Point Multiplication area-time trade-of for GF(2^571)

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	1640497	1,9	3116,9	14,3	44622
4	1	414415	1,8	745,9	14,9	11105
4	2	413271	2,3	950,5	18,3	17401
8	2	210353	2,4	504,8	19,5	9822
8	2	210353	2,4	504,8	19,5	9822
24	3	72789	2,8	203,8	24,6	5024
32	3	55641	3,0	166,9	26,9	4498
32	4	55449	3,3	183,0	30,4	5560
two multiplier – one divider						
g	***d***	**# Cycles**	**T (ns)**	**Time (µs)**	**area**	**AxD**
1	1	985558	1,9	1872,6	16,0	30049
4	1	249823	1,8	449,7	17,2	7730
8	2	126914	2,4	304,6	22,9	6977
16	2	65174	2,7	176,0	27,5	4841
24	3	44214	2,8	123,8	32,7	4048
32	3	33924	3,0	101,8	37,3	3796
two multiplier – two divider						
g	***d***	**# Cycles**	**T (ns)**	**Time (µs)**	**area**	**AxD**
1	1	984412	1,9	1870,4	18,9	35397
4	1	248677	1,8	447,6	20,1	8982
8	2	126340	2,4	303,2	29,2	8855
16	2	64600	2,7	174,4	33,8	5897
24	3	43830	2,8	122,7	39,6	4859
32	3	33540	3,0	100,6	44,2	4446
three multiplier – one divider						
g	***d***	**# Cycles**	**T (ns)**	**Time (µs)**	**area**	**AxD**
1	1	658375	1,9	1250,9	17,8	22239
4	1	167599	1,8	301,7	19,5	5880
8	1	86375	2,4	207,3	22,9	4755
8	2	85231	2,4	204,6	26,4	5392
16	1	45191	2,7	122,0	29,8	3642
16	2	44047	2,7	118,9	33,3	3956
24	2	30319	2,8	84,9	40,2	3409
24	3	29939	2,8	83,8	40,8	3416
32	2	23455	3,0	70,4	47,1	3311
32	3	23075	3,0	69,2	47,6	3298