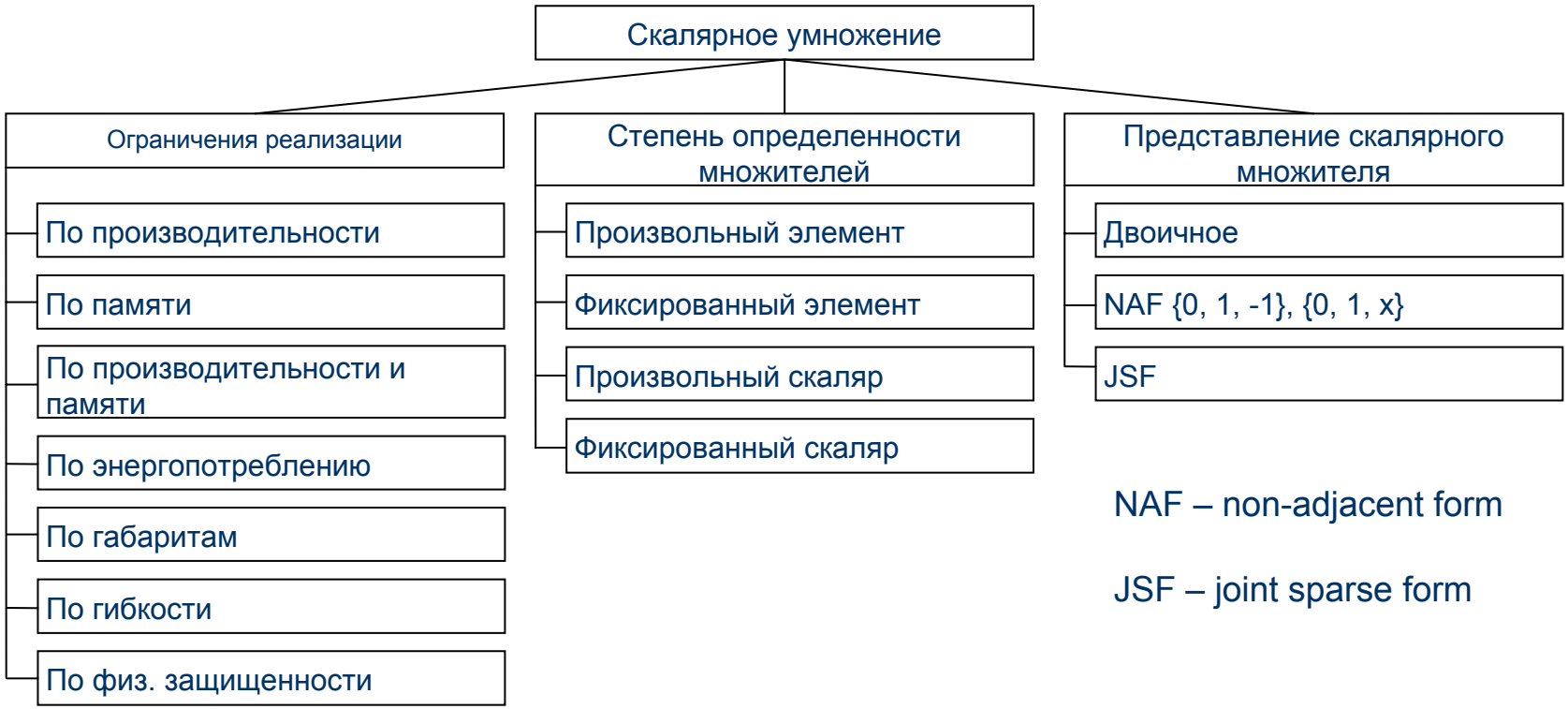
АЛГОРИТМЫ СКАЛЯРНОГО УМНОЖЕНИЯ В ГРУППЕ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ И НЕКОТОРЫЕ ИХ МОДИФИКАЦИИ

КОВТУН В.Ю.

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

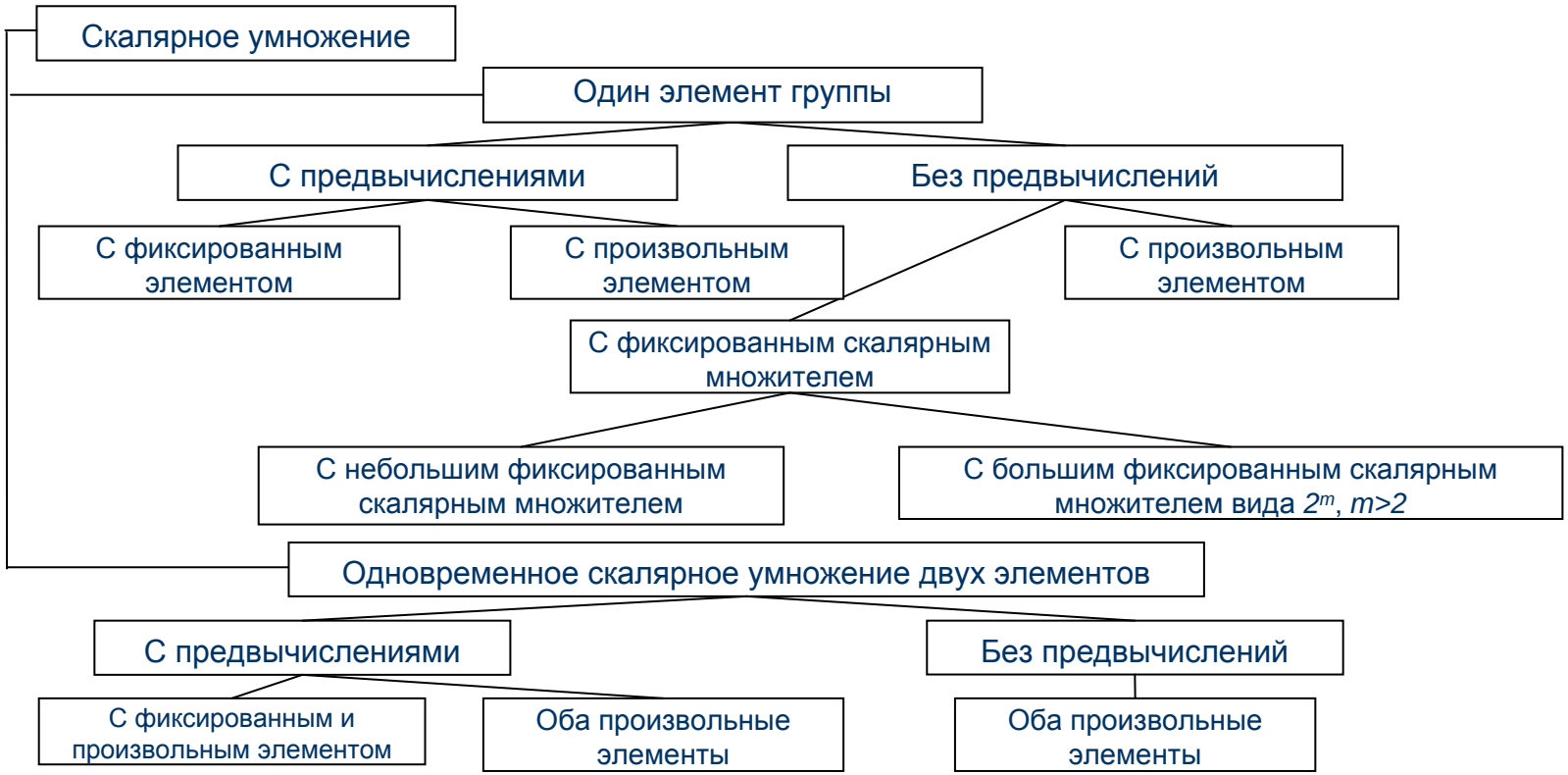


Рис. Классификация алгоритмов скалярного умножения по наличию предвычислений и по степени определенности множителей

АЛГОРИТМ ОДНОВРЕМЕННОГО СКАЛЯРНОГО УМНОЖЕНИЯ

Алгоритм. Одновременного умножения на основе умножения методом Лим-Лии и «оконного» умножения

Вход: $k = (k_{d-1}, \ldots, k_1, k_0)_{2^w}$, $l = (l_{d-1}, \ldots, l_1, l_0)_{2^w}$, $d = \lceil t/w \rceil$, $P, Q \in \mathbf{G}$

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. $u \leftarrow (u_{h-1}, \ldots, u_1, u_0)_2$, $P_{s,u} \leftarrow 2^{sb} \sum_{i=0}^{h-1} u_i 2^{vbi} P$.
2. $P' \leftarrow O$.
3. For $t = b - 1$ 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
   6.1. For each i for which $k_i = j$ do
      6.1.1. $B \leftarrow B + Q_i$.
   6.2. $Q' \leftarrow Q' + B$.
7. $R \leftarrow P' + Q'$.
8. Return (R).

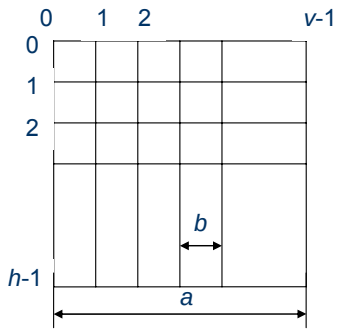


Рис. Таблица предвычислений алгоритма Лим-Лии

УСОВЕРШЕНСТВОВАННЫЙ АЛГОРИТМ ОДНОВРЕМЕННОГО СКАЛЯРНОГО УМНОЖЕНИЯ

Метод Усовершенствованного одновременного умножения на основе умножения Лим-Лии и «оконного» умножения

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

Выход: $kP+lQ$

1. For $u=1$ to 2^h-1 do
   1.1. $u=(u_{h-1},\ldots,u_1,u_0)_2$.
   1.2. $P_{0,u}=\sum_{r=0}^{h/2-1}u_{2r}2^{2rvb}P$, $G_{0,u}\leftarrow 2^{vb}P_{0,u}$.
   1.3. For $s=1$ to $v-1$ do
      1.3.1. $P_{s,u}\leftarrow 2^{sb}P_{0,u}$.
      1.3.2. $G_{s,u}\leftarrow 2^{vb}P_{s,u}$.
2. $P'\leftarrow O$.
3. For $r=b/2-1$ downto 0 do
   3.1. $P'\leftarrow 2P'$.
   3.2. For $s=v-1$ downto 0 do
      3.2.1. $I_{s,r}\leftarrow\sum_{i=0}^{h/2-1}2^{2i}\left(K_{2vbi+bs+2r}+2K_{2vbi+bs+2r+1}\right)$.
      3.2.2. If $(I_{s,r}\neq 0)$ then $u\leftarrow I_{s,r}$, $P'\leftarrow P'+P_{s,u}$.
      3.2.3. $I_{s,r}\leftarrow\sum_{i=0}^{h/2-1}2^{2i}\left(K_{vb(2i+1)+bs+2r}+2K_{vb(2i+1)+bs+2r+1}\right)$.
      3.2.4. If $(I_{s,r}\neq 0)$ then $u\leftarrow I_{s,r}$, $P'\leftarrow P'+G_{s,u}$.
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
   6.1. For each i for which $k_i=j$ do
      6.1.1. $B\leftarrow B+Q_i$.
   6.2. $Q'\leftarrow Q'+B$.
7. $R\leftarrow P'+Q'$.
8. Return (R).

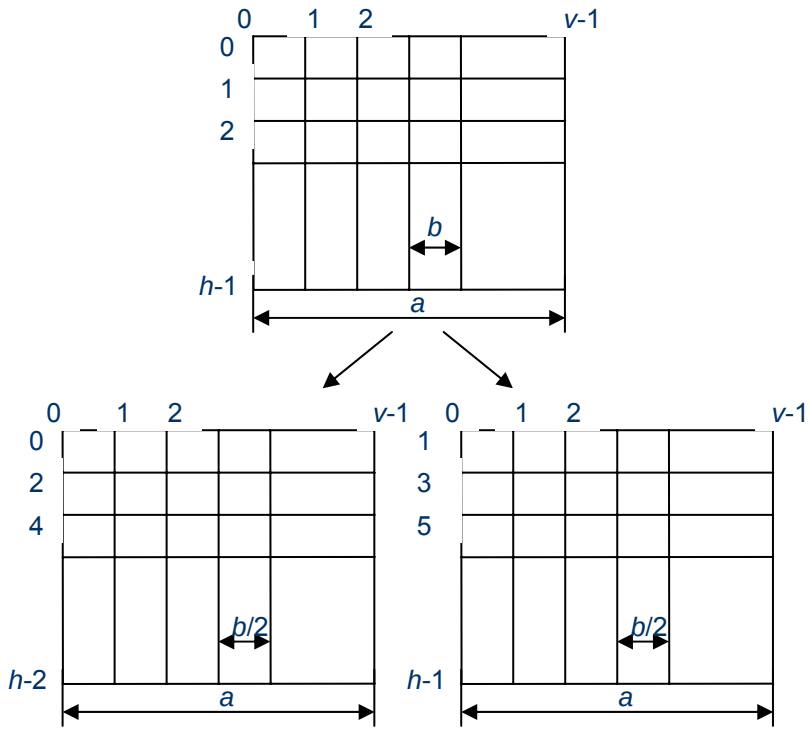


Рис. Таблица предвычислений метода Лим-Лии (сверху) и две таблицы предвычислений усовершенствованного метода (снизу)

УСОВЕРШЕНСТВОВАННЫЙ АЛГОРИТМ ОДНОВРЕМЕННОГО СКАЛЯРНОГО УМНОЖЕНИЯ

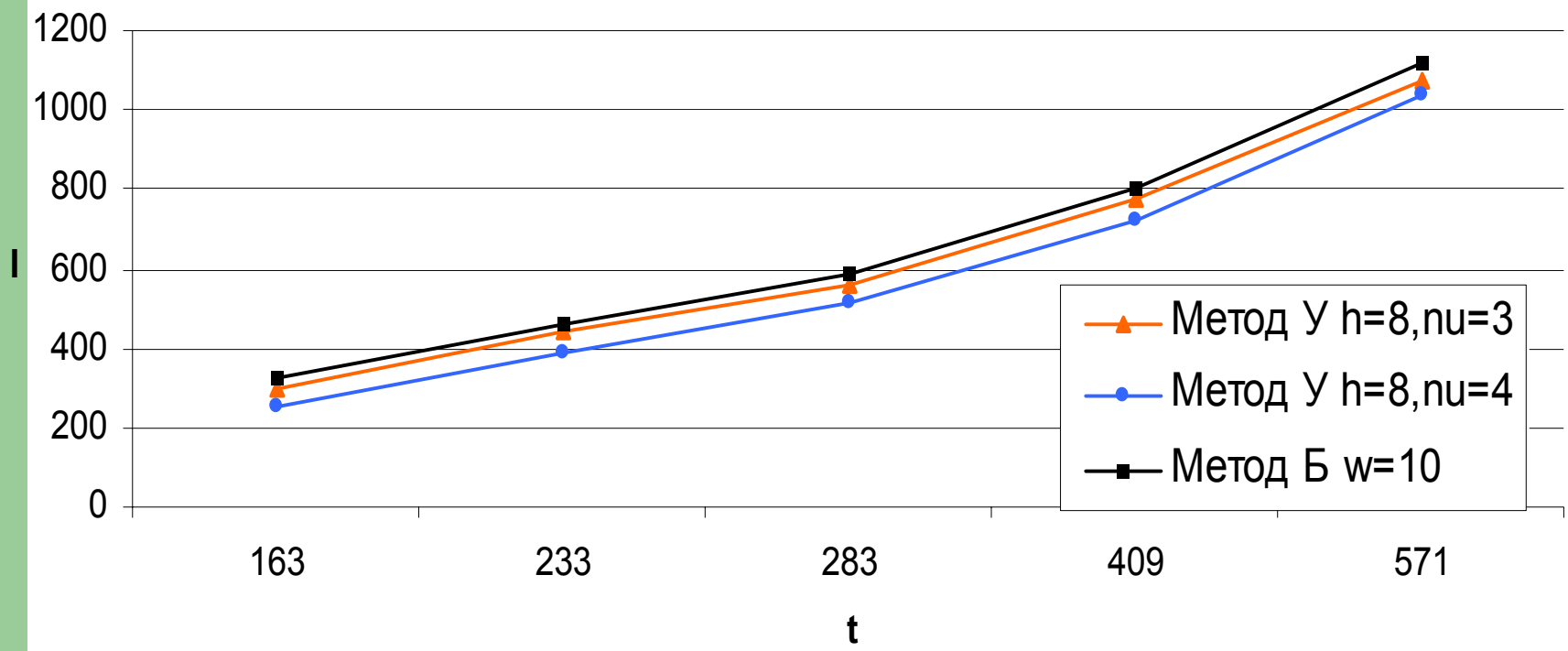
- ***Утверждение 1.*** Вычислительная сложность алгоитма одновременного умножения на основе усовершенствованного метода Лим-Лии с параметрами ***h*** и ***v*** и «оконного» умножения шириной окна предвычислений ***w*** для скалярных множителей ***k*** и ***l*** , битовой длины ***t***, составит:

$$I\left(A^{aver}\right)=\left(\left(\left(2^h-1\right)/2^h\right)a-1\right)I_{add}^G+b/2\,I_{dbl}^G+\left(\left(d\left(2^w-1\right)/2^w-1\right)+\left(2^w-2\right)\right)I_{add}^G+\left(w+d\right)I_{dbl}^G$$

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

$$S(A)=\left(2v\left(2^h-1\right)+2^w-1\right)S^G$$

Вычислительные сложности предложенного и базового методов при соизмеримых размерах предвычислений



Аналитические и количественные оценки

Таблица 8.1

Аналитические оценки вычислительной сложности алгоритмов СУ без предвычислений

Наименование	Вычислительная сложность
Алгоритм 2.1. Двоичное умножение слева направо	$I\left(A_{2.1}^{aver}\right) = \frac{t}{2} I_{add}^{G} + tI_{dbl}^{G}$
Алгоритм 2.2. Двоичное NAF умножение	$I\left(A_{2.2}\right) = \frac{t}{3} I_{add}^{G} + tI_{dbl}^{G}$
Алгоритм 2.3. Двоичное умножение Монтгомери	$I\left(A_{2.3}\right) = tI_{add}^{G} + tI_{dbl}^{G}$

Таблица 8.2

Количественные оценки вычислительной сложности алгоритмов СУ без предвычислений, в групповых операциях

Наименование	Вычислительная сложность									
	t=163		t=233		t=283		t=409		t=571	
	I_{add}^{G}	I_{dbl}^{G}	I_{add}^{G}	I_{dbl}^{G}	I_{add}^{G}	I_{dbl}^{G}	I_{add}^{G}	I_{dbl}^{G}	I_{add}^{G}	I_{dbl}^{G}
Алгоритм 2.1. Двоичное умножение слева направо	82	163	117	233	142	283	205	409	286	571
Алгоритм 2.2. Двоичное NAF умножение	55	163	78	233	95	283	167	409	191	571
Алгоритм 2.3. Двоичное умножение Монтгомери	163	163	233	233	283	283	409	409	571	571

Аналитические и количественные оценки

Таблица 9.1

Аналитические оценки вычислительной сложности алгоритмов СУ с предвычислениями

Наименование	Вычислительная сложность
Алгоритм 2.4. «Оконное» умножение	$I\left(A_{2.4}^{aver}\right)=\left(\left(d\left(2^w-1\right)/2^w-1\right)+\left(2^w-2\right)\right)I_{add}$
Алгоритм 2.5. «Оконное» NAF умножение	$I\left(A_{2.5}\right)=\left(1I_{dbl}+\left(2^{w-2}-1\right)I_{add}\right)+\left(t/\left(w+1\right)I_{add}+tI_{dbl}\right)$
Алгоритм 2.6. Умножение Лим-Лии фиксированного элемента	$I\left(A_{2.6}^{aver}\right)=\left(\left(\left(2^h-1\right)/2^h\right)a-1\right)I_{add}+bI_{dbl}$
Алгоритм 2.7. Комбинированное умножение фиксированного элемента	$I\left(A_{2.7}^{aver}\right)=\left(d\left(2^w-1\right)/2^w\right)I_{add}+dI_{dbl}$

Таблица 9.2

Количественные оценки вычислительной сложности алгоритмов СУ с предвычислениями, в групповых операциях

Наименование	Вычислительная сложность									
	t=163		t=233		t=283		t=409		t=571	
	I_{add}^{G}	I_{dbl}^{G}	I_{add}^{G}	I_{dbl}^{G}	I_{add}^{G}	I_{dbl}^{G}	I_{add}^{G}	I_{dbl}^{G}	I_{add}^{G}	I_{dbl}^{G}
Алгоритм 2.4. «Оконное» умножение, $w=4$	52	0	68	0	80	0	109	0	147	0
Алгоритм 2.5. «Оконное» NAF умножение, $w=4$	36	164	50	234	60	284	85	410	118	572
Алгоритм 2.6. Умножение Лим-Лии фиксированного элемента, $h=8$, $v=3$	20	7	29	10	35	12	51	18	71	24
Алгоритм 2.7. Комбинированное умножение фиксированного элемента, $w=10$	17	17	24	24	29	29	41	41	58	58

$I_{add}^{P}\approx 13{,}4I_{mul}$, $I_{dbl}^{P}\approx 5{,}55I_{mul}$

Аналитические оценки

Таблица 2.9

Аналитические оценки вычислительной сложности алгоритмов одновременного СУ

Наименование	Вычислительная сложность
Алгоритм 2.8. Одновременное умножение	$I(A_{2.8}) = (2^{2w} - 3)I_{add} + (d-1)(2^{2w} - 1)/2^{2w} I_{add} + tI_{dbl}$
Алгоритм 2.9. Одновременное умножение Шамира, без предвычислений (двоичное представление)	$I(A_{2.9}^{aver}) = (\frac{3}{4}t + 1)I_{add} + tI_{dbl}$
Алгоритм 2.9. Одновременное умножение Шамира, без предвычислений (NAF)	$I(A_{2.9}^{aver} NAF) = (\frac{5}{9}t + 2)I_{add} + tI_{dbl}$
Алгоритм 2.9. Одновременное умножение Шамира, без предвычислений (JSF)	$I(A_{2.9}^{aver} JSF) = (\frac{1}{2}t + 2)I_{add} + tI_{dbl}$
Алгоритм 2.10. Одновременное умножение на основе комбинированного умножения фиксированного элемента и «оконного» умножения	$I(A_{2.10}^{aver}) = (d(2^w - 1)/2^w)I_{add}^G + dI_{dbl}^G + + ((d(2^w - 1)/2^w - 1) + (2^w - 2))I_{add}^G$
Алгоритм 2.11. Одновременное умножение на основе умножения Лим-Лии фиксированного элемента и «оконного» умножения	$I(A_{2.11}^{aver}) = (((2^h - 1)/2^h)a - 1)I_{add} + b/2\, I_{dbl} + + ((d(2^w - 1)/2^w - 1) + (2^w - 2))I_{add}$

Количественные оценки

Таблица 11.1

Количественные оценки вычислительной сложности алгоритмов одновременного СУ, в групповых операциях

Наименование	Вычислительная сложность									
	t=163		*t*=233		*t*=283		*t*=409		*t*=571	
	I^G_{add}	I^G_{dbl}	I^G_{add}	I^G_{dbl}	I^G_{add}	I^G_{dbl}	I^G_{add}	I^G_{dbl}	I^G_{add}	I^G_{dbl}
Алгоритм 2.8. Одновременное умножение, $w=4$	293	163	311	233	323	283	354	409	395	571
Алгоритм 2.9. Одновременное умножение Шамира, без предвычислений (двоичное представление)	124	163	176	233	214	283	308	409	430	571
Алгоритм 2.9. Одновременное умножение Шамира, без предвычислений (NAF)	93	163	132	233	160	283	230	409	320	571
Алгоритм 2.9. Одновременное умножение Шамира, без предвычислений (JSF)	84	163	119	233	144	283	206	409	288	571
Алгоритм 2.10. Одновременное умножение на основе комбинированного умножения фиксированного элемента и «оконного» умножения, $h=10$, $w=4$	69	17	92	24	109	29	150	41	205	58
Алгоритм 2.11. Одновременное умножение на основе умножения Лим-Лии и «оконного» умножения, $h=8$, $v=4$, $w=4$	72	3	97	4	115	5	160	7	218	9

$I^P_{add} \approx 13{,}4 I_{mul}$, $I^P_{dbl} \approx 5{,}55 I_{mul}$