О перспективах использования скрученных эллиптических кривых Эдвардса со стандартом ГОСТ Р 34.10-2012 и алгоритмом ключевого обмена на его основе

Алексеев Е.К.
Ошкин И.Б., Попов В.О., Смышляев С.В., Сонина Л.А.

ГОСТ 34.10-2012 и кривые Вейерштрасса

Стандарт ЭП ГОСТ 34.10-2012 требует, чтобы результаты преобразований, связанных с точками эллиптических кривых, были представлены в аффинных координатах на кривой Вейерштрасса.

Использование различных представлений для кривых

Отсутствие требования простоты порядка используемой группы точек эллиптической кривой дает возможность использовать кривые в различных формах.

Использование различных координат

Производительность вычислений увеличивается за счет представления точек в неаффинных координатах. Работа в неаффинных координатах также обусловлена требованиями к построению защищенных программных продуктов.

КРИПТО ПРО

Формы кривых

- Кривая Вейерштрасса
- Кривая Эдвардса
- Скрученная кривая Эдвардса
- Кривая Хессе
- Скрученная кривая Хессе
- Кривая Монтгомери
- Пересечения Якоби
- Квартики Якоби

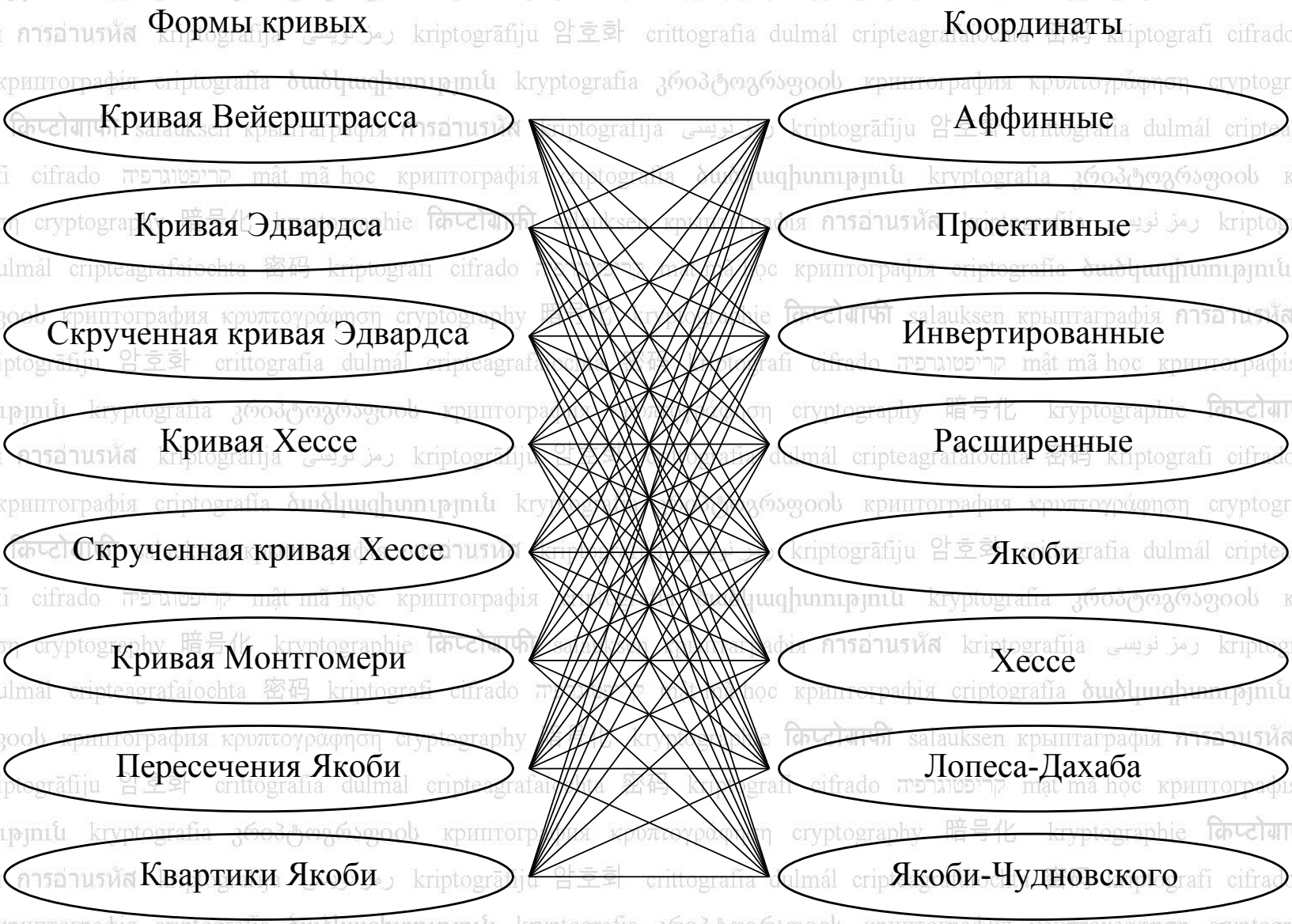
КРИПТО ПРО

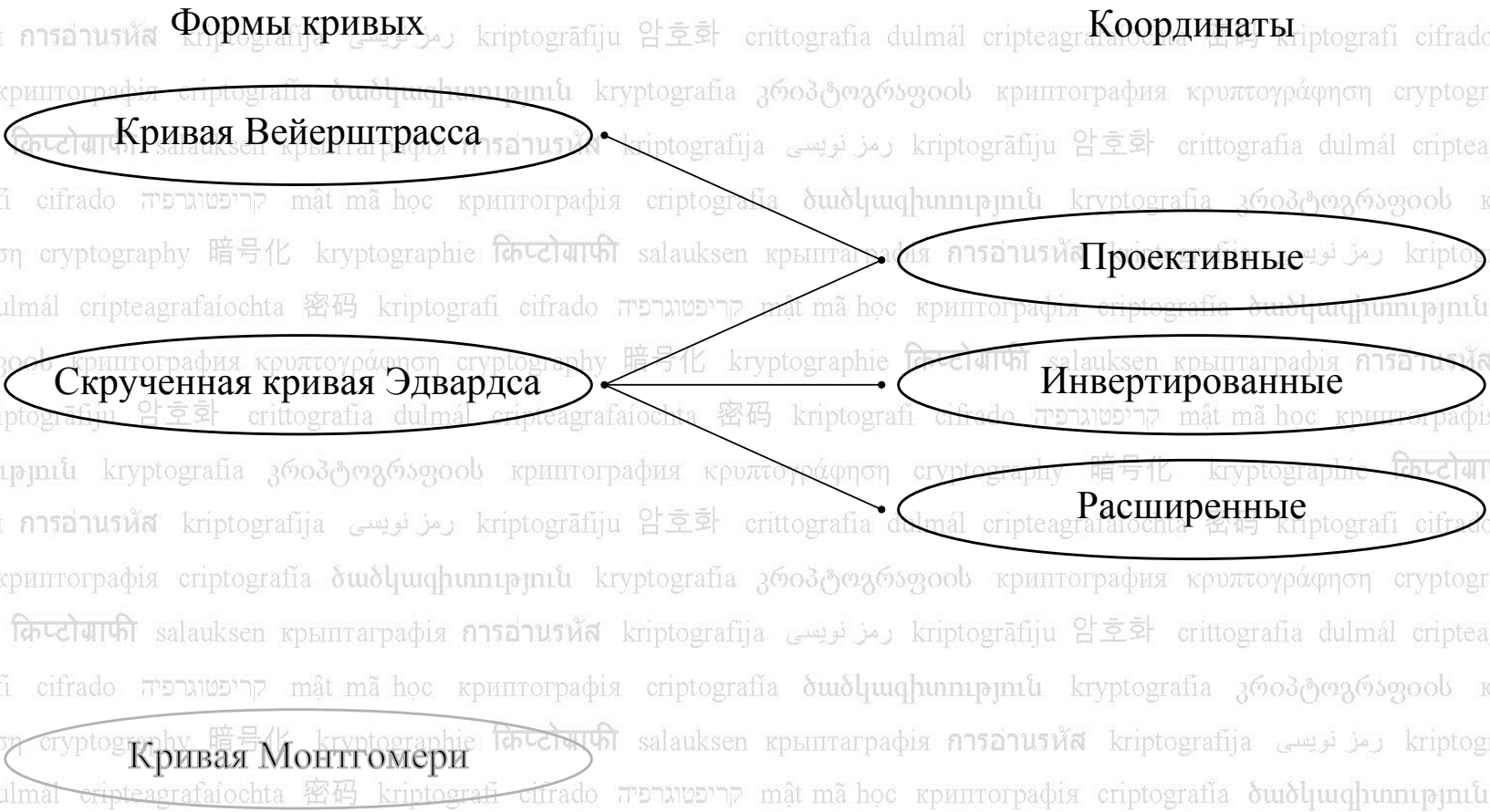
Формы кривых

- Кривая Вейерштрасса
- Кривая Эдвардса
- Скрученная кривая Эдвардса
- Кривая Хессе
- Скрученная кривая Хессе
- Кривая Монтгомери
- Пересечения Якоби
- Квартики Якоби

Координаты

- Аффинные
- Проективные
- Инвертированные
- Расширенные
- Якоби
- Хессе
- Лопеса-Дахаба
- Якоби-Чудновского





КРИПТО ПРО

Кривые:

- Кривая Вейерштрасса: $\{(x, y)|y^2 = x^3 + ax + b\}$
- Скрученная кривая Эдвардса: $\{(x, y)|\varepsilon x^2 + y^2 = 1 + \delta x^2 y^2\}$
- Кривая Монтгомери: $\{(x, y)|By^2 = x^3 + Ax^2 + x\}$

Координаты:

- Аффинные $(\mathcal{A})$: $(x_{\mathcal{A}}, y_{\mathcal{A}})$
- Проективные $(\mathcal{P})$: $(X_{\mathcal{P}}, Y_{\mathcal{P}}, Z_{\mathcal{P}})$, где $x_{\mathcal{A}} = \frac{X_{\mathcal{P}}}{Z_{\mathcal{P}}}$, $y_{\mathcal{A}} = \frac{Y_{\mathcal{P}}}{Z_{\mathcal{P}}}$
- Инвертированные $(\mathcal{I})$: $(X_{\mathcal{I}}, Y_{\mathcal{I}}, Z_{\mathcal{I}})$, где $x_{\mathcal{A}} = \frac{Z_{\mathcal{I}}}{X_{\mathcal{I}}}$, $y_{\mathcal{A}} = \frac{Z_{\mathcal{I}}}{Y_{\mathcal{I}}}$
- Расширенные $(\mathcal{E})$: $(X_{\mathcal{E}}, Y_{\mathcal{E}}, Z_{\mathcal{E}}, T_{\mathcal{E}})$, где $x_{\mathcal{A}} = \frac{X_{\mathcal{E}}}{Z_{\mathcal{E}}}$, $y_{\mathcal{A}} = \frac{Y_{\mathcal{E}}}{Z_{\mathcal{E}}}$, $x_{\mathcal{A}} \cdot y_{\mathcal{A}} = \frac{T_{\mathcal{E}}}{Z_{\mathcal{E}}}$

КРИПТО ПРО

Кривые Вейерштрасса

$y^2 = x^3 + ax + b$

$x^3 + ax + b$ имеет корень в F_p

$3\alpha^2 + a$ - квадратичный вычет в F_p

α - корень $x^3 + ax + b$

$$a = \frac{1}{B^2} - \frac{A^2}{3B^2} \qquad b = \frac{2A^3 - 9A}{27B^3} \qquad x = \frac{X}{B} + \frac{A}{3B} \qquad y = \frac{Y}{B}$$

$$s = \sqrt{\frac{1}{3\alpha^2 + a}} \qquad B = s \qquad A = 3\alpha s \qquad X = s(x - \alpha) \qquad Y = sy$$

$$BY^2 = X^3 + AX^2 + X$$

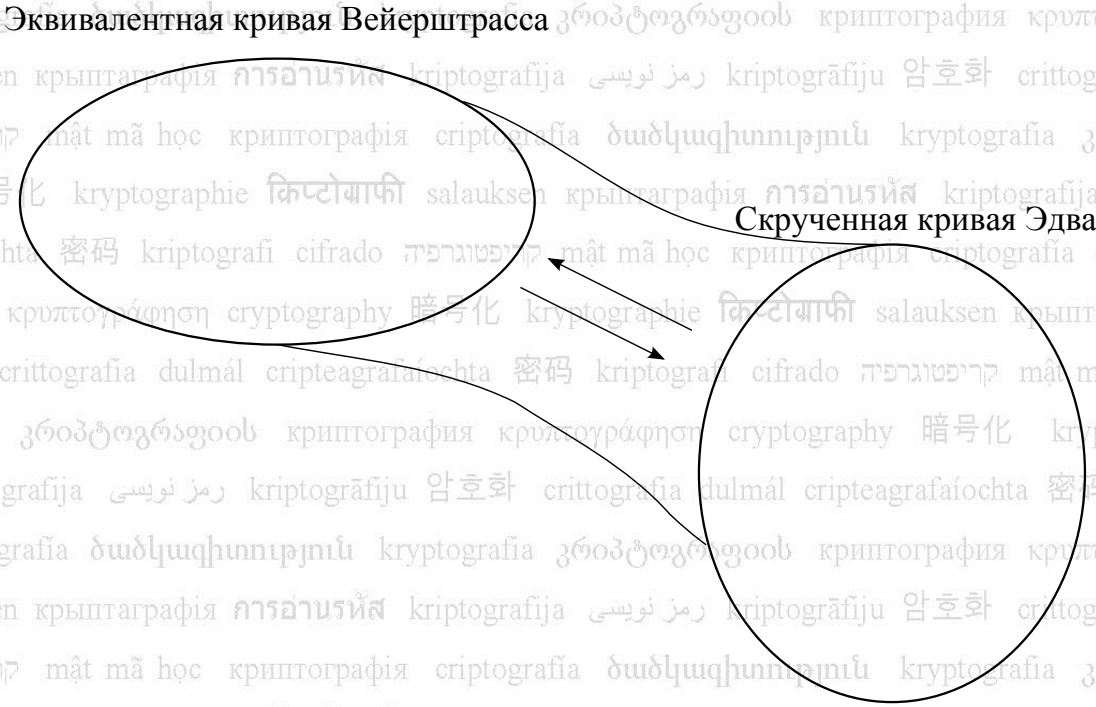
Кривые Монтгомери

$$\varepsilon u^2 + v^2 = 1 + \delta u^2 v^2$$

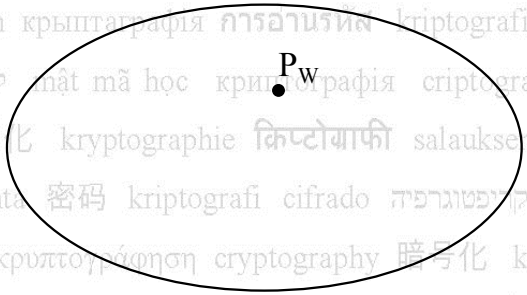
$$\varepsilon = \frac{A+2}{B} \qquad \delta = \frac{A-2}{B} \qquad u = \frac{X}{Y} \qquad v = \frac{X-1}{X+1}$$

$$X = \frac{1+v}{1-v} \qquad Y = \frac{1+v}{(1-v)u} \qquad B = \frac{4}{\varepsilon - \delta} \qquad A = \frac{2(\varepsilon + \delta)}{\varepsilon - \delta}$$

Скрученные кривые Эдвардса



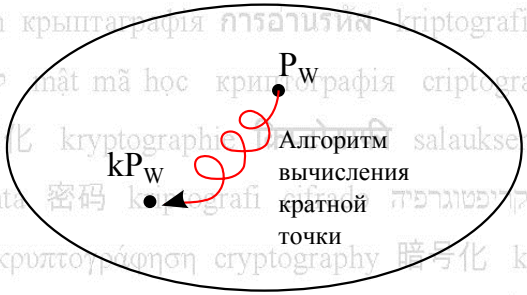
Эквивалентная кривая Вейерштрасса



Скрученная кривая Эдвардса

Задача: по P_W и k вычислить kP_W

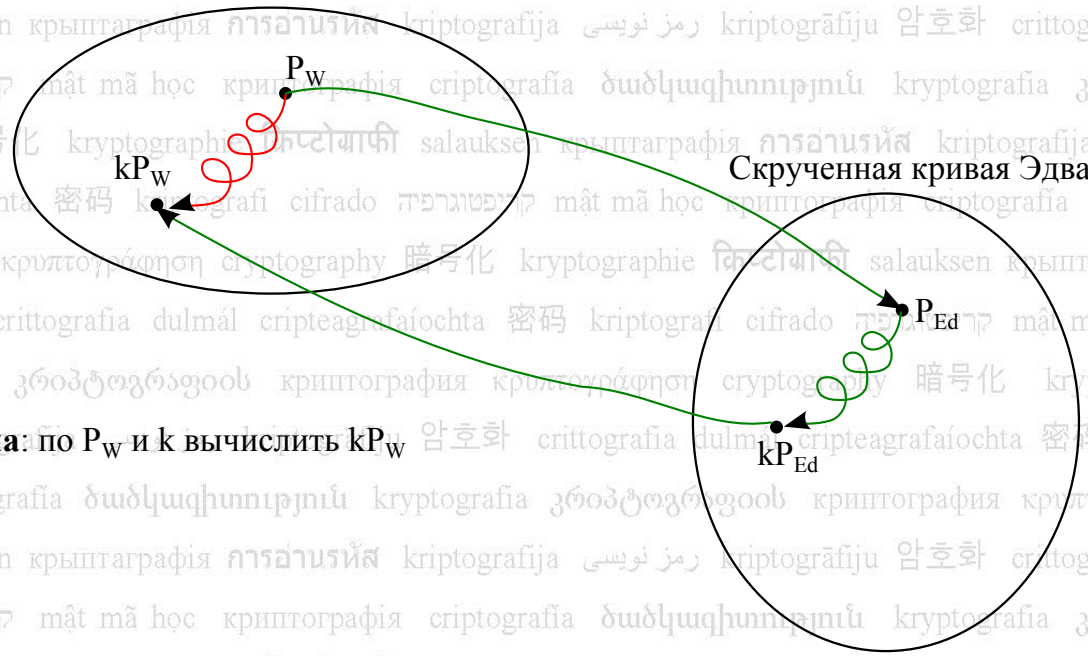
Эквивалентная кривая Вейерштрасса



Скрученная кривая Эдвардса

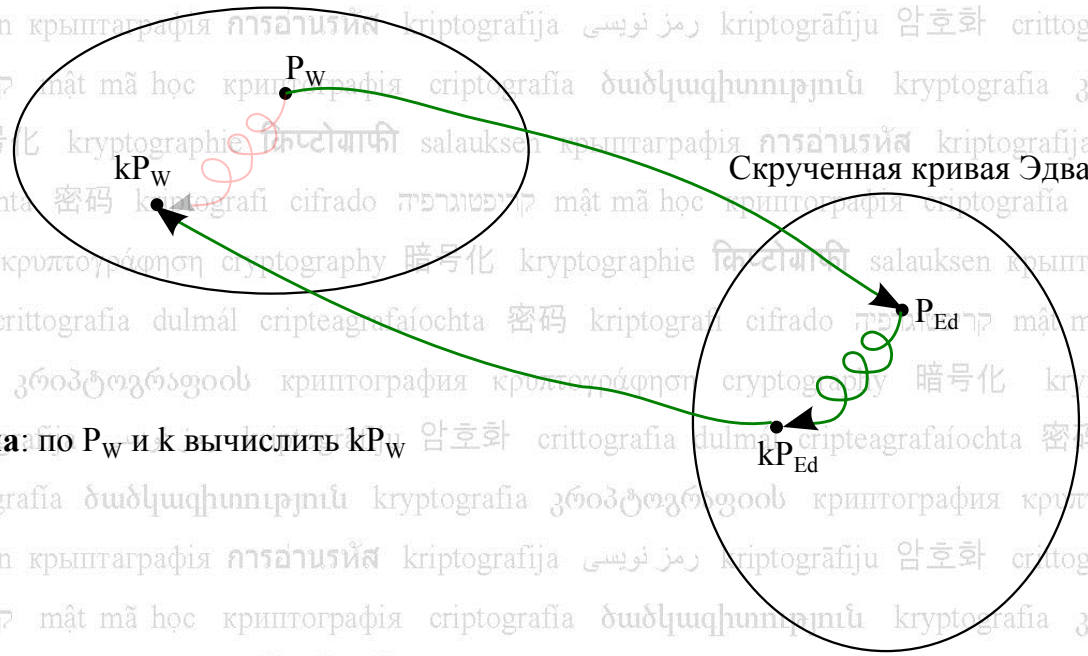
Задача: по P_W и k вычислить kP_W

Эквивалентная кривая Вейерштрасса



Задача: по P_W и k вычислить kP_W

Эквивалентная кривая Вейерштрасса



Задача: по P_W и k вычислить kP_W

КРИПТО ПРО

Обозначения

$x^{W}_{\mathcal{A}}$ — аффинная x-координата точки на кривой Вейерштрасса

$W,\mathcal{P}\to$ — операция перехода от представления в проективных координатах на кривой Вейерштрасса к другому представлению

TE — скрученная кривая Эдвардса

W — кривая Вейерштрасса

Трудоемкость операций

	W, $\mathcal{P}$	TE, $\mathcal{P}$	TE, $\mathcal{I}$	TE, $\mathcal{E}$
Сложение	$12M+2S$	$10M+1S$	$9M+1S$	$9M$
Удвоение	$5M+6S$	$3M+4S$	$3M+4S$	$4M+4S$
$W,\mathcal{P}\to$		$1I+8M$	$1I+8M$	$1I+9M$
Вычисление $x^{W}_{\mathcal{A}}$	$1I+1M$	$1I+2M$	$1I+2M$	$1I+2M$

D.M.Dygin, S.V.Grebnev «Efficient implementation of the GOST R 34.10 digital signature scheme using modern approaches to elliptic curve scalar multiplication».

Исследовалась эффективность реализации операций подписи и проверки подписи на кривых в формах Вейерштрасса, Хессе, Эдвардса и на скрученных кривых Эдвардса.

	Sign-256	Verify-256	Sign-512	Verify-512
Weierstrass, $\mathcal{P}$	1.12	1.43	4.23	5.23
Twisted Edwards, $\mathcal{E}$	0.7	0.98	2.52	3.38

Таблица: Экспериментальные результаты

Криптографические преобразования

Алгоритмы вычисления кратной точки

Операции в группе точек эллиптической кривой

Арифметика в простом конечном поле

КРИПТО ПРО

Реализация с учетом требований по защищенности

Криптографические преобразования

Алгоритмы вычисления кратной точки

Операции в группе точек эллиптической кривой

Арифметика в простом конечном поле

КРИПТО ПРО

Реализация с учетом требований по защищенности

Криптографические преобразования

* создание подписи
* проверка подписи
* согласование ключей

Алгоритмы вычисления кратной точки

* GornerPC
* WTNAF
* FTNAF

Операции в группе точек эллиптической кривой

* Weierstrass, Projective
* Twisted Edwards, Projective
* Twisted Edwards, Inverted
* Twisted Edwards, Extended

Арифметика в простом конечном поле

M=S I=100M

КРИПТО ПРО

Исходные данные

Параметры кривой (в том числе порождающая точка P), ключ подписи d

Алгоритм формирования подписи

- Вход $\leftarrow$ сообщение m
- $h = H(m)$
- $e = h \mod q$
- $k \in_R \{1, 2, \ldots, q-1\}$
- $r = x_{\mathcal{A}}(k \cdot P) \mod q$
- $s = r \cdot d + k \cdot e \mod q$
- Выход $\rightarrow$ подпись $\zeta = (r, s)$

КРИПТО ПРО

Исходные данные

Параметры кривой, порождающая точка P

Алгоритм проверки подписи

- Вход $\leftarrow$ сообщение m, подпись $\zeta = (r, s)$, ключ проверки подписи Q
- $h = H(m)$
- $e = h \mod q$
- $v = e^{-1} \mod q$
- $z_1 = s \cdot v \mod q$, $z_2 = -r \cdot v \mod q$
- $r' = [x_{\mathcal{A}}(z_1 \cdot P + z_2 \cdot Q)] \mod q$
- Выход $\rightarrow$ верно ли, что $r' = r$

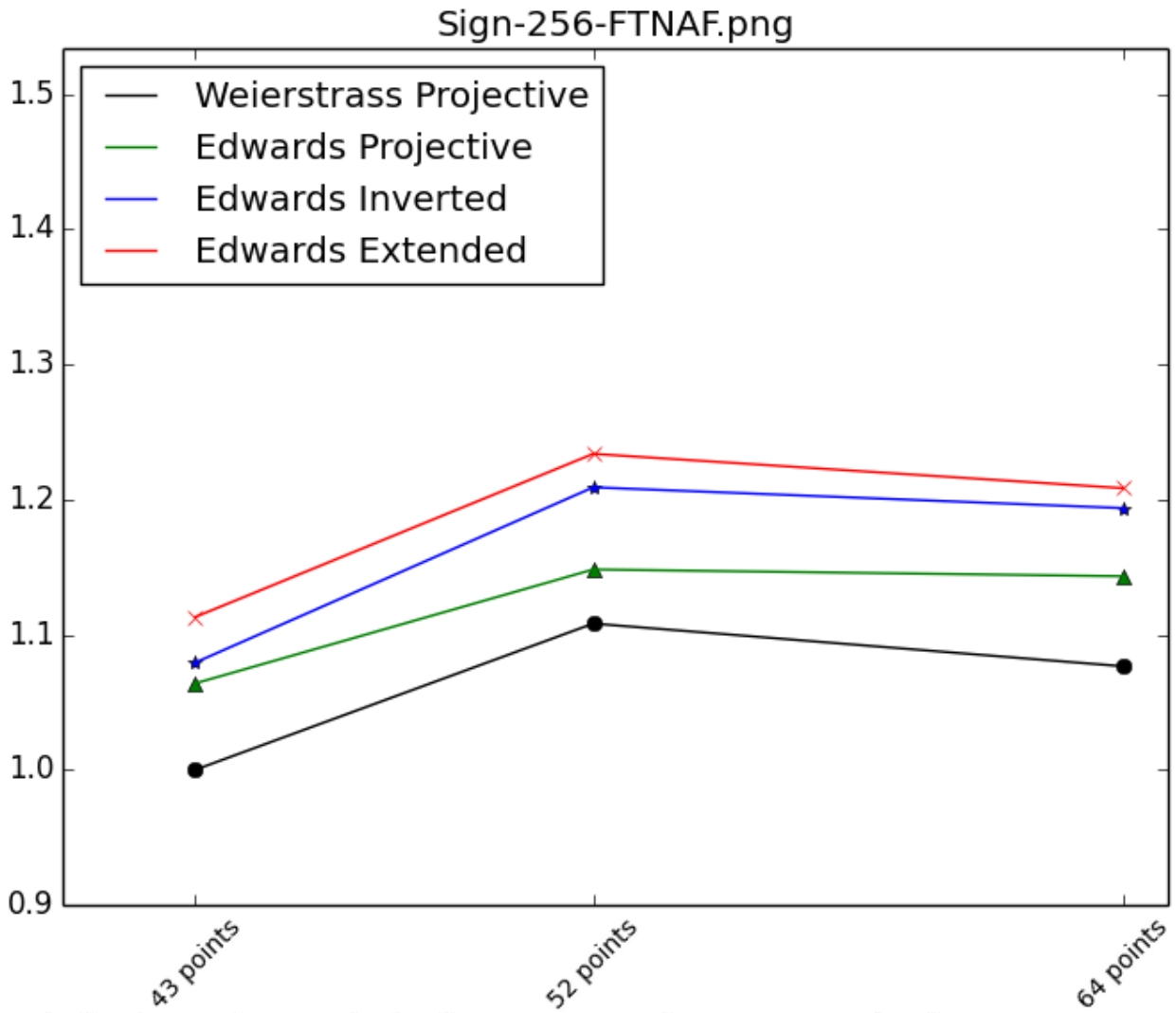
КРИПТО ПРО

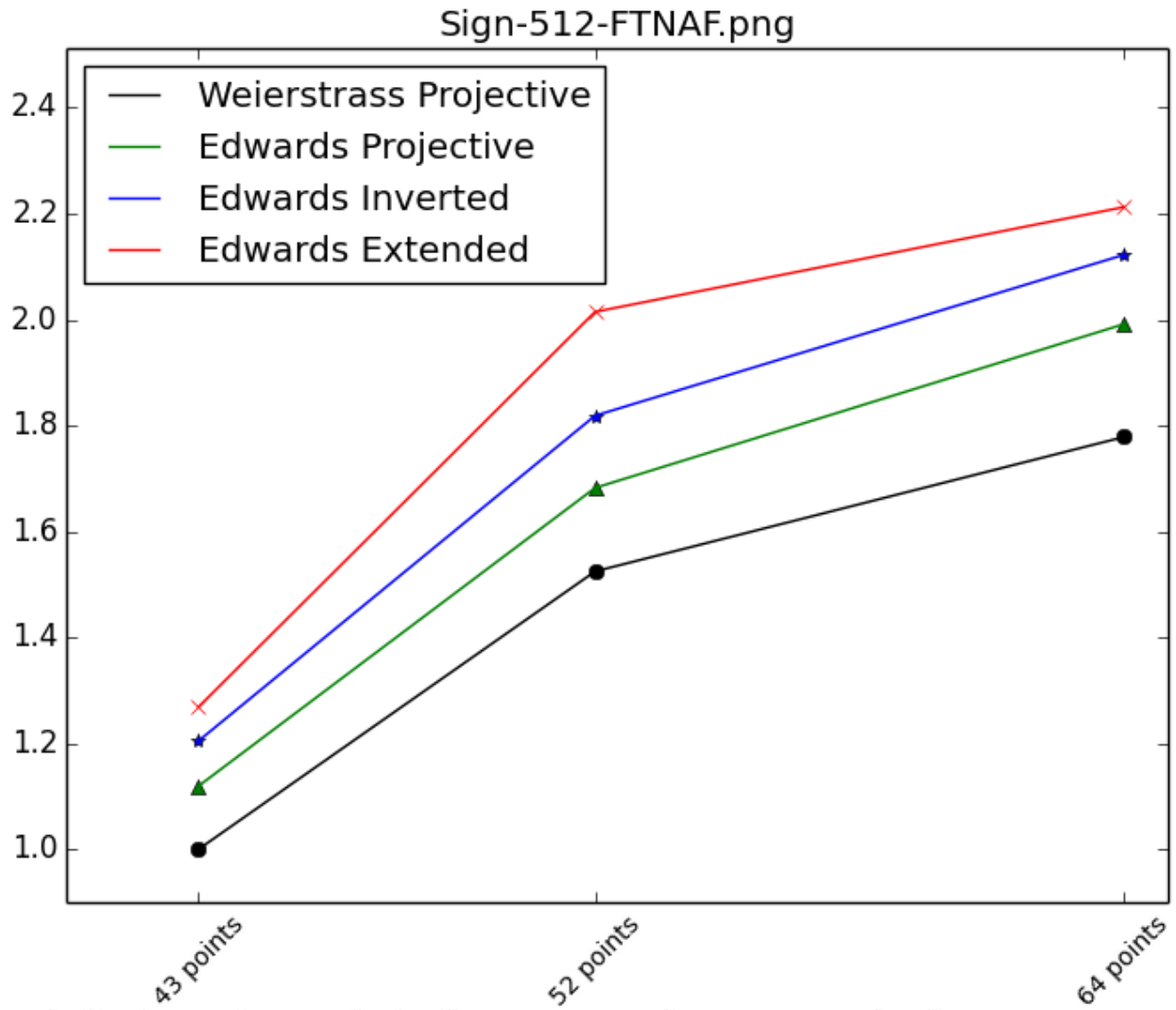
Исходные данные

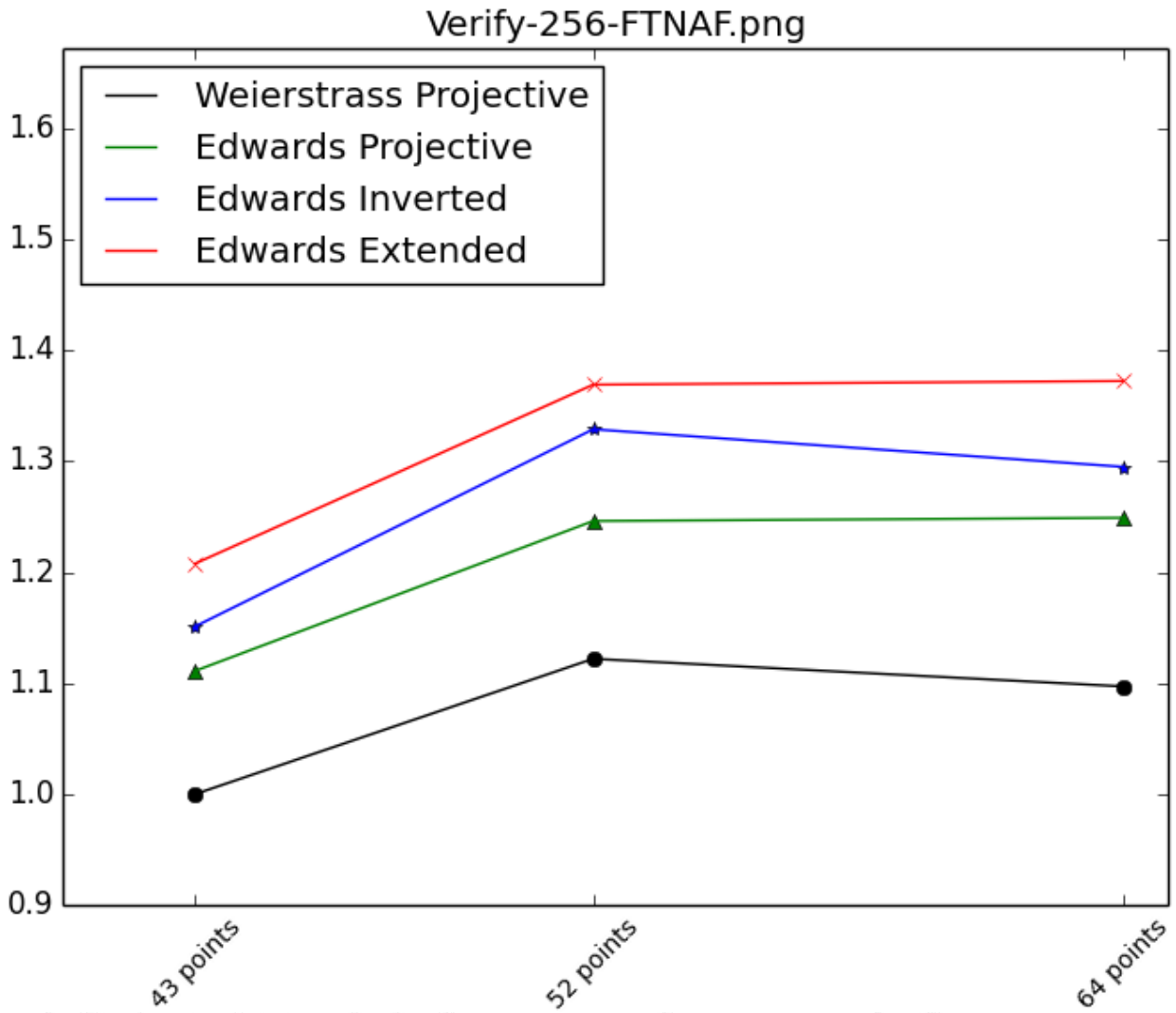
Параметры кривой, порождающая точка P

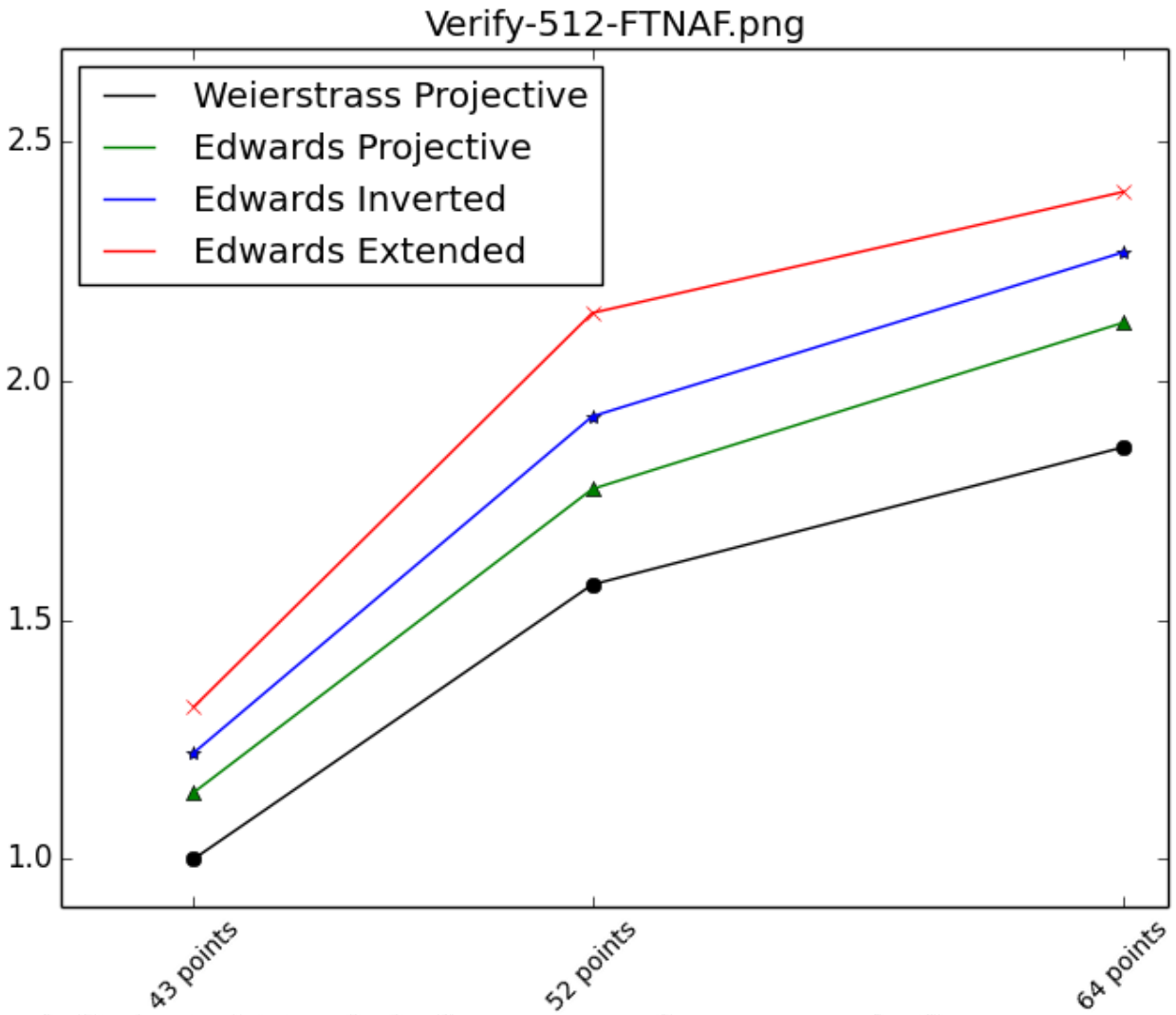
Алгоритм VKO

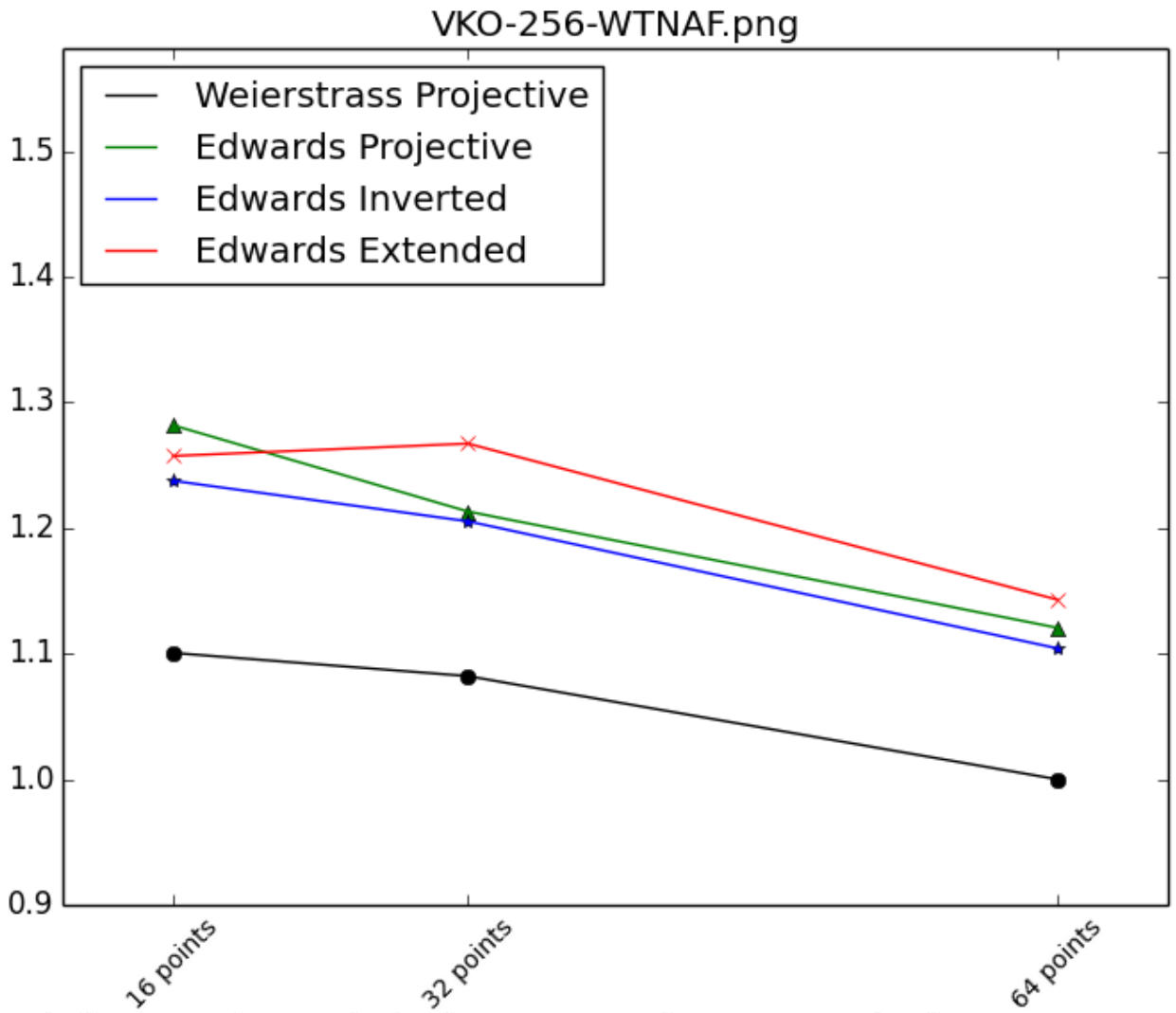
- Вход ← точка Q, UKM
- $V = (UKM \cdot d \mod q) \cdot Q$
- $h = H(V)$
- Выход → h











КРИПТО ПРО

Итоговые соотношения производительностей

Sign-256	Verify-256	VKO-256	Sign-512	Verify-512	VKO-512
+18%	+22%	+14%	+24%	+28%	+22%

КРИПТО ПРО

Закрытые ключи, контейнеры и сертификаты

В некоторых случаях бывает необходимо осуществлять проверку соответствия закрытого ключа, хранящегося в контейнере, открытому ключу, указанному в сертификате. При этом открытый ключ в сертификате хранится в аффинных координатах на кривой Вейерштрасса. Это приводит к тому, что при проверке указанного соответствия приходится делать дополнительное преобразование из одного представления в другое, так как предполагается использование одних координат при основных вычислениях из-за нежелательности хранения предвычисленных таблиц двух типов.

КРИПТО ПРО

Кривые Вейерштрасса простого порядка

Сейчас в основном используются кривые простого порядка в форме Вейерштрасса. Эквивалентные им скрученные кривые в форме Эдвардса могут существовать только над расширенными полями. Увеличение размера элементов поля нивелирует любое преимущество от использование скрученных кривых Эдвардса.

КРИПТО ПРО

Спасибо за внимание!