Методы и алгоритмы арифметических преобразований с пониженной вычислительной сложностью на алгебраических кривых для криптографических приложений

Ковтун Владислав
Харьковский университет
Воздушных Сил

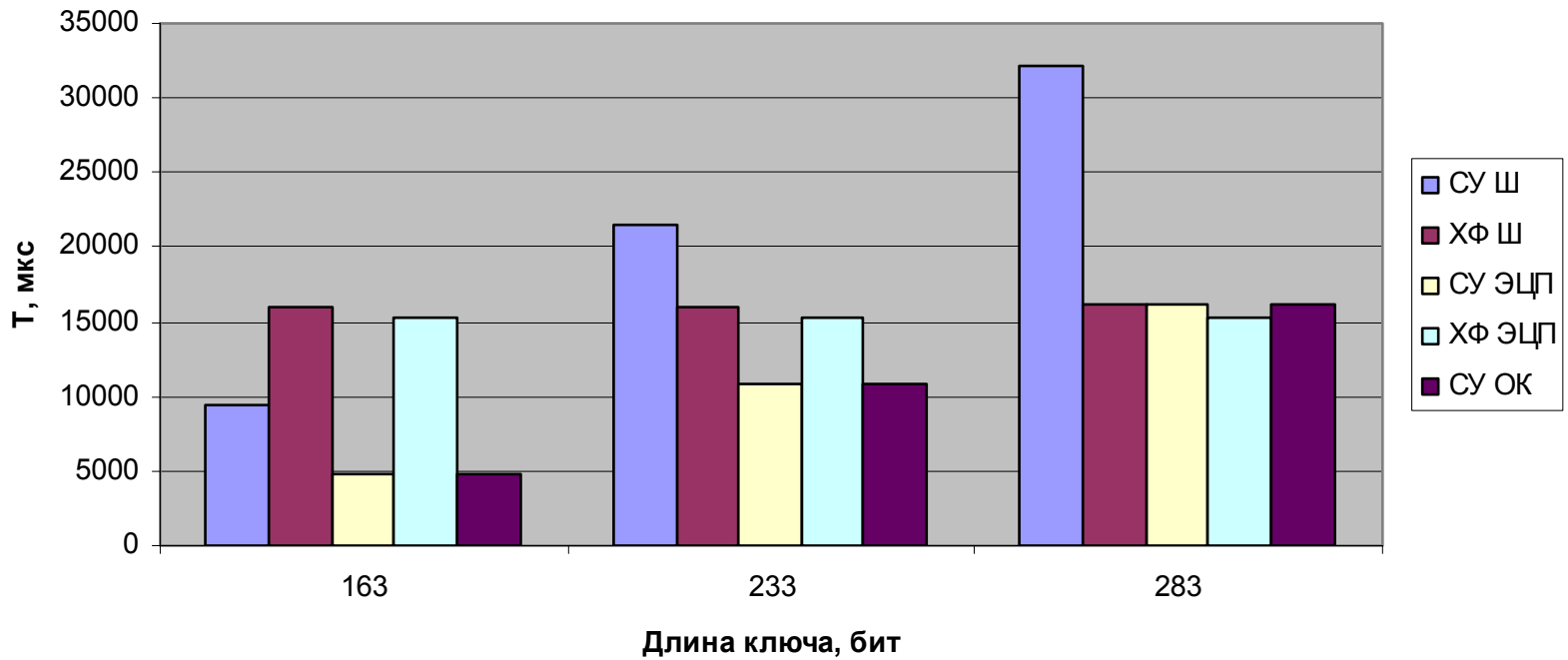
ОБЩИЕ ПОЛОЖЕНИЯ

- **Цель:** повышение быстродействия программно-технического комплекса криптографической защиты информации центров сертификации ключей, путем уменьшения вычислительной сложности алгоритмов криптопреобразований на основе разработки новых методов и алгоритмов арифметических преобразований с пониженной вычислительной сложностью на алгебраических кривых
- **Объект исследований:** процесс криптографических преобразований с открытым ключом на алгебраических кривых в программно-техническом комплексе криптографической защиты информации центров сертификации ключей
- **Предмет исследований:** арифметические преобразования на алгебраических кривых, что применяются для криптопреобразований с открытым ключом

ЧАСТНЫЕ ЗАДАЧИ

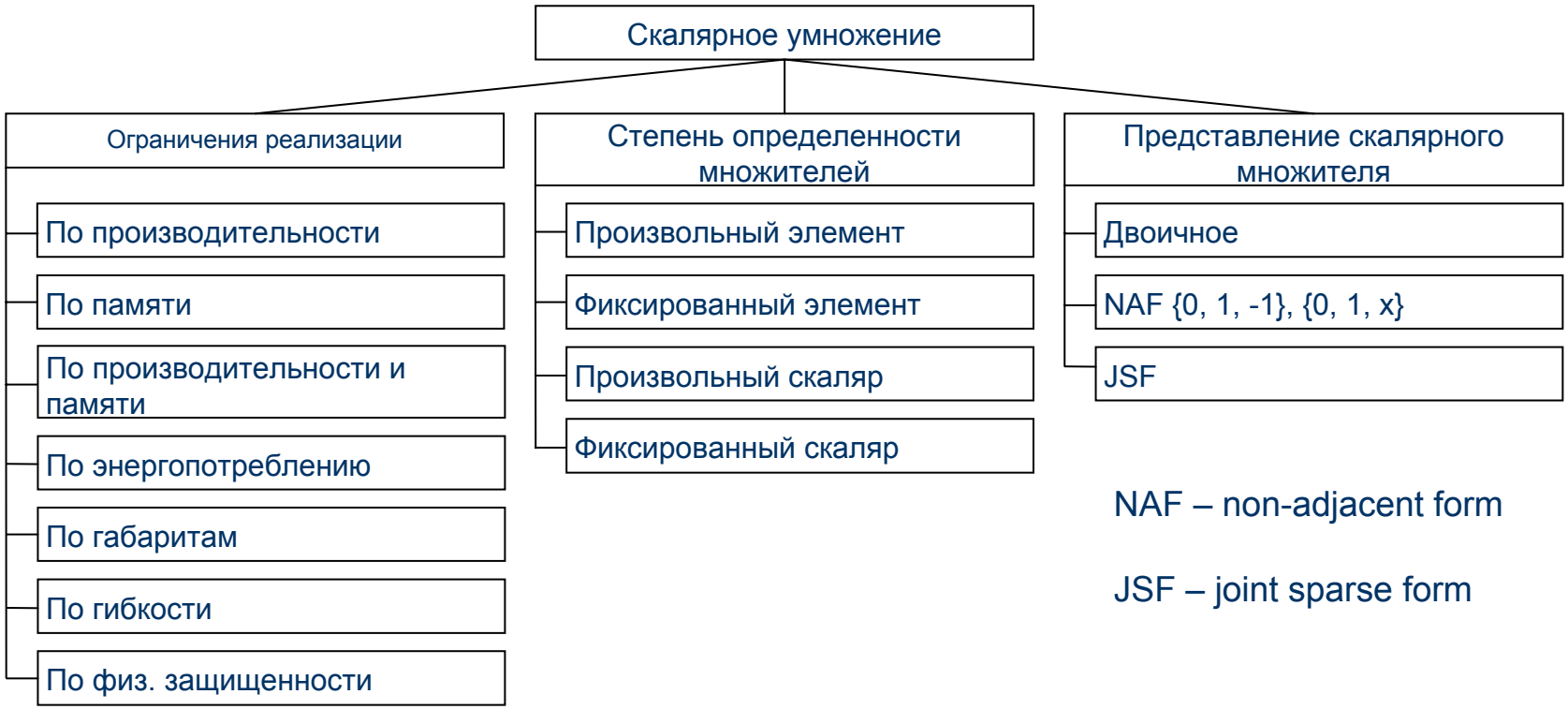
- Разработать алгоритм одновременного скалярного умножения элементов аддитивной группы точек/якобиана дивизоров с пониженной вычислительной сложностью для быстрых криптопреобразований на алгебраических кривых
- Разработать метод арифметических преобразований точек с пониженной вычислительной сложностью в проективных координатах Лопеса-Дахаба для скалярного умножения в группе точек эллиптической кривой над полем четной характеристики
- Разработать методы арифметических преобразований дивизоров с уменьшенной вычислительной сложностью в якобиане гиперэллиптической кривой второго рода над полем как четной так и нечетной характеристики
- Разработать программные модели криптопреобразований на алгебраических кривых, создать на их основе библиотеки
- Экспериментально исследовать разработанные библиотеки

Оценка доли времени основных операций в криптопреобразованиях с открытым ключом



Размер сообщения составляет 16384 байт

КЛАССИФИКАЦИЯ АЛГОРИТМОВ СКАЛЯРНОГО УМНОЖЕНИЯ



NAF – non-adjacent form

JSF – joint sparse form

Рис. Классификация алгоритмов СУ по ограничениям на реализацию, степени определенности множителей, представлению скаляров

КЛАССИФИКАЦИЯ АЛГОРИТМОВ СКАЛЯРНОГО УМНОЖЕНИЯ

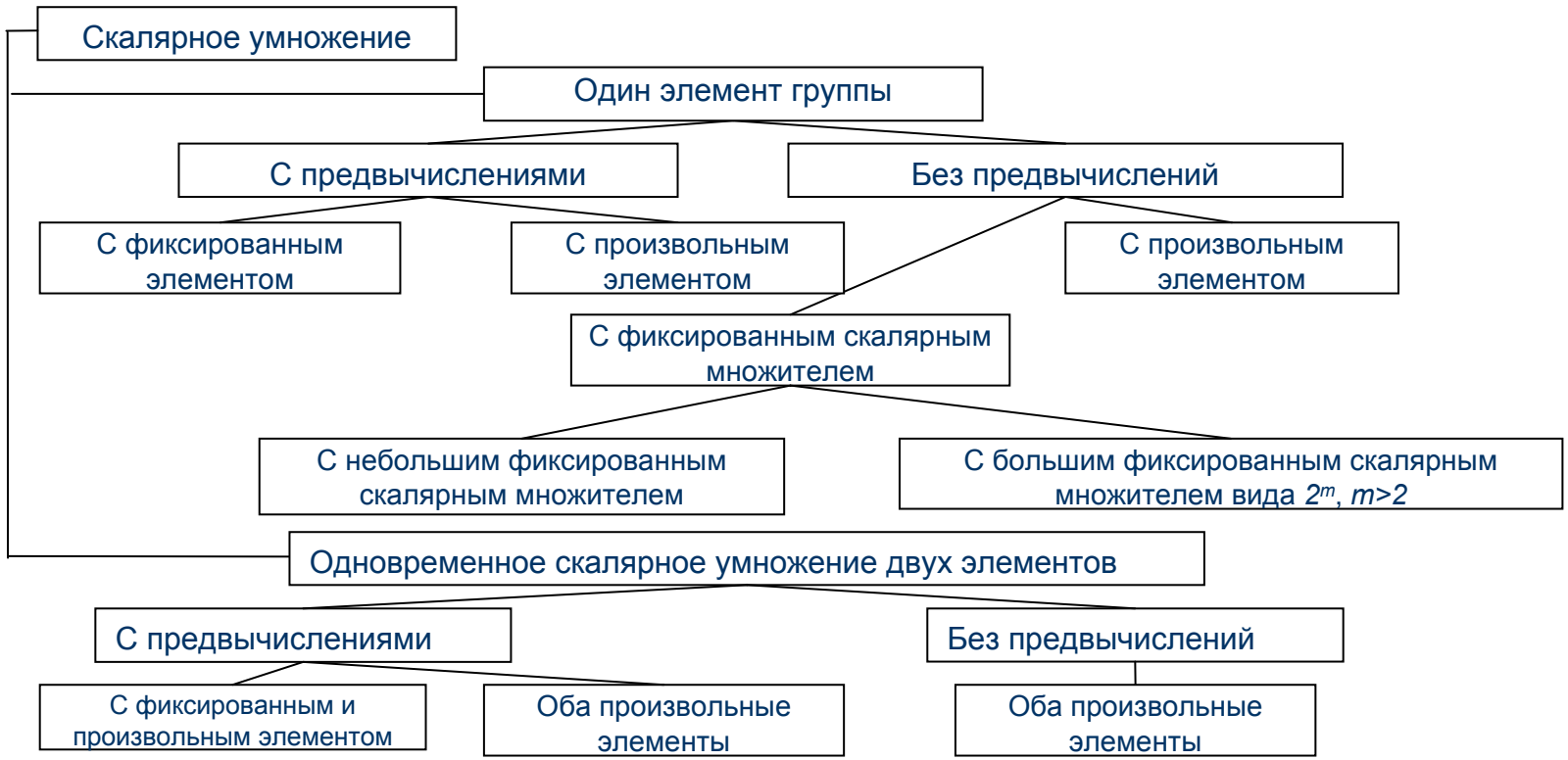


Рис. Классификация алгоритмов скалярного умножения по наличию предвычислений и по степени определенности множителей

УСОВЕРШЕНСТВОВАННЫЙ АЛГОРИТМ ОДНОВРЕМЕННОГО СКАЛЯРНОГО УМНОЖЕНИЯ

Алгоритм одновременного умножения на основе методов Лим-Лии и «оконного» умножения

Вход: скалярные множетели $k = \sum_{r=0}^{h-1}\sum_{s=0}^{v-1}\sum_{j=0}^{b-1} K_{vbr+bs+j}\,2^{vbr+bs+j}$, $l = (l_{d-1}, \ldots, l_1, l_0)_{2^w}$, h, v, w - параметры алгоритма, $a = \lceil t/h \rceil$, $b = \lceil a/v \rceil$, $d = \lceil t/w \rceil$, множители $P, Q \in \mathbf{G}$, такие, что $P = const$, $Q \neq const$ та $\mathbf{G}$ - аддитивная группа

Выход: $R = kP + lQ$

1. For $u = 1$ to $2^h - 1$ do
   1.1. For $s = 0$ to $v - 1$ do
      1.1.1. $u = (u_{h-1}, \ldots, u_1, u_0)_2$, $P_{s,u} \leftarrow 2^{sb}\sum_{i=0}^{h-1} u_i 2^{vbi} P$.
2. $P' \leftarrow O$.
3. For $r = b - 1$ downto 0 do
   3.1. $P' \leftarrow 2P'$.
   3.2. For $s = v - 1$ downto 0 do
      3.2.1. $I_{s,r} \leftarrow \sum_{i=0}^{h-1} 2^i K_{vbi+bs+r}$.
      3.2.2. If $(I_{s,r} \neq 0)$ then $u \leftarrow I_{s,r}$, $P' \leftarrow P' + P_{s,u}$.
4. Вычисление: $Q_i = 2^{wi} Q$, $i = \overline{0, d-1}$.
5. $Q' \leftarrow O$, $B \leftarrow O$.
6. For $j = 2^{w-1}$ downto 1 do
   7.1. For each i for which $k_i = j$ do
      7.1.1. $B \leftarrow B + Q_i$.
   7.2. $Q' \leftarrow Q' + B$.
8. $R \leftarrow P' + Q'$.
9. Return (R).

Алгоритм одновременного умножения на основе комбинированного умножения и «оконного» умножения

Вход: скалярные множители $k = (k_{t-1}, \ldots, k_1, k_0)_2$, $l = (l_{d-1}, \ldots, l_1, l_0)_{2^w}$, w - параметр алгоритма, $d = \lceil t/w \rceil$, множители $P, Q \in \mathbf{G}$, такие, что $P = const$, $Q \neq const$ та $\mathbf{G}$ - аддитивная группа

Выход: $R = kP + lQ$

1. Вычисление: $\sum_{i=0}^{2^w-1} a_i 2^{di} P$, $\forall (a_{w-1}, \ldots, a_0) \in Z_{2^w}$.
2. Представить скалярный множитель в виде:
$k = k_{d(w-1)+(d-1)}2^{d(w-1)+(d-1)} + \cdots k_{d(w-1)}2^{d(w-1)} + k_{d(w-2)+(d-1)}2^{d(w-2)+(d-1)} + \cdots + k_{d(w-w)}2^{d(w-w)}$,.
3. $P' \leftarrow O$.
4. For $i = d - 1$ downto 0 do
   4.1. $P' \leftarrow 2P'$.
   4.2. $P' \leftarrow P' + \left[(k_{d(w-1)+i}, \ldots, k_{d(w-w)+i})\right]P$.
5. Вычисление: $Q_i = 2^{wi} Q$, $i = \overline{0, d-1}$.
6. $Q' \leftarrow O$, $B \leftarrow O$.
7. For $j = 2^{w-1}$ downto 1 do
   7.1. For each i for which $k_i = j$ do
      7.1.1. $B \leftarrow B + Q_i$.
   7.2. $Q' \leftarrow Q' + B$.
8. $R \leftarrow P' + Q'$.
9. Return (R).

УСОВЕРШЕНСТВОВАННЫЙ АЛГОРИТМ ОДНОВРЕМЕННОГО СКАЛЯРНОГО УМНОЖЕНИЯ

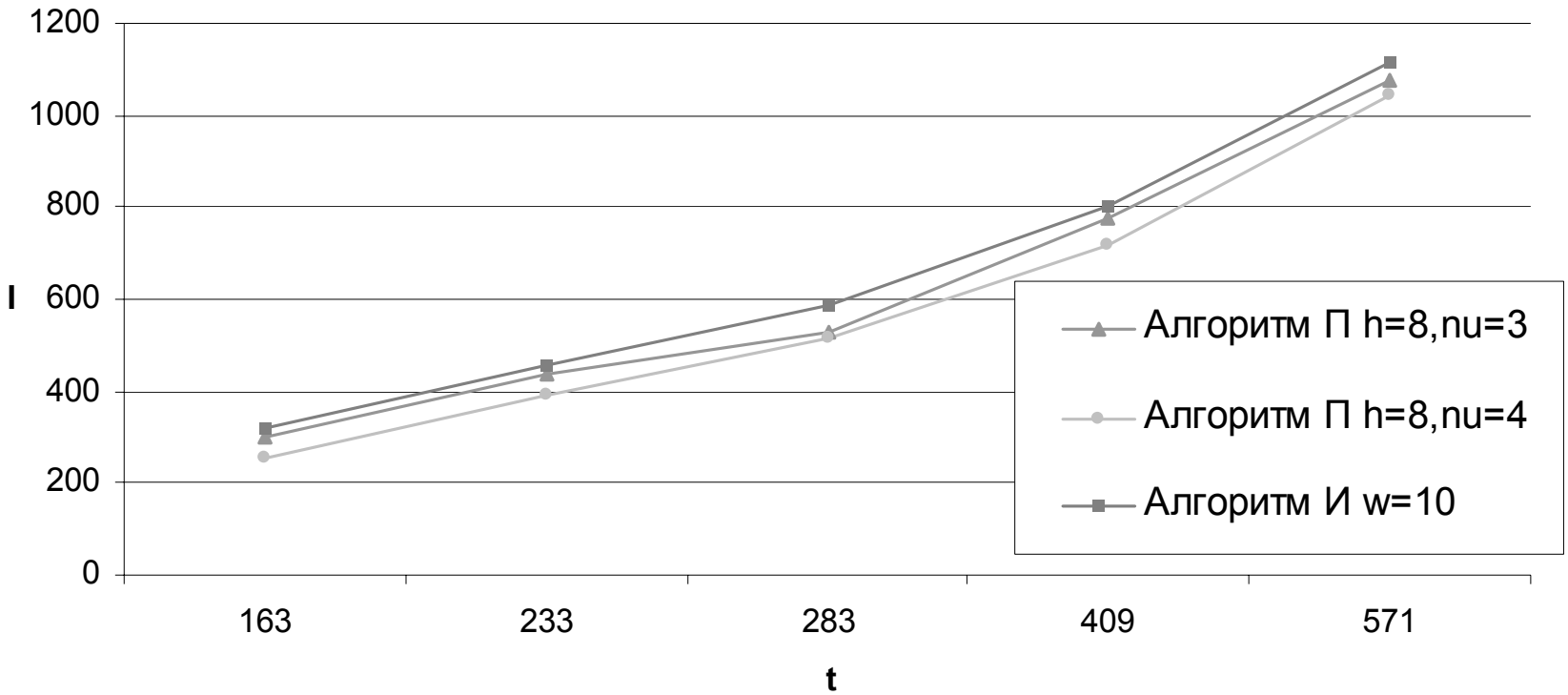
- ***Утверждение 1.*** Вычислительная сложность алгоритма одновременного умножения на основе методов Лим-Лии с параметрами ***h*** и ***v*** и «оконного» умножения шириной окна предвычислений ***w*** для скалярных множителей ***k*** и ***l*** , битовой длины ***t***, составит:

  $$(a(2^h\text{-}1)/2^h\text{-}1)I_{add}+bI_{dbl}+(\mathrm{d}(2^w\text{-}1)/2^w2^w\text{-}3)\ I_{dbl}$$

- ***Утверждение 2.*** Пространственная сложность алгоритма одновременного умножения на основе методов Лим-Лии с параметрами ***h*** и ***v*** и «оконного» умножения шириной окна предвычислений ***w*** для скалярных множителей ***k*** и ***l*** , битовой длины ***t***, составит:

  $$((\mathrm{v}+1)/2^h+2^w\text{-}2)S$$

Вычислительные сложности предложенного и базового алгоритмов при соизмеримых размерах предвычислений



Преобразования на эллиптических кривых

МЕТОДЫ АРИФМЕТИЧЕСКИХ ПРЕОБРАЗОВАНИЙ В ГРУППЕ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

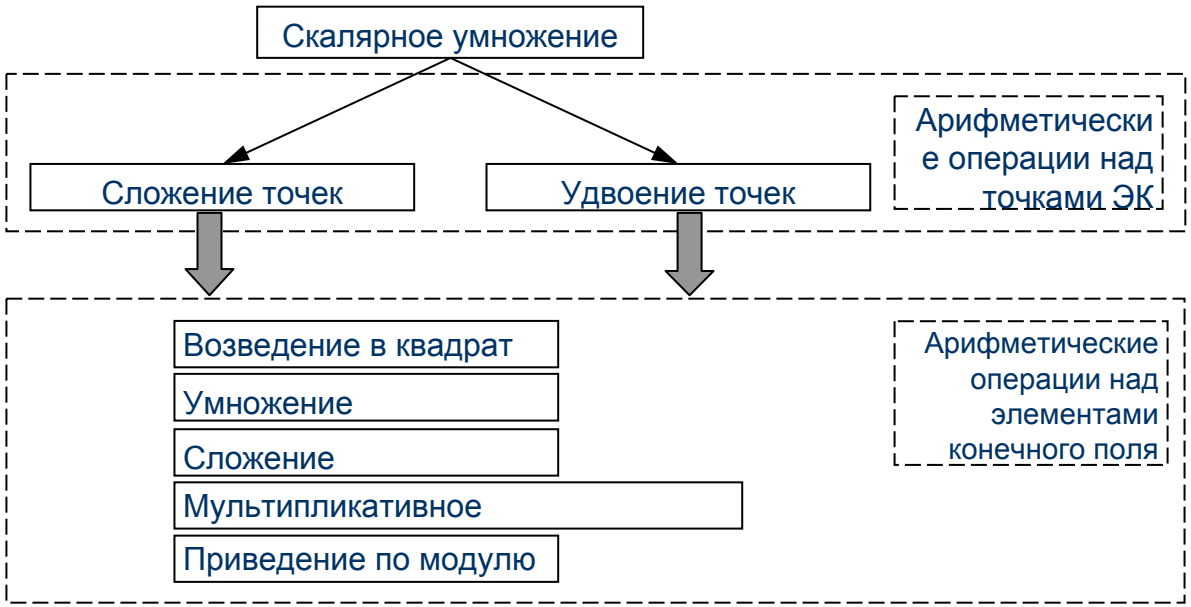


Рис. Иерархия операций используемых для СУ точек ЭК

Пути уменьшения вычислительной сложности преобразований в группе точек эллиптической кривой

Пути уменьшения вычислительной сложности СУ точек ЭК:

- уменьшение количества (избежание) наиболее вычислительно емких операций в поле;
- замена наиболее вычислительно емких операций менее емкими операциями в поле;
- использование предвычислений;
- уменьшение веса по Хеммингу коэффициентов ЭК;
- сжатие координат.

На сегодняшний день известны следующие координатные представления точек ЭК над полем четной характеристики:

- аффинные координаты (x, y);
- стандартные проективные координаты (X:Y:Z)->(X/Z, Y/Z);
- проективные координаты Якоби (X:Y:Z)->(X/Z^2, Y/Z^3);
- проективные координаты Чудновского (X:Y:Z:Z^2:Z^3)->(X/Z^2, Y/Z^3);
- модифицированные проективные координаты Якоби (X:Y:Z:Z^2)->(X/Z^2, Y/Z^3);
- проективные координаты Лопеса-Дахаба (X:Y:Z)->(X/Z, Y/Z^2);
- модиф. проективные координаты Лопеса-Дахаба (X:Y:Z:Z^2)->(X/Z, Y/Z^2).

МЕТОД АРИФМЕТИЧЕСКИХ ПРЕОБРАЗОВАНИЙ В ГРУППЕ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ В ПРОЕКТИВНЫХ КООРДИНАТАХ ЛОПЕСА-ДАХАБА

Базовый

$P_3(X_3:Y_3:Z_3)=P_1(X_1:Y_1:Z_1)+P_2(X_2:Y_2:Z_2)$

Сложение P_1 и P_2 не принадлежат одному классу смежности

$X_3=A^2+J(D+\mathbf{a}C^2)+AD$

$Z_3=D^2$

$Y_3=Z_3(X_3+JE)+AB(FZ_3+X_3J)$

$E=Y_2Z_1^2$, $A=Y_1Z_2^2+E$, $F=X_1Z_2$, $B=F+X_2Z_1$, $C=Z_1Z_2$, $D=BC$, $J=B^2$

Удвоение P_1 и P_2 принадлежат одному классу смежности

$X_3=B^2+A$

$Z_3=BC$

$Y_3=AZ_3+X_3(\mathbf{a}Z_3+Y_1^2+A)$

$A=\mathbf{b}C^2$, $B=X_1^2$, $C=Z_1^2$

Предложенный

$P_3(X_3:Y_3:Z_3)=P_1(X_1:Y_1:Z_1)+P_2(X_2:Y_2:Z_2)$

Сложение P_1 и P_2 не принадлежат одному классу смежности

$X_3=D(G+J)+E(F+H)$

$Z_3=KC$

$Y_3=AB(KD+X_3)+(FK^2+X_3Z_3)$

$D=X_1Z_2$, $E=X_2Z_1$, $F=X_1Z_2^2$, $G=Y_2Z_1^2$, $A=D+E$, $B=F+G$, $C=Z_1Z_2$, $H=D^2$, $J=E^2$, $K=H+J$

Удвоение P_1 и P_2 принадлежат одному классу смежности

$X_3=B^2+A$

$Z_3=BC$

$Y_3=AZ_3+X_3(\mathbf{a}Z_3+Y_1^2+A)$

$A=\mathbf{b}C^2$, $B=X_1^2$, $C=Z_1^2$

Оценки вычислительной сложности известных и усовершенствованных методов арифметических преобразований в группе точек ЭК

Система координат	Вычислительная сложность														
	Сложение					Смешанное сложение					Удвоение				
	$()^{-1}$	^2	*	+	Σ*	$()^{-1}$	^2	*	+	Σ*	$()^{-1}$	^2	*	+	Σ*
Аффинная, (x, y)	1	1	2	9	12,6	-	-	-	-		1	1	2	7	12,6
Стандартная проективная, $(X/Y, Y/Z)$	-	3	14	8	14,3	-	2	12	8	12,2	-	2	8	3	8,22
Проективная Якоби, $(X/Z^2, Y/Z^3)$	-	5	15	8	15,5	-	3	11	8	11,3	-	5	5	4	5,55
Модифицированная проективная Якоби, $(X/Z^2, Y/Z^3)$	-	3	15	8	15,3	-	3	11	8	11,3	-	5	5	4	5,55
Проективная Чудновского, $(X/Z^2, Y/Z^3)$	-	3	15	8	15,3	-	2	11	8	11,2	-	5	6	4	6,55
Проективная Лопес-Дахаб, $(X/Z, Y/Z^2)$	-	6	15	8	15,7	-	4	10	8	10,4	-	5	5	4	5,55
Проективная Лопес-Дахаб, $(X/Z, Y/Z^2)$	-	5	13	9	13,5	-	4	10	9	10,4	-	5	5	4	5,55
Модиф. проективная Лопес-Дахаб, $(X/Z, Y/Z^2)$	-	5	15	8	15,5	-	4	10	8	10,4	-	5	5	4	5,55
Модиф. проективная Лопес-Дахаб, $(X/Z, Y/Z^2)$	-	3	14	9	13,3	-	4	10	9	10,4	-	4	5	4	5,44

$()^{-1}$ – операция инвертирования в поле, ^2 – операция возведения в квадрат в поле, * - операция умножения в поле, + - операция сложения в поле, Σ* - общая вычислительная сложность в операциях умножения в поле.

Условия: $I_{inv} \approx 10{,}5 I_{mul}$, $I_{sqr} \approx 0{,}11 I_{mul}$

Оценка эффективности усовершенствованного метода

Наименование алгоритма	Вычислительная сложность		
	Лопеса-Дахаба, I_{mul}	Предложенный, I_{mul}	Выигрыш, %
Алгоритм 2.1. Двоичное умножение слева направо	2184,2	2004,9	8,2
Алгоритм 2.3. Двоичное NAF умножение	1757,683	1638,15	6,8
Алгоритм 2.4. Двоичное умножение Монтгомери	3463,75	3105,15	10,35
Алгоритм 2.5. «Оконное» умножение	803,89	691,24	14,01
Алгоритм 2.7. «Оконное» NAF умножение	1469,12	1390,8	5,33
Алгоритм 2.8. Умножение Лим-Лии фиксированного элемента, $h = 6$, $v = 4$	457,54	398,71	12,86
Алгоритм 2.9. Комбинированное умножение фиксированного элемента	825,95	741,9	10,18
Алгоритм 2.10. Одновременное умножение	2293,61	2098,98	8,49
Алгоритм 2.11. Одновременное умножение Шамира, без предвычислений (двоичное представление).	2839,675	2568,525	9,55
Алгоритм 2.11. Одновременное умножение Шамира, без предвычислений (NAF)	2357,775	2154,15	8,63
Алгоритм 2.11. Одновременное умножение Шамира, без предвычислений (JSF)	2215,6	2031,9	8,29
Алгоритм 2.12. Одновременное умножение на основе комбинированного умножения фиксированного элемента и «оконного» умножения	1177,65	1025,85	12,89
Алгоритм 2.13. Одновременное умножение на основе умножения Лим-Лии и «оконного» умножения, $h = 8$, $v = 4$, $w = 4$	1150,8	993,5	13,67

Условия: $I_{inv} \approx 10{,}5 I_{mul}$, $I_{sqr} \approx 0{,}11 I_{mul}$. Эллиптическая кривая вида $E(GF(2^{163}))$.

Экспериментальные оценки времени выполнения известных и усовершенствованных методов арифметических преобразований в группе точек ЭК

Метод преобразований	Время, мкс						Время, мкс	
	Сложение		Смешанное сложение		Удвоение		Скалярное умножение	
	ws1	Ws2	ws1	ws2	ws1	ws2	ws1	ws2
Параметры кривой: $a \notin \{0, 1\}$								
В аффинных	51,77	117,3			52,63	120,4	17,58	40,25
Лопеса-Дахаба – прототип	21,72	26,11	14,48	17,45	6,17	7,36	3,716	4,314
Лопеса-Дахаба – предложенный	18,8	22,8	14,48	17,75	6,17	7,36	3,418	3,973
Параметры кривой: $a \in \{0, 1\}$								
В аффинных	51,77	117,3			52,63	120,4	17,58	40,25
Лопеса-Дахаба – прототип	20,27	25,48	13,11	15,72	6,18	7,36	3,571	4,162
Лопеса-Дахаба – предложенный	18,78	22,78	14,48	17,75	6,18	7,36	3,419	3,973

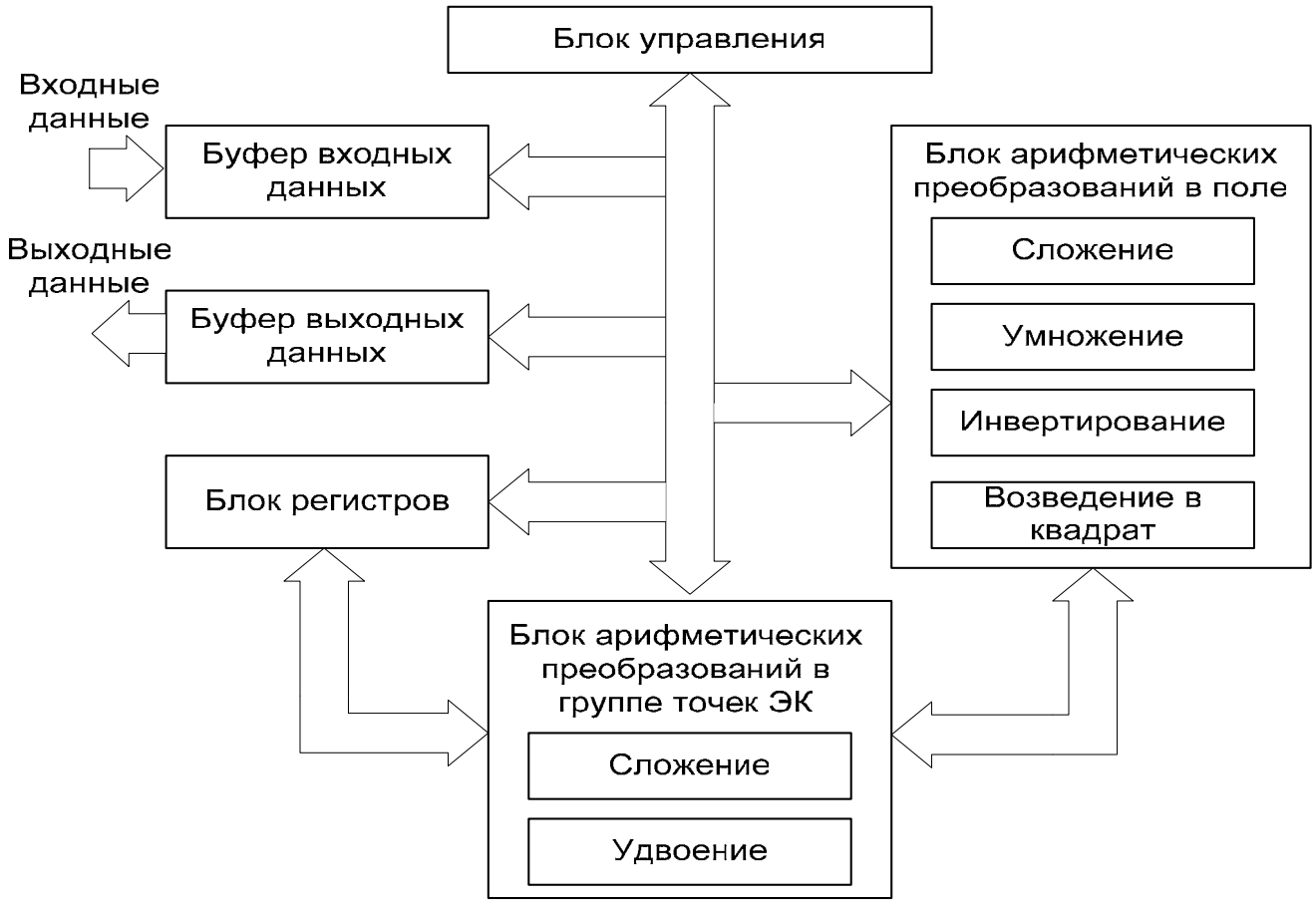
Условия: рабочая станция (ws1) с процессором AMD AthlonXP 2500+ GHz (Barton), под операционной системой Windows 2000 Pro, (ws2) с процессором Intel Celeron 2,4GHz, под операционной системой Windows XP Pro программа скомпилирована с помощью Visual C++ 6.0.

Количественная оценка вычислительной сложности - метода ρ-Полларда решения ЗДЛЭК над полем GF(2^{233})

Условия	Вычислительная сложность, I_{mul}	Время (ws1), года
$I^P_{add}=15,7I_{mul}$, базовый	$2*15,7*2^{116}*\sqrt{(\pi/2)}$	$1,466*10^{23}$
$I^P_{add}=15,7I_{mul}$, предложенный	$2*13,5*2^{116}*\sqrt{(\pi/2)}$	$1,26*10^{23}$
Выигрыш	$2*2,2*2^{116}*\sqrt{(\pi/2)}$	$2,054*10^{22}$

Условия: рабочая станция (ws1) с процессором AMD AthlonXP 2500+ GHz (Barton), под операционной системой Windows 2000 Pro, программа скомпилирована с помощью Visual C++ 6.0.

Аппаратная реализация сопроцессора преобразований в группе точек ЭК



Преобразования на гиперэллиптических кривых второго рода

МЕТОДЫ АРИФМЕТИЧЕСКИХ ПРЕОБРАЗОВАНИЙ В ЯКОБИАНЕ ГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВОЙ

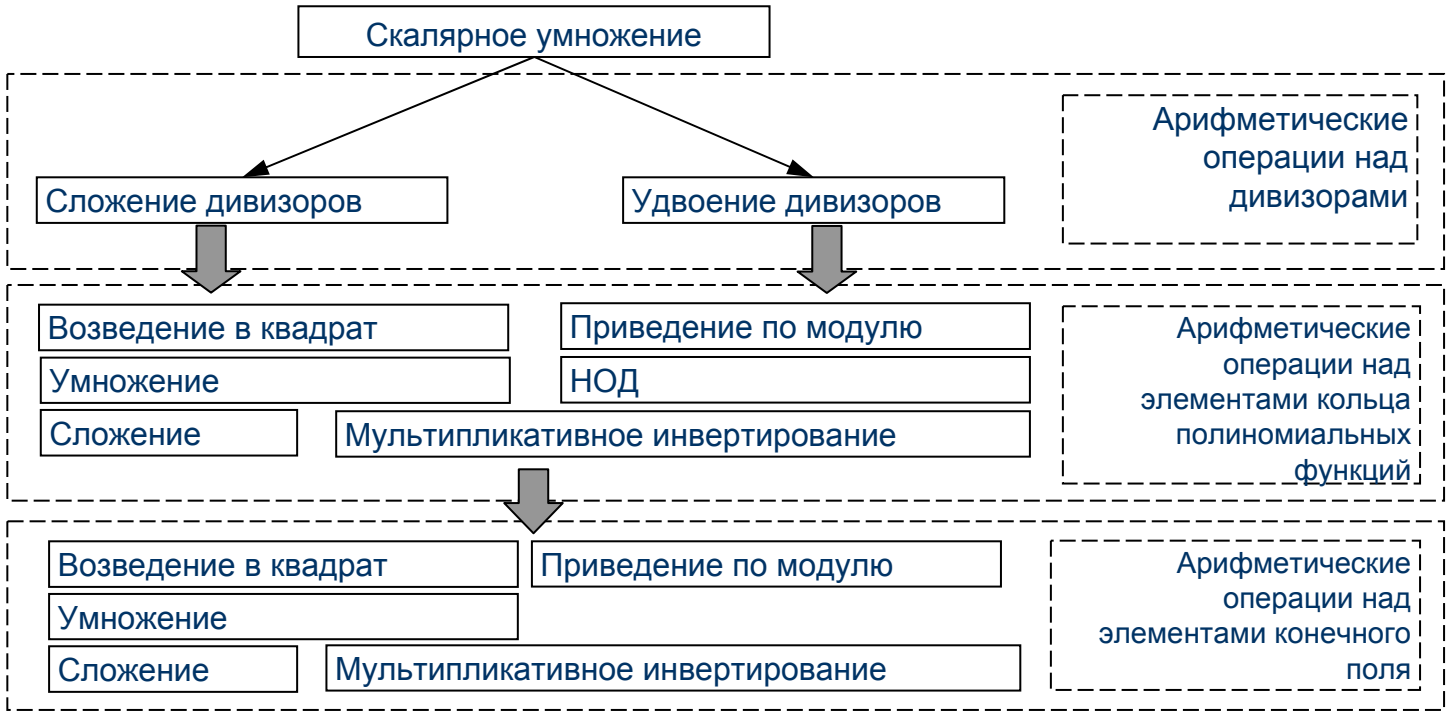


Рис. Иерархия методов используемых для СУ дивизоров ГЭК

Пути уменьшения вычислительной сложности преобразований в якобиане дивизоров гиперэллиптической кривой

Пути уменьшения вычислительной сложности СУ дивизоров якобиана ГЭК:

- уменьшения количества операций над дивизорами;
- уменьшения сложности операций над дивизорами;
- перехода от выполнения операций над дивизорами, непосредственно к выполнению операций над полиномиальными функциями.

На сегодняшний день известны следующие координатные представления дивизоров якобиана ГЭК второго рода:

- аффинные координаты, методы преобразований Ланге и Воллингера;
- проективные координаты, char(GF(q))≠2, метод преобразований Ланге;
- взвешенные координаты char(GF(q))≠2, метод преобразований Ланге;
- проективные координаты char(GF(q))=2, метод преобразований Воллингера;
- взвешенные координаты char(GF(q))=2, метод преобразований Ланге.

Методы уменьшения вычислительной сложности преобразований в якобиане гиперэллиптической кривой второго рода

- Непосредственное вычисление результатов арифметических операций над полиномиальными функциями.
- Использование кривых особого вида.
- Выполнение одновременного инвертирования элементов поля методом Монтгомери.
- Выполнение нормализации полиномиальных функций.
- Изменение последовательности вычислений.
- Выполнение умножения и приведения полиномиальных функций посредством метода Карацубы.
- Эффективного вычисления частного при делении двух полиномиальных функций.
- Эффективного вычисления результанты двух полиномиальных функций.
- Использование проективных координат.
- Использование смешанных координат.
- Использование предвычислений.
- Совершенствование методов арифметических операций над дивизорами якобиана ГЭК.

ОЦЕНКИ ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ ИЗВЕСТНЫХ И УСОВЕРШЕНСТВОВАННЫХ МЕТОДОВ АРИФМЕТИЧЕСКИХ ПРЕОБРАЗОВАНИЙ В ЯКОБИАНЕ ГЭК ВТОРОГО РОДА, CHAR(GF(q))≠2

Условия, $I_{inv}=33I_{mul}$, $I_{sqr}=0{,}8I_{mul}$	Сложение				Смешанное сложение				Удвоение				Смешанное удвоение			
	$()^{-1}$	^2	*	Σ*	$()^{-1}$	^2	*	Σ*	$()^{-1}$	^2	*	Σ*	$()^{-1}$	^2	*	Σ*
Аффинные координаты div(u_1, u_0, v_1, v_0), метод Ланге																
$f_4=0$	1	3	22	57,4					1	5	22	59				
Проективные координаты div(U_1, U_0, V_1, V_0, Z), метод Ланге																
deg(h)=2, $h_i \in$ GF(2)		4	47	50,2		3	40	42,4		6	40	44,8		5	25	29
Проективные координаты div(U_1, U_0, V_1, V_0, Z), предложенный метод																
deg(h)=2, $h_i \in$ GF(2)		4	46	49,2		4	39	42,2		6	39	43,8		5	25	29
$h(x)=0$, $f_4=0$		4	46	49,2		4	39	42,2		6	33	37,8		5	24	28
Взвешенные координаты div(U_1, U_0, V_1, V_0, Z_1, Z_2, Z_1^2, Z_2^2), метод Ланге																
$h(x)=0$, $f_4=0$		7	47	52,6		5	36	40		7	34	39,6		5	21	25

ОЦЕНКИ ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ ИЗВЕСТНЫХ И УСОВЕРШЕНСТВОВАННЫХ МЕТОДОВ АРИФМЕТИЧЕСКИХ ПРЕОБРАЗОВАНИЙ В ЯКОБИАНЕ ГЭК ВТОРОГО РОДА, CHAR(GF(q))=2

Условия, $I_{inv}=8I_{mul}$, $I_{sqr}=0{,}2I_{mul}$	Сложение				Смешанное сложение				Удвоение				Смешанное удвоение			
	$()^{-1}$	^2	*	Σ*	$()^{-1}$	^2	*	Σ*	$()^{-1}$	^2	*	Σ*	$()^{-1}$	^2	*	Σ*
Аффинные координаты div(u_1, u_0, v_1, v_0), метод Ланге																
$f_4=0$	1	3	21	29,6					1	5	20	29				
$h_2=0$, $f_4=0$	1	3	21	29,6					1	5	17	26				
Проективные координаты div(U_1, U_0, V_1, V_0, Z), метод Воллингера																
$h(x)=x$, $f_4=0$, $f_3=f_2=0$		5	45	46		5	38	39		6	31	32,2		5	18	19
Проективные координаты div(U_1, U_0, V_1, V_0, Z), предложенный метод																
$h(x)=x$, $f_4=0$, $f_3=f_2=0$		4	44	44,8		4	37	37,8		6	30	31,2		4	17	17,8
Взвешенные координаты div(U_1, U_0, V_1, V_0, Z_1, Z_2, Z_1^2, Z_2^2, Z_1Z_2, $Z_1^3Z_2$), метод Ланге																
deg(h)=2, $f_4=0$		4	46	46,8		5	35	36		6	35	36,2		5	20	21
$h(x)=x$, $f_4=0$		6	44	45,2		6	34	35,2		6	29	30,2		6	19	20,2

ОЦЕНКА ЭФФЕКТИВНОСТИ УСОВЕРШЕНСТВОВАННЫХ МЕТОДОВ, CHAR(GF(*q*))≠2

Наименование алгоритма	Вычислительная сложность, I_{mul}			
	Проективные, Воллингер	Взвешенные, Ланге	Проективные, предложенный	Проективные, предложенный
	$\deg(h)=2,\ h_i \in \mathbf{F}_2$	$h(x)=0,\ f_4=0$	$\deg(h)=2,\ h_i \in \mathbf{F}_2$	$h(x)=0,\ f_4=0$
Алгоритм 2.1. Двоичное умножение слева направо	5801,7	5469,7	5677,2	5179,2
Алгоритм 2.3. Двоичное NAF умножение	5107,27	4742,07	4996,6	4498,6
Алгоритм 2.4. Двоичное умножение Монтгомери	7885	7652,6	7719	7221
Алгоритм 2.5. «Оконное» умножение	1640,9	1719,36	1608,23	1608,23
Алгоритм 2.7. «Оконное» NAF умножение	4747,12	4357,36	4643,52	4139,52
Алгоритм 2.8. Умножение Лим-Лии фиксированного элемента, $h=8,\ v=4$	634,24	642,54	621,29	603,29
Алгоритм 2.9. Комбинированное умножение фиксированного элемента, $w=10$	759,61	737,18	743,62	741,44
Алгоритм 2.10. Одновременное умножение	6300,56	5992,4	6166,13	5645,06
Алгоритм 2.11. Одновременное умножение Шамира, без предвычислений (двоичное представление).	6893,55	6613,75	6747,3	6249,3
Алгоритм 2.11. Одновременное умножение Шамира, без предвычислений (NAF)	6133,58	5817,44	6002,47	5504,47
Алгоритм 2.11. Одновременное умножение Шамира, без предвычислений (JSF)	5902,1	5574,9	5775,6	5277,6
Алгоритм 2.12. Одновременное умножение на основе комбинированного умножения фиксированного элемента и «оконного» умножения, $h=10,\ w=4$	2400,52	2456,55	2342,62	2303,84
Алгоритм 2.13. Одновременное умножение на основе умножения Лим-Лии и «оконного» умножения, $h=8,\ v=4,\ w=4$	2325,36	2414,5	2278,71	2260,71

Условия: $I_{inv} \approx 33 I_{mul}$, $I_{sqr} \approx 0{,}8 I_{mul}$. Гиперэллиптическая кривая вида $C_2(GF(p_{83}))$.

ОЦЕНКА ЭФФЕКТИВНОСТИ УСОВЕРШЕНСТВОВАННЫХ МЕТОДОВ, CHAR(GF(*q*))=2

Наименование алгоритма	Вычислительная сложность, I_{mul}			
	Проективные, Воллингер	Взвешенные, Ланге	Взвешенные, Ланге	Проективные, предложенный
	$h(x)=x,\ f_4=0,\ f_3=0,\ f_2=0$	$\deg(h)=2,\ f_4=0$	$h(x)=x,\ f_4=0$	$h(x)=x,\ f_4=0,\ f_3=0,\ f_2=0$
Алгоритм 2.1. Двоичное умножение слева направо	4581,6	4946,8	4382,4	4365,8
Алгоритм 2.3. Двоичное NAF умножение	3945,27	4299,4	3757,13	3746,07
Алгоритм 2.4. Двоичное умножение Монтгомери	6490,6	6889	6258,2	6225
Алгоритм 2.5. «Оконное» умножение	1503,63	1529,78	1477,48	1464,4
Алгоритм 2.7. «Оконное» NAF умножение	3606,4	3958,08	3422,72	3414,88
Алгоритм 2.8. Умножение Лим-Лии фиксированного элемента, $h=8,\ v=4$	554,62	574,59	540,66	536,68
Алгоритм 2.9. Комбинированное умножение фиксированного элемента, $w=10$	625,24	663,63	602,85	599,65
Алгоритм 2.10. Одновременное умножение	5038,73	5411,88	4831,58	4811
Алгоритм 2.11. Одновременное умножение Шамира, без предвычислений (двоичное представление).	5582,1	5964,7	5365,5	5340,2
Алгоритм 2.11. Одновременное умножение Шамира, без предвычислений (NAF)	4885,71	5256,2	4681,22	4661,98
Алгоритм 2.11. Одновременное умножение Шамира, без предвычислений (JSF)	4673,6	5040,4	4472,8	4455,4
Алгоритм 2.12. Одновременное умножение на основе комбинированного умножения фиксированного элемента и «оконного» умножения, $h=10,\ w=4$	2128,87	2193,41	2080,32	2064,05
Алгоритм 2.13. Одновременное умножение на основе умножения Лим-Лии и «оконного» умножения, $h=8,\ v=4,\ w=4$	2104,25	2151,16	2063,33	2045,87

Условия: $I_{inv}\approx 8I_{mul}$, $I_{sqr}\approx 0{,}8I_{mul}$. Гиперэллиптическая кривая вида $C_2(GF(2^{83}))$.

Экспериментальные оценки времени выполнения известных и усовершенствованных методов арифметических преобразований в якобиане ГЭК рода 2

Наименование метода преобразований	Время, мкс						Время, мкс	
	Общее сложение		Смешанное сложение		Удвоение		Скалярное умножение	
	ws1	ws2	ws1	ws2	ws1	ws2	ws1	ws2
Воллингер – базовый	63,46	76,69	53,8	65,02	44,05	53,22	18,62	22,41
Предложенный	62,14	75,16	52,43	63,41	41,41	49,63	17,76	21,33

Условия: рабочая станция (ws1) с процессором AMD AthlonXP 2500+ GHz (Barton), под операционной системой Windows 2000 Pro, (ws2) с процессором Intel Celeron 2,4GHz, под операционной системой Windows XP Pro программа скомпилирована с помощью Visual C++ 6.0.

Количественная оценка вычислительной сложности - метода *Theriault* решения ЗДЛГЭК над полем GF(2^{233})

Условия	Вычислительная сложность, I_{mul}	Время (ws1), года
$I^D_{add} \approx 39 I_{mul}$, базовый	$2*39*2^{284,6}$	$3,59*10^{73}$
$I^D_{add} \approx 37,8 I_{mul}$, предложенный	$2*37,8*2^{284,6}$	$3,48*10^{73}$
Выигрыш	$2*1,2*2^{284,6}$	$0,1*10^{73}$

Условия: рабочая станция (ws1) с процессором AMD AthlonXP 2500+ GHz (Barton), под операционной системой Windows 2000 Pro, программа скомпилирована с помощью Visual C++ 6.0.

Особенности аппаратной реализации преобразований в якобиане ГЭК

Результаты исследований

- **Научная новизна** работы заключается в решении актуальной научно-технической задачи повышения производительности программно – технического комплекса криптографической защиты информации центров сертификатов ключей на основе применения методов арифметических преобразований с пониженной вычислительной сложностью на алгебраических кривых

Результаты исследований

Научная новизна полученных результатов.

1. Усовершенствован алгоритм одновременного скалярного умножения элементов аддитивной группы точек либо дивизоров для быстрых криптографических преобразованиях на алгебраических кривых, который отличается от известных введением процедуры предвычислений произведений элементов группы и компоновки результатов предвычислений, что позволяет снизить вычислительную сложностью.
2. Усовершенствован метод арифметических преобразований точек эллиптической кривой в проективных координатах Лопеса-Дахаба для быстрого скалярного умножения в криптографических преобразованиях в группе точек эллиптической кривой над полем $GF(2^m)$, отличающийся от известного метода учетом уравнения эллиптической кривой в слагаемых точках, что на этапе вычисления результирующей точки позволяет избавиться от зависимости параметров кривой и уменьшить вычислительную сложность.
3. Усовершенствованы методы арифметических преобразований в якобиане гиперэллиптической кривой второго рода в проективных координатах для быстрого скалярного умножения в якобиане гиперэллиптической кривой второго рода, отличающийся от известных методов, уравнением кривой особого вида и учетом ранее неизвестных зависимостей между координатами - полиномиальными функциями результирующего дивизора, что позволяет снизить вычислительную сложностью.

Таким образом, получила дальнейшее развитие теория арифметических преобразований на эллиптических и гиперэллиптических кривых.

Результаты исследований

Практическое значение полученных результатов заключается:

1. В разработке усовершенствованного алгоритма одновременного скалярного умножения элементов аддитивной группы точек либо дивизоров при проверке цифровой подписи, который позволил снизить вычислительную сложность на 5,3%. Алгоритм реализован в программном обеспечении системы криптографической защиты информации комплекса средств автоматизации «Ореанда-2000», «Ореанда-Інфо» на основе преобразований на алгебраических кривых. (Акт от 28.12.2003 №429).
2. В разработке алгоритма сложения точек эллиптической кривой над полем построенного на основании усовершенствованного метода арифметических преобразований в проективных координатах Лопеса-Дахаба, который позволяет уменьшить вычислительную сложность алгоритма скалярного умножения при формировании цифровой подписи на 13%, при проверке на 14%. Реализовано в программном обеспечении криптографической защиты информации терминала пользователя электронной почты в работах «Egyptsat-1» и «Хвыля». (Акт от 4.03.2005 №85а/8).
3. В создании библиотеки алгоритмов преобразований в якобиане гиперэллиптической кривой второго рода. Применение алгоритмов сложения и удвоения дивизоров якобиана гиперэллиптической кривой второго рода над конечными полями, построенных на основании усовершенствованных методов арифметических преобразований в якобиане в проективных координатах позволяет уменьшить вычислительную сложность алгоритма скалярного умножения при формировании цифровой подписи на 5%, при проверке на 7%. (Акт от 09.03.2005 №94а/8).
4. Результаты диссертационной работы используются в учебном процессе на кафедре компьютерных систем Харьковского университета Воздушных Сил. (Акт от 29.03.2005 №133/8).

Результаты исследований

Апробация результатов диссертации. Основные результаты диссертации докладывались и были одобрены на следующих научно-технических конференциях:

- на 7-ом и 8-ом Международном форуме «Радиоэлектроника и молодежь в XXI веке» (Харьков, 2003, 2004 гг.);
- на 7-ой Международной научно-практической конференции «Безопасность информации» (Киев, 2004 г.);
- на 10-ой Международной научной конференции «Теория и техника передачи, приема и обработки информации» (Харьков-Туапсе, 2004 г.);
- на 4-ой научной конференции молодых ученых Харьковского военного университета (Харьков, 2004 г.).
- на 1-ой научной конференции молодых ученых Харьковского университета Воздушных Сил (Харьков, 2005 г.).

Публикации. Основные положения и результаты диссертационной работы изложены в 16 научных трудах, включающих 10 научных статей, 6 тезисов выступлений, 3 отчетах по НИР. Получено 4 акта о реализации.

МЕТОД АРИФМЕТИЧЕСКИХ ПРЕОБРАЗОВАНИЙ В ЯКОБИАНЕ ГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВОЙ ВТОРОГО РОДА, char(GF(q))≠2

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

1. Предвычисления:
$Z = Z_1 \cdot Z_2$, $\widetilde{U}_{21} = Z_1 \cdot U_{21}$, $\widetilde{U}_{20} = Z_1 \cdot U_{20}$, $\widetilde{V}_{21} = Z_1 \cdot V_{21}$, $\widetilde{V}_{20} = Z_1 \cdot V_{20}$,
$y_0 = U_{11} \cdot y_1$.
2. Вычисление результанты r для u_1 и u_2:
$y_1 = U_{11} \cdot Z_2 - \widetilde{U}_{21}$, $y_2 = \widetilde{U}_{20} - U_{10} \cdot Z_2$, $y_3 = y_0 + y_2 \cdot Z_1$, $r = y_2 \cdot y_3 + y_1^2 \cdot U_{10}$
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 $s = (v_1 - v_2) inv \bmod u_1$, $s = s_1 x + s_0$:
$w_0 = V_{10} \cdot Z_2 - \widetilde{V}_{20}$, $w_1 = V_{11} \cdot Z_2 - \widetilde{V}_{21}$, $w_2 = inv_0 \cdot w_0$, $w_3 = inv_1 \cdot w_1$,
$s_1 = (inv_0 + Z_1 \cdot inv_1) \cdot (w_0 + w_1) - w_2 - w_3 \cdot (Z_1 + U_{11})$, $s_0 = w_2 - U_{10} \cdot w_3$
If $s_1 = 0$ then consider special case
5. Предвычисления:
$R = r \cdot Z$, $s_2 = s_0 \cdot Z$, $s_3 = s_1 \cdot Z$, $\widetilde{R} = R \cdot s_3$, $w_0 = s_1 \cdot s_0$, $w_1 = s_1 \cdot s_3$,
$w_2 = s_0 \cdot s_3$, $w_3 = w_1 \cdot \widetilde{U}_{21}$, $w_4 = R \cdot s_1$
6. Вычисление $l = su_2$, $l = x^3 + l_2 x^2 + l_1 x + l_0$:
$l_0 = w_0 \cdot \widetilde{U}_{20}$, $l_2 = w_3 + w_2$, $l_1 = (w_1 + w_0) \cdot (\widetilde{U}_{21} + \widetilde{U}_{20}) - l_0 - w_3$
7. Вычисление $u' = (s(l + h + 2v_1) - k) u_1^{-1}$, $k = (f - v_1 h - v_1^2)/u_1$,
$u' = x^2 + u_1' x + u_0'$:
$\widetilde{U}_0' = s_2^2 + s_1^2 \cdot y_1 U_{11} + y_2 \cdot w_1 + \widetilde{R} + R \cdot r \cdot y_1$, $\widetilde{U}_1' = w_1 \cdot y_1 - R^2$
8. Корректировка:
$U_0' = \widetilde{U}_0' \cdot \widetilde{R}$, $U_1' = \widetilde{U}_1' \cdot \widetilde{R}$, $Z' = s_3^2 \cdot \widetilde{R}$
9. Вычисление $v' \equiv -(h + s_1 l + v_2) \bmod u'$, $v' = v_1' x + v_0'$:
$V_1' = \widetilde{U}_1' \cdot (l_2 - \widetilde{U}_1') + s_3^2 \cdot (\widetilde{U}_0' - w_4 \cdot \widetilde{V}_{21} - l_1)$, $V_0' = \widetilde{U}_0' \cdot (l_2 - \widetilde{U}_1') - s_3^2 \cdot (l_0 + w_4 \cdot \widetilde{V}_{20})$

Алгоритм. Сложение дивизоров методом Ланге

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:
$\mathrm{div}(U_1', U_0', V_1', V_2', Z') = \mathrm{div}(U_{11}, U_{10}, V_{11}, V_{10}, Z_1) + \mathrm{div}(U_{21}, U_{20}, V_{21}, V_{20}, Z_2)$

1. Предвычисления:
$Z = Z_1 \cdot Z_2$, $\widetilde{U}_{21} = Z_1 \cdot U_{21}$, $\widetilde{U}_{20} = Z_1 \cdot U_{20}$, $\widetilde{V}_{21} = Z_1 \cdot V_{21}$, $\widetilde{V}_{20} = Z_1 \cdot V_{20}$.
2. Вычисление результанты r для u_1 и u_2:
$z_1 = U_{11} \cdot Z_2 - \widetilde{U}_{21}$, $z_2 = \widetilde{U}_{20} - U_{10} \cdot Z_2$, $z_3 = U_{11} \cdot z_1 + z_2 \cdot Z_1$,
$r = z_2 \cdot z_3 + z_1^2 \cdot U_{10}$.
3. Вычисление квази-инверсии $inv = r/u_2 \bmod u_1$, $inv = inv_1 x + inv_0$:
$inv_1 = z_1$, $inv_0 = z_3$.
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 consider special case.
5. Предвычисления:
$R = r \cdot Z$, $s_0 = s_0 \cdot Z$, $s_3 = s_1 \cdot Z$, $\widetilde{R} = R \cdot s_3$, $t = s_1 \cdot (z_1 + \widetilde{U}_{21})$, $S_3 = s_3^2$,
$S = s_0 s_1$, $\widetilde{S} = s_1 \cdot s_3$, $\widetilde{\widetilde{S}} = s_0 \cdot s_3$, $\widetilde{\widetilde{R}} = \widetilde{R} \cdot \widetilde{S}$.
6. Вычисление $l = su_2$, $l = x^3 + l_2 x^2 + l_1 x + l_0$:
$l_0 = S \cdot \widetilde{U}_{20}$, $l_2 = \widetilde{S} \cdot \widetilde{U}_{21}$, $l_1 = (\widetilde{S} + S) \cdot (\widetilde{U}_{21} + \widetilde{U}_{20}) - l_0 - l_2$, $l_2 = l_2 + \widetilde{\widetilde{S}}$.
7. Вычисление $u' = (s(l + h + 2v_1) - k) u_1^{-1}$, $k = (f - v_1 h - v_1^2)/u_1$,
$u' = x^2 + u_1' x + u_0'$: $\widetilde{U}_1' = 2\widetilde{\widetilde{S}} - \widetilde{S} \cdot z + h_2 \widetilde{R} - R^2$,
$\widetilde{U}_0' = s_2^2 + s_1 \cdot z_1 \cdot (t - 2s_0) + z_2 \cdot \widetilde{s} + R \cdot (h_2 (s_0 - t) + s_1 \cdot (h_1 Z + 2\widetilde{V}_{21}) + r \cdot (z_1 + 2\widetilde{U}_{21} - f$
8. Предвычисления: $l_2 = l_2 - U_1'$, $w_0 = U_0' l_2 - S_3 l_0$, $w_1 = U_1' l_2 + S_3 (U_0' - l_1)$.
9. Корректировка: $U_0' = \widetilde{U}_0' \cdot \widetilde{R}$, $U_1' = \widetilde{U}_1' \cdot \widetilde{R}$, $Z' = S_3 \cdot \widetilde{R}$.
10. Вычисление $v' \equiv -(h + s_1 l + v_2) \bmod u'$, $v' = v_1' x + v_0'$:
$V_1' = w_1 + h_2 U_1' - \widetilde{\widetilde{R}} \widetilde{V}_{21} - h_1 Z'$, $V_0' = w_0 + h_2 U_0' - \widetilde{\widetilde{R}} \widetilde{V}_{20} - h_0 Z'$.

МЕТОДЫ АРИФМЕТИЧЕСКИХ ПРЕОБРАЗОВАНИЙ В ЯКОБИАНЕ ГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВОЙ ВТОРОГО РОДА , char(GF(*q*))≠2

Алгоритм. Усовершенствованное удвоение дивизоров

Вход: $\mathrm{div}(U_1, U_0, V_1, V_0, Z)$

Выход: $\mathrm{div}(U_1', U_0', V_1', V_2', Z') = 2\,\mathrm{div}(U_1, U_0, V_1, V_0, Z)$

1. Предвычисления: $Z_2 = Z^2$, $\widetilde{V}_1 = h_1 Z + 2V_1 - h_2 U_1$, $\widetilde{V}_0 = h_0 Z + 2V_0 - h_2 U_2$.
2. Вычисление результанты r для u и $h + 2v$ (причем $\widetilde{v} \equiv (h + 2v) \bmod u$):
$w_0 = V_1^2$, $w_1 = U_1^2$, $w_2 = \widetilde{V}_1^2 = h_1^2 Z_2 + 4w_0 - h_2^2 w_1$, $w_3 = \widetilde{V}_0 \cdot Z - U_1 \cdot \widetilde{V}_1$,
$r = \widetilde{V}_0 \cdot w_3 + w_2 \cdot U_0$.
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 $k \equiv \left[\left(f - hv - v^2\right)/u\right] \bmod u$, $k = k_1 x + k_0$:
$w_3 = f_3 \cdot Z_2 + w_1$, $w_4 = 2U_0$, $k_1 = 2w_1 + w_3 - Z \cdot (w_4 + 2f_4 U_1 + h_2 V_1)$,
$k_0 = U_1 \cdot (Z \cdot (2w_4 + f_4 U_1 + h_2 V_1) - w_3) + Z \cdot (Z \cdot (f_2 \cdot Z - h_1 V_1 - h_2 V_0 - 2f_4 U_0) - w_0)$
5. Вычисление $s = k \cdot inv \bmod u$, $s = s_1 x + s_0$:
$w_0 = k_0 \cdot inv_0$, $w_1 = k_1 \cdot inv_1$, $s_3 = (inv_0 + inv_1) \cdot (k_0 + k_1) - w_0 - w_1 \cdot (1 + U_1)$,
$s_0 = w_0 - Z \cdot U_0 \cdot w_1$, $s_1 = s_3 \cdot Z$.
If $s_1 = 0$ then consider special case.
6. Предвычисления: $R = r \cdot Z_2$, $\widetilde{R} = R \cdot s_1$, $w_0 = s_1 \cdot s_3$, $w_1 = s_0 \cdot s_3$,
$w_3 = w_1 \cdot Z$, $w_4 = R \cdot s_3$.
7. Вычисление $l = su$, $l = l_2 x^2 + l_1 x + l_0$:
$l_0 = U_0 \cdot w_1$, $l_2 = U_1 \cdot w_0$, $l_1 = (w_1 + w_0) \cdot (U_1 + U_0) - l_0 - l_2$.
8. Вычисление $u' = \left[l^2 + \frac{1}{s} l(2v + h) - \frac{1}{s^2}\left(f - vh - v^2\right)\right]/u^2$, $u' = x^2 + u_1' x + u_0'$:
$\widetilde{U}_0' = s_0^2 + 2w_4 \cdot V_1 + R \cdot (s_3 \cdot (h_1 Z - h_2 U_1) + h_2 s_0 + R \cdot (2U_1 - f_4 Z))$,
$\widetilde{U}_1' = 2w_3 + h_2 \widetilde{R} - R^2$.
9. Корректировка: $U_0' = \widetilde{U}_0' \cdot \widetilde{R}$, $U_1' = \widetilde{U}_1' \cdot \widetilde{R}$, $Z' = s_1^2 \cdot \widetilde{R}$.
10. Вычисление $v' \equiv -(h + s_1 l + v_2) \bmod u'$, $v' = v_1' x + v_0'$:
$V_1' = \widetilde{U}_1' \cdot (l_2 - \widetilde{U}_1' + w_3 + h_2) + s_1^2 \cdot (\widetilde{U}_0' - h_1 \widetilde{R} - w_4 V_1 - l_1)$,
$V_0' = \widetilde{U}_0' \cdot (l_2 - \widetilde{U}_0' + w_3 + h_2) - s_1^2 \cdot (l_0 + h_0 \widetilde{R} + w_4 \cdot V_0)$.

Алгоритм. Удвоение дивизоров методом Ланге

Вход: $\mathrm{div}(U_1, U_0, V_1, V_0, Z)$

Выход: $\mathrm{div}(U_1', U_0', V_1', V_2', Z') = 2\,\mathrm{div}(U_1, U_0, V_1, V_0, Z)$

1. Вычисление результанты r для u и $h + 2v$ (причем $\widetilde{v} \equiv (h + 2v) \bmod u$):
$Z_2 = Z^2$, $\widetilde{V}_1 = h_1 Z + 2V_1 - h_2 U_1$, $\widetilde{V}_0 = h_0 Z + 2V_0 - h_2 U_2$, $w_0 = V_1^2$, $w_1 = U_1^2$,
$w_2 = \widetilde{V}_1^2 = h_1^2 Z_2 + 4w_0 - h_2^2 w_1$, $w_3 = \widetilde{V}_0 \cdot Z - U_1 \cdot \widetilde{V}_1$, $r = \widetilde{V}_0 \cdot w_3 + w_2 \cdot U_0$.
2. Вычисление квази-инверсии $inv \equiv r/\widetilde{v} \bmod u$, $inv = inv_1 x + inv_0$:
$inv_1 = -\widetilde{V}_1$, $inv_0 = w_3$.
3. Вычисление $k \equiv \left[\left(f - hv - v^2\right)/u\right] \bmod u$, $k = k_1 x + k_0$:
$w_3 = f_3 \cdot Z_2 + w_1$, $w_4 = 2U_0$, $k_1 = 2w_1 + w_3 - Z \cdot (w_4 + 2f_4 U_1 + h_2 V_1)$,
$k_0 = U_1 \cdot (Z \cdot (2w_4 + f_4 U_1 + h_2 V_1) - w_3) + Z \cdot (Z \cdot (f_2 \cdot Z - h_1 V_1 - h_2 V_0 - 2f_4 U_0) - w_0)$
4. Вычисление $s = k \cdot inv \bmod u$, $s = s_1 x + s_0$:
$w_0 = k_0 \cdot inv_0$, $w_1 = k_1 \cdot inv_1$, $s_0 = w_0 - Z \cdot U_0 \cdot w_1$,
$s_3 = (inv_0 + inv_1) \cdot (k_0 + k_1) - w_0 - w_1 \cdot (1 + U_1)$, $s_1 = s_3 \cdot Z$, $s_0 = w_0 - ZU_0 w_1$.
If $s_1 = 0$ then consider special case.
5. Предвычисления: $R = r \cdot Z_2$, $\widetilde{R} = R \cdot s_1$, $S_1 = s_1^2$, $S_0 = s_0^2$, $t = h_2 s_0$,
$s_1 = s_1 \cdot s_3$, $s_0 = s_0 \cdot s_3$, $S = s_0 \cdot Z$, $\widetilde{\widetilde{R}} = \widetilde{R} \cdot s_1$.
6. Вычисление $l = su$, $l = l_2 x^2 + l_1 x + l_0$:
$l_0 = U_0 \cdot s_0$, $l_2 = U_1 \cdot s_1$, $l_1 = (s_1 + s_0) \cdot (U_1 + U_0) - l_0 - l_2$.
7. Вычисление $u' = \left[l^2 + \frac{1}{s} l(2v + h) - \frac{1}{s^2}\left(f - vh - v^2\right)\right]/u^2$, $u' = x^2 + u_1' x + u_0'$:
$\widetilde{U}_0' = S_0 + R \cdot (s_3 \cdot (2V_1 - h_2 U_1 + h_1 Z) + t + Z \cdot r \cdot (2U_1 - f_4 Z))$, $\widetilde{U}_1' = 2S + h_2 \widetilde{R} - R^2$.
8. Предвычисления: $l_2 = l_2 + S - U_1'$, $w_0 = U_0' l_2 - S_1 l_0$, $w_1 = U_1' l_2 + S_1 (U_0' - l_1)$.
9. Корректировка: $U_0' = \widetilde{U}_0' \cdot \widetilde{R}$, $U_1' = \widetilde{U}_1' \cdot \widetilde{R}$, $Z' = S_1 \cdot \widetilde{R}$.
10. Вычисление $v' \equiv -(h + s_1 l + v_2) \bmod u'$, $v' = v_1' x + v_0'$:
$V_0' = w_0 + h_2 U_0' - \widetilde{\widetilde{R}} V_{20} - h_0 Z'$, $V_1' = w_1 + h_2 U_1' - \widetilde{\widetilde{R}} V_{21} - h_1 Z'$.