УДК 004.056.53+004.057.4

А. В. Неласая, Г. Л. Козина, Н. А. Молдовян

ПРОТОКОЛЫ КОЛЛЕКТИВНОЙ ЦИФРОВОЙ ПОДПИСИ НА ЭЛЛИПТИЧЕСКИХ И ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ

В статье представлены новые протоколы коллективной цифровой подписи на эллиптических и гиперэллиптических кривых. Вычислительные схемы проиллюстрированы примерами.

ВВЕДЕНИЕ

Развитие технологий электронного документооборота требует новых механизмов обеспечения юридической силы коллективных электронных документов. В частности, при разработке коллективных проектов важной проблемой является использование протоколов [1–4], обеспечивающих реализацию коллективной электронной цифровой подписи.

Известные в настоящее время протоколы электронной цифровой подписи позволяют осуществить реализацию кратной подписи (директор, главный бухгалтер, ведущий инженер и т. д.), но при этом, в силу последовательной реализации кратной подписи, возникают следующие проблемы. При подписании электронного документа важна последовательность формирования подписей каждого из участников, при проверке подписей также важна проверяющая последовательность проверки подписей участников. Кроме этого, размер подписи увеличивается пропорционально числу участников, подписавших электронный документ.

Для устранения указанных недостатков были предложены новые протоколы [2–4] формирования и проверки подлинности коллективной электронной цифровой подписи. В этих протоколах используется общий (коллективный) открытый ключ, который формируется на основе индивидуальных открытых ключей группы пользователей. Применяемые на практике системы электронной цифровой подписи предоставляют возможность использования (доступности через Internet) стандартных справочников открытых ключей и/или типовых сертификатов открытых ключей, что благоприятствует практическому применению нового подхода генерации коллективной электронной цифровой подписи.

Важен также вопрос минимизации размера коллективной электронной цифровой подписи при необходимости ее записи в виде штрих-кода на бумажных носителях, например, в методах защиты от подделки документов с помощью электронной цифровой подписи [4]. В данном аспекте представляет интерес изучение вопроса о возможности реализации новых протоколов коллективной электронной цифровой подписи как с использованием процедур проверки электронной цифровой подписи, специфицируемых стандартами подписи, так и новых протоколов, позволяющих уменьшить размер подписи.

В настоящей работе представлены новые протоколы коллективной цифровой подписи на эллиптических и гиперэллиптических кривых на основе стандарта электронной цифровой подписи ДСТУ 4145-2002 и предложенного в [6] протокола электронной цифровой подписи с предвычислениями ECPR. Вычислительные схемы протоколов проиллюстрированы примерами.

1 ГИПЕРЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

В качестве источника абелевой группы для протокола коллективной подписи на основе ДСТУ-4145, предложенного в [4], можно взять группу дивизоров гиперэллиптической кривой. Основное преимущество использования гиперэллиптических кривых состоит в том, что размер основного поля, над которым определена кривая, уменьшается пропорционально роду кривой без потери стойкости, хотя сама формула группового сложения выглядит более громоздко.

Пусть F – конечное поле и пусть $\overline{F}$ – алгебраическое замыкание поля F. Гиперэллиптическая кривая C рода $g \ge 1$ над F представляет собой [7] набор решений $(x, y) \in F \times F$ уравнения

$$C: y^2 + h(x)y = f(x), \qquad (1)$$

где $h(x) \in F[x]$ – полином степени не более g, $f(x) \in F[x]$ – нормированный полином степени $2g+1$ и не существует решений $(x, y) \in \overline{F} \times \overline{F}$, которые бы одновременно удовлетворяли уравнению (1) и уравнениям $2y + h(x) = 0$ и $h'(x)y - f'(x) = 0$. Считаем, что бесконечно удаленная точка ∞ также принадлежит кривой.

Согласно [7], в качестве групповой структуры в случае гиперэллиптических кривых рассматривается якобиан кривой C. Каждый элемент якобиана – это класс эквивалентности дивизоров, который может быть представлен уникально приведенным дивизором в виде пары полиномов в форме Мамфорда. На якобиане определены групповые операции сложения и дублирования дивизоров.

Согласно [8] порядок якобиана гиперэллиптической кривой ограничен интервалом Хассе – Вейла

$$\left|(\sqrt{q}-1)^{2g}\right| \le \#J/F_q \le [(\sqrt{q}+1)^{2g}],$$

где q – характеристика поля, над которым определена кривая, g – род кривой. Будем считать, что порядок якобиана

$$\#J/F_q \approx q^g.$$

Большинство криптографических приложений базируются на эллиптических или гиперэллиптических кривых с длиной ключа не менее 160 бит, то есть с порядком группы не менее 2^{160}. Следовательно, для криптосистем на гиперэллиптических кривых над полем F_q должно выполняться как минимум

$$g \cdot \log_2 q \approx 160.$$

В частности, для кривой рода 2 необходимо выбрать основное поле F_q с $|F_q| \approx 2^{80}$, с длиной операндов 80 бит. Для кривой рода 3 мощность основного поля $|F_q| \approx 2^{54}$, для кривой рода 4 $|F_q| \approx 2^{40}$.

Поскольку элементы подписи принадлежат основному полю, над которым определена кривая, в случае гиперэллиптических кривых размер итоговой коллективной подписи уменьшается пропорционально роду кривой. Так, при использовании гиперэллиптической кривой второго рода размер коллективной подписи окажется приблизительно в два раза меньше, чем при использовании эллиптической кривой, обладающей аналогичным уровнем криптостойкости. Соответственно, при использовании кривой третьего, рода размер коллективной подписи уменьшится приблизительно в три раза и т. д.

В криптографических целях используются гиперэллиптические кривые рода 2 и 3. Кривые более высокого рода не являются стойкими.

2 ПРОТОКОЛ КОЛЛЕКТИВНОЙ ПОДПИСИ НА ОСНОВЕ СТАНДАРТА ДСТУ 4145-2002 НА ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ

Введем обозначения:

D – базовый дивизор гиперэллиптической кривой;

l – количество пользователей;

n – порядок циклической подгруппы якобиана гиперэллиптической кривой;

d_i – секретный ключ i-го пользователя;

h – хэш-образ сообщения.

$\psi(R)$ – функция преобразования дивизора в элемент основного поля. Авторами предлагается следующее преобразование: коэффициенты первого полинома дивизора R представим в виде числа в системе счисления с основанием, равным модулю основного поля, над которым определена кривая (в случае простого поля). А затем переведем это представление в десятичную систему счисления.

Генерация открытого коллективного ключа.

1. Каждый i-й пользователь ($I = 1 \ldots l$) формирует открытый ключ вида

$$Q_i = -d_i D.$$

2. Коллективный открытый ключ вычисляется как сумма открытых ключей группы из l пользователей

$$Q = \sum_{i=1}^{l} Q_i = \sum_{i=1}^{l} -d_i D.$$

Формирование коллективной подписи.

1. Каждый пользователь рассчитывает дивизор R_i следующим образом:

а) выбирает случайный параметр k_i, $1 < k_i < n$;

б) вычисляет $R_i = k_i D$. .

2. По представленным пользователями дивизорам R_i вычисляется общий дивизор

$$R = \sum_{i=1}^{l} R_i.$$

3. Вычисляется значение функции $\psi(R)$.

4. Первая часть подписи определяется формулой $r = h\psi(R) \bmod n$.

5. Каждый пользователь вычисляет свой параметр s_i

$$s_i = (k_i + d_i r) \bmod n.$$

6. Вторая часть подписи определяется формулой $s = \sum_{i=1}^{l} s_i \bmod n$.

Коллективной подписью является пара чисел – (r, s).

Проверка коллективной подписи.

1. Проверяющий вычисляет хэш-образ h' общего сообщения.

2. Используя открытый коллективный ключ Q, вычисляет дивизор $R' = sD + rQ$ и

3. значение $v = h'\psi(R')$.

4. Если $v = r$, то подпись признается подлинной.

Пример 1. Проиллюстрируем протокол коллективной подписи, используя гиперэллиптическую кривую рода 2 над полем F_7:

$$y^2 = x^5 + 2x^2 + x + 3 \bmod 7.$$

Как показано в [9], якобиан этой кривой содержит 34 дивизора. Дивизор $D = <x + 4, 1>$ формирует подгруппу порядка $n = 17$.

Генерация открытого коллективного ключа.

Пусть число пользователей $l = 3$ и их секретные ключи соответственно равны:

$$d_1 = 5,\ d_2 = 7,\ d_3 = 11.$$

Тогда открытыми ключами пользователей являются:

$$\begin{gathered} Q_1 = -5D = -\langle x^2 + 5x + 2, 2x\rangle = \langle x^2 + 5x + 2, 5x\rangle, \\ Q_2 = -7D = -\langle x^2 + 5x + 5, 5\rangle = \langle x^2 + 5x + 5, 2\rangle, \\ Q_3 = -11D = -\langle x^2 + 4x + 6, x + 4\rangle = \\ = \langle x^2 + 4x + 6, 6x + 3\rangle. \end{gathered}$$

Общий открытый ключ группы пользователей равен:

$$Q = Q_1 + Q_2 + Q_3 = \langle x^2 + 4x + 6, x + 4\rangle.$$

Формирование коллективной подписи.

Каждый пользователь генерирует случайный параметр k_i:

$$k_1 = 5,\ k_2 = 9,\ k_3 = 12$$

и вычисляет дивизор $R_i = k_i D$:

$$\begin{gathered} R_1 = 5\langle x + 4, 1\rangle = \langle x^2 + 5x + 2, 2x\rangle, \\ R_2 = 9\langle x + 4, 1\rangle = \langle x^2 + 3x + 5, 6x + 5\rangle, \\ R_3 = 12\langle x + 4, 1\rangle = \langle x^2 + 5x + 2, 5x\rangle. \end{gathered}$$

Вычисленные дивизоры R_i предоставляются для вычисления общего дивизора

$$R = \sum_{i=1}^{3} R_1 = \langle x^2 + 3x + 5, 6x + 5\rangle.$$

По дивизору R вычисляется функция $\psi(R)$:

$$\psi(R) = 135_7 \bmod 17 = (7^2 + 3*7 + 5) \bmod 17 = 7.$$

Пусть хэш-образ h общего для группы пользователей сообщения равен 15: $h = 15$. Тогда первая часть коллективной подписи r вычисляется по формуле:

$$r = h\psi(R) = 15*7 \bmod 17 = 3.$$

Далее каждый пользователь по своему секретному ключу d_i, значению k_i и общему значению r вычисляет свою долю второй части подписи:

$$s = 5 + 5*3 \bmod 17 = 3,\ s = 9 + 7*3 \bmod 17 = 13,$$
$$s = 12 + 11*3 \bmod 17 = 11.$$

Вторая часть коллективной подписи равна:

$$s = \sum_{i=1}^{3} s_i = (3 + 13 + 11) \bmod 17 = 10.$$

Таким образом, коллективная подпись группы из трех пользователей под общим сообщением есть $(r, s) = (3, 10)$.

Проверка коллективной подписи.

Проверяющий вычисляет хэш-образ $h' = 15$ общего сообщения.

Используя открытый коллективный ключ Q, вычисляет дивизор

$$\begin{gathered} R' = sD + rQ = 10D + 3Q = \\ = 10\langle x + 4, 1\rangle + 3\langle x^2 + 4x + 6, x + 4\rangle = \\ = \langle x^2 + 5x + 5, 2\rangle + \langle x + 4, 6\rangle = \\ = \langle x^2 + 3x + 5, 6x + 5\rangle \end{gathered}$$

и находит значение

$$\begin{gathered} \psi(R') = \psi(\langle x^2 + 3x + 5, 6x + 5\rangle) = \\ = 135_7 \bmod 17 = 7 + 3*7 + 5 = 7. \end{gathered}$$

Поскольку

$$v = h'\psi(R') = 15*7 \bmod 17 = 3$$

совпадает с r, то подпись признается подлинной.

3 ПРОТОКОЛ КОЛЛЕКТИВНОЙ ПОДПИСИ НА ОСНОВЕ ПРОТОКОЛА ECPR НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Протокол электронной цифровой подписи с предвычислениями ECPR [6] был предложен с целью уменьшить трудоемкость операции верификации подписи в корпоративной сети за счет умножения только на базовую точку, которое можно выполнить с предвычислениями. Модифицируем этот протокол для реализации коллективной подписи.

Введем обозначения:

P – базовая точка эллиптической кривой;

l – количество пользователей;

n – порядок циклической подгруппы точек эллиптической кривой;

d_i – секретный ключ i-го пользователя;

h – хэш-образ сообщения;

$\pi(R) = X_R \bmod n$ – выделение x-координаты точки $R = (X_R, Y_R)$ эллиптической кривой.

Генерация открытого коллективного ключа.

1. Каждый i-й пользователь ($i = 1 \ldots l$) формирует открытый ключ вида

$$Q_i = -d_i P.$$

2. Коллективный открытый ключ вычисляется как сумма открытых ключей группы из l пользователей

$$Q = \sum_{i=1}^{l} Q_i = \sum_{i=1}^{l} -d_i P.$$

Формирование коллективной подписи.

1. Каждый i-й пользователь ($i = 1 \ldots l$) рассчитывает точку R_i следующим образом:

а) выбирает случайный параметр k_i, $1 < k_i < n$;

б) вычисляет значение $t_i = \frac{k_i}{h} \bmod n$;

в) и точку $R_i = t_i P$.

2. По представленным пользователями точкам R_i вычисляется общая точка

$$R = \sum_{i=1}^{l} R_i = (X_R, Y_R)$$

3. и значение $w = \pi(R) = X_R \bmod n$.

4. Формируется точка $wR = (x, y)$ и

5. первая часть коллективной подписи

$$r = \pi(x, y) = x \bmod n.$$

6. Каждый пользователь вычисляет свой параметр s_i

$$s_i = (wk_i + hd_i) \bmod n$$

7. и предоставляет его для вычисления второй части коллективной подписи

$$s = \sum_{i=1}^{l} s_i.$$

Коллективной подписью является пара чисел – (r, s).

Проверка коллективной подписи.

1. Проверяющий вычисляет хэш-образ h' общего сообщения

2. и значение $t = \frac{s}{h'} \bmod n$.

3. Используя открытый коллективный ключ Q, формирует точку $tP + Q = (x, y)$

4. и вычисляет значение $v = \pi(x, y) = x \bmod n$.

5. Если $v = r$, то подпись признается подлинной.

Обоснование корректности представленного протокола

Поскольку при формировании подписи значение r определяется формулой $r = \pi(wR) = \pi\left(w \sum_{i=1}^{l} \frac{k_i}{h} P\right)$, а при проверке подписи проверочное выражение $tP + Q$ дает точку wR

$$tP + Q = \frac{s}{h}P - \sum_{i=1}^{l} d_i P = \frac{\sum_{i=1}^{l}(wk_i + hd_i)}{h} P - \sum_{i=1}^{l} d_i P =$$
$$= w\sum_{i=1}^{l} \frac{k_i}{h} P + \sum_{i=1}^{l} d_i P - \sum_{i=1}^{l} d_i P = w \sum_{i=1}^{l} \frac{k_i}{h} P = wR,$$

в итоге имеем:

$$v = \pi(tP + Q) = \pi(wR),$$

что соответствует r при формировании подписи.

Пример 2. Проиллюстрируем протокол коллективной подписи, используя эллиптическую кривую над полем F_{79}:

$$y^2 = x^3 + x + 1 (\mathrm{mod}\, 79).$$

Базовая точка $P(5,62)$ этой эллиптической кривой образует циклическую подгруппу порядка 43.

Генерация открытого коллективного ключа.

Пусть число пользователей $l = 3$ и их секретные ключи соответственно равны:

$$d_1 = 11,\ d_2 = 26,\ d_3 = 38.$$

Тогда открытыми ключами пользователей являются:

$$Q_1 = (30, 48),\ Q_2 = (15, 28),\ Q_3 = (32, 4).$$

Общий открытый ключ группы пользователей равен:

$$Q = Q_1 + Q_2 + Q_3 = (30, 31).$$

 ISSN 1607-3274 «Радіоелектроніка. Інформатика. Управління» № 1, 2008

Формирование коллективной подписи.

Каждый пользователь генерирует случайный параметр k_i:

$$k_1 = 5,\ k_2 = 17,\ k_3 = 23.$$

Следуя протоколу, каждый пользователь рассчитывает значение t_i:

$$t_1 = \frac{5}{37}\mathrm{mod}43 = 35,\ t_2 = \frac{17}{37}\mathrm{mod}43 = 33,$$
$$t_3 = \frac{23}{37}\mathrm{mod}43 = 32$$

и находит точку R_i:

$$R_1 = 35P = (29, 18),\ R_2 = 33P = (16, 20),$$
$$R_3 = 32P = (30, 48).$$

Вычисленные точки R_i предоставляются для вычисления общей точки

$$R = R_1 + R_2 + R_3 = (34, 32).$$

По точке R вычисляется функция $\pi(R)$

$$w = \pi(R) = 34\mathrm{mod}43 = 34.$$

С использованием полученного значения определяется точка

$$wR = 34R = (31, 35)$$

и первая часть коллективной подписи r

$$r = \pi(31, 35) = 31\mathrm{mod}43 = 31.$$

Пусть хэш-образ h общего для группы пользователей сообщения равен 37: $h = 37$.

Далее каждый пользователь по своему секретному ключу d_i, значению k_i и общим значениям w и h вычисляет свою долю второй части подписи:

$$s_1 = (43*5 + 37*11)\mathrm{mod}43 = 18,$$
$$s_2 = (34*17 + 37*26)\mathrm{mod}43 = 35,$$
$$s_3 = (34*23 + 37*38)\mathrm{mod}43 = 38.$$

Вторая часть коллективной подписи равна:

$$s = (s_1 + s_2 + s_3)\mathrm{mod}n = (18 + 35 + 38)\mathrm{mod}43 = 5.$$

Таким образом, коллективная подпись группы из трех пользователей под общим сообщением есть $(r, s) = (31,5)$.

Проверка коллективной подписи.

Проверяющий вычисляет хэш-образ $h' = 37$ общего сообщения.

Используя хэш-образ сообщения и открытый коллективный ключ Q, вычисляет значение

$$t = \frac{s}{h}\mathrm{mod}n = \frac{5}{37}\mathrm{mod}43 = 35$$

и точку

$$tP + Q = 35*(5, 62) + (30, 31) =$$
$$= (29, 18) + (30, 31) = (31, 35).$$

Поскольку

$$v = 31\mathrm{mod}43 = 31,$$

то есть $v = r$, то подпись признается подлинной.

4 ПРОТОКОЛ КОЛЛЕКТИВНОЙ ПОДПИСИ НА ОСНОВЕ ПРОТОКОЛА ECPR НА ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ

В качестве источника абелевой группы для предложенного протокола можно также взять группу дивизоров гиперэллиптической кривой, как это было сделано выше для ДСТУ-4145. В этом случае базовой точке, открытым ключам пользователей, и промежуточной точке R соответствуют дивизоры гиперэллиптической кривой.

Генерация открытого коллективного ключа.

1. Каждый i-й пользователь $(i = 1...l)$ формирует открытый ключ вида

$$Q_i = -d_i D.$$

2. Коллективный открытый ключ вычисляется как сумма открытых ключей группы из l пользователей

$$Q = \sum_{i=1}^{l} Q_i = \sum_{i=1}^{l} -d_i D.$$

Формирование коллективной подписи.

1. Каждый пользователь рассчитывает дивизор R_i следующим образом:

а) выбирает случайный параметр k_i, $1 < k_i < n$;

б) вычисляет $t_i = \frac{k_i}{h}\mathrm{mod}n$

в) и $R_i = t_i D$.

2. По представленным пользователями дивизорам R_i вычисляется общий дивизор

$$R = \sum_{i=1}^{l} R_i$$

3. и значение $w = \psi(R)$.

4. Формируется дивизор wR и

5. первая часть коллективной подписи $r = \psi(wR)$.

6. Каждый пользователь вычисляет свой параметр s_i

$$s_i = (wk_i + hd_i)\bmod n$$

7. и предоставляет его для вычисления второй части коллективной подписи

$$s = \sum_{i=1}^{l} s_i.$$

Коллективной подписью является пара чисел – (r, s).

Проверка коллективной подписи.

1. Проверяющий вычисляет хэш-образ h' общего сообщения

2. и значение $t = \frac{s}{h'}\bmod n$.

3. Используя открытый коллективный ключ Q, формирует дивизор $tD + Q$

4. и вычисляет значение $v = \psi(tD + Q)$.

5. Если $v = r$, то подпись признается подлинной.

Пример 3. Проиллюстрируем протокол коллективной подписи, используя гиперэллиптическую кривую, секретные ключи, открытый коллективный ключ, хэш-образ сообщения и случайные параметры k_i из примера 1.

Формирование коллективной подписи.

Следуя протоколу, каждый пользователь рассчитывает значения t_i:

$$t_1 = \frac{5}{15}\bmod 17 = 6,\quad t_2 = \frac{9}{15}\bmod 17 = 4,$$
$$t = \frac{12}{15}\bmod 17 = 11$$

и находит дивизор R_i:

$$R_1 = 6D = \langle x^2 + 4x + 6, 6x + 3\rangle,$$
$$R_2 = 4D = \langle x^2 + 5x + 3, 5x\rangle,$$
$$R_3 = 11D = \langle x^2 + 4x + 6, x + 4\rangle.$$

Вычисленные дивизоры R_i предоставляются для вычисления общего дивизора

$$R = R_1 + R_2 + R_3 = \langle x^5 + 5x + 3, 5x\rangle.$$

По дивизору R вычисляется функция $\psi(R)$:

$$w = \psi(R) = 153_7\bmod 17 = 7^2 + 5*7 + 3\bmod 17 = 2.$$

С использованием полученного значения определяется дивизор

$$wR = 2R = \langle x^2 + 3x + 5, x + 2\rangle$$

и первая часть коллективной подписи r

$$r = \pi(x^2 + 3x + 5, x + 2) = 135_7\bmod 17 =$$
$$= (7^2 + 3*7 + 5)\bmod 17 = 7.$$

Далее каждый пользователь по своему секретному ключу d_i, значению k_i и общим значениям w и h вычисляет свою долю второй части подписи:

$$s_1 = (2*5 + 15*5)\bmod 17 = 0,$$
$$s_2 = (2*9 + 15*7)\bmod 17 = 4,$$
$$s_3 = (2*12 + 15*11)\bmod 17 = 2.$$

Вторая часть коллективной подписи равна:

$$s = (s_1 + s_2 + s_3)\bmod n = (0 + 4 + 2)\bmod 17 = 6.$$

Таким образом, коллективная подпись группы из трех пользователей под общим сообщением есть $(r, s) = (7,6)$.

Проверка коллективной подписи.

Проверяющий вычисляет хэш-образ $h' = 15$ общего сообщения.

Используя хэш-образ сообщения и открытый коллективный ключ Q, вычисляет

$$t = \frac{s}{h}\bmod n = \frac{6}{15}\bmod 17 = 14$$

и

$$tD + Q = 14*\langle x + 4, 1\rangle + \langle x^2 + 4x + 6, x + 4\rangle =$$
$$= \langle x^2 + x + 6, 6x + 1\rangle + \langle x^2 + 4x + 6, x + 4\rangle =$$
$$= \langle x^2 + 3x + 5, x + 2\rangle.$$

Поскольку

$$v = \psi(\langle x^2 + 3x + 5\rangle) = 135_7\bmod 17 =$$
$$= (7^2 + 3*7 + 5)\bmod 17 = 7,$$

то есть $v = r$, то подпись признается подлинной.

Таким образом, действие предложенных протоколов наглядно показано на примерах с небольшими размерами параметров. На практике для обеспечения достаточной стойкости порядок группы, для которой определен протокол, должен превышать 2^{160}.

ЗАКЛЮЧЕНИЕ

Представленные в статье протоколы основаны на предложенном недавно способе формирования и проверки подлинности коллективной цифровой подписи, базирующейся на понятии общего (коллективного) открытого ключа. Они обладают тем качеством, что размер подписи не увеличивается пропорционально числу подписавших участников. В дальнейшем необходимо рассмотреть вопросы стойкости предложенных схем к различным типам атак.

ПЕРЕЧЕНЬ ССЫЛОК

1. *Min-Shiang Hawng, Cheng-Chi Le.* Research issues and challenges for multiple digital signature // Int. J. of Network Security. – 2005. – Vol. 1, No 1. – P. 1–7.
2. *Молдовян Н. А., Молдовян П. А.* Новые протоколы слепой подписи // Безопасность информационных технологий. – М.:МИФИ. –2007. – № 3. – С. 17–21.
3. *Артамонов А. В., Маховенко Е. Б.* Применение алгоритма Шнорра в протоколе коллективной подписи // Материалы XIV Всероссийской научной конференции «Проблемы информационной безопасности в системе высшей школы». – 2007. – С. 17–18.
4. *Гортинская Л. В., Молдовян Н. А., Козина Г. Л.* Реализация протоколов коллективной подписи на основе стандартов ГОСТ 34.310–95 и ДСТУ 4145-2002 // Правове, нормативне та метрологичне забезпечення системи захисту інформації в Україні. – Киев: НТУУ «КПІ». – 2008. – № 1. – С.21–25.
5. *Карякин Ю. Д.* Технология «AXIS-2000» защиты материальных объектов от подделки // Управление защитой информации. – Минск: Институт технической кибернетики АН Белоруссии. – 1997. – Т. 1, № 2. – С. 90–97.
6. *Anna Nelasa, Victor Dolgov, Anatolij Pogorily.* Digital Signature Protocol for corporate network // Proceedings of International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2008). – Lviv-Slavsko (Ukraine). – 2008. – Pp. 396–397.
7. *A. Menezes, Y. Wu, R. Zuccherato.* An Elementary Introduction to Hyperelliptic Curves – Springer-Verlag, Berlin (Germany), 1998. – 31 p.
8. *D. G. Cantor.* Computing in Jacobian of a Hyperelliptic Curve // In Mathematics of Computation, volume 48 (177). – January 1987. – P. 95–101.
9. *Неласая А. В.* Протокол цифровой подписи на гиперэллиптических кривых // Радіоелектроніка. Інформатика. Управління. – Запорожье: ЗНТУ. – 2006. – № 1. – С. 113–118.

Після доробки 17.03.2008

В статті пропонуються нові протоколи колективного цифрового підпису на еліптичних та гіпереліптичних кривих. Обчислювальні схеми проілюстровані на прикладах.

New collective digital signature protocols on elliptic and hyperelliptic curves are proposed. Computational algorithms are illustrated with numerical examples.

УДК 65.012.8(043)

В. И. Слепцов, Л. М. Карпуков

ПРАВОВАЯ ПОДГОТОВКА КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматриваются некоторые вопросы правовой подготовки специалистов по направлениям, входящим в отрасль знаний «Информационная безопасность», с учетом специфики их будущей профессиональной деятельности, учебных задач, законодательства Украины и опыта работы кафедры защиты информации Запорожского национального технического университета.

ВВЕДЕНИЕ

Уровень информационной безопасности, как в государственных структурах, так и в сфере хозяйственной деятельности, во многом определяется качеством подготовки работающих там специалистов, получивших образование по различным направлениям, объединяемым областью знаний «Информационная безопасность». Эффективность их усилий, направленных на защиту интересов субъектов информационных отношений зависит, прежде всего, от умения выявлять и оценивать угрозы, определять состояние защищенности информации, обоснованно выбирать способы ее защиты от совокупности реальных угроз, разрабатывать и внедрять системы защиты на основе требований законодательства Украины.

Базовые теоретические знания с получением необходимых практических навыков студенты, обучающиеся в ЗНТУ по специальностям «Защита информации в компьютерных системах и сетях» и «Системы защиты от несанкционированного доступа», приобретают при изучении дисциплин: «Основы информационной безопасности», «Физико-технические методы защиты информации», «Организационно-техническое обеспечение систем защиты информации», «Криптографические методы защиты информации» и др. Не возникает особых проблем при определении объема лекционного материала, методологии преподавания, если речь идет о традиционных вопросах, связанных с изучением технических каналов утечки информации и методов их закрытия, программно-аппаратных способов получения несанкционированного доступа к защищаемой информации, обрабатываемой в информационно-теле-