по выбранной системе оснований НПСС.

1. Введение

Криптографическая стойкость системы шифрования Эль-Гамаля с открытым ключом основана на сложности проблемы дискретного логарифмирования в мультипликативной группе конечного поля. Эта задача сложно реализуема для значений p, содержащих более 150 десятичных знаков. Рекомендуется выбирать p таким, чтобы число p-1 содержало большой простой делитель. Недостатком криптосистемы Эль-Гамаля является удвоение длины открытого текста при шифровании, а также необходимость использования различных значений рандомизатора для зашифрования различных открытых текстов [1-4].

Синонимы непозиционных полиномиальных систем счисления (НПСС) – полиномиальные системы счисления в остаточных классах, непозиционные системы счисления и модулярная арифметика. Алгоритмы и методы, созданные на базе этих систем, называют также нетрадиционными, непозиционными или модулярными [5-7]. В классической системе счисления в остаточных классах (СОК) в качестве системы оснований выбираются положительные попарно простые целые числа, и в ней целое положительное число представляется своими остатками (вычетами) от деления на эту систему оснований [5]. Построение СОК основано на использовании китайской теоремы об остатках. В соответствии с этой теоремой представление числа в виде последовательности вычетов является единственным, если основания будут попарно просты между собой. В отличие от классических СОК в НПСС основаниями служат неприводимые многочлены над полем $GF(2)$, то есть с двоичными коэффициентами [6,7].

Использование алгебраического подхода на базе НПСС при разработке и исследовании нетрадиционных криптографических алгоритмов и методов позволяет повысить надежность и эффективность этих криптографических процедур [7].

2. Непозиционная система шифрования на основе алгоритма Эль-Гамаля

Разработанный нетрадиционный асимметричный алгоритм шифрования электронного сообщения M по схеме Эль-Гамаля осуществляется следующим образом.

1. Вначале производится формирование НПСС. Для этого выбираются основаниями неприводимые многочлены

$$p_1(x), p_2(x),..., p_S(x) \tag{1}$$

над полем $GF(2)$ степени $m_1, m_2,..., m_S$ соответственно. Полиномы (1) с учетом порядка их расположения образуют одну систему оснований. Все основания должны быть различными, и в том случае, если они имеют одну степень (для выполнения китайской теоремой об остатках). Рабочий диапазон НПСС определяется многочленом (модулем)

$$P_S(x) = p_1(x)p_2(x)\cdots p_S(x)$$

степени $m = \sum_{i=1}^{S} m_i$. В НПСС любой многочлен $F(x)$ степени меньше m имеет единственное непозиционное представление вида

$$F(x) = (z_1(x), z_2(x),..., z_S(x)), \tag{2}$$

где $F(x) \equiv z_i(x) (\mathrm{mod}(p_i(x))$, $i = \overline{1,S}$. По виду (2) восстанавливается позиционное представление $F(x)$ следующим образом:

$$F(x) = \sum_{i=1}^{S} z_i(x) B_i(x), \text{ где } B_i(x) = \frac{P_S(x)}{p_i(x)} M_i(x) \equiv 1 (\mathrm{mod}\, p_i(x)). \tag{3}$$

Выбор многочленов $M_i(x)$ осуществляется таким образом, чтобы выполнялось сравнение в (3).

2. Для каждого основания $p_i(x)$ выбирается порождающий элемент (многочлен) $\alpha_i(x)$ из полной системы вычетов по модулю $p_i(x)$, т. е. степени $\alpha_i(x)$ не превышают m_i, где $i = \overline{1,S}$. Тогда порождающий элемент в нетрадиционном алгоритме шифрования интерпретируется как последовательность остатков от деления некоторого многочлена $\alpha(x)$ на основания $p_1(x), p_2(x),..., p_S(x)$ соответственно:

$$\alpha(x) = (\alpha_1(x), \alpha_2(x),..., \alpha_S(x)),$$

где $\alpha(x) \equiv \alpha_i(x) (\mathrm{mod}\, p_i(x))$, $i = \overline{1,S}$.

Выбранные основания НПСС и соответствующие им порождающие многочлены $\alpha_i(x)$ держатся в секрете. Порождающий элемент – это аналог примитивного элемента первообразного корня по модулю простого числа.