2. Схемы цифровой подписи

*Схемы цифровой подписи на основе симметричных и асимметричных криптосистем. Код аутентификации сообщения. Схемы Эль-Гамаля, Фиата-Фейга-Шамира. ЭЦП на эллиптических кривых.*

*Стандарты США, России и Республики Беларусь электронной цифровой подписи.*

*Одноразовые подписи. Слепые ЭЦП. Схема электронной подписи с доказуемостью подделки. Схема конфиденциальной электронной цифровой подписи*

Электронная подпись (ЭП), электронная цифровая подпись (ЭЦП), цифровая подпись (ЦП) — реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого (секретного) ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

Определение электронного документа, электронной цифровой подписи и порядка их обращения и генерирования на территории РБ даны в Законе РБ *«Об электронном документе и электронной цифровой подписи»* от 28 декабря 2009 г. № 113-З:

**электронный документ** – документ в электронном виде с реквизитами, позволяющими установить его целостность и подлинность;

**электронная цифровая подпись** – последовательность символов, являющаяся реквизитом электронного документа и предназначенная для подтверждения его целостности и подлинности;

**сертификат открытого ключа** – электронный документ, изданный поставщиком услуг и содержащий информацию, подтверждающую принадлежность указанного в нем открытого ключа определенным организациям или физическому лицу;

**средство электронной цифровой подписи** – программное, программно-техническое или техническое средство, с помощью которого реализуются одна или несколько из следующих функций: выработка электронной цифровой подписи, проверка электронной цифровой подписи, выработка личного ключа или открытого ключа;

**карточка открытого ключа проверки электронной цифровой подписи (далее – карточка открытого ключа) – документ на бумажном носителе, содержащий значение открытого ключа проверки электронной цифровой подписи (далее – открытый ключ), информацию, подтверждающую его принадлежность определенным организации или гражданину.**

Строго говоря для контроля целостности данных можно использовать:

‑ сравнение нескольких копий сообщения;

‑ контрольные суммы сообщений;

‑ значение хеш-функций от сообщений;

‑ имитовставки или коды аутентификации сообщений (Message Authentication Codes – MAC);

‑ ЭЦП.

Для проверки подлинности сообщений, как правило, используют коды аутентификации сообщений (Message Authentication Codes ‑ MAC) либо электронную цифровую подпись. Целесообразность применения одного из двух механизмов определяется требованием обеспечения в конкретном приложении невозможности отказа от сообщений (или отсутствием этого требования). Невозможность отказа может быть обеспечена только асимметричными криптосхемами, т.е. в данном случае схемами цифровой подписи, так как в любой схеме цифровой подписи секретные ключи подписи имеют только одного владельца. Следовательно, при возникновении спора о факте создания какого-либо документа, заверенного цифровой подписью, его автора всегда можно установить однозначно. Симметричные криптосхемы сделать этого не позволяют, так как в них используются ключи, которые являются общими секретами как минимум для двух, а то и более участников криптосистемы. Следовательно, однозначно установить единственное лицо, применившее секретный ключ для выполнения криптографического преобразования, не представляется возможным.

Традиционно известны два метода обеспечения подлинности данных в электронных каналах связи: вычисление значения хеш-функции с ключом и использование блочных шифров в режимах работы, обеспечивающих аутентификацию сообщений (режим выработки имитовставки). Независимо от способа, результат вычисления прикрепляется отправителем к сообщению, а получатель самостоятельно тем же способом пересчитывает хеш-код (проверяет имитовставку) полученного им сообщения и сверяет его с тем, которое прикреплено к сообщению. При положительном результате проверки источник сообщения считается аутентичным, так как верно сгенерировать хеш-код могло только то лицо, которое знает общий с получателем секретный ключ.

Существует две группы схем построения ЭЦП:

1. На основе алгоритмов симметричного шифрования. Данная схема предусматривает наличие в системе третьего лица — арбитра, пользующегося доверием обеих сторон. Авторизацией документа является сам факт шифрования его секретным ключом и передача его арбитру.

2. На основе алгоритмов асимметричного шифрования. Такие схемы ЭЦП наиболее распространены.

Кроме этого, существуют другие разновидности цифровых подписей (групповая подпись, неоспоримая подпись, доверенная подпись), которые являются модификациями описанных выше схем.

Поскольку подписываемые документы — переменного (и как правило достаточно большого) объёма, в схемах ЭП зачастую подпись ставится не на сам документ, а на его хэш. Для вычисления хэша используются криптографические хэш-функции, что гарантирует выявление изменений документа при проверке подписи. Хэш-функции не являются частью алгоритма ЭП, поэтому в схеме может быть использована любая надёжная хэш-функция.

Использование хэш-функций даёт следующие преимущества:

1. Вычислительная сложность. Обычно результат от вычисление хэш-функции цифрового документа во много раз меньшего объёма, чем объём исходного документа, и алгоритмы вычисления хэша являются более быстрыми, чем алгоритмы ЭЦП. Поэтому формировать хэш документа и подписывать его получается намного быстрее, чем подписывать сам документ.

2. Совместимость. Большинство алгоритмов оперирует со строками бит данных, но некоторые используют другие представления. Хэш-функцию можно использовать для преобразования произвольного входного текста в подходящий формат.

3. Целостность. Без использования хэш-функции большой электронный документ в некоторых схемах нужно разделять на достаточно малые блоки для применения ЭЦП. При верификации невозможно определить, все ли блоки получены и в правильном ли они порядке.

Использование хэш-функции не обязательно при электронной подписи, а сама функция не является частью алгоритма ЭЦП, поэтому хэш-функция может использоваться любая или не использоваться вообще.

Симметричные схемы ЭП менее распространены, чем асимметричные, так как не удалось реализовать эффективные алгоритмы подписи, основанные на симметричных шифрах. Симметричные схемы цифровой подписи опираются на гипотезу о вычислительной сложности некоторых математических задач, поэтому невозможно определить, могут ли эти схемы быть скомпрометированы в ближайшее время.

Симметричные схемы ЭЦП имеют следующие преимущества:

1. Стойкость симметричных схем ЭЦП вытекает из стойкости используемых блочных шифров, надежность которых также хорошо изучена.

2. Если стойкость шифра окажется недостаточной, его легко можно будет заменить на более стойкий с минимальными изменениями в реализации.

Однако у симметричных ЭЦП есть и ряд недостатков:

1. Нужно подписывать отдельно каждый бит передаваемой информации, что приводит к значительному увеличению подписи. Подпись может превосходить сообщение по размеру на два порядка.

2. Сгенерированные для подписи ключи могут быть использованы только один раз, так как после подписывания раскрывается половина секретного ключа.

Одной из самых распространенных схем ЭЦП является схема Эль-Гамаля (1984 г.), которая является криптосхемой с открытым ключом, криптостойкость которой основана на вычислительной сложности проблемы дискретного логарифмирования, где по известным p, g и y требуется вычислить x, удовлетворяющий сравнению:

y ≡ gx mod p.

Параметры:

m – сообщение;

p – большое простое число;

g – порождающий элемент группы Z p\* ;

k ∈ Z\*p - случайное число;

d = gk mod p - вычисление открытого ключа;

h = h(m) – значение хэш-функции от текста;

Ключ подписания: (k).

Ключ верификации: (p, g, d).

Подписание:

a – случайное число, (a, p-1) = 1;

s = ga mod p;

r = (h - sk)a-1mod (p - 1);

Подпись: (m; s, r).

Верификация:

Проверить сравнение dssr ≡ gh mod p. Если сравнение верно, то подпись принимается, иначе – отвергается.

Схема Эль-Гамаля может быть использована как для шифрования, так и для построения цифровых подписей. Существует большое количество алгоритмов, основанных на схеме Эль-Гамаля: это алгоритмы DSA, ECDSA, KCDSA, схема Шнорра.

Проблема схемы цифровой подписи Эль-Гамаля в том, что p должно быть очень большим, не менее 1024 бит, чтобы сделать трудной проблему дискретного логарифмирования.

Схема ЭЦП Фейга-Фиата-Шамира относится к схемам с нулевым разглашением и является вариантом реализации протокол Фейга — Фиата — Шамира. Получатель генерирует случайные значения ei, для чегоиспользует секретную функцию h.

Параметры

m – сообщение;

Генерация подписи:

r ‑ случайное число, такое что 1 ≤ r ≤ n - 1;

x = r2 mod n;

ei =h(x||m), 1 ≤ i ≤ k;

;

Подпись: (m, ei, …, ek, y).

Верификация

Вычислить: ;

Вычислить: e′i =h(x′||m), 1 ≤ i ≤ k;

Если вычисленные значения (e'1, …, e'k) совпадают с полученными (e1, …, ek), то подпись m подтверждена.

DSA (Digital Signature Algorithm) ‑ криптографический алгоритм с использованием открытого ключа для создания электронной подписи. Алгоритм предложег Национальным институтом стандартов и технологий (США) и основан на вычислительной сложности взятия логарифмов в конечных полях. DSA является частью DSS (Digital Signature Standard ‑ стандарт цифровой подписи), впервые опубликованного в 1998 г. (FIPS-186). Стандарт несколько раз обновлялся, последняя версия ‑ FIPS-186-4 (2013 г.). Стандарт определяет использование алгоритма SHA-1 вычисления значений хеш-функций.

Параметры:

p – простое число L битов, где L принимает значение кратное 64 в диапазоне от 512 до 1024;

q – 160 – битовый множитель p – 1;

a = g(p-1)/q mod p, где g < p – 1, для которого g(p-1)/q mod p > 1 ;

y = ax mod p, где x < q;

m – текст.

Ключ подписания: (y, p, q, a).

Ключ верификации: (x).

Подписание:

k – случайное число, k < q;

r = (ak mod p) mod q – вычисление первой части подписи;

s = (k-1(H(m) + xr)) mod q – вычисление второй части подписи.

Подпись: (r , s).

Верификация:

w = s-1 mod q;

u1 = (H(m)⋅w) mod q;

u2 = (rw) mod q;

, если v = r – то подпись подлинная.

Достоинством схем ЭЦП на эллиптических кривых перед «классическими» (RSA, Эль Гамаля, Диффи-Хеллмана, DSA) является использование меньших размеров ключей при одинаковой криптостойкости, что снижает требования к вычислительной мощности оборудования и увеличивает скорость выполнения операций шифрования‑дешифрования.

ECDSA (Elliptic Curve Digital Signature Algorithm) — алгоритм с открытым ключом для создания цифровой подписи, аналогичный по своему строению DSA, но определённый, в отличие от него, не над кольцом целых чисел, а в группе точек эллиптической кривой.

Параметры

q ‑ порядок одной из циклических подгрупп группы точек эллиптической кривой, большое простое число. Если размерность этого числа в битах меньше размерности в битах значений хэш-функции H(x), то используются только левые биты значения хэш-функции;

p ‑ характеристика поля координат Fp, простое число;

P ‑ точка простого порядка q кривой E(Fp);

x ‑ случайное или псевдослучайное целое число x из интервала [1, q-1];

Q = x⋅P.

Открытым ключом отправителя является точка Q, а закрытым ‑ x.

Для того, чтобы подписать какое-либо сообщение, для которого подсчитано значение h хэш-функции H, отправитель должен сделать следующее:

Выбрать случайное целое число k € [1,q-1].

Вычислить k⋅p= (x1, y1) и принять r = x1 mod q, где r получается из целого числа x1 между 0 и (p - 1), приведенным по модулю q. При этом, если r = 0, то уравнение подписи s = k-1 (h + x⋅r) mod q не зависит от секретного ключа x, и следовательно, (r,s) не подходит в качестве цифровой подписи. Значит, в случае r=0 необходимо вернуться к шагу 1.

Вычислить k-1 mod q и положить s=k-1 (h + x⋅r) mod q, где h ‑ значение хеш-функции подписываемого сообщения. Если s=0, то значение s-1 mod q, нужное для проверки, не существует. Значит, в случае s=0 необходимо вернуться к шагу 1.

Подписью для сообщения является пара целых чисел (r, s).

Верификация ЭЦП:

Получить подтвержденную копию открытого ключа Q отправителя

Проверить, что числа r и s являются целыми числами из интервала [1, q-1], и вычислить значение хеш-функции h от сообщения;

Вычислить u1 = s-1 h mod q и u2 = s-1 r mod q;

Вычислить u1⋅P + u2⋅Q = (x0, y0), и относительно x0, как целого числа между 0 и (p - 1), положить v=x0 mod q;

Принять подпись, тогда и только тогда, когда v = r.

Для подтверждения публичного ключа Q необходимо

Проверить, что Q ≠ O, где O – бесконечно удаленная точка и координаты верны;

Проверить, что Q лежит на кривой;

Проверить, что qQ = O;

Ниже в таблице 2.1 приведено сравнение основных характеристик наиболее распространенных схем ЭЦП.

Таблица 2.1 – Сравнение современных схем ЭЦП

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Алгоритм | Ключ | Назначение | Криптостойкость, MIPS | Примечания |
| [RSA](https://ru.wikipedia.org/wiki/RSA) | До 4096 бит | Шифрование и подпись | 2,7•1028 для ключа 1300 бит | Основан на трудности задачи [факторизации больших чисел](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%BA%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D1%86%D0%B5%D0%BB%D1%8B%D1%85_%D1%87%D0%B8%D1%81%D0%B5%D0%BB); один из первых асимметричных алгоритмов. Включен во многие стандарты |
| ElGamal | До 4096 бит | Шифрование и подпись | При одинаковой длине ключа криптостойкость равная RSA, т.е. 2,7•1028 для ключа 1300 бит | Основан на трудной задаче вычисления дискретных логарифмов в конечном поле; позволяет быстро генерировать ключи без снижения стойкости. Используется в алгоритме цифровой подписи DSA-стандарта DSS |
| [DSA](https://ru.wikipedia.org/wiki/DSA) | До 1024 бит | Только подпись |  | Основан на трудности задачи [дискретного логарифмирования](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D1%81%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D1%8B%D0%B9_%D0%BB%D0%BE%D0%B3%D0%B0%D1%80%D0%B8%D1%84%D0%BC) в [конечном поле](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D0%B5%D1%87%D0%BD%D0%BE%D0%B5_%D0%BF%D0%BE%D0%BB%D0%B5); принят в качестве гос. стандарта США; применяется для секретных и несекретных коммуникаций; разработчиком является АНБ. |
| [ECDSA](https://ru.wikipedia.org/wiki/ECDSA) | До 4096 бит | Шифрование и подпись | Криптостойкость и скорость работы выше, чем у RSA | Современное направление. Разрабатывается многими ведущими математиками |

ГОСТ Р 34.10-2012 (полное название: «ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи») — российский стандарт, описывающий алгоритмы формирования и проверки электронной цифровой подписи. ГОСТ Р 34.10-2012 основан на эллиптических кривых. Стойкость этих алгоритмов основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также на стойкости хэш-функции. Для ГОСТ Р 34.10-2012 используется хэш-функция по ГОСТ Р 34.11-2012.

СТБ 34.101.45-2013 (полное название «СТБ 34.101.45-2013. Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых») также основан на эллиптических кривых.

Традиционные системы электронной подписи, которые используются в практике уязвимы к атакам квантовых компьютеров. Одним из решений проблемы является использование одноразовых схем ЭЦП, которые действительны только для одного сообщения.

Подпись Лэмпорта относится к одноразовым ЭЦП. Выработка ЭЦП строится на использовании однонаправленных функций хеширования и генераторов псевдослучайных чисел. Работу схемы рассмотрим на примере 256 битной функции хеширования.

Генерация ключей:

секретный ключ отправителя – сгенерованные на генераторе псевдослучайных чисел 256 пар 256-битных чисел;

открытый ключ – 521 256-битных хешей от каждого из чисел открытого ключа.

Подпись сообщений:

получается 256-битный хеш от сообщения;

в соответствие каждому биту в хеше берется соответствущее случайное число в секретном ключе («0» ‑ первое число, «1» ‑ второе число из соответствующей пары в секретном ключе);

Подпись – это 256 случайных числе по 256 бит каждое. При этом секретный ключ не должен повторно использоваться или публиковаться.

Проверка подписи:

вычисляется 256-битный хеш от полученного сообщения;

для каждого бита в хеше выбирается соответствующее число в открытом ключе (если бит равен «0», то первое число в открытом ключе, если «1», то второе число в открытом ключе);

хешируется каждое из 256 чисел полученной подписи в 256-битный хеш;

если вычисленные 256 хешей из пункта выше соответствуют полученным из открытого ключа числам, то подпись подтверждена.

Слепая подпись (blind signature) ‑ разновидность ЭЦП, особенностью которой является то, что подписывающая сторона не может точно знать содержимое подписываемого документа.

Существует две разновидности слепой подписи – полностью слепая подпись и слепая подпись.

В схеме полностью слепой подписи Алиса хочет, чтобы Боб вслепую подписал сообщение m. Для этого:

1. Алиса зашифровывает сообщение m функцией f, получая зашифрованное сообщение c = f(m).

2. Алиса отсылает зашифрованное сообщение Бобу.

3.Боб вслепую (так как не знает, что находится внутри) подписывает сообщение c функцией g, получая c' =g(c) = g(f(m)).

4. Боб посылает c' обратно Алисе. displaystyle c'' = g(f(m))\*f-1 = g(m).

Этот протокол работает, только если функции подписи и шифрования коммутативны.

Схема слепой подписи работает следующим образом:

1. Боб готовит n документов на каждом из которых написано некоторое уникальное слово (чем больше n, тем меньше у Боба шансов смошенничать).

2. Боб маскирует каждый документ уникальным маскирующим множителем и отправляет их Алисе.

3. Алиса получает все документы и случайным образом выбирает n-1 из них.

4. Алиса просит Боба выслать маскирующие множители для выбранных документов.

5. Боб делает это.

6. Алиса вскрывает n-1 документов и убеждается, что они корректны.

7. Алиса подписывает оставшийся документ и отсылает Бобу.

8. Теперь у Боба есть подписанный Алисой документ с уникальным словом, которое Алиса не знает.

Возможные сферы применения слепых подписей – системы электронного голосования, эмиссия цифровых денег в банковской сфере.

Схема электронной подписи с доказуемостью подделки (fail-stop signature scheme) ‑ cхема электронной подписи, в которой каждому открытому ключу соответствует множество секретных ключей достаточно большой мощности. При этом подпись зависит от используемого секретного ключа. Подписывающий знает, по модулю некоторого криптографического предположения, только один секретный ключ из указанного множества и при обнаружении подделки подписи может почти всегда доказать этот факт третьим лицам.

Схема конфиденциальной электронной цифровой подписи (undeniable signature scheme) ‑  схема, в которой сам факт подписания сообщения является конфиденциальным. При этом алгоритм проверки ЭЦП замещается несколькими протоколами доказательства с нулевым разглашением.