Московский институт электроники и математики им. А.Н. Тихонова

Кафедра информационной безопасности киберфизических систем

Москва 2024

# Криптографические методы защиты информации

ГОСТ Р 34.10-2012

# Стандарты электронной подписи

- **ГОСТ Р 34.10-94**. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма (устаревший):
  - схема подписи реализуется над $F_p$;
  - длина подписи 512 бит;
  - хэш-функция ГОСТ Р 34.11-94.
- **ГОСТ Р 34.10-2001**. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи (устаревший):
  - схема подписи реализуется над $E_{a,b}(F_p)$;
  - длина подписи 512 бит;
  - хэш-функция ГОСТ Р 34.11-94.
- **ГОСТ Р 34.10-2012**. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи:
  - схема подписи реализуется над $E_{a,b}(F_p)$;
  - длина подписи 512 бит или 1024 бита;
  - хэш-функция ГОСТ Р 34.11-2012.

# Основные определения

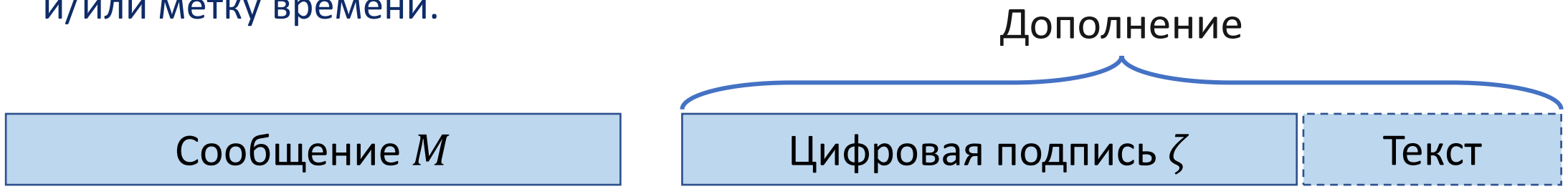
- **Процесс проверки подписи** (verification process) – процесс, в качестве исходных данных которого используются подписанное сообщение, ключ проверки и параметры схемы ЭЦП и результатом которого является заключение о правильности или ошибочности подписи.
- **Процесс формирования подписи** (signature process) – процесс, в качестве исходных данных которого используются сообщение, ключ подписи и параметры схемы ЭЦП, а в результате формируется цифровая подпись.
- **Ключ подписи** (signature key) – элемент секретных данных, специфичный для субъекта и используемый только данным субъектом в процессе формирования цифровой подписи.
- **Ключ проверки** (verification key) – элемент данных, математически связанный с ключом подписи и используемый проверяющей стороной в процессе проверки цифровой подписи.

# Основные определения

- **Хэш-функция** (hash-function) – функция, отображающая строки бит в строки бит фиксированной длины и удовлетворяющая следующим свойствам:
  1) по данному значению хэш-функции сложно вычислить исходные данные, отображенные в это значение;
  2) для заданных исходных данных трудно найти другие исходные данные, отображаемые с тем же результатом;
  3) трудно найти какую-либо пару исходных данных с одинаковым значением хэш-функции.

# Основные свойства подписи

- Цифровая подпись позволяет:
  - осуществить контроль целостности передаваемого подписанного сообщения,
  - доказательно подтвердить авторство лица, подписавшего сообщение,
  - защитить сообщение от возможной подделки
- Подписанное сообщение:
  - Поле «Текст» может содержать идентификаторы субъекта, подписавшего сообщение, и/или метку времени.



# Параметры схемы цифровой подписи

- Простое число $p$ – модуль эллиптической кривой.
- Эллиптическая кривая $E$, задаваемая своим инвариантом $J(\mathrm{E})$ или коэффициентами $a$, $b$.
- Целое число $m$ – порядок группы точек эллиптической кривой $E$, такое, что
  - $p + 1 - 2\sqrt{p} \leq m \leq p + 1 + 2\sqrt{p}$.
- Простое число $q$ – порядок циклической подгруппы группы точек эллиптической кривой $E$, для которого выполнены следующие условия:
  - $\begin{cases} m = nq, n \in \mathbb{N}, \\ 2^{254} < q < 2^{256} \text{ или } 2^{508} < q < 2^{512}. \end{cases}$
- Точка $P \neq \mathrm{O}$ эллиптической кривой $E$, с координатами $(x_P, y_P)$, удовлетворяющая равенству $qP = O$.
- Хэш-функция $h(\cdot): V^* \to V_l$, $l = 256, 512$.
- Ключ подписи — целое число $d$.
- Ключ проверки — точка эллиптической кривой $Q = dP$.

# Алгоритм формирования подписи

1. Вычислить хэш-код сообщения $M$ : $\overline{h} = h(M)$.
2. Вычислить целое число $a$, двоичным представлением которого является вектор $\overline{h}$, и определить
$$e = a \pmod q.$$
Если $e = 0$, то определить $e = 1$.
3. Сгенерировать случайное целое число $k$, удовлетворяющее неравенству
$$0 < k < q.$$
4. Вычислить точку эллиптической кривой $C = kP$ и определить
$$r = x_C \pmod q.$$
Если $r = 0$, то вернуться к шагу 3
5. Вычислить значение
$$s = (rd + ke) \pmod q.$$
Если $s = 0$, то вернуться к шагу 3.
6. Вычислить двоичные векторы, соответствующие числам $r$ и $s$, и определить цифровую подпись $\zeta = \overline{r} \parallel \overline{s}$ как конкатенацию данных двоичных векторов.

# Алгоритм проверки подписи

1. По полученной подписи $\zeta$ вычислить целые числа $r$ и $s$. Если выполнены неравенства $0 < r < q$, $0 < s < q$, то перейти к следующему шагу. В противном случае подпись неверна.
2. Вычислить хэш-код сообщения $M$:
$$\overline{h} = h(M).$$
3. Вычислить целое число $a$, двоичным представлением которого является вектор $\overline{h}$, и определить
$$e = a \pmod q.$$
Если $e = 0$, то определить $e = 1$.
4. Вычислить значение $v = e^{-1} \pmod q$.
5. Вычислить значения
$$z_1 = sv \pmod q, z_2 = -rv \pmod q.$$
6. Вычислить точку эллиптической кривой $C = z_1P + z_2Q$ и определить
$$R = x_C \pmod q.$$
7. Если выполнено равенство $R = r$, то подпись принимается, в противном случае, подпись неверна.

# Пример вычисления подписи

- Модуль эллиптической кривой: $p = 97, 78 \leq \left|E_{a,b}\right| \leq 118.$
- Коэффициенты эллиптической кривой: $a = 9, b = 3.$
- Порядок группы точек эллиптической кривой: $\left|E_{9,3}\right| = 94 = 2 \cdot 47.$
- Порядок циклической подгруппы: $q = 47.$
- Точка $P \in E_{9,3}$ порядка $q$: $P = (-8, 1).$

- Ключевая пара: $d = 5, Q = 5P = (-47, -41).$

# Пример вычисления подписи

- Алгоритм формирования подписи:
  1. Хэш-код сообщения $M$: $h = h(M) = 101010;$
  2. Десятичное представление $h(M)$: $a = 42, e = 42 \pmod{47} = 42;$
  3. Случайное целое число $k$: $k = 18;$
  4. Точка эллиптической кривой $C = kP$: $C = 18P = (12,\ 44), r = 12 \pmod{47} = 12;$
  5. Значение $s$: $s = (12 \cdot 5 + 18 \cdot 42) \pmod{47} = 17.$
  6. Двоичные векторы $\bar{r}$ и $\bar{s}$ : $\bar{r} = 001100$ и $\bar{s} = 010001,$

- Подпись: $\xi = \bar{r}||\bar{s} = 001100||010001 = 001100010001.$

# Пример вычисления подписи

- Алгоритм проверки подписи:
  1. Целые числа $r$ и $s$: $r = 12, s = 17;$
  2. Хэш-код сообщения $M$: $h = h(M) = 101010;$
  3. Десятичное представление $h(M)$: $a = 42, e = 42 \pmod{47} = 42;$
  4. Значение $v$: $v = 42^{-1} \pmod{47} = 28;$
  5. Значения $z_1$ и $z_2$: $z_1 = 17 \cdot 28 \pmod{47} = 6;$
     $z_2 = -12 \cdot 28 \pmod{47} = 40;$
  6. Точка эллиптической кривой $C$: $C = 6P + 40Q = (12, 44);$
     $6P = (20, 36); 40Q = (-29, 31);$
     $R = 12 \pmod{47} = 12$
  7. Подпись верна, так как $R = r$.

# Спасибо за внимание!

**Евсютин Олег Олегович**
Заведующий кафедрой информационной безопасности киберфизических систем
Канд. техн. наук, доцент

+7 923 403 09 21
oevsyutin@hse.ru