УДК 004.056.5

Р.Г. БИЯШЕВ, С.Е. НЫСАНБАЕВА

АЛГОРИТМ ФОРМИРОВАНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ С ВОЗМОЖНОСТЬЮ ОБНАРУЖЕНИЯ И ИСПРАВЛЕНИЯ ОШИБКИ

Ключевые слова: *электронная цифровая подпись, непозиционная полиномиальная система счисления, полная система вычетов, криптостойкость.*

Системы электронной цифровой подписи (ЭЦП) включают два алгоритма: формирование цифровой подписи и ее проверка. При разработке схем ЭЦП используются принципиально различные подходы, которые можно разделить на три группы. Это схемы на базе:

- систем шифрования с открытыми ключами;
- симметричных систем шифрования;
- специально разработанных алгоритмов вычисления и проверки подписи.

Предлагаемая ниже схема цифровой подписи относится к последней группе.

В основе известных систем ЭЦП лежат алгоритмы RSA, Эль Гамаля, а также DSA, предложенный в 1991 г. для использования в качестве стандарта цифровой подписи DSS (Digital Signature Standard) в США. Российский стандарт ГОСТ Р 34.10–94 вступил в действие в 1995 г. Эти алгоритмы и стандарты разработаны на базе криптосистем с открытыми ключами.

В Республике Казахстан государственным стандартом СТ РК 1073-2007 определены четыре уровня безопасности систем ЭЦП [1]. В соответствии с установленными в нем требованиями к средствам криптографической защиты информации первого, второго, третьего и четвертого уровней длина ключа ЭЦП должна быть не менее 60, 100, 150 и 200 бит соответственно.

Предлагаемый алгоритм разработан с использованием непозиционных полиномиальных систем счисления (НПСС), синонимами которых являются модулярная арифметика и системы счисления в остаточных классах. В НПСС основаниями являются не простые числа [2], а неприводимые многочлены над полем $GF(2)$ [3]. Алгоритмы и методы, созданные на базе этих систем, называют нетрадиционными. Применение НПСС при построении нетрадиционных алгоритмов криптографической защиты хранимой и передаваемой информации позволяет значительно повысить их эффективность и криптостойкость [4–7]. На базе НПСС созданы две системы электронной подписи. Первая схема ЭЦП представлена в [4, 6]. Ниже приведены результаты построения второй системы ЭЦП.

Рассмотрим процедуру построения НПСС. Пусть основаниями НПСС выбраны неприводимые многочлены $p_1(x), p_2(x), \ldots, p_S(x)$ над полем $GF(2)$ степени $m_1, m_2, \ldots, m_S$ соответственно. Эти полиномы с учетом порядка их расположения образуют системы оснований и называются рабочими (информационными или символами). В соответствии с китайской теоремой об остатках все основания должны быть различными, в том числе и тогда, когда они имеют одну степень. Основным рабочим диапазоном в НПСС является многочлен $P_S(x) = p_1(x)\,p_2(x)\ldots p_S(x)$ степени $m = \sum_{i=1}^{S} m_i$. В этой системе любой многочлен $F(x)$ степени меньше m имеет единственное представление вида

$$F(x) = (\alpha_1(x), \alpha_2(x), \ldots, \alpha_S(x)), \qquad (1)$$

где $F(x) \equiv \alpha_i(x) \pmod{p_i(x)}$. Позиционное представление $F(x)$ восстанавливается по его непозиционному виду (1) [2, 3]:

$$F(x) = \sum_{i=1}^{S} \alpha_i(x) B_i(x), \tag{2}$$

где $B_i(x) = \dfrac{P_S(x)}{p_i(x)} M_i(x) \equiv 1 (\mathrm{mod}\ p_i(x))$.

Многочлены $M_i(x)$ выбираются такими, чтобы выполнялось сравнение в (2). Эта формула восстановления $F(x)$ применяется при обработке, хранении и передаче информации. Если рассматриваются только процессы передачи и хранения непозиционной информации, то восстановление позиционного вида полинома $F(x)$ осуществляется по формуле [3–6]:

$$F(x) = \sum_{i=1}^{S} \alpha_i(x) P_i(x), \tag{3}$$

где $P_i(x) = \dfrac{P_S(x)}{p_i(x)}$.

При разработке криптосистем электронное сообщение длиной N бит в НПСС интерпретируется как последовательность остатков от деления некоторого многочлена (который обозначим 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 (1). Эти основания выбираются из числа всех неприводимых полиномов степени от m_1 до m_S из условия выполнения уравнения [8]:

$$k_1 m_1 + k_2 m_2 + \ldots + k_S m_S = N, \tag{4}$$

из которого находятся неизвестные коэффициенты k_i, $i = 1, 2, \ldots, S$, где $0 \le k_i \le n_i$, n_i — количество всех неприводимых многочленов степени m_i, $1 \le m_i \le N$, $S = k_1 + k_2 + \ldots + k_S$ — число выбранных рабочих оснований. Каждое решение (4) задает одну систему полиномиальных оснований. Полные системы вычетов по модулям многочленов степени m_i включают в себя все полиномы степени не выше $m_i - 1$, для записи которых необходимы m_i бит. С увеличением степени неприводимых многочленов их количество стремительно возрастает (табл. 1), соответственно в связи с этим также значительно увеличивается количество решений уравнения (4).

Таблица 1

Степень неприводимых многочленов	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Количество неприводимых многочленов	1	1	2	3	6	9	18	30	56	120	240	488	972	1938	3876	7749
Количество битов, покрываемых неприводимыми многочленами	1	2	6	12	30	54	126	240	504	1200	2640	5856	12636	27132	58140	123984

Алгоритм формирования (вычисления) ЭЦП для электронного сообщения заданной длины N бит состоит из трех этапов.

Этап 1. Формируется НПСС путем выбора системы рабочих полиномиальных оснований для сообщения длиной N бит в соответствии с требованиями выполнения уравнения (4). Затем производится восстановление функции $F(x)$ по формуле (3).

Этап 2. Осуществляется хэширование сообщения длиной от N бит до N_k бит путем введения избыточных (дополнительных или контрольных) оснований из числа всех неприводимых многочленов степени не выше N_k и вычисления избыточных вычетов по модулям этих оснований. Из этих вычетов составляется хэш-значение длиной N_k бит.

Этап 3. Шифрованием найденного хэш-значения получаем ЭЦП длиной N_k. Для этого используется алгоритм шифрования электронного сообщения заданной длины, разработанный на базе НПСС [4–6, 9].

Условия выбора дополнительных оснований зависят от процедуры хэширования, которая и определяет различные алгоритмы формирования электронной подписи.

Проверка ЭЦП осуществляется по следующему алгоритму. При получении подписанного сообщения адресат должен осуществить проверку ЭЦП, т.е. удостовериться в ее подлинности. Для этого он вычисляет два хэш-значения: первое адресат определяет от полученного им сообщения, а второе он находит в результате расшифрования прикрепленной ЭЦП. Если значения этих хэш-значений совпадают, то подпись принимается, в противном случае — не принимается.

В предложенном алгоритме формирования электронной подписи на этапе хэширования выбирается только одно избыточное (контрольное) основание $p_{S+1}(x)$ из числа всех неприводимых многочленов степени меньше N_k. Затем формируются три избыточных вычета $\alpha_{S+1}(x)$, $\alpha_{S+2}(x)$, $\alpha_{S+3}(x)$, которые в этом же порядке составляют хэш-значение из N_k бит. Эти вычеты используются не только для создания ЭЦП, но и для обнаружения и коррекции одиночной ошибки и выявления многократной ошибки.

Первый вычет — это остаток по модулю дополнительного основания $p_{S+1}(x)$ от суммирования произведений рабочих вычетов и их порядковых номеров

$$\alpha_{S+1}(x) = \sum_{i=1}^{S} \oplus |i\alpha_i(x)|_{p_{S+1}(x)}, \tag{5}$$

где знак суммы $\sum$ означает поразрядное сложение по модулю 2, $|i\alpha_i(x)|_{p_{S+1}(x)}$ — вычет по модулю $p_{S+1}(x)$ или вычет от деления произведения $i\alpha_i(x)$ на избыточное основание $p_{S+1}(x)$.

Второй из дополнительных вычетов определяется как сумма всех рабочих вычетов по модулю 2:

$$\alpha_{S+2}(x) = \sum_{i=1}^{S} \oplus \alpha_i(x). \tag{6}$$

Третий остаток вычисляется по модулю дополнительного основания от позиционного представления многочлена $F(x)$ по формуле (3):

$$\alpha_{S+3}(x) = \sum_{i=1}^{S} \oplus |\alpha_i(x)P_i(x)|_{p_{S+1}(x)}. \tag{7}$$

Корректирующие функции алгоритма формирования ЭЦП предназначены для проверки наличия ошибок и исправления одиночной ошибки. При расширении многочлена $F(x)$, в виде которого интерпретируется электронное сообщение, на избыточные вычеты выражение (1) примет вид

$$F(x) = (\alpha_1(x), \alpha_2(x), \ldots, \alpha_j(x), \ldots, \alpha_S(x), \alpha_{S+1}(x), \alpha_{S+2}(x), \alpha_{S+3}(x)).$$

Предположим, что произошла ошибка в j-м рабочем основании $p_j(x)$. При наличии одной ошибки в информационных вычетах избыточные вычеты (5)–(7) изменят свои значения на $\alpha^*_{S+1}(x)$, $\alpha^*_{S+2}(x)$, $\alpha^*_{S+3}(x)$. Ошибка — это любое ис-

кажение $\alpha_j(x)$ по модулю $p_j(x)$, и ее величина может быть равна любому элементу из полной системы вычетов по модулю $p_j(x)$, $1 \le j \le S$. Тогда $F(x)$ представится в виде

$$F(x) = (\alpha_1(x), \alpha_2(x), \dots, \overline{\alpha}_j(x), \dots, \alpha_S(x), \alpha^*_{S+1}(x), \alpha^*_{S+2}(x), \alpha^*_{S+3}(x)),$$

где $\overline{\alpha}_j(x)$ принадлежит полной системе вычетов по модулю основания $p_j(x)$.

Выявление и коррекция одиночной ошибки осуществляется двумя избыточными вычетами [2, 3]. В рассматриваемом алгоритме для этого используются вычеты (5) и (6). Пусть $\overline{\alpha}_j(x) = \alpha_j(x) + \Delta_j(x)$, где $\Delta_j(x)$ — величина ошибки. Если в хранимом или передаваемом сообщении произошла ошибка $\Delta_j(x)$, то система (5), (6) запишется в виде

$$\begin{cases} \alpha^*_{S+1}(x) = \sum\limits_{i=1}^{S} | i\alpha_i(x)|_{p_{S+1}(x)} \oplus | j\Delta_j(x)|_{p_{S+1}(x)}, \\ \alpha^*_{S+2}(x) = \sum\limits_{i=1}^{S} \alpha_i(x) \oplus \Delta_j(x), \end{cases} \tag{8}$$

где $\oplus$ — операция поразрядного сложения по модулю 2. Вычитая (5) из первого уравнения (8), а (6) — из второго уравнения (8), получим

$$\alpha^*_{S+1}(x) \oplus \alpha_{S+1}(x) = | j\Delta_j(x)|_{p_{S+1}(x)}, \ \alpha^*_{S+2}(x) \oplus \alpha_{S+2}(x) = \Delta_j(x). \tag{9}$$

Введем обозначения для невязок, определяемых как

$$\xi(x) = \alpha^*_{S+1}(x) \oplus \alpha_{S+1}(x), \ \eta(x) = \alpha^*_{S+2}(x) \oplus \alpha_{S+2}(x). \tag{10}$$

Тогда систему (9) можно переписать в виде

$$\xi(x) = | j\Delta_j(x)|_{p_{S+1}(x)}, \ \eta(x) = \Delta_j(x). \tag{11}$$

Как видно, величина ошибки определяется вторым уравнением (11). Номер ошибочного основания находится из первого уравнения (11), в связи с этим возникает необходимость определения инверсного для $\Delta_j(x)$ многочлена $\Delta_j^{-1}(x)$.

Для проверки того, была ли ошибка одиночной, вычисляются значения вычета $\alpha_{S+3}(x)$ до и после обнаружения и коррекции ошибки: если эти значения не совпадают, то выявленная ошибка является многократной.

Рассмотрим процесс обнаружения и исправления ошибок.

Предложение 1. Каждой ошибке $\Delta_j(x)$ соответствует одна пара невязок $\xi(x)$, $\eta(x)$.

Предположим обратное, т.е. одной ошибке $\Delta_j(x)$ соответствуют две пары невязок $\xi(x), \eta(x)$ и $\xi'(x)$, $\eta'(x)$. Тогда, кроме системы (11), будет иметь место также и система

$$\xi'(x) = | j\Delta_j(x)|_{p_{S+1}(x)}, \ \eta'(x) = \Delta_j(x). \tag{12}$$

При вычитании (11) из (12) получим, что $\xi'(x) \oplus \xi(x) = 0$, $\eta'(x) \oplus \eta(x) = 0$, откуда следует, что $\xi'(x) = \xi(x)$ и $\eta'(x) = \eta(x)$. Таким образом, предположение о том, что одной ошибке соответствуют две пары невязок, оказалось неверным.

Предложение 2. Каждой паре невязок $\xi(x)$, $\eta(x)$ соответствует одна ошибка $\Delta_j(x)$.

Допустим противоположное. Пусть одной паре невязок $\xi(x)$, $\eta(x)$ соответствуют две ошибки, например, $\Delta_j(x)$ и $\Delta_t(x)$ соответственно по основаниям $p_j(x)$ и $p_t(x)$. В этом случае получим, кроме системы (11), еще одну систему

$$\xi(x) = | t\Delta_t(x)|_{p_{S+1}(x)}, \ \eta(x) = \Delta_t(x). \tag{13}$$

Вычтем (11) из (13), результатом будет система

$$0 = |t\Delta_t(x) \oplus j\Delta_j(x)|_{p_{S+1}(x)},\ 0 = \Delta_t(x) \oplus \Delta_j(x), \tag{14}$$

откуда следует, что $\Delta_t(x) = \Delta_j(x)$. Тогда из первого уравнения (14) вытекает, что $|(t-j)\Delta_j(x)|_{p_{S+1}(x)} = 0$. Так как $\Delta_j(x) \neq 0$, то $t = j$, а это означает, что допущение было неверным.

Для того чтобы алгоритм обнаружения и исправления ошибок удовлетворял предложениям 1 и 2, должно выполняться условие изоморфности множества ошибок и множества невязок: общее число ошибок не может превышать общего количества всех невязок. Поскольку избыточные вычеты $\alpha_{S+1}(x)$, $\alpha_{S+2}(x)$, $\alpha_{S+3}(x)$ определяются по одному избыточному основанию $p_{S+1}(x)$, указанное условие изоморфности накладывает определенное ограничение на выбор этого дополнительного основания.

Предложение 3. Выбор избыточного основания зависит от используемой системы полиномиальных рабочих оснований и их количества.

Покажем это. Введем обозначение $||\varphi||_{p_i(x)}$ — число элементов в полной системе вычетов по модулю основания $p_i(x)$, $i = 1, 2, \ldots, S+1$. Упорядочим (для удобства изложения) расположение рабочих оснований в порядке увеличения их степеней $m_1 \le m_2 \le \ldots \le m_S$, т.е. здесь и далее m_1 — наименьшая их степень, а m_S — наибольшая. Тогда для полных систем вычетов по модулям рабочих оснований можно записать

$$||\varphi||_{p_1(x)} \le ||\varphi||_{p_2(x)} \le \ldots \le ||\varphi||_{p_S(x)}$$

или

$$2^{m_1} \le 2^{m_2} \le \ldots \le 2^{m_S}. \tag{15}$$

Общее число ошибок есть сумма элементов полных систем вычетов по всем основаниям. Число всех невязок определяется произведением числа элементов полной системы вычетов по модулю избыточного основания и количества элементов полной системы вычетов по модулю информационного основания наибольшей степени $||\varphi||_{p_{S+1}(x)} \cdot ||\varphi||_{p_S(x)}$, что следует из (11). Тогда требуемое условие ограничения на избыточное основание $p_{S+1}(x)$ запишется в виде неравенства

$$\sum_{i=1}^{S} ||\varphi||_{p_i(x)} \le ||\varphi||_{p_{S+1}(x)} \cdot ||\varphi||_{p_S(x)}. \tag{16}$$

Расписывая (16) с использованием числа элементов в полной системе вычетов, получим

$$\sum_{i=1}^{S} 2^{m_i} \le 2^{m_{S+1}} 2^{m_S}. \tag{17}$$

Тогда из выражения (17) с учетом (15) следует, что

$$2^{m_{S+1} + m_S - m_1} \ge S. \tag{18}$$

Таким образом, доказано: неравенство (18) определяет условия выбора степени избыточного основания в общем случае и характеризует ее зависимость от наибольшей и наименьшей степеней конкретной системы рабочих оснований и их количества S.

Рассмотрим некоторые частные случаи выбора избыточного основания.

Случай 1. Пусть все основания, рабочие и дополнительное, $p_1(x)$, $p_2(x)$, … … , $p_S(x)$, $p_{S+1}(x)$ имеют одинаковые степени $m_1 = m_2 = \ldots = m_S = m_{S+1}$. Тогда из неравенства (18) получим выражение

$$2^{m_{S+1}} \ge S, \tag{19}$$

показывающее, что количество элементов в полной системе вычетов по модулю избыточного основания должно быть не меньше числа всех информационных оснований S.

Пример 1. Выберем в качестве всех оснований (рабочих и избыточного) 30 неприводимых многочленов восьмой степени. Если все их использовать в качестве оснований, то рабочих будет 29, а 30-е основание — избыточным. Подставляя в (19) $S = 29$, $m_i = 8$, получим $2^8 \geq 29$, $256 \geq 29$, что означает, что для этого набора оснований условие (19) выполняется. При этом выражение (19) правильно для максимального значения $S = 29$, следовательно, оно будет справедливо и при меньших значениях количества S рабочих оснований.

Случай 2. Рассмотрим еще один вариант выбора оснований, когда все рабочие основания имеют одну степень, а степень контрольного основания m_{S+1} отличается от нее. Тогда из (18) получим неравенство (19).

По результатам предыдущего случая (когда все основания имеют одну степень) следует, что если избыточное основание имеет степень не меньше степени рабочих оснований, то условие (19) выполняется.

Рассмотрим случай, когда избыточное основание имеет степень меньшую наибольшей степени рабочих оснований m_S.

Предложение 4. Степень избыточного основания m_{S+1} должна быть не меньше наибольшей степени рабочих оснований m_S.

Как указывалось ранее, ошибка — это любое искажение вычета $\alpha_j(x)$ по модулю $p_j(x)$, и ее величина может быть равна любому элементу из полной системы вычетов по модулю $p_j(x)$. Предположим, что избыточное основание имеет степень $m_{S_{+1}} < m_S$, а ошибка произошла по рабочему основанию, степень которого больше m_{S+1}. Тогда ошибка (вычет) может совпасть с избыточным основанием. В этом случае невозможно определить местоположение ошибки из (11), т.е. номер ошибочного основания из выражения

$$j = |\Delta_j(x)\Delta_j^{-1}(x)|_{p_{S+1}(x)} = |\Delta_j(x)\Delta_j^{-1}(x)|_{\Delta_j(x)}.$$

Из этого следует, что число элементов полной системы вычетов по модулю избыточного основания $p_{S+1}(x)$ не должно быть меньше количества элементов полной системы вычетов по модулю рабочего основания $p_S(x)$:

$$m_{S+1} \geq m_S. \tag{20}$$

Таким образом, при формировании ЭЦП по представленному алгоритму избыточное основание выбирается таким, чтобы выполнялись одновременно два налагаемых на него условия (18) и (20).

Ошибки могут произойти не только по рабочим вычетам. Рассмотрим возможные варианты ошибок по контрольным вычетам.

Ошибочным является один из двух первых вычетов: $\alpha_{S+1}(x)$ и $\alpha_{S+2}(x)$. При проверке ЭЦП невязка по ошибочному вычету окажется отличной от нуля, другие две невязки будут равны нулю. После проверки ЭЦП ошибочный вычет исправляется заменой вновь вычисленным. Если в этом случае ошибка произошла также и в третьем контрольном вычете $\alpha_{S+3}(x)$, то ошибочные вычеты заменяются вновь вычисленными.

Ошибочными являются оба первых вычета: $\alpha_{S+1}(x)$ и $\alpha_{S+2}(x)$. Поскольку по этим вычетам обе невязки отличны от нуля, получаем вариант наличия ошибки, которая произошла в информационном символе сообщения. Исходя из этого ищем ошибку как одиночную по информационному основанию. Ошибочный вычет

можно выявить и исправить, т.е. правильный вычет заменить на неверный и таким образом внести третью ошибку. Завершаем проверку вычислением третьего дополнительного вычета $\alpha_{S+3}(x)$, которая покажет, что невязка по вычету $\alpha_{S+3}(x)$ не будет равна нулю. Следовательно, ошибка в сообщении не одиночна.

Неверными могут оказаться все три избыточных вычета $\alpha_{S+1}(x)$, $\alpha_{S+2}(x)$ и $\alpha_{S+3}(x)$. В этом случае поступаем также.

При формировании ЭЦП ее длина N_k должна быть существенно меньше длины N электронного сообщения, т.е. $N_k << N$. В рассматриваемом алгоритме длина подписи формируется тремя избыточными вычетами $\alpha_{S+1}(x)$, $\alpha_{S+2}(x)$ и $\alpha_{S+3}(x)$. Для записи каждого из вычетов $\alpha_{S+1}(x)$ и $\alpha_{S+2}(x)$ по модулю избыточного основания $p_{S+1}(x)$ необходимо m_{S+1} бит, а для записи вычета $\alpha_{S+3}(x)$ необходимо m_S бит. Поэтому длина ЭЦП ограничена условием

$$N_k = 2m_{S+1} + m_S < N. \tag{21}$$

Тогда степень избыточного вычета определяется неравенством

$$(N_k - m_S)/2 < m_{S+1} < (N - m_S)/2. \tag{22}$$

Из (20) и (21) следует еще одно ограничение на длину ЭЦП и степень $p_{S+1}(x)$

$$3m_S < N_k < 3m_{S+1} < N. \tag{23}$$

Как показано выше, выбор контрольного основания $p_{S+1}(x)$ зависит от наибольшей степени m_S информационных оснований. Существует определенное количество всех возможных систем рабочих оснований, покрывающих подписываемое сообщение длиной N и используемых для формирования ЭЦП. В каждой из этих систем имеется свое наибольшее значение их степени. Поэтому при подписывании некоторого электронного сообщения длиной N степень m_S принимает значения из конкретного диапазона возможных наибольших степеней. Тогда, как следует из выражений (22) и (23), по описанному алгоритму можно сформировать несколько ЭЦП с различными длинами N_k, $k = 1, 2, \ldots, K$, где K — число всех цифровых подписей, которые могут быть получены для сообщения длиной N.

Предложение 5. Криптостойкость нетрадиционного алгоритма формирования ЭЦП по модулю одного избыточного основания определяется числом всевозможных способов выбора оснований на всех этапах алгоритма формирования ЭЦП: системы рабочих оснований из множества неприводимых многочленов степени не выше N, избыточного основания из множества неприводимых многочленов степени не выше N_k с учетом всех ограничений на его выбор и полного ключа для шифрования хэш-значения длиной N_k.

Покажем это.

1. Выбор одной системы рабочих оснований $p_1(x), p_2(x), \ldots, p_S(x)$ степеней от m_1 до m_S ограничен условием, описываемым уравнением (4), с учетом всех перестановок рабочих оснований. Число различных комбинаций выбора оснований для какой-либо одной степени определяется k_i-сочетаниями из всех n_i неприводимых многочленов степени m_i. При выборе m_S должно учитываться условие (23). В непозиционных системах счисления существенен и порядок расположения оснований, поэтому число систем из S выбранных оснований будет

$$Z_1 = (k_1 + k_2 + \ldots + k_s)! C_{n_1}^{k_1} C_{n_2}^{k_2} \ldots C_{n_S}^{k_S}. \tag{24}$$

2. Количество способов выбора одного избыточного основания $p_{S+1}(x)$ равно числу n_{S+1} всех неприводимых многочленов степени m_{S+1}:

$$Z_2 = C_{n_{S+1}}^{1} = n_{S+1}. \tag{25}$$

Тогда все способы выбора дополнительного основания для одной конкретной системы рабочих оснований равно произведению $Z_1 Z_2$.

3. Шифрование хэш-значения длиной N_k осуществляется нетрадиционным алгоритмом шифрования, включающим формирование НПСС (выбор системы оснований степени не выше N_k с учетом порядка их расположения) и генерацию ключевой (псевдослучайной) последовательности [9]. Все основания (рабочие и для шифрования хэш-значения), используемые на этапах 1 и 3 алгоритма построения цифровой подписи, выбираются независимо друг от друга, но среди них могут быть и совпадающие.

Выбор системы оснований $r_1(x), r_2(x), \ldots, r_W(x)$ для шифрования хэш-значения осуществляется из числа неприводимых многочленов с двоичными коэффициентами степени не выше N_k. Тогда хэш-значение длиной N_k интерпретируется как последовательность остатков $\gamma_1(x), \gamma_2(x), \ldots, \gamma_W(x)$ от деления некоторого многочлена $F_1(x)$ на выбранные основания $r_1(x), r_2(x), \ldots, r_W(x)$ соответственно

$$F_1(x) = (\gamma_1(x), \gamma_2(x), \ldots, \gamma_W(x)), \tag{26}$$

где $F_1(x) \equiv \gamma_j(x) \pmod{r_j(x)}$, $j = \overline{1, W}$.

Ключевая последовательность генерируется длиной N_k и интерпретируется как последовательность остатков $\eta_1(x), \eta_2(x), \ldots, \eta_W(x)$ от деления некоторого полинома $G_1(x)$ на те же основания $r_1(x), r_2(x), \ldots, r_W(x)$:

$$G_1(x) = (\eta_1(x), \eta_2(x), \ldots, \eta_W(x)), \tag{27}$$

при этом $G_1(x) \equiv \eta_j(x) \pmod{\mathrm{r}_j(x)}$, $j = \overline{1, W}$.

Тогда полученную в результате шифрования криптограмму $\lambda_1(x), \lambda_2(x), \ldots, \lambda_W(x)$ можно представить как некоторую функцию $H_1(F_1(x), G_1(x))$:

$$H_1(x) = (\lambda_1(x), \lambda_2(x), \ldots, \lambda_W(x)), \tag{28}$$

при этом $H_1(x) \equiv \lambda_j(x) \pmod{r_j(x)}$, $j = \overline{1, W}$.

Операции в функциях (26)–(28) в соответствии с операциями непозиционной системы счисления выполняются параллельно по модулям многочленов $r_1(x), r_2(x), \ldots, r_W(x)$, выбранных в качестве оснований.

Обозначим степени и число неприводимых многочленов, используемых при выборе оснований $r_1(x), r_2(x), \ldots, r_W(x)$, соответственно $b_1, b_2, \ldots, b_W$ и $l_1, l_2, \ldots, l_W$. Из уравнения (аналога (4))

$$v_1 b_1 + v_2 b_2 + \ldots + v_W b_W = N_k, \tag{29}$$

где $0 \le v_i \le l_i$ — неизвестные коэффициенты, $1 \le b_j \le N_k$, $W = v_1 + v_2 + \ldots + v_W$, находятся W оснований, запись вычетов по которым покрывает шифруемое хэш-значение длиной N_k.

Тогда количество комбинаций полных ключей при шифровании хэш-значения (выбор одной системы из W оснований и ключа, распределение оснований в системе) определится соотношением

$$Z_3' = 2^{N_k} (v_1 + v_2 + \ldots + v_W)! C_{l_1}^{v_1} C_{l_2}^{v_2} \ldots C_{l_W}^{v_W}.$$

Все варианты выбора различных систем оснований и ключа получим из выражения

$$Z_3 = 2^{N_k} \sum_{v_1, v_2, \ldots, v_{\mathrm{W}}} (v_1 + v_2 + \ldots + v_W)! C_{l_1}^{v_1} C_{l_2}^{v_2} \ldots C_{l_W}^{v_W}. \tag{30}$$

В (30) суммирование проводится по всем возможным комбинациям целых положительных чисел $\nu_1, \nu_2, \ldots, \nu_W$, удовлетворяющих уравнению (29), т.е. по всем возможным комбинациям W оснований из общего числа неприводимых многочленов степени $b_1, b_2, \ldots, b_W$.

Для одной системы рабочих оснований при конкретных значениях m_S и m_{S+1} все способы формирования проверяющей подписи будут определяться произведением $Z_1 Z_2 Z_3$. Тогда всевозможные варианты формирования ЭЦП длиной N_k должны учитывать все системы рабочих оснований, определяемых уравнением (4), т.е. описываться формулой

$$Z_k = \sum_{k_1, k_2, \ldots, k_S} Z_1 Z_2 Z_3. \tag{31}$$

Все способы формирования ЭЦП с проверяющими функциями для сообщения одной определенной длины N есть сумма всех Z_k из (31)

$$Z = \sum_{k=1}^{K} Z_k. \tag{32}$$

Тогда обратная величина (32) определяет криптостойкость алгоритма формирования подписи с корректирующими свойствами

$$p_{\text{sig}} = 1 / \left[\sum_{k=1}^{K} 2^{N_k} n_{S+1} \left(\sum_{k_1, k_2, \ldots, k_S} (k_1 + k_2 + \ldots + k_s)! C_{n_1}^{k_1} C_{n_2}^{k_2} \ldots C_{n_S}^{k_S} \times \right. \right.$$

$$\left. \left. \times \sum_{\nu_1, \nu_2, \ldots, \nu_W} (\nu_1 + \nu_2 + \ldots + \nu_W)! C_{l_1}^{\nu_1} C_{l_2}^{\nu_2} \ldots C_{l_W}^{\nu_W} \right) \right]. \tag{33}$$

Таким образом, полный ключ алгоритма определяется процедурами выбора оснований на каждом из этапов формирования цифровой подписи.

Рассмотрим примеры определения криптостойкости ЭЦП.

Пример 2. Пусть ЭЦП создается для сообщения длиной 16 бит. В этом случае минимальное значение наибольшей степени информационных оснований $m_S = 4$, так как при меньших его значениях не существует систем рабочих оснований, покрывающих 16 бит. Из неравенства (20) следует, что возможны два варианта значений m_S, для которых получаем следующие ограничения на контрольное основание m_{S+1}: 1) $m_S = 4$, $m_{S+1} \le 6$; 2) $m_S = 5$, $m_{S+1} \le 5$. В связи с этим при построении цифровой подписи в соответствии с уравнением (4) могут быть сформированы две системы рабочих оснований при $m_S = 4$, и шесть систем при $m_S = 5$. Состав этих восьми систем оснований приведен в строках табл. 2. Так, система рабочих оснований под номером 1 включает неприводимые многочлены 1-й, 3-й и 4-й степени, количество которых равно соответственно 1, 1 и 3.

Таблица 2

Номер используемых систем рабочих оснований	Степень неприводимых многочленов, выбранных в качестве рабочих оснований				
	1	2	3	4	5
1	1	—	1	3	—
2	—	1	2	2	—
3	1	—	—	—	3
4	—	1	—	1	2
5	1	1	1	—	2
6	—	—	1	2	1
7	1	1	—	2	1
8	1	—	2	1	1

Допустимыми являются указанные далее варианты значений избыточного основания m_{S+1} и длин ЭЦП: 1) $m_S = 4$, $m_{S+1} = 4$, $N_1 = 12$;

2) $m_S = 4$, $m_{S+1} = 5$, $N_2 = 14$; 3) $m_S = 5$, $m_{S+1} = 5$, $N_4 = 15$. В результате по формуле (33) получим следующую величину криптостойкости: $p_{\text{sig}} \approx 10^{-13}$.

Пример 3. Сообщение имеет длину 256 байт или 2048 бит. Определим криптостойкость проверяющей подписи при выборе одной системы информационных оснований.

Пусть в качестве системы выбраны 80 многочленов 16-й степени, 60 многочленов 12-й степени и 6 многочленов 8-й степени. Тогда $S = 146$ и $Z_1 \approx 5 \cdot 10^{529}$. Контрольным основанием выберем неприводимый многочлен 16-й степени: $Z_2 = 7749$. В результате хэширования получим хэш-значение длиной 48 бит. Для его шифрования формируем систему из трех оснований 16-й степени, $W = 3$. В результате получим $p_{\text{sig}} \approx 10^{-560}$.

Как видно из вышеизложенного, при использованном подходе длина и надежность формируемой подписи определяются длиной подписываемого сообщения, выбором системы рабочих оснований и избыточного основания, а ее криптостойкость может достигать высоких значений. В настоящее время программные реализации криптографических алгоритмов защиты информации могут успешно соперничать с традиционными аппаратными средствами. Применение НПСС позволяет создавать эффективные криптографические средства повышенной надежности, которые обеспечивают конфиденциальность, аутентификацию и целостность хранимой и передаваемой информации.

СПИСОК ЛИТЕРАТУРЫ

1. СТ РК 1073-2007. Средства криптографической защиты информации. Общие технические требования. — Введ. 2009. 01.01. — Астана, 2009. — 15 с.
2. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. — М.: Сов. радио, 1968. — 439 с.
3. Бияшев Р.Г. Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ: Дис. ... докт. техн. наук. — М., 1985. — 328 с.
4. Амербаев В.М., Бияшев, Р.Г., Нысанбаева С.Е. Применение непозиционных систем счисления при криптографической защите // Изв. Нац. акад. наук Республики Казахстан. Сер. физ.-мат. наук. — Алматы: Гылым, 2005. — № 3. — С. 84–89.
5. Бияшев Р.Г., Нысанбаева С.Е. Влияние состава полиномиальных оснований непозиционной системы счисления на надежность шифрования // Материалы VIII Междунар. науч.-практ. конф. «Информационная безопасность». — Таганрог: Изд-во ТРТУ, 2006. — С. 66–69.
6. Бияшев Р.Г., Нысанбаева С.Е. Нетрадиционный подход к созданию криптосистем // Информационные технологии и безопасность: Сб. науч. тр. — 2006. — Вып. 9. — С. 20–28.
7. Бияшев Р.Г., Капалова Н.А., Нысанбаева С.Е. Разработка и исследование модифицированного алгоритма Диффи–Хэллмана на базе модулярной арифметики // Актуальные проблемы безопасности информационных технологий: материалы III Междунар. науч.-практ. конф. / Под общ. ред. О.Н. Жданова, В. В. Золотарева; Сиб. гос. аэрокосм. ун-т, Красноярск, 9–11 сент. 2009 г. — Красноярск, 2009. — С. 18–22.
8. Моисил Гр. К. Алгебраическая теория дискретных автоматических устройств. — М: Изд-во иностр. лит., 1963. — 680 с.
9. Капалова Н.А., Нысанбаева С.Е. Исследование алгоритма генерации псевдослучайных последовательностей // Информационные технологии и безопасность. Менеджмент информационной безопасности: Сб. науч. тр. — 2007. — Вып. 10. — С. 32–39.

Поступила 02.07.2010