Современные алгоритмы вычисления кратной точки и суммы кратных точек эллиптической кривой над конечным простым полем и их приложение к реализации схемы электронной цифровой подписи ГОСТ Р 34.10

С. В. Гребнев, Д. М. Дыгин

Исходные положения

В 2011 году были предложены новые варианты государственных стандартов электронной цифровой подписи (ГОСТ Р 34.10-2001) и хэш-функции (ГОСТ Р 34.11-94). В частности, стандарт ЭЦП предлагается дополнить вариантом требований к параметрам, предполагающим использование эллиптических кривых над полями размера порядка 512 бит.

В докладе представлены результаты исследований эксплуатационных характеристик вариантов схемы ЭЦП ГОСТ Р 34.10, реализованных на универсальном процессоре в соответствии с предлагаемыми дополнениями к стандарту.

Схема ЭЦП ГОСТ Р 34.10

- Вариант обобщенной схемы Эль-Гамаля, реализованной в подгруппе простого порядка q группы точек эллиптической кривой в *(краткой) форме Вейерштрасса*

$$E = (x, y) : y^2 = x^3 + ax + b$$

над конечным простым полем из p элементов, где $2^{254} < q < 2^{256}$ или $2^{508} < q < 2^{512}$

- Уравнение подписи: $s = dr + kh(M) \pmod{q}$, где $r = x_{(kP)}$

- Уравнение проверки: $x_{(h(M) \bmod q))P-(rh(M) \bmod q)Q} \pmod{q} = r$

Оптимальная реализация схемы ЭЦП ГОСТ Р 34.10

- Выбор эффективного способа представления элементов поля ($p < 2^{256}$ или $p < 2^{512}$ позволяет использовать минимально возможное количество машинных слов для представления элементов поля, а умножение в поле выполнять с помощью алгоритма Карацубы (gmp));
- выбор эффективного представления показателей кратности;
- выбор эффективного представления точек кривой с учетом того, что после вычисления кратной точки и суммы кратных точек в этом представлении необходимо перейти к (краткой) форме Вейерштрасса

Общая схема алгоритмов вычисления кратной точки

1. Определяется специальное представление показателя k;
2. предварительно вычисляются вспомогательные точки $\pm 3P, \pm 5P, \ldots;$
3. "сканируется" представление показателя, и на каждом шаге выполняется сложение (если цифра отлична от 0) и умножение на одно или несколько оснований.

Задача – построить представление, минимизирующее количество сложений (количество умножений в общем случае определяется битовой длиной числа). Например, в классическом бинарном алгоритме необходимо выполнить $\lfloor \log_2 k \rfloor$ умножений и $w(k)$ сложений, $w(k) \approx \lfloor log_2 k/2 \rfloor$.

Пример

- Двоичное представление:

$$3410_{10} = 110101010010_2;$$

- разреженное знаковое представление:

$$NAF(3410_{10}) = 10\overline{1}0101010010;$$

- разреженное представление с двумя основаниями $(2,3)$ и окном 3:

$$(2,3)NAF_3(3410_{10}) = \left\{1^2 0^3 0^3 0^2 0^2 \overline{1}^2 0^3 0^2 0^2 1^2 0^2\right\}.$$

Существуют и другие способы представления показателей.

Разреженная форма с несколькими основаниями и окном

P. Longa, 2008: *Разреженное представление числа k с несколькими основаниями и окном* $(a_1, \ldots, a_J)NAF_w(k) = \{d_1^{(a_1)} \ldots d_m^{(a_m)}\}$ – это последовательность элементов d_i, каждому из которых соответствует основание a_i из множества A так, что:

1. любое положительное d имеет единственное представление в виде $(a_1, \ldots, a_J)NAF_w(d)$ для набора оснований A и окна w;
2. любые w последовательных цифр содержат не более одной ненулевой;
3. $d_i \in \{0, \pm 1, \pm 2, \ldots, \pm\lfloor (a_1^w - 1)/2 \rfloor\} / \{\pm a_1, \pm 2a_1 \ldots, \pm\lfloor (a_1^{w-1} - 1)/2 \rfloor a_1\}$, $d_1 > 0$;
4. $k = (\ldots((d_1 \cdot a_2 + d_2) \cdot a_3) + \cdots + d_{m-1}) \cdot a_m + d_m$.

Разреженная форма с несколькими основаниями и окном

Частные случаи:

- если множество оснований A состоит только из одного элемента – *разреженная форма с окном*, $NAF_w(d)$;

- если множество оснований A состоит из более чем одного элемента, но окно $w = 2$ – *разреженная форма с несколькими основаниями*, $(a_1, \ldots, a_J)NAF(d)$;

- если множество оснований A состоит только из одного элемента и окно $w = 2$ – *разреженная форма*, $NAF(d)$.

Эксперименты (512 бит)

	NAF	$(2,3)NAF_2$	$(2,3)NAF_6$	$(2,3)NAF_9$	$(2,3)NAF_{11}$
Длина	512	458	490	495	497
Вес	170	122	65	47	40
Удвоений	511	366	456	470	475
Утроений	-	91	34	25	21
# предварительно вычисленных точек	-	-	2^5	2^8	2^{10}

Алгоритм вычисления суммы кратных точек

Общая схема: $kP + lQ$

1. Определяется специальное (совместное) представление показателей k, l;
2. предварительно вычисляются вспомогательные точки $iP+jQ$;
3. “сканируется” представление показателя, и на каждом шаге выполняется сложение с соответствующими предвычисленными точками и умножение на одно или несколько оснований.

Алгоритм вычисления суммы кратных точек

М.А. Калинин, 2010: *объединенная разреженная форма с несколькими основаниями и окном*

$$(a_1,\ldots,a_J)\overleftarrow{NAF}_w(k_1,k_2)=\begin{pmatrix}(d_1^{(a_1)},\ldots,d_l^{(a_l)})\\(e_1^{(a_1)},\ldots,e_l^{(a_l)})\end{pmatrix},$$

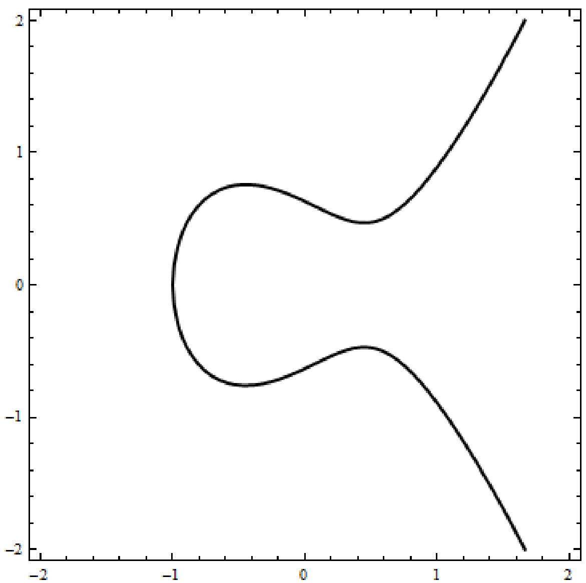
$$k_1P+k_2Q=a_{l-1}(\ldots a_3(a_2(d_1P+e_1Q)+d_2P+e_2Q)+\ldots$$
$$+d_{l-1}P+e_{l-1}Q)+d_lP+e_lQ.$$

Эксперименты (512 бит)

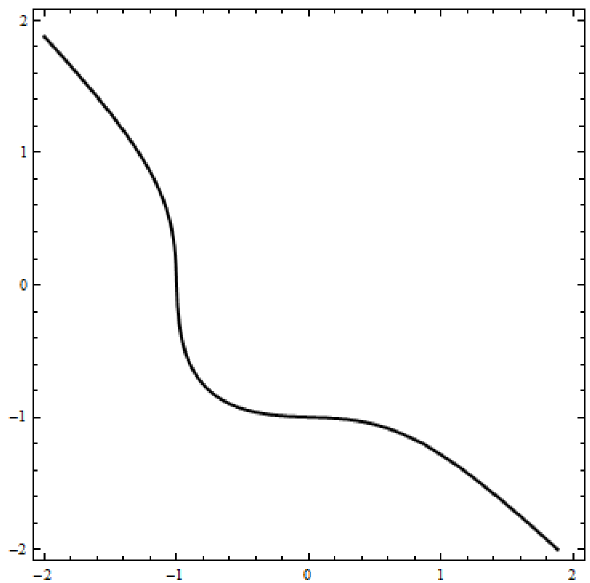
	JSF	$(2,3)NAF_2$	$(2,3)NAF_6$	$(2,3)NAF_9$
Длина	512	460	464	463
Вес	427	226	126	100
Удвоений	511	372	388	390
Утроений	-	87	75	72
# предварительно вычисленных точек	-	0(4)	$2^6(2^{12})$	$2^9(2^{18})$

Выбор эффективного представления точек кривой

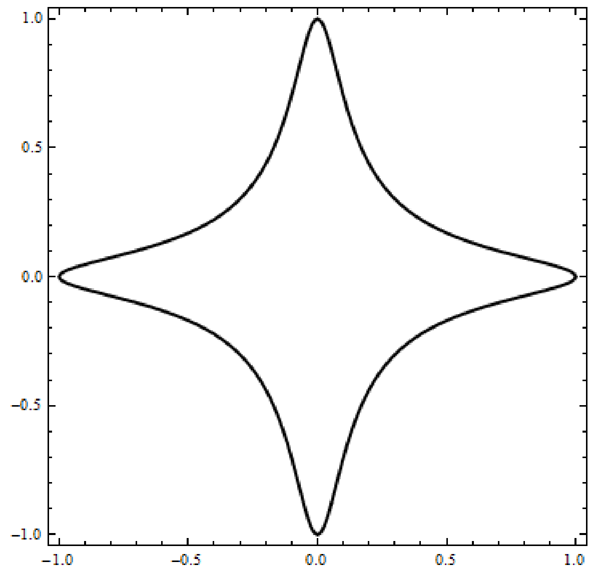
`http://hyperelliptic.org/EFD`



Вейерштрасс
$y^2 = x^3 - 0.6x + 0.4$



Хесс
$x^3 + y^3 + 1 = 0.1xy$



Эдвардс
$x^2 + y^2 = 1 - 100x^2y^2$

Выбор эффективного представления точек кривой

Особенности применения нестандартных представлений кривых при реализации схемы ГОСТ Р 34.10:

- Стандарт требует представления r как X-координаты точки в аффинных координатах Вейерштрасса;

- эффективная реализация требует выполнения условий для порядка группы точек: $2^{508} < q < 2^{512}$, ограничивая размер сомножителя $c = m/q$ $(m = \#E)$

Проективные координаты на кривой Вейерштрасса

Точка (x,y) на кривой $E(GF(p)) : y^2 = x^3 + ax + b$ представляется в проективных координатах в виде тройки $(X : Y : Z)$ такой, что $Y^2Z = X^3 + aXZ^2 + bZ^3$, $(x,y) = (X/Z, Y/Z)$.

Трудоемкость алгоритмов:

	Общий случай	$a = -3$
Сложение	$12M + 2S$	$5M + 6S$
Удвоение	$5M + 6S$	$7M + 3S$
Скалярные координаты	$1S + 1I$	$1S + 1I$

M, S, I – трудоемкость умножения, возведения в квадрат и вычисления обратного элемента $\pmod p$.
Критерий эффективности: $S = k_1 M, I = k_2 M, M \longrightarrow \min$ (k_1, k_2 – экспериментально).

Кривые Хесса

Кривая Хесса $H(GF(p))$ задается уравнением

$$x^3 + y^3 + 1 = 3dxy,$$

$d \in GF(p)$.

Сложение и удвоение точек задается формулами

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{(y_1^2 x_2 - y_2^2 x_1)}{(x_2 y_2 - x_1 y_1)}, \frac{x_1^2 y_2 - x_2^2 y_1}{(x_2 y_2 - x_1 y_1)} \right),$$

$$2(x_1, y_1) = \left(\frac{(y_1(1 - x_1^3)}{(x_1^3 - y_1^3)}, \frac{x_1(y_1^3 - 1)}{(x_1^3 - y_1^3)} \right).$$

Системы координат на кривых Хесса

Проективные координаты: точка (x, y) представляется в виде тройки $(X : Y : Z)$ такой, что $X^3 + Y^3 + Z^3 = 3dXYZ$, $(x, y) = (X/Z, Y/Z)$. Нейтральный элемент группы точек имеет координаты $(1 : -1 : 0)$. Обратным элементом к точке $(X : Y : Z)$ является точка $(Y : X : Z)$.

Интересное свойство проективных координат: $2(X : Y : Z) = (Z : X : Y) + (Y : Z : X)$.

Расширенные координаты: точка (x, y) представляется в виде набора $(X : Y : Z : XX : YY : ZZ : XY : YZ : XZ)$ такого, что $X^3 + Y^3 + Z^3 = 3dXYZ$, $(x, y) = (X/Z, Y/Z)$, и $XX = X^2, YY = Y^2, ZZ = Z^2, XY = 2X \cdot Y, XZ = 2X \cdot Z, YZ = 2Y \cdot Z$.

Кривые Хесса

Трудоемкость алгоритмов:

	Проективные координаты	Расширенные кординаты
Сложение	$12M$	$6M + 5S$
Удвоение	$6M + 3S$	$3M + 6S$
Утроение	$8M + 6S$	$-$
Скалярные координаты	$1I + 2M$	$1I + 2M$
x в форме Вейерштрасса	$1I + 1M$	$1I + 1M$

Кривые Эдвардса

Кривая Эдвардса $E_{Edw,c,d}(GF(p))$ задается уравнением

$$x^2 + y^2 = c^2(1 + dx^2y^2),$$

где $c, d \in GF(p)$, $cd(1 - c^4d) \neq 0$.

Групповая операция на кривой Эдвардса задается формулой

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{c(1 + dx_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)}\right),$$

нейтральным элементом является точка $(0, c)$. Обратным элементом к точке (x, y) является точка $(-x, y)$. Точка $(0, -1)$ имеет порядок 2, точки $(\pm 1, 0)$ имеют порядок 4.

Скрученные кривые Эдвардса

Скрученная кривая Эдвардса $\overline{E}_{Edw,a,d}(GF(p))$ задается уравнением

$$ax^2 + y^2 = 1 + dx^2y^2,$$

где $a, d \in GF(p)$, $a, d \neq 0$ (для скрученных кривых Эдвардса рассматриваем только случай $c = 1$).

Групповая операция на скрученной кривой Эдвардса задается формулой

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right),$$

нейтральным элементом является точка $(0, 1)$. Обратным элементом к точке (x, y) является точка $(-x, y)$.

Системы координат на кривых Эдвардса

Проективные координаты: точка (x, y) представляется в виде тройки $(X : Y : Z)$ такой, что $(X^2 + Y^2)Z^2 = Z^4 + dX^2Y^2$, $(x, y) = (X/Z, Y/Z)$. Нейтральный элемент: $(0 : 1 : 1)$. Обратный элемент к точке $(X : Y : Z)$: точка $(-X : Y : Z)$.

Инвертированные координаты: точка (x, y) представляется в виде тройки $(X : Y : Z)$ такой, что $(X^2 + Y^2)Z^2 = c(Z^4 + dX^2Y^2)$, $(x, y) = (Z/X, Z/Y)$, $XYZ \neq 0$. Нейтральный элемент: $(c : 0 : 0)$. Обратный элемент к точке $(X : Y : Z)$: точка $(-X : Y : Z)$. Имеются исключительные точки $(0, 1), (0, -1), (1, 0), (-1, 0)$.

Системы координат на кривых Эдвардса

Расширенные координаты на скрученных кривых: точка (x, y) представляется в виде набора $(X : Y : Z : T)$ такого, что $(aX^2 + Y^2)Z^2 = Z^4 + dX^2Y^2$, $(x, y) = (X/Z, Y/Z)$, $x \cdot y = T/Z$. Нейтральный элемент: $(0 : 1 : 1 : 1)$. Обратный элемент к точке $(X : Y : Z : T)$: точка $(-X : Y : Z : -T)$.

Кривые Эдвардса

Трудоемкость алгоритмов:

	Проективные координаты	Инверти-рованные кординаты	Расширенные кординаты на скрученных кривых
Сложение	$10M + 1S$	$9M + 1S$	$9M$
Удвоение	$3M + 4S$	$3M + 4S$	$4M + 4S$
Утроение	$9M + 4S$	$9M + 4S$	–
Скалярные координаты	$1I + 1M$	$1I + 1M$	$1I + 1M$
x в форме Вейерштрасса	$1I + 2M$	$1I + 2M$	$1I + 2M$

Ограничения: кривые Хесса

- На кривой Хесса есть точка порядка 3, т.е. $m = 3q$.

- Кривая в форме Вейерштрасса $E(GF(p))$ с j-инвариантом $j(E)$ изоморфна кривой Хесса iff $\exists d \in GF(p)$ такой, что

$$d^3(d^3+216)^3 - j(E))(d^9 - 81d^6 + 2187d^3 - 19683) = 0 \pmod p.$$

Ограничения: кривые Эдвардса

- Точки $(\pm 1, 0)$ имеют порядок 4, т.о. $m = 4q$.

- Рассмотрим кривые Монтгомери: $M_{A,B} = (x, y) : By^2 = x^3 + Ax + x$. Тогда:

  – если $p \equiv 3 \pmod 4$, то любая кривая Монтгомери бирационально эквивалентна над $GF(p)$ некоторой кривой Эдвардса;
  – каждая скрученная кривая Эдвардса $\overline{E}_{Edw,a,d}$ бирационально эквивалентна над $GF(p)$ кривой Монтгомери $M_{A,B}$;
  – каждая кривая Монтгомери $M_{A,B}$ бирационально эквивалентна над $GF(p)$ некоторой скрученной кривой Эдвардса.

Результаты экспериментов

	$(2,3)NAF_9(k)$, $(2,3)NAF_6(k,l)$		$NAF(k)$, $(2)NAF_2(k,l)$	
	256 бит	512 бит	256 бит	512 бит
Вейерштрасс	1.12/1.43	4.23/5.23	1.25/1.76	4.82/6.35
Хесс (расширенные)	0.7/0.98	2.65/3.54	0.89/1.23	3.32/4.5
Эдвардс (проективные)	0.66/0.98	2.36/3.37	0.89/1.26	3.07/4.34
Эдвардс (инвертированные)	0.7/0.98	2.56/3.48	0.89/1.26	3.18/4.38
Эдвардс (скрученные, расширенные)	0.7/0.98	2.52/3.38	0.87/1.25	3.12/4.30

Время выработки/проверки подписи, мс
(умножение с приведением по модулю)

MS VS 2010; Intel C++ Composer XE 2011; gmp 5.0.2; Xeon 3.0GHz (1 ядро)

Результаты экспериментов

	$(2,3)NAF_9(k)$, $(2,3)NAF_6(k,l)$		$NAF(k)$, $(2)NAF_2(k,l)$	
	256 бит	512 бит	256 бит	512 бит
Вейерштрасс	1.33/1.4	7.36/7.63	1.5/2.12	8.69/11.45
Хесс (расширенные)	0.69/0.83	2.6/3.31	0.91/1.14	3.15/4.24
Эдвардс (проективные)	0.71/0.85	3.45/4.07	1.03/1.54	5.18/7.67
Эдвардс (инвертированные)	0.69/0.81	3.37/4.8	0.89/1.28	4.37/6.12
Эдвардс (скрученные, расширенные)	0.75/0.87	3.54/3.92	0.98/1.4	4.7/6.52

Время выработки/проверки подписи, мс
(умножение без приведения по модулю)

MS VS 2010; Intel C++ Composer XE 2011; gmp 5.0.2; Xeon 3.0GHz (1 ядро)

Выводы

- Показана возможность построения эффективной программной реализации схемы ЭЦП ГОСТ Р 34.10 с дополнительным вариантом требований к параметрам;

- определены рекомендованные параметры такой реализации:

  - использование (в зависимости от реализации арифметики в поле)проективных или инвертированных координат на кривых Эдвардса, расширенных координат на скрученной кривой Эдвардса или расширенных координат на кривой

Хесса (разница в эффективности – в пределах погрешности эксперимента);

– использование алгоритмов класса $(2,3)NAF$ с окном 9 для вычисления кратной точки и 6(9) для суммы кратных точек;

- показано, что при использовании оптимальных алгоритмов трудоемкость выработки и проверки ЭЦП ГОСТ Р 34.10 на универсальном процессоре для нового варианта требований к параметрам увеличится не более чем в 5 раз по сравнению с действующим стандартом.

Спасибо за внимание.