Point Multiplication area-time trade-of for GF(2^233)

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	275653	1,8	496,2	5,9	2908,6
8	2	36913	2,4	88,6	8,0	704,9
16	3	19237	2,5	48,1	9,1	439,8
30	3	11061	2,8	31,0	10,8	334,2
39	3	8725	2,9	25,3	12,0	302,6
47	3	7557	2,9	21,9	12,7	278,3
47	4	7481	3,4	25,4	14,1	358,7
47	5	7433	3,7	27,5	14,7	404,1
59	3	6389	3,1	19,8	13,9	275,2
59	4	6313	3,4	21,5	15,3	328,3
two multiplier – one divider						
g	***d***	**# Cycles**	**T (ns)**	**Time (µs)**	**area**	**AxD**
1	1	165908	1,8	298,6	6,6	1963,8
4	1	43233	1,8	77,8	7,0	548,0
16	3	11765	2,5	29,4	11,5	338,1
30	3	6858	2,8	19,2	14,8	283,9
47	3	4755	2,9	13,8	18,6	256,6
59	3	4054	3,1	12,6	21,0	263,8
two multiplier – two divider						
g	***d***	**# Cycles**	**T (ns)**	**Time (µs)**	**area**	**AxD**
1	1	165438	1,8	297,8	7,8	2311,7
4	1	42763	1,8	77,0	8,2	633,4
16	3	11607	2,5	29,0	14,3	415,8
39	3	5298	2,9	15,4	20,0	306,7
47	3	4597	2,9	13,3	21,4	285,8
59	3	3896	3,1	12,1	23,8	287,7
three multiplier – one divider						
g	***d***	**# Cycles**	**T (ns)**	**Time (µs)**	**area**	**AxD**
1	1	111153	1,8	200,1	3,3	666,1
4	1	29253	1,8	52,7	4,0	212,1
16	2	8193	2,4	19,7	9,6	189,5
16	3	8037	2,5	20,1	9,9	198,6
39	3	3825	2,9	11,1	18,3	203,4
47	3	3357	2,9	9,7	20,6	200,1
47	4	3281	3,4	11,2	22,0	244,9
59	3	2889	3,1	9,0	24,1	216,1
59	4	2813	3,4	9,6	25,5	244,2