УДК 681.3.06

В.Ю. КОВТУН канд. техн. наук

ПРЕОБРАЗОВАНИЯ В ЯКОБИАНЕ ГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВОЙ РОДА 2 В ПРОЕКТИВНЫХ КООРДИНАТАХ НАД ПОЛЕМ НЕЧЕТНОЙ ХАРАКТЕРИСТИКИ

Введение

Комплексы криптографической защиты информации (ККЗИ) стали неотъемлемым элементом широкого спектра современных информационно-телекоммуникационных систем (ИТС). Увеличение объемов циркулирующей информации, необходимость в оперативности обслуживая абонентов ИТС, с одной стороны, и интенсивно растущие вычислительные мощности вычислительной техники, развивающиеся математические методы криптоанализа, с другой стороны, выдвигают серьезные требования к существующим и перспективным ККЗИ. Другими словами, основным требованием к ККЗИ является обеспечение необходимого уровня стойкости, однако возможность практического использования подобных комплексов определяется сложностью эффективной реализации на современных вычислительных платформах. Отметим, что основу ККЗИ составляют именно криптографические преобразования с открытым ключом [1].

Наряду с хорошо зарекомендовавшими себя, в последнее десятилетие, преобразованиями в кольцах и полях, широкое применение получили преобразования в группе точек эллиптической кривой, о чем свидетельствует множество международных и государственных стандартов [2-4]. Такие преобразования позволяют строить ККЗИ более высокого класса стойкости. Следующим шагом является использование более сложных кривых – гиперэллиптических, что в свою очередь приводит к повышению вычислительной сложности реализации такого комплекса. Поэтому работы, посвященные уменьшению вычислительной сложности перспективных криптопреобразований, являются весьма актуальными.

В криптопреобразованиях на гиперэллиптических кривых (ГЭК) основную роль играют операции над приведенными дивизорами, в частности скалярное умножение приведенного дивизора [5], для которого, базовыми операциями выступают сложение и удвоение дивизора.

Существенного снижения вычислительной сложности (для краткости – сложности) в отношении трудоемкости криптографических примитивов на основе преобразований дивизоров в якобиане ГЭК можно достигнуть, в соответствии со сказанным выше, за счет снижения сложности операции скалярного умножения дивизоров.

К наиболее ранним публикациям, посвященным арифметическим преобразованиям в якобиане ГЭК, следует отнести [6, 7], которые имели сугубо теоретический интерес.

В последнее время отечественные и зарубежные исследователи интенсивно занимались вопросами эффективной реализации арифметических преобразований в якобиане ГЭК, о чем свидетельствуют публикации [5-19]. Среди этих работ существенное внимание уделяется уменьшению количества полевых операций за счет использования ГЭК с фиксированным родом, это в свою очередь привело к появлению различных модификаций методов арифметических преобразований в якобиане ГЭК. В работах [1, 16], рассматриваются методы сложения и удвоения дивизоров в якобиане ГЭК второго рода. Первая практическая реализация этих методов описывается в [14]. В публикации [12] обобщаются результаты [14] для кривых над полями четной характеристики. Развитие методов сложения и удвоения описано в работах [3, 7, 14, 15].

Время, необходимое для выполнения скалярного умножения дивизора в якобиане ГЭК рода 2 над полем $GF(p_{83})$ 8.232 мс (библиотека операций в поле GMP) [7, 17], свидетельствует о необходимости дальнейшей оптимизации скалярного умножения. В этих условиях задача повышения производительности ККЗИ и, в частности, операции скалярного умножения дивизоров якобиана ГЭК, приобретает особую актуальность.

Поскольку основной интерес для понижения сложности методов арифметических преобразований в якобиане ГЭК представляют кривые именно рода 2, далее рассмотрим кривые этого вида.

Как известно из [6, 8], в операциях сложения и удвоения дивизоров в якобиане ГЭК присутствует наиболее сложная полевая операция – инвертирование. Согласно [8, 9], для поля нечетной характеристики сложность операции инвертирования I_{inv} принимает значения на интервале $(40I_{mul}, 80I_{mul})$ [9], где I_{mul} – сложность операции умножения в поле. В [10], впервые предложен подход к реализации арифметических операций в якобиане ГЭК рода 2 без использования операции инвертирования в поле. Дальнейшее развитие предложенного подхода было проведено в работах [6, 11], результаты которых были улучшены и распространены на более широкий класс ГЭК над полем четной характеристики в работах [6, 11]. В качестве прототипа, для разрабатываемых методов, рассматриваются именно результаты [6, 11].

Представление дивизоров в форме Мамфорда $[u, v]$, $u(x) = x^2 + u_1 x + u_0$, $v(x) = v_1 x + v_0$, $\deg v < \deg u \le 2$ будем называть аффинным; представление, арифметические преобразования в котором не используют инвертирование в поле, назовем проективным; в этом случае дивизор $[u, v]$, $u(x) = x^2 + U_1/Z\, x + U_0/Z$, $v(x) = V_1/Z\, x + V_0/Z$, представлен в виде $[U_1, U_0, V_1, V_0, Z]$ [6(4)], а взвешенным, если дивизор $[u, v]$, $u(x) = x^2 + U_1/Z_1^2\, x + U_0/Z_1^2$, $v(x) = V_1/Z_1^3 Z_2\, x + V_0/Z_1^3 Z_2$, представлен в виде $[U_1, U_0, V_1, V_0, Z_1, Z_2]$ [11].

В соответствии с выше сказанным, целью работы является разработка модифицированного метода арифметических преобразований в якобиане ГЭК второго рода в проективных координатах, для повышения производительности операции скалярного умножения.

Согласно принятой модели [13, 14], под типовым сложением понимается сложение дивизоров $[u_1(x), v_1(x)]$ и $[u_2(x), v_2(x)]$, в котором результанта $r(u_1(x), u_2(x))$ отлична от нуля, а под удвоением – удвоение дивизора $[u_1(x), v_1(x)]$, в котором результанта $r(u_1(x), h(x) + 2v_1(x))$ отлична от нуля.

В основу предложенной модификации, обеспечивающей понижение сложности, положен метод Харлея [14], а также его модификация [12]. С этой целью в описанном методе предлагается использовать проективное представление дивизоров.

В алгоритмах сложения и удвоения [12, 14] наиболее сложными, с точки зрения трудоемкости, являются операции в кольце полиномиальных функций: деление, мультипликативное инвертирование, приведение по модулю, умножение.

Для уменьшения числа этих операций предлагается модифицировать алгоритмы сложения и удвоения следующим образом:

- перейти от операций в кольце полиномиальных функций непосредственно к операциям в поле используются ГЭК небольшого фиксированного рода (в данном случае второго) [14, 15];
- упростить процедуры арифметических операций в кольце полиномиальных функций посредством их нормализации;
- нормализировать и минимизировать вес по Хеммингу параметров $h(x)$ и $f(x)$ ГЭК посредством использования ГЭК особого вида [10, 12];
- одновременно инвертировать нескольких элементов поля посредством метода Монтгомери [12-14];
- умножать полиномиальные функции различных степеней посредством метода Карацубы [12];
- приводить по модулю полиномиальные функции различных степеней посредством метода Карацубы [14];

- исключить операции мультипликативного инвертирования в поле посредством проективного представления дивизоров [6, 10].

Арифметика в якобиане ГЭК над полем нечетной характеристики

Использование предложенных модификаций, получаем следующие алгоритмы арифметических преобразований для ГЭК, заданного уравнением $v^2 + h(u)v = f(u)$ над полем $\mathbf{F}_q$ нечетной характеристики в проективных координатах, где $h(x) = 0$, $f(x) = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0,\ f_i \in \mathbf{F}_q$.

Алгоритм 1. Усовершенствованное сложение дивизоров
Вход: $\mathrm{div}(U_{11}, U_{10}, V_{11}, V_{10}, Z_1),\ \mathrm{div}(U_{21}, U_{20}, V_{21}, V_{20}, Z_2)$
Выход: $\mathrm{div}(U_1', U_0', V_1', V_2', Z') = \mathrm{div}(U_{11}, U_{10}, V_{11}, V_{10}, Z_1) + \mathrm{div}(U_{21}, U_{20}, V_{21}, V_{20}, Z_2)$

	Выражение	Количество операций
1	Предвычисления: $Z = Z_1 \cdot Z_2,\ \widetilde{U}_{21} = Z_1 \cdot U_{21},\ \widetilde{U}_{20} = Z_1 \cdot U_{20},\ \widetilde{V}_{21} = Z_1 \cdot V_{21},\ \widetilde{V}_{20} = Z_1 \cdot V_{20}$	$5I_{mul}$
2	Вычисление результанты r для u_1 и u_2: $y_1 = U_{11} \cdot Z_2 - \widetilde{U}_{21},\ y_2 = \widetilde{U}_{20} - U_{10} \cdot Z_2,\ y_3 = U_{11} \cdot y_1 + y_2 \cdot Z_1,\ r = y_2 \cdot y_3 + y_1^2 \cdot U_{10}$	$1I_{sqr}$, $6I_{mul}$
3	Вычисление квази-инверсии $inv = r/u_2 \bmod u_1,\ inv = inv_1x + inv_0$: $inv_1 = y_1,\ inv_0 = y_3$	
4	Вычисление $s = (v_1 - v_2)inv \bmod u_1,\ s = s_1x + s_0$: $w_0 = V_{10} \cdot Z_2 - \widetilde{V}_{20},\ w_1 = V_{11} \cdot Z_2 - \widetilde{V}_{21},\ w_2 = inv_0 \cdot w_0,\ w_3 = inv_1 \cdot w_1,$ $s_1 = (inv_0 + Z_1 \cdot inv_1) \cdot (w_0 + w_1) - w_2 - w_3 \cdot (Z_1 + U_{11}),\ s_0 = w_2 - U_{10} \cdot w_3$ If $s_1 = 0$ then consider special case	$8I_{mul}$
5	Предвычисления: $R = r \cdot Z,\ s_2 = s_0 \cdot Z,\ s_3 = s_1 \cdot Z,\ \widetilde{R} = R \cdot s_3,\ w_0 = s_1 \cdot s_0,\ w_1 = s_1 \cdot s_3,\ w_2 = s_0 \cdot s_3,$ $w_3 = w_1 \cdot \widetilde{U}_{21},\ w_4 = R \cdot s_1$	$9I_{mul}$
6	Вычисление $l = su_2,\ l = x^3 + l_2x^2 + l_1x + l_0$: $l_0 = w_0 \cdot \widetilde{U}_{20},\ l_2 = w_3 + w_2,\ l_1 = (w_1 + w_0) \cdot (\widetilde{U}_{21} + \widetilde{U}_{20}) - l_0 - w_3$	$2I_{mul}$
7	Вычисление $u' = (s(l + 2v_1) - k)u_1^{-1},\ k = (f - v_1^2)/u_1,\ u' = x^2 + u_1'x + u_0'$: $\widetilde{U}_0' = s_2^2 + s_1 \cdot y_1 \cdot (s_1 \cdot \widetilde{U}_{11} - 2s_2) + y_2 \cdot w_1 + 2w_4 \cdot \widetilde{V}_{21} + R \cdot r \cdot (y_1 + 2\widetilde{U}_{21})$ $\widetilde{U}_1' = 2w_2 - s_3 \cdot s_1y_1 - R^2$	$2I_{sqr}$, $8I_{mul}$
8	Корректировка: $U_0' = \widetilde{U}_0' \cdot \widetilde{R},\ U_1' = \widetilde{U}_1' \cdot \widetilde{R},\ Z' = s_3^2 \cdot \widetilde{R}$	$1I_{sqr}$, $3I_{mul}$
9	Вычисление $v' \equiv -(s_1l + v_2) \bmod u',\ v' = v_1'x + v_0'$: $V_1' = \widetilde{U}_1' \cdot (l_2 - \widetilde{U}_1') + s_3^2 \cdot (\widetilde{U}_0' - w_4\widetilde{V}_{21} - l_1),\ V_0' = \widetilde{U}_0' \cdot (l_2 - \widetilde{U}_1') - s_3^2 \cdot (l_0 + w_4 \cdot \widetilde{V}_{20})$	$5I_{mul}$
		$4I_{sqr}$, $46I_{mul}$

В частности, для алгоритма сложения на практике часто возникает ситуация, когда один из входных дивизоров представлен в аффинном (Z координата равна 1), а другой – в проективном виде. Результат сложения представляется в проективном виде. Такие входные данные для алгоритма 1 позволяют упростить его до алгоритма 2, содержащего меньшее количество полевых операций, что обеспечивает понижение сложности.

Алгоритм 2. Усовершенствованное смешанное сложение дивизоров
Вход: $\mathrm{div}(U_{11}, U_{10}, V_{11}, V_{10}, 1)$, $\mathrm{div}(U_{21}, U_{20}, V_{21}, V_{20}, Z_2)$
Выход: $\mathrm{div}(U_1', U_0', V_1', V_2', Z') = \mathrm{div}(U_{11}, U_{10}, V_{11}, V_{10}, 1) + \mathrm{div}(U_{21}, U_{20}, V_{21}, V_{20}, Z_2)$

	Выражение	Количество операций
1	Предвычисления: $\widetilde{U}_{11} = Z_2 \cdot U_{11}$	$1I_{mul}$
2	Вычисление результанты r для u_1 и u_2: $y_1 = \widetilde{U}_{11} - U_{21}$, $y_2 = U_{20} - U_{10} \cdot Z_2$, $y_3 = U_{11} \cdot y_1 + y_2$, $r = y_2 \cdot y_3 + y_1^2 \cdot U_{10}$	$1I_{sqr}$, $4I_{mul}$
3	Вычисление квази-инверсии $inv = r/u_2 \bmod u_1$, $inv = inv_1 x + inv_0$: $inv_1 = y_1$, $inv_0 = y_3$	
4	Вычисление $s = (v_1 - v_2) inv \bmod u_1$, $s = s_1 x + s_0$: $w_0 = V_{10} \cdot Z_2 - V_{20}$, $w_1 = V_{11} \cdot Z_2 - V_{21}$, $w_2 = inv_0 \cdot w_0$, $w_3 = inv_1 \cdot w_1$, $s_1 = (inv_0 + inv_1) \cdot (w_0 + w_1) - w_2 - w_3 \cdot (U_{11} + 1)$, $s_0 = w_2 - U_{10} \cdot w_3$ If $s_1 = 0$ then consider special case	$7I_{mul}$
5	Предвычисления: $R = r \cdot Z_2$, $s_2 = s_0 \cdot Z_2$, $s_3 = s_1 \cdot Z_2$, $\widetilde{R} = R \cdot s_3$, $w_0 = s_1 \cdot s_0$, $w_1 = s_1 \cdot s_3$, $w_2 = s_0 \cdot s_3$, $w_3 = w_1 \cdot U_{21}$, $w_4 = R \cdot s_1$.	$9I_{mul}$
6	Вычисление $l = su_2$, $l = l_2 x^2 + l_1 x + l_0$: $l_0 = w_0 \cdot U_{20}$, $l_2 = w_3 + w_2$, $l_1 = (w_1 + w_0) \cdot (U_{21} + U_{20}) - l_0 - w_3$	$2I_{mul}$
7	Вычисление $u' = (s(l + 2v_1) - k) u_1^{-1}$, $k = (f - v_1^2)/u_1$, $u' = x^2 + u_1' x + u_0'$: $\widetilde{U}_0' = s_2^2 + s_1 \cdot y_1 \cdot (s_1 \cdot \widetilde{U}_{11} - 2s_2) + y_2 \cdot w_1 + 2w_4 \cdot V_{21} + R \cdot r \cdot (y_1 + 2U_{21})$ $\widetilde{U}_1' = 2w_2 - s_3 \cdot s_1 y_1 - R^2$	$2I_{sqr}$, $8I_{mul}$
8	Корректировка: $U_0' = \widetilde{U}_0' \cdot \widetilde{R}$, $U_1' = \widetilde{U}_1' \cdot \widetilde{R}$, $Z' = s_3^2 \cdot \widetilde{R}$	$1I_{sqr}$, $3I_{mul}$
9	Вычисление $v' \equiv -(h + s_1 l + v_2) \bmod u'$, $v' = v_1' x + v_0'$: $V_1' = \widetilde{U}_1' \cdot (l_2 - \widetilde{U}_1') + s_3^2 \cdot (\widetilde{U}_0' - w_4 V_{21} - l_1)$, $V_0' = \widetilde{U}_0' \cdot (l_2 - \widetilde{U}_1') - s_3^2 \cdot (l_0 + w_4 \cdot V_{20})$	$5I_{mul}$
		$4I_{sqr}$, $39I_{mul}$

Ниже приведем алгоритм удвоения дивизора в типовом случае.

Алгоритм 3. Усовершенствованное удвоение дивизоров
Вход: $\mathrm{div}(U_1, U_0, V_1, V_0, Z)$
Выход: $\mathrm{div}(U_1', U_0', V_1', V_2', Z') = 2\,\mathrm{div}(U_1, U_0, V_1, V_0, Z)$

	Выражение	Количество операций
1	Предвычисления: $Z_2 = Z^2$, $\widetilde{V}_1 = 2V_1$, $\widetilde{V}_0 = 2V_0$.	$1I_{sqr}$
2	Вычисление результанты r для u и $2v$ (причем $\widetilde{v} \equiv (2v) \bmod u$): $w_0 = V_1^2$, $w_1 = U_1^2$, $w_2 = \widetilde{V}_1^2 = 4w_0$, $w_3 = \widetilde{V}_0 \cdot Z - U_1 \cdot \widetilde{V}_1$, $r = \widetilde{V}_0 \cdot w_3 + w_2 \cdot U_0$.	$2I_{sqr}$, $4I_{mul}$
3	Вычисление квази-инверсии $inv \equiv r/\widetilde{v} \bmod u$, $inv = inv_1 x + inv_0$: $inv_1 = -\widetilde{V}_1$, $inv_0 = w_3$.	
4	Вычисление $k \equiv [(f - v^2)/u] \bmod u$, $k = k_1 x + k_0$:	$5I_{mul}$

	$w_3 = f_3 \cdot Z + w_1,\ k_1 = 2w_1 + w_3 - Z \cdot 2U_0,\ k_0 = U_1 \cdot (4ZU_0 - w_3) + Z \cdot (f_2 \cdot Z - w_0).$	
5	Вычисление $s = k \cdot inv \bmod u$, $s = s_1 x + s_0$: $w_0 = k_0 \cdot inv_0,\ w_1 = k_1 \cdot inv_1,$ $s_0 = w_0 - ZU_0 \cdot w_1,\ s_3 = (inv_0 + inv_1) \cdot (k_0 + k_1) - w_0 - w_1 \cdot (1 + U_1),\ s_1 = s_3 \cdot Z.$ If $s_1 = 0$ then consider special case.	$6I_{mul}$
6	Предвычисления: $R = r \cdot Z_2,\ \widetilde{R} = R \cdot s_1,\ w_0 = s_1 \cdot s_3,\ w_1 = s_0 \cdot s_3,\ w_3 = w_1 \cdot Z,\ w_4 = R \cdot s_3.$	$6I_{mul}$
7	Вычисление $l = su$, $l = l_2 x^2 + l_1 x + l_0$: $l_0 = U_0 \cdot w_1,\ l_2 = U_1 \cdot w_0,\ l_1 = (w_1 + w_0) \cdot (U_1 + U_0) - l_0 - l_2.$	$3I_{mul}$
8	Вычисление $u' = \left\lfloor l^2 + \frac{1}{s} l 2v - \frac{1}{s^2}(f - v^2) \right\rfloor / u^2$, $u' = x^2 + u_1' x + u_0'$: $\widetilde{U}_0' = s_0^2 + 2w_4 \cdot V_1 + R \cdot r \cdot 2U_1,\ \widetilde{U}_1' = 2w_3 - R^2.$	$2I_{sqr}$, $2I_{mul}$
9	Корректировка: $U_0' = \widetilde{U}_0' \cdot \widetilde{R},\ U_1' = \widetilde{U}_1' \cdot \widetilde{R},\ Z' = s_1^2 \cdot \widetilde{R}.$	$1I_{sqr}$, $3I_{mul}$
10	Вычисление $v' \equiv -(s_1 l + v_2) \bmod u'$, $v' = v_1' x + v_0'$: $V_1' = \widetilde{U}_1' \cdot (l_2 - \widetilde{U}_1' + w_3) + s_1^2 \cdot (\widetilde{U}_0' - w_4 V_1 - l_1),\ V_0' = \widetilde{U}_0' \cdot (l_2 - \widetilde{U}_1' + w_3) - s_1^2 \cdot (l_0 + w_4 \cdot V_0).$	$5I_{mul}$
		$6I_{sqr}$, $35I_{mul}$

В частности, для алгоритма удвоения на практике часто возникает ситуация, когда входной дивизор представлен в аффинном виде (Z координата равна 1). Результат удвоения представляется в проективном виде. Такие входные данные для алгоритма 3 позволяют упростить его до алгоритма 4, содержащего меньшее количество полевых операций, что обеспечивает понижение сложности.

Алгоритм 4. Усовершенствованное смешанное удвоение дивизоров
Вход: $\mathrm{div}(U_1, U_0, V_1, V_0, 1)$
Выход: $\mathrm{div}(U_1', U_0', V_1', V_2', Z') = 2\,\mathrm{div}(U_1, U_0, V_1, V_0, 1)$

	Выражение	Количество операций
1	Предвычисления: $\widetilde{V}_1 = 2V_1,\ \widetilde{V}_0 = 2V_0.$	
2	Вычисление результанты r для u и $2v$ (причем $\widetilde{v} \equiv (2v) \bmod u$): $w_0 = V_1^2,\ w_1 = U_1^2,\ w_2 = \widetilde{V}_1^2 = 4w_0,\ w_3 = \widetilde{V}_0 - U_1 \cdot \widetilde{V}_1,\ r = \widetilde{V}_0 \cdot w_3 + w_2 \cdot U_0.$	$2I_{sqr}$, $3I_{mul}$
3	Вычисление квази-инверсии $inv \equiv r/\widetilde{v} \bmod u$, $inv = inv_1 x + inv_0$: $inv_1 = -\widetilde{V}_1,\ inv_0 = w_3.$	
4	Вычисление $k \equiv \left[(f - v^2)/u\right] \bmod u$, $k = k_1 x + k_0$: $w_3 = f_3 + w_1,\ w_4 = 2U_0,\ k_1 = 2w_1 + w_3 - w_4,\ k_0 = U_1 \cdot (2w_4 - w_3) + f_2 - w_0.$	$1I_{mul}$
5	Вычисление $s = k \cdot inv \bmod u$, $s = s_1 x + s_0$: $w_0 = k_0 \cdot inv_0,\ w_1 = k_1 \cdot inv_1,\ s_0 = w_0 - U_0 \cdot w_1,$ $s_1 = (inv_0 + inv_1) \cdot (k_0 + k_1) - w_0 - w_1 \cdot (1 + U_1).$ If $s_1 = 0$ then consider special case.	$5I_{mul}$
6	Предвычисления: $\widetilde{R} = r \cdot s_1,\ w_0 = s_1^2,\ w_1 = s_0 \cdot s_1.$	$1I_{sqr}$, $2I_{mul}$
7	Вычисление $l = su$, $l = l_2 x^2 + l_1 x + l_0$:	$3I_{mul}$

$l_0 = U_0 \cdot w_1,\ l_2 = U_1 \cdot w_0,\ l_1 = (w_1 + w_0) \cdot (U_1 + U_0) - l_0 - l_2.$

8 Вычисление $u' = \left\lfloor l^2 + \frac{1}{s} l 2v - \frac{1}{s^2}\left(f - v^2\right)\right\rfloor / u^2,\ u' = x^2 + u'_1 x + u'_0$: $2I_{sqr},\ 2I_{mul}$

$\widetilde{U}'_0 = s_0^2 + 2\widetilde{R} \cdot V_1 + r^2 \cdot 2U_1,\ \widetilde{U}'_1 = 2w_1 - r^2.$

9 Корректировка: $U'_0 = \widetilde{U}'_0 \cdot \widetilde{R},\ U'_1 = \widetilde{U}'_1 \cdot \widetilde{R},\ Z' = w_0 \cdot \widetilde{R}.$ $3I_{mul}$

10 Вычисление $v' \equiv -(s_1 l + v_2) \bmod u',\ v' = v'_1 x + v'_0$: $5I_{mul}$

$V'_1 = \widetilde{U}'_1 \cdot \left(l_2 - \widetilde{U}'_1 + w_1\right) + w_0 \cdot \left(\widetilde{U}'_0 - \widetilde{R} V_1 - l_1\right),\ V'_0 = \widetilde{U}'_0 \cdot \left(l_2 - \widetilde{U}'_1 + w_1\right) - w_0 \cdot \left(l_0 + \widetilde{R} \cdot V_0\right).$

$5I_{sqr},\ 24I_{mul}$

Анализ вычислительной сложности

В таблице 1 сведены оценки сложности известных [10-11, 13] и предложенных в работе алгоритмов арифметических преобразований в якобиане ГЭК для типовых случаев. Сложность алгоритмов выражена в полевых операциях.

Таблица 1

Параметры ГЭК второго рода	Алгоритмы											
	Сложение			Смешанное сложение			Удвоение			Смешанное удвоение		
	$()^{-1}$	^2	*	$()^{-1}$	^2	*	$()^{-1}$	^2	*	$()^{-1}$	^2	*
Поле нечетной характеристики												
Аффинные координаты												
$f_4 = 0$ [13]	1	3	22				1	5	22			
Проективные координаты $[U_1, U_0, V_1, V_0, Z]$												
$\deg(h) = 2,\ h_i \in \mathbf{F}_2$ [6]		4	47		3	40		6	40		5	25
$\deg(h) = 2,\ h_i \in \mathbf{F}_2$ [20]		4	46		4	39		6	39		5	25
Взвешенные координаты $[U_1, U_0, V_1, V_0, Z_1, Z_2, Z_1^2, Z_2^2]$												
$h(x) = 0,\ f_4 = 0$ [11]		7	47		5	36		7	34		5	21
$h(x) = 0,\ f_4 = 0$ [*]		4	46		4	39		6	35		5	24
Поле четной характеристики												
Аффинные координаты												
$f_4 = 0$ [13]	1	3	21				1	5	20			
$h_2 = 0,\ f_4 = 0$ [13]	1	3	21				1	5	17			
$h(x) = x,\ f_4 = 0,\ f_3 = f_2 = 0$ [12]							1	6	9			
Проективные координаты $[U_1, U_0, V_1, V_0, Z]$												
$h(x) = x,\ f_4 = 0,\ f_3 = f_2 = 0$ [12]		5	45		5	38		6	31		5	18
$h(x) = x,\ f_4 = 0,\ f_3 = f_2 = 0$ [20]		4	44		4	37		6	30		4	17
Взвешенные координаты $[U_1, U_0, V_1, V_0, Z_1, Z_2, Z_1^2, Z_2^2, Z_1 Z_2, Z_1^3 Z_2]$												
$f_4 = 0,\ h_2 \neq 0$ [11]		4	46		5	35		6	35		5	24
$f_4 = 0,\ h_2 = 0$ [11]		6	44		6	34		6	29		6	19

Символом [*] – отмечены условия, используемые в предложенных модификациях.

Данные, из таблицы 1, свидетельствуют о том, что для поля нечетной характеристики, алгоритмы, построенные на основе предложенного автором модифицированного метода, обладают меньшей сложностью в сравнении с [6, 12].

Заключение

Согласно цели работы, разработана модификация метода арифметических преобразований в якобиане ГЭК второго рода в проективных координатах, она обеспечивает понижение сложности по сравнению с существующими методами [6, 12] – повысить производительность скалярного умножения. Эта модификация определяется следующим:

- уменьшенным количеством повторно вычисляемых величин – осуществляется предвычисление и хранение результатов, в сравнении с [12–14];
- увеличенным количеством предвычисленных величин – изменятся порядок выполнения полевых операций, в сравнении [12–14];
- увеличенным количеством предвычисленных величин – учитываются ранее неизвестные зависимости между результирующими полиномиальными функциями;
- уменьшенным весом по Хэммингу коэффициентов ГЭК, по аналогии с [11].

Предложенная модификация арифметических преобразований в якобиане ГЭК второго рода позволяет понизить вычислительную сложность на 2%. Известно [8, 9], что сложность операции скалярного умножения в среднем составляет:

$$I^D_{mul} = \tfrac{1}{2} t I^D_{add} + t I^D_{dbl},$$

где t – битовая длина скалярного множителя, I^D_{add}, I^D_{dbl} - сложности операций сложения и удвоения дивизоров, соответственно. Поэтому, в результате использования предложенного метода преобразований, возможно уменьшение вычислительной сложности скалярного умножения на 4% по сравнению с известными аналогами [6, 12].

Использование предложенного алгоритма в комбинации с описанным в работе [11] в процессинговом центре банка позволит сократить время проверки цифровой подписи на величину порядка 2%.

Список литературы 1. *W. Diffie, M. Hellman*. New directions in cryptography. IEEE Transactions on information theory. pp. 644-654. November 1976. 2. International Organization for Standardization. ISO/IEC FCD 15946-2: Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures, Final Committee Draft, 1999. 3. IEEE P1363-2000. Standard Specifications for Public Key Cryptography. Available at: http://www.ieee.org 4. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. 5. *N. Koblitz.* Hyperelliptic cryptosystems. Journal of cryptology, No 1. pp.139-150, 1989. 6. *T. Lange.* Inversion-free arithmetic on genius 2 hyperelliptic curves. Cryptology ePrint Archive, report 2002/147, 2002. Available http://eprint.iacr.org. 7. *D.G. Cantor.* Computing in the jacobian of hyperelliptic curve. Math. Comp., No 48. pp. 95-101, 1987. 8. *D. Hankerson, J. Lopez Hernandez, A. Menezes.* Software implementation of elliptic curve cryptography over binary fields. 9. *M. Brown, D. Hankerson, J. Lopez, A. Menezes.* Software implementation of the NIST elliptic curves over prime fields. 10. *Y. Miyamoto, H. Doi, K. Matsuo, J. Chao, S.Tsujii.* A fast addition algorithm of genius two hyperelliptic curve. In the 2002 Symposium on cryptography and information security – SCIS 2002, IEICE Japan, pp.497-502, 2002. In Japanese. 11. *T. Lange.* Weighted coordinates on genius 2 hyperelliptic curves. Cryptology ePrint Archive, report 2002/153, 2002. Available http://eprint.iacr.org. 12. *T. Wollinger.* Software and hardware implementation of hyperelliptic curve cryptosystems. PhD dissertation. Bochum, Germany, May 2004. 13. *T. Lange.* Efficient arithmetic on genius 2 hyperelliptic curves over finite fields via explicit formulae. Cryptology ePrint Archive, report 2002/121, 2002. Available http://eprint.iacr.org. 14. *R. Harley.* Fast arithmetic on genius 2 curves. Available at: http://cristal.infra.fr/~harley/hyper. 2000. 15. *A.M. Spallek.* Kurven vom geschlecht 2 und ihre anwendung in public-key-kryptosystemen. PhD thesis, Universitat Gesamthochschule Essen, 1994. 16. *U. Kriger.* Anwendung hyperellipischer kurven in der kryptographie. Master's thesis, Universitat Gesamthochschule Essen, 2001. 17. *T. Lange.* Efficient arithmetic on hyperelliptic curves. PhD thesis, Universitat Gesamthochschule Essen, 2001. 18. *M. Takahashi.* Improving Harley algorithms for jacobians of

genius 2 hyperelliptic curves. In Proc. of SCIS2002, IEICE Japan, 2002. in Japanese. 19. *H. Suguzaki, K. Matsuo, J. Chao, S. Tsujii.* An extension of Harley algorithm addition algorithm for hyperelliptic curves over finite fields of characteristic two. Technical report ISEC2002-9 (2002-5), IEICE Japan, 2002. pp. 49-56. 20. *В.Ю. Ковтун, С.И. Збитнев*. Арифметические операции в якобиане гиперэллиптической кривой рода 2 в проективных координатах с уменьшенной сложностью // Восточно–Европейский журнал передовых технологий. –2004. –Вып. №½ (13). –С. 14–22.