УДК 681.3

СХЕМА СЛЕПОЙ 240-БИТОВОЙ ЦИФРОВОЙ ПОДПИСИ

Д. Н. Молдовян,
аспирант
И. Н. Васильев,
аспирант
Санкт-Петербургский государственный электротехнический университет им. В. И. Ульянова (Ленина)
А. И. Краснова,
канд. техн. наук, доцент
Санкт-Петербургский государственный университет аэрокосмического приборостроения

На основе конечных групп с двухмерной цикличностью реализована схема слепой 240-битовой электронной цифровой подписи. Использованная группа представляет собой подгруппу мультипликативной группы кольца вычетов по трудно разложимому модулю.

Ключевые слова *— электронная цифровая подпись, слепая подпись, группа с двухмерной цикличностью, трудная задача, задача факторизации, открытый ключ.*

Введение

В технологии криптографической защиты материальных объектов от подделки [1] предусматривается запись электронной цифровой подписи (ЭЦП) на бумажный носитель в виде машиночитаемой метки. В таких случаях актуальной является задача разработки схем ЭЦП с достаточно малым размером подписи. Известны схемы ЭЦП, основанные на вычислительной трудности задач дискретного логарифмирования (ЗДЛ), с размером подписи $4L$ бит в случае L-битовой стойкости (т. е. в случае трудоемкости взлома таких схем, равной 2^L операций умножения по модулю). Схемы ЭЦП, основанные на трудности задачи факторизации (ЗФ), обычно имеют существенно больший размер подписи, однако сравнительно недавно над ЗФ были предложены схемы ЭЦП с малым размером подписи [2, 3]. Важным для информационных технологий типом схем ЭЦП являются протоколы слепой подписи [4, 5], используемые в системах электронных денег и тайного электронного голосования. Для протоколов слепой ЭЦП также актуальной является задача получения подписей достаточно малого значения при обеспечении заданного уровня стойкости.

В настоящей работе рассматривается построение схемы слепой ЭЦП размером $3L$ бит, основанной на трудности ЗФ. Схема строится с использованием подгруппы мультипликативной группы конечного кольца вычетов по трудно разложимому модулю. Особенностью использованной подгруппы является ее двухмерное циклическое строение. Ранее схемы ЭЦП над конечными группами с многомерной цикличностью предложены в работах [6–8], однако реализация протоколов слепой ЭЦП с малым размером подписи не рассматривалась.

Задание подгруппы с двухмерной цикличностью

Для построения протокола слепой $3L$-битовой ЭЦП используется подгруппа мультипликативной группы конечного кольца Z_n, где n — натуральное число, равное произведению двух сильных простых чисел [9] q и p длиной $|q| \approx |p| \approx 512$ бит. Числа q и p являются секретными значениями и имеют следующую структуру: $p = N_p r^2 + 1$ и $q = N_q r^2 + 1$, где N_p и N_q — два больших четных числа, содержащих большой простой делитель; r — 80-битовое простое число. Мультипликативная группа Z_n^* кольца Z_n порождается базисом, включающим два элемента. Это следует из того, что значение обобщенной функции Эйлера $L(n)$ от числа n меньше значения функции Эйлера от числа n:

$$\varphi(n) = (q-1)(p-1) = \text{НОД}(q-1, p-1)\text{НОК}[q-1, p-1] = \text{НОД}(q-1, p-1)L(n) \geq r^2 L(n),$$

где НОД — наибольший общий делитель; НОК — наименьшее общее кратное.

В предлагаемой схеме ЭЦП применяется примарная подгруппа Г порядка r^2 группы Z_n^*, обладающая двухмерной цикличностью и порождаемая базисом, включающим два элемента α и β порядка r. Все элементы подгруппы Г, кроме единицы, обладают порядком r. Значения базисных элементов α и β генерируются по следующей вероятностной процедуре:

1) выбирается случайное число b, превосходящее 1 и меньшее числа n;

2) вычисляется значение $\gamma = L(n)/r$ и число $z = b^{\gamma} \bmod n$;

3) если $z \neq 1$, то в качестве числа α (числа β) взять число z. В противном случае повторить шаги 1–3.

Действительно, для полученного числа $z \neq 1$ имеем $z = b^{L(n)/r} \bmod p$. Следовательно, согласно обобщенной теореме Ферма, имеем $z^r \equiv b^{L(n)} \equiv \equiv 1 \bmod n$, т. е. порядок числа z равен r. (Известно, что при выполнении условия $z^r \equiv 1 \bmod n$ порядок числа z делит r. Так как r есть простое число, то оно и является показателем.) Выполнив два раза эту процедуру, получим два случайных числа порядка r по модулю n. Вероятность того, что эти два числа принадлежат одной циклической подгруппе, равна отношению числа неединичных элементов в циклической подгруппе простого порядка r к числу элементов порядка r, содержащихся в Z_n^*. В группе Z_n^* содержится примарная подгруппа порядка r^2, порождаемая двумя элементами порядка r. В этой примарной подгруппе содержится $r^2 - 1$ элементов порядка r [10]. Следовательно, указанная ранее вероятность равна $r/(r^2 - 1) \approx 1/r \approx 2^{-80}$. Данной вероятностью можно пренебречь и не выполнять трудоемкую процедуру проверки того, что сгенерированные числа α и β не лежат в одной и той же циклической подгруппе.

Данная вероятность может быть понижена до значения $\approx 2^{-160}$ при генерации чисел α и β по следующей модифицированной процедуре:

1) выбирается случайное число b, превосходящее 1 и меньшее числа n;

2) вычисляется значение $\gamma = L(n)/r^2$ и число $z = b^{\gamma} \bmod n$;

3) если $z \neq 1$ и $\alpha'(\beta') = z^r \bmod n \neq 1$, то в качестве числа α (числа β) взять число $\alpha'^r \bmod n$ (число $\beta'^r \bmod n$). В противном случае повторить шаги 1–3.

Снижение вероятности достигается за счет того, что предварительно генерируется число порядка r^2, а затем это число возводится в степень r и полученный результат берется в качестве числа α (числа β). Если генерируемые числа α' и β' порядка r^2 принадлежат различным циклическим подгруппам Γ_{p^2}, то и числа α и β также будут принадлежать различным циклическим подгруппам. Вероятность $\Pr(\alpha', \beta' \in \Gamma_{p^2})$, что α' и β' лежат в одной циклической подгруппе, равна отношению количества элементов порядка r^2, лежащих в одной циклической подгруппе, к числу элементов порядка r^2, содержащихся в Z_n^*. Учитывая наличие в Z_n^* примарной подгруппы, порождаемой базисом из двух элементов порядка r^2, и используя формулы [10], выражающие количество элементов заданного порядка в примарных группах, можно получить следующую оценку вероятности:

$$\Pr(\alpha', \beta' \in \Gamma_{p^2}) = \\ = \frac{r(r-1)}{r^2(r^2-1)} \approx \frac{1}{r^2} \approx 2^{-160}.$$

Таким образом, вторая процедура генерации случайных значений α и β является предпочтительной, поскольку дает уменьшение вероятности генерации значений α и β, принадлежащих одной и той же циклической подгруппе, в 2^{80} раз.

Используемая трудная задача

В предлагаемом далее протоколе слепой ЭЦП используется трудность ЗДЛ по модулю трудно разложимого составного числа n. В отличие от криптосхем Фиата—Шамира [11], Рабина [12] и RSA [13], предложенная схема имеет построение, аналогичное построению схем ЭЦП на основе сложности ЗДЛ в конечной группе с многомерной цикличностью [14], и относится к рандомизированным алгоритмам ЭЦП. Возможны следующие два варианта практического использования разработанного протокола. В первом варианте предполагается, что число n является частью открытого ключа и каждый владелец открытого ключа генерирует свое уникальное значение n, а значит, делители этого числа являются секретным ключом. Во втором варианте число n является системным параметром и вырабатывается доверительным центром, который уничтожает секретные делители сразу после генерации n. Во втором варианте открытый ключ является более коротким, однако смена значения n потребует замены всех открытых ключей. Далее будем полагать использование первого варианта, в котором секретным ключом является четверка чисел (p, q, x, w), где x и w — случайные 80-битовые числа ($x < r$, $w < r$). Открытый ключ представляет собой набор значений (n, r, α, β, y), где элемент y вычисляется по формуле

$$y = \alpha^x \beta^w \bmod n.$$

При генерации ЭЦП владелец открытого ключа использует только секретные значения x

и w, поэтому для того, чтобы иметь возможность подделывать подпись за владельца открытого ключа, потенциальному атакующему достаточно вычислить x и w по известному открытому ключу y и основаниям α и β. Данная задача известна как задача дискретного логарифмирования по многомерному основанию [15], в рассматриваемом случае — по двухмерному основанию. Детально ЗДЛ по модулю n рассмотрена в работе [16, с. 54–55], где показано, что данная задача имеет один порядок сложности с задачей факторизации числа n. В частности, при наличии эффективного полиномиального алгоритма вычисления двухмерного логарифма он может быть преобразован в полиномиальный алгоритм факторизации модуля n. Поскольку ЗФ и ЗДЛ по простому модулю являются различными независимыми трудными задачами, то это означает, что логарифмирование по простому модулю и по трудно разложимому модулю являются существенно различными задачами.

Описание протокола слепой подписи

В протоколах слепой подписи предполагается, что лицо, подписывающее некоторое электронное сообщение M, не имеет отношения к формированию M. При этом формирование ЭЦП осуществляется таким способом, что подписывающий 1) не может ознакомиться с сообщением в процессе генерации ЭЦП и 2) впоследствии при получении M и соответствующей этому сообщению ЭЦП не может однозначно идентифицировать пользователя, предоставлявшего данный документ на подпись. Последнее требование известно как требование анонимности (неотслеживаемости). Протоколы слепой ЭЦП реализуются на основе известных алгоритмов ЭЦП, использующих следующие три вычислительно сложные задачи:

1) ЗФ чисел вида $n = qr$, где q и r — два сильных простых числа;

2) ЗДЛ по простому модулю p;

3) ЗДЛ на эллиптической кривой специального вида [16, 17]. Разрабатываемая в данной работе схема слепой ЭЦП основана на трудности ЗДЛ по трудно разложимому модулю.

В основе протокола слепой ЭЦП лежит процедура формирования обычной ЭЦП к сообщению M, которая осуществляется владельцем открытого ключа следующим образом.

Схема базовой ЭЦП.

1. Подписывающий генерирует пару случайных чисел k и t ($1 < k < r$ и $1 < t < r$) и вычисляет значение $R = \alpha^k \beta^t \bmod n$.

2. Подписывающий вычисляет значение $H = F_H(M)$ и значение $E = F_H(R \| M) \bmod r$.

3. Подписывающий вычисляет второй S и третий U элементы ЭЦП по формулам $S = (k + xE) \bmod r$ и $U = (t + wE) \bmod r$.

В результате выполнения данной процедуры генерируется 240-битовая ЭЦП в виде тройки 80-битовых чисел (E, S, U).

Процедура генерации ЭЦП в соответствии с разработанным протоколом слепой 240-битовой подписи включает следующие шаги.

Схема слепой ЭЦП.

1. Подписывающий вырабатывает случайный разовый секретный ключ в виде пары чисел k и t ($1 < k < r$ и $1 < t < r$), по которому вычисляет значение $\overline{R} = \alpha^k \beta^t \bmod n$ и направляет $\overline{R}$ пользователю А, имеющему намерение получить подлинную подпись к сообщению M вслепую.

2. Пользователь А, используя некоторую специфицированную 160-битовую хэш-функцию F_H, вычисляет значение $H = F_H(M)$, где M — документ, который требуется подписать. Затем он генерирует тройку ослепляющих параметров ε, μ и τ, имеющих случайное значение из интервала целых чисел $(1, q)$, и вычисляет значения $R = H\overline{R}^{\varepsilon} y^{\mu} \alpha^{\tau} \bmod n$, $E = F_H(R \| M) \bmod r$ и $\overline{E} = \varepsilon^{-1}(E + \mu) \bmod r$. Если $E = 0$, то повторить шаг 2 при новых случайных значениях ослепляющих параметров. Значение $\overline{E}$ (первый элемент слепой подписи) пользователь А направляет подписывающему. (Значение E является первым элементом ЭЦП к сообщению M.)

3. Подписывающий вычисляет второй $\overline{S}$ и третий $\overline{U}$ элементы слепой подписи по формулам $\overline{S} = (k + x\overline{E}) \bmod r$ и $\overline{U} = (t + w\overline{E}) \bmod r$ и направляет их значения пользователю А.

4. Пользователь А вычисляет второй и третий элементы S и U подлинной подписи (E, S, U) к сообщению M по формулам $S = \varepsilon\overline{S} + \tau \bmod r$ и $U = \varepsilon\overline{U} \bmod r$.

В результате выполнения протокола слепой подписи генерируется 240-битовая ЭЦП в виде тройки 80-битовых чисел (E, S, U). Проверка подлинности ЭЦП не зависит от того, какая схема генерации подписи (обычная или «слепая») была использована для формирования ЭЦП. Это соответствует положению о неразличимости процедуры генерации подлинной ЭЦП. Процедура проверки подлинности ЭЦП включает следующие шаги:

1) вычислить значение $F_H(M) = H$;

2) вычислить значения $\tilde{R} = Hy^{-E} \alpha^S \beta^U \bmod n$ и $\tilde{E} = F_H(\tilde{R} \| M) \bmod r$;

3) сравнить значения $\tilde{E}$ и E. Если $\tilde{E} = E$, то ЭЦП признается подлинной.

Заметим также, что по соотношениям, использованным на шаге 3 протокола слепой ЭЦП, легко видеть, что генерируемая слепая подпись $(\overline{E}, \overline{S}, \overline{U})$ удовлетворяет соотношению

$$\overline{R} = y^{-\overline{E}} \alpha^{\overline{S}} \beta^{\overline{U}} \bmod n .$$

Корректность и анонимность

Корректность функционирования разработанной схемы слепой ЭЦП показывается путем подстановки правильно сформированного значения ЭЦП в процедуру проверки подлинности подписи. Такая подстановка дает следующее:

$$\tilde{R} = Hy^{-E} \alpha^{S} \beta^{U} \bmod n = Hy^{-\varepsilon\overline{E}+\mu} \alpha^{\varepsilon\overline{S}+\tau} \beta^{\varepsilon\overline{U}} \bmod n =$$
$$= Hy^{-\varepsilon\overline{E}} y^{\mu} \alpha^{\varepsilon\overline{S}} \alpha^{\tau} \beta^{\varepsilon\overline{U}} \bmod n =$$
$$= H\left(y^{-\overline{E}} \alpha^{\overline{S}} \beta^{\overline{U}}\right)^{\varepsilon} y^{\mu} \alpha^{\tau} \bmod n =$$
$$= H\overline{R}^{\varepsilon} y^{\mu} \alpha^{\tau} \bmod n =$$
$$= R \Rightarrow \tilde{E} = F(\tilde{R} \| M) = F(R \| M) = E.$$

Поскольку для ЭЦП (E, S, U), сформированной в соответствии с протоколом слепой подписи, на последнем шаге процедуры проверки ЭЦП выполняется условие $\tilde{E} = E$, то подпись (E, S, U) проходит процедуру проверки подлинности. Легко показать, что ЭЦП (E, S, U), сформированная в соответствии с процедурой формирования обычной ЭЦП, также удовлетворяет процедуре проверки подлинности.

Рассматриваемый протокол слепой подписи обеспечивает анонимность пользователя А, если подписывающий формировал слепые подписи ко многим электронным сообщениям и передавал их различным пользователям. Действительно, с подлинной подписью (E, S, U) к некоторому заданному документу M может быть связана любая слепая подпись $(\overline{E}, \overline{S}, \overline{U})$ с помощью значений ослепляющих параметров $\varepsilon = U / \overline{U} \bmod r$, $\tau = S - U\overline{S} / \overline{U} \bmod r$ и $\mu = U\overline{E} / \overline{U} - E \bmod r$. Поскольку значения ослепляющих параметров выбираются по случайному закону, то у подписывающего нет оснований для какого-то предпочтительного предположения по идентификации пользователя, участвовавшего в ходе протокола генерации ЭЦП вслепую, в результате которой была сформирована заданная подпись (E, S, U).

Несмотря на то, что выбор документа, который будет подписан, определяется пользователем А, после формирования слепой ЭЦП он не может сформировать по слепой ЭЦП подлинную подпись к другому документу. На шаге 2 схемы слепой ЭЦП пользователь А должен определиться с выбором подписываемого сообщения. Выбор сообщения фиксируется вычисленным пользователем А значением $\overline{E}$. После передачи значения $\overline{E}$ подписывающему изменение выбора вычислительно неосуществимо.

Заключение

В настоящей работе предложена схема слепой 240-битовой ЭЦП, основанная на ЗДЛ по трудно разложимому модулю. Ввиду сводимости последней задачи к решению ЗФ и ЗДЛ по простому модулю, в определенном смысле можно говорить, что построенная криптосхема основана на трудности ЗФ. Представляет интерес разработка на основе ЗДЛ по трудно разложимому модулю протоколов коллективной ЭЦП по аналогии с построением криптосхем [18–20], а также протоколов слепой коллективной ЭЦП по аналогии с построением протоколов такого типа, описанных в работах [21–23]. Использование предложенного механизма формирования открытого ключа позволит сократить размер подписи в протоколах перечисленных типов, что представляет практический интерес. Детальное рассмотрение синтеза протоколов слепой и слепой коллективной ЭЦП на основе ЗДЛ по трудно разложимому модулю представляет собой предмет отдельного исследования.

В рамках рассмотренных схем ЭЦП любая подпись (E, S, U), полученная по процедуре формирования обычной ЭЦП, может быть интерпретирована как слепая ЭЦП. Действительно, из уравнения проверки ЭЦП $R = Hy^{-E} \alpha^{S} \beta^{U} \bmod n$ следует $\overline{R} = R / H = y^{-E} \alpha^{S} \beta^{U} \bmod n$. Последнее соотношение явно показывает возможность такой интерпретации, ввиду чего любые две подписи можно связать тремя случайными значениями ослепляющих параметров как слепую подпись и полученную по ней подлинную подпись к некоторому сообщению. Этот факт показывает, что формирование большого числа слепых ЭЦП не может быть использовано нарушителем для формирования новой подлинной ЭЦП. Если бы такая возможность существовала, то в силу рассмотренной интерпретации потенциальный нарушитель мог бы сформировать новую подлинную ЭЦП по некоторому числу имеющихся подписей. То есть схема слепой ЭЦП является стойкой, если базовая схема ЭЦП является стойкой. Другими словами, анализ стойкости схемы слепой подписи сводится к анализу стойкости базовой схемы ЭЦП. Детальное рассмотрение этого вопроса представляет самостоятельную задачу.

Работа выполнена в рамках ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (контракт № П635).

Литература

1. **Карякин Ю. Д.** Технология «AXIS-2000» защиты материальных объектов от подделки // Управление защитой информации. 1997. Т. 1. № 2. С. 90–97.
2. **Moldovyan A. A., Moldovyan D. N., Gortinskaya L. V.** Cryptoschemes based on new signature formation mechanism // Computer Science Journal of Moldova. 2006. Vol. 14. N 3(42). P. 397–411.
3. **Moldovyan N. A.** Short Signatures from Difficulty of Factorization Problem // International Journal of Network Security. 2009. Vol. 8. N 1. P. 90–95.
4. **Chaum D.** Blind Signatures for Untraceable Payments. Advances in Cryptology: Proc. of CRYPTO'82. Plenum Press, 1983. P. 199–203.
5. **Camenisch J. L., Piveteau J.-M., Stadler M. A.** Blind Signatures Based on the Discrete Logarithm Problem // Advances in Cryptology — EUROCRYPT'94 Proc. / Lecture Notes in Computer Science. Springer Verlang, 1995. Vol. 950. P. 428–432.
6. **Молдовяну П. А., Молдовян Д. Н., Хо Нгок Зуй.** Конечные группы с четырехмерной цикличностью как примитивы цифровой подписи // Информационно-управляющие системы. 2010. № 3. С. 61–68.
7. **Moldovyan N. A.** Fast Signatures Based on Non-Cyclic Finite Groups // Quasigroups and related systems. 2010. Vol. 18. P. 83–94.
8. **Молдовян Н. А.** Аутентификация информации в АСУ на основе конечных групп с многомерной цикличностью // Автоматика и телемеханика. 2009. № 8. С. 177–190.
9. **Gordon J.** Strong primes are easy to find, Advances in cryptology — EUROCRYPT'84, Springer-Verlag LNCS, 1985. Vol. 209. P. 216–223.
10. **Молдовян Д. Н.** Примитивы схем цифровой подписи: строение мультипликативных конечных групп векторов // Вопросы защиты информации. 2009. № 4. С. 18–24.
11. **Fiat A., Shamir A.** How to prove yourself: Practical solutions to identification and signature problems // Advances in cryptology — CRYPTO'86. Springer-Verlag LNCS, 1987. Vol. 263. P. 186–194.
12. **Rabin M. O.** Digitalized signatures and public key functions as intractable as factorization. — Technical report MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.
13. **Rivest R., Shamir A., Adleman A.** A method for Obtaining Digital Signatures and Public-Key Cryptosystems // Communication of the ACM. 1978. Vol. 21. N 2. P. 120–126.
14. **Молдовяну П. А., Молдовян Д. Н., Дернова Е. С.** Гомоморфизм и многомерная цикличность конечных групп векторов в синтезе алгоритмов ЭЦП // Вопросы защиты информации. 2009. № 3. С. 2–8.
15. **Молдовян Н. А., Молдовяну П. А., Дернова Е. С., Костина А. А.** Гомоморфизм конечных групп векторов малой размерности и синтез схем цифровой подписи // Информационно-управляющие системы. 2009. № 4. С. 26–32.
16. **Молдовян Н. А.** Теоретический минимум и алгоритмы цифровой подписи. — СПб.: БХВ-Петербург, 2010. — 304 с.
17. **Болотов А. А., Гашков С. Б., Фролов А. Б.** Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. — М.: КомКнига, 2006. — 274 с.
18. **Молдовян Д. Н., Дернова Е. С., Сухов Д. К.** Расширение функциональности стандартов электронной цифровой подписи // Информационно-управляющие системы. 2011. № 2. С. 63–67.
19. **Молдовян А. А., Молдовян Н. А.** Коллективная ЭЦП — специальный криптографический протокол на основе новой трудной задачи // Вопросы защиты информации. 2008. № 1. С. 14–18.
20. **Молдовян А. А., Молдовян Н. А.** Новые алгоритмы и протоколы для аутентификации информации в АСУ // Автоматика и телемеханика. 2008. № 7. С. 157–169.
21. **Дернова Е. С., Куприянов И. А., Молдовян Д. Н., Молдовян А. А.** Протоколы слепой подписи с новыми свойствами // Информатизация и связь. 2010. № 1. С. 72–76.
22. **Moldovyan N. A.** Blind Signature Protocols from Digital Signature Standards // Int. Journal of Network Security. 2011. Vol. 13. N 1. P. 22–30.
23. **Moldovyan N. A., Moldovyan A. A.** Blind Collective Signature Protocol Based on Discrete Logarithm Problem // Int. Journal of Network Security. 2010. Vol. 11. N 2. P. 106–113.