Point Multiplication area-time trade-of for GF(2^409)

g. Bits computed per clock cycle in GF multiplication.
d. Bits computed per clock cycle in GF division.
AxD is the area by delay metric in LUTs by *ms* (less is better).
area measured in 1000 6 input LUTs

one multiplier – one divider						
g	***d***	**# Cycles**	**T (ns)**	**Time (µs)**	**area**	**AxD**
1	1	843781	1,9	1603,2	10,3	16457
4	1	215045	1,8	387,1	10,7	4132
4	2	214225	2,3	492,7	13,1	6467
8	2	109777	2,3	252,5	13,9	3521
8	2	109777	2,3	252,5	13,9	3521
23	3	39873	2,8	111,6	17,6	1960
32	3	29633	2,9	85,9	19,3	1658
32	4	29497	3,4	100,3	21,8	2182
two multiplier – one divider						
g	***d***	**# Cycles**	**T (ns)**	**Time (µs)**	**area**	**AxD**
1	1	507172	1,9	963,6	11,5	11090
4	1	129869	1,8	233,8	12,3	2882
8	2	66370	2,3	152,7	16,4	2506
16	2	34416	2,4	82,6	19,7	1627
23	3	24312	2,8	68,1	23,2	1580
32	3	18167	2,9	52,7	26,7	1407
two multiplier – two divider						
g	***d***	**# Cycles**	**T (ns)**	**Time (µs)**	**area**	**AxD**
1	1	506350	1,9	962,1	13,6	13062
4	1	129047	1,8	232,3	14,4	3344
8	2	65958	2,3	151,7	20,9	3176
16	2	34004	2,4	81,6	24,2	1977
23	3	24036	2,8	67,3	28,2	1895
32	3	17891	2,9	51,9	31,6	1642
three multiplier – one divider						
g	***d***	**# Cycles**	**T (ns)**	**Time (µs)**	**area**	**AxD**
1	1	339073	1,9	644,2	12,8	8216
4	1	87333	1,8	157,2	14,0	2198
8	1	45513	2,3	104,7	16,4	1720
8	2	44693	2,3	102,8	18,9	1941
16	1	24193	2,4	58,1	21,4	1240
16	2	23373	2,4	56,1	23,8	1336
23	2	16813	2,8	47,1	28,4	1338
23	3	16541	2,8	46,3	28,9	1337
32	2	12713	2,9	36,9	33,7	1241
32	3	12441	2,9	36,1	34,1	1230