О скрытых возможностях отечественного варианта уравнения Эль-Гамаля

Антон Гуселев

— РусКрипто 2025 —

Содержание

Механизмы с дополнительным функционалам

- схемы кольцевой подписи
- схемы группой подписи
- схемы редактируемой подписи
- схемы подписи вслепую
- схемы пороговой подписи
- схемы агрегируемой подписи
- схемы подписи на основе идентификаторов
- схемы одновременного формирования подписи и шифрования

Механизмы с дополнительным функционалам

- ✗ схемы кольцевой подписи
- ○ схемы редактируемой подписи
- ○ схемы подписи вслепую
- ○ схемы пороговой подписи
- ○ схемы агрегируемой подписи
- ○ схемы подписи на основе идентификаторов
- ○ схемы одновременного формирования подписи и шифрования

Механизмы с дополнительным функционалам

- ✗ схемы кольцевой подписи
- ? схемы группой подписи
- ? схемы редактируемой подписи
- ○ схемы подписи вслепую
- ○ схемы пороговой подписи
- ○ схемы агрегируемой подписи
- ○ схемы подписи на основе идентификаторов
- ○ схемы одновременного формирования подписи и шифрования

Механизмы с дополнительным функционалам

- ✗ схемы кольцевой подписи
- ? схемы группой подписи
- ? схемы редактируемой подписи
- ✓ схемы подписи вслепую
- ✓ схемы пороговой подписи
- ✓ схемы агрегируемой подписи
- ✓ схемы подписи на основе идентификаторов
- ✓ схемы формирования подписи и шифрования

Содержание

Схема подписи на основе уравнения Шнорра

Формирование подписи

Вход: ключ d, сообщение m

1: Выбрать $k \in_R \{1, 2, \ldots, q-1\}$
2: Вычислить $R = kP$
3: Вычислить $r = R_x \bmod q$
4: Вычислить $\hat{e} = \mathrm{H}(r \| m)$
5: Вычислить $s = k + \hat{e}d \bmod q$

Выход: $(\hat{e}, s)$ – подпись

Проверка подписи

Вход: ключ Q, сообщение m, подпись $(\hat{e}, s)$

1: Вычислить $R = sP - \hat{e}Q$
2: Вычислить $r = R_x$
3: **Если** $\mathrm{H}(r \| m) = \hat{e} \bmod q$ **то** подпись верна
4: **иначе** отвергнуть подпись

Схемы на основе уравнения Эль-Гамаля

Формирование подписи в ГОСТ

Вход: ключ d, сообщение m

1: Вычислить $e = \mathrm{H}(m)$
2: Выбрать $k \in_R \{1, 2, \ldots, q-1\}$
3: Вычислить $R = kP$
4: Вычислить $r = R_x \bmod q$
5: Вычислить $s = rd + ke \bmod q$

Выход: (r, s) – подпись

Проверка подписи

Вход: ключ Q, сообщение m, подпись (r, s)

1: Вычислить $e = \mathrm{H}(m)$
2: Вычислить $R = se^{-1}P - re^{-1}Q$
3: **Если** $r = R_x \bmod q$ **то** подпись верна
4: **иначе** отвергнуть подпись

Формирование подписи в ECDSA

Вход: ключ d, сообщение m

1: Вычислить $e = \mathrm{H}(m)$
2: Выбрать $k \in_R \{1, 2, \ldots, q-1\}$
3: Вычислить $R = kP$
4: Вычислить $r = R_x \bmod q$
5: Вычислить $s = k^{-1}(e + dr) \bmod q$

Выход: (r, s) – подпись.

Проверка подписи

Вход: ключ Q, сообщение m, подпись (r, s)

1: Вычислить $e = \mathrm{H}(m)$
2: Вычислить $s' = s^{-1} \bmod q$
3: Вычислить $R = s'(eP + rQ)$
4: **Если** $r = R_x \bmod q$ **то** подпись верна
5: **иначе** отвергнуть подпись

Содержание

Схемы агрегируемой подписи. Уравнение Шнорра

Задача

Два пользователя с ключами проверки Q_1 и Q_2 хотят выработать подпись под одинаковым сообщением такую, что ее размер будет равен размеру одной подписи $(\hat{e}, s)$ и ее можно будет верифицировать с использованием ключа проверки $Q = Q_1 + Q_2$

Очевидное решение

- $s_1 + s_2 = (k_1 + \hat{e}_1 d_1) + (k_2 + \hat{e}_2 d_2)$
- но $\hat{e}_1 = \mathrm{H}(r_1, m) \neq \mathrm{H}(r_2, m) = \hat{e}_2$
- нужно, чтобы $\hat{e}_1 = \hat{e}_2 = \hat{e}$
- $s_1 + s_2 = (k_1 + k_2) + \hat{e}(d_1 + d_2)$
- т.о. нужно научится выносить за скобки

Формирование подписи*

Вход: ключи d_1, d_2, сообщение m

1: Выбрать $k_i \in_R \{1, 2, \ldots, q-1\}$
2: Вычислить $R_i = k_i P$
3: Опубликовать R_i
4: Вычислить $r = (R_1 + R_2)_x \bmod q$
5: Вычислить $\hat{e} = \mathrm{H}(r, m)$
6: Вычислить $s_i = k_i + \hat{e} d_i \bmod q$
7: Опубликовать $(\hat{e}, s_i)$

Выход: $(\hat{e}, s_1 + s_2)$ – подпись

Схемы агрегируемой подписи. Уравнение из ГОСТ

Можно ли выносить за скобки в схеме ГОСТ?

Да, но для этого нужно

- выполнить дополнительные преобразования открытых параметров
- сделать замену

$$s'_i = r_i^{-1} s_i = r_i^{-1}(r_i d_i + k_i e) = d_i + r_i^{-1} k_i e$$

- и тогда

$$s'_1 + s'_2 = (d_1 + d_2) + e(r_1^{-1} k_1 + r_2^{-1} k_2)$$

Схемы агрегируемой подписи. Уравнение из ГОСТ

Формирование подписи

Вход: ключи d_1, d_2, сообщение m

1: По ГОСТ вычислить (r_i, s_i)
2: Опубликовать (r_i, s_i)
3: Вычислить $s'_i = s_i r_i^{-1} \bmod q$
4: Вычислить $R'_i = r_i^{-1} R_i$
5: Вычислить $r' = (R'_1 + R'_2)_x$

Выход: $(r', s'_1 + s'_2)$ – подпись

Проверка подписи

Вход: ключ $Q = Q_1 + Q_2$, сообщение m, подпись (r', s')

1: Вычислить $e = \mathrm{H}(m)$
2: Вычислить $R'' = e^{-1}(s'P - Q)$
3: **Если** $(R'')_x = r'$ **то** подпись верна
4: **иначе** отвергнуть подпись

Схемы агрегируемой подписи. Уравнение из ГОСТ

Формирование подписи

Вход: ключи d_1, d_2, сообщение m

1: По ГОСТ вычислить (r_i, s_i)
2: Опубликовать (r_i, s_i)
3: Вычислить $s'_i = s_i r_i^{-1} \bmod q$
4: Вычислить $R'_i = r_i^{-1} R_i$
5: Вычислить $r' = (R'_1 + R'_2)_x$

Выход: $(r', s'_1 + s'_2)$ – подпись

Проверка подписи

Вход: ключ $Q = Q_1 + Q_2$, сообщение m, подпись (r', s')

1: Вычислить $e = \mathrm{H}(m)$
2: Вычислить $R'' = e^{-1}(s'P - Q)$
3: **Если** $(R'')_x = r'$ **то** подпись верна
4: **иначе** отвергнуть подпись

Положительные особенности

- не требуется предварительная публикация параметров
- возможна агрегация подписей, полученных с использованием схемы ГОСТ и Шнорра, однако необходимо использовать «модифицированное» уравнение Шнорра $s\hat{e}^{-1} = \hat{e}^{-1}k + d$

Схемы агрегируемой подписи. Уравнение из ECDSA

Гипотеза/Утверждение

- с учетом вида уравнения подписи

$$s = k^{-1}(e + dr) \bmod q$$

  «освобождение» ключа подписи от других секретных параметров (и как следствие вынесение за скобки) без потери свойства безопасности не представляется возможным

- возможно именно из-за этого схема (EC)DSA не используется при создании асимметричных механизмов, обладающих дополнительным функционалам*

* *За исключением схем для одновременного формирования подписи и шифрования*

Содержание

Схемы подписи на основе идентификаторов

Что за механизм?

- механизм позволяет произвести вычисление ключа подписи на основе ключа проверки подписи

  (в классическом случае ключ проверки вычисляется на основе ключа подписи)

- ключ проверки подписи может представлять из себя «осмысленную» информацию

Как реализовать?

- необходим особый участник, который на основе информации пользователя и своего секретного ключа сформирует ключ подписи для пользователя
- для того, чтобы стать субъектом схемы подписи необходимо обратится к особому участнику и выработать ключ подписи

Схемы подписи на основе идентификаторов

Существующие подходы к синтезу

- Наиболее распространенный синтезный подход заключается в использовании билинейных отображений. Однако, использование билинейных отображений требует «аккуратности»
- Известны две (почти одинаковые) схемы на основе схемы Шнорра
- Не известно схем на основе ECDSA
- Возможно построение схемы на основе ГОСТ

Схемы подписи на основе идентификаторов

Формирование ключа подписи

Вход: «мастер ключ» d, информация $\mathtt{id}$

1: Вычислить $h_1 = \mathrm{H}(\mathtt{id})$
2: Выбрать $k_1 \in_R \{1, 2, \ldots, q-1\}$
3: Вычислить $R_1 = k_1 P$
4: Вычислить $r_1 = (R_1)_x \bmod q$
5: Вычислить $d_{\mathtt{id}} = r_1 d + k_1 h_1 \bmod q$

Выход: ключ пользователя $(d_{\mathtt{id}}, R_1)$

Что произошло?

- подписали с использованием «мастер ключа» идентифицирующую информацию пользователя

Схемы подписи на основе идентификаторов

Формирование подписи

Вход: ключ $d_{\mathtt{id}}$, информация $\mathtt{id}$, сообщение m

1: Вычислить $h_2 = \mathrm{H}(m \| \mathtt{id})$
2: Выбрать $k_2 \in_R \{1, 2, \ldots, q-1\}$
3: Вычислить $R_2 = k_2 P$
4: Вычислить $r_2 = (R_2)_x \bmod q$
5: Вычислить $s = r_2 d_{\mathtt{id}} + k_2 h_2 \bmod q$

Выход: подпись (s, R_1, R_2)

Проверка подписи

Вход: ключ Q, информация $\mathtt{id}$, сообщение m, подпись (s, R_1, R_2)

1: Вычислить $h_1 = \mathrm{H}(\mathtt{id})$
2: Вычислить $h_2 = \mathrm{H}(m \| \mathtt{id})$
3: Вычислить $r_1 = (R_1)_x \bmod q$
4: Вычислить $r_2 = (R_2)_x \bmod q$
5: Вычислить $S = r_1 r_2 Q + r_2 h_1 R_1 + h_2 R_2$
6: **Если** $S = sP$ **то** подпись верна
7: **иначе** отвергнуть подпись

Что произошло?

- при формировании подписи, подписали с использованием «подписи»
- при проверке, последовательно верифицируются две подписи
- возможно перейти от R_1, R_2 к r_1, r_2

Содержание

Одновременне формирование подписи и шифрование

Что за механизм?

- механизм предназначен одновременного зашифрования информации и обеспечения ее аутентичности при ее передаче между **A** и **B**
- можно решить использовать KEM или протокол Диффиа-Хеллмана, но потребуется больше ключей

Недостатки

- чтение назад, в случае, если секретный ключ **A** станет известным
- не возможно верифицировать сообщение без секретного ключа **B**

Существующие подходы к синтезу

- на основе уравнения Эль-Гамаля из схемы подписи (EC)DSA
- известны схемы на основе уравнения Шнорра

Одновременне формирование подписи и шифрование

Формирование подписи

Вход: ключи d_A, Q_B и сообщение m

1: Выбрать $k \in_R \{1, 2, \ldots, q-1\}$
2: Вычислить $R = kP = (r_x, r_y)$
3: Вычислить $K = kQ_B = (k_x, k_y)$
4: Вычислить $c = E_{k_x}(m)$
5: Вычислить $e = \mathrm{H}(m)$
6: Вычислить $s = d_A - r_x^{-1} ek \bmod q$

Выход: c – шифртекст и (R, s) – подпись

Проверка подписи

Вход: ключи d_B, Q_A, шифртекст c и подпись (R, s)

1: Вычислить $K = d_B R = (k_x, k_y)$.
2: Вычислить $m' = D_{k_x}(c)$.
3: Вычислить $e = \mathrm{H}(m')$.
4: **Если** $sP + r_x^{-1} eR = Q_A$ **то** принять m'
5: **иначе** отвергнуть m'.

Что здесь с недостатками?

- чтение назад в случае публикации секретного ключа **A** невозможно
- возможна верификация без публикации секретного ключа **B**

Спасибо за внимание