27 ЭЦП

27.1 ЭЦП ЭльГамаля

В 1984 году ЭльГамаль предложил криптосистему с открытым ключом и систему ЭЦП, которые впоследствии были названы его именем. Стойкость систем ЭльГамаля базируется не на сложности проблемы факторизации, как в RSA, а на сложности проблемы дискретного логарифмирования в определенных циклических группах G.

Опишем систему ЭЦП ЭльГамаля для случая, когда G является подгруппой мультипликативной группы конечного поля.

В этом случае группа описывается тройкой $par = (p, q, g)$, где p и q — простые, $q \mid p-1$ и g — элемент порядка q по модулю p. Личным ключом является число $x \in \mathbb{F}_q$, открытым — $y = g^x \bmod p$.

Алгоритм Gen (ЭльГамаль)

Вход: 1^ℓ (ℓ — уровень стойкости).

Выход: (p, q, g), x, y.

Шаги:

1. $p, q \leftarrow PRIMES$: $q \mid p-1$, $2^{\ell-1} < p < 2^\ell$ (можно использовать теорему Диемитко).
2. $\alpha \xleftarrow{R} \mathbb{F}_p^*$.
3. $g \leftarrow \alpha^{(p-1)/q} \bmod p$.
4. Если $g = 1$, то вернуться к шагу 2.
5. $x \xleftarrow{R} \mathbb{F}_q^*$.
6. $y \leftarrow g^x \bmod p$.
7. Возвратить $((p, q, g), x, y)$

Корректность. По завершении алгоритма $g \not\equiv 1 \pmod p$ и $g^q \equiv 1 \pmod p$. Поскольку q — простое, отсюда следует, что $\operatorname{ord} g = q$ (в группе $\mathbb{F}_p^*$).

Сложность. Пусть α_0 — примитивный элемент $\mathbb{F}_p^*$. Тогда элемент α, который генерируется на шаге 2, имеет вид α_0^i, $i \xleftarrow{R} \{0, 1, \ldots, p-2\}$. Вероятность успеха за один проход цикла 2–4:

$$\mathbf{P}\{g \neq 1\} = \mathbf{P}\left\{\alpha_0^{i(p-1)/q} \neq 1\right\} = \mathbf{P}\{i \not\equiv 0 \pmod q\} = \frac{q-1}{q}.$$

Поэтому в среднем потребуется $q/(q-1)$ проходов.

В алгоритмах выработки и проверки ЭЦП используется функция хэширования $h\colon \{0,1\}^* \to \{0, 1, \ldots, q-1\}$. Эта функция может быть получена из стандартной функции $h^*\colon \{0,1\}^* \to \{0,1\}^n$, где $2^n > q$: $h(X) = h^*(X) \mod q$ (двоичные слова $h^*(X)$ представляется числом).

Подписью сообщения $X \in \{0,1\}^*$ является пара чисел (r, s), $r \in \mathbb{F}_p^*$, $s \in \mathbb{F}_q$, которая является решением уравнения

$$g^{h(X)} \equiv y^r r^s \pmod p \qquad (\star)$$

При выработке ЭЦП уравнение $(\star)$ решается, а при проверке ЭЦП — проверяется решение.

Алгоритм Sign (ЭльГамаль)

Вход: par, y, $X \in \{0,1\}^*$.

Выход: (r, s).

Шаги:

1. $k \xleftarrow{R} \mathbb{F}_q^*$.

2. $r \leftarrow g^k \bmod p$.

3. $s \leftarrow k^{-1}(h(X) - xr) \bmod q$.

4. Возвратить (r, s).

Корректность: При этом действительно

$$y^r r^s \equiv g^{xr} g^{ks} \equiv g^{h(X)} \pmod p,$$

так как $xr + ks \equiv h(X) \pmod q$.

Алгоритм Vfy (ЭльГамаль)

Вход: *par*, x, X, (r, s).

Выход: 0 или 1.

Шаги:

1. Если $r \notin \mathbb{F}_p^*$, $s \notin \mathbb{F}_q$ или нарушается $(\star)$, то возвратить 0.

2. Возвратить 1.

27.2 Стойкость ЭЦП ЭльГамаля

Связь с DLP. Проанализируем, как Виктор может решить уравнение $(\star)$.

1. Виктор может определить x по y. Но это означает решение задачи DL: $g^x \equiv y \pmod p$.

2. Виктор может определить k по r с последующим определением $x = r^{-1}(h(X) - ks) \bmod q$. Но это снова DL: $g^k \equiv r \pmod p$.

3. Виктор может зафиксировать r и решить $(\star)$ относительно s. При этом ему снова требуется решить DL:
$$r^s \equiv g^{h(X)} y^{-r} \bmod p.$$

В целом система ЭЦП проектируется так, чтобы противник который решает проверочное уравнение типа $(\star)$ всегда «натыкался» на трудную задачу, в данном случае DL.

Атака Блейхенбахера. Блейхенбахер в 1996 г. нашел способ выбора r, при котором уравнение $(\star)$ может решаться просто. А именно, пусть известны целые α и β такие, что

$$\alpha q = g^\beta \pmod p.$$

Тогда противник может без труда подделать подпись при любом выборе личного и открытого ключей. Противник выбирает $r = \alpha q$. Проверочное соотношение принимает вид:

$$g^{h(X)} \equiv y^{\alpha q} (\alpha q)^s \equiv g^{\beta s} \bmod p.$$

Теперь можно определить s: $s = \beta^{-1} h(X) \bmod q$.

Виктор может провести атаку Блейхенбахера, если ему поручено генерировать параметры (p, q, g). Виктор может, например, выбирать секретные (маскировочные) α и β и искать (g в виде $(\alpha q)^{\beta^{-1} \bmod q} \bmod p$.

К счастью, от атаки Блейхенбахера легко защититься. В алгоритм выработки ЭЦП следует ввести дополнительная проверка: если $r \equiv 0 \pmod q$, то генерация k повторяется. Соответственно, при выработке ЭЦП следует дополнительно проверять, что $r \not\equiv 0 \pmod q$.

Требования к функции хэширования. Используемая функция хэширования h должна быть строго свободной от коллизий и односторонней.

Первое требования обеспечивает защиту от переноса подписи с документа X на документ X' с тем же хэш-значением.

Второе требование обеспечивает защиту от следующей атаки: Виктор выбирает $\alpha \in \mathbb{F}_q$, $\beta \in \mathbb{F}_q^*$ и вычисляет:

1) $r = g^{\alpha} y^{\beta} \bmod p$;

2) $s = -r\beta^{-1} \bmod q$;

3) X такое, что $h(X) = \alpha s \bmod q$.

Тогда (r, s) является действительной подписью по схеме Эль-Гамаля к документу X:

$$y^r r^s \equiv y^r g^{\alpha s} y^{\beta s} \equiv g^{\alpha s} y^{r-r} \equiv g^{h(X)} \pmod p.$$

27.3 Модификации ЭЦП ЭльГамаля

Рассмотрим некоторые модификации ЭЦП ЭльГамаля.

1. *Изменение проверочного уравнения.* Схема Эль-Гамаля послужила образцом для создания семейства ЭЦП, в которых проверка подписи (r, s) выполняется по правилу

$$g^A y^B \equiv r^C \pmod p,$$

где тройка (A, B, C) совпадает с одной из перестановкой чисел $(\pm h(X), \pm s, \pm r)$ при некотором выборе знаков. Например, для базовой схемы: $A = h(X)$, $B = -r$, $C = s$.

Американский стандарт DSA: $A = h(X)$, $B = r$, $C = s$. Российский стандарт ГОСТ Р 34.10-94: $A = s$, $B = -r$, $C = h(X)$.

2. *Ускорение проверки.* Для ускорения проверки ЭЦП можно организовать ее следующим образом:

$$g^{AC^{-1} \bmod q} y^{BC^{-1} \bmod q} \stackrel{?}{\equiv} r \pmod p.$$

Теперь вместо 3 возведений в степень требуется выполнить только 2.

Требуется, чтобы $C \neq 0 \bmod q$. Поэтому, например, в ГОСТ Р 34.10-94 нулевые хэш-значения $h(X)$ заменяют на 1.

3. *Сокращение длины ЭЦП.* Еще одна модификация: для сокращения длины подписи вместо пары (r, s) используют пару $(r \bmod q, s)$ и соотношение для проверки заменяют на

$$(g^{AC^{-1} \bmod q} y^{BC^{-1} \bmod q} \bmod p) \bmod q \stackrel{?}{=} r \bmod q.$$

Упражнение 27.1 (скрытый канал). *Скрытый канал* — это способ встраивания секретной информации в общедоступную. Показать, как, располагая общедоступной подписью по схеме Эль-Гамаля (r, s) к документу с хэш-значением $h(X)$, доверенные лица (знающие ключ x) могут определить секретное число k. □

27.4 Метод Монтгомери

При выработке и проверке подписи ЭльГамаля приходится выполнять возведение в степень по модулю. При этом приходится производить много делений. Деление является более трудоемкой операцией чем умножение. *Метод Монтгомери* позволяет уменьшить число делений.

Пусть R – натуральное число, взаимно простое с модулем n, $R > n$, $m' = -m^{-1} \bmod R$, $a \in \{0, 1, \ldots, nR-1\}$. *Приведение по Монтгомери* — вычисление $aR^{-1} \bmod m$.

Алгоритм Приведение по Монтгомери

Вход: a, n, R, m'.
Выход: $aR^{-1} \bmod m$.
Шаги:

1. $b \leftarrow m'a \bmod R$.

2. $c \leftarrow (a+nb)/R$ (далее мы обоснуем, что $(a+nb)$ делится нацело на R).

3. Если $c > n$, то $c \leftarrow c - n$.

4. Возвратить c.

Корректность:

1) $a + bm \equiv a(1+mm') \equiv 0 \pmod R$ и $(a+bm)/R$ — целое число;

2) $c = (a+bm)/R \equiv aR^{-1} \pmod m$;

3) $a + bm < 2mR$.

Таким образом, $c = xR^{-1} \bmod m$ или $c = xR^{-1} \bmod m + m$.

Сложность. Если используется представление чисел по основанию $B = 2^w$, а R является степенью B, то для вычисления $aR^{-1} \bmod m$ достаточно выполнить два умножения $a \cdot m'$ и $b \cdot m$, одно сложение $a + bm$ и, возможно, одно вычитание $(a+bm)/R - m$. Деление на R состоит в сдвиге разрядов делимого вправо.

С помощью приведения по Монтгомери можно реализовать *умножение по Монтгомери*:

$$a \circ b = abR^{-1} \bmod m.$$

Если $a, b \in \mathbb{Z}_m$, $R > m$, то обычное произведение ab лежит в интервале $\{0, 1, \ldots, mR-1\}$ и произведение Монтгомери $abR^{-1} \bmod m$ можно найти с помощью предыдущего алгоритма.

Пусть $a^{(e)}$ — e-ая степень a относительно операции $\circ$:

$$a^{(e)} = \underbrace{a \circ a \circ \ldots \circ a}_{e \text{ раз}}.$$

Значение $a^{(e)}$ можно найти с помощью бинарного метода, выполнив $\ll(e)$ возведений в квадрат по Монтгомери и $w(e)$ умножений ($\ll(e)$ — длина двоичной записи e, $w(e)$ — число единиц в двоичной записи).

Покажем как найти обычную степень $a^e \bmod m$.

Алгоритм Возведение в степень

Вход: n, $a \in \mathbb{Z}_n$, $e \in \mathbb{Z}_n$.

Выход: $a^e \bmod m$.

Шаги:

1. Выбрать $R > m$ — степень двойки, рассчитать $m' = -m^{-1} \bmod R$. Число R определяет операцию $\circ$, а m' используется для умножения с помощью $\circ$.

2. $b \leftarrow aR \bmod m$.

3. $B \leftarrow b^{(e)}$ (возведение в степень по Монтгомери).

4. $B \leftarrow BR^{-1} \bmod m$ (приведение по Монтгомери).

5. Возвратить B.

Корректность: после выполнения шага 3

$$B = b^{(e)} = (aR)^e (R^{-1})^{e-1} = a^e R \bmod m.$$

Поэтому на последнем шаге $B = a^e \bmod m$.

27.5 ЭЦП Шнорра

В 1990 году немецкий криптограф К. Шнорр предложил модификацию схемы ЭльГамаля, названную впоследствии *схемой Шнорра*.

В схеме Шнорра используются те же параметры и ключи, что и в схеме ЭльГамаля. Снова используется хэш-функция $h\colon \{0,1\}^* \to \mathbb{F}_q$.

Подписью к документу $X \in \{0,1\}^*$ является решение (s,e) уравнения

$$h(X \parallel (g^s y^{-e} \bmod p)) = e, \quad e, s \in \mathbb{F}_q. \tag{$\star\star$}$$

Алиса находит решение $(\star\star)$ по следующему алгоритму:

1. $k \overset{R}{\leftarrow} \{1, \ldots, q-1\}$.
2. $r \leftarrow g^k \bmod p$.
3. $e \leftarrow h(X \parallel r)$.
4. $s \leftarrow (xe + k) \bmod q$.
5. Возвратить (s, e).

При этом действительно

$$h(X \parallel (g^s y^{-e} \bmod p)) = h(X \parallel (g^{s-xe} \bmod p)) = h(X \parallel (g^k \bmod p)) = e.$$

Сравнительный анализ сложности реализации схем ЭльГамаля и Шнорра приводится в следующей таблице (следует дополнительно учесть операции хэширования и аддитивные операции по модулю q):

операции	схема ЭльГамаля	схема Шнорра
выработка подписи		
возведение в степень $\bmod p$	1	1
умножение $\bmod q$	2	1
обращение $\bmod q$	1	–
проверка подписи (домножение $h(X)^{-1} \bmod q$ в схеме ЭльГамаля)		
умножение $\bmod q$	2	–
обращение $\bmod q$	1	–
возведение в степень $\bmod p$	2	2
умножение $\bmod p$	1	1

Введенный в 1999 г. стандарт Республики Беларусь `СТБ 1176.2` «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи» базируется на схеме Шнорра.

Отличия от схемы Шнорра состоят в следующем:

1. Длины чисел p и q фиксированы: допустимые значения $l = \lceil \log_2 p \rceil$ и $r = \lceil \log_2 q \rceil$ приведены в следующей таблице:

Уровень стойкости	r	l	Уровень стойкости	r	l
1	143	638	6	208	1534
2	154	766	7	222	1790
3	175	1022	8	235	2046
4	182	1118	9	249	2334
5	195	1310	10	257	2462

2. Часть преобразований стандарта выполняется в группе G, определяемой множеством $B_p = \{1, 2, \ldots, p-1\}$ и операцией $\circ$: $u \circ v = uvR^{-1} \bmod p$, где $R = 2^{l+2}$. Использование операции $\circ$ вместо обычного умножения по модулю p упрощает применение алгоритма Монтгомери. Как и раньше, $a^{(e)}$ есть e-я степень числа $a \in B_p$ как элемента G.

3. Функция h действует не на $\mathbb{F}_q$, а на $\{0, 1\}^{r-1}$.

4. Уравнение $(\star\star)$ меняется на уравнение:

$$h(g^{(s)} \circ y^{(e)} \parallel X) = e.$$