Представления точек на эллиптических кривых

Захаров П.С., Пискун М.Г.

2018

План доклада

- Алгебра точек на эллиптических кривых
- Эллиптические кривые в криптографии
- Представления точек на эллиптических кривых
- Постановка эксперимента
- Результаты

Эллиптические кривые

Общий вид:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Форма Вейерштрасса:

$$y^2 = x^3 + ax + b,\ a, b, x, y \in K$$

1.1 Алгебра точек на эллиптических кривых

Групповые операции

Пусть $P = (x_P, y_P), Q = (x_Q, y_Q) \in E, P \neq \pm Q$

Сложение:

$$x_R = \left(\frac{y_Q - y_P}{x_Q - x_P} \right)^2 - x_P - x_Q,$$

Удвоение:

$$y_R = \left(\frac{y_Q - y_P}{x_Q - x_P} \right)(x_P - x_R) - y_P$$

Дискретный логарифм на эллиптических кривых

Пусть E - кривая над полем K, $G \in E$.

Задачей дискретного логарифмирования на E называется нахождение для данной

$P \in E \; a \in \mathbb{F}_q : P = aG$ (если существует)

Криптографические алгоритмы и системы на эллиптических кривых

- ECDSA – цифровая подпись
- ECDH – переложение протокола Диффи-Хеллмана
- Переложение криптосистемы Эль-Гамаля
- Криптосистема Месси-Омуры

2.2 Эллиптические кривые в криптографии

ECDSA

Пусть $m = h(M)$ – хэш сообщения,

k – случайное число из $[1, q-1]$,

P – генератор подгруппы с порядком q

$$C = kP = (x_c, y_c)$$
$$r = x_c \bmod q$$
$$s = k^{-1}(m + rd)$$
$$(r, s) - \text{подпись}$$

$$v_1 = s^{-1}h \bmod q$$
$$v_2 = s^{-1}r \bmod q$$
$$v_1 P + v_2 Q = (x_b, y_b)$$
$$\hat{r} = x_b$$

Представления точек

- Афинные координаты
- Стандартные проективные координаты
- Координаты Якоби

3.1 Представления точек на эллиптических кривых

Проективные координаты

Пусть $c, d \in \mathbb{Z},\ c, d > 0$, и

$$(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2) \Leftrightarrow \exists\, \lambda \in K:$$

$$X_1 = \lambda^c X_2, Y_1 = \lambda^d Y_2, Z_1 = \lambda Z_2$$

Для каждого класса эквивалентности S выполняется одно из:

1) $\forall\, (X, Y, Z) \in S\ \ Z = 0$
2) $\exists\, (X, Y, Z) \in S: Z = 1$

Стандартные проективные координаты: $c = 1, d = 1$

Уравнение кривой: $Y^2Z = X^3 + aX^2Z + bZ^3$

Формула сложения: Пусть

$$M = Y_Q Z_P - Y_P Z_Q, N = X_Q Z_P - X_P Z_Q$$

$$X_R = NM^2 Z_P Z_Q - N^3 (X_P Z_Q + X_Q Z_P)$$

$$Y_R = M\left(N^2\left(2 * X_P Z_Q + X_Q Z_P\right) - M^2 Z_P Z_Q\right) - Y_P Z_Q N^3$$

$$Z_R = N^3 Z_P Z_Q$$

Формула сложения: Пусть

$$M = 3X_P^2 + aZ_P^2, N = 2Y_P Z_P$$

$$X_R = M^2 N - 4N^2 X_P Y_P$$

$$Y_R = 6X_P Y_P MN - M^3 - 2N^2 Y_P^2$$

$$Z_R = N^3$$

3.3 Представления точек на эллиптических кривых

Координаты Якоби: $c = 2, d = 3$

Уравнение кривой: $Y^2 = X^3 + aXZ^4 + bZ^6$

Формула сложения: Пусть

$$M = Y_Q Z_P^3 - Y_P Z_Q^3, N = X_Q Z_P^2 - X_P Z_Q^2$$

$$X_R = M^2 - N^2\left(X_P Z_Q^2 + X_Q Z_P^2\right)$$

$$Y_R = MN^2(2X_P Z_Q^2 + X_Q Z_P^2) - M^3 - Y_P Z_Q^3 N^3$$

$$Z_R = NZ_P Z_Q$$

Формула сложения:

$$X_R = (3X_P^2 + aZ_P^4)^2 - 8X_P Y_P^2$$

$$Y_R = (3X_P^2 + aZ_P^4)(4X_P Y_P^2 - X_R) - 8Y_P^4$$

$$Z_R = 2Y_P Z_P$$

Вычислительный эксперимент

- Измеряется время:
  - 100 000 операций сложения
  - 100 000 операций удвоения
  - 1000 циклов создания и проверки ЭП протокола ECDSA
- 3 представления
- 5 кривых

Используемые кривые

Эллиптич. кривая	Характеристика поля p	Длина p в битах
secp192r1	$2^{192} - 1$	192
secp224r1	$2^{224} - 2^{96} + 1$	224
secp256r1	$2^{224}(2^{32} - 1) + 2^{192} + 2^{96} - 1$	256
secp384r1	$2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$	384
secp521r1	$2^{521} - 1$	521

4.2 Вычислительный эксперимент

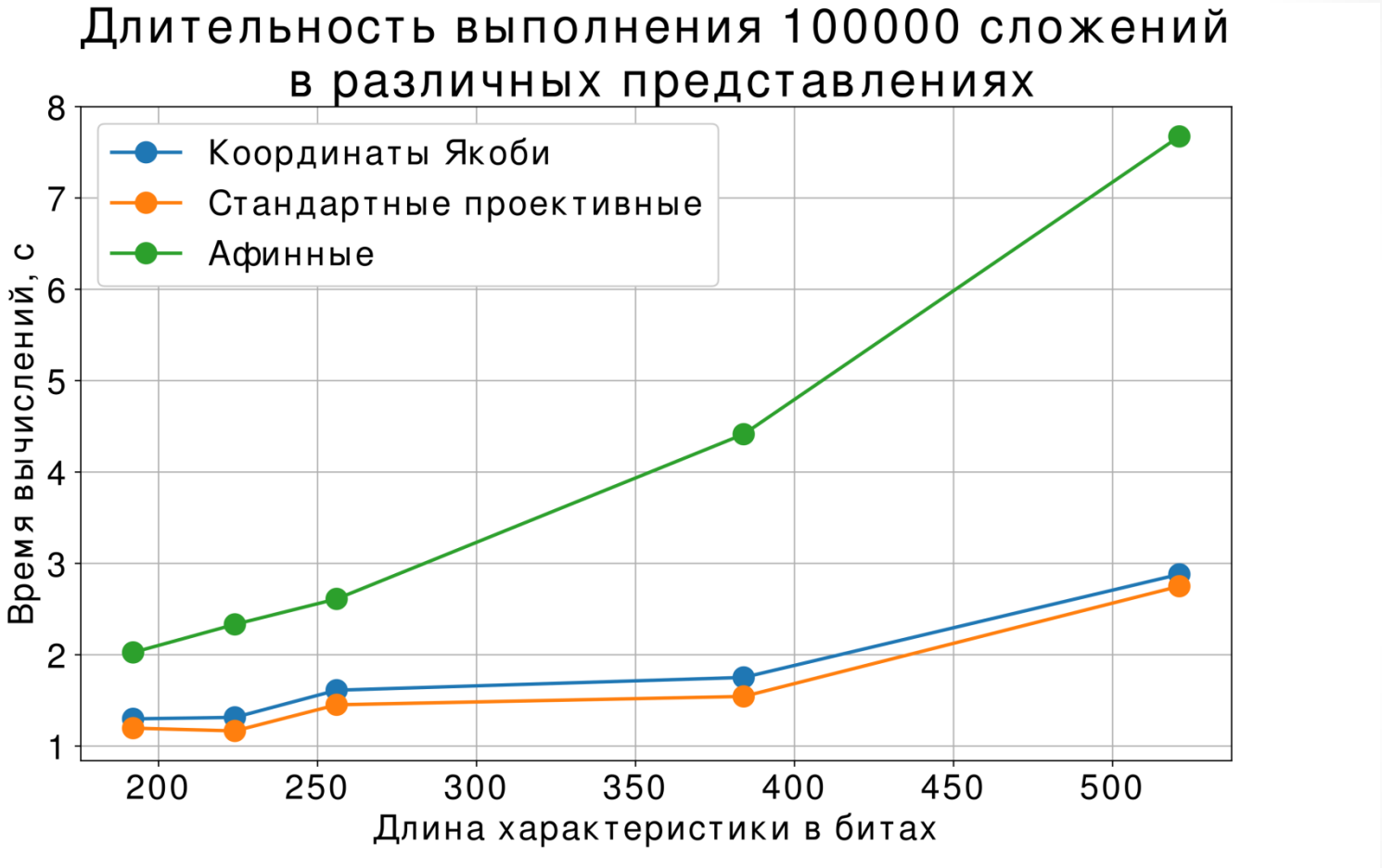
Результаты

Время выполнения 100000 сложений точек, сек.

Эллиптич. кривая	**Представление точек**		
	Стандартное представление	Стандартные проективные координаты	Координаты Якоби
secp192r1	2.0253	1.1964	1.2983
secp224r1	2.3322	1.1659	1.3144
secp256r1	2.6110	1.4522	1.6116
secp384r1	4.4141	1.5437	1.7516
secp521r1	7.6734	2.7499	2.8803

5.1 Результаты

Результаты



5.1 Результаты

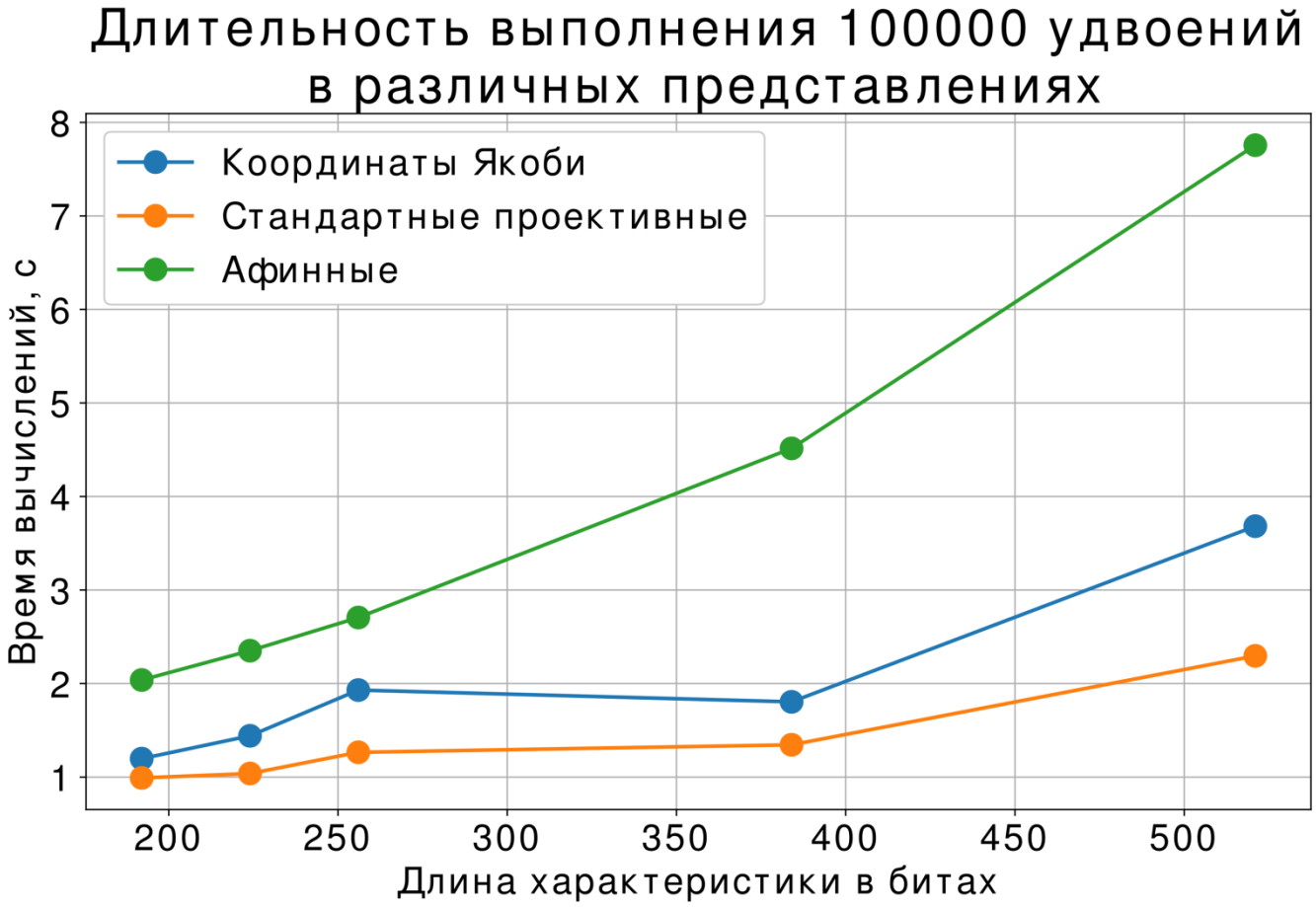
Результаты

Время выполнения 100000 удвоений точки, сек.

Эллиптич. кривая	**Представление точек**		
	Стандартное представление	Стандартные проективные координаты	Координаты Якоби
secp192r1	2.0380	0.991167	1.1971
secp224r1	2.35125	1.03813	1.4413
secp256r1	2.7061	1.2649	1.9303
secp384r1	4.51443	1.3450	1.8044
secp521r1	7.756	2.2959	3.6825

5.2 Результаты

Результаты



5.2 Результаты

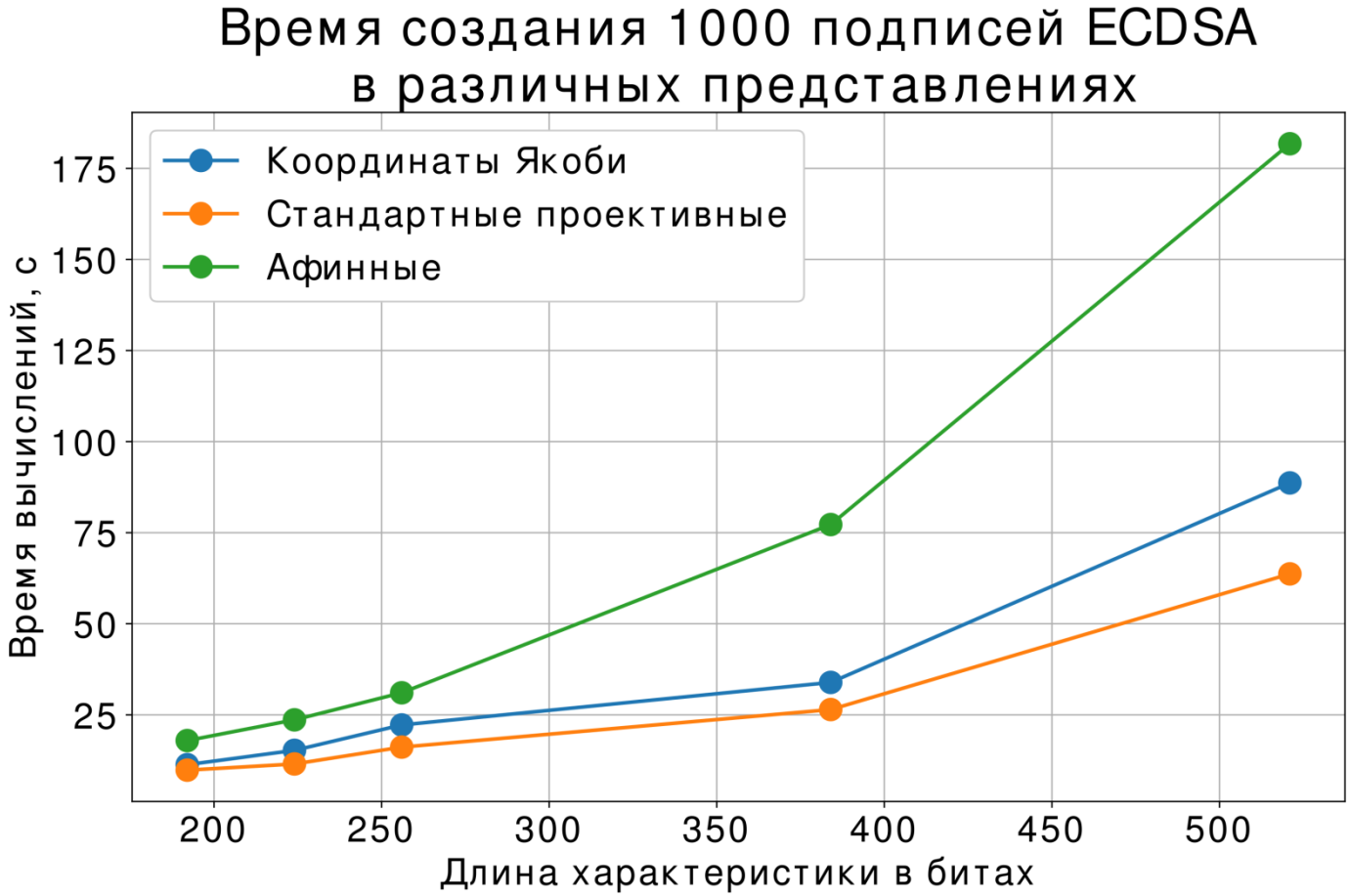
Результаты

Время выполнения 1000 циклов «создание-проверка подписи», сек.

Эллиптич. кривая	**Представление точек**		
	Стандартное представление	Стандартные проективные координаты	Координаты Якоби
secp192r1	17.9406	9.82302	11.3276
secp224r1	23.6296	11.5241	15.2622
secp256r1	31.0576	16.1472	22.2321
secp384r1	77.2325	26.4536	33.9038
secp521r1	181.749	63.6901	88.6589

5.3 Результаты

Результаты



5.3 Результаты

Ссылки

- Репозиторий проекта: https://github.com/PaulZakharov/elcurves_2018
- Hankerson D., Menezes A., Vanstone S. - Guide to Elliptic Curve Cryptography. New York: Springer-Verlag, 2004 311 P.
- Коблиц Н. Курс теории чисел и криптографии. – М.: Научное издательство ТВП, 2001. – 254 С.
- Владимиров С.М. [и др.] – Криптографические методы защиты информации. – М.: МФТИ, 2016. – 266 С.