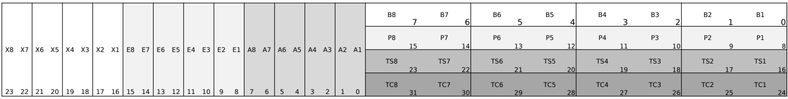
MWMAC binary field point addition function Memory plan

MWMAC RAM

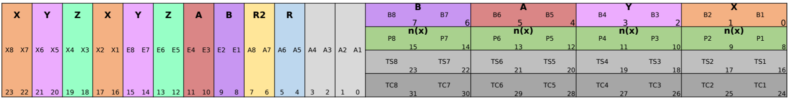
Empty start



X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

B8	B7	B6	B5	B4	B3	B2	B1
7	6	5	4	3	2	1	0
P8	P7	P6	P5	P4	P3	P2	P1
15	14	13	12	11	10	9	8
TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1
23	22	21	20	19	18	17	16
TC8	TC7	TC6	TC5	TC4	TC3	TC2	TC1
31	30	29	28	27	26	25	24

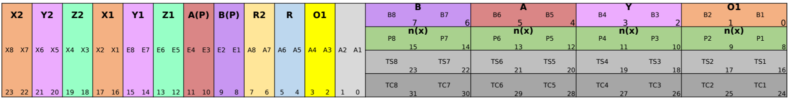
After prepartation



X	Y	Z	X	Y	Z	A	B	R2	R		
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

B		A		Y		X	
B8	B7	B6	B5	B4	B3	B2	B1
7	6	5	4	3	2	1	0
n(x)		n(x)		n(x)		n(x)	
P8	P7	P6	P5	P4	P3	P2	P1
15	14	13	12	11	10	9	8
TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1
23	22	21	20	19	18	17	16
TC8	TC7	TC6	TC5	TC4	TC3	TC2	TC1
31	30	29	28	27	26	25	24

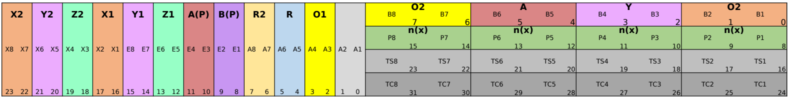
O1 = Z1*Z1*rinvpoly
A3 = MontMult(E5, E5, P1)　　　　CopyH2V(B1, A3)



X2	Y2	Z2	X1	Y1	Z1	A(P)	B(P)	R2	R	O1	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

B		A		Y		O1	
B8	B7	B6	B5	B4	B3	B2	B1
7	6	5	4	3	2	1	0
n(x)		n(x)		n(x)		n(x)	
P8	P7	P6	P5	P4	P3	P2	P1
15	14	13	12	11	10	9	8
TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1
23	22	21	20	19	18	17	16
TC8	TC7	TC6	TC5	TC4	TC3	TC2	TC1
31	30	29	28	27	26	25	24

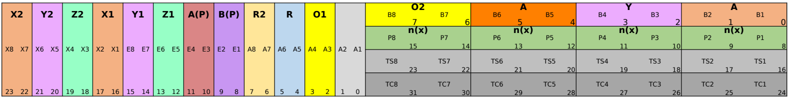
O2 = Z2*Z2*rinvpoly
B7 = MontMult(X3,X3,P1)　　　　CopyH2H(B1,B7)



X2	Y2	Z2	X1	Y1	Z1	A(P)	B(P)	R2	R	O1	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

O2		A		Y		O2	
B8	B7	B6	B5	B4	B3	B2	B1
7	6	5	4	3	2	1	0
n(x)		n(x)		n(x)		n(x)	
P8	P7	P6	P5	P4	P3	P2	P1
15	14	13	12	11	10	9	8
TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1
23	22	21	20	19	18	17	16
TC8	TC7	TC6	TC5	TC4	TC3	TC2	TC1
31	30	29	28	27	26	25	24

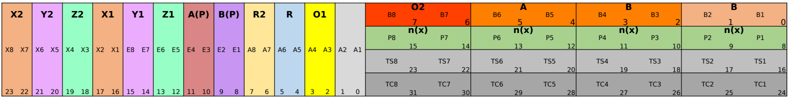
A = X1*O2*rinvpoly
B5 = MontMult(X1,B7,P1)　　　　CopyH2H(B1,B5)



X2	Y2	Z2	X1	Y1	Z1	A(P)	B(P)	R2	R	O1	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

O2		A		Y		A	
B8	B7	B6	B5	B4	B3	B2	B1
7	6	5	4	3	2	1	0
n(x)		n(x)		n(x)		n(x)	
P8	P7	P6	P5	P4	P3	P2	P1
15	14	13	12	11	10	9	8
TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1
23	22	21	20	19	18	17	16
TC8	TC7	TC6	TC5	TC4	TC3	TC2	TC1
31	30	29	28	27	26	25	24

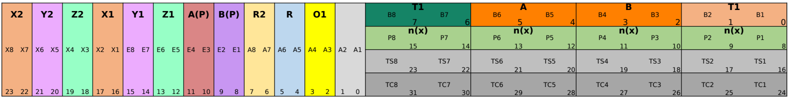
B = X2*O1*rinvpoly
B3 = MontMult(X7,A3,P1)　　　　CopyH2H(B1,B3)



X2	Y2	Z2	X1	Y1	Z1	A(P)	B(P)	R2	R	O1	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

O2		A		B		B	
B8	B7	B6	B5	B4	B3	B2	B1
7	6	5	4	3	2	1	0
n(x)		n(x)		n(x)		n(x)	
P8	P7	P6	P5	P4	P3	P2	P1
15	14	13	12	11	10	9	8
TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1
23	22	21	20	19	18	17	16
TC8	TC7	TC6	TC5	TC4	TC3	TC2	TC1
31	30	29	28	27	26	25	24

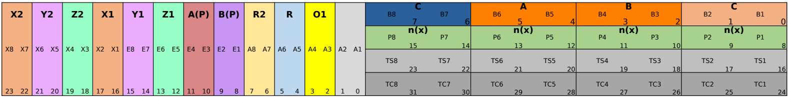
T1 = Y1*O2*rinvpoly
B7 = MontMult(E7,B7,P1)　　　　CopyH2H(B1,B7)



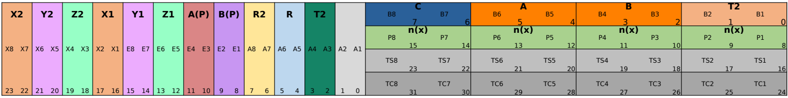
X2	Y2	Z2	X1	Y1	Z1	A(P)	B(P)	R2	R	O1	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

T1		A		B		T1	
B8	B7	B6	B5	B4	B3	B2	B1
7	6	5	4	3	2	1	0
n(x)		n(x)		n(x)		n(x)	
P8	P7	P6	P5	P4	P3	P2	P1
15	14	13	12	11	10	9	8
TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1
23	22	21	20	19	18	17	16
TC8	TC7	TC6	TC5	TC4	TC3	TC2	TC1
31	30	29	28	27	26	25	24

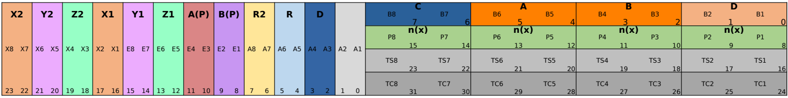
C = T1*Z2*rinvpoly
B7 = MontMult(B7,X3,P1) CopyH2H(B1,B7)



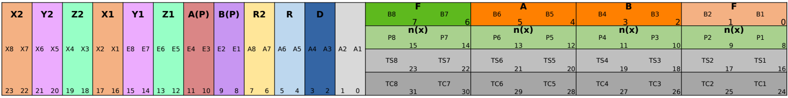
T2 = Y2*O1*rinvpoly
A3 = MontMult(X5,A3,P1) CopyH2V(B1, A3)



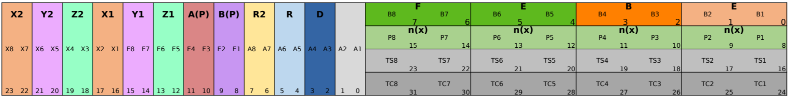
D = T2*Z1*rinvpoly
A3 = MontMult(A3,E5,P1) CopyH2V(B1, A3)



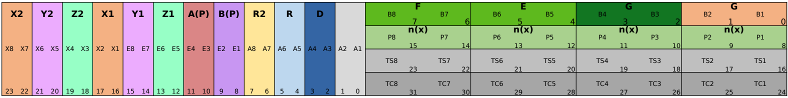
F = C+D
B7 = ModAdd(B7,A3,P1) CopyH2H(B1, B7)



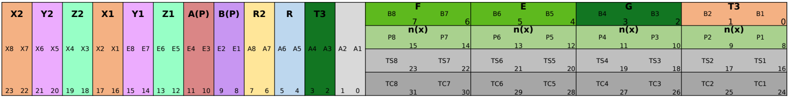
E = A+B
A3 = ModAdd(B5,B3,P1) CopyH2H(B1,B5)



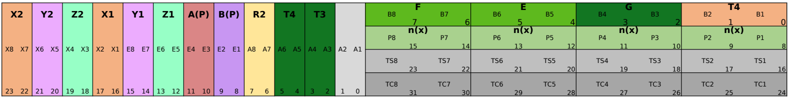
G = E*Z1*rinvpoly
B3 = MontMult(B5,E5,P1) CopyH2H(B1,B3)



T3 = F*X2*rinvpoly
A3 = MontMult(B7,X7,P1) CopyH2V(B1,A3)



T4 = G*Y2*rinvpoly
A5 = MontMult(B3,X5,P1) CopyH2V(B1,A5)

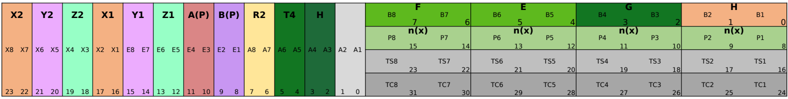


X2	Y2	Z2	X1	Y1	Z1	A(P)	B(P)	R2	T4	T3	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

F		E		G		T4	
B8	B7	B6	B5	B4	B3	B2	B1
7	6	5	4	3	2	1	0
n(x)		n(x)		n(x)		n(x)	
P8	P7	P6	P5	P4	P3	P2	P1
15	14	13	12	11	10	9	8
TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1
23	22	21	20	19	18	17	16
TC8	TC7	TC6	TC5	TC4	TC3	TC2	TC1
31	30	29	28	27	26	25	24

H = T3+T4

A3 = ModAdd(A3,A5,P1)   CopyH2V(B1,A5)

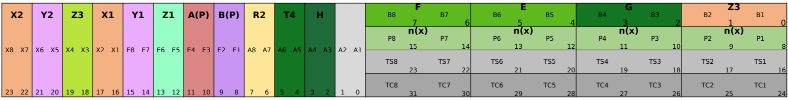


X2	Y2	Z2	X1	Y1	Z1	A(P)	B(P)	R2	T4	H	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

F		E		G		H	
B8	B7	B6	B5	B4	B3	B2	B1
7	6	5	4	3	2	1	0
n(x)		n(x)		n(x)		n(x)	
P8	P7	P6	P5	P4	P3	P2	P1
15	14	13	12	11	10	9	8
TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1
23	22	21	20	19	18	17	16
TC8	TC7	TC6	TC5	TC4	TC3	TC2	TC1
31	30	29	28	27	26	25	24

Z3 = G*Z2*rinvpoly

X3 = MontMult(B3,X3,P1)   CopyH2V(B1,X3)

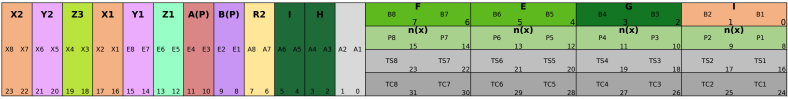


X2	Y2	Z3	X1	Y1	Z1	A(P)	B(P)	R2	T4	H	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

F		E		G		Z3	
B8	B7	B6	B5	B4	B3	B2	B1
7	6	5	4	3	2	1	0
n(x)		n(x)		n(x)		n(x)	
P8	P7	P6	P5	P4	P3	P2	P1
15	14	13	12	11	10	9	8
TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1
23	22	21	20	19	18	17	16
TC8	TC7	TC6	TC5	TC4	TC3	TC2	TC1
31	30	29	28	27	26	25	24

I = F+Z3

A5 = ModAdd(B7,X3)   CopyH2V(B1,A5)

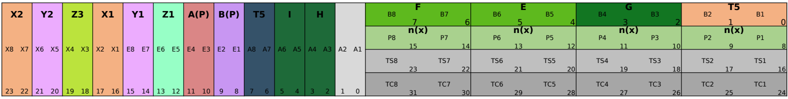


X2	Y2	Z3	X1	Y1	Z1	A(P)	B(P)	R2	I	H	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

F		E		G		I	
B8	B7	B6	B5	B4	B3	B2	B1
7	6	5	4	3	2	1	0
n(x)		n(x)		n(x)		n(x)	
P8	P7	P6	P5	P4	P3	P2	P1
15	14	13	12	11	10	9	8
TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1
23	22	21	20	19	18	17	16
TC8	TC7	TC6	TC5	TC4	TC3	TC2	TC1
31	30	29	28	27	26	25	24

T5 = Z3*Z3*rinvpoly

A7 = MontMult(X3,X3,P1)   CopyH2V(B1,A7)

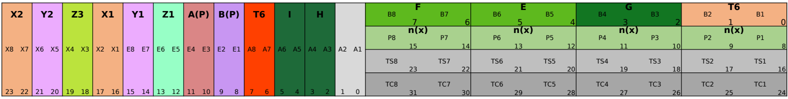


X2	Y2	Z3	X1	Y1	Z1	A(P)	B(P)	T5	I	H	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

F		E		G		T5	
B8	B7	B6	B5	B4	B3	B2	B1
7	6	5	4	3	2	1	0
n(x)		n(x)		n(x)		n(x)	
P8	P7	P6	P5	P4	P3	P2	P1
15	14	13	12	11	10	9	8
TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1
23	22	21	20	19	18	17	16
TC8	TC7	TC6	TC5	TC4	TC3	TC2	TC1
31	30	29	28	27	26	25	24

T6 = apoly_mont*T5*rinvpoly

A7 = MontMult(E3,A7,P1)   CopyH2V(B1,A7)

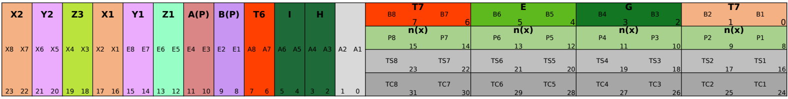


X2	Y2	Z3	X1	Y1	Z1	A(P)	B(P)	T6	I	H	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

F		E		G		T6	
B8	B7	B6	B5	B4	B3	B2	B1
7	6	5	4	3	2	1	0
n(x)		n(x)		n(x)		n(x)	
P8	P7	P6	P5	P4	P3	P2	P1
15	14	13	12	11	10	9	8
TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1
23	22	21	20	19	18	17	16
TC8	TC7	TC6	TC5	TC4	TC3	TC2	TC1
31	30	29	28	27	26	25	24

T7 = F*I*rinvpoly

B7 = MontMult(B7,A5,P1)   CopyH2H(B1,B7)

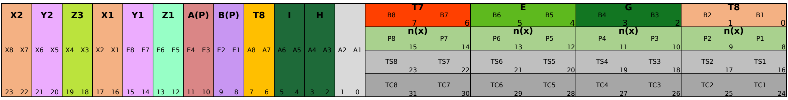


X2	Y2	Z3	X1	Y1	Z1	A(P)	B(P)	T6	I	H	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

T7		E		G		T7	
B8	B7	B6	B5	B4	B3	B2	B1
7	6	5	4	3	2	1	0
n(x)		n(x)		n(x)		n(x)	
P8	P7	P6	P5	P4	P3	P2	P1
15	14	13	12	11	10	9	8
TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1
23	22	21	20	19	18	17	16
TC8	TC7	TC6	TC5	TC4	TC3	TC2	TC1
31	30	29	28	27	26	25	24

T8 = T6+T7

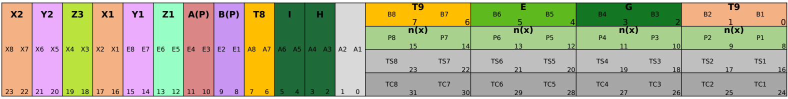
A7 = ModAdd(A7,B7,P1)   CopyH2V(B1,A7)



X2	Y2	Z3	X1	Y1	Z1	A(P)	B(P)	T8	I	H	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

T7		E		G		T8	
B8	B7	B6	B5	B4	B3	B2	B1
7	6	5	4	3	2	1	0
n(x)		n(x)		n(x)		n(x)	
P8	P7	P6	P5	P4	P3	P2	P1
15	14	13	12	11	10	9	8
TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1
23	22	21	20	19	18	17	16
TC8	TC7	TC6	TC5	TC4	TC3	TC2	TC1
31	30	29	28	27	26	25	24

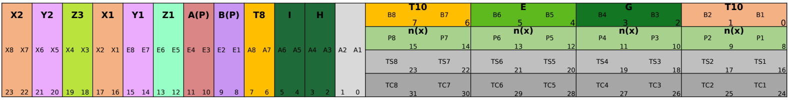
T9 = E*E*rinvpoly
B7 = MontMult(B5,B5,P1) CopyH2H(B1,B7)



X2	Y2	Z3	X1	Y1	Z1	A(P)	B(P)	T8	I	H	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

T9	E	G	T9
B8 B7 7 6	B6 B5 5 4	B4 B3 3 2	B2 B1 1 0
n(x) P8 P7 15 14	n(x) P6 P5 13 12	n(x) P4 P3 11 10	n(x) P2 P1 9 8
TS8 TS7 23 22	TS6 TS5 21 20	TS4 TS3 19 18	TS2 TS1 17 16
TC8 TC7 31 30	TC6 TC5 29 28	TC4 TC3 27 26	TC2 TC1 25 24

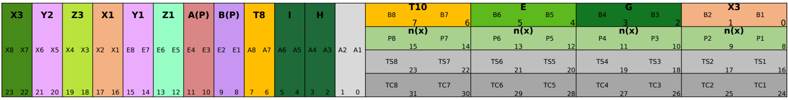
T10 = T9*E*rinvpoly
B7 = MontMult(B7,B5,P1) CopyH2H(B1,B7)



X2	Y2	Z3	X1	Y1	Z1	A(P)	B(P)	T8	I	H	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

T10	E	G	T10
B8 B7 7 6	B6 B5 5 4	B4 B3 3 2	B2 B1 1 0
n(x) P8 P7 15 14	n(x) P6 P5 13 12	n(x) P4 P3 11 10	n(x) P2 P1 9 8
TS8 TS7 23 22	TS6 TS5 21 20	TS4 TS3 19 18	TS2 TS1 17 16
TC8 TC7 31 30	TC6 TC5 29 28	TC4 TC3 27 26	TC2 TC1 25 24

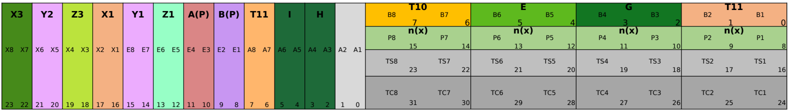
X3 = T8+T10
X7 = ModAdd(A7,B7,P1) CopyH2V(B1,X7)



X3	Y2	Z3	X1	Y1	Z1	A(P)	B(P)	T8	I	H	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

T10	E	G	X3
B8 B7 7 6	B6 B5 5 4	B4 B3 3 2	B2 B1 1 0
n(x) P8 P7 15 14	n(x) P6 P5 13 12	n(x) P4 P3 11 10	n(x) P2 P1 9 8
TS8 TS7 23 22	TS6 TS5 21 20	TS4 TS3 19 18	TS2 TS1 17 16
TC8 TC7 31 30	TC6 TC5 29 28	TC4 TC3 27 26	TC2 TC1 25 24

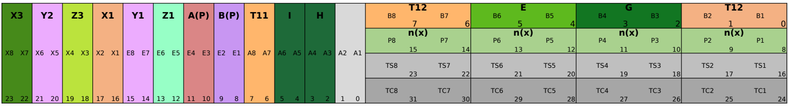
T11 = I*X3*rinvpoly
A7 = MontMult(A5,X7,P1) CopyH2V(B1,A7)



X3	Y2	Z3	X1	Y1	Z1	A(P)	B(P)	T11	I	H	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

T10	E	G	T11
B8 B7 7 6	B6 B5 5 4	B4 B3 3 2	B2 B1 1 0
n(x) P8 P7 15 14	n(x) P6 P5 13 12	n(x) P4 P3 11 10	n(x) P2 P1 9 8
TS8 TS7 23 22	TS6 TS5 21 20	TS4 TS3 19 18	TS2 TS1 17 16
TC8 TC7 31 30	TC6 TC5 29 28	TC4 TC3 27 26	TC2 TC1 25 24

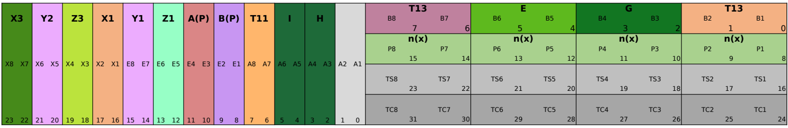
T12 = G*G*rinvpoly
B7 = MontMult(B3,B3,P1) CopyH2H(B1,B7)



X3	Y2	Z3	X1	Y1	Z1	A(P)	B(P)	T11	I	H	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

T12	E	G	T12
B8 B7 7 6	B6 B5 5 4	B4 B3 3 2	B2 B1 1 0
n(x) P8 P7 15 14	n(x) P6 P5 13 12	n(x) P4 P3 11 10	n(x) P2 P1 9 8
TS8 TS7 23 22	TS6 TS5 21 20	TS4 TS3 19 18	TS2 TS1 17 16
TC8 TC7 31 30	TC6 TC5 29 28	TC4 TC3 27 26	TC2 TC1 25 24

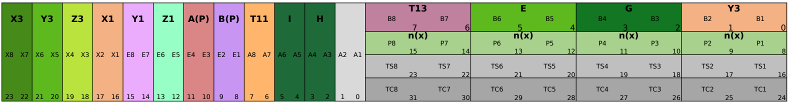
T13 = T12*H*rinvpoly
B7 = MontMult(B7,A3,P1) CopyH2H(B1,B7)



X3	Y2	Z3	X1	Y1	Z1	A(P)	B(P)	T11	I	H	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

T13	E	G	T13
B8 B7 7 6	B6 B5 5 4	B4 B3 3 2	B2 B1 1 0
n(x) P8 P7 15 14	n(x) P6 P5 13 12	n(x) P4 P3 11 10	n(x) P2 P1 9 8
TS8 TS7 23 22	TS6 TS5 21 20	TS4 TS3 19 18	TS2 TS1 17 16
TC8 TC7 31 30	TC6 TC5 29 28	TC4 TC3 27 26	TC2 TC1 25 24

Y3 = T11+T13
X5 = ModAdd(A7,B7,P1) CopyH2V(B1,X5)



X3	Y3	Z3	X1	Y1	Z1	A(P)	B(P)	T11	I	H	
X8 X7	X6 X5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3	A2 A1
23 22	21 20	19 18	17 16	15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0

T13	E	G	Y3
B8 B7 7 6	B6 B5 5 4	B4 B3 3 2	B2 B1 1 0
n(x) P8 P7 15 14	n(x) P6 P5 13 12	n(x) P4 P3 11 10	n(x) P2 P1 9 8
TS8 TS7 23 22	TS6 TS5 21 20	TS4 TS3 19 18	TS2 TS1 17 16
TC8 TC7 31 30	TC6 TC5 29 28	TC4 TC3 27 26	TC2 TC1 25 24

All Steps are:

```
O1 = Z1*Z1*rinvpoly
A3 = MontMult(E5, E5, P1)
CopyH2V(B1, A3)

O2 = Z2*Z2*rinvpoly
B7 = MontMult(X3,X3,P1)
CopyH2H(B1,B7)

A = X1*O2*rinvpoly
B5 = MontMult(X1,B7,P1)
CopyH2H(B1,B5)

B = X2*O1*rinvpoly
B3 = MontMult(X7,A3,P1)
CopyH2H(B1,B3)

T1 = Y1*O2*rinvpoly
B7 = MontMult(E7,B7,P1)
CopyH2H(B1,B7)

C = T1*Z2*rinvpoly
B7 = MontMult(B7,X3,P1)
CopyH2H(B1,B7)

T2 = Y2*O1*rinvpoly
A3 = MontMult(X5,A3,P1)
CopyH2V(B1, A3)

D = T2*Z1*rinvpoly
A3 = MontMult(A3,E5,P1)
CopyH2V(B1, A3)

F = C+D
B7 = ModAdd(B7,A3,P1)
CopyH2H(B1, B7)

E = A+B
A3 = ModAdd(B5,B3,P1)
CopyH2H(B1,B5)

G = E*Z1*rinvpoly
B3 = MontMult(B5,E5,P1)
CopyH2H(B1,B3)

T3 = F*X2*rinvpoly
A3 = MontMult(B7,X7,P1)
CopyH2V(B1,A3)

T4 = G*Y2*rinvpoly
A5 = MontMult(B3,X5,P1)
CopyH2V(B1,A5)

H = T3+T4
A3 = ModAdd(A3,A5,P1)
CopyH2V(B1,A5)

Z3 = G*Z2*rinvpoly
X3 = MontMult(B3,X3,P1)
CopyH2V(B1,X3)

I = F+Z3
A5 = ModAdd(B7,X3)
CopyH2V(B1,A5)

T5 = Z3*Z3*rinvpoly
A7 = MontMult(X3,X3,P1)
CopyH2V(B1,A7)

T6 = apoly_mont*T5*rinvpoly
A7 = MontMult(E3,A7,P1)
CopyH2V(B1,A7)

T7 = F*I*rinvpoly
B7 = MontMult(B7,A5,P1)
CopyH2H(B1,B7)

T8 = T6+T7
A7 = ModAdd(A7,B7,P1)
CopyH2V(B1,A7)

T9 = E*E*rinvpoly
B7 = MontMult(B5,B5,P1)
CopyH2H(B1,B7)

T10 = T9*E*rinvpoly
B7 = MontMult(B7,B5,P1)
CopyH2H(B1,B7)

X3 = T8+T10
X7 = ModAdd(A7,B7,P1)
CopyH2V(B1,X7)

T11 = I*X3*rinvpoly
A7 = MontMult(A5,X7,P1)
CopyH2V(B1,A7)

T12 = G*G*rinvpoly
B7 = MontMult(B3,B3,P1)
CopyH2H(B1,B7)

T13 = T12*H*rinvpoly
B7 = MontMult(B7,A3,P1)
CopyH2H(B1,B7)

Y3 = T11+T13
X5 = ModAdd(A7,B7,P1)
CopyH2V(B1,X5)
```