УДК 681.3

РАСШИРЕНИЕ ФУНКЦИОНАЛЬНОСТИ СТАНДАРТОВ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Д. Н. Молдовян,
аспирант
Е. С. Дернова,
канд. техн. наук, преподаватель
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
Д. К. Сухов,
аспирант
Санкт-Петербургский институт информатики и автоматизации РАН

Рассмотрена реализация схем слепой и слепой коллективной подписи, использующих процедуры проверки подлинности электронной цифровой подписи, рекомендуемые российскими стандартами.

Ключевые слова *— электронная цифровая подпись, слепая подпись, открытый ключ, стандарты электронной цифровой подписи, коллективная слепая подпись.*

Введение

Электронная цифровая подпись (ЭЦП) широко применяется для решения различных практических задач электронного документооборота и других современных информационных технологий. Важными типами схем ЭЦП являются протоколы слепой [1, 2] и коллективной [3, 4] ЭЦП. Протокол коллективной подписи позволяет сформировать единую ЭЦП фиксированного размера как криптографическую сумму индивидуальных цифровых подписей практически произвольного числа подписывающих. Схемы слепой ЭЦП применяются в системах тайного электронного голосования и системах электронных денег. Протоколы данного вида решают задачу обеспечения неотслеживаемости (анонимности), которая состоит в том, что требуется подписать электронное сообщение M таким способом, что подписывающий 1) не может ознакомиться с сообщением в процессе формирования подписи и 2) впоследствии при получении сообщения M и подлинной подписи к нему не может однозначно идентифицировать пользователя, предоставлявшего данное сообщение для формирования ЭЦП. Прикладной интерес представляют также схемы ЭЦП, объединяющие возможности протоколов указанных двух типов, которые впервые были предложены в работе [5] как протоколы слепой коллективной ЭЦП. Для практических приложений важным является использование процедур формирования и проверки ЭЦП, рекомендуемых официальными стандартами.

В настоящей работе рассматривается построение схем слепой и слепой коллективной ЭЦП с использованием процедур формирования и проверки ЭЦП, рекомендуемых ГОСТ Р 34.10–94 [6] и Р 34.10–2001 [7, 8].

Схемы слепой ЭЦП на основе российских стандартов

Стандарт ЭЦП ГОСТ Р 34.10–94 рекомендует использование простого числа p, размер которого $|p|$ удовлетворяет условиям $1022 \le |p| \le 1024$ бит. При этом число p выбирается таким, что значение $p - 1$ содержит большой простой делитель $2^{511} \le q \le 2^{512}$ соответственно. Специфицируемые стандартом процедуры генерации и проверки ЭЦП используют число $\alpha < p$ такое, что $\alpha \ne 1$ и $\alpha^q \bmod p = 1$ (α является генератором циклической подгруппы конечного простого поля $GF(p)$, имеющей порядок q). Формирование ЭЦП в соответствии с ГОСТ Р 34.10–94 [6] осуществляется следующим образом.

1. Генерируется случайное число k, удовлетворяющее условию $1 < k < q$.

2. Формируется рандомизирующий параметр ЭЦП — значение $R = (\alpha^k \bmod p) \bmod q$, являющийся первой частью подписи.

3. По ГОСТ Р 34.11–94 вычисляется хэш-функция H от подписываемого сообщения M.

4. Вычисляется второй элемент ЭЦП в виде числа $S = kH + zR \bmod q$, где z — личный секретный ключ пользователя, формирующего свою подпись к сообщению M. Если $S = 0$, то следует перейти к шагу 1 и процедура генерации подписи повторяется.

Процедура проверки подлинности ЭЦП состоит в выполнении следующих шагов.

1. Выполняется проверка условий $r < q$ и $s < q$. Если хотя бы одно из этих условий не выполняется, то подпись признается недействительной.

2. Вычисляется (по ГОСТ Р 34.11–94) хэш-функция H от подписываемого сообщения M.

3. Вычисляется значение

$$R^* = (\alpha^{S/H} y^{-R/H} \bmod p) \bmod q. \qquad (1)$$

4. Сравниваются значения R и R^*. Если $R = R^*$, то подпись признается действительной.

Протокол слепой ЭЦП на основе ГОСТ Р 34.10–94 строится с использованием двух «ослепляющих» множителей, формируемых в виде $y^{\mu} \bmod p$ и $\alpha^{\varepsilon} \bmod p$. Множители такого типа использовались ранее в схеме слепой подписи на основе алгоритма ЭЦП Шнорра [9, 10]. Разработанный протокол слепой ЭЦП на основе ГОСТ Р 34.10–94 описывается следующим образом.

1. Подписывающий генерирует случайное значение $k < q$, вычисляет число $\rho = \alpha^k \bmod p$ и направляет его пользователю А, который намерен представить некоторое электронное сообщение M для получения к нему слепой ЭЦП подписывающего, из которой пользователь А сможет самостоятельно вычислить правильное значение ЭЦП, которое пройдет процедуру проверки ЭЦП по ГОСТ Р 34.10–94.

2. Пользователь А генерирует случайные равновероятные значения $\mu, \varepsilon \in \{1, 2, \ldots, q-1\}$, вычисляет значения $\rho' = \rho y^{\mu} \alpha^{\varepsilon} \bmod p$, $R' = \rho' \bmod q$ и $R = R'/H + \mu \bmod q$, где H — значение хэш-функции от подписываемого документа, вычисленное по ГОСТ Р 34.11–94. Значение R', которое остается неизвестным подписывающему, представляет собой первый элемент подлинной ЭЦП. Значение R представляет собой первый элемент формируемой слепой подписи.

3. Пользователь А отправляет подписывающему значение R, из которого нельзя вычислить R', поскольку для любого значения R' существует пара значений μ и ε, которые связывают значение R' с полученным числом R.

4. Подписывающий вычисляет значение $S = k + zR \bmod q$, где z — его секретный ключ, передает вычисленный элемент слепой подписи пользователю А.

5. Пользователь А вычисляет значение $S' = H(S + \varepsilon) \bmod q$, которое является вторым элементом подписи.

Полученная в соответствии с этим протоколом ЭЦП (R', S') является подлинной, т. е. она вместе со значением хэш-функции H от сообщения M проходит уравнение проверки ЭЦП, специфицируемое ГОСТ Р 34.10–94. Корректность работы описанной схемы слепой ЭЦП доказывается следующим путем.

Доказательство корректности. Элемент слепой подписи S вычисляется на шаге 4 по формуле $S = k + zR \bmod q$, из которой с учетом того, что число α имеет порядок q по модулю p, следует справедливость сравнения $\alpha^S \equiv \alpha^k \alpha^{zR} \bmod p$, откуда имеем $\rho \equiv \alpha^k \equiv \alpha^S \alpha^{-zR} \bmod p$. Учитывая, что $R' = H(R - \mu) \bmod q$, вычисление правой части уравнения проверки подлинности ЭЦП (1) для подписи (R', S') и значения хэш-функции H дает следующее:

$$\rho^* = y^{-\frac{R'}{H}} \alpha^{\frac{S'}{H}} = y^{-\frac{H(R-\mu)}{H}} \alpha^{\frac{H(S+\varepsilon)}{H}} = y^{-R+\mu} \alpha^{S+\varepsilon} =$$
$$= y^{-R} \alpha^S y^{\mu} \alpha^{\varepsilon} = \rho y^{\mu} \alpha^{\varepsilon} = \rho' \Rightarrow \rho^* \bmod q = R'. \qquad (2)$$

Последнее равенство означает, что подпись (R', S') к сообщению M является подлинной.

Рассмотренный протокол обеспечивает анонимность пользователя, предоставляющего сообщение для получения подписи вслепую в том смысле, что нельзя однозначно установить пользователя, предоставлявшего данное сообщение для формирования слепой ЭЦП (предполагается, что число сообщений, подписанных данным подписывающим с помощью протокола слепой подписи, $N > 1$). Подписывающий при предъявлении ему его подлинной подписи (R', S') к сообщению M не может установить пользователя, который предоставлял ему этот документ на подпись, с вероятностью выше значения d/N, где N — количество документов, подписанных (данным подписывающим) с помощью протокола слепой подписи; d — число документов, предоставлявшихся данным пользователем, поскольку любая подпись (R', S') может быть с равной вероятностью отнесена к каждой из N выполненных процедур протокола слепой подписи.

Действительно, любая тройка значений (ρ, R, S) из множества таких троек, которые известны подписывающему из N выполненных им процедур подписывания сообщений вслепую, может быть ассоциирована с произвольной подлинной подписью (R', S'), относящейся к некоторому сообщению, представленному значением хэш-функции H. Это связано с тем, что тройки (ρ, R, S) и (R', S', H) в соответствии с описанным протоколом слепой ЭЦП связаны случайными рав-

новероятными значениями μ и ε с помощью следующих соотношений: $\rho = \alpha^S y^{-R} \bmod p$ и $\rho' = \alpha^{S'/H} y^{-R'/H} \bmod p = \alpha^S y^{-R} y^{\mu} \alpha^{\varepsilon} \bmod p$, т. е. $\rho' = \rho y^{\mu} \alpha^{\varepsilon} \bmod p$, поэтому тройка (R', S', H) с равной вероятностью могла бы быть порождена из любой тройки (ρ, R, S), фигурировавшей в одной из N выполненных процедур слепого подписывания сообщений. (Отметим, что значение ρ однозначно определяется парой чисел R и S.)

Стандарт ЭЦП ГОСТ Р 34.10–2001 по построению подобен рассмотренному выше стандарту. Основное отличие состоит в том, что в нем вычисления выполняются не в циклической подгруппе конечного поля, а в конечной группе другой природы, в качестве которой используется эллиптическая кривая (ЭК) над конечным полем. Групповой операцией в группе точек ЭК является композиция или сложение точек ЭК. Аналогами операций умножения и возведения в степень по модулю, используемых в стандарте ЭЦП ГОСТ Р 34.10–94, в ГОСТ Р 34.10–2001 являются операции сложения точек ЭК и умножения точки на число соответственно. В силу указанной аналогии рассмотренный выше протокол слепой подписи может быть реализован также и на основе ГОСТ Р 34.10–2001.

ГОСТ Р 34.10–2001 регламентирует использование простого числа p — модуля ЭК, которая задается в декартовой системе координат уравнением вида $y^2 = x^3 + ax + d \bmod p$, где $a, b \in GF(p)$; простого числа q — порядка циклической подгруппы точек ЭК; точки G с координатами (x_G, y_G) такой, что $G \neq O$, $qG = O$, где O — бесконечно удаленная точка, являющаяся нейтральным элементом (нулем) группы точек ЭК. Секретным ключом является достаточно большое целое число $d < q$, а открытым ключом — точка $Q = dG$. Формирование подписи (R, S) осуществляется в соответствии со следующим алгоритмом.

1. Генерируется случайное целое число k $(0 < k < q)$.

2. Вычисляется точка $C = kG$ и определяется значение $r = x_C \bmod q$, где x_C — координата точки C.

3. Вычисляется значение $s = (rd + ke) \bmod q$, где $e = H \bmod q$, H — значение хэш-функции от подписываемого сообщения.

Подписью являются два числа (r, s). Проверка подписи заключается в вычислении координат точки C^*:

$$C^* = (se^{-1} \bmod q)G + ((q - r)e^{-1} \bmod q)Q, \quad (3)$$

определении значения $r^* = x_{C^*} \bmod q$ и проверке выполнения равенства $r^* = r$.

Протокол слепой подписи на основе рассмотренного алгоритма реализуется следующим образом.

1. Подписывающий генерирует случайное число $k < q$, вычисляет точку ЭК $C = kG$ и направляет ее пользователю А, который намерен получить слепую ЭЦП к сообщению M.

2. Пользователь А генерирует случайные значения $\mu, \varepsilon \in \{1, 2, \ldots, q - 1\}$, вычисляет точку ЭК $C' = C + \mu Q + \varepsilon G$ с координатами $(x_{C'}, y_{C'})$, значения $r' = x_{C'} \bmod q$, $e = H \bmod q$, где H — значение хэш-функции, вычисленное от M, и $r = r'e^{-1} + \mu \bmod q$. Значение r', которое остается неизвестным подписывающему, представляет собой первый элемент формируемой ЭЦП. Значение r является рандомизирующим элементом слепой ЭЦП.

3. Пользователь А отправляет подписывающему значение r, из которого нельзя вычислить r' (для любого r' существует пара чисел μ и ε, которые связывают значения r' и r).

4. Подписывающий вычисляет значение $s = k + dr \bmod q$, где d — его секретный ключ, передает вычисленный второй элемент s слепой подписи пользователю А.

5. Пользователь А вычисляет значение $s' = e(s + \varepsilon) \bmod q$, которое является вторым элементом подписи.

Вычисленная подпись (r', s') является подлинной ЭЦП к сообщению M.

Доказательство корректности. Элемент слепой подписи S вычисляется на шаге 4 по формуле $s = k + dr \bmod q$, из которой следует выполнимость соотношения $sG = kG + drG$. Из последнего уравнения получаем $C = kG = sG - drG$. Вычисление правой части проверочного уравнения (3) для ЭЦП (r', s') и значения хэш-функции H (которое определяет значение $e = H \bmod q$) дает следующее:

$$(s'e^{-1} \bmod q)G - r'Q =$$
$$= (s + \varepsilon \bmod q)G - (r - \mu \bmod q)Q = (sG - rQ) +$$
$$+ \varepsilon G + \mu Q = C + \varepsilon G + \mu Q = C' \Rightarrow r^* = x_{C'} = r'.$$

В соответствии с процедурой проверки ЭЦП выполнение равенства $r^* = r$ означает подлинность подписи (r', s'). Схема слепой ЭЦП на основе ГОСТ Р 34.10–2001 обеспечивает анонимность субъектов, предоставляющих электронные сообщения для подписывания, что легко доказывается по аналогии со случаем слепой ЭЦП на основе ГОСТ Р 34.10–94.

Протоколы слепой коллективной подписи

Протоколы слепой коллективной ЭЦП на основе ГОСТ Р 34.10–94 и Р 34.10–2001 разработаны путем встраивания в описанные в предыдущем разделе схемы слепой ЭЦП механизма свертки открытых ключей всех субъектов, входящих в коллектив подписывающих, ранее апробированного в работах [3, 4]. Схема слепой коллективной ЭЦП на основе ГОСТ Р 34.10–94 описывается следующим образом.

Пусть пользователь А желает подписать вслепую электронное сообщение M у m подписывающих, владеющих открытыми ключами $y_i = \alpha^{z_i} \bmod p$, где z_i — личный секретный ключ i-го подписывающего ($i = 1, 2, ..., m$). Предполагается, что проверка коллективной ЭЦП осуществляется по проверочному уравнению, специфицируемому ГОСТ Р 34.10–94 с использованием коллективного открытого ключа y в виде произведения открытых ключей всех подписывающих $y = y_1 y_2 ... y_m \bmod p$. Процедура формирования коллективной подписи вслепую состоит в выполнении следующих шагов.

1. Каждый i-й подписывающий генерирует случайное число $k_i (1 < k_i < q)$ и вычисляет свое индивидуальное рандомизирующее значение $\rho_i = \alpha^{k_i} \bmod p$.

2. Подписывающие вычисляют общее рандомизирующее значение ρ путем перемножения всех индивидуальных рандомизирующих значений ρ_i, т. е. в виде $\rho = \prod_{i=1}^{m} \rho_i \bmod p$. Значение ρ направляется пользователю А.

3. Пользователь А генерирует случайные значения $\mu, \varepsilon \in \{1, 2, ..., q-1\}$, вычисляет значения $\rho' = \rho y^{\mu} \alpha^{\varepsilon} \bmod p$, $R' = \rho' \bmod q$ и $R = R'/H + \mu \bmod q$, где H — значение хэш-функции от подписываемого документа. Значение R является первым элементом слепой коллективной подписи, а R' — первым элементом коллективной подписи к сообщению M.

4. Пользователь А отправляет подписывающим значение R.

5. Каждый i-й подписывающий вычисляет значение $S_i = k_i + z_i R \bmod q$, где z_i — его секретный ключ.

6. Подписывающие вычисляют свертку значений S_i в виде суммы $S = \sum_{i=1}^{m} S_i \bmod q$ и направляют ее пользователю А. Значение S является вторым элементом слепой коллективной подписи.

7. Пользователь А вычисляет значение $S' = H(S + \varepsilon) \bmod q$, которое является вторым элементом коллективной подписи.

Полученная в соответствии с этим протоколом ЭЦП (R', S') является подлинной, что подтверждается следующим доказательством.

Доказательство корректности. Элемент слепой подписи S, вычисляемый на шаге 6, может быть представлен в виде

$$S = \sum_{i=1}^{m} S_i \bmod q = \sum_{i=1}^{m} (k_i + z_i R) \bmod q = \left(\sum_{i=1}^{m} k_i + R \sum_{i=1}^{m} z_i \right) \bmod q.$$

Из последнего соотношения с учетом того, что число α имеет порядок q по модулю p, следует справедливость сравнения

$$\alpha^S \equiv \alpha^{\sum_{i=1}^{m} k_i} \alpha^{R \sum_{i=1}^{m} z_i} \equiv \rho y^R \bmod p,$$

из которого имеем $\rho \equiv \alpha^S y^{-R} \bmod p$. Учитывая, что $R' = H(R - \mu) \bmod q$, вычисление правой части проверочного уравнения (1) в случае проверяемой коллективной подписи (R', S') и значения хэш-функции H дает соотношения, совпадающие с (2), т. е. правая часть проверочного уравнения равна элементу R' проверяемой подписи, следовательно, подпись (R', S') к сообщению M является подлинной. Действительно, подстановка значений R' и S' в (1) дает

$$R^* = \left(y^{-\frac{R'}{H}} \alpha^{\frac{S'}{H}} \bmod p \right) \bmod q =$$

$$= \left(y^{-\frac{H(R-\mu)}{H}} \alpha^{\frac{H(S+\varepsilon)}{H}} \bmod p \right) \bmod q =$$

$$= (y^{-R+\mu} \alpha^{S+\varepsilon} \bmod p) \bmod q = (y^{-R} \alpha^S y^{\mu} \alpha^{\varepsilon} \bmod p) \bmod q =$$

$$= (R y^{\mu} \alpha^{\varepsilon} \bmod p) \bmod q = R' \Rightarrow R^* \bmod q = R'.$$

Протокол слепой коллективной подписи на основе ГОСТ Р 34.10–2001 реализуется следующим образом.

1. Каждый i-й подписывающий генерирует случайное число k_i, $1 < k_i < q$, вычисляет точку ЭК $C_i = k_i G$.

2. Подписывающие вычисляют результирующую точку $C = C_1 + C_2 + ... + C_m$ и направляют ее пользователю А, который намерен получить слепую подпись к электронному сообщению M.

3. Пользователь А генерирует случайные значения $\mu, \varepsilon \in \{1, 2, ..., q-1\}$, вычисляет точку ЭК $C' = C + \mu Q + \varepsilon G$ с координатами ($x_{C'}$, $y_{C'}$), значения $r' = x_{C'} \bmod q$ и $r = (r'/e + \mu) \bmod q$, где $e = H \bmod q$; H — значение хэш-функции от подписываемого сообщения. Значение r' является первым элементом формируемой подписи.

4. Пользователь А отправляет подписывающему значение r.

5. Каждый i-й подписывающий вычисляет значение $s_i = k_i + d_i r \bmod q$, где d_i — его личный секретный ключ.

6. Подписывающие вычисляют значение $s = s_1 + s_2 + ... + s_m \bmod q$, которое является элементом слепой подписи, и передают значение s пользователю А.

7. Пользователь А вычисляет значение $s' = e(s + \varepsilon) \bmod q$, которое является вторым элементом подписи.

Проверка подлинности коллективной ЭЦП выполняется по проверочному уравнению (3), в которое вместо индивидуального открытого ключа подставляется коллективный открытый ключ, равный точке $Q = Q_1 + Q_2 + ... + Q_m$.

Подписывающие не могут вычислить пару чисел (r', s'), которая представляет собой подпись, полученную пользователем А в результате выполнения протокола слепой коллективной ЭЦП.

Подпись (r', s') является подлинной и соответствует сообщению M. Корректность последнего протокола легко доказать по аналогии с доказательствами корректности приведенных выше протоколов. Действительно, подстановка значений r' и s' в (3) дает

$$C^* = (s'e^{-1} \bmod q)G - r'e^{-1}Q = (s + \varepsilon \bmod q)G - \\ - (r - \mu \bmod q)Q = (sG - rQ) + \varepsilon G + \mu Q = \\ = C + \varepsilon G + \mu Q = C' \Rightarrow r^* = x_{C^*} = x_{C'} = r'. \quad (4)$$

Описанные в этом разделе схемы слепой ЭЦП на основе российских стандартов ЭЦП решают задачу обеспечения анонимности. Доказательство этого выполняется аналогично для случаев использования обоих приведенных стандартов. Рассмотрим случай ГОСТ Р 34.10–2010.

Пусть коллектив подписавших получил некоторый документ M и коллективную подпись к нему в виде пары чисел (r', s'). Покажем, что любое из зарегистрированных им значений слепой подписи (r, s) может быть соотнесено с (r', s'). Вычисление долей подписи индивидуальными подписывающими выполнялось по формуле $s_i = k_i + d_i r \bmod q$, поэтому имеем

$$s = \sum_{j=1}^{m} s_j = \sum_{j=1}^{m} k_j + d_j r \bmod q = \left(\sum_{j=1}^{m} k_j + r \sum_{j=1}^{m} d_j \right) \bmod q \Rightarrow$$

$$\Rightarrow sG = \left(\sum_{j=1}^{m} k_j \bmod q \right) G + \left(r \sum_{j=1}^{m} d_j \bmod q \right) G =$$

$$= \sum_{j=1}^{m} k_j G + r \sum_{j=1}^{m} d_j G = \sum_{j=1}^{m} C_j + r \sum_{j=1}^{m} Q_j = C + rQ.$$

Из уравнения проверки подлинности ЭЦП и соотношений (4) для правильной подписи имеем

$$C' = s'e^{-1}G - r'e^{-1}Q = C + (s'e^{-1}G - r'e^{-1}Q) - \\ - (sG - rQ) = C + (s'e^{-1} - s \bmod q)G + \\ + (r - r'e^{-1} - s \bmod q)Q = C + \varepsilon G + \mu Q.$$

Следовательно, для каждой из сформированных слепых коллективных подписей (r, s) имеется единственная пара значения μ и ε, которая связывает (r, s) с (r', s'). Поскольку данные значения формировались субъектами, представлявшими электронные сообщения для получения слепой ЭЦП, то любая из сформированных слепых подписей с одинаковой вероятностью может быть связана с данной конкретной подписью (r', s').

Заключение

Предложенные схемы слепой и коллективной слепой ЭЦП используют проверочные уравнения, рекомендуемые стандартами ЭЦП ГОСТ Р 34.10–94 и Р 34.10–2001. Это означает, что разработанные протоколы могут быть положены в основу расширения функциональности этих стандартов, благодаря чему механизмы ЭЦП могут найти более широкое применение в информационных технологиях, в частности при построении систем электронных денег и систем тайного электронного голосования.

Работа выполнена в рамках исследований по Федеральной целевой программе «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (конкурсная заявка № НК-563П/59).

Литература

1. **Chaum D.** Blind Signatures for Untraceable Payments // Intern. Conf. Advances in Cryptology: Proc. CRYPTO'82. Plenum Press, 1983. P. 199–203.
2. **Chaum D.** Security Without Identification: Transaction Systems to Make Big Brother Obsolete // Communication of the ACM. Oct. 1985. Vol. 28. N 10. P. 1030–1044.
3. **Молдовян А. А., Молдовян Н. А.** Новые алгоритмы и протоколы для аутентификации информации в АСУ // Автоматика и телемеханика. 2008. № 7. С. 157–169.
4. **Ананьев М. Ю., Гортинская Л. В., Молдовян Н. А.** Протоколы коллективной подписи на основе свертки индивидуальных параметров // Информационно-управляющие системы. 2008. № 2. С. 22–27.
5. **Moldovyan N. A., Moldovyan A. A.** Blind Collective Signature Protocol Based on Discrete Logarithm Problem // Intern. Journal of Network Security. 2010. Vol. 11. N 2. P. 106–113.
6. **ГОСТ** Р 34.10–94. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — М.: Изд-во стандартов, 1994. — 18 с.
7. **ГОСТ** Р 34.10–2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — М.: Изд-во стандартов, 2001. — 12 с.
8. **Рябко Б. Я., Фионов А. Н.** Криптографические методы защиты информации. — М.: Горячая линия — Телеком, 2005. — 229 с.
9. **Pointcheval D., Stern J.** Security arguments for digital signatures and blind signatures // J. Cryptology. 2000. Vol. 13. N 3. P. 361–396.
10. **Молдовян Н. А.** Теоретический минимум и алгоритмы цифровой подписи. — СПб.: БХВ-Петербург, 2010. — 290 с.