

Подпись «вслепую» на эллиптической кривой для электронных денег

Предлагаются протоколы подписи «вслепую» на эллиптической кривой над конечным полем, основанные на протоколах Эль-Гамала, Шнорра, RSA. Протоколы используют существование категорного морфизма для схем подписи Эль-Гамала и Шнорра и гомоморфизма групп для схемы подписи RSA. Проведен оценочный анализ безопасности протоколов с учетом специфики эллиптических кривых.

1. Введение

Подпись «вслепую» (blind signature) используется в протоколах электронных платежей, основанных на использовании электронной монеты (electronic coin) — информации, не имеющей трудно подделываемого физического воплощения в отличие от обычных денег [1, 2]. Подпись «вслепую» выполняется банком для уникального номера монеты, известного только ее владельцу. Таким образом, протокол подписи «вслепую» должен обеспечивать возможность подписи для сообщения, текст которого не известен подписывающему.

Практически, если стоимость монеты не фиксирована, подпись «вслепую» выглядит следующим образом.

1. Пользователь генерирует n случайных номеров монеты m_i , содержащих ее денежное выражение, накладывает на них случайную маску α_i , вычисляя функцию $F(m_i, \alpha_i)$, и посылает в банк. Функция должна быть такой, что по данному значению трудно подобрать пару аргументов (m_i, α_i) и трудно вычислить коллизию, т. е. найти две пары аргументов, дающих одно значение функции.
2. Банк выбирает наугад $n - 1$ замаскированных монет и просит раскрыть их аргументы.
3. Пользователь раскрывает значения (m_i, α_i) для каждой из $n - 1$ выбранных монет.
4. Банк убеждается, что все они имеют одинаковое денежное значение, например, 100 рублей. Если число n достаточно велико, то банк может быть убежден с достаточной вероятностью, что и оставшаяся монета тоже имеет достоинство в 100 рублей.
5. Банк генерирует подпись s для оставшейся нераскрытой монеты и отправляет пользователю.
6. Пользователь проверяет, что замаскированная монета подписана банком правильно. Затем он снимает с монеты маску, вычисляя функцию $G(s, \alpha_i)$ так, что подпись остается верной и для открытого номера монеты.

В случае монет фиксированной стоимости первые четыре этапа не нужны. Отличие подписи «вслепую» от обычной цифровой подписи состоит в возможности вычисления маски и ее последующего снятия так, что подпись остается верной. Кроме того, наложение и снятие маски должно выполняться без знания ключа подписи. Снятие маски должно исключать возможность изменения сообщения. Таким образом, необходима вычислимость функций F и G в одну сторону.

Таким образом, для подписи «вслепую» требуется наличие вычислимых функций F_i , G_i таких, что для операции подписи S оказывается справедливым выражение $G_i S F_i(m) = S(m)$ или $G_i S F_i = S$. Это свойство можно интерпретировать как существование вычислимого гомоморфизма схемы подписи, не требующего знания ключа. Известно [3], что популярные протоколы подписи (RSA, Эль-Гамала), не использующие хэш-функцию, обладают гомоморфизмами. Эти гомоморфизмы являются категорными морфизмами. Здесь объектами категории являются пары сообщение/подпись, выдерживающие проверку. Морфизмами категории являются вычисляемые отображения одной пары в другую.

Существование вычислимых гомоморфизмов позволяет на основе одной правильной пары сообщение/подпись создавать множество других формально правильных пар для (возможно, бессмысленных) сообщений. Однако, если тексты лишены избыточности, то все сообщения являются осмысленными. Подпись «вслепую» использует такие гомоморфизмы во благо.

На безопасность протоколов «вслепую» влияет то обстоятельство, что в создании подписи участвуют две стороны, которые не могут абсолютно доверять друг другу. В частности, пользователь может предлагать такие сообщения, которые позволят вскрыть ключ (атака на основе подобранных сообщений и адаптивно подобранных сообщений). С другой стороны, банк может быть заинтересован в раскрытии замаскированного сообщения пользователя.

Известны протоколы подписи «вслепую» на основе группы вычислимого и трудно вычислимого порядка [1, 2]. Эллиптические кривые позволяют реализовать подпись для обоих вариантов групп.

Эллиптическая кривая $E(\mathbf{F}_q)$ над конечным полем \mathbf{F}_q , $q = p^m$, характеристики $p > 3$ представляет собой множество решений уравнения

$$y^2 = x^3 + Ax + B,$$

дополненное точкой «бесконечность». При этом кривая не должна иметь особых точек, т. е. удовлетворять условию $4A^3 + 27B^2 \neq 0$. Точки кривой образуют абелеву группу по сложению. Закон сложения точек описан во многих книгах, например в [3]. Для данного уравнения кривой над полем \mathbf{F}_q число точек может быть вычислено алгоритмом Чуфа с полиномиальной сложностью.

Повторное использование монеты исключается тем, что при погашении банк запоминает персональный номер монеты. Однако защита от повторного использования предполагает также распознавание виновника повторного использования. В этом случае номер монеты должен содержать разовый открытый ключ подписи пользователя. Протокол покупки должен включать в себя процедуру доказательства того, что покупатель знает секретный ключ, парный к открытому ключу в номере монеты. В этом случае при погашении монеты продавец предъявляет в банк запись протокола покупки, включая указанное доказательство. Если доказательство повторное, то обманывает продавец, в противном случае обманывает покупатель.

2. Группа вычислимого порядка

В основу протокола положена задача логарифмирования в группе точек эллиптической кривой: для данных точек P, Q эллиптической кривой найти показатель l такой, что $P = lQ$. Очевидно, что для этого точки должны лежать в одной циклической группе. Если порядок группы точек свободен от квадратов, то группа является циклической. Для того, чтобы задача логарифмирования на кривой была сложной, необходимо, чтобы порядок группы был простым или имел большой простой делитель p' . Кроме того, требуется, чтобы $p \neq p'$ и чтобы число p' не делило бы ни один из порядков мультипликативных групп для нескольких последовательных расширений поля \mathbb{F}_q степени не более 20. Тогда сложность логарифмирования имеет оценку $O(\sqrt{p'})$ (единица измерения — сложность сложения точек на эллиптической кривой).

2.1. Подпись «вслепую» на основе протокола Эль-Гамала

Этот протокол требует диалога, который позволяет придать гомоморфизму подписи требуемые свойства. Открытым ключом банка является уравнение эллиптической кривой, образующая точка Q , точка P , простой порядок группы p' . Оба участника протокола умеют вычислять хэш-функцию h .

Секретным ключом банка является показатель l такой, что $P = lQ$. Подпись вырабатывается для сообщения m , $0 < m < p'$.

Протокол Эль-Гамала для обычной подписи на эллиптической кривой заключается в следующем. Подписывающий вырабатывает случайный показатель k , вычисляет точку $R = kQ$ и решает относительно s сравнение по модулю порядка группы $m = lh(R) + ks$. Подписью является пара (R, s) . Для проверки подписи следует проверить равенство $mQ = h(R)P + sR$. Тогда, используя гомоморфизм схемы подписи, можно сконструировать другое правильно подписанное сообщение следующим образом.

1. Выбрать произвольный показатель α , положить $k' = \alpha k$ (поскольку k неизвестно, то и k' тоже неизвестно). Этому показателю будет соответствовать точка $R' = \alpha k Q = \alpha R$.
2. Вычислить показатель $\beta = h(R')h(R)^{-1}$ по модулю порядка группы.
3. Вычислить новое сообщение и подпись $m' = \beta m$, $s' = \alpha^{-1}\beta s$.

Здесь существует односторонняя вычислимость коэффициента β из показателя α и, следовательно, односторонняя вычислимость нового сообщения m' из сообщения m . Это можно рассматривать как маску, накладываемую на сообщение. Однако маска накладывается банком, тогда как для подписи «вслепую» требуется, чтобы маска накладывалась пользователем. Для получения возможности подписи «вслепую» изменим протокол Эль-Гамала следующим образом.

1. Банк выбирает случайный показатель \bar{k} , $0 < \bar{k} < p'$, вычисляет точку $\bar{R} = \bar{k}Q$, проверяет, что $h(\bar{R}) \neq 0$, и посылает точку \bar{R} пользователю. Если $h(\bar{R}) = 0$, то заменяется случайный показатель.
2. Пользователь проверяет, что точка \bar{R} лежит на кривой, выбирает случайный показатель α , $0 < \alpha < p'$, вычисляет точку $R = \alpha\bar{R}$, проверяет, что $h(R) \neq 0$ (в противном случае нужно повторить п. 2), вычисляет коэффициент $\beta \equiv \frac{h(R)}{h(\bar{R})} \pmod{p'}$, вычисляет замаскированное сообщение $\bar{m} \equiv \alpha\beta^{-1}m \pmod{p'}$ для открытого сообщения m и посылает \bar{m} банку. Если точка \bar{R} не лежит на кривой, то это может быть расценено как попытка банка узнать некоторую информацию о содержании сообщения m .
3. Банк проверяет, что $\bar{m} \neq 0$, вычисляет подпись

$$\bar{s} \equiv l \cdot h(\bar{R}) + \bar{k} \cdot \bar{m} \pmod{p'}$$

для сообщения под маской и посылает ее пользователю. Если $\bar{m} = 0$, то создание подписи немедленно ведет к раскрытию ключа, в этом случае протокол прерывается.

4. Пользователь проверяет выполнение равенства $\bar{s}Q = h(\bar{R})P + \bar{m}\bar{R}$ для сообщения под маской. Если равенство выполняется, то подпись верна. Затем пользователь снимает маску, вычисляя подпись для исходного сообщения: $s \equiv \bar{s}\beta \pmod{p'}$. Подписанное сообщение, как и в оригинальном протоколе Эль-Гамала, представляет собой тройку (m, R, s) .

Проверка подписи проводится следующим образом.

1. Для точки R вычисляется хэш-функция. Если $h(R) = 0$ или $m = 0$, то подпись считается недействительной.
2. Если $h(R) \neq 0$, $m \neq 0$, то проверяется выполнение равенства $sQ = h(R)P + mR$. Если равенство выполняется, то подпись верна.

Покажем действие протокола на примере одного из n подготовленных пользователем сообщений. Для подписи «вслепую» сообщения m , $0 < m < p'$, пользователь и банк выполняют п. 1 и 2 протокола. Затем банк просит раскрыть содержание сообщения под маской \bar{m} или подписывает это сообщение. В первом случае пользователь предъявляет показатель α . Банк проверяет выполнение условия $\bar{m} \neq 0$, и если оно выполняется, то вычисляет точку $\alpha\bar{R}$, вычисляет коэффициент β , вычисляет значение m . Если $\bar{m} = 0$, то пользователь нарушает протокол и пытается раскрыть ключ подписи банка. Во втором случае выполняются п. 3, 4 протокола.

Поскольку отечественный стандарт подписи ГОСТ Р34.10–94 построен на основе протокола Эль-Гамала, подпись «вслепую» очевидным образом может быть адаптирована и к стандарту подписи.

Рассмотрим кратко безопасность этого протокола. В этом протоколе может быть несколько направлений атак. Во-первых, это раскрытие ключа подписи. Во-вторых, подделка подписи без раскрытия ключа, например, подменой сообщения. В-третьих, это раскрытие подлинного текста сообщения (такая атака может быть предпринята со стороны банка).

В основу безопасности протокола положена задача логарифмирования в группе точек кривой. Для раскрытия ключа подписи банка достаточно найти логарифм l . Однако могут быть предприняты и другие варианты атаки. Например, использование банком дважды одного и того же показателя \bar{k} или использование хоть однажды предсказуемого показателя \bar{k} позволяет раскрыть ключ подписи решением линейных сравнений. При этом введение в состав k неповторяющегося порядкового номера или времени приводит к уменьшению допустимого количества подписей на одном ключе. Таким образом, к генератору случайного числа предъявляются требования столь же жесткие, как и к генератору ключей. Если $h(\bar{R}) = 0$, то подпись не зависит от ключа l . В этом случае пользователю достаточно было бы найти точку, которая дает нулевое значение хэш-функции.

Подделка подписи без знания ключа, в отличие от протокола, основанного на логарифмировании в конечном поле, представляется не менее сложной, чем логарифмирование в группе точек эллиптической кривой при условии, что ключ выбран правильно. Неправильный выбор ключа (например, использование не поля из q элементов, а кольца с делителями нуля из q элементов, использование группы составного порядка p' и т. п.) может быть легко выявлен с помощью известных тестов проверки на простоту. Варианты нарушения протокола, связанные с тем, что точка \bar{R} может не лежать на кривой, выявляются в ходе протокола. Возможны атаки, связанные с неправильным выбором точки R , например, так, что она не лежит в группе $\langle Q \rangle$. Если число точек на кривой равно $N = p't$, то для исключения такой атаки следует проверить, что $tR \neq P_\infty$ и $t\bar{R} \neq P_\infty$.

Изменение значения подписанного сообщения под маской может быть предпринято пользователем на основе указанного гомоморфизма подписи. Этот недостаток неустраим, так как наличие гомоморфизма — основа подписи «вслепую». Поэтому индивидуальный номер монеты должен содержать достаточно большой избыточный отрезок, априорно известный магазину и банку. Если сложность подмены положить равной сложности раскрытия ключа, то длина избыточного отрезка должна быть равна $\frac{\log_2 p'}{2}$. Избыточность может быть введена, например, заменой сообщения m на конкатенацию $m||g(m)$ с соответствующим сокращением длины m для некоторой хэш-функции g , стойкой в части обращения и в части вычисления коллизий.

2.2. Подпись «вслепую» на основе протокола Шнорра

Открытый ключ подписи содержит уравнение эллиптической кривой $E(\mathbb{F}_q)$, образующую точку Q , точку P и порядок группы p' . Секретный ключ содержит показатель l такой, что $P = lQ$.

Для подписи «вслепую» сообщения m участники протокола действуют следующим образом.

1. Банк генерирует случайное число \bar{k} , $0 < \bar{k} < p'$, вычисляет точку $\bar{R} = \bar{k}Q$ такую, что $h(\bar{R}) \neq 0$, и посылает эту точку пользователю.
2. Пользователь генерирует случайное число α , $0 < \alpha < p'$, и «полагает» $k \equiv \alpha\bar{k} \pmod{p'}$. Затем он вычисляет точку $R = \alpha\bar{R}$, проверяет, что $h(R) \neq 0$. В противном случае генерируется другое число α . Пользователь вычисляет коэффициент $\beta \equiv \frac{h(R)}{h(\bar{R})} \pmod{p'}$, вычисляет сообщение по маской $\bar{m} \equiv \alpha^{-1}\beta m \pmod{p'}$ и посылает это сообщение банку.
3. Банк вычисляет подпись для сообщения под маской:

$$\bar{s} \equiv \bar{k} + l\bar{m}h(\bar{R}) \pmod{p'}$$

и посылает ее пользователю.

4. Пользователь проверяет правильность подписи: если выполняется равенство $\bar{s}Q = \bar{R} + \bar{m}h(\bar{R})P$. Затем он снимает маску с подписи и вычисляет $s \equiv \alpha\bar{s} \pmod{p'}$. Подписанное сообщение представляет собой тройку (m, s, R) .

Для проверки подписи достаточно проверить равенство $sQ = R + mh(R)P$. При этом должно выполняться неравенство $h(R) \neq 0$. Если равенство выполняется, то подпись верна.

В основу безопасности этого протокола также положена задача логарифмирования в группе точек кривой. Для раскрытия ключа подписи банка достаточно найти логарифм l . Здесь также использование банком дважды одного и того же показателя \bar{k} (или использование хоть однажды предсказуемого показателя \bar{k}) позволяет раскрыть ключ подписи решением системы из двух линейных сравнений.

Подделка подписи без знания ключа требует вычисления точки, координаты которой находятся в требуемом соотношении с ее логарифмом. Эта задача представляется такой же сложной, как логарифмирование.

Для того, чтобы защититься от подмены сообщения, в него следует внести избыточность, как и в протоколе Эль-Гамала.

3. Подпись «вслепую» на основе группы трудно вычислимого порядка

Этот протокол подписи аналогичен известному протоколу подписи «вслепую» Шаума [2] и основан на том, что функция шифрования RSA является мультипликативной, то есть если s_1, s_2 — подписи для сообщений m_1, m_2 , то $s_1 s_2$ — подпись для $m_1 m_2$. Если S — функция, вычисляющая подпись s для сообщения m , и множество подписей совпадает с множеством сообщений, то S является эндоморфизмом группы $(\mathbf{Z}/n\mathbf{Z})^*$.

Открытый ключ представляет собой эллиптическую кривую $E(\mathbf{Z}/n\mathbf{Z})$ над кольцом классов вычетов по модулю где $n = pq$, и p, q — различные простые числа, $\#E(\mathbf{Z}/n\mathbf{Z}) = N$. Кроме того, открытый ключ содержит показатель e , обратимый по модулю N . Секретный ключ содержит показатель d такой, что $ed \equiv 1 \pmod{N}$. Сообщение M представлено точкой кривой.

По китайской теореме об остатках кривая E изоморфна прямой сумме $E(\mathbf{Z}/n\mathbf{Z}) \cong E(\mathbf{F}_p) \oplus E(\mathbf{F}_q)$, следовательно, число N не может быть простым. Кольцо $\mathbf{Z}/n\mathbf{Z}$ имеет делители нуля, поэтому точки кривой $E(\mathbf{Z}/n\mathbf{Z})$ не образуют группу относительно обычной операции сложения точек. Это обусловлено тем, что каждая точка кривой $E(\mathbf{Z}/n\mathbf{Z})$ имеет две составляющих — по модулю p и по модулю q . Поэтому, если две точки кривой $E(\mathbf{Z}/n\mathbf{Z})$ S и T имеют составляющие S_p, S_q и T_p, T_q , и $S_p = T_p, S_q \neq T_q$, то по модулю p нужно применять формулы для удвоения, а по модулю q — формулы для сложения разных точек. Поэтому существующие формулы сложения могут давать ошибку. Однако вероятность такого события при сложении двух точек пренебрежимо мала и имеет порядок $O\left(\frac{1}{\min(p, q)}\right)$.

Порядки групп $E(\mathbf{F}_p)$ и $E(\mathbf{F}_q)$ должны иметь большие простые делители. Подпись RSA на эллиптической кривой является автоморфизмом группы $E(\mathbf{Z}/N\mathbf{Z})$. Подпись «вслепую» использует это свойство.

Протокол предусматривает следующие действия.

1. Пользователь генерирует случайную точку кривой R , вычисляет для сообщения $M \in E(\mathbf{Z}/n\mathbf{Z})$ точку $\bar{M} = M + eR$ и посылает банку.
2. Банк вычисляет подпись для точки \bar{M} : $\bar{S} = d\bar{M} = d(M + eR) = dM + R$.
3. Пользователь проверяет правильность подписи (если $\bar{M} = e\bar{S}$, то подпись верна) и снимает маску с подписи, вычисляя $S = \bar{S} - R = dM$.

Подписью для точки M является точка S . Проверка подписи выполняется вычислением eS и сравнением с точкой M . В случае равенства подпись верна.

Для снятия маски с сообщения \bar{M} предъявляется точка R .

Безопасность протокола в части раскрытия ключа подписи основана на сложности разложения составного числа n и на сложности нахождения порядка группы N . Поэтому размер задачи в этом случае оказывается в несколько раз больше, чем, например, в протоколе Эль-Гамала. Следовательно, использование эллиптических кривых в таком протоколе приводит к снижению скорости вычислений в десятки раз по сравнению с протоколом, использующим группу вычислимого порядка.

В силу гомоморфизма схемы подписи теоретически возможна подмена пользователем подписанного персонального номера монеты (например, на больший номинал). Использование вместо M обычной хэш-функции, стойкой в части вычисления коллизий и в части обращения, устранит указанный гомоморфизм, и сделает невозможным подписи «вслепую». Действительно, замена сообщения m на значение хэш-функции $h(m)$ в уравнении шифрования приведет к тому, что снятие маски станет невозможным.

Для исключения этого можно, например, ввести избыточность в текст сообщения. Отметим, что в случае обычной подписи RSA недопустимо вводить избыточность путем использования нулевых младших или старших разрядов. В первом случае это можно обойти, используя гомоморфное вложение кольца $\mathbf{Z}/n\mathbf{Z}$ в кольцо \mathbf{Z} . Во втором случае указанный обход основан на гомоморфном вложении $\mathbf{Z}/n\mathbf{Z}$ в кольцо целых алгебраического расширения поля рациональных чисел и на использовании алгоритма LLL для минимизации базиса решетки. Однако в случае эллиптических кривых этот недостаток исключен.

Литература

1. A. Menezes, P. van Oorschot, S. Vanstone. Handbook of applied cryptography. — CRC press, 1997.
2. B. Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C, second edition. — J. Wiley & Sons, New York, 1996.
3. А. Г. Ростовцев, В. А. Матвеев. Элементы криптологии. Под ред. П. Д. Зегжды. Изд-во СПбГТУ, 1993.