УДК 681.3.06

БЫСТРЫЕ ПРЕОБРАЗОВАНИЯ В ЯКОБИАНЕ ГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВОЙ РОДА 2 В ПРОЕКТИВНЫХ КООРДИНАТАХ

В.Ю. Ковтун, С.И. Збитнев

В работе предлагается модификация метода арифметических преобразований дивизоров в якобиане гиперэллиптической кривой над полями как четной, так и нечетной характеристики в проективных координатах, обеспечивающая повышение оперативности системы криптографической защиты в информационно-телекоммуникационных системах.

1. Введение

Стремительное развитие информационных технологий выдвигает жесткие требования к современным информационно-телекоммуникационным системам (ИТС) по обеспечению конфиденциальности, целостности, наблюдаемости и достоверности создающейся, циркулирующей и хранящейся в них информации. Примером такой ИТС может служить ИТС банка. Исследования [20] показали, что такие требования к ИТС могут быть обеспечены посредством использования в ИТС системы криптографической защиты информации, включающей подсистему криптопреобразований с открытым ключом.

В основу современных методов криптографической защиты информации с открытым ключом положены преобразования в группе точек эллиптической кривой (ЭК). Использование таких криптопримитивов в ряде стран положено в основу криптографических стандартов [16-19]. В настоящее время преобразования в якобиане гиперэллиптической кривой (ГЭК) рассматриваются как наиболее перспективная замена ЭК, т.к. это позволяет образовывать большее количество абелевых групп и при существенно меньшем размере базового поля обеспечивать соизмеримую стойкость. В стандартах [16-19] описаны криптографические примитивы, где основной операцией является скалярное умножение точки ЭК. В основе криптографических преобразований в якобиане ГЭК также лежит скалярное умножение [12], но не точки, а приведенных дивизоров. Базовыми операциями для скалярного умножения дивизоров в приведенном представлении (для краткости – дивизоров) являются сложение и удвоение дивизоров.

Вместе с тем, увеличение количества вкладчиков и популярности удаленных средств управления банковскими счетами приводит к постоянному росту нагрузки на систему защиты информации и, в частности на подсистему криптопреобразований с открытым ключом, что приводит к снижению оперативности обслуживания клиентов.

Поэтому, существенное снижение вычислительной сложности (для краткости – сложности) в отношении трудоемкости криптографических примитивов на основе преобразований дивизоров в якобиане ГЭК может быть

достигнуто, в соответствии со сказанным выше, за счет снижения сложности операции скалярного умножения дивизоров.

До сих пор арифметические преобразования в якобиане ГЭК выполнялись посредством метода Кантора [11] с модификациями, сделанными Коблицем [4] и считались сложными, как с точки зрения описания, так и вычислений, что не позволяло их применять на практике в криптографических целях.

Поэтому в последнее время зарубежными и отечественными учеными [1-15] значительное внимание уделяется повышению эффективности преобразований в якобиане ГЭК с фиксированным родом, что привело к появлению усовершенствованных методов арифметических преобразований в якобиане ГЭК. Методы сложения и удвоения для кривых второго рода были рассмотрены в работах [9, 10]. Первая практическая реализация этих методов была произведена Харлеем [8]. Обобщение результатов [8] для кривых над полями четной характеристики приведено в [6]. Дальнейшее развитие методов сложения и удвоения описано в работах [3, 14], чьи результаты также были обобщены для кривых над полями четной характеристики в [7, 15].

Однако, анализ вычислительной сложности известных методов арифметических преобразований в якобиане ГЭК рода 2 над полями четной и нечетной характеристики, показывает, что существующие методы не обеспечивают требуемый уровень оперативности обслуживания банковских клиентов.

Действительно, согласно исследованиям [7], время, необходимое для выполнения скалярного умножения дивизора, по методу Харлея в якобиане ГЭК рода 2 над полем $GF(2^{81})$ на рабочей станции с процессором Intel Pentium IV@1,5 GHz составляет 18,87 мс, что не обеспечивает заданного уровня оперативности обслуживания банковских клиентов. В этих условиях задача повышения производительности системы защиты информации 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 над полями, как четной, так и нечетной характеристики, далее рассмотрим кривые этого вида.

Как известно из [1, 4], в операциях сложения и удвоения дивизоров в якобиане ГЭК присутствует наиболее сложная полевая операция – инвертирование. Согласно [1, 2], для поля нечетной характеристики сложность операции инвертирования I_{inv} принимает значения на интервале $(40I_{mul}, 80I_{mul})$ [2], а для поля четной характеристики – на интервале $(6I_{mul}, 11I_{mul})$ [1], где I_{mul} – сложность операции умножения в поле. В [3], 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 [4, 5], результаты которых были улучшены и распространены на более широкий класс ГЭК над полем

четной характеристики в работах [4, 5]. Эти методы далее рассматриваются как прототип для разработки их более эффективной модификации.

По аналогии с ЭК, обычное 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, а 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 $[U_1, U_0, V_1, V_0, Z]$ [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 $[U_1, U_0, V_1, V_0, Z_1, Z_2]$ [5].

В соответствии с введенными конструкциями, целью работы является модификация метода арифметических преобразований в якобиане ГЭК второго рода в проективных координатах, в отношении понижения его сложности, для повышения производительности операции скалярного умножения.

В соответствии с принятой моделью [7, 8], 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.

2. Арифметические операции в проективных координатах в якобиане ГЭК с пониженной сложностью

В основу предложенной модификации, обеспечивающей понижение сложности, положен метод Харлея [8], а также его модификация [6]. С этой целью в описанном методе предлагается использовать проективное представление дивизоров.

Алгоритм сложения дивизоров в соответствии с методом Харлея [6, 8] для типового случая можно представить следующим образом.

Алгоритм А. Сложение дивизоров ГЭК рода 2

Вход: Приведенный дивизор $D_1 = [u_1, v_1]$ и $D_2 = [u_2, v_2]$

Выход: Приведенный дивизор $D_3 = [u_3, v_3] = D_1 + D_2$

1. $k = \dfrac{f - v_1 h - v_1^2}{u_1}$; (целая часть от деления)
2. $s \equiv \dfrac{v_2 - v_1}{h + 2v_1} \bmod u_1$;
3. $z = s u_1$;
4. $u' = \dfrac{k - s(z + h + 2v_1)}{u_2}$; (целая часть от деления)
5. $u_3 = \mathrm{monic}(u')$;
6. $v_3 \equiv -(h + z + v_1) \bmod u_3$;
7. Return $[u_3, v_3]$.

Алгоритм удвоения дивизоров в соответствии с методом Харлея [6, 8] для типового случая можно представить следующим образом.

Алгоритм В. Удвоение дивизора ГЭК рода 2
Вход: Приведенный дивизор $D_1 = [u_1, v_1]$
Выход: Приведенный дивизор $D_2 = [u_2, v_2] = 2D_1$

1. $k = \dfrac{v_1^2 - v_1 h - f}{u_1}$; (целая часть от деления)
2. $s \equiv \dfrac{k}{h + 2v_1} \bmod u_1$;
3. $u' = s^2 + \dfrac{k - s(h + 2v_1)}{u_1}$; (целая часть от деления)
4. $u_2 = monic(u')$;
5. $v_2 \equiv -(h + su_1 + v_1) \bmod u'$;
6. Return (u_2, v_2).

В алгоритмах А и В 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 А и В следующим образом (в скобках указаны шаги алгоритмов, к которым относятся эти модификации):

- с целью ограничения степени полиномиальных функций/ задающих дивизор, и перехода от операций в кольце полиномиальных функций непосредственно к операциям в поле используются ГЭК небольшого фиксированного рода (в данном случае второго) [8, 9] (на всех шагах);
- с целью упрощения процедур арифметических операций в кольце полиномиальных функций выполняется их нормализация (А.3, В.2);
- с целью нормализации и минимизации веса по Хеммингу параметров $h(x)$ и $f(x)$ ГЭК используется ГЭК особого вида [3, 7] (А.1, А.2, А.4, А.6, В.1, В.2, В.3, В.5);
- с целью одновременного инвертирования нескольких элементов поля используется метод Монтгомери [6-8] (А.2, В.2)
- с целью умножения полиномиальных функций различных степеней используется метод Карацубы [6] (А.1, А.2, А.3, А.4, В.1, В.2, В.3, В.5);
- с целью приведения по модулю полиномиальных функций различных степеней используется метод Карацубы [8] (А.3, В.2);
- с целью исключения операций мультипликативного инвертирования в поле используется проективное представление дивизоров [3, 4] (А.2, А.5, В.2, В.4).

Арифметика в якобиане ГЭК над полем четной характеристики

На основе использования 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 $h = h_2x^2 + h_1x + h_0$, $h_i \in \mathbf{F}_2$ и $f = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$, $f_4 \in \mathbf{F}_2$, $f_i \in \mathbf{F}_q$.

Алгоритм 1. Сложение приведенных дивизоров

Вход:	$[U_{11}, U_{10}, V_{11}, V_{10}, Z_1]$, $[U_{21}, U_{20}, V_{21}, V_{20}, Z_2]$
Выход:	$[U_1', U_0', V_1', V_2', Z'] = [U_{11}, U_{10}, V_{11}, V_{10}, Z_1] + [U_{21}, U_{20}, V_{21}, V_{20}, Z_2]$

	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 почти 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 <Рассматривается особый случай>	$8I_{mul}$
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 $u' = (s(l + h + 2v_1) - k)u_1^{-1}$, $k = (f - v_1h - v_1^2)/u_1$, $u' = x^2 + u_1'x + u_0'$: $\widetilde{U}_0' = s_2^2 + s_1 \cdot y_1 \cdot (s_1 \cdot U_{11} - 2s_2) + y_2 \cdot w_1 + 2w_4 \cdot \widetilde{V}_{21} + h_1\widetilde{R} +$ $+ R \cdot [h_2(s_2 - s_1U_{11}) + r \cdot (y_1 + 2\widetilde{U}_{21} - f_4Z)]$ $\widetilde{U}_1' = 2w_2 - s_3 \cdot s_1y_1 + h_2\widetilde{R} - R^2$	$2I_{sqr}$, $8I_{mul}$
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 $v' \equiv -(h + s_1l + v_2) \bmod u'$, $v' = v_1'x + v_0'$: $V_1' = \widetilde{U}_1' \cdot (l_2 - \widetilde{U}_1' + h_2\widetilde{R}) + s_3^2 \cdot (\widetilde{U}_0' - h_0\widetilde{R} - w_4\widetilde{V}_{21} - l_1)$, $V_0' = \widetilde{U}_0' \cdot (l_2 - \widetilde{U}_1' + h_2\widetilde{R}) - s_3^2 \cdot (l_0 + h_2\widetilde{R} + w_4 \cdot \widetilde{V}_{20})$	$5I_{mul}$
		$4I_{sqr}$, $46I_{mul}$

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. Смешанное сложение приведенных дивизоров

Вход:	$[U_{11}, U_{10}, V_{11}, V_{10}, 1]$, $[U_{21}, U_{20}, V_{21}, V_{20}, Z_2]$
Выход:	$[U_1', U_0', V_1', V_2', Z'] = [U_{11}, U_{10}, V_{11}, V_{10}, 1] + [U_{21}, U_{20}, V_{21}, V_{20}, Z_2]$

	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 почти 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 <Рассматривается особый случай>	$7I_{mul}$
5	Предвычисления: $R = r \cdot Z_2,\quad s_2 = s_0 \cdot Z_2,\quad s_3 = s_1 \cdot Z_2,\quad \widetilde{R} = R \cdot s_3,\quad w_0 = s_1 \cdot s_0,\quad w_1 = s_1 \cdot s_3,$ $w_2 = s_0 \cdot s_3,\ w_3 = w_1 \cdot U_{21},\ w_4 = R \cdot s_1$	$9I_{mul}$
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 $u' = (s(l + h + 2v_1) - k) u_1^{-1}$, $k = (f - v_1 h - v_1^2)/u_1$, $u' = x^2 + u_1' x + u_0'$: $\widetilde{U}_0' = s_2^2 + s_1 \cdot y_1 \cdot (s_1 \cdot \widetilde{U}_{11} - 2s_2) + y_2 \cdot w_1 + 2w_4 \cdot V_{21} + h_1 \widetilde{R} +$ $+ R \cdot [h_2 (s_2 - s_1 \widetilde{U}_{11}) + r \cdot (y_1 + 2U_{21} - f_4 Z_2)]$ $\widetilde{U}_1' = 2w_2 - s_3 \cdot s_1 y_1 + h_2 \widetilde{R} - R^2$	$2I_{sqr}$, $8I_{mul}$
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 $v' \equiv -(h + s_1 l + v_2) \bmod u'$, $v' = v_1' x + v_0'$: $V_1' = \widetilde{U}_1' \cdot (l_2 - \widetilde{U}_1' + h_2 \widetilde{R}) + s_3^2 \cdot (\widetilde{U}_0' - h_0 w_5 - w_4 V_{21} - l_1),$ $V_0' = \widetilde{U}_0' \cdot (l_2 - \widetilde{U}_1' + h_2 \widetilde{R}) - s_3^2 \cdot (l_0 + h_2 w_5 + w_4 \cdot V_{20})$	$5I_{mul}$
		$4I_{sqr}$, $39I_{mul}$

Алгоритм удвоения дивизора в типовом случае имеет вид.

Алгоритм 3. Удвоение приведенного дивизора

Вход:	$[U_1, U_0, V_1, V_0, Z]$
Выход:	$[U_1', U_0', V_1', V_2', Z'] = 2[U_1, U_0, V_1, V_0, Z]$

	Выражение	Количество операций
1	Предвычисления: $Z_2 = Z^2,\ \widetilde{V}_1 = h_1 Z + 2V_1 - h_2 U_1,\ \widetilde{V}_0 = h_0 Z + 2V_0 - h_2 U_2.$	$1I_{sqr}$

2	Вычисление результанты r для u и $h+2v$ (причем $\widetilde{v} \equiv (h+2v) \bmod u$): $w_0 = V_1^2$, $w_1 = U_1^2$, $w_2 = \widetilde{V}_1^2 = h_1^2 Z_2 + 4w_0 - h_2^2 w_1$, $w_3 = \widetilde{V}_0 \cdot Z - U_1 \cdot \widetilde{V}_1$, $r = \widetilde{V}_0 \cdot w_3 + w_2 \cdot U_0$.	$2I_{sqr}$, $4I_{mul}$
3	Вычисление почти 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 $k \equiv \left[\left(f - hv - v^2\right)/u\right] \bmod u$, $k = k_1 x + k_0$: $w_3 = f_3 \cdot Z_2 + w_1$, $w_4 = 2U_0$, $k_1 = 2w_1 + w_3 - Z \cdot \left(w_4 + 2f_4 U_1 + h_2 V_1\right)$, $k_0 = U_1 \cdot \left(Z \cdot \left(2w_4 + f_4 U_1 + h_2 V_1\right) - w_3\right) +$ $+ Z \cdot \left(Z \cdot \left(f_2 \cdot Z - h_1 V_1 - h_2 V_0 - 2f_4 U_0\right) - w_0\right)$.	$7I_{mul}$
5	Вычисление $s = k \cdot inv \bmod u$, $s = s_1 x + s_0$: $w_0 = k_0 \cdot inv_0$, $w_1 = k_1 \cdot inv_1$, $s_0 = w_0 - Z \cdot U_0 \cdot w_1$, $s_3 = \left(inv_0 + inv_1\right) \cdot \left(k_0 + k_1\right) - w_0 - w_1 \cdot \left(1 + U_1\right)$, $s_1 = s_3 \cdot Z$. If $s_1 = 0$ then <Рассматривается особый случай>	$7I_{mul}$
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 $l = su$, $l = l_2 x^2 + l_1 x + l_0$: $l_0 = U_0 \cdot w_1$, $l_2 = U_1 \cdot w_0$, $l_1 = \left(w_1 + w_0\right) \cdot \left(U_1 + U_0\right) - l_0 - l_2$.	$3I_{mul}$
8	Вычисление $u' = \left[l^2 + \frac{1}{s} l(2v + h) - \frac{1}{s^2}\left(f - vh - v^2\right)\right]/u^2$, $u' = x^2 + u_1' x + u_0'$: $\widetilde{U}_0' = s_0^2 + 2w_4 \cdot V_1 + R \cdot \left(s_3 \cdot \left(h_1 Z - h_2 U_1\right) + h_2 s_0 + R \cdot \left(2U_1 - f_4 Z\right)\right)$, $\widetilde{U}_1' = 2w_3 + h_2 \widetilde{R} - R^2$.	$2I_{sqr}$, $4I_{mul}$
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 $v' \equiv -\left(h + s_1 l + v_2\right) \bmod u'$, $v' = v_1' x + v_0'$: $V_1' = \widetilde{U}_1' \cdot \left(l_2 - \widetilde{U}_1' + w_3 + h_2\right) + s_1^2 \cdot \left(\widetilde{U}_0' - h_1 \widetilde{R} - w_4 V_1 - l_1\right)$, $V_0' = \widetilde{U}_0' \cdot \left(l_2 - \widetilde{U}_1' + w_3 + h_2\right) - s_1^2 \cdot \left(l_0 + h_0 \widetilde{R} + w_4 \cdot V_0\right)$.	$5I_{mul}$
		$6I_{sqr}$, $39I_{mul}$

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. Смешанное удвоение приведенного дивизора

Вход:	$\left[U_1, U_0, V_1, V_0, 1\right]$
Выход:	$\left[U_1', U_0', V_1', V_2', Z'\right] = 2\left[U_1, U_0, V_1, V_0, 1\right]$

	Выражение	Количество операций
1	Предвычисления: $\widetilde{V}_1 = h_1 + 2V_1 - h_2 U_1$, $\widetilde{V}_0 = h_0 + 2V_0 - h_2 U_2$.	

2	Вычисление результанты r для u и $h+2v$ (причем $\widetilde{v} \equiv (h+2v) \bmod u$): $w_0 = V_1^2,\ w_1 = U_1^2,\ w_2 = \widetilde{V}_1^2 = h_1^2 + 4w_0 - h_2^2 w_1,\ w_3 = \widetilde{V}_0 - U_1 \cdot \widetilde{V}_1,$ $r = \widetilde{V}_0 \cdot w_3 + w_2 \cdot U_0.$	$2I_{sqr},\ 3I_{mul}$
3	Вычисление почти 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 $k \equiv \left[\left(f - hv - v^2\right)/u\right] \bmod u,\ k = k_1 x + k_0$: $w_3 = f_3 + w_1,\ w_4 = 2U_0,$ $k_1 = 2w_1 + w_3 - \left(w_4 + 2f_4 U_1 + h_2 V_1\right),\ k_0 = U_1 \cdot \left(\left(2w_4 + f_4 U_1 + h_2 V_1\right) - w_3\right) +$ $+ \left(f_2 - h_1 V_1 - h_2 V_0 - 2f_4 U_0\right) - w_0.$	$1I_{mul}$
5	Вычисление $s = k \cdot inv \bmod u,\ s = s_1 x + s_0$: $w_0 = k_0 \cdot inv_0,\ w_1 = k_1 \cdot inv_1,\ s_0 = w_0 - U_0 \cdot w_1,$ $s_1 = \left(inv_0 + inv_1\right) \cdot \left(k_0 + k_1\right) - w_0 - w_1 \cdot \left(1 + U_1\right).$ If $s_1 = 0$ then <Рассматривается особый случай>	$5I_{mul}$
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 $l = su,\ l = l_2 x^2 + l_1 x + l_0$: $l_0 = U_0 \cdot w_1,\ l_2 = U_1 \cdot w_0,\ l_1 = \left(w_1 + w_0\right) \cdot \left(U_1 + U_0\right) - l_0 - l_2.$	$3I_{mul}$
8	Вычисление $u' = \left[l^2 + \frac{1}{s} l\left(2v + h\right) - \frac{1}{s^2}\left(f - vh - v^2\right)\right]/u^2,\ u' = x^2 + u_1' x + u_0'$: $\widetilde{U}_0' = s_0^2 + 2\widetilde{R} \cdot V_1 + h_1 \widetilde{R} + r \cdot \left(h_2 s_0 - U_1 \cdot \left(2r - h_2 s_1\right) - f_4 r\right),\ \widetilde{U}_1' = 2w_1 + h_2 \widetilde{R} - r^2.$	$2I_{sqr},\ 3I_{mul}$
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 $v' \equiv -\left(h + s_1 l + v_2\right) \bmod u',\ v' = v_1' x + v_0'$: $V_1' = \widetilde{U}_1' \cdot \left(l_2 - \widetilde{U}_1' + w_1 + h_2\right) + w_0 \cdot \left(\widetilde{U}_0' - h_1 \widetilde{R} - \widetilde{R} V_1 - l_1\right),$ $V_0' = \widetilde{U}_0' \cdot \left(l_2 - \widetilde{U}_1' + w_1 + h_2\right) - w_0 \cdot \left(l_0 + h_0 \widetilde{R} + \widetilde{R} \cdot V_0\right).$	$5I_{mul}$
		$5I_{sqr},\ 25I_{mul}$

Рассмотрим арифметические преобразования над дивизорами в якобиане ГЭК над полями четной характеристики. Использование ГЭК над такими полями заведомо позволяет сократить количество полевых операций в алгоритмах арифметических преобразований, за счет приведения подобных слагаемых.

Арифметика в якобиане ГЭК над полем четной характеристики

В соответствии с предложенными модификациями алгоритмов сложения и удвоения дивизоров в типовом случае, приведем разработанные алгоритмы преобразований в якобиане ГЭК заданной уравнением $v^2 + h(u)v = f(u)$ над полем $\mathbf{F}_q$ четной характеристики в проективных координатах, где $h(x) = x$ и $f = x^5 + f_1 x + f_0,\ f_i \in \mathbf{F}_2$.

Алгоритм 5. Сложение приведенных дивизоров	
Вход:	$[U_{11}, U_{10}, V_{11}, V_{10}, Z_1],\ [U_{21}, U_{20}, V_{21}, V_{20}, Z_2]$
Выход:	$[U_1', U_0', V_1', V_2', Z'] = [U_{11}, U_{10}, V_{11}, V_{10}, Z_1] + [U_{21}, U_{20}, V_{21}, V_{20}, Z_2]$

	Выражение	Количество операций
1	Предвычисления: $Z = Z_1 \cdot Z_2$, $\widetilde{U}_{21} = Z_1 \cdot U_{21}$, $\widetilde{U}_{20} = Z_1 \cdot U_{20}$, $\widetilde{V}_{21} = Z_1 \cdot V_{21}$, $\widetilde{V}_{20} = Z_1 \cdot V_{20}$, $y_0 = U_{11} \cdot y_1$.	$5I_{mul}$
2	Вычисление результанты r для u_1 и u_2: $y_1 = U_{11} \cdot Z_2 - \widetilde{U}_{21}$, $y_2 = \widetilde{U}_{20} - U_{10} \cdot Z_2$, $y_3 = y_0 + y_2 \cdot Z_1$, $r = y_2 \cdot y_3 + y_1^2 \cdot U_{10}$	$1I_{sqr}$, $6I_{mul}$
3	Вычисление почти инверсии $inv = r/u_2 \bmod u_1$, $inv = inv_1 x + inv_0$: $inv_1 = y_1$, $inv_0 = y_3$	
4	Вычисление $s = (v_1 - v_2) inv \bmod u_1$, $s = s_1 x + s_0$: $w_0 = V_{10} \cdot Z_2 - \widetilde{V}_{20}$, $w_1 = V_{11} \cdot Z_2 - \widetilde{V}_{21}$, $w_2 = inv_0 \cdot w_0$, $w_3 = inv_1 \cdot w_1$, $s_1 = (inv_0 + Z_1 \cdot inv_1) \cdot (w_0 + w_1) - w_2 - w_3 \cdot (Z_1 + U_{11})$, $s_0 = w_2 - U_{10} \cdot w_3$ If $s_1 = 0$ then <Рассматривается особый случай>	$8I_{mul}$
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 $l = su_2$, $l = x^3 + l_2 x^2 + l_1 x + l_0$: $l_0 = w_0 \cdot \widetilde{U}_{20}$, $l_2 = w_3 + w_2$, $l_1 = (w_1 + w_0) \cdot (\widetilde{U}_{21} + \widetilde{U}_{20}) - l_0 - w_3$	$2I_{mul}$
7	Вычисление $u' = (s(l + h + 2v_1) - k) u_1^{-1}$, $k = (f - v_1 h - v_1^2)/u_1$, $u' = x^2 + u_1' x + u_0'$: $\widetilde{U}_0' = s_2^2 + s_1^2 \cdot y_1 U_{11} + y_2 \cdot w_1 + \widetilde{R} + R \cdot r \cdot y_1$, $\widetilde{U}_1' = w_1 \cdot y_1 - R^2$	$2I_{sqr}$, $5I_{mul}$
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 $v' \equiv -(h + s_1 l + v_2) \bmod u'$, $v' = v_1' x + v_0'$: $V_1' = \widetilde{U}_1' \cdot (l_2 - \widetilde{U}_1') + s_3^2 \cdot (\widetilde{U}_0' - w_4 \cdot \widetilde{V}_{21} - l_1)$, $V_0' = \widetilde{U}_0' \cdot (l_2 - \widetilde{U}_1') - s_3^2 \cdot (l_0 + w_4 \cdot \widetilde{V}_{20})$	$6I_{mul}$
		$4I_{sqr}$, $44I_{mul}$

Алгоритм смешанного сложения дивизоров имеет вид.

Алгоритм 6. Смешанное сложение приведенных дивизоров	
Вход:	$[U_{11}, U_{10}, V_{11}, V_{10}, 1]$, $[U_{21}, U_{20}, V_{21}, V_{20}, Z_2]$
Выход:	$[U_1', U_0', V_1', V_2', Z'] = [U_{11}, U_{10}, V_{11}, V_{10}, 1] + [U_{21}, U_{20}, V_{21}, V_{20}, Z_2]$

	Выражение	Количество операций
1	Предвычисления: $\widetilde{U}_{11} = Z_2 \cdot U_{11}$, $y_0 = U_{11} \cdot y_1$.	$1I_{mul}$
2	Вычисление результанты r для u_1 и u_2: $y_1 = \widetilde{U}_{11} - U_{21}$, $y_2 = U_{20} - U_{10} \cdot Z_2$, $y_3 = y_0 + y_2$, $r = y_2 \cdot y_3 + y_1^2 \cdot U_{10}$	$1I_{sqr}$, $4I_{mul}$
3	Вычисление почти инверсии $inv = r/u_2 \bmod u_1$, $inv = inv_1 x + inv_0$: $inv_1 = y_1$, $inv_0 = y_3$	
4	Вычисление $s = (v_1 - v_2) inv \bmod u_1$, $s = s_1 x + s_0$: $w_0 = V_{10} \cdot Z_2 - V_{20}$, $w_1 = V_{11} \cdot Z_2 - V_{21}$, $w_2 = inv_0 \cdot w_0$, $w_3 = inv_1 \cdot w_1$,	$7I_{mul}$

	$s_1 = (inv_0 + inv_1)\cdot(w_0 + w_1) - w_2 - w_3\cdot(U_{11}+1)$, $s_0 = w_2 - U_{10}\cdot w_3$ If $s_1 = 0$ then <Рассматривается особый случай>	
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 $l = su_2$, $l = l_2x^2 + l_1x + l_0$: $l_0 = w_0\cdot U_{20}$, $l_2 = w_3 + w_2$, $l_1 = (w_1 + w_0)\cdot(U_{21} + U_{20}) - l_0 - w_3$	$2I_{mul}$
7	Вычисление $u' = (s(l + h + 2v_1) - k)u_1^{-1}$, $k = (f - v_1h - v_1^2)/u_1$, $u' = x^2 + u_1'x + u_0'$: $\widetilde{U}_0' = s_2^2 + s_1^2\cdot y_1U_{11} + y_2\cdot w_1 + \widetilde{R} + R\cdot r\cdot y_1$, $\widetilde{U}_1' = w_1\cdot y_1 + R^2$	$2I_{sqr}$, $5I_{mul}$
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 $v' \equiv -(h + s_1l + v_2) \bmod u'$, $v' = v_1'x + v_0'$: $V_1' = \widetilde{U}_1'\cdot(l_2 + \widetilde{U}_1') + s_3^2\cdot(\widetilde{U}_0' + w_4\cdot V_{21} + l_1)$, $V_0' = \widetilde{U}_0'\cdot(l_2 + \widetilde{U}_1') + s_3^2\cdot(l_0 + w_4\cdot V_{20})$	$6I_{mul}$
		$4I_{sqr}$, $37I_{mul}$

Алгоритм удвоения дивизора в типовом случае представлен ниже.

Алгоритм 7. Удвоение приведенного дивизора

Вход:	$[U_1, U_0, V_1, V_0, Z]$
Выход:	$[U_1', U_0', V_1', V_2', Z'] = 2[U_1, U_0, V_1, V_0, Z]$

	Выражение	Количество операций
1	Предвычисления: $Z_2 = Z^2$, $w_0 = V_1^2$, $w_1 = U_1^2$.	$1I_{sqr}$
2	Вычисление результанты r для u и $h + 2v$ (причем $\widetilde{v} \equiv (h + 2v) \bmod u$): $R = U_0\cdot Z_2^2$.	$2I_{sqr}$, $1I_{mul}$
3	Вычисление почти инверсии $inv \equiv r/\widetilde{v} \bmod u$, $inv = inv_1x + inv_0$: $inv_1 = Z$, $inv_0 = Z\cdot U_1$.	$1I_{mul}$
4	Вычисление $k \equiv [(f - hv - v^2)/u] \bmod u$, $k = k_1x + k_0$: $k_1 = w_1$, $k_0 = U_1\cdot w_1 + Z\cdot(Z\cdot V_1 + w_0)$.	$3I_{mul}$
5	Вычисление $s = k\cdot inv \bmod u$, $s = s_1x + s_0$: $w_0 = k_0\cdot inv_0$, $w_1 = k_1\cdot Z$, $s_0 = w_0 + Z\cdot U_0\cdot w_1$, $s_3 = (inv_0 + Z)\cdot(k_0 + k_1) + w_0 + w_1\cdot(1 + U_1)$, $s_1 = s_3\cdot Z$. If $s_1 = 0$ then <Рассматривается особый случай>	$7I_{mul}$
6	Предвычисления: $\widetilde{R} = R\cdot s_1$, $w_0 = s_1\cdot s_3$, $w_1 = s_0\cdot s_3$, $w_3 = w_1\cdot Z$, $w_4 = R\cdot s_3$.	$6I_{mul}$
7	Вычисление $l = su$, $l = l_2x^2 + l_1x + l_0$: $l_0 = U_0\cdot w_1$, $l_2 = U_1\cdot w_0$, $l_1 = (w_1 + w_0)\cdot(U_1 + U_0) - l_0 - l_2$.	$3I_{mul}$
8	Вычисление $u' = \left[l^2 + \frac{1}{s}l(2v + h) - \frac{1}{s^2}(f - vh - v^2)\right]/u^2$, $u' = x^2 + u_1'x + u_0'$: $\widetilde{U}_0' = s_0^2 + \widetilde{R}$, $\widetilde{U}_1' = R^2$.	$2I_{sqr}$

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 $v' \equiv -(h + s_1 l + v_2) \bmod u'$, $v' = v_1' x + v_0'$: $V_1' = \widetilde{U}_1' \cdot (l_2 + \widetilde{U}_1' + w_3) + s_1^2 \cdot (\widetilde{U}_0' + \widetilde{R} + w_4 \cdot V_1 + l_1)$, $V_0' = \widetilde{U}_0' \cdot (l_2 + \widetilde{U}_1' + w_3) + s_1^2 \cdot (l_0 + w_4 \cdot V_0)$.	$6I_{mul}$
		$6I_{sqr}$, $30I_{mul}$

Алгоритм смешанного удвоения дивизора в типовом случае представлен ниже.

Алгоритм 8. Смешанное удвоение приведенного дивизора

Вход:	$[U_1, U_0, V_1, V_0, 1]$
Выход:	$[U_1', U_0', V_1', V_2', Z'] = 2[U_1, U_0, V_1, V_0, 1]$

	Выражение	Количество операций
1	Вычисление почти инверсии для $inv \equiv r/\widetilde{v} \bmod u$, $inv = inv_1 x + inv_0$: $inv_1 = 1$, $inv_0 = U_1$.	
2	Вычисление $k \equiv [(f - hv - v^2)/u] \bmod u$, $k = k_1 x + k_0$: $w_0 = V_1^2$, $w_1 = U_1^2$, $k_1 = w_1$, $k_0 = U_1 \cdot w_1 + V_1 + w_0$.	$2I_{sqr}$, $1I_{mul}$
3	Вычисление $s = k \cdot inv \bmod u$, $s = s_1 x + s_0$: $w_0 = k_0 \cdot inv_0$, $w_1 = k_1$, $s_0 = w_0 + U_0 \cdot w_1$, $s_1 = k_0$.	$2I_{mul}$
4	Предвычисления: $\widetilde{R} = U_0 \cdot s_1$, $w_0 = s_1^2$, $w_1 = s_0 \cdot s_1$.	$2I_{mul}$
5	Вычисление $l = su$, $l = l_2 x^2 + l_1 x + l_0$: $l_0 = U_0 \cdot w_1$, $l_2 = U_1 \cdot w_0$, $l_1 = (w_1 + w_0) \cdot (U_1 + U_0) + l_0 + l_2$.	$3I_{mul}$
6	Вычисление $u' = [l^2 + \frac{1}{s} l(2v + h) - \frac{1}{s^2}(f - vh - v^2)]/u^2$, $u' = x^2 + u_1' x + u_0'$: $\widetilde{U}_0' = s_0^2 + \widetilde{R}$, $\widetilde{U}_1' = U_0^2$.	$2I_{sqr}$
7	Корректировка: $U_0' = \widetilde{U}_0' \cdot \widetilde{R}$, $U_1' = \widetilde{U}_1' \cdot \widetilde{R}$, $Z' = w_0 \cdot \widetilde{R}$.	$3I_{mul}$
8	Вычисление $v' \equiv -(h + s_1 l + v_2) \bmod u'$, $v' = v_1' x + v_0'$: $V_1' = \widetilde{U}_1' \cdot (l_2 + \widetilde{U}_1' + w_1) + w_0 \cdot (\widetilde{U}_0' + \widetilde{R} + \widetilde{R} \cdot V_1 + l_1)$, $V_0' = \widetilde{U}_0' \cdot (l_2 + \widetilde{U}_1' + w_1) + w_0 \cdot (l_0 + \widetilde{R} \cdot V_0)$.	$6I_{mul}$
		$4I_{sqr}$, $17I_{mul}$

Анализ вычислительной сложности

В таблице 1 приведены оценки сложности известных [3- 5, 7] 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												
$f_4 = 0$ [7]	1	3	22				1	5	22			
Проективные координаты $[U_1, U_0, V_1, V_0, Z]$												
$\deg(h) = 2,\ h_i \in \mathbf{F}_2$ [4]		4	47		3	40		6	40		5	25
$\deg(h) = 2,\ h_i \in \mathbf{F}_2$ [*]		4	46		4	39		6	39		5	25
Взвешенные координаты $[U_1, U_0, V_1, V_0, Z_1, Z_2, Z_1^2, Z_2^2]$												
$f_4 = 0,\ h(x) = 0$ [5]		7	47		5	36		7	34		5	21
Поле четной характеристики												
Аффинные координаты												
$f_4 = 0$ [7]	1	3	21				1	5	20			
$h_2 = 0,\ f_4 = 0$ [7]	1	3	21				1	5	17			
$h(x) = x,\ f_4 = 0,\ f_3 = f_2 = 0$ [6]							1	6	9			
Проективные координаты $[U_1, U_0, V_1, V_0, Z]$												
$h(x) = x,\ f_4 = 0,\ f_3 = f_2 = 0$ [6]		5	45		5	38		6	31		5	18
$h(x) = x,\ f_4 = 0,\ f_3 = f_2 = 0$ [*]		4	44		4	37		6	30		4	17
Взвешенные координаты $[U_1, U_0, V_1, V_0, Z_1, Z_2, Z_1^2, Z_2^2, Z_1Z_2, Z_1^3Z_2]$												
$f_4 = 0,\ h_2 \neq 0$ [5]		4	46		5	35		6	35		5	24
$f_4 = 0,\ h_2 = 0$ [5]		6	44		6	34		6	29		6	19

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

Из данных, приведенных в таблице 1 видно, что наименьшей сложностью обладают алгоритмы сложения, смешанного сложения, удвоения и смешанного удвоения в проективных координатах для поля нечетной и четной характеристики, построенные согласно модифицированного авторами метода, что приводит к сокращению одной операции умножения в поле по сравнению с [4, 6].

Заключение

В соответствии с целью работы, разработана модификация метода арифметических преобразований в якобиане ГЭК второго рода в проективных координатах, которая обеспечивает пониженную сложность по сравнению с существующими методами [4, 6], что позволяет повысить производительность скалярного умножения. Эта модификация определяется следующим:

- с целью уменьшения количества повторно вычисляемых величин осуществляется предвычисление и хранение результатов, что уменьшает временную сложность по сравнению с [6-8];

- с целью увеличения количества предвычисленных величин изменяется последовательность выполнения полевых операций по сравнению с существующими методами [6-8];
- с целью увеличения количества предвычисленных величин учитываются ранее неизвестные зависимости между результирующими полиномиальными функциями.

Предложенный модифицированный метод арифметических преобразований в якобиане ГЭК второго рода позволяет понизить вычислительную сложность на 3–15%, в зависимости от используемых арифметических операций и вида кривой. Известно [1-2], что сложность операции скалярного умножения в среднем составляет:

$$I_{mul}^{D} = \tfrac{1}{2} t I_{add}^{D} + t I_{dbl}^{D},$$

где t – битовая длина скалярного множителя, I_{add}^{D}, I_{dbl}^{D} - 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 [4, 6].

В частности, при обработке транзакций в процессинговом центре банка это приводит к сокращению времени верификации цифровых подписей на величину порядка 4%.

Литература

1. *D. Hankerson, J. Lopez Hernandez, A. Menezes.* Software implementation of elliptic curve cryptography over binary fields.

2. *M. Brown, D. Hankerson, J. Lopez, A. Menezes.* Software implementation of the NIST elliptic curves over prime fields.

3. *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.

4. *T. Lange.* Inversion-free arithmetic on genius 2 hyperelliptic curves. Cryptology ePrint Archive, report 2002/147, 2002. Available http://eprint.iacr.org.

5. *T. Lange.* Weighted coordinates on genius 2 hyperelliptic curves. Cryptology ePrint Archive, report 2002/153, 2002. Available http://eprint.iacr.org.

6. *T. Wollinger.* Software and hardware implementation of hyperelliptic curve cryptosystems. PhD dissertation. Bochum, Germany, May 2004.

7. *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.

8. *R. Harley.* Fast arithmetic on genius 2 curves. Available at: http://cristal.infra.fr/~harley/hyper. 2000.

9. *A.M. Spallek.* Kurven vom geschlecht 2 und ihre anwendung in public-key-kryptosystemen. PhD thesis, Universitat Gesamthochschule Essen, 1994.

10. *U. Kriger.* Anwendung hyperellipischer kurven in der kryptographie. Master's thesis, Universitat Gesamthochschule Essen, 2001.

11. *D.G. Cantor.* Computing in the jacobian of hyperelliptic curve. Math. Comp., No 48. pp. 95-101, 1987.

12. *N. Koblitz.* Hyperelliptic cryptosystems. Journal of cryptology, No 1. pp.139-150, 1989.

13. *T. Lange.* Efficient arithmetic on hyperelliptic curves. PhD thesis, Universitat Gesamthochschule Essen, 2001.

14. *M. Takahashi.* Improving Harley algorithms for jacobians of genius 2 hyperelliptic curves. In Proc. of SCIS2002, IEICE Japan, 2002. in Japanese.

15. *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.

16. 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.

17. IEEE P1363-2000. Standard Specifications for Public Key Cryptography. Available at: http://www.ieee.org

18. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной подписи. М. Росстандарт.

19. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка.

20. W. Diffie, M. Hellman. New directions in cryptography. IEEE Transactions on information theory. pp. 644-654. November 1976.

Збитнев Станислав Иванович, кандидат технических наук.
Преподаватель кафедры безопасности информационных технологий Национального технического университета радиоэлектроники, пр. Ленина 14, г. Харьков, Украина, 61166.
Круг научных интересов: Защита информационных технологий, криптопреобразования на алгебраических кривых.
e-mail: staszb@ukr.net
Ковтун Владислав Юрьевич.
Адъюнкт кафедры компьютерных систем Харьковского университета Воздушных Сил, ул. Сумская 77/79, г. Харьков, Украина, 61023.
Круг научных интересов: Защита информационных технологий, криптопреобразования на алгебраических кривых.
e-mail: vladislav.kovtun@gmail.com