КРИПТОСИСТЕМЫ И ЦИФРОВАЯ ПОДПИСЬ ЭЛЬ ГАМАЛЯ

1 Варианты криптосистемы Эль Гамаля

Элементы рассмотренного протокола Диффи-Хеллмана с использованием эллиптических кривых можно усмотреть в варианте криптосистемы Эль Гамаля [1] применительно к группе точек эллиптической кривой.

Допустим, что множество сообщений представляется точками эллиптической кривой $\mathcal{E}$ («вложено» в эту кривую условленным способом, например, пусть сообщение вложено в x-координату точки, для упрощения дальнейшего изложения будем считать, что передаваемым сообщением является некоторая точка M эллиптической кривой, которая для сообщения m выбирается известным способом и из которой нужная форма сообщения m также просто получается).

Пусть абонент B намерен переслать абоненту A секретное сообщение m. Для этого можно построить криптосистему Эль Гамаля на основе алгебраических свойств эллиптической кривой. В качестве внешних параметров выбираются

[1]Классический вариант криптосистемы Эль-Гамаля формулируется применительно к группе Z_p^*. Внешними параметрами криптосистемы являются простое число p, и образующий элемент α мультипликативной группы Z_p^*. Секретным ключом абонента A является выбираемый им вычет $a \in Z_p^*$, его открытым ключом объявляется тройка $(p, \alpha, \alpha^a \bmod p)$.

Абонент B для передачи абоненту A секретного сообщения $m \in Z_p^*$

1. получает авторизованную копию открытого ключа (p, α, β);
2. выбирает случайное число $r \in Z_p^*$ (рандомизатор);
3. вычисляет сеансовый ключ $\delta = \beta^r \bmod p$;
4. вычисляет криптограмму $c = (c_1, c_2) = (\alpha^r, m \cdot \delta) \bmod p$;
5. отправляет криптограмму c абоненту A.

Для расшифрования криптограммы абонент A, используя свой секретный ключ a,

1. вычисляет $c_1^a \bmod p$ (получает в результате $\alpha^{r \cdot a}$);
2. инвертирует результат п.1 и умножает полученный вычет на c_2 по модулю p, получая при этом сообщение m :

$$\alpha^{-r \cdot a} \cdot c_2 \bmod p = \alpha^{-r \cdot a} \cdot m \cdot \alpha^{a \cdot r} \bmod p = \alpha^{-r \cdot a} \cdot \alpha^{r \cdot a} \cdot m \bmod p = 1 \cdot m = m.$$

эллиптическая кривая $\mathcal{E}$, точка P высокого порядка из группы точек $\mathcal{E}(F)$ и порядок N этой точки.

Абонент A выбирает секретный ключ $k_A \in Z_N^*$, вычисляет и объявляет свой открытый ключ $(\mathcal{E}, P, A)$, где $A = k_A P$.

Абонент B для передачи абоненту A секретного сообщения m

1. получает авторизованную копию открытого ключа $(\mathcal{E}, N, P, A)$;
2. «вкладывает» сообщение m в точку $M \in \mathcal{E}(F)$;
3. выбирает случайное число $r \in Z_N^*$ (рандомизатор);
4. вычисляет сеансовый ключ $\Delta = rA$;
5. вычисляет криптограмму $C = (C_1, C_2) = (rP, M + \Delta)$;
6. отправляет криптограмму C абоненту A.

Для расшифрования криптограммы абонент A, используя свой секретный ключ k_A,

1. вычисляет $k_A C_1$ (получает в результате $k_A r P$);
2. обращает результат п.1 и складывает полученную точку $-k_A r P$ с точкой C_2 , получая при этом точку M :

$$-k_A r P + M + \Delta = M + r k_A P - k_A r P = M.$$

Криптоаналитику известны открытый ключ $(\mathcal{E}, P, A)$ и криптограмма (C_1, C_2), таким образом для получения точки M ему необходимо вычислить точку $k_A r P$. Для этого ему придется решить задачу Диффи-Хеллмана для эллиптической кривой: найти эту точку по известным точкам rP и $A = k_A P$, либо ему придется решать задачи дискретного логарифмирования, вычисляя секретный ключ k_A и рандомизатор r по точкам $k_A P$, rP и P известной ему эллиптической кривой $\mathcal{E}$ и известному ему порядку точки P.

Отметим также, что как и в классическом варианте криптосистемы Эль Гамаля, повторное использование рандомизатора r недопустимо. Действительно, если криптоаналитику удалось расшифровать одну криптограмму (C_1, C_2) или узнать точку M иным способом, то он легко получит и другие сообщения, зашифрованные с тем же рандомизатором. Пусть (C_1, C_2') криптограмма, полученная с тем же рандомизатором r, что и криптограмма (C_1, C_2). Первые точки в этих парах одинаковые, а вторые связаны соотношением

$$C_2' = C_2 - M + M'.$$

Поэтому $M' = C_2' - C_2 + M$ и второе сообщение найдено.

Пример 1.1

Используем эллиптическую кривую

$$Y^2 + XY = X^3 + X^2 + 1$$

над полем $GF(2^{163})$. Она имеет порядок $2 \times P49$. Выберем неприводимый многочлен

$$1 + X + X^2 + X^8 + X^{163}$$

Возьмем точку P

$$\begin{aligned} P = \quad & (d42149e09429df4563ec1816488c92de89f93a9b2, \\ & ccd18d6cc3042c4c17a213506345c809b5ac1d476). \end{aligned} \tag{1}$$

Проверим, что ее порядок не равен 2:

$$\begin{aligned} 2P = \quad & (ccd18d6cc3042c4c17a213506345c809b5ac1d476, \\ & 835a2f56b88d6a249b4bd2a7550a4375e531d8a37) \neq \mathcal{O}. \end{aligned}$$

Значит, ее порядок равен порядку $2 \times P49$ группы или числу $P49$, и ее можно использовать для построения ключа. Определим порядок точки P, используя разложение

$$2 \times 5846006549323611672814741753598448348329118574063$$

порядка кривой. Получим

$$N = 5846006549323611672814741753598448348329118574063,$$

(так как $2P \neq \mathcal{O}$, а
$5846006549323611672814741753598448348329118574063P = \mathcal{O}$.)

Допустимы сообщения длиной до 159 бит

Пусть сообщение

$$m = 7ffac32319a7fcfa8be7edd7634d0b15af2ec.$$

Вложим его в эллиптическую кривую, получим, например, точку[2] $M =$

$$= (7ffac32319a7fcfa8be7edd7634d0b15af2eca465,$$

$$bee7fef7bf8683f5ae5e6feb1a1458d81c774906).$$

Пусть $k_a = 12$, тогда $Y = k_a P =$

$$(bd9776bbe87a8b1024be2e415952f527eee928b43,$$

[2] Точка выбирается случайно из нескольких возможных вариантов

$$c67a28ed7b137e756c37654f186a71bf64e5ac546).$$

Пусть рандомизатор $r = 123$, тогда первая точка криптограммы $C_1 = 123P =$

$$(bb7856cece13c71919534878bcb6f3a887d613c92,$$
$$f661ffdfe1ba8cb1b2ad17b6550c65aa6d4f07f41).$$

Вычислим сеансовый ключ $\Delta = rA = 123A =$

$$(bb7856cece13c71919534878bcb6f3a887d613c92,$$

$$f661ffdfe1ba8cb1b2ad17b6550c65aa6d4f07f41).$$

Вычислим вторую точку криптограммы $C_2 = M + \Delta =$

$$(dd18e5099e285430d67e8611a1802137d565b9c67,$$

$$f99de0ef9cf4975f79c82be1312ba5a2ee5f2c947).$$

Для расшифрования умножим первую точку криптограммы на секретный ключ $a = k_A$, получим $(a \cdot r)P =$

$$(bb7856cece13c71919534878bcb6f3a887d613c92,$$

$$f661ffdfe1ba8cb1b2ad17b6550c65aa6d4f07f41).$$

Обращая полученную точку, получим $-(a \cdot r)P =$

$$(bb7856cece13c71919534878bcb6f3a887d613c92,$$

$$4d19a9112fa94ba8abfe5fcee9ba9602ea99143d3).$$

Складывая результат обращения со второй точкой криптограммы, получим точку $M : -(a \cdot r)P + M + \Delta =$

$$(7ffac32319a7fcfa8be7edd7634d0b15af2eca465,$$

$$bee7fef7bf8683f5ae5e6feb1a1458d81c774906).$$

Как видим, результат расшифрования оказался правильным (это есть точка M). Из нее извлекается сообщение

$$m = 7\ ffac3231\ 9a7fcfa8\ be7edd76\ 34d0b15a\ f2ec$$

заранее согласованной длины.

2 Протоколы цифровой подписи

2.1 Электронная цифровая подпись

Электронная цифровая подпись (Digitalsignature) под сообщением m представляет собой некоторый цифровой код $\mathrm{Sign}(m, k, r)$, зависящий от этого сообщения, *ключа подписи* k и, возможно, рандомизатора (случайного кода) r. Обозначим $M,\ K,\ R,\ S$ – множества возможных сообщений, ключей подписи, рандомизаторов и значений цифровой подписи. Тогда цифровую подпись можно рассматривать как отображение

$$\mathrm{Sign}(M, K, R) : M \times K \times R \to S.$$

При фиксированных $m \in M$ и $r \in R$ и при фиксированных $m \in M$ и $k \in K$ отображения $\mathrm{Sign}(m, K, r) \to S$ и $\mathrm{Sign}(m, k, R)$ являются инъекциями, а отображение $\mathrm{Sign}(M, k, r) \to S$ сюръективно. Однако и этому отображению можно придать свойство инъективности, если рассматривать отображения $\mathrm{Sign}(M, K, R)$ вида $\mathrm{Sign}(h(M), K, R)$, где $h(M) : M \to H$ – хеш-функция[3], отображающая множество M сообщений в множество H кодов фиксированной длины, и цифровую подпись формировать как значение отображения $\mathrm{Sign}(H, K, R)$.

В этом случае подпись рассматривается как подпись под парой $(m, h(m))$, которую иногда называют сообщением, подготовленным к подписи. Множество M_S таких пар обладает рядом важных в криптографическом отношении

[3]Хэш-функция (подробнее см., напр. [1])- это легко вычисляемая функция $h : X \to Y,\ X \in \{0,1\}*,\ Y \in \{0,1\}^n$, предназначенная для «сжатия» произвольного двоичного сообщения $x \in X$ в некоторую битовую комбинацию $y \in Y$ фиксированной длины n, называемую «сверткой». (Число n есть длина блока, который, как правило, соответствует нескольким машинным словам). В криптографии используют только хеш-функции, которые обладают определенными свойствами, обеспечивающими безопасность использующих их протоколов. Такими свойствами являются 1) Однонаправленность – высокая вычислительная сложность нахождения сообщения x с заданным значением h свертки (то есть такого x, что $h(x) = h$). 2) Устойчивость хеш-функции к нахождению второго прообраза – сообщения x' с тем же значением свертки $h(x') = h(x)$, которое получено для заданного сообщения x. 3) Устойчивость к коллизиям – высокая вычислительная сложность нахождения пары сообщений x и x' с одинаковым значением свертки (то есть сообщений, для которых $h(x) = h(x')$). Здесь и ниже под высокой вычислительной сложностью понимается отсутствие соответствующих полиномиальных алгоритмов (см. следующую сноску).

свойств[4].

1)Мощность множества H много меньше мощности множества M_S : $|H| << |M \times H| = |M_S|$ (мощность области определения хеш-функции много больше мощности области ее значений).

2) Каждый элемент h множества H имеет большое число прообразов:

$$|H| << |\text{Im } m^{-1}(h)| = |\{m : (m, h) \in M_S\}|.$$

3)Легко получить элемент этого множества с заданной первой координатой m, для этого надо вычислить значение $h(m)$ первой координаты по алгоритму вычисления значения хеш-функции. Тем самым легко проверить, принадлежит ли данная пара элементов (m, h), $m \in M$, $h \in H$ множеству M_S. В то же время вычисление первой координаты элемента этого множества по заданной второй координате практически невозможно вследствие свойства односторонности хеш-функции. [5]

4)При заданном элементе $(m, h(m)) \in M_S$, практически невозможно подобрать элемент $(m', h(m')) = (m', h(m)) \in \mathcal{M_S}$, $m' \neq m$, то есть элемент, отличающийся от заданного только первой координатой (подобрать второе значение m' аргумента хеш функции при котором она получает то же значение, что и при заданном значении m аргумента).

[4]Поскольку множество M_S, по существу, является графиком хеш-функции h, то перечисляемые его свойства соответствуют ее свойствам.

[5]Односторонние функции f определяются в классе функций $f_n : \Sigma^n \to \Sigma^m$, $m = m(n)$, где $m(n)$ – некоторый полином.

Функция называется *честной* [2], если существует полином $q(n)$, такой, что $n \leq q(m(n))$. Это означает, что такая функция не слишком сильно «сжимает» входные значения. Честная функция f называется *односторонней,* если

1) Существует полиномиальный алгоритм (алгоритм, исполняющий не более $P(n)$ элементарных операций при вычислении значения функции, $P(n)$ есть некоторый полином) , вычисляющий ее значение $f(x)$ при любом x. Ниже для сокращения подобное условие мы будем формулировать так: «$f(x)$ легко вычислить для всякого x», а если такой алгоритм не существует, будем говорить «практически невозможно вычислить»

2) Для любого вероятностного алгоритма A и случайно выбранной строки $x \in_R \Sigma^n$ и любого полинома $p(n)$ вероятность

$$Pr\{f(A(f(x))) = f(x)\} < 1/p(x).$$

5) Практически невозможно подобрать два произвольных элемента (m, h) и (m', h) с одинаковыми значениями второй координаты (два сообщения m и m' с одним и тем же значением хеш-функции $h(m) = h(m')$.

Цифровая подпись сообщения $h(m)$ на ключе подписи k допускает проверку с использованием опубликованного *ключа проверки* k', алгебраически связанного с k.

Проверка основана на вычислении предиката $P(S, K')$ проверки, где K' – множество ключей проверки. Цифровая подпись $\mathrm{Sign}(h(m), k, r)$ удостоверяется с использованием ключа проверки k', если

$$P(\mathrm{Sign}(h(m), k, r), k') = 1.$$

Предикат проверки цифровой подписи с возвратом сообщения [6] описывается как

$$P(S, K') = \{((m', h'(m)) \in M_S\},$$

где m' проверяемое сообщение, а $h'(m)$ – хеш-значение подписанного сообщения, извлеченное из цифровой подписи $\mathrm{Sign}(h(m), k, r)$ на заданном ключе проверки $k',\ k' \in K'$.

Отображение $\mathrm{Sign}(M, K, R)$ обладает рядом свойств, гарантирующих возможность и достоверность подтверждения подлинности подписи и, тем самым гарантирующих невозможность отказа от авторства подписавшим документ, как и невозможность вскрытия ключа подписи.

1) Односторонность отображения

$$\mathrm{Sign}(h(m), K, R):$$

по значению отображения $s = \mathrm{Sign}(h(m), k, r)$, такого, что $P(s, k')$, практически невозможно (при известных $h(m)$ и k') узнать ключ k.

2) Для заданного сообщения m и известного значения цифровой подписи $s = \mathrm{Sign}(h(m), k, r),\ \ P(s, k') = 1$, практически невозможно подобрать другое (фальсифицированное) сообщение m' с тем же значением $\mathrm{Sign}(h(m'), k, r) = \mathrm{Sign}(h(m), k, r)$ цифровой подписи. То есть, невозможно подделать подпись под сообщением m.

[6] Основана на возможности извлечения «отпечатка» $h(m)$ сообщения m из цифровой подписи $\mathrm{Sign}(m, k, r)$.

3)Практически невозможно найти два произвольных сообщения m и m' с одинаковым значением подписи s, таким, что $P(s, k') = 1$, то есть удовлетворяющих предикат проверки на заданном ключе проверки k'. То есть, невозможно подменить подписанное сообщение.

4)Не зная ключ подписи, практически невозможно найти произвольное сообщение m и правильное значение цифровой подписи под ним. То есть, невозможно создать подписанное сообщение.

Эти свойства обеспечиваются использованием *криптографически стойкой* хеш-функции, обладающей перечисленными выше свойствами, а также биективных преобразований, соответствующих трудным алгебраическим проблемам.

2.2 Обобщенная схема электронной подписи Эль Гамаля

Эта схема работает в любой абелевой группе с трудной проблемой дискретного логарифма. Это могут быть мультипликативная группа любого поля Галуа, группа точек несуперсингулярной эллиптической кривой или подгруппы высокого порядка этих групп. Ввиду того, что обозначения мультипликативной и аддитивной степени различаются удобнее дать два варианта описания протокола.

Обобщенная подпись Эль-Гамаля в мультипликативной группе. Публикуемыми системными параметрами являются описание группы (или подгруппы) G (характеристика поля, неприводимый многочлен (в случае использования расширения поля), образующий элемент α, порядок N группы).

Ключ подписи выбирается как целое число $k,\ 0 < k < N$.

Публикуемый ключ проверки вычисляется как элемент $\beta = \alpha^k$.

Цифровой подписью под документом m является пара (c, d), где $c = \alpha^r$ – случайный элемент группы G, определяемый случайным выбором рандомизатора $r,\ 0 < r < N - 1$,

$$d = r^{-1}(h(m) - kh(c)) \bmod N -$$

число, вычисляемое с использованием ключа подписи k, того же рандомизатора r и значений $h(m)$ хеш-функции от сообщения m и $h(c)$ от соответствующего рандомизатору случайного элемента c группы G (код описания этого случайного элемента рассматривается как значение аргумента хеш-функции).

Предикат проверки цифровой подписи (c, d) под документом m, полученной на ключе подписи k, описывается следующим образом:

$$c \in G, 0 < d < N-1, \beta^{h(c)} c^d = \alpha^{h(m)} \tag{2}$$

Если подпись вычислена абонентом, владеющим секретным ключом k, то данный предикат выполняется. Действительно, в этом случае

$$d \equiv r^{-1}(h(m) - kh(c)) \pmod N.$$

Умножив обе части сравнения на r, получим

$$rd \equiv h(m) - kh(c) (\mathrm{mod}\ N),$$

что эквивалентно сравнению

$$h(m) \equiv kh(c) + rd \pmod N.$$

Отсюда следует

$$\alpha^{h(m)} = \alpha^{kh(c)+rd} = (\alpha^k)^{h(c)}(\alpha^r)^d = \beta^{h(c)} c^d.$$

Если же ключ подписи другой, то предикат имеет значение 0.

Заметим, что генерация подписи требует вычислений как в группе G, так и в группе Z_n, в то же время проверка подписи связана с вычислениями только в группе G.

Чтобы подделать подпись под сообщением m' злоумышленник вынужден взять случайное число r и вычислить $c = \alpha^r$ с тем, чтобы затем определить $d = r^{-1}(h(m') - kh(c)) \bmod N$. Для этого надо, зная $\beta = \alpha^k$, найти ключ подписи k, то есть найти дискретный логарифм от β по основанию α, что практически невозможно. Остается выбирать d наугад с вероятностью успеха $\frac{1}{N}$.

Если же он подделает подпись под сообщением $m' \neq m$ каким-то другим способом (то есть возьмет некоторое число r, вычислит $c = \alpha^r$ и затем каким-то образом найдет d так, что при подстановке $h(m')$ вместо $h(m)$ будет выполняться предикат проверки (2)), то этим способом он сможет решать задачи дискретного логарифмирования в соответствующей мультипликативной группе: он сможет вычислить ключ подписи $k = (h(m') - rd)h(c)^{-1}$. Таким образом проблема подделки подписи столь же сложна, как и проблема дискретного логарифма в этой группе.

Число r должно уничтожаться сразу после вычисления подписи, так как по этому числу (если оно станет известно злоумышленнику) и значению подписи (c, d) под известным сообщением m вычисляется секретный ключ:

$$k = (h(m) - rd)h(c)^{-1} \bmod N$$

Это же возможно в случае повторного использования числа r, так как в этом случае оно с большой вероятностью вычисляется. Действительно, пусть с использованием одного и того же числа r получены две подписи (c_1, d_1) и (c_2, d_2), $c_1 = c_2 = \alpha^r = c$ под сообщениями m_1 и m_2. При этом

$$d_1 = r^{-1}\{h(m_1) - kh(c)\} \bmod N,\ d_2 = r^{-1}\{h(m_2) - kh(c)\} \bmod N.$$

Тогда

$$(d_1 - d_2)r \equiv (h(m_1) - h(m_2))(\text{mod } N).$$

При $d_1 \neq d_2$ получаем $r = (d_1 - d_2)^{-1}(h(m_1) - h(m_2)) \bmod N$. теперь можно вычислить k, как описано выше.

В алгоритме подписи используется не само сообщение, а значение хеш-функции от него. Иначе возможен подбор сообщения с известным значением подписи (то есть не выполняется четвертое свойство цифровой подписи). Например, можно выбрать случайные числа $i, j,\ 1 < i < N,\ 1 < j < \ N,\ (j, N) = 1$, и положить

$$c = \alpha^i \beta^j = \alpha^{i+kj};$$

$$d = -h(c)j^{-1} \text{mod } N,$$

Тогда пара (c, d) является подписью под сообщением

$$m = di \bmod N = -h(c)ij^{-1} \text{mod } N,$$

так как

$$(\alpha^m \alpha^{-kh(c)})^{d^{-1}} = \alpha^i \beta^j = c.$$

Действительно,

$$(\alpha^m \alpha^{-kh(c)})^{d^{-1}} = (\alpha^{-h(c)ij^{-1}} \alpha^{-kh(c)})^{(-h(c)j^{-1})^{-1}} =$$

$$= \alpha^{-h(c)ij^{-1}(-h(c))^{-1}j} \alpha^{-kh(c)(-h(c))^{-1}j} = \alpha^i \alpha^{kj} = \alpha^{i+kj} = c.$$

Теперь можно получить $\alpha^m \alpha^{-kh(c)} \equiv c^d$, откуда следует подтверждение подписи (напоминаем, что $\alpha^a = \beta$):

$$\beta^{h(c)} c^d \equiv \alpha^m.$$

В предикате проверки подписи предусматривается проверка, что $c \in G$. Если эту проверку не делать, то в некоторых случаях, например, при построении протокола на основе группы Z_p^* (порядка $N = p - 1$) злоумышленник может подписать выбираемое им сообщение m', если располагает подписанным на секретном ключе k сообщением m. Пусть (c, d) – подпись под сообщением m. Допустим, что существует $m^{-1} \bmod (p-1)$. Тогда можно вычислить $u = m' \cdot m^{-1}$. Затем по китайской теореме об остатках можно вычислить $d' = du \bmod N$ и c', такие, что

$$c' \equiv cu \ (\text{mod } N) \text{ и } c' \equiv c \ (\text{mod } N + 1).$$

Пара (c', d') является подписью под сообщением m', которая подтверждается предикатом проверки подписи и сообщение m' будет принято, если указанная проверка игнорируется.

Обобщенная подпись Эль-Гамаля в аддитивной группе. Рассматриваемая схема наиболее удачно может быть реализована при использовании в качестве группы G группы E(F) точек эллиптической кривой E над конечным полем F или ее подгруппы. Проблема дискретного логарифма в этой группе гораздо сложнее, чем в мультипликативной группе конечного поля F. Поэтому может быть выбрано меньшее q, чем в случае реализации в группе F^*.

В случае использования группы точек эллиптической кривой системными параметрами являются уравнение эллиптической кривой $\mathcal{E}$, описание поля F и точка P кривой известного большого порядка N – образующий элемент подгруппы $G \subseteq \mathcal{E}(F)$ группы точек эллиптической кривой. Публикуемым ключом проверки k' является точка $Q = kP$ эллиптической кривой. Цифровая подпись $(c, d) = (R, d)$, где $c = R = rP$ – случайная точка, элемент группы G, определяется случайным выбором рандомизатора $r, 0 < r < N - 1$,

$$d = r^{-1}(h(m) - kh(R)) \bmod N -$$

число, вычисляемое с использованием ключа подписи k, того же рандомизатора r и значений $h(m)$ хеш-функции от сообщения m и $h(R)$ от соответствующей рандомизатору случайной точки $R = (x, y)$ группы G (конкатенация $x||y$ координат x и y этой точки рассматривается как значение аргумента хеш-функции).

Предикат проверки цифровой подписи на документе m, полученной на ключе подписи k, описывается следующим образом:

$$R \in G, 0 < d < N - 1, h(c)Q + dR = h(m)P. \tag{3}$$

Если генерация подписи требует вычислений как в группе $\mathcal{E}(F)$, так и в группе Z_n, то проверка подписи связана с вычислениями только в группе $\mathcal{E}(F)$.

Алгебраически и криптографически эквивалентным рассмотренному варианту цифровой подписи является вариант, отличающийся тем, что вместо точки $c = R$ эллиптической кривой в качестве первого элемента цифровой подписи берется число $c = h(R)$, хеш-значение от этой точки. При вычислении второго числа подписи не производится умножение на число r^{-1} :

$$d = h(m) - kh(R).$$

Соответственно упрощается и предикат проверки подписи:

$$0 < s < N - 1, 0 < d < N - 1, cQ + dP = h(m)P.$$

В данном случае алгоритм получения подписи использует только операции модульной арифметики, а алгоритм проверки- только операции группы точек эллиптической кривой.

Последний вариант подписи используется в алгоритме ECDSA, применяемом в американском стандарте электронной подписи [3].

3 Контрольные вопросы

1. Перечислите свойства цифровой подписи.

2. Какими свойствами обладает криптографическая хеш-функция.

3. Сформулируйте алгоритм цифровой подписи Эль Гамаля и алгоритм проверки цифровой подписи Эль Гамаля применительно к мульи=типликативной группе поля $GF(2^n)$.

4. В чем отличие мультипликативного и аддитивного вариантов цифровой подписи Эль Гамаля?

5. Какие трудные проблемы лежат в основе безопасности различных вариантов цифровой подписи Эль Гамаля.

6. докажите эквивалентность по безопасности цифровой подписи Эль Гамаля и проблемы Диффи-Хеллмана, имея в виду атаки на цифровую подпись по выбираемому шифртексту.

Литература

1.Алферов А.П.,Зубов А.Ю.,Кузьмин А.С., Черемушкин А.В. Основы криптографии.–М: Гелиос АРВ, 2001.

2. Введение в криптографию. //Подред В.В.Ященко. – СПб: Питер, 2001.

3.Koblitz N. Algebraic aspects of Cryptography. Springer-Verlag.1998.